

Forum:[Hack Forums](#)

Thread: [Need a php backdoor for exploiting xss vulnerable site.](#)

phe0nix404 - February 18, 2016, 4:59 am

Can anyone provide me a php backdoor script for xss exploitation. Or if you can tell me where to find it. It would be a great help.

-Regards.?

p007 - February 18, 2016, 6:48 am

PHP Code

```
<?php
header('XSS-Protection: 0');
print $_GET["str"];
?>
```

phe0nix404 - February 18, 2016, 10:11 am

(Feb 18, 2016 07:48 AM)p007 Wrote: [\[CITE\]](#) PHP Code

```
<?php
header('XSS-Protection: 0');
print $_GET["str"];
?>
```

Thanks man.. Let me try this.

Gee4rce - February 19, 2016, 2:44 am

I do not get what you are trying to achieve,
but with the information given, you have a website that is vulnerable to XSS,
and now want to get in a php Backdoor? If yes, then you are on the wrong path as it doesn't work like that.

Cheers, Gee.

phe0nix404 - February 21, 2016, 7:34 pm

(Feb 19, 2016 03:44 AM)Gee4rce Wrote: [\[CITE\]](#) I do not get what you are trying to achieve,
but with the information given, you have a website that is vulnerable to XSS,
and now want to get in a php Backdoor? If yes, then you are on the wrong path as it doesn't work like that.

Cheers, Gee.

Yes Gee4rce you predicted right. I am still learning these things so can you show me the way where I should proceed? And yeah one more thing I've got hashes from sqlmap and trying to crack it but can't find the answer can you help me on that?

Niko - February 21, 2016, 7:38 pm

(Feb 21, 2016 08:34 PM)phe0nix404 Wrote: [\[CITE\]](#) Yes Gee4rce you predicted right. I am still learning these things so can you show me the way where I should proceed? And yeah one more thing I've got hashes from sqlmap and trying to crack it but can't find the answer can you help me on that?

You can use <http://hashcat.net> to crack hashes.

Or PM them to me, and I'll give them a shot.

phe0nix404 - February 21, 2016, 7:50 pm

Alright let me give a shot to hashcat. ?

Hey Gee4rce while I try to figure out things with hashcat can you also help encrypting that hash? Since I do not have enough credit to PM you I am leaving hash in this reply. I tried to find the hash type but with my poor knowledge i couldn't do that so I am really sorry for giving you so much trouble..

This is the secure hash : 74d0d013fbbf7a7a59cfe3f01603562f

Thank you very much for helping me man.. ?

Niko - February 21, 2016, 8:09 pm

74d0d013fbbf7a7a59cfe3f01603562f:27643@45@#889!

?

Gee4rce - February 22, 2016, 2:15 am

LegitBytes seems to be the man for cracking hashes,
i am not that experienced when it comes to hashcracking.

The thing i can help you with is explaining why a php backdoor doesn't come along with XSS: XSS is always client-sided, meaning if you inject javascript code into a website, it will only be executed at the guy who browses the XSS'ed website. The code will be rendered by his browser, and therefore you will have no code execution on the server side. PHP works server side, so unless you have a vulnerability that works server sided, you can not manipulate the server.

Hope this helped you understanding.

LegitBytes Wrote:74d0d013fbbf7a7a59cfe3f01603562f:27643@45@#889!
Good job man!

Cheers, Gee.

phe0nix404 - February 22, 2016, 4:05 am

(Feb 22, 2016 03:15 AM)Gee4rce Wrote: [\[CITE\]](#) LegitBytes seems to be the man for cracking hashes,
i am not that experienced when it comes to hashcracking.

The thing i can help you with is explaining why a php backdoor doesn't come along with XSS: XSS is always client-sided, meaning if you inject javascript code into a website, it will only be executed at the guy who browses the XSS'ed website. The code will be rendered by his browser, and therefore you will have no code execution on the server side. PHP works server side, so unless you have a vulnerability that works server sided, you can not manipulate the server.

Hope this helped you understanding.

Good job man!

Cheers, Gee.

Really appreciate your help man you set things clear for me.
I'll keep you posted about if this thing of mine work out or not.
Thank you brother.

-Regards.

Gee4rce - February 22, 2016, 5:14 am

(Feb 22, 2016 05:05 AM)phe0nix404 Wrote: [\[CITE\]](#) Really appreciate your help man you set things clear for me.

I'll keep you posted about if this thing of mine work out or not.

Thank you brother. -Regards.

No problem, i'm glad i was able to help you!

Cheers, Gee.

phe0nix404 - February 22, 2016, 11:08 am

Hey folks,

I encountered an issue.

When i try to login with that cracked host I get an error. Are you guys sure it is the correct password?

Gee4rce - February 22, 2016, 11:29 am

How and where are you trying to log in?

SSH or adminpanel, or maybe regular user login?

You could also try things like ftp login or mailgateway.

Maybe you have connected the wrong username with that cracked hash?

Could also be an old DB entry that the admin hasn't removed yet,

i faced non working logins pretty often when hacked DB's.

Cheers, Gee.

phe0nix404 - February 22, 2016, 12:15 pm

(Feb 22, 2016 12:29 PM)Gee4rce Wrote: [\[CITE\]](#) How and where are you trying to log in?

SSH or adminpanel, or maybe regular user login?

You could also try things like ftp login or mailgateway.

Maybe you have connected the wrong username with that cracked hash?

Could also be an old DB entry that the admin hasn't removed yet,

i faced non working logins pretty often when hacked DB's.

Cheers, Gee.

Let me explain..

On the first look the website was dam vulnerable to xss and nothing else but then i run OWASP-ZAP which gave me one url which was vulnerable to sql injection.

So i tried to exploit that and got 2 db entries and one of them contains admin table.

all the admin username and password hashes are there but not admins are heaving full excess but one that i have provided hash string of has " " in the allowed pages column. So I guessed that it has all the excess since is a wildcard.

Alright after that I tried to find admin panel with various scripts and they all pointed to login.php (It could be a wrong page because login.php is really very common name even for a client login page) And this page is same as the customer/client login page. I tried there to login. I very much suspect this page but I wont be able to find another login page.

I know I am doing some noob mistake but I don't know what it is. What should I try to do next?

And yeah one more important thing. I am able to get os-shell through sqlmap.

What are the possibilities with this?

Sorry for giving you so much trouble and for adding you to buddy list without even asking you but It was kind of lonely here so...

FalconGreyHat - February 23, 2016, 6:54 am

this post helped me with a similar problem thanks.

phe0nix404 - April 9, 2016, 7:03 am

@gee4rce No man didn't find any way to login. have the hash for admin that I retrived from sqlinjection but that password doesn't work. I thought its the wrong page from where I tried to login so run dirb and many scripts to find cpanel but no luck. Its like I have the key but not the lock.

And I am sorry I couldn't reply you earlier kind of going through bad time. It would be great if you can find a way to this thing. Might solve many of my problems. And thank you.

-Regards