

Forum:[Hack Forums](#)

Thread: [Mega Hacking Tutorial - Protecting Yourself - Shelling websites completely -Monetize](#)

Crystallize. - May 27, 2018, 12:00 pm

We are only as strong as we are united, as weak as we are divided.

Hello!

I have decided to release mega hacking tutorials. Starting from protecting yourself to shelling a website. These are all written by myself.

In this tutorial we will cover: Setting up VPN to protect yourself.

Finding vulnerable websites

Exploiting the websites

Shelling A.K.A uploading your shell to modify files.

Monetizing

Setting up a VPN to protect yourself

-What is a VPN?

A VPN (Virtual Private Network) is a method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet.

-Why to use a VPN?

Because governments have tracked people down by their IP address, with the help of the person's Internet Service Provider.

Also, online businesses of all kinds monitor activity coming from IP addresses. They may not know your name, but they know you like their website.

This is a MUST before starting the other steps, some webmasters are douchebags and will report your IP to authorities and you will get in trouble.

-Which VPN do you use?

I normally use my private VPN but you can use my VPN - HarborVPN or you can find yourself a FREE one (Not suggested at ALL.)

-What should I do after I connect to a VPN?

First use a website which tells you your IP to see if you actually connected: [WhatIsMyIp](#) this one should work fine.

You also might want to check if your browser is affected by WEBRTC IP LEAK. To do that visit [ExpressVPN WebRTC Leak Test](#) or any other website which tells you if your browser leaks it.

If everything is green you are ready to start. If not look below and I will explain how to prevent the IP leak.

-Preventing WebRTC IP leak.

If you are a firefox user head over to about:config in the search bar. And search for

Code media.peerconnection.enabled and set the value to false.

If you are a google chrome user you can just install "WebRTC Network Limiter" and configure it. Download the addon by clicking this [link](#)

Now visit the webrtc ip leak site and see if your IP leaks if not then you're all setup to move on with the next step.

Crystallize. - May 27, 2018, 12:01 pm

Finding Vulnerable Sites.

SQLi vulnerable pages

-How do we find sites that are vulnerable?

Normally you can use google dorks or you can find your own sites manually. I suggest to use dorks because you can find thousands of vulnerable websites.

-What are dorks?

Dorks are google search strings that reveal login portals and other data. An example how dorks can be used:

inurl:article.php?ID=

This dork will search for sites with /article.php?ID= in the end which you can use to exploit with SQLi. You can make your own dorks easy. By just searching for specific articles, products etc.

Example:

inurl:blabla.php?ID=

This will list all the websites with blabla.php?ID= in google.

Some dorks you can use:

inurl:clanek.php?id=inurl:announce.php?id=inurl:chappies.php?id=inurl:read.php?id=

-How to exploit them?

Normally not every website listed there is vulnerable. If you really have time of the world in hands then you can check them one by one with the ' syntax to see if they throw an error. But if you really like to do things automated, I suggest you use Havij.

-What is Havij?

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

-How to use Havij?

Insert the vulnerable website in the target and click Analyze.

After the process is done click get DBs/Tables/Columns.

After that Havij will sort all gathered tables, you will have to click "Get Columns" this will show all usernames, passwords and other data saved in the table.

In this case we will use only the id, username, password as columns.

After you sort the columns out, login information should show up, most of the times password is encrypted with MD5 which is easy to decrypt. Sometimes password can be in plaintext too or heavily encrypted. Now if we are lucky we will hit MD5/plaintext. I will use MD5 as an example.

You can use the MD5 button in the havij to decrypt the password or you can use an online MD5 decrypter. It's the same!

Now if you know the admin panel you can proceed to login but if you don't then use an online admin panel scanner or the Havij's implemented admin panel scanner.

Done! You now have access to the site's panel! Most of the times they have an upload button so from there you can upload your shell.

Crystallize. - May 27, 2018, 12:02 pm

Exploiting WordPress websites

-Finding Vulnerable WordPress websites.

For that we will use [SE HTML5 Album Audio Player <= 1.1.0 - Local File Include](#) or you can use your own vulns.

You can check if the website is vulnerable to the bug with this code.

site.com/wp-content/plugins/se-html5-album-audio-player/

If the website allows plugins listing it will show files like this:

But if it doesn't list the files you will have to use a tool to scan installed plugins. You can use [ScanWp.net](#) or [HacketTarget.com/wordpress-security-scan/](#)

The site I am using is vulnerable to the exploit so we will carry on.

I will use the payload:

Code

`https://site.com/wp-content/plugins/se-html5-album-audio-player/download_audio.php?file=/wp-content/uploads/../../wp-config.php`

This will download the wp-config.php file where the DB information is saved.

After downloading the wp-config.php , open it with notepad or notepad++ and you should see DB infos.

Now I will take the password and login via site.com/wp-admin/.

Usually the username is "admin".

VOILA!! IM IN.

Uploading Shells in WordPress.

There are many ways to upload shells in wordpress but I will explain my method which is the easiest.

Head over to Plugins>Editor

Pick one of the plugins listed, paste your own upload code and click save.

So we go to the plugin page `wp-content/plugins/pluginname/xxx.php`
in my case its(I only put a simple uploader in the code but you can put a shell script or anything)
Code `xxx/wp-content/plugins/woocommerce/i18n/locale-info.php[*]`

You've uploaded your shell in less than 2 minutes. ?

As a bonus I will add my half-ass working python scanner to identify if website is wordpress.S/O Elitas.

```
Code import requestswith open("websitelist.txt") as f: for url in f: try: r =
requests.get(url) if "wp-content" in r.text: print("Wordpress detected: " + url)
else: continue except: continueYou will need a websitelist.txt in the same
folder as the python script.
```

Crystallize. - May 27, 2018, 12:02 pm

Shelling Joomla websites

In this step I will not explain how to find Joomla websites but instead only the shelling part, sorry.
After you have found your target most of the times the admin panel is `/administrator/` and the
user/admin are "admin|123456" or "admin|password" etc.You can use a bruteforcer to find the
username and password.

After logging in the admin panel head over to "Media" the website I am using is in Italian sorry ?

Head over to options to see if PHP uploading is allowed:

Now if it allowed it will be shown under there but if not then just add 'php' under there.

Now you can upload your shell directly or use an uploader, the directory where the file are being
uploaded in this case is `site/images/` so the shell would be like `/site/images/shellname.php`

This was all folks, in the next days I will add more methods to exploit vulnerable sites.
Enjoy. ?

Source/s:

Code Wiki

Images of Havij are borrowed from another tutorial (only the images nothing else).

Crystallize. - May 27, 2018, 12:28 pm

-How to monetize?

First you would have to register at [CoinHive](#)

Coinhive is a Crypto Miner for websites. It mines XMR via the traffic.

After signing up head over to copy the javascript code at "Documentations".

Replace the site key with yours. You can get your API key from "Settings".

Now you can put it in index.php of the shelled websites.

Or you can sell the shells!

Enjoy! ?

Elitas - May 27, 2018, 12:54 pm

Looks really nice! Good job Cryst.

2Chode2Furious - May 27, 2018, 12:55 pm

I read the whole thing and it's pretty damn solid. Quality tutorial.

+1

Elitas - May 27, 2018, 12:58 pm

EDIT: For the wordpress one, you dump the database information, but then assume the password is the same?

I think you should try directly connecting to their database (there are sites to try and remotely login to a site's MySQL), from there you can dump the database and crack the hashes.

BTW, don't say 'decrypt MD5', as that's obviously not possible, you need to CRACK an MD5 hash! Really great tutorial though for those of you looking to immediately get into a hands on experience of web exploitation. Wish I saw this type of stuff when I was a newbie, so I could practice. Remember though, practicing on other people's sites are illegal, and you are fully responsible for that yourself. We would recommend you do this WITH WEBSITE OWNER'S PERMISSION, but personally we don't give a shit what you do in your spare time, so have fun.

Exodus - May 27, 2018, 1:00 pm

Damn high quality tutorial, would +1 rep but i'm not upgraded.

SIM-1589588 - May 27, 2018, 2:28 pm

Great tutorial, need to be stucked in this forum :)

Crystallize. - May 27, 2018, 3:39 pm

Thank you everyone.I hope you learn something from one of these!

Condescend - May 27, 2018, 5:41 pm

Very good post. Will definitely help those in need of quick insight into WebApp pentesting.

Crystallize. - May 27, 2018, 5:54 pm

(May 27, 2018 05:41 PM)Condescend Wrote: [\[CITE\]](#) Very good post. Will definitely help those in need of quick insight into WebApp pentesting.

Indeed and thanks!

I am planning to make #2 version sometime soon with more exploits/informations etc.

Condescend - May 27, 2018, 6:01 pm

(May 27, 2018 05:54 PM)Crystallize. Wrote: [\[CITE\]](#) Indeed and thanks!

I am planning to make #2 version sometime soon with more exploits/informations etc.

That's a really good idea. I know Mr. Robot was doing a massive mega tutorial or something similar to this, but it went unfinished.

I feel like you could make a lot of threads on this topic, since Web pentesting is so attractive to some.

Crystallize. - May 27, 2018, 6:02 pm

(May 27, 2018 06:01 PM)Condescend Wrote: [\[CITE\]](#) That's a really good idea. I know Mr. Robot was doing a massive mega tutorial or something similar to this, but it went unfinished.

I feel like you could make a lot of threads on this topic, since Web pentesting is so attractive to some.

I could ask Robot to do it together if he wants.But not many people are getting interested in hacking nowadays. :(

Condescend - May 27, 2018, 6:07 pm

(May 27, 2018 06:02 PM)Crystallize. Wrote: [\[CITE\]](#) I could ask Robot to do it together if he wants.But not many people are getting interested in hacking nowadays. :(

Well, that is true realistically; at least if you are looking into the general spectrum of people wanting to learn hacking and/or penetration testing. We get a lot of those people who want a quick hack for Facebook, and then book it when they don't know what to do.

It would definitely be helpful to the spectrum who aren't actually braindead though. ;)

`RaZoR - May 28, 2018, 12:44 am

great tutorial, I don't think its better use Havij just my opinion.

you could explain something ethical blue teaming, red teaming, etc..

WhiteYeti - May 28, 2018, 3:53 am

Some suggestions on practical web application vulnerabilities that we actually see "in the wild" on assessments:

-XXE (Server Side Request Forgery in general)

- XSS (both stored and reflected, maybe some evasive methods to bypass WAFs)
- CSRF (practical example for priv esc or password change upon header manipulation)
- SQLi (blind, time-based application and enumerating DB table names and contents through this)

Good web app vulns for beginners to look out for!

Crystallize. - May 28, 2018, 3:54 am

Thank you guys.

I will add more it's just matter of time.I cannot cover all the topics alone.

The_Defiant_One - May 28, 2018, 6:32 am

Great tutorial here. Looking forward to 2 version or any more to come. Thanks for sharing.

Crystallize. - May 30, 2018, 6:17 am

(May 28, 2018 06:32 AM)The_Defiant_One Wrote: [\[CITE\]](#) Great tutorial here. Looking forward to 2 version or any more to come. Thanks for sharing.

I believe tomorrow everything should be ready.Thanks!

sharkkiller - June 10, 2018, 9:57 pm

Great tutorial, need to be stucked in this forum

Crystallize. - June 13, 2018, 6:49 pm

I will probably release part 2 some time this week.

Meanwhile enjoy this and throw me some green apples.<3

the princess - June 13, 2018, 7:10 pm

Very well made guide! sqlmap is another tool for those that don't like/want to use havij, though a bit more complicated to use (Not difficult though!) :)

gotta go - June 13, 2018, 11:21 pm

Thank you sir, that is useful

Crystallize. - June 16, 2018, 6:20 pm

Thank you both for your kind comments.Hope you learned something!

Crystallize. - June 20, 2018, 4:44 pm

Just information for everyone:

Part 2 is coming real soon.

Ahmed El Melegy - June 21, 2018, 3:17 am

wow good work Crystallize.

Crystallize. - June 25, 2018, 5:08 am

(Jun 21, 2018 03:17 AM)Ahmed El Melegy Wrote: [\[CITE\]](#) wow good work Crystallize.
Thank you.

Part 2 is almost finished, stay tuned!

TheChi?f - June 25, 2018, 8:13 am

<http://www.creedsec.net/2013/01/hacking-website-using-sql-injectionfull.html>

Nice job.

Crystallize. - June 25, 2018, 8:16 am

(Jun 25, 2018 08:13 AM)TheChi?f Wrote: [\[CITE\]](#)

<http://www.creedsec.net/2013/01/hacking-website-using-sql-injectionfull.html>

Nice job.

??

I said photos are borrowed smartass.

pharaoh6ways - June 29, 2018, 8:55 pm

Lots of VPN are not strong and they say they are because they barely get you into any dating sites without being detected at first sight, anyone with a good suggestion kindly help a brother out ,Thanks

CreativeHold - July 1, 2018, 10:23 am

Thank you very much for the HQ guide. I am very new to learning and this will def. help me!