

Forum:[Hack Forums](#)

Thread: [I want to become a grey hat!](#)

B?ue - January 13, 2014, 12:33 pm

Hi!

I'm not new to hacking, but I'm still very basic, and I probably know what your thinking "oh god another 12 year old skid has found this site and wants to be some anon ub3r l33t h4cker" but trust me I'm not.

My friend set up a website recently so i helped him out but doing a couple of SQLi tests on it and I helped him fix it, however those were really basic. like hackthis level 1 and 2 quality. I'm just wondering does anybody have any guides that can teach me ALOT more about SQLi and javascript weak spots that can be easily exploited. I wanna run a small service(nothing big), for free in which, at request, I "hack" websites then tell the founders how I did it.

Thanks in advance!

tux1 - January 13, 2014, 12:35 pm

Before you can learn "sqli and javascript weak spots"

You need to learn SQL and javascript. Once you have an understanding of how they work then you ill understand how exploits work.

B?ue - January 13, 2014, 12:38 pm

(Jan 13, 2014 01:35 PM)tux1 Wrote: [\[CITE\]](#) Before you can learn "sqli and javascript weak spots"

You need to learn SQL and javascript. Once you have an understanding of how they work then you ill understand how exploits work.

Thanks for reply! can you link me to a couple of guide on here or anywhere that will help alot?

Kerberos - January 13, 2014, 1:45 pm

You dont just learn to hack. You need to have in-depth technical understanding of the systems you wish to exploit. Learn Linux, learn to install drivers, compile binaries, start writing little bash scripts to automate things for you. Learn how windows server works and the different services. Know how DNS, DHCP, LDAP, etc work. Learn the TCP/IP stack and the OSI model. Play with some SQL Databases, learn to write scripts to read and write to them. Pickup some Python, Perl, Java, etc. Set up labs to practice...

Thats a good place to start, then work up from there, tere are too many skids on HF, dont be another statistic ?

Basically, if you want to ever be a decent hacker, you need to be well-rounded IT professional, whether its a job or a hobby, you are going to need to know some shit, then worry about hacking.

B?ue - January 13, 2014, 2:07 pm

(Jan 13, 2014 02:45 PM)Kerberos Wrote: [\[CITE\]](#) You dont just learn to hack. You need to have in-depth technical understanding of the systems you wish to exploit. Learn Linux, learn to install drivers, compile binaries, start writing little bash scripts to automate things for you. Learn how windows server works and the different services. Know how DNS, DHCP, LDAP, etc work. Learn the

TCP/IP stack and the OSI model. Play with some SQL Databases, learn to write scripts to read and write to them. Pickup some Python, Perl, Java, etc. Set up labs to practice...

Thats a good place to start, then work up from there, tere are too many skids on HF, dont be another statistic ?

Basically, if you want to ever be a decent hacker, you need to be well-rounded IT professional, whether its a job or a hobby, you are going to need to know some shit, then worry about hacking. I already know alot about some of the things you have mentions, I can do driver installation, and compile binaries, as well as extremely basic stuff like batch files. As far as servers and stuff go, I only have hardware knowledge. I've been studying computer hardware (and electrical engineering which despite being completely different, have some overlapping topics) so like I said, I know the basics, however searching on youtube and google, alot of the guides I find are either too basic and I already know it, or its too complex.

thanks alot for the tips anyway! Im here to learn stuff, Can't stand skids they just get everyone to work for them ?

Natalie Portman - January 13, 2014, 9:56 pm

First of all, download a KaliLinux distribution if you're looking to become a pentester. It has a vast suite of tools which will all prove useful to you.

Second, learn C, C++, Python, and Java. NOT. JAVASCRIPT.

Java is not Javascript. Don't learn JS, it's a waste of time.

Then, I'd move onto launching remote attacks using suites like MSF, Armitage, Cobalt Strike, etc. etc. From Kali Linux.

SQLi, XSS, LFI, RFI are all small-time when it comes to attacking real websites.

What you're looking for is a vulnerability in an application which the website is running, for that I recommend going to exploit-db.

They have a list of most exploits that aren't private and you should be able to search an application and it's version if it's outdated, and find a remote exploit which will yield some kind of result.

Also, install Acunetix WVS, and run a scan of the site, it's great for finding vulnerabilities.

If you have any other issues, PM me.

ykrajina_boy - January 14, 2014, 10:14 am

I recommend reading hacking for dummies. good book for beginners. It also has a lot of tools. One of the first hacking books i read- itly help u get started

Pentatonic - January 18, 2014, 10:20 am

(Jan 13, 2014 10:56 PM)illustrious Wrote: [\[CITE\]](#) First of all, download a KaliLinux distribution if you're looking to become a pentester. It has a vast suite of tools which will all prove useful to you.

Second, learn C, C++, Python, and Java. NOT. JAVASCRIPT.

Java is not Javascript. Don't learn JS, it's a waste of time.

Then, I'd move onto launching remote attacks using suites like MSF, Armitage, Cobalt Strike, etc.

etc. From Kali Linux.

SQLi, XSS, LFI, RFI are all small-time when it comes to attacking real websites.

What you're looking for is a vulnerability in an application which the website is running, for that I recommend going to exploit-db.

They have a list of most exploits that aren't private and you should be able to search an application and it's version if it's outdated, and find a remote exploit which will yield some kind of result.

Also, install Acunetix WVS, and run a scan of the site, it's great for finding vulnerabilities.

If you have any other issues, PM me. Double facepalm...

-JavaScript is a waste of time?

Yes of course when the 99% of today's website use JavaScript, JS is a waste of time. Legit idea! XSS without JavaScript isn't possible.

-Second, learn C, C++, Python, and Java.

Which of these languages will help him understand the attacks behind web applications? C probably or maybe ASM? Hmmm?

Devisual - January 18, 2014, 11:40 am

I recommend reading hacking for dummies. good book for beginners. It also has a lot of tools, and don't be afraid of asking people for help that's my advice. Goodluck

-Devisual

Natalie Portman - January 18, 2014, 1:31 pm

(Jan 18, 2014 11:20 AM)Pentatonic Wrote: [\[CITE\]](#) Double facepalm...

-JavaScript is a waste of time?

Yes of course when the 99% of today's website use JavaScript, JS is a waste of time. Legit idea! XSS without JavaScript isn't possible.

-Second, learn C, C++, Python, and Java.

Which of these languages will help him understand the attacks behind web applications? C probably or maybe ASM? Hmmm?

lol looks like u got rolled xddd

lol at you buttlbasted

x\$pl0it - January 18, 2014, 1:51 pm

(Jan 13, 2014 03:07 PM)Lesky Wrote: [\[CITE\]](#) I already know a lot about some of the things you have mentioned, I can do driver installation, and compile binaries, as well as extremely basic stuff like batch files. As far as servers and stuff go, I only have hardware knowledge. I've been studying computer hardware (and electrical engineering which despite being completely different, have some overlapping topics) so like I said, I know the basics, however searching on youtube and google, a lot of the guides I find are either too basic and I already know it, or it's too complex.

thanks a lot for the tips anyway! I'm here to learn stuff, Can't stand skids they just get everyone to work for them ?

Electrical engineering is good if you want to get in to hardware hacking.

jimi123 - *January 18, 2014, 8:27 pm*

If you succeed, please contact me. I need some good web database