

Forum:[Hack Forums](#)

Thread: [Need Help Hacking a Website \[Wanna know if it's Possible & Wanna Learn the Skills\]](#)

Exodian - July 24, 2015, 11:22 pm

Hey Guys, Just to get a couple of things straight, im not a complete noob when it comes to hacking ect. But I do need help sometimes.

I was recently into searching up how to attack/hack websites. Like sql injections, xss and stuff like that. So i went on a website to try it out and found the website wasn't vulnerable to any of these methods. But I'm pretty sure it's very insecure. I scanned the website using vega v1.0 (Kali linux) and it said it had heaps of stuff (but could be also false-positives, but the problem is i don't know if they are and need to try them out but don't know how to) which include,

.Cleartext Password over http (The site is also using http, not https which might come in handy while sniffing for passwords and stuff, but people would rarely login to the site)

.Cross-Site Script Include (Pretty sure that means the site is vulnerable to xss)

.Possible Social Security Number Detected (Not needed)

.Possible SQL-Injection (Think this is a false-positive)

and many more in the High Risk section. Im wondering how would I use these vulnerabilities if they aren't false-positives, and if you manage to hack/gain control of this website, please let me know how. I was just wondering are there any ways of hijacking, dns spoofing, or hacking the website for me to display a particular html line of code. I'm simply trying to do this attack to learn more about hacking and attacks in general & also to gain an understanding on scanning then exploiting a particular vulnerability.

It would be awesome for someone to respond with some feedback or help on how to actually do this attack on the site.

Also, if you think I am doing things wrong like using vega or something, let me know, and tell me how you guys do stuff :D

Quick Vega Scan (Not a full scan of it, there are a lot more vulneranbilties): prntscr.com/7wqugk

Website trying to gain access to: cccgympie.qld.edu.au

Email me: digitalaeofficial@gmail.com

Skype: [exodian_exodus](#)

PhantomElite - July 25, 2015, 12:04 am

the first rule above all with scanners if you ARE going to use them is to know what the hell you're scanning FOR

read Web Application Hacker's Handbook, 2nd Edition is an amazing book you want to read to know your shit about web app sec.

or google for tutorials

Exodian - July 28, 2015, 1:36 am

I just wanted to know how I would actually do these sorts of attacks ect. The scanning part was to give people an idea of the website i'm looking at to explain what this website could potentially be vulnerable to and to hack. It doesn't matter if i do or don't know what im scanning for, im scanning for vulnerabilities and thats all I need to know. I was just wondering if anyone could actually get into or show me how to find these vulnerabilities and how to get into this certain website.

N0c7urn - July 28, 2015, 2:03 am

If the scan shows it has vulnerabilities, google the vulnerability. Thats the best way

Exodian - July 28, 2015, 2:22 am

Yes I know that, but i was wondering if they were false-positives and if the site was actually vulnerable to them. Because vega shows for example "this site has 32 vulnerabilities of cross-site scripting" or whatever, and i search up how to xss and you need a text box to like enter javascript ect when the website doesn't have one. So how can I xss? I can't can I?

PhantomElite - July 28, 2015, 2:35 am

Web Application Hacker's Handbook, 2nd Edition

that is all

Exodian - July 28, 2015, 2:44 am

Lel, Ok, I hate reading books, but love reading information! Sucks but good at the same time. Hacking Requires time, which I get unlike some script kiddies who just want a quick short answer xD

PhantomElite - July 28, 2015, 3:02 am

you hate reading books but love reading information

books ARE information

Exodian - July 28, 2015, 6:10 pm

Sorry I put that the wrong way, I meant to say that I hate reading fictional books, like stories and stuff, but love reading information. Lel soz

XPRMX - July 28, 2015, 6:21 pm

This is a christian college ffs. Respect their religion and its a school website.

Exodian - July 28, 2015, 6:31 pm

Dude, that site was just an example, because i am at the school. Im am a christian and wanted to learn the skills to do it. You can take my word for it but I am a white hat hacker. Planning to get a CEH when I leave this school. So I am just curious to see was kind of holes the school has and stuff, and how I would get about doing that. Like I said I scanned using VEGA in kali linux and it said it has heaps of vulnerabilities that could be exploitable. It's just that I wanna know how I would go about figuring out how to exploit these. Information = Power. I do respect their religion/my religion.

I have just always wanted to know. Because shitty Youtube Videos don't actually show you real life targets, all they do is find vulnerable SQL injection websites. They usually don't show you how to find an vulnerabilities, test if it's a false-positive, then exploit it if it's not. Hopefully you get what Im saying and Im not trying to bring any harm to anyone, that website was just an example.

XPRMX - July 28, 2015, 6:37 pm

(Jul 28, 2015 06:31 PM)Exodian Wrote: [\[CITE\]](#) Dude, that site was just an example, because i am at the school. Im am a christian and wanted to learn the skills to do it. You can take my word for it but I

am a white hat hacker. Planning to get a CEH when I leave this school. So I am just curious to see what kind of holes the school has and stuff, and how I would go about doing that. Like I said I scanned using VEGA in kali linux and it said it has heaps of vulnerabilities that could be exploitable. It's just that I wanna know how I would go about figuring out how to exploit these. Information = Power. I do respect their religion/my religion.

I have just always wanted to know. Because shitty Youtube Videos don't actually show you real life targets, all they do is find vulnerable SQL injection websites. They usually don't show you how to find an vulnerabilities, test if it's a false-positive, then exploit it if it's not. Hopefully you get what Im saying and Im not trying to bring any harm to anyone, that website was just an example. White hats dont exploit their own school....

Quote:then exploit it if it's not

Exodian - July 28, 2015, 7:27 pm

It's no illegal in any way, shape or form to find exploits and report them to the school. It only become illegal if u gain further access to things such as personal information and stuff using the exploit. The reason is because I don't wanna scan all these vulnerabilities and see they are false-positives. You should see what im saying here. Thats exactly what ethical hacking is, Im in Australia by the way so law might be different from where u r from. :P But from what I have read, finding an exploit and confirming it works to gain access to whatever, isn't illegal at all. Unless u actually use that to gain access.

If you still do not agree with me I would love to know your definition of what a white hat hacker/ethical hacker [Qualified] would do to find any vulnerabilities for a school website.

Im not here to argue, even if I was doing this for illegal purposes (which im clearly not) it wouldn't matter because people tell others how to do illegal shit on hf all the time xD. Im simply wanting to learn how to do things to help further security and to get a better understanding of black hats (Pretty much the main purpose of an Ethical Hacker)

PhantomElite - July 28, 2015, 7:41 pm

(Jul 28, 2015 07:27 PM)Exodian Wrote: [\[CITE\]](#) It's no illegal in any way, shape or form to find exploits and report them to the school. It only become illegal if u gain further access to things such as personal information and stuff using the exploit. The reason is because I don't wanna scan all these vulnerabilities and see they are false-positives. You should see what im saying here. Thats exactly what ethical hacking is, Im in Australia by the way so law might be different from where u r from. :P But from what I have read, finding an exploit and confirming it works to gain access to whatever, isn't illegal at all. Unless u actually use that to gain access.

If you still do not agree with me I would love to know your definition of what a white hat hacker/ethical hacker [Qualified] would do to find any vulnerabilities for a school website.

Im not here to argue, even if I was doing this for illegal purposes (which im clearly not) it wouldn't matter because people tell others how to do illegal shit on hf all the time xD. Im simply wanting to learn how to do things to help further security and to get a better understanding of black hats (Pretty much the main purpose of an Ethical Hacker)

Speaking from a US perspective here.

Exploiting is most certainly illegal. It's not just if you access personal information or anything. Hell, companies even tried to pursue people for port scans (which, by the way, are 100% legal).

If you gain access you have committed a felony, if not multiple ones.

EXTREMELY GRACIOUS companies like Microsoft have been so merciful! They promised not to prosecute people for reporting vulnerabilities.

Fuck, it might even be illegal for you to enter 1' lol. Don't get it twisted.

Skorn Virus - July 28, 2015, 7:48 pm

(Jul 28, 2015 07:27 PM)Exodian Wrote: [\[CITE\]](#) It's no illegal in any way, shape or form to find exploits and report them to the school. It only become illegal if u gain further access to things such as personal information and stuff using the exploit. The reason is because I don't wanna scan all these vulnerabilities and see they are false-positives. You should see what im saying here. Thats exactly what ethical hacking is, Im in Australia by the way so law might be different from where u r from. :P But from what I have read, finding an exploit and confirming it works to gain access to whatever, isn't illegal at all. Unless u actually use that to gain access.

If you still do not agree with me I would love to know your definition of what a white hat hacker/ethical hacker [Qualified] would do to find any vulnerabilities for a school website.

Im not here to argue, even if I was doing this for illegal purposes (which im clearly not) it wouldn't matter because people tell others how to do illegal shit on hf all the time xD. Im simply wanting to learn how to do things to help further security and to get a better understanding of black hats (Pretty much the main purpose of an Ethical Hacker)

Unless you're a hired pentesting forensics who is purposely searching for holes in there security then no it's legal by all means. But if you're some random guy on a computer saying "HEY ima hack this site just to see if I can" and if you're detected by a IDS or a firewall in general then of course you're going to be reported or in short "illegaly" attempting to get into the site.

Also Black hats != Ethical hackers. Ethical hackers only need to know the information black hackers know just so they can more easily reverse engineer the damage done because if you know how something works. You can easily break it down and remove it.

Exodian - July 28, 2015, 8:07 pm

I get what you guys are both saying. I understand facebook & microsoft pay people to find exploits and stuff for their websites. Just to clear things up i'm no expert, but I honestly don't think for example if you find a site has an SQL injection vulnerability, and then proceed to tell the school admins (because this is in my case not saying this is true for all circumstances) they will not think at all it's illegal, but your trying to help secure it. If you did find a SQL injection vulnerabilities, then from experience you know that you could get into a database ect, that's no illegal at all. I'm like 100% positive. But what I was asking, was to know how to actually scan, then exploit (use) that vulnerability, some might say thats illegal, but I find that it's not as long as I don't do anything malicious or access any important stuff.

In some peoples eyes gaining access to something that isn't yours is probably illegal, yes, but if I just know how to actually use the exploit, I will definitely know how to prevent it on websites. So this website I had was just a test to see, and how to exploit a vulnerability for a scan. Some might see it illegal, I don't if Im helping them out honestly.

[Also, Im not a hacker saying, "Lets see if I can hack this to see if I can!", im more like "I wonder how hackers gain access, (searches up couple of methods) oh ok, but then how do I use this to gain access (for example gains access) ok sweet, now I know how this works, so now I can tell the owners of the website, and I know how to prevent it from blocking this method" which is what Im kinda like (while doing this learning a new skill)

PhantomElite - July 28, 2015, 8:10 pm

They do not need to "think" it's illegal- it is.

Yes. It is illegal. Go read a few chapters on hacking law.

What the fuck are you rambling on about how "in some peoples eyes"- it IS illegal. That is a FACT not an OPINION.

It's not some people "seeing" it as illegal jesus fucking christ.

You're confusing ethical behavior with legality.

Is it really unethical to exploit something with benign intentions to help get the problem fixed? No. Is it illegal? Yes.

Exodian - July 28, 2015, 8:24 pm

Calm down xD, I though you would know what I mean in some peoples eyes, or think it's illegal. But clearly I need to explain it to you. When you are talking about actual law, yes it's illegal. But in some peoples eyes it might not, and they might find it's helping them. So when I say in some peoples eyes, I mean some people won't find it to be a bad, illegal thing, and might find it to be a good thing and not try and charge you for it. Laws like that are in place for malicious people, not necessarily people helping out, and whats your defintion of Ethical Hacking, how is an Ethical Hacker meant to go about doing this type of stuff, without directly being hired by the company, legally.

Please don't tell me they can't, because they most certainly can. My definition is that as long as they find an exploit, and report it, there is nothing illegal about that. But if they use/gain access to the site through the exploit, then later tell the owners about it, ye that is. If you find an exploit, that's not illegal at all.

I do admit what Im trying to learn is by law, Illegal. But I find it morally to be right (Learning a skill to prevent people who actually wanna use the exploit maliciously. Because you would rather someone report an exploit, than leaving it until a black hat comes around and reks u). Still, why am I being lectured about law when I just wanted to know how to do something to a website xD Hundreds of people ask way more illegal shit than legal on hf. So ye xD Imfao

PhantomElite - July 28, 2015, 8:30 pm

holy fuck can you just learn what the word "legal" means

legal is in relation to the LAW

not ethics

not morales

the LAW

"i think recreational weed is legal all across the US" like what the fuck use your brain

il·le·gal

i(l)'leg?l/

adjective

adjective: illegal

1.

contrary to or forbidden by law, especially criminal law.

Exodian - July 28, 2015, 9:23 pm

Dude wtf, xD I never said it was legal, I said morally some people might find it to be helpful. Some people don't agree with the law and have there own opinion and morals on whats right and wrong.

Clearly twelve because you can't read what I wrote. I didn't write all of that for nothing xD

(Also, hate to be a grammar nazi but like, spell right before you like insult me.)

PhantomElite - July 28, 2015, 9:32 pm

(Jul 28, 2015 09:23 PM)Exodian Wrote: [\[CITE\]](#) (Also, hate to be a grammar nazi but like, spell right before you like insult me.)

holy crap i don't even know someone could be this obviously ignorant

(Jul 28, 2015 09:23 PM)Exodian Wrote: [\[CITE\]](#) Clearly twelve because you can't read what I wrote.

(Jul 28, 2015 09:23 PM)Exodian Wrote: [\[CITE\]](#) I didn't write all of that for nothing xD
even when you're criticizing my grammar you say "but like"

you have fucking dozens of grammar mistakes all over your post from not capitalizing Facebook to missing apostrophe's and you try to call someone out on grammar lmao

Exodian - July 28, 2015, 9:40 pm

Sorry Man, I was really looking for a response on what I said, not about my grammar. Only reason I was pointing you out was because you were insulting me. Got any comments on what I actually said? xD lmfao

abyhfnw - July 28, 2015, 9:41 pm

I want to know how to hack Gmail and Instagram

PhantomElite - July 28, 2015, 9:58 pm

(Jul 28, 2015 09:40 PM)Exodian Wrote: [\[CITE\]](#) Sorry Man, I was really looking for a response on what I said, not about my grammar. Only reason I was pointing you out was because you were insulting me. Got any comments on what I actually said? xD lmfao

yes you have no idea what the word illegal means

Exodian - July 28, 2015, 10:04 pm

I think I do, but anyways, can someone reply on how I would do this xD