

Forum:[Hack Forums](#)

Thread: [Finding exploits in websites](#)

Triops - June 20, 2016, 8:04 pm

How would I got about finding an exploit in a website I plan on trying to hack? I know about pentesting and all of that, but other than that, what are other ways of doing it? I also know of finding vulns in products they use like OpenCart.

Any tips would be appreciated.

Essence - June 20, 2016, 8:16 pm

Good starter for people like you is Sqlmap. Download Kali Linux and install it on a virtual machine and lookup some tutorials.

Triops - June 20, 2016, 8:25 pm

(Jun 20, 2016 08:16 PM)? ?????????? ? Wrote: [\[CITE\]](#) Good starter for people like you is Sqlmap. Download Kali Linux and install it on a virtual machine and lookup some tutorials.

I've already tried using SQLmap, none of the urls on the site or the store page are injectable. Unless i'm missing something entirely obvious. I've also tried XSS but haven't gotten anything yet

Insurmountable - June 20, 2016, 10:38 pm

A great idea when trying to hack a site is identifying what plugins / web frameworks they are running (in this case it's OpenCart) and then searching for exploits on a site like exploit-db.com

Example: I found a remote code execution exploit for OpenCart versions 2.1.0.2 to 2.2.0.0
URL: exploit-db.com/exploits/39679/

If that one doesn't work you can keep looking for more at exploit-db.com/search

Teferi - June 21, 2016, 6:44 am

(Jun 20, 2016 08:25 PM)Triops Wrote: [\[CITE\]](#) I've already tried using SQLmap, none of the urls on the site or the store page are injectable. Unless i'm missing something entirely obvious. I've also tried XSS but haven't gotten anything yet

"Unless i'm missing something entirely obvious." are you sure the URL's you blindly enter in SQLmap are even vulnerable?..

Triops - June 21, 2016, 9:07 am

(Jun 20, 2016 10:38 PM)Insurmountable Wrote: [\[CITE\]](#) A great idea when trying to hack a site is identifying what plugins / web frameworks they are running (in this case it's OpenCart) and then searching for exploits on a site like exploit-db.com

Example: I found a remote code execution exploit for OpenCart versions 2.1.0.2 to 2.2.0.0
URL: exploit-db.com/exploits/39679/

If that one doesn't work you can keep looking for more at exploit-db.com/search

Yeah, I already saw that exploit on another site and I even know how to do it myself, but I was hoping for one that wouldn't require the admin to have to look at a page for it to take effect.

Dark TruTH - June 21, 2016, 10:28 am

(Jun 20, 2016 08:04 PM)Triops Wrote: [\[CITE\]](#) How would I got about finding an exploit in a website I plan on trying to hack? I know about pentesting and all of that, but other than that, what are other ways of doing it? I also know of finding vulns in products they use like OpenCart.

Any tips would be appreciated.

Man try to hack other sites hosted on that server using sql injection and then use symlink to access the config file of the your target site and get there mysql uname and pass from the config file....

Disparity - June 21, 2016, 10:31 am

(Jun 20, 2016 08:16 PM)OhEssence Wrote: [\[CITE\]](#) Good starter for people like you is Sqlmap. Download Kali Linux and install it on a virtual machine and lookup some tutorials.

Please please please please please please please please please please please please please please please please pleaseNo

OP, let me tell you this: If you want to be a 'hacker', an actual hacker, who doesn't just run acunetix or use dorks, learn PHP, SQL, and Javascript. I want to be a good 'hacker', so that's what I'm doing too.

Don't listen to anyone who instantly refers you to using fucking Kali linux. 100% guarantee they know nothing.

Cxdde3990xc - June 21, 2016, 10:35 am

(Jun 20, 2016 08:16 PM)OhEssence Wrote: [\[CITE\]](#) Good starter for people like you is Sqlmap. Download Kali Linux and install it on a virtual machine and lookup some tutorials.

Terrible Terrible advice

Triops - June 21, 2016, 10:35 am

(Jun 21, 2016 10:31 AM)Disparity Wrote: [\[CITE\]](#) Please please please please please please please please please please please please please please please please pleaseNo

OP, let me tell you this: If you want to be a 'hacker', an actual hacker, who doesn't just run acunetix or use dorks, learn PHP, SQL, and Javascript. I want to be a good 'hacker', so that's what I'm doing too.

Don't listen to anyone who instantly refers you to using fucking Kali linux. 100% guarantee they know nothing.

I'm already learning PHP as a developer on a small social networking site. I know some basics of SQL and Javascript already, just need to refreshen my memory.

(Jun 21, 2016 10:28 AM)Dark TruTH Wrote: [\[CITE\]](#) Man try to hack other sites hosted on that server using sql injection and then use symlink to access the config file of the your target site and get there mysql uname and pass from the config file....

They are hosted on a dedicated server so i'm not sure that's possible to do.

Elitas - June 21, 2016, 10:42 am

(Jun 21, 2016 10:31 AM)Disparity Wrote: [\[CITE\]](#) Please please please please please please please please please please please please please please please please pleaseNo

OP, let me tell you this: If you want to be a 'hacker', an actual hacker, who doesn't just run acunetix or use dorks, learn PHP, SQL, and Javascript. I want to be a good 'hacker', so that's what I'm doing too.

Don't listen to anyone who instantly refers you to using fucking Kali linux. 100% guarantee they know nothing.

Although I agree with you, Kali Linux is still used by people like myself who know PHP, mySQL and Javascript.

tbh i dont use it that much... but it's still pretty useful.

i wouldnt rule it out is all.

STRYAN - June 21, 2016, 10:52 am

(Jun 21, 2016 10:31 AM)Disparity Wrote: [\[CITE\]](#) Please please please please please please please please please please please please please please pleaseNo

OP, let me tell you this: If you want to be a 'hacker', an actual hacker, who doesn't just run acunetix or use dorks, learn PHP, SQL, and Javascript. I want to be a good 'hacker', so that's what I'm doing too.

Don't listen to anyone who instantly refers you to using fucking Kali linux. 100% guarantee they know nothing.

Out of any advice the above is probably best if im honest.

I know asking for advice is good but... learning yourself and giving yourself that buzz of "ive done something good" will make you feel alot better rather than getting someone else to spoon feed you. GG Disparity

Disparity - June 21, 2016, 11:33 am

(Jun 21, 2016 10:42 AM)xHackerPr0 Wrote: [\[CITE\]](#) Although I agree with you, Kali Linux is still used by people like myself who know PHP, mySQL and Javascript.

tbh i dont use it that much... but it's still pretty useful.

i wouldnt rule it out is all.

I'm not saying Kali linux is useless. I'm saying some of the worst advice you can give to someone looking to start hacking is to go straight to kali.

Elitas - June 21, 2016, 3:17 pm

(Jun 21, 2016 11:33 AM)Disparity Wrote: [\[CITE\]](#) I'm not saying Kali linux is useless. I'm saying some of the worst advice you can give to someone looking to start hacking is to go straight to kali.

From personal advice, you should go straight to Kali. Become a skid, then un-skid yourself.

Just learning how to program in PHP takes way longer than using Kali, then learning what you gotta learn in PHP to hack. Just my thought, learn the two at the same time.

Triops - June 21, 2016, 5:05 pm

(Jun 21, 2016 03:17 PM)xHackerPr0 Wrote: [\[CITE\]](#) From personal advice, you should go straight to Kali. Become a skid, then un-skid yourself.

Just learning how to program in PHP takes way longer than using Kali, then learning what you gotta learn in PHP to hack. Just my thought, learn the two at the same time.

I definitely know the frustration of learning PHP, the language is so difficult to learn, especially with PHPFox.

Wireless Network - June 22, 2016, 2:40 am

(Jun 21, 2016 10:35 AM)Triops Wrote: [\[CITE\]](#) They are hosted on a dedicated server so i'm not sure that's possible to do.

Scan server with nmap, if you're lucky they might use vulnerable version of ftp or other services, the least thing you could do is to bruteforce ftp/ssh if there's no luck with vulns.

OGLIA - June 23, 2016, 9:03 am

Its all about knowledge and skills.

knowledge you can get it by trying.

skills with hacking.

hint : visit pentesteracademy they have some good tutorials.