

Forum:[Hack Forums](#)

Thread: [Learning SQL Injection and various other attack methods](#)

SysAdmin - January 6, 2016, 2:49 am

So i've been off the hacking scene for a while, mostly focusing on protecting my PC and trying the White-Hat function.

Now i know SQL Injection is not easy as you need to find a vulnerability on a website, but i've never found any, even on simple websites. Any suggestions or tutorials i should follow? Should i use a program to find a vulnerability or find my own? I would also like to know how useful a Brute-Force attack on an admin panel would be, and any other methods of website hacking, that would work at the moment.

I thank everyone in advance for any links or eBooks provided in this thread :)

yoyo123456 - January 6, 2016, 3:12 am

you need to google dork for the vulnerable sites first then check them and then try to inject.

SysAdmin - January 6, 2016, 5:47 am

(Jan 6, 2016 04:12 AM)yoyo123456 Wrote: [\[CITE\]](#) you need to google dork for the vulnerable sites first then check them and then try to inject.

I'm very aware of that but i'm not sure what exactly to look for.

Pwn_star_60 - January 6, 2016, 7:35 am

So you don't know what google dorks to use? There is a list here that might give you some decent results. It's old but might be a good place for you to start:

coolhackingtrick.com/2012/02/list-of-google-dorks-for-sql-injection.html

If you are looking to learn SQL injection within a lab environment then I would suggest the Damn Vulnerable Web App (DVWA) which you can find information on here:

dvwa.co.uk

Nomad.Null - January 6, 2016, 7:57 am

Using Dorks is for skids trying to find an easy deface. Real pentesters don't have that luxury. In pentesting, your target is dictated to you, and you have to find a vulnerability somewhere in that system. Sql injection is among one of the most common web exploits that pentesters will repair because they are difficult to catch and prevent, yet easily exploited.

It used to be a very arduous task, finding SQL vulnerabilities, because you would need to understand the SQL language and understand it's logic and syntax well enough so that you can circumvent it. SQL vulnerabilities are all about user input. Basically, when you are injecting SQL code into a webpage, you are trying to interrupt the syntax that exists on the page in order to replace it with your own. You can do this with comments, logical errors, syntax errors, and so on, but the basic idea is that you have to guess what the code is doing so that you can interrupt it and inject your own. This can be rather difficult and tedious because there are easily thousands of different ways to do this. Back in the day, the only way was to manually type the code out yourself and repeatedly run and modify it until it finally worked and you were successfully able to execute code.

Actually, finding sql injection vulnerabilities is no longer a serious issue. There is no shortage of them. In reality, SQL injection vulnerabilities are commonly found through input fuzzing. A fuzzer is a program that sends thousands of http or other input requests to a website, remote service, or application, in an attempt to make something happen. Fuzzers are something that requires quite a bit of fine tuning so that you don't accidentally DOS your customer.

Some common fuzzers can be found in the Kali pentesting suite, but just to name a few, you've got Burpsuite, Owasp ZAP, SQLmap, SQLninja, and some windows fuzzers such as Acunetix WVS and Nessus scanner.

This is something I should probably write a book on as well...

Nuclear3mbargo - January 7, 2016, 5:51 am

May I ask you how are you learning SQL injection, do you know how to write web applications and how to work with RDBMS and SQL?

Just write a few web applications and put vulnerability everywhere where SQL is used, then fix the vulnerabilities. Play a few wargames(e.g. enigmagroup has some SQL vulnerabilities), and then try to find vulnerabilities in real sites.

Nomad.Null - January 7, 2016, 7:11 am

(Jan 7, 2016 06:51 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) May I ask you how are you learning SQL injection, do you know how to write web applications and how to work with RDBMS and SQL?

Just write a few web applications and put vulnerability everywhere where SQL is used, then fix the vulnerabilities. Play a few wargames(e.g. enigmagroup has some SQL vulnerabilities), and then try to find vulnerabilities in real sites.

Why go through all that headache when you can just download purposeful vulnerable practice labs for free?

Visit any of the following and go get some real practice simulation labs:www.pentesterlab.com

www.root-me.org

hacking-labs.com

www.pentesteracademy.com

www.cybrary.it

Some of my best sources for practice environments here ?

Nuclear3mbargo - January 7, 2016, 1:14 pm

(Jan 7, 2016 08:11 AM)True Demon Wrote: [\[CITE\]](#) Why go through all that headache when you can just download purposeful vulnerable practice labs for free?

Visit any of the following and go get some real practice simulation labs:www.pentesterlab.com

www.root-me.org

hacking-labs.com

www.pentesteracademy.com

www.cybrary.it

Some of my best sources for practice environments here ?

Everybody has different learning method, I prefer to learn how to implement and fix the vulnerability then how to exploit it.