

Forum:[Hack Forums](#)

Thread: [\[TUT\] sql inject a website with sqlmap \(Linux\)](#)

TheSploit - December 16, 2016, 1:16 am

Introduction

Hello and today I will be talking about how you can sql inject websites with Kali Linux using sqlmap. Sqlmap comes pre installed with Kali Linux. If you don't have Linux you can get it from offensive security (for virtualbox).

Finding vulnerable websites

1) To find a vulnerable website, you must type into google `.phpid?='`

2) You will see a bunch of websites come up. Note that the ending of the URL will be what you typed in, which is good. Then click on a website and at the end of the URL, leave a space and put an apostrophe (') in. So the URL should look like this `Code websiteName.phpid?='36 ' NOTE It doesn't matter which number the website has after the .phpid?='. Also I don't recommend trying for this on government associated websites and websites that look good, because there is 99.99% that the websites will have some protection.`

4) If the server returns with a sql error, that means the website is vulnerable. If the website will say 'whatever you were searching for was not found', the website isn't vulnerable.

Tip Research sql dorks. Sql dorks are lists of websites that are vulnerable to sql injection. Be careful because some sql dorks websites are quite shady.

5) Now let's get to hacking. Open up terminal in Linux, and type the following in. `Code sqlmap -u websiteName --dbs` the `-u` command tells sqlmap what URL you are using, and `--dbs` tells it to access the database.

6) It's gonna load for a while, and then sometimes it might ask you to type yes or no, depends on what you want or do. If you have no idea of what you are doing, I recommend keep typing in yes for whatever option comes up.

NOTE if something like this website isn't vulnerable comes up find a new website.

7) Now you will see different databases come up on the screen. The most useful information in a database would be usernames and passwords. I can't give you the name of the database that you need to look passwords and usernames in, because different websites have different names for databases, so you will have to do some poking around.

8) To look what's in a database type in `Code sqlmap -u websiteName -D databaseName --tables`

9) Now to look what's inside the tables, type in `Code sqlmap -u websiteName -D databaseName -T tableName --columns`

10) To look what's inside a column type in `Code sqlmap -u websiteName -D databaseName -T tableName -C columnName --dump`

11) Now you went through all the 'folders' and found the information. Thanks for reading.?

Nik321 - February 15, 2017, 1:15 pm

What if you want to attack a website that does not have vuln parameters in the URL? but you are 100% certain they are using MySQL