

Forum:[Hack Forums](#)

Thread: [\[MASSIVE TUT\]SQLi|Db Intrusion|Website backdoor|Mass_Defacement\[COMPLETE\]](#)

imghostin - November 22, 2016, 8:24 am

Hello everyone! This is my first tutorial. In this tut, I'm gonna try to cover almost all the basic/intermediate level knowledge of SQL injections and be as much as possible n00b friendly. All constructive critics are welcome.

So this is the plan we're going to follow through this thread:

I-What is a SQL injection and what can we do with it

II-Detecting a vulnerable website

III-Intruding the Database

IV-Getting access to the admin panel

V-Uploading a shell to maintain access

VI- Mass defacement

The tools we're gonna need, and where to find it:

- SQLmap: included in Kali Linux

- Acunetix or any other web vulnerability scanner: Find it on your own :p

- A PHP shell, a good free one is b374k's shell: <https://github.com/b374k/b374k>

- Brain could be useful as well

- TamperData (firefox plugin) or any tampering tool:

<https://addons.mozilla.org/en-US/firefox/addon/tamper-data/> (If you don't want to use firefox, Burpsuite is a good tampering tool as well)

PS: No I'm NOT a skid, but in this tutorial will be used ready-made tools to be as much as possible noob friendly. We're not getting into so much theory and SQL commands.

That been said, let's get into our main subject

I-What is SQL injection and what can we do with it

SQL is a standard language for manipulating databases.

A SQL injection attack consists of injecting a SQL query command in a webapp/website letting the attacker take control of the database. A successful SQL injection exploit can read sensitive data from the database, modify its data, execute administration operations on it, and in some cases issue command the operating system which we will see later how to do.

A very basic example of how a SQL command is injected (theory, you can skip it):

Spoiler [\(Click to View\)](#)

Where inputted_username is the username inputted by the user.

Now a hacker can exploit this code by typing in the input_username textbox:

Result:

Which is always true and will basically dump ALL the addresses of all users in the database

II-Detecting a vulnerable website

Where?

You can test for SQLi vulnerabilities in a website in the pages where there is a request to the database.

How?

You can find if there is a request quickly by just checking the URL:

The following syntax: `site.com/random.php?id=1` shows the site is requesting the element in the DB with `id=1`. A quick technique to find if it is vulnerable is dropping a ' symbol next to `id=1` and checking the output. If an error like in the following image appears, the website is prone to SQLi because the developer did not properly escape the parameter `id`.

That's the manual way. You can also scan the website with acunetix for more deep and accurate results, which I recommend.

III-Intruding the Database

Okay things are getting more serious. We've previously found a SQLi vulnerable website. Now we're gonna intrude the database with SQLmap.

Sqlmap is one of the most popular and powerful SQL injection automation tools out there. Given a vulnerable http request URL, sqlmap can exploit the remote. Written in python it is one of the most powerful hacking tools out there. Sqlmap is the metasploit of sql injections.

Fire up your Kali, get in the terminal and type in:

Code `sqlmap -u site.com/random.php?id=1 --dbs` Where `site.com/random.php?id=1` is the vulnerable page on the website you want to hack. Sqlmap will confirm the website's vulnerability and the "--dbs" option is used to get the list of available DBs.

Code `sqlmap -u site.com/random.php?id=1 -D dbname --tables` Will find the tables in the DB named `dbname`. Here is an example image of the output:

We are interested in the admin table.

Code `sqlmap -u site.com/random.php?id=1 -D dbname -T admin --columns` will dump the columns of the table. There is multiple columns from which user and password columns. We're interested in them

So finally, getting the useful infos:

Code `sqlmap -u site.com/random.php?id=1 -D dbname -T admin --C user,password --dump` will show use the user and password info of the admin login page.

NB: If the passwords are encrypted e.g: `098f6bcd4621d373cade4e832627b4f6` (md5,sha1) you'll have to decrypt it. Its easy with Google :p

CONGRATZ We've intruded the DB and found the login info of the adminPage. Let's advance then ;)

IV-Getting access to the admin panel

So first, for getting access to adminPanel we have to know where it is located right?

There is different ways to do that, I personally use acunetix which will crawl the whole site while scanning it (We've already done it in partII).

Now let's go to the page. Login with the credentials we got previously in our data dump.

Anddd we're in !!

Spoiler ([Click to View](#))

V-Uploading a shell

OK now we got access to the admin panel. We need to backdoor it so we could always have our way in the site, even if the admin changes his login credentials. Let's upload a PhP shell! Here in the admin Panel I can upload images to the /photos directory, unfortunately it's the only place where I can upload something to the website.

It only accepts JPG and PNG file formats, dw we're gonna find our way around ;)

On your computer, rename your shell.php (I use b374k) to shell.php.jpeg. On firefox, start tamperData or any tampering tool and start tampering. Now upload shell.php.jpeg to the website, it will accept it thinking it's an image. In tamperData we've caught the request: Just rename the file from shell.php.jpeg to shell.php and submit (see pics below)

Our shell is now uploaded to /photos directory! You can access it on site.com/photos/shell.php

Now with a php shell, you have almost full control on the website. You can remove, replace files etc, access a terminal and get infos about the server, or backConnect the server to your pc for rooting it later on, and have admin rights on it so you can delete logs/hack into the other existing websites.

If all goes well, I may show it in another tutorial

Now part VI-Mass Defacement. I'm too poor to upgrade :p, just scroll down check my next post for the next part

VI- Mass Defacement

Now, with the php shell, we've got control of website's files. Defacing a site consists of uploading an index.html or index.php in the root directory of the website, with what you want on it. You can make your own file. I personally coded my own index.php, but you can easily make one with Adobe Dreamweaver if you don't have web coding skills.

In our php shell, in the explorer tab, go to the root directory of the website (often public_html), and make a copy of the index.php (It will be a backup for the site, we're not blackhats right?).

Spoiler ([Click to View](#))

Click on index.php , a notepad-like window containing the code of the file opens. Click on action -> edit. Just delete all the content (the code) and paste your own defacement code, then save.

And the Result:

Finally CONGRATZ you've done it!

B O N U S :

Code `sqlmap -u site.com/random.php?id=1 --current-user --is-dba` Will check if the website have admin permissions on the server.

If it outputs `:Quote:is-dba= true;`

It means that you can have access to `--os-shell` sqlmap feature which will give you a shell on the website' server; letting you take control of the Operating system!

NOT TO FORGET: This tutorial is only for educational purpose. I'm not responsible of any of your actions and blackhat activities against websites.

I hope my tutorial helped you. As I already said, if there is something you didn't like, all constructive critics are more than welcome. Otherwise a friendly thank you is OK too :p . Any questions, I'll reply as possible on this thread.

Peace ? !!

ChaoticForce - November 22, 2016, 8:26 am

I learned how to hack myself... finally, I am making this post towards this accomplishment as I have finally mastered myself

Evanescence - November 22, 2016, 8:27 am

Noice tutorial bro, bookmarking this, so I can use it later when I get really bored and want to fuck with some websites. Thanks! ?

Armada - November 22, 2016, 8:29 am

Looks like a pretty thorough tutorial.

Never ceases to amaze me how many sites are vulnerable to these type of attacks.

Rafaelinio - November 22, 2016, 8:29 am

looks great, i'll go through this tutorial later. Good Job!

Codestroy - December 21, 2016, 2:45 pm

Nice tutorial here, this will help out a lot of people :)

Cryptic5 - December 22, 2016, 11:55 am

This really caught my attension! Nice tutorial thank you :)

Codestroy - December 23, 2016, 1:25 pm

Noice tutorial bro ?

imghostin - December 26, 2016, 1:14 pm

I'm grateful you've liked it. Any questions do not hesitate ;)

StringTheory - December 26, 2016, 7:38 pm

very hq tutorial, thank you very much op

t0msawyer - January 5, 2017, 8:46 pm

thank for you tutorial and information :D

GhostintheShock - January 5, 2017, 10:40 pm

Very nice tutorial. But did you mean this is mass defacement?

Mass defacement: Deface all the websites hosted on the same server when either you have root on the server if it is Linux or there is symlink on entire server. For window if you have hijacked special token you can do anything.

This is only one web site deface. But the hard work you have put in for this tutorial is admirable.

?Adroit - January 6, 2017, 6:54 am

Nice HQ tutorial. Posting to come back later

bloodyprince - January 6, 2017, 8:26 pm

That's really very HQ tutorial OP. Thanks a lot :)

imghostin - January 7, 2017, 4:45 pm

(Jan 5, 2017 11:40 PM)mikewaals Wrote: [CITE](#) Very nice tutorial. But did you mean this is mass defacement?

Mass defacement: Deface all the websites hosted on the same server when either you have root on the server if it is Linux or there is symlink on entire server. For window if you have hijacked special token you can do anything.

This is only one web site deface. But the hard work you have put in for this tutorial is admirable. I am sorry this was unclear from my side. It may come in my second tutorial which will follow this one.

@everybody, if you liked it, I may do a second tutorial about server rooting/shelling or you can leave requests here if you'd like to have another topic.

minecrafter6969 - January 23, 2017, 1:46 am

looking really nice young man!!