

Forum:[Hack Forums](#)

Thread: [Need Help - Got Vuln - No Idea what to do](#)

N01Knowz - January 29, 2020, 1:57 am

Okay so its my first try to SQL Inject

I got a DB Link that looks like this xxxxx.ga

I downloaded SQLMAP and ran it, it found 2 Vulnerabilities for injection in Username and Password

Code Parameter: password (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: Doesnt let me post this here

Parameter: username (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username Also doesnt let me post here xDDDDD

there were multiple injection points, please select the one to use for following injections:

[0] place: POST, parameter: username, type: Single quoted string (default)

[1] place: POST, parameter: password, type: Single quoted string

[q] Quit

> 0

do you want to exploit this SQL injection? [Y/n] y

[09:38:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file

The results File show This:

Code Target URL,Place,Parameter,Technique(s),Note(s)

http://xxxxxxx.ga/index.php,POST,password,T,

http://xxxxxxx.ga,POST,username,T,

http://xxxxxxx.ga,POST,password,T,

On the Log File i have this:

Code sqlmap identified the following injection point(s) with a total of 85 HTTP(s) requests:

Parameter: username (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username=cant post

web application technology: Apache 2.4.6, PHP 7.2.24

back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)

sqlmap identified the following injection point(s) with a total of 51 HTTP(s) requests:

Parameter: password (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload:cant post

Vulnerabilities were found with sqlmap.py -u URL --forms
--dbs gives error and says its not vulnerable

but now im lost, idk what to do with those vulnerabilities, the program asks me to exploit, i press yes and it doesnt, it stops

can someone help me ? maybe come disccord and shed some light ?? I try guys, i really try to do it myself without asking too much around because i know a lot of people dont like and will tell me to use google, but im kinda lost

let me know what else do you need to help me, i have a payload i cant post here but idk how to use it now

KoYoGotit - February 1, 2020, 2:39 am

Pm on ill help you with the commands

RONALD - February 1, 2020, 2:48 am

Try using Sqli first, input the full url target on url analyzer box.

If its injectables, it will shown the DB's link url to explored.

ghonter - February 1, 2020, 8:34 pm

maybe you should try it manually Sql injection with your browser,