

Authentication Based Attacks

Tools in Kali Linux

Module #30

SQL Injection

A database stores data and organizes it in some sort of logical manner. Postgres SQL and Microsoft SQL are examples of database management systems that allow users to create multiple types of databases used to store, query, and organize data in creative ways.

Structured Query Language, which is better known as SQL, is the underlining common programming language that is understood by most database management systems. It provides a common way for application to access the data in the database by using a common set of commands the database can understand.

Attackers exploit these databases by making them output information that they should not be displaying.

SQL Injection

Sometimes this is as simple as the attacker asking for privileged information from the database management system. Other times, it is taking advantage of poor configurations by database administrators.

Attackers may also take advantage of a vulnerability in the database management system that allows the attacker to view or write privileged commands to and from the database.

Attackers typically send malicious code through forms or other parts of a webpage that have the ability to accept user input.

SQL Injection

For example, an attacker may enter random characters, as well as long statements, with the goal of identifying weakness in how the input variables and parameters are designed.

If an input field is set to only accept usernames up to 15 characters long, an error message may appear revealing details about how the database is configured.

The Firefox plugin HackBar will let you test SQL queries and inject your own queries for changing SQL requests. The HackBar plugin will also let a Penetration Tester examine HTTP post information.

SQL Injection example

We will try to perform a SQL injection on the website DrChaos.com . Let's navigate to www.DrChaos.com using Firefox on our Kali server console and try to log into the website.

First, we will try the username administrator and the password 12345 to login. You should see that will fail.

Now, navigate to the View menu bar in Firefox and select the HackBar menu. Click the Load URL button and click the Enable Post data button. You will see the URL we were logging into as well as the username and password we just attempted.

SQL Injection example

The screenshot shows a web application security tool interface. At the top, there is a tab labeled 'INT' and a row of icons for 'SQL', 'XSS', 'Encryption', 'Encoding', and 'Other'. Below this, there are three main sections: 'Load URL', 'Split URL', and 'Execute'. The 'Load URL' section contains a text box with the URL 'https://www.dxchaos/aqli/admin/index.php?route=common/login'. The 'Split URL' section is empty. The 'Execute' section has a checkbox for 'Enable Post data' which is checked, and a checkbox for 'Enable Referrer' which is unchecked. Below these checkboxes is a 'Post data' section with a text box containing the payload 'username=administrator&password=12345'.

INT SQL XSS Encryption Encoding Other

Load URL `https://www.dxchaos/aqli/admin/index.php?route=common/login`

Split URL

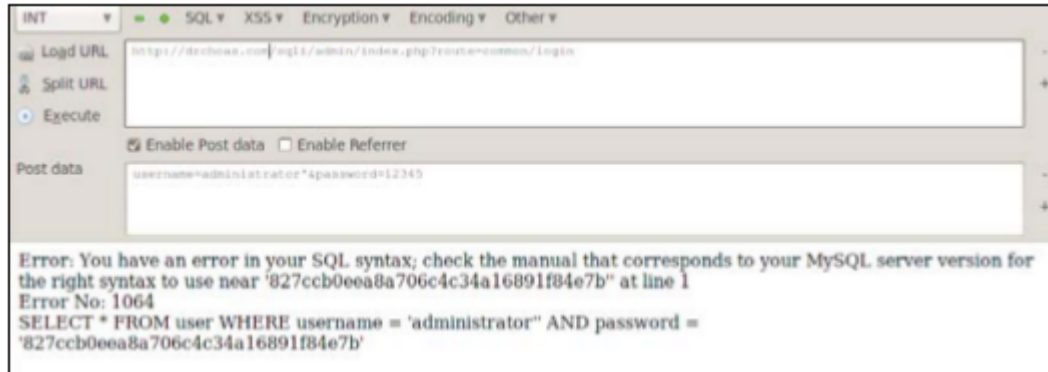
Execute

☒ Enable Post data ☐ Enable Referrer

Post data `username=administrator&password=12345`

SQL Injection example

We will now add a single quotation mark after the administrator username. Soon as we click on the Execute button, we receive a message like below: This may mean the server is vulnerable to SQL injection, because the server is responding to SQL errors.



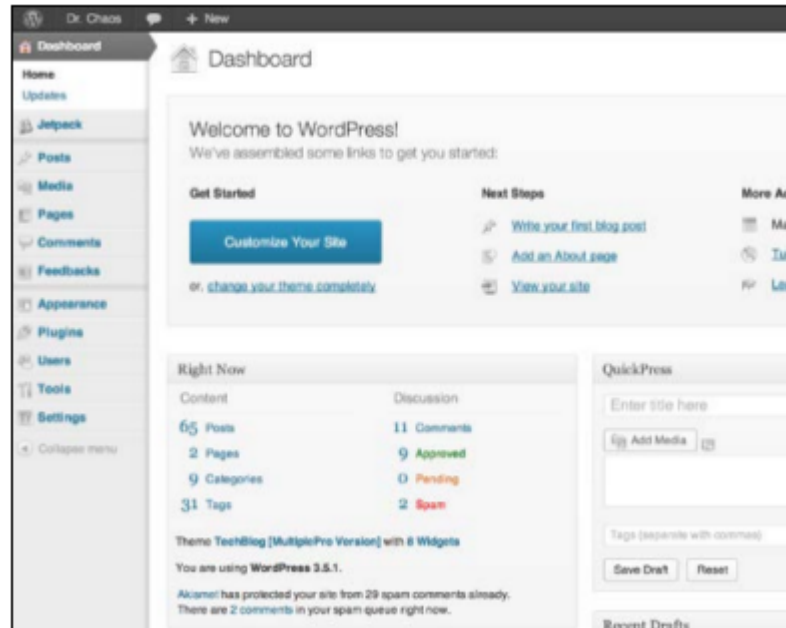
SQL Injection example

We will put in SQL injection by adding an OR 1=1 ### statement at the end of the line.



SQL Injection example

Once we execute the code, we are logged on as administrator to www.drchaos.com.



sqlmap

sqlmap automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. sqlmap comes with a detection engine, as well as a broad range of Penetration Testing features that range from database fingerprinting to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Features include support for common database management systems, support for many SQL injection techniques, enumerating users, password hashes, and many others. sqlmap also supports database process' user privilege escalation using Metasploit's Meterpreter getsystem command.

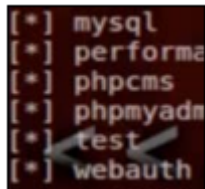
sqlmap

sqlmap under Vulnerability Analysis | Database Assessment |
Sqlmap.

The basic syntax to use sqlmap is:
`sqlmap -u URL -- function`

A common function is `dbms`. The `dbms` keyword will have sqlmap get the databases.

`sqlmap -u http://www.drchaous.com/article.php?id=5 -dbms`



```
[*] mysql
[*] performe
[*] phpcms
[*] phpmyn
[*] test
[*] webauth
```

A screenshot of a terminal window showing the output of a sqlmap command. The output lists several detected databases, each preceded by an asterisk in brackets. The list includes 'mysql', 'performe', 'phpcms', 'phpmyn', 'test', and 'webauth'. The 'test' entry is highlighted with a green cursor arrow pointing to it from the left.

sqlmap

Once you have found a vulnerable web server, you select the database by using the -D command and the name of the database.

```
sqlmap -u http://www.drchaos.com/article.php?id=5 -D test -tables
```

The table keyword is used to retrieve all the tables in the test database on our web server.

Once you issue the following command, sqlmap will display all tables:

```
sqlmap -u http://www.drchaous.com/article.php?id=5 -D test --tables
```

Specific columns can be selected by using the following command:

```
sqlmap -u http://www.drchaous.com/article.php?id=5 --columns
```

Thank You