SQL Injection Scanner Report

✔ http://www.pentest-ground.com:81/

Summary

Overall risk level:

High

Risk ratings:

Scan information:

Start time:	2023-04-25 10:37:41 UTC+03
Finish time:	2023-04-25 10:38:53 UTC+03
Scan duration:	1 min, 12 sec
Tests performed:	3/3
Scan status:	Finished

Findings

SQL Injection

CONFIRMED

URL	Method	Parameters	Evidence	Replay Attack
http://www.pentest-ground.com:81/search	POST	Body: query=' Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36	Injecting the value `'` in the **query body parameter** generated the following error(s) in the response: `<title>sqlite3.OperationalError: unrecognized token: "''''"` Request / Response	

Details

Risk description:

We found that the web application is vulnerable to SQL Injection attacks.
SQL Injection is a vulnerability caused by improper input sanitization and allows an attacker to inject arbitrary SQL commands and execute them directly on the database.

The risk exists that an attacker gains unauthorized access to the information from the database of the application. He could extract information such as: application usernames, passwords, client information and other application specific data.

Recommendation:

We recommend implementing a validation mechanism for all the data received from the users.
The best way to protect against SQL Injection is to use prepared statements for every SQL query performed on the database.
Otherwise, the user input can also be sanitized using dedicated methods such as: mysqli_real_escape_string.

References:

https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Classification:

CWE : CWE-89
OWASP Top 10 - 2013 : A1 - Injection
OWASP Top 10 - 2017 : A1 - Injection

Screenshot:

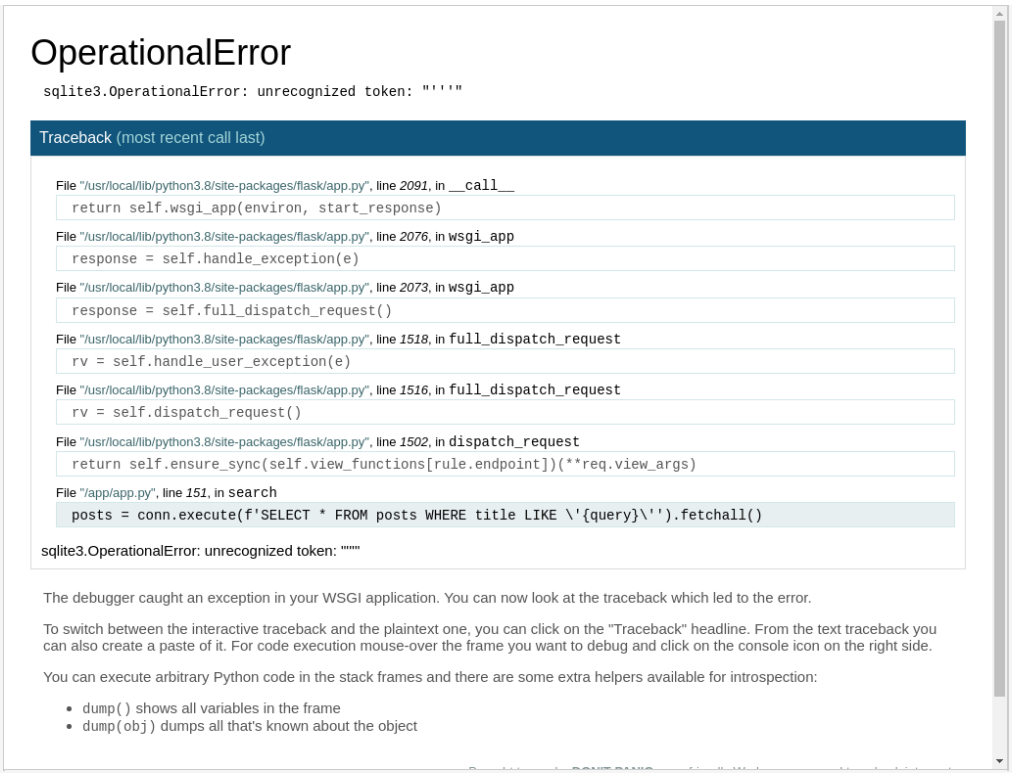

Figure 1. SQL Injection

Spider results

URL	Method	Parameters
http://www.pentest-ground.com:81/1/edit	POST	Body: content=content...
http://www.pentest-ground.com:81/1/edit	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/2/edit	POST	Body: content=content...
http://www.pentest-ground.com:81/2/edit	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/about	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/blog	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/contact	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/create	POST	Body: content=content reference=reference title= Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

http://www.pentest-ground.com:81/create	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/login	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/post/1	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/post/2	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/search	POST	Body: query= Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/search	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/services	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
http://www.pentest-ground.com:81/static/js	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Website is accessible.

Scan coverage information

List of tests performed (3/3)

- Checking for website accessibility...
- Spidering target...
- Checking for SQL Injection...

Scan parameters

Website URL:	http://www.pentest-ground.com:81/
Scan type:	Full
Authentication:	False

Scan stats

Unique Injection Points Detected:	17
URLs spidered:	59
Total number of HTTP requests:	1882
Average time until a response was received:	19ms