SQL Injection Scanner Report

https://demo.owasp-juice.shop/
Target added due to a redirect from https://demo.owasp-juice.shop/#

Summary

Overall risk level:
Info

Risk ratings:

High:	0
Medium:	0
Low:	0
Info:	3

Scan information:

Start time:	Nov 06, 2023 / 18:44:28
Finish time:	Nov 06, 2023 / 18:44:45
Scan duration:	17 sec
Tests performed:	3/3
Scan status:	Finished

Findings

Spider results

URL	Method	Parameters
https://demo.owasp-juice.shop/	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

Details

Risk description:
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

Website is accessible.

Nothing was found for SQL Injection.

Scan coverage information

List of tests performed (3/3)

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

Scan parameters

Target: https://demo.owasp-juice.shop/

Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	5
Total number of HTTP requests:	89
Average time until a response was received:	90ms