XSS Scanner Report

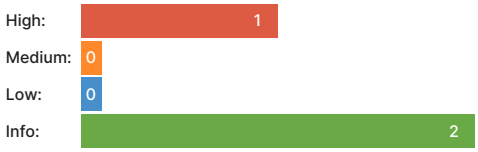
✔ http://www.pentest-ground.com:81/

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2023-04-25 10:37:30 UTC+03
Finish time:	2023-04-25 10:38:33 UTC+03
Scan duration:	1 min, 3 sec
Tests performed:	3/3
Scan status:	Finished

Findings

Cross-Site Scripting

CONFIRMED

URL	Method	Parameters	Evidence	Replay Attack
http://www.pentest-ground.com:81/1/edit	POST	Body: content=content...	Injected the payload `'"--></noscript></title></textarea></style></template></noembed></script><svg/*/onload=document.body.append`${522260-52226}`//>` in the **title body parameter** and the expected result `470034` was found in the response. Request / Response	
http://www.pentest-ground.com:81/2/edit	POST	Body: content=content...	Injected the payload `'"--></noscript></title></textarea></style></template></noembed></script><svg/*/onload=document.body.append`${104130-10413}`//>` in the **title body parameter** and the expected result `93717` was found in the response. Request / Response	

Details

Risk description:

The web application is vulnerable to reflected Cross-Site Scripting attacks. The risk exists that a malicious actor injects JavaScript code and runs it in the context of a user session in the application. This could potentially lead to various effects such as stealing session cookies, calling application features on behalf of another user, exploiting browser vulnerabilities.
Successful exploitation of Cross-Site Scripting attacks requires human interaction (ex. determine the user to access a special link by social engineering).

Recommendation:

There are several ways to mitigate XSS attacks. We recommend to:
- never trust user input
- always encode and escape user input (using a Security Encoding Library)
- use the HTTPOnly cookie flag to protect from cookie theft
- implement Content Security Policy
- use the X-XSS-Protection Response Header.

References:

https://owasp.org/www-community/attacks/xss
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Classification:

CWE : CWE-79
OWASP Top 10 - 2013 : A3 - Cross-Site Scripting (XSS)

OWASP Top 10 - 2017 : A7 - Cross-Site Scripting (XSS)

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/images/	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 Cross-Site Scripting...

Scan parameters

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

Scan stats

Unique Injection Points Detected:	17
URLs spidered:	53
Total number of HTTP requests:	530
Average time until a response was received:	67ms