New issue

Jump to bottom

Time-based blind SQL injection Vulnerability in CSZCMS-1.2.4 #22

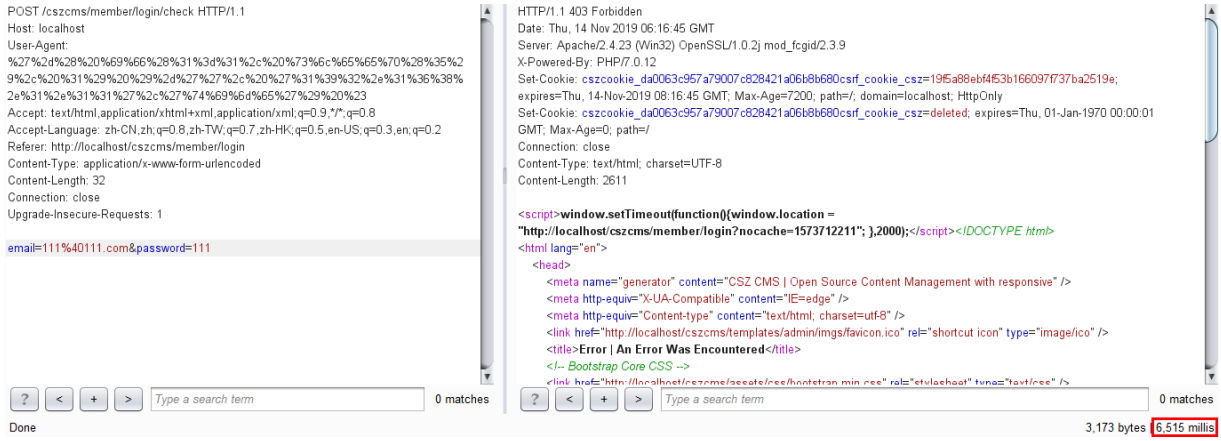
Closed **edwatering** opened this issue on Nov 14, 2019 · 2 comments

edwatering commented on Nov 14, 2019

Hi, **@cskaza** and I found an arbitrary file upload vulnerability in cszcms-1.2.4. The vulnerable code is on cszcms/core/MY_Security.php file line 47.

```
47      VALUES ('', 'CSRF Protection Invalid', 'CSRF_INVALID', '".$this->xss_clean($mysqli->escape_string($_SERVER['HTTP_USER_AGENT'])
```

I think using the function 'escape-string' can solve the sql injection vulnerability,but you use function 'xss_clean' after it.The function 'xss_clean' can decode str with function 'rawurldecode',so I can exploit like #19 .
Urlencode the value of UA:
Before:
User-Agent: '-(if(1=1, sleep(5), 1))-'', '192.168.1.11','time') #
After:
User-Agent:
%27%2d%28%20%69%66%28%31%3d%31%2c%20%73%6c%65%65%70%28%35%29%2c%20%31%29%20%29%2d%27%27%2c%20%27%31%39%32%2e%31%36%38%2e%31%2e%31%31%27%2c%27%74%69%6d%65%27%29%20%23



Suggest: Remove function 'xss_clean' here.

cskaza commented on Nov 24, 2019 Owner

Thanks for your suggest. I will resolve it.

cskaza commented on Nov 27, 2019 • edited Owner

This bug has been to resolved.
https://gitlab.com/cszcms/cszcms/commit/64b4851c5d79eb4ef4c4d99708d3f03c239bf63b

Thanks.

cskaza closed this as completed on Nov 27, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants