orangehrm / **orangehrm** Public

Code Issues 37 Pull requests 8 Actions Projects 1 Wiki ···

New issue

Jump to bottom

Referer header injection redirect vulnerability #1174

Closed **vulf** opened this issue on Mar 10 · 1 comment

Labels env-configuration

vulf commented on Mar 10

Environment details
OrangeHRM version: 4.10
OrangeHRM source: Release build from Sourceforge or Git clone
Platform: Ubuntu
PHP version: 7.3.33
Database and version: MariaDB 10.3
Web server: Apache 2.4.52

If applicable:
Browser: Firefox

Describe the bug
This is similar to the Host header injection redirect vulnerability, except the issue lies in the **Referer** header and the vulnerable endpoints are **different**.

To Reproduce

1. Login to the OrangeHRM application
2. Navigate to "My Info"
3. Under "Add Attachment", click on "Add"
4. Turn on Intercept in Burp Suite (or any other web proxy)
5. Select any PNG file and Click on "Upload"
6. Change the value of the `Referer` header to `example.com`
7. Click on Forward in Burp and turn off Intercept
8. You will notice that the page gets redirected to `http://example.com/symfony/web/index.php/pim/viewPersonalDetails/empNumber/X`

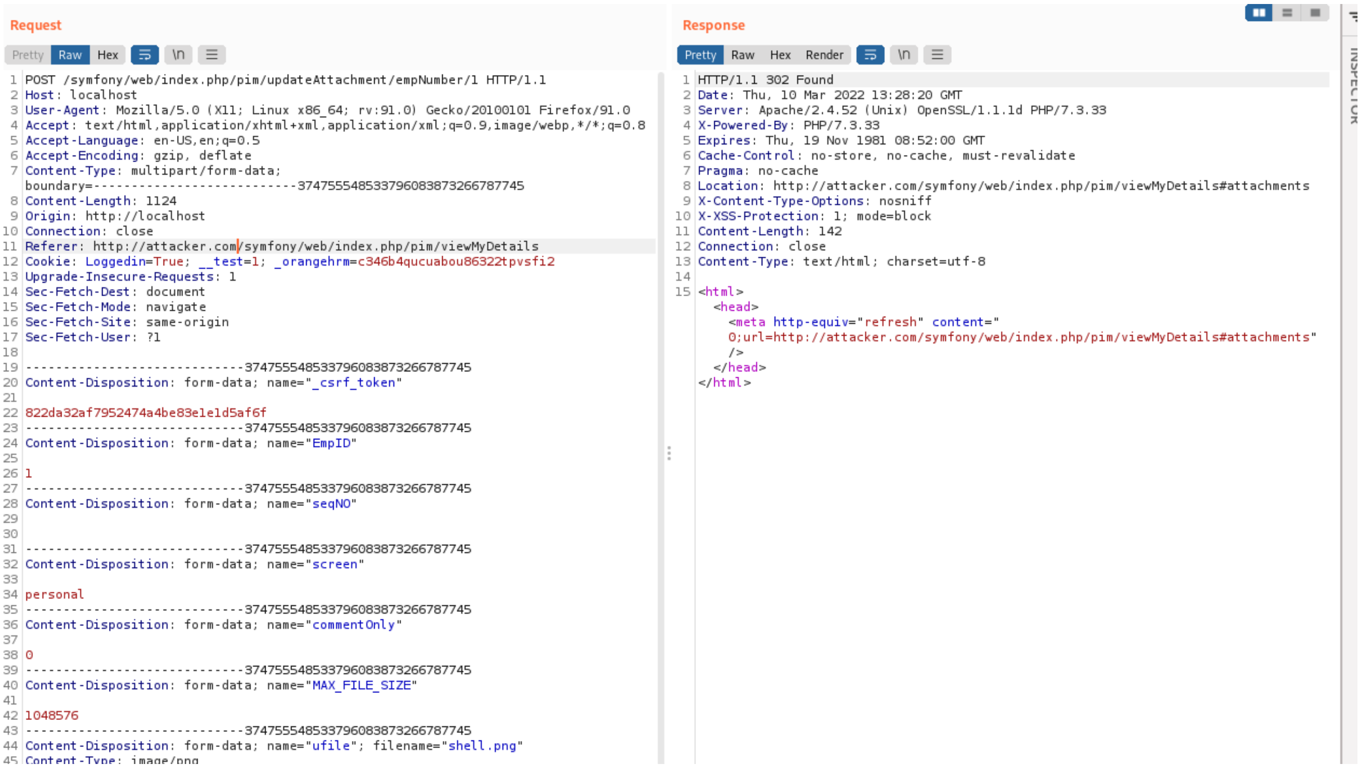
Expected behavior

A 404 error.

What do you see instead:

A 302 redirect to the malicious domain.

Screenshots



```
POST /symfony/web/index.php/pim/updateAttachment/empNumber/1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Content-Type: multipart/form-data;
boundary=---------------------------374755548533796083873266787745
Content-Length: 1124
Origin: http://localhost
Connection: close
Referer: http://attacker.com/symfony/web/index.php/pim/viewMyDetails
Cookie: Loggedin=True; __test=1; _orangehrm=c346b4qucuabou86322tpvsfi2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="_csrf_token"

822da32af7952474a4be83e1e1d5af6f
-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="EmpID"

1
-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="seqNO"


-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="screen"

personal
-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="commentOnly"

0
-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="MAX_FILE_SIZE"

1048576
-----------------------------374755548533796083873266787745
Content-Disposition: form-data; name="ufile"; filename="shell.png"
Content-Type: image/png
```

```
HTTP/1.1 302 Found
Date: Thu, 10 Mar 2022 13:28:20 GMT
Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1d PHP/7.3.33
X-Powered-By: PHP/7.3.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://attacker.com/symfony/web/index.php/pim/viewMyDetails#attachments
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 142
Connection: close
Content-Type: text/html; charset=utf-8

<html>
  <head>
    <meta http-equiv="refresh" content="
    0;url=http://attacker.com/symfony/web/index.php/pim/viewMyDetails#attachments"
    />
  </head>
</html>
```

samanthajayasing... commented on Mar 22 Member

Hi **@vulf**
It's recommended to deploy the application with the valid hostname

```
eg: nginx
server {
    listen 80 default_server;
    server_name mydomain.com;
   ...
}
```

samanthajayasinghe closed this as completed on Mar 22

samanthajayasinghe added the **env-configuration** label on Mar 22

Assignees

No one assigned

Labels

env-configuration

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants