orangehrm / **orangehrm** Public

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

New issue

Jump to bottom

Stored XSS in the "Share Video" section under "OrangeBuzz" via the GET/POST "createVideo[linkAddress]" parameter #1176

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

Labels bug Security

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
In order to share a video, a user provides the URL in the "Share Video" feature under "Buzz". A GET request is then sent to the /symfony/web/index.php/buzz/addNewVideo endpoint with the url as a parameter. The application's backend then validates the url against a whitelist of domains and sends an appropriate response. If the domain in the url is in the whitelist, the application creates an iframe element and embeds the video link in it. The user then submits the post by clicking the "Save Video" button.

The "OrangeBuzz" page, including the newly posted video, is sent back in the response body. The initial whitelist based validation can be bypassed by sending a request, like the above, containing any arbitrary URL in the createVideo%5BlinkAddress%5D parameter. The value of this parameter is injected into the iframe's src attribute. Due to this, it is possible to inject the javascript: pseudo-protocol and gain arbitrary JavaScript execution in the browser of anyone who visits the "OrangeBuzz" page. For example, the string javascript:alert(document.domain) can be passed as the value of the createVideo%5BlinkAddress%5D parameter. When a user visits the OrangeBuzz page, the payload will be interpreted as JavaScript and get executed so an alert will pop-up with the domain hosting the application at that instance.

To Reproduce

1. Login to the OrangeHRM application
2. Navigate to "Buzz" > "Share Video"
3. Paste any youtube.com video link
4. Turn on Intercept in Burp Suite (or any other web proxy)
5. Click on "Save video"
6. Replace the value in the POST parameter `createVideo%5BlinkAddress%5D` to `javascript:alert(document.domain)` and click on "Forward" in Burp
7. Turn off Intercept in Burp
8. Navigate to "Buzz"
9. Notice that an alert will pop-up with the Domain value of the application's server printed which means the payload we injected into the `createVideo%5BlinkAddress%5D` parameter is interpreted as valid Javascript and is executed.

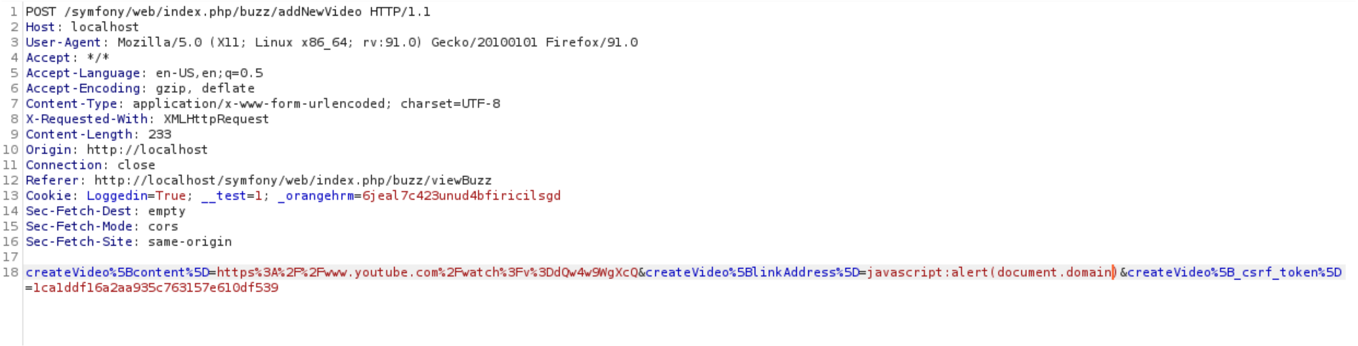
Expected behavior

The value of the `createVideo%5BlinkAddress%5D` parameter is validated by the application's backend and an error is thrown.

What do you see instead:

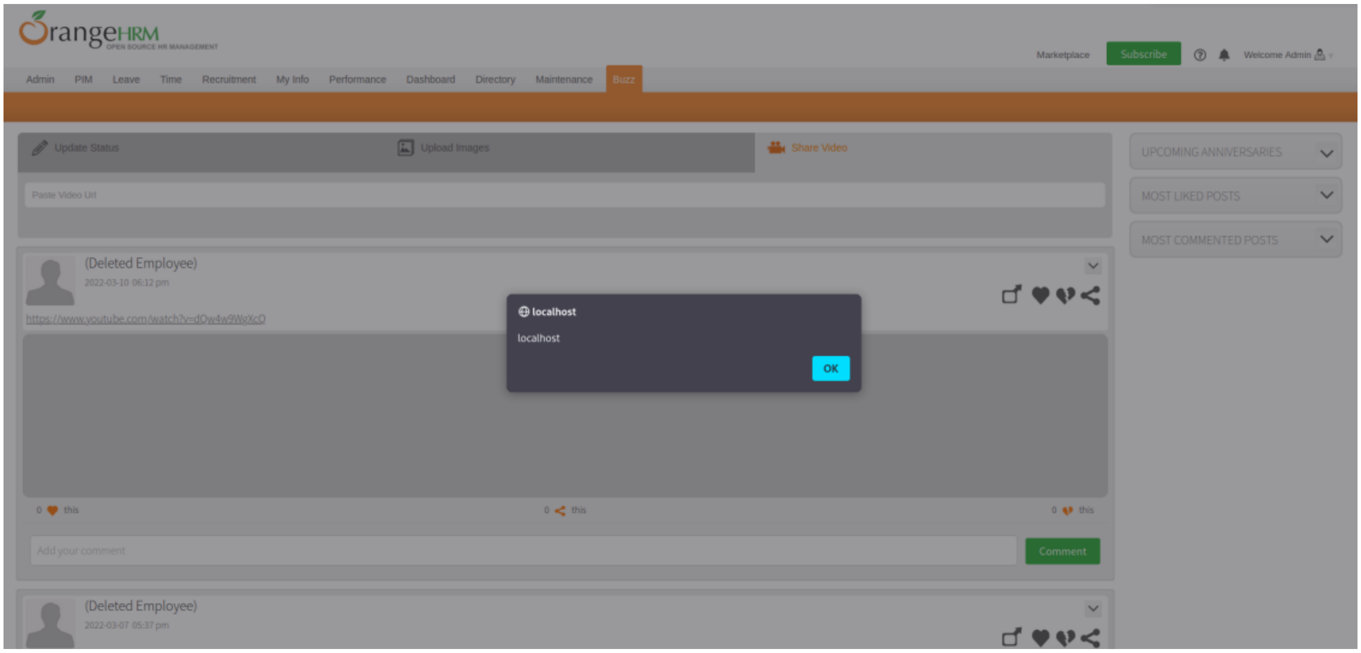
The post gets uploaded successfully.

Screenshots



```
POST /symfony/web/index.php/buzz/addNewVideo HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 233
Origin: http://localhost
Connection: close
Referer: http://localhost/symfony/web/index.php/buzz/viewBuzz
Cookie: Loggedin=True; __test=1; _orangehrm=6jeal7c423unud4bfiricilsgd
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

createVideo%5Bcontent%5D=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DdQw4w9WgXcQ&createVideo%5BlinkAddress%5D=javascript:alert(document.domain)&createVideo%5B_csrf_token%5D
=1calddf16a2aa935c763157e610df539
```



localhost

localhost

OK

samanthajayasinghe added bug Security labels on Mar 22

samanthajayasing... commented on Mar 25 Member

Hi **@vulf**
This issue is fixed on v4.10.1
https://github.com/orangehrm/orangehrm/releases/tag/v4.10.1

samanthajayasinghe closed this as completed on Mar 25

RajithaKumara mentioned this issue on Mar 26

OHRM-1154: Bump OrangeHRM version to 4.10.1 #1190

Merged

Assignees

No one assigned

Labels

bug Security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants