Open Redirect on Rudloff/alltube in rudloff/alltube

0

Valid Reported on Feb 18th 2022

Description

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain.
`https://github.com/Rudloff/alltube` is vulnerable to open redirects as shown below:

Proof of concept

Vuln variable: `$_SERVER['REQUEST_URI']`
Snippet:

```
if (isset($_SERVER['REQUEST_URI']) && strpos($_SERVER['REQUEST_URI'], '/inc
    header('Location: ' . str_ireplace('/index.php', '/', $_SERVER['REQUEST
```

Payload

In a browser perform a request to `index.php` resource:

```
http://localhost/index.php/example.com
```

Observe the user is redirected to `example.com`

Impact

This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and valid SSL certificate (if SSL is used), lends credibility to the phishing attack because most users, if they verify these features, will not notice the subsequent redirection to a different domain.

References

https://portswigger.net/kb/issues/00500100_open-redirection-reflected
https://www.netsparker.com/blog/web-security/open-redirect-vulnerabilities-netsparker-pauls-security-weekly/

Occurrences

index.php L8-L9

CVE
CVE-2022-0692
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (4.7)

Visibility
Public

Status
Fixed

Found by

hitisec
@hitisec
pro

This report was seen 475 times.

We are processing your report and will contact the **rudloff/alltube** team within 24 hours.
9 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md`

Chat with us

Pierre Rudloff validated this vulnerability 9 months ago

hitisec has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Pierre Rudloff marked this as fixed in **3.0.1** with commit **bc14b6** 9 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

index.php#L8-L9 has been validated ✔

Sign in to join this conversation