Create-Project Manager 1.07 Cross Site Scripting / HTML Injection

Authored by thelastvvv | Posted May 7, 2020

Create-Project Manager version 1.07 suffers from cross site scripting and html injection vulnerabilities.

tags | exploit, vulnerability, xss
SHA-256 | 1aa7c38232d6dd3bd6ccfc8545d14032cc87c5de81e372da208b77b848c63fab | Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror | Download

```
# Exploit Title: Create-Project Manager 1.07 Multi XSS /HTML injection Vunlerabilities
# Google Dork:N/A
# Date: 2020-05-06
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://codecanyon.net/item/create-project-manager-with-authenticator/20483329?s_rank=3
# Version: 1.6
# Tested on: 5.4.0-kali4-amd64

------------------------------------------------------------

About :

Create! freelancer manager is a complete project management solution for developers, freelancers and software
companies, it offers powerful tools for project development, tracking each developer work time for each
project, generating invoices for online payment, complete social network with chat and news feed for
developers, and powerful financial section for income and expenses..

Summary:

Multi Persistent Cross-site Scripting and HTML injection in Create 1.07 - Freelancer Project Manager


PoC :

1- Go to any of following:

A-Online chat
B-Social feed
C-Message (title-tag)
B-Add new client (all-tags)

2- In the text  field  type your payload :
<h1>vvv</h1>
<svg onload=confirm()>

3-then hit Enter


4- Once the admin or users receive the message or read /visit the post feed   ... they will be xssed


Impact:
XSS can lead the adminstators & users Session Hijacking,it can also lead to disclosure of sensitive data  and
other critical  attacks on administrators and the webapp directly.



Screentshoots:
A-Online chat https://i.imgur.com/nNGVoXI.png
B-Social feed https://i.imgur.com/yQle2Mn.png
C-Message (title-tag) https://i.imgur.com/8usFkJ7.png
B-Add new client (all-tags) https://i.imgur.com/oWYA88d.png
```


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
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
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 (1,690)
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)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

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