WordPress Car Rental System 1.3 Cross Site Scripting

Authored by thelastvvv

Posted Apr 5, 2020

WordPress Car Rental System plugin version 1.3 suffers from a cross site scripting vulnerability.

tags | exploit, xss

SHA-256 | 523216c145f26fc498052954f1e88ae2f86eb16a3ce5c722d0524a6e721be633 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: WordPress Car Rental System 1.3 XSS Vunlerability
# Google Dork:N/A
# Date: 2020-04-04
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://codecanyon.net/item/car-rental-system-wordpress-plugin/4239755?s_rank=3
# Version: 1.3
# Tested on: 5.4.0-kali4-amd64

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


Summary:

Persistent Cross-site Scripting in Customer registration-form   all-tags

PoC 1:



1- Go to the car renting page then choose new customor
http://example/wp-car/

2- In "any " field of registration form type your payload :
 "><img src=x onerror=prompt(document.domain);>

3-then hit CONTINUE


4- Once the admin logs in and go to Booking list or customer lookup page ... the admin will be xssed


http://example/wp-car/wp-admin/admin.php?page=booking-list
or
http://example/wp-car/wp-admin/admin.php?page=cust-lookup




Impact:
XSS can lead to adminstators/users's Session Hijacking, and if used in conjunction with a social engineering
attack it can also lead to disclosure of sensitive data, CSRF attacks and other critical  attacks on
administrators directly.


Other infos:

Supported Wordpress versions:
  WordPress 4.9.x
  WordPress 4.8.x
  WordPress 4.7.x
  WordPress 4.6.1
  WordPress 4.6
  WordPress 4.5.x
  WordPress 4.5.2
  WordPress 4.5.1
  WordPress 4.5
  WordPress 4.4.2
  WordPress 4.4.1
  WordPress 4.4
  WordPress 4.3.1
  WordPress 4.3,
  WordPress 4.2,
  WordPress 4.1,
  wordPress 4.0

Screentshoots:

https://imgur.com/5Mt5sR0
https://imgur.com/xyd4dur
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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