Web安全 -- 逻辑漏洞讲解

小峰 / 2018-02-01 18:09:12 / 浏览数 8865 新手 入门资料 顶(2) 踩(0)

逻辑漏洞

逻辑漏洞应用在方方面面，主要是根据应用不通产生的逻辑方面漏洞不同。比如金融网站和互联网网站以及购物网站，挖掘逻辑漏洞方法完全不一样。所以本篇算是冰山

常规漏洞漏洞

逻辑漏洞是指由于程序逻辑不严或逻辑太复杂，导致一些逻辑分支不能够正常处理或处理错误，一般出现在一下几个方面：

- 任意密码修改（没有旧密码验证）
- 越权访问
- 密码找回
- 交易支付金额
- ……

登陆时，是否可以绕过验证码形成撞库

登录处主要存在的点

- 返回包中有验证码
- 返回页面 hidden中有验证码
- 有些其他登陆url中不需要验证码
- 验证码不变，验证码没有一个完整的服务请求，只在刷新url时才变
- 第一次请求包验证了验证码是否正确，第二次请求不需要验证
- 拦截登录时验证码的刷新请求，第一次验证码未失效，可绕过
- 验证码和用户名、密码是否一次同时提交
- 公众号，app无验证

实例-反向爆破漏洞

在我们得到相关信息后，可以通过截断把加密后的密码确定为固定项，把其他用户信息用密码本的形式进行爆破，可以暴力测试账号与密码是否匹配。

168168加密后得到以下字符串，并尝试登录成功

```
08E304A899D50BC4ACDBFB56D0EBFD1E303FD10D1A37BB45547CB5D98323191003EBC244F8480D9110B403E621B40327B3E41B96D0FD87D803DFC176E0B580
```

当我们把密码固定后利用系统验证可以绕过的漏洞，可以对银行号进行爆破，众所周知，银行卡密码为6位数字，而且有很多为123456等弱口令，可以利用他系统的加密方

密码找回

- 验证码回传
- 验证码时间长，不失效可爆破（字典可去除全1重复数多的）
- 修改密码，修改发送手机号修改为自己可控，
- 邮箱验证可猜测
- 假如找回需要4部，最后一部有user参数，用自己账号正常到第三部，第四部修改user实现逻辑
- 可以跳步找回（直接访问页面）
- 本地验证，修改返回值
- 服务器验证为空，包中直接删除验证码
- 个别验证码全0可绕过
- token生成可控（wooyun两篇实例）
- cookie覆盖
- 删除验证码校验，绕过

实站-网易邮箱密码重置

首先注册一个126邮箱测试帐号

然后会跳转到一个手机绑定得安全提示上

这个链接注意下参数，有个uid，将uid修改为要黑掉的网易邮箱帐户

填入一个你可控的手机号码，将确认码发回来

点击确定并进入邮箱，这个时候这个目标网易邮箱已经被越权绑定了密保手机。
然后走正常的密码取回流程，发现这个邮箱多了一个通过手机的取回方式，这个手机尾号就是我刚刚绑定的手机！

密码重置成功！！

漏洞证明：

存在权限判断不当，越权操作的接口是：

`http://security.mail.126.com/mobileserv/mbp.do?uid=[■■■■■■■■■■■■]&backurl=`

支付

- 金额运费修改
- 修改bxprice，可改成任意负数金额数量
- 请求重放，多次下单
- 并发（数据库操作加锁）
- 参数污染 请求没该参数，却返回该参数，可请求该参数污染返回值

越权逻辑漏洞

越权访问漏洞，又可以分为横向越权访问漏洞与纵向越权访问漏洞两类。

横向越权访问漏洞

指的是权限平级的两个用户之间的越权访问。
比如，一个正常的用户A通常只能够对自己的一些信息进行增删改查，但是由于程序员的一时疏忽未对信息进行增删改查的时候进行一个判断，判断所需要操作的信息是否属

实例- 51社保某处越权查看任意用户信息漏洞

厂商 dingxue
问题点

/shebao/fillinfomation?insurance_location_id=6&employee_id=203§66§&person_id=*&action=zr01

危害描述

- 权限绕过查看任意用户个人信息，姓名，身份证等
- 漏洞产生原因
- 参数未过滤
- 测试过程

访问微小宝 `http://***.***.**.***:8015/` ，注册登录，填写个人信息，
在填写参保人信息处存在越权，`employee\_id`参数可被遍历：

数据包如下：

```
GET /shebao/fillinfomation?insurance_location_id=6&employee_id=***§66§&person_id=***&action=zr01 HTTP/1.1
Host: ***.***.**.***:8015
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://101.200.47.130:8015/insuranceGoods/InsuredCity?employee_id=20367&person_id=1906&action=zr01&ppkstr=23a0c06b&si
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=38472b126ad61367accf611ee2177868; sensorsdata_is_new_user=true; mediav=%7B%22eid%22%3A%22247642%22%2C%22ep%2
Connection: close
```

纵向越权访问漏洞

- 指的是权限不等的两个用户之间的越权访问。
- 一般都是，低权限的用户可以直接访问高权限的用户的信息。

比如，在论坛中，你是一个普通用户，有一天，你通过burpsuite抓包修改了自己的用户ID为管理员的用户ID，一不小心，成功登陆了管理员的账号。

实例-湖南科创cms通用注入漏洞

打开网站，经过查找探测发现注入点，漏洞参数为ZNSearch，类型为盲注、字符型注入。

http://www.chinacreator.com/login.jsp

发现注入点存在于字段userName中
当用户利用万能密码进行测试时就可以突破网站的权限限制，成功利用到管理员的身份。这是最简单的也是最典型的纵向越权，可以让普通用户获得管理员的身份进行访问。

```
POST /login.jsp HTTP/1.1
Host: www.chinacreator.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.chinacreator.com/login.jsp
Cookie: JSESSIONID=34BA53DE1B50A0A67339B330D6E26E2E; USERNAME=admin'
X-Forwarded-For: 8.8.8.8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 102

flag=yes&macaddr_=&machineName_=&machineIp_=&userName=admin%27&password=asdf&yzm=7407&subsystem_id=cms
```


上一篇：Web漏洞导图 下一篇：AceBear Security ...
1. 0 条回复
   - 动动手指，沙发就是你的了！