

这些年遇到过的逻辑漏洞

Blood_Zer0

About Me

ID: Blood_Zer0

目前就职于 饿了么

漏洞盒子,滴滴,平安,携程等SRC活跃白帽子

配过设备,做过运维,搞过渗透,现在专职研究漏洞

目 录

1· 挖洞神器

2· 漏洞介绍

3· 案例分析

4· Q&A

The background is a deep, dark blue. The lower portion of the image shows a textured surface, possibly a floor or ground, with subtle variations in tone and some faint, darker lines. Above this surface, numerous light blue hexagonal shapes of varying sizes are scattered across the upper half of the frame. These shapes appear to be floating or falling, creating a sense of depth and movement. The overall lighting is dim, with the hexagons providing the primary source of light in the scene.

挖洞神器

White Hat

WAF功能的增强;

安全测试演变为第三阶段;

- 1、基于功能/性能的"安全测试"
- 2、基于漏洞的安全测试
- 3、基于业务的安全测试

开发人员代码安全性增强;

Application

逻辑漏洞特点	Bypass一切防护设备
	没有有效的自动化工具
	再牛逼的程序员都可能造坑
	业务逻辑复杂造成的坑

正常操作流程
记录数据包

分析数据包
找到敏感参数

修改数据包
验证猜想

分析程序逻辑
判断验证机制



	地址	介绍
Burpsuit	https://portswigger.net/burp/	收费，基于Java，跨平台，功能强大
Fiddler	http://www.telerik.com/fiddler	免费&开源，基于.Net，支持通过mono的方式运行在mac和Linux上
Charles	https://www.charlesproxy.com/	收费，基于Java，跨平台
Mitmproxy	https://mitmproxy.org/	免费，开源，基于Python，跨平台

The background is a dark blue gradient. The bottom half of the image shows a textured, cracked floor that recedes into the distance. The top half is filled with numerous glowing blue hexagonal shapes of varying sizes, some of which are slightly out of focus, creating a sense of depth and movement.

漏洞介绍

逻辑漏洞

逻辑漏洞	用户相关	密码重置
		身份认证
		验证突破
		权限控制
	交易相关	请求篡改
		并发请求
		时序绕过
	恶意攻击	锁定账户
		变量篡改
		接口调用
		薅羊毛
	More	More

The background is a dark blue gradient. In the upper half, there are numerous semi-transparent blue hexagons of varying sizes, some of which are slightly blurred, creating a bokeh effect. The lower half of the image shows a dark, textured surface that resembles a stone or concrete floor, with a subtle vertical line running down the center.

案例分析

1. 购买商品，如何获取最大的优惠？

场景描述

优惠券

无可⽤ >

可⽤优惠券(0)

不可⽤优惠券(1)

1. 购买商品，如何获取最大的优惠？

攻击手法

```
GET
/?c=fnget&a=getMobileInfo&mobile=13221021764&rechargeType=1&text=50&callback=jQuery111102733480976538213_1489286441769&_=1489286441784
HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: [REDACTED]
Connection: close
```

```
GET
/?c=fnget&a=getMobileInfo&mobile=13221021764&rechargeType=1&text=10&callback=jQuery111102733480976538213_1489286441769&_=1489286441784
HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: [REDACTED]
Connection: close
```

2. 想要优惠券，如何让系统发更多？

场景描述

输入手机号领取红包

请输入手机号码

马上领取

红包已放至账户 [修改>](#)
登录 App 即可使用

2. 想要优惠券，如何让系统发更多？

攻击手法

? Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads:

并发的线程数

Number of retries on network failure:

网络失败重试次数

Pause before retry (milliseconds):

重试的暂停间隔

Throttle (milliseconds):

☒ Fixed

请求延时

☐ Variable: start

step

Start time:

☒ Immediately

☐ In

minutes

☐ Paused

3. 只有一个self-xss，如何扩大危害？

场景描述

编辑用户 Blood_Zer0

用户名 *

Blood_Zer0

此用户名将作为用户登录时所用的名称。
请不要与系统中现有的用户名重复。

电子邮箱地址 *

Blood_Zer0@126.com

电子邮箱地址将作为此用户的主要联系方式。
请不要与系统中现有的电子邮箱地址重复。

用户昵称

Blood_Zer0

用户昵称可以与用户名不同，用于前台显示。



3. 只有一个self-xss，如何扩大危害？

攻击手法

```
POST /video/tags/update?tt=1481553822940364 HTTP/1.1
[redacted]
Connection: close
Content-Length: 31
Origin: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Maxthon/4.9.3.1000 Chrome/39.0.2146.0 Safari/537.36
Content-type: application/json
Accept: */*
DNT: 1
Referer: [redacted]
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN
Content-Length: 32

{"ids":["93902"],"tags":"aaaa"}
```

```
POST /video/tags/update?tt=1481553822940364 HTTP/1.1
[redacted]
Connection: close
Content-Length: 32
Origin: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Maxthon/4.9.3.1000 Chrome/39.0.2146.0 Safari/537.36
Content-type: application/json
Accept: */*
DNT: 1
Referer: http://www.kayun.com/manga.html
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN
Content-Length: 32

{"ids":["93901"],"tags":"aaaa"}
```

漏洞延伸

T

H

A

N

K

S



Q&A