

wife_wife

wife_wife

×

题目详情

WriteUP

上一题

下一题

随机一题

wife_wife

GFSJ1192

积分 4

金币 4

62 最佳Writeup由 why404 提供

收藏

反馈

难度: 4

方向: Web

题解数: 4

解出人数: 2441

题目来源: CATCTF

题目描述: cat-wifi

本题不需要爆破

题目场景: http://61.147.171.105:51192

100%

倒计时: 3时24分23秒


延时

删除场景

题目已回答正确 ✓

今日终于可以用adworld了，就直接先把封面三道题写了

第一道题明确表示不是爆破，可以通过注册手段获得一个伪flag，这个是假的



Username


tll123

Flag

CatCTF{no_fl4g_4_u_6ut_you_h@ve_w1fe}

Wife

nilou.jpg



接着如何扩展是问题，网上偷看了一下wp后，明白这是一个js原型链污染

这里需要先学习一下Javascript原型链污染的知识: [https://drun1baby.top/2022/12/29/JavaScript-原型链污染/#1-什么是原型 \(JavaScript-原型链继承\)](https://drun1baby.top/2022/12/29/JavaScript-原型链污染/#1-什么是原型 (JavaScript-原型链继承))

简单来说就是：

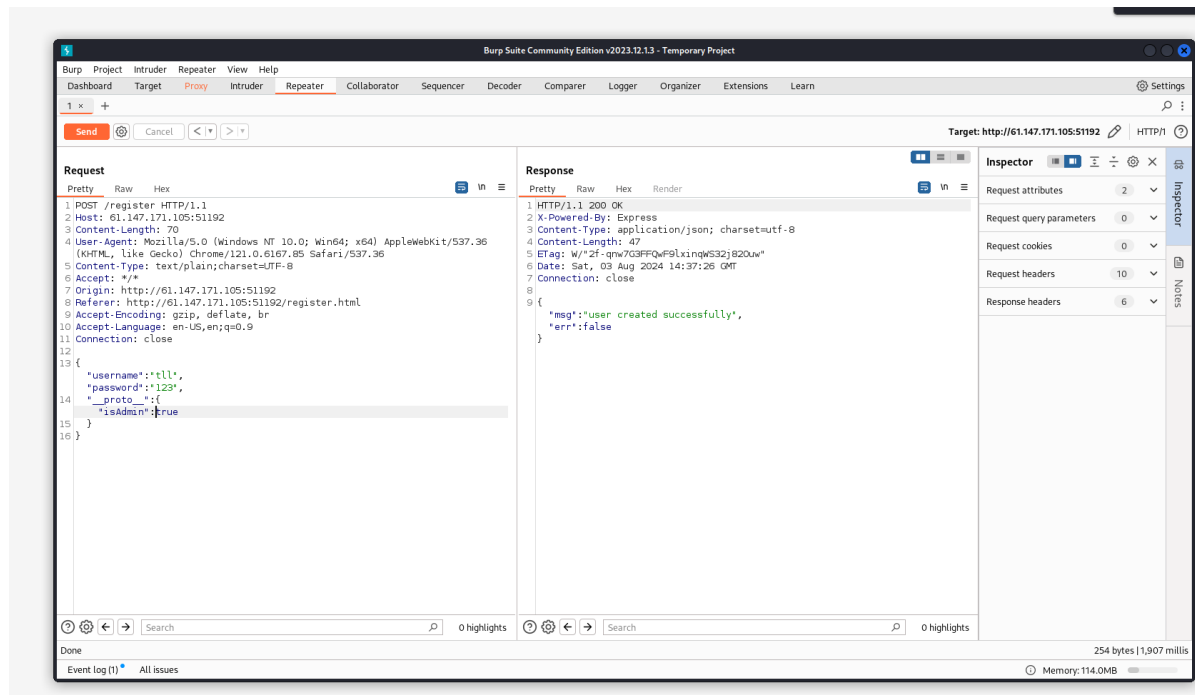
`prototype` 是 `newClass` 类的一个属性，而所有用 `newClass` 类实例化的对象，都将拥有这个属性中的所有内容

- `newClass` 类实例化的对象 `newObj` 不能访问 `prototype`，但可以通过 `.__proto__` 来访问 `newClass` 类的 `prototype`
- `newClass` 实例化的对象 `newObj` 的 `.__proto__` 指向 `newClass` 类的 `prototype`

这其实就导致了“未授权”的出现

利用该漏洞的前提是后端使用**Node.js**语言

所以对于这道题，我们使用`__proto__`越权对于后端进行管理员权限的获取



但我说实话这题没有给暗示下要想到这里，还是一个黑盒测试的情况太难想了，更别说谁用js做服务器处理信息啊。

ezbypass-cat

这道题上来也是一个登录框，尝试了一下wffuzz, ssti, sql都没结果

在js的框架中找到是华夏erp，可以去searchsploit漏洞

[华夏ERP漏洞之授权绕过漏洞+后台命令执行漏洞=未授权命令执行 | CN-SEC 中文网](#)

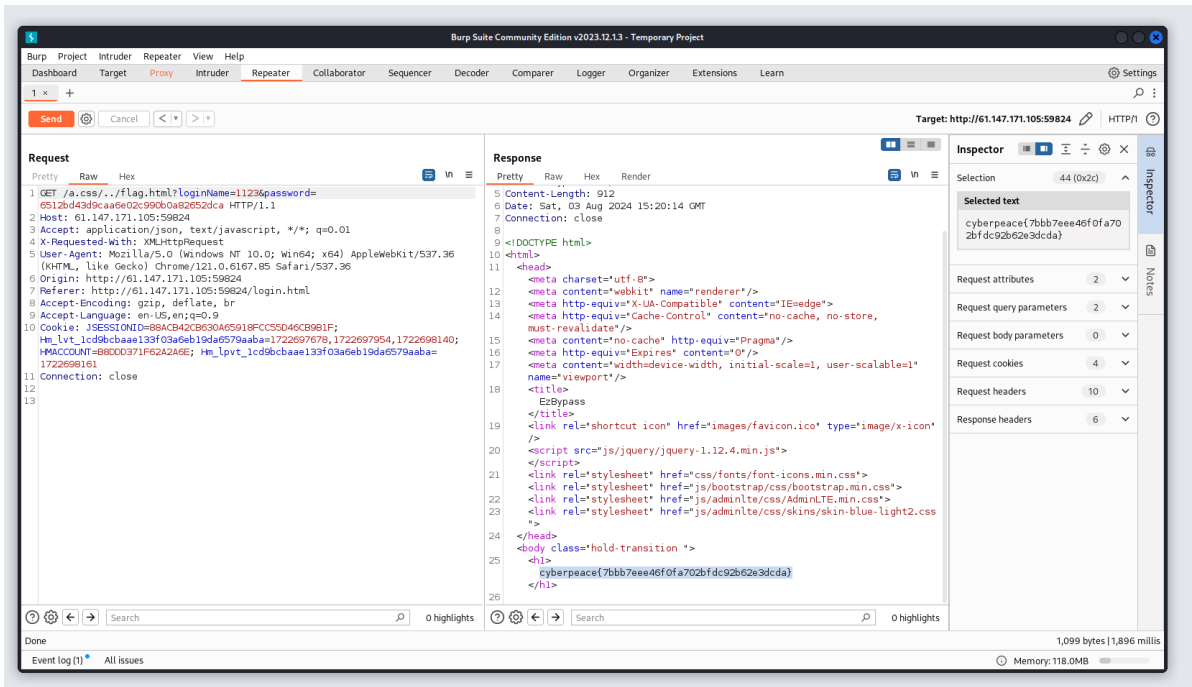
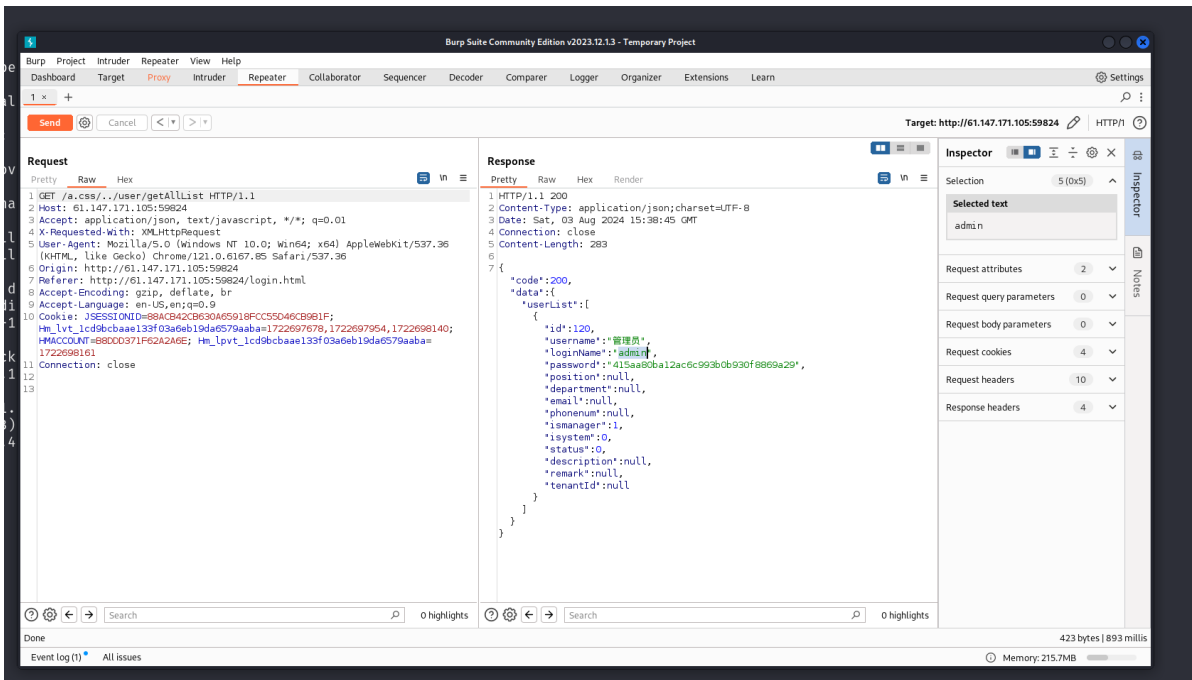
在这个文章中介绍华夏erp存在白名单绕过漏洞，所以通过构造白名单直接抓出flag（不过这样的方法太有目的性了，应该追求一个更普遍性的方法

我的想法是通过gobuster跟着/a.css/..下的目录继续爆破

不过看到网上说可以直接访问接口/jshERP-boot/user/getAllList;.ico 获取后台账户，不过这里却是404

更改了一下构造，用css绕过白名单后猜测目录，获取密码

直接就可以获取cookie直接用dirsearch获取到想要的目录，比上面说的盲猜flag文件好多了



上一题

下一题

随机一题

ezbypass-cat

GFSJ1183

积分 4

金币 4

15 最佳Writeup由 cxj9699 提供

收藏

反馈

难度: 4

方向: Web

题解数: 8

解出人数: 1371

题目来源: CATCTF

题目描述: ezbypass-cat

题目场景: http://61.147.171.105:59824

100%

倒计时: 3时29分43秒

延时

删除场景

题目已回答正确

近30天答题人数统计