BUG-adworld

一个登录框，又是sql?

首先随便点点，可以通过注册账户登录，但是manage提示非admin

那这么越权？看看找回密码功能？也不知道生日和地址

在登录抓包时候发现cookie多了一个user后面跟了一串

这个可以通过hashi识别一下（简单题也就md5了还能有啥

还真是，虽然但是原来的md5网站解密要钱！但肯定是md5，，，解不出来偷偷看wp吧（

是一个uid：username的配置，这里尝试能不能提权到admin，猜测是1：admin

但是这样的尝试登录上去还是普通用户

在persional处发现有id=的url，并且这里发现cookie也有相同的user，进行一次cookie的串改

```
1: admin------4b9987ccafacb8d8fc08d22bbca797ba
```

成功获得信息，进行改密码登录

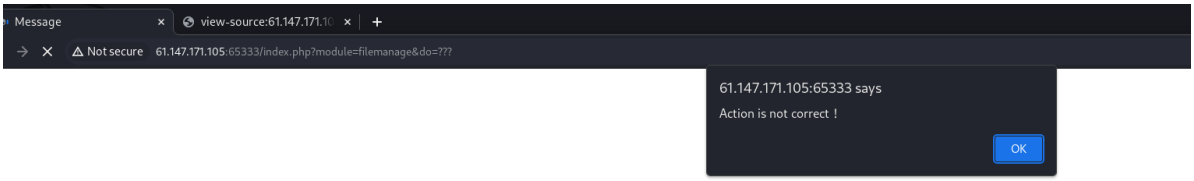
然后要求改ip，添加http头就行了，很简单的一关

```
X-Forwarded-For: 127.0.0.1
```

这里又卡住，只能枚举找思路

filter中间流？不对

看到代码页面·指向一个filename的文件，但是不让我访问



啥意思啊。？？？是让我来猜吗？那我用wfuzz来fuzz

wfuzz爆破不了，他都是200能访问，只不过重新定位回去而已。

直接问ai来手工测吧

可以尝试以下操作名称，看看是否有响应：

- `upload`
- `download`
- `delete`
- `edit`
- `view`
- `rename`
- `move`
- `copy`

运气不错第一个就是upload

猜测先搞个图片码上去，回复 你知道我想要什么，把我pass。

接着我尝试改成php4文件后缀，上传说这不是一个php文件，但是回显不一样，肯定是在后缀上绕过了，但内容不过。（同样试php5可以，php7，8不行

但是这个内容哪里有问题？

通过查询得知古老的语法

```
<script language="php">system("ls");</script>
```

但是这种古老的php4语法谁还用呢？觉得有点冷门了

最后看了下wp还说有文件头查询，不过我传的就是图片码，这一个绕过就自动过了

总结：首先是简单的过程分析提权，和x-forward代理（这里可以用firefox插件进行自动）

对php语言版本的学习，与文件上传的绕过