

对湾湾两所大学的初步渗透（常规思路）

这两所大学在下文中分别简称湾仔和口罩。湾仔的描述过程中因为时间原因，缺少了一些截图，所有过程也只是利用的 top10 罢了。主要讲述了我从 0 到 1 积累的经验(大佬莫笑)。

湾仔

初步成果：GET 教學務系統

过程概述：1.湾仔网上报修系统 2.湾仔造物学系主页 3.湾仔資源 xx 研究学院 4.华侨管理系统 5.体育器材管理系统 6.整理数据 7.撞入邮箱 8. 教學務系統

信息搜集：只确定了所在的 B 段 1x0.xxx.0.0/16

1. 湾仔网上报修系统

失败方法：

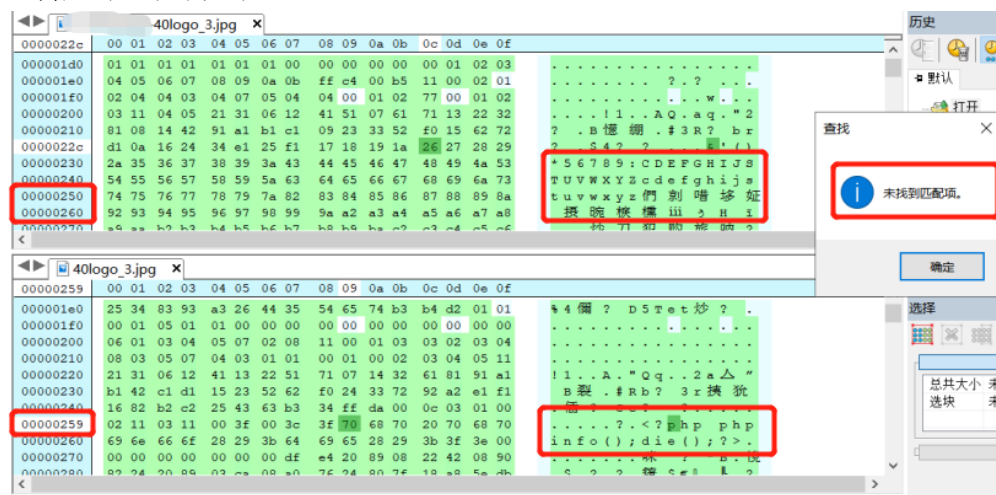
(1) 在这个系统里无需注册即可发布修复信息，且在水电维修时可以上传图片。且后续未更改。



首先用的图片马进行黑白名单尝试，可以为 PHP 后缀。但是发现上传的图片进行了图片渲染。尝试多次上传再嵌入 PHP 代码也无果，后放弃。在这里不再重新上传，使用之前的图片。



上传后对比效果如下：



(2) 通过维修分类处拿到系统的登陆账号密码

三个账号中只有 reply 为 0 的可以登录，且登陆后发现账户只有查看删除的作用，无法 GETSHELL，后放弃。



ID	password		name	email	firstTime	lastTime	reply
NONE			等待處理中		20		00 (1
Z0	80	120		cg0000@edu.tw	20	019	1
ta	a8	ad	泰	tai@.com	21	019	0
Z0	bc	a5		yuhsu@edu.tw	25	019	1

Tai:

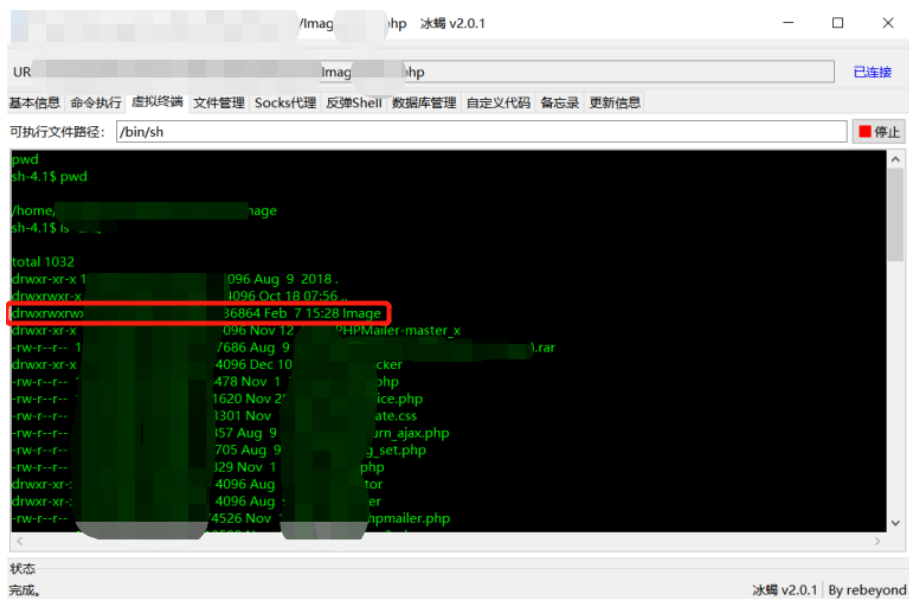


成功方法：

在维修分类处存在 SQL 注入，root 权限，但未得到绝对路径。

假装有注入图

尝试了 sqlmap 字典中的路径皆无果。尝试写入爆破出来的文件路径，images、gmail、Image 等等。最后成功写入 Image，shell 上去后看到了 Image 如 upload 这种文件夹一样为 777

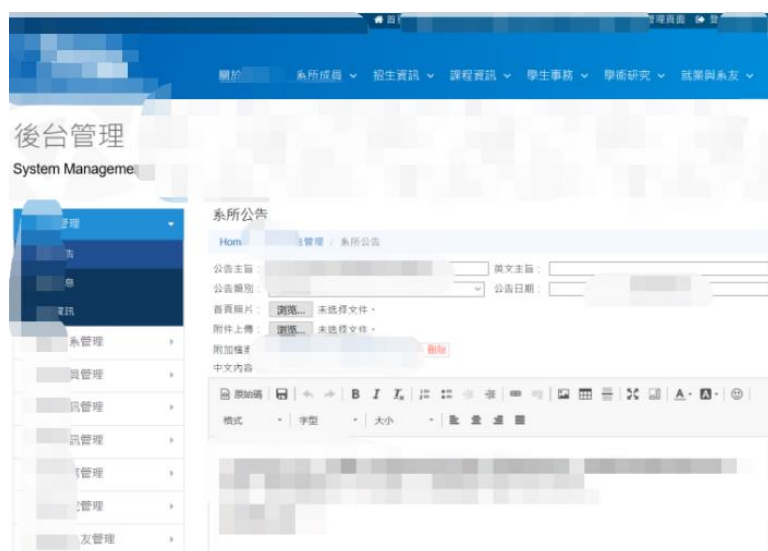


最后在数据库里得到了一些账号，暂且放着。

名称	修改日期	类型	大小
...	2019/10/...	文件夹	
...he_borrow	2019/10/...	文件夹	
...l	2019/10/...	文件夹	
...est	2019/10/...	文件夹	
...ess	2019/10/...	文件夹	
...em	2019/10/...	文件夹	
...m2014	2019/10/...	文件夹	
...2014old	2019/10/...	文件夹	
...azu	2019/10/...	文件夹	
...4old2	2019/10/...	文件夹	

2.湾仔造物学系主页

在某处发现时间盲注（哪里忘了，sqlmap 记录清空了），经过大半天的时间拿到了一些类似密码的 MD5 值。很多都解不出来，只解出了账号 `txx dxxxxxx`，成功登录后台。



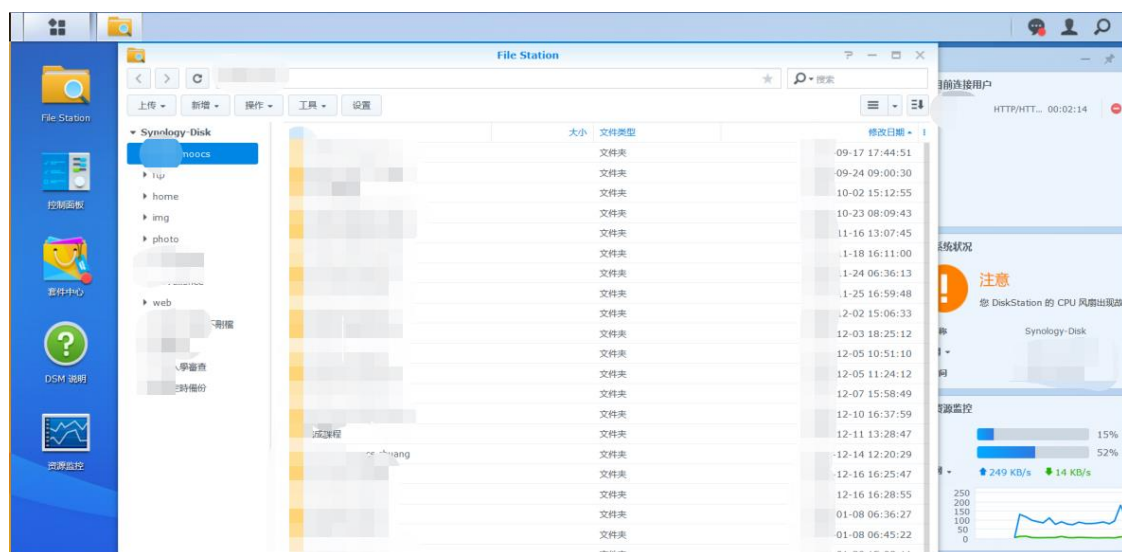
浏览了一遍所有功能，虽有上传点。但是用的是某个新版本的编辑器，无法绕过上传。测目录浏览时发现网站的报错很特别，仔细一看这不是某晖的服务器么。

404

您要找的页面未找到。

这台服务器还是 5001 端口，抱着试一试的心情输入后台解出来的唯一的账密。最后成

功撞入。



通过浏览发现除了某系主页之外，还有一些老师学生 2014 年的活动信息。综合得到了一两百个账号密码。先留着最后再一起撞。

sMap	2019/10	文件夹
	2019/10	文件夹
	2019/10	文件夹
2014	2019/10	文件夹
2019	2019/10	文件夹
atas	2019/10	文件夹
2014	2019/10	文件夹

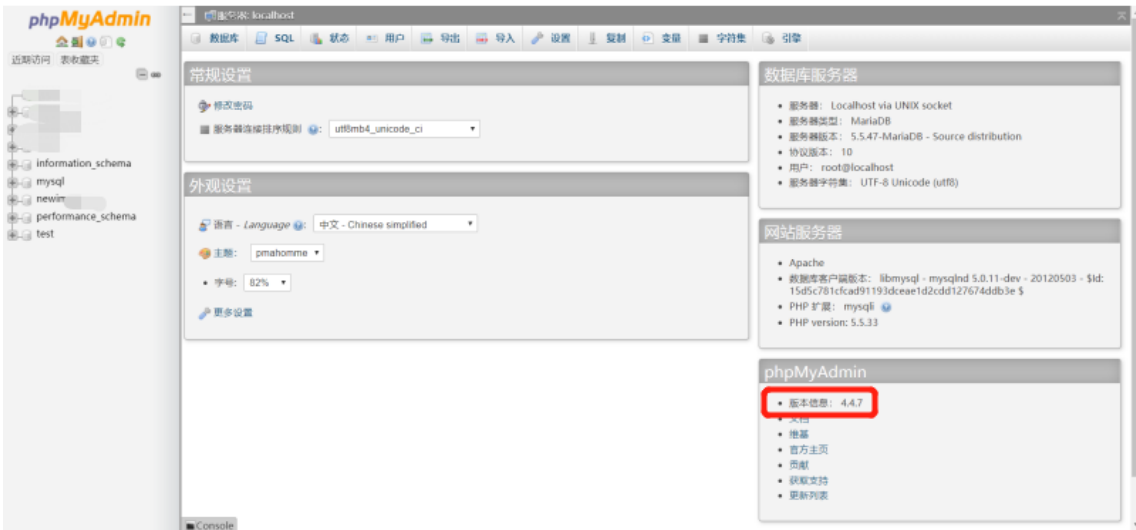
3.湾仔资源 xx 研究院

看到这学院主页时发现适合 2 一样的模板，且都是某晖服务器。

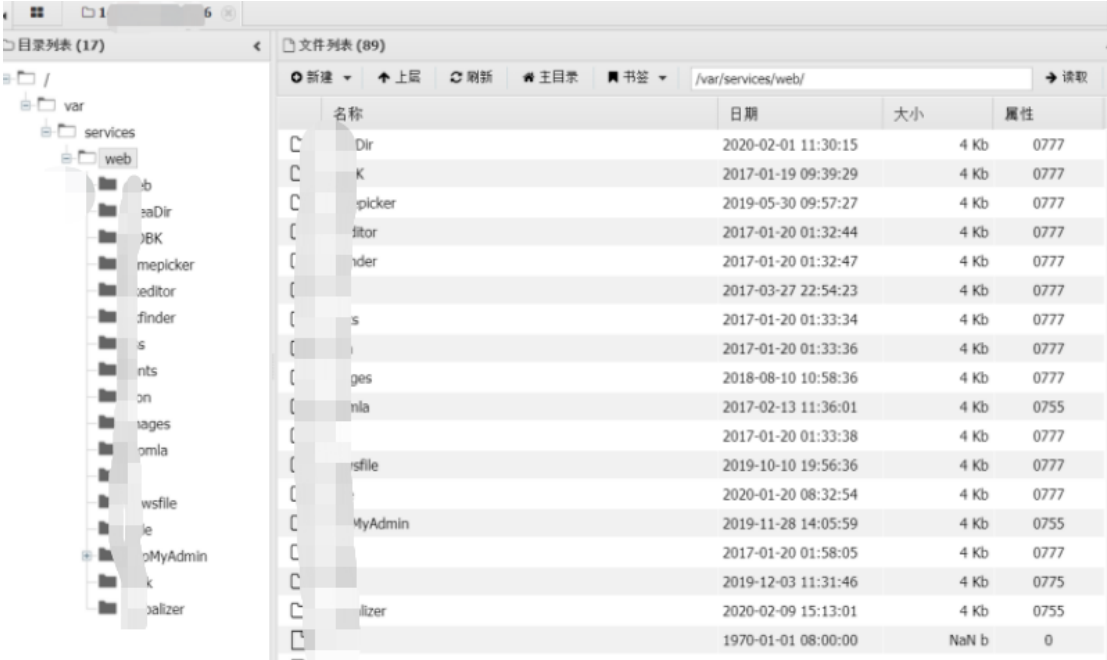


尝试 2 的管理员密码撞失败，还是大半天得到了几个解不出后台 MD5。看来按照 2 的做法是行不通了。

信息搜集时发现 phpMyAdmin，通过注入解管理员密码得到账密 imaxxx imaxxx46xx。成功登录，发现版本 4.4.7。尝试日志和写入木马。但是没有绝对路径最后无果。



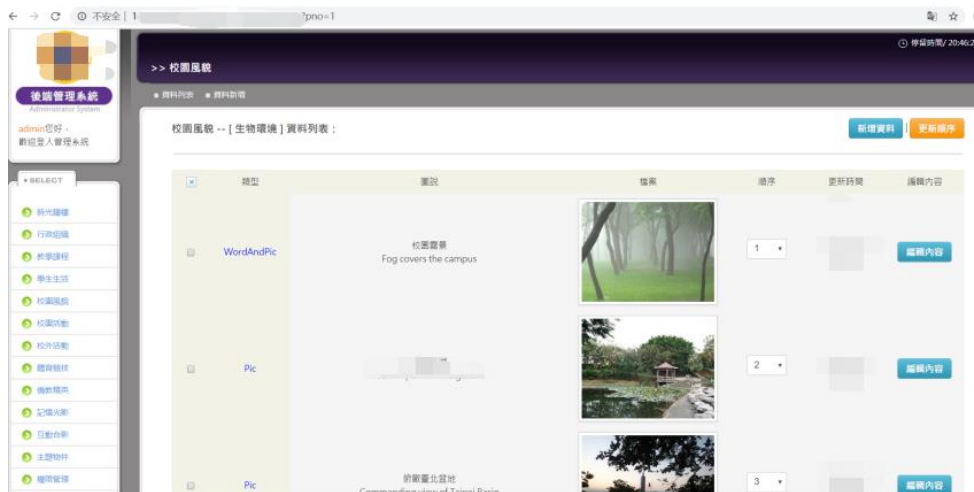
虽然得到了数据，按理说可以撤了。但是就差一点了，想再试试。突然想到同样的模板路径和文件会不会是一样的呢？最后尝试 2 的服务器所有的 777 目录，成功写入 webshell。连入后发现自己运气不错，有好几个 777 的目录。



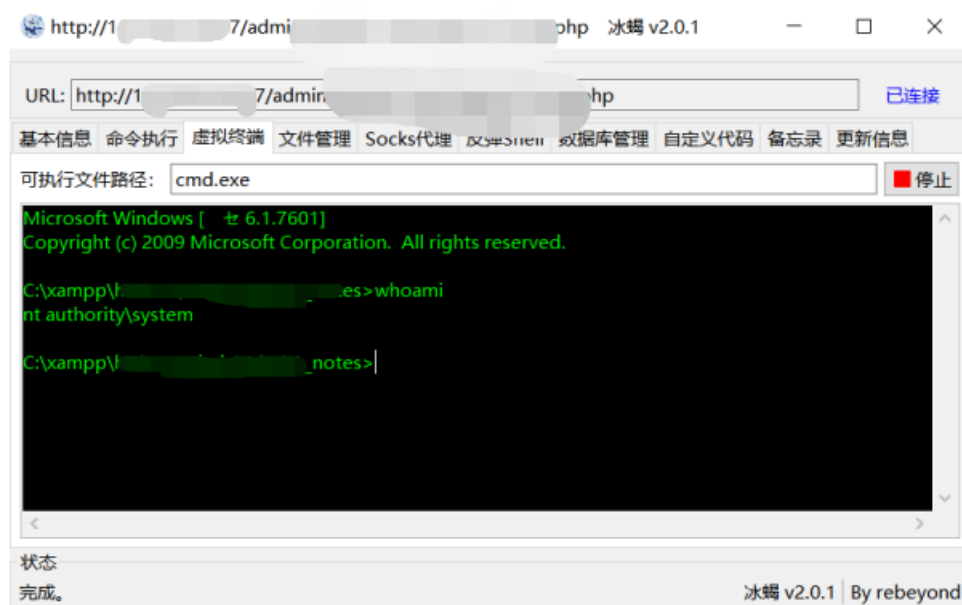
最后得到了一堆账号杂乱的信息，暂且放着。

4. 华侨管理系统

admin admin 进去，上传文件处 GetShell。



权限为 system，但是无内网，数据库无价值。故留着做跳板机。



5. 体育器材管理系统

我也忘了，大概是禁用 JS 跳转后，未授权上传吧。没什么重要数据且是低权限。也就没啥印象了。

名称	日期	大小	属性
GameUserCfg	8-21 06:04:17	0 b	0777
Imges	8-21 06:04:17	0 b	0777
SQL	8-21 06:04:17	0 b	0777
Server	8-21 06:04:17	0 b	0777
Shop	8-21 06:04:17	0 b	0777
char	8-21 06:04:17	0 b	0777
images	8-21 06:04:17	0 b	0777
imagess	8-21 06:04:17	0 b	0777
includes	8-21 06:04:17	0 b	0777
javascript	8-21 06:04:17	0 b	0777
map	8-21 06:04:17	0 b	0777
uco	8-21 06:04:17	0 b	0777
	3-16 19:59:10	3.17 Kb	0666
	3-16 19:59:10	1.61 Kb	0666
	3-16 19:59:10	244.67 Kb	0666
	3-16 19:59:36	6.1 Kb	0666
	3-16 19:59:36	1.05 Kb	0666
	3-16 19:59:44	8.89 Kb	0666
	3-16 19:59:56	1.58 Kb	0666

6.整理数据

俗话说得好,渗透就是信息搜集的过程。这时候我要做的就是整理之前的所有账号密码,如果数据无价值则继续拿 shell。

5 个 shell 里面头 3 个数据很多, 4、5 几乎放弃。首先确认自己要撞的接口, 一个是教务系统, 一个邮箱。

帳號account: [redacted]@mail[redacted].edu.tw

密碼password: [redacted]

語言language: Personal Predefined Config.

☐ 記住帳號 ☐ 開新視窗

登入

[\[電子郵件管理辦法\]](#) [軟體使用說明](#)



在这里都有限定登录账号的格式，且都没有验证码。故此偷懒些只需要把 md5 解出来，提取出部分邮箱的账号直接撞就行了。

花了整整一下午把 3 个 shell 的数据库都看了一遍，筛选出了 423 个账号。

410	ts	WKR3	HLVcFpea37fo=	ya	War	gmail.com
411	r	Orbb	yWit4zNLk7A=	r05	恒	.edu.tw
412	c'	sqB3	luznvCY2ORc=		L	.com.tw
413		Khvq	cq8br+/H8g=	b8	恒	7@gmail.com
414	HaC	Khyc	cq8br+/H8g=	b8	恒	7@gmail.com
415	Li	gln	tfBT10kEmk=	48	合	3@gmail.com
416	cs	mQe'	Y3Xx3n9xYY=	70	彦	gmail.com
417	r0F	JFM	ixJqyT7dE0=	neul	自	.edu.tw
418	yu-	nUin	vF1pRokyog=	47	so	27@gmail.com
419	al	H97v	zuiEH2JEvY=	phds	亞	ail.hinet.net
420	cm	sqw0B	+oInvu7moQ=		振	.soic.org.tw
421				b01		
422	D			lur		
423	Z			882		

但是里面有两百多个 MD5! 很多都是 somd5 解不出来,cmd5 要钱。想着氪金才能变强，狠心冲了 100 进行解密。最后到吃晚饭时终于结束了这部分工作。

密码.txt	2019/10/	32	文本文档	4 KB
账号.txt	2019/10/	32	文本文档	4 KB

7.撞入邮箱

首先撞了教务系统，发现一个账号都不行。心凉了大半截，心疼我解密那钱够吃一顿麻辣烫了。

继续撞邮箱，发现成功了 3 个账号。Rexxxr、jaxxxn、Lxxxd

Rexxxr:

发件人	主题	日期
	维修通知 水高修繕	02/07 16:03
	维修通知 水高修繕	02/07 15:41
	维修通知 廁所修繕	02/07 15:31
	维修通知 廁所修繕	02/07 14:34
	维修通知 廁所修繕	02/07 11:00
	维修通知 水高修繕	02/07 10:21
	维修通知 水高修繕	02/07 09:30
	维修通知 廁所修繕	02/07 09:04
	维修通知 廁所修繕	02/07 09:04
	维修通知 水高修繕	02/06 15:03
	维修通知 水高修繕	02/06 11:42
	维修通知 水高修繕	02/06 11:40
	维修通知 水高修繕	02/06 09:25
	维修通知 水高修繕	02/06 09:23
	维修通知 水高修繕	02/05 21:15
	维修通知 廁所修繕	02/05 20:54
	维修通知 水高修繕	02/05 16:37
	维修通知 水高修繕	02/05 16:28
	维修通知 水高修繕	02/05 15:55
	维修通知 廁所修繕	02/05 15:48
	维修通知 水高修繕	02/05 11:57
	维修通知 水高修繕	02/05 11:49
	维修通知 水高修繕	02/05 10:00
	维修通知 水高修繕	02/04 22:10
	维修通知 水高修繕	02/04 16:37

Jaxxxn:

发件人	主题	日期
	维修通知	01/05 09:11 2 K
	维修通知	12/31 11:13 19 K
	维修通知	12/29 08:38 10 K
	维修通知	12/29 08:59 12960 K
	维修通知	12/19 16:12 2 K
	维修通知	12/09 13:48 58 K
	维修通知	12/09 11:40 45 K
	维修通知	11/26 09:52 20 K
	维修通知	11/15 15:34 1071 K
	维修通知	11/15 08:06 278 K
	维修通知	11/08 17:20 10 K
	维修通知	11/07 14:32 1024 K
	维修通知	11/07 14:05 28 K
	维修通知	10/28 15:38 102 K
	维修通知	10/28 11:20 16 K
	维修通知	10/25 08:21 14 K
	维修通知	10/14 11:13 20 K
	维修通知	10/14 10:30 19 K
	维修通知	10/09 13:15 23 K
	维修通知	10/08 22:44 16 K
	维修通知	10/08 21:48 15 K
	维修通知	10/03 15:51 8 K
	维修通知	09/29 14:40 431 K
	维修通知	27 11:59 413 K
	维修通知	26 14:43 22 K

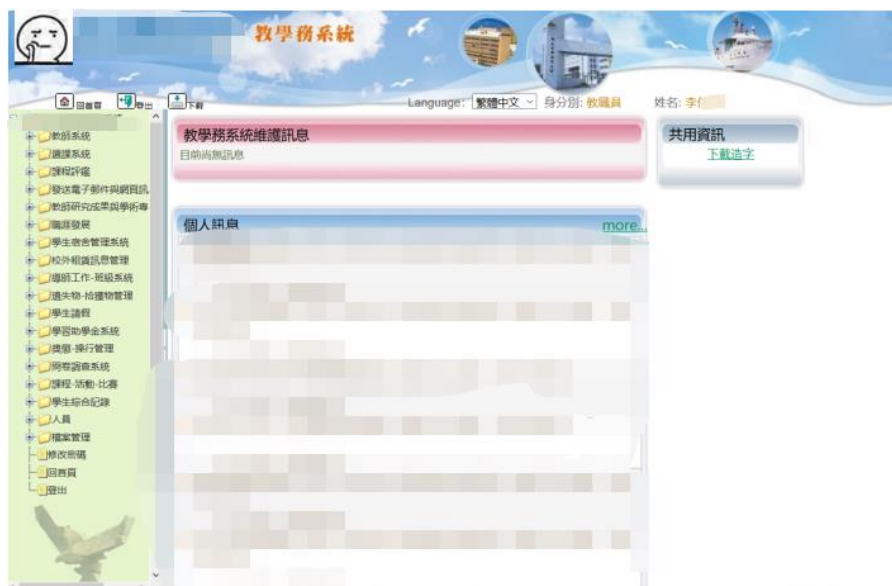
Lxxxd:

https://arspb.most.gov.tw/info.do
帳號 a[redacted]7
密碼 a[redacted]9
管2A 00[redacted]
李[redacted]
00[redacted] 黃[redacted]
學號: 00[redacted]
姓名: 曾[redacted]
邱[redacted]
D22200****
[redacted].edu.tw
092[redacted]

这些信息无法开拓战果，故此认为本次获取的数据毫无作用。
但是峰回路转，没想到在邮箱处竟然有此教授教务系统的账号！



因此使用邮箱密码+泄露的账号，成功进入教务系统。



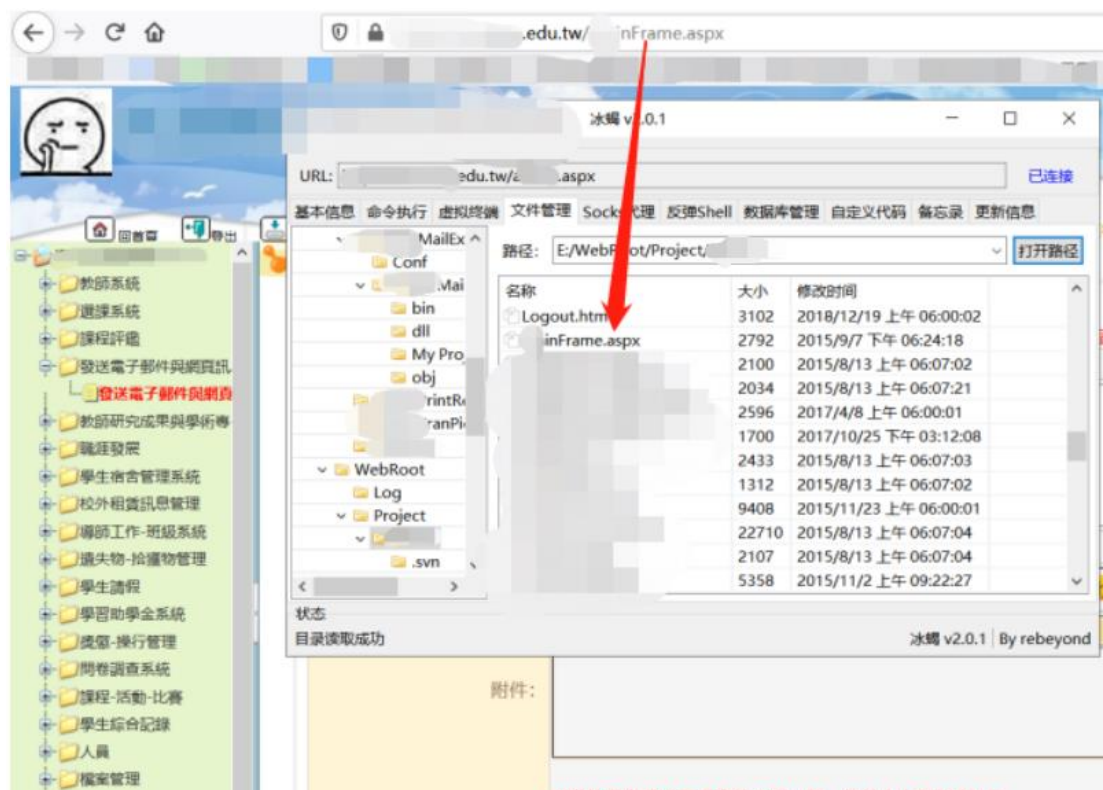
8. 教學務系統

进入教务系统后把每一个选项都点开来看了一遍，发现这里仅有一处上传。

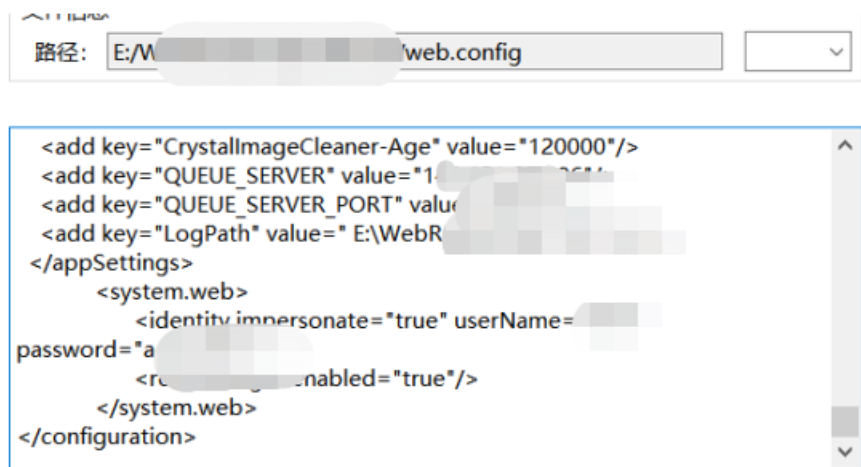
但是上传的文件找不到路径，也没有 fuzz 到路径。事已至此不能放弃，又把所有功能都看了一遍。竟然找到了一个任意文件下载，故此从下载主页看代码到最后找到文件的路径！



最后拿到教务处的 shell



也拿到了最重要的数据库的 IP 账号密码



湾仔初期篇到此结束

口罩

初步成果：同服：教师差勤系统、学校人事部、大学内部投票系统等等 4 个系统...

过程概述：1.口罩某学院 Axxxx 认证系统 2.口罩大学生实习申请系统 3.口罩大学农用教学申请中心 4.口罩大学兽医医院 5.口罩大学公共研究所 6.口罩物理系主页 7.整理数据 8.口罩大学教师服务器

信息搜集：只确定了所在的 B 段 1x0.xxx.0.0/16

1.口罩某学院 Axxxx 认证系统

遍地注入，拿到系统的登录账号密码。后台直接上传 PHP，拿到数据库的连接信息。



```
1 <?php
2 require_once 'db.php';
3 require_once 'config.php';
4 require_once 'db.php';
5 require_once 'db.php';
6
7 class SysGlobal{
8     public $dbHost      = "127.0.0.1";
9     public $dbName      = "a";
10    public $dbUser       = "a";
11    public $dbPwd        = "aa";
12    public $dbPort       = 3306;
13    public $prefix       = "a";
14    public $parasys      = "a";
15
16    public function __construct()
17    {
18    }
19
20    public function __destruct()
21    {
22    }
23
24    public function __call($name, $arguments)
25    {
26    }
27 }
```

脱裤子时遇到问题，蚁剑冰蝎都无法连接数据库，流量代理进去也不行，3306 端口映射出来也不行，msf 也不行。最后使用拖库马儿解决。

2.口罩大学生实习申请系统

口罩这个平台提供了注册功能，且不验证你的身份



申請帳號

用戶帳號申請

*申請帳號 (本校學生請使用學號)

*申請姓名

*申請密碼

*確認密碼

*申請身份

*電子郵件

*聯絡人員

帳號

密碼

注册后上传 GET

名称	日期	大小	属性
[REDACTED]	2020-01-07 15:45:46	650 b	0644
[REDACTED]	2020-01-03 23:01:08	145 b	0644
[REDACTED]	2019-06-19 23:26:32	20.41 Kb	0644
[REDACTED]	2019-05-22 14:13:42	39.29 Kb	0644
[REDACTED]	2019-05-06 01:44:58	514.91 Kb	0644
[REDACTED]	2019-05-06 01:44:21	514.91 Kb	0644
[REDACTED]	2019-05-01 23:45:23	78.88 Kb	0644
[REDACTED]	2019-05-01 23:28:17	133.1 Kb	0644
[REDACTED]	2019-05-01 23:10:23	216.39 Kb	0644
[REDACTED]	2019-05-01 15:15:18	20 Mb	0644
[REDACTED]	2019-05-01 14:50:26	60 Kb	0644
[REDACTED]	2019-05-01 01:16:34	62.77 Kb	0644
[REDACTED]	2019-05-01 01:15:21	133.1 Kb	0644
[REDACTED]	2019-04-30 23:51:42	1.79 Mb	0644
[REDACTED]	2019-04-30 23:51:41	1.78 Mb	0644
[REDACTED]	2019-04-30 22:21:36	99.52 Kb	0644
[REDACTED]	2019-04-30 20:23:29	74.69 Kb	0644
[REDACTED]	2019-04-30 17:55:34	2.54 Mb	0644
[REDACTED]	2019-04-30 14:50:17	34.68 Kb	0644

在这个平台获取大量的学生老师信息

3. 口罩大学农用教学申请中心

此平台使用了 low cms，注入进后台上传 GET。



数据没用，且无内网。故此 shell 无价值。

```

(*) 基础信息
当前路径: /var/www/
磁盘列表: /
系统信息: Linux 2.6.32-431.17.1.el6.x86_64 #1 SMP Wed May 7 23:32:49 UTC 2014 x86_64
当前用户: apache
(*) 输入 ashelp 查看本地命令
(apache:/var/www/...) $ cd /var/www/
(apache:/var/www/...) $ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::21c:56ff:fe80::21c:56ff scope link
        valid_lft forever preferred_lft forever
(apache:/var/www/...) $
  
```

4. 口罩大学兽医医院



盲注+后台+传马, 服务器中的数据价值不大。但是疑似连接学校内网, 先留着中期玩玩。

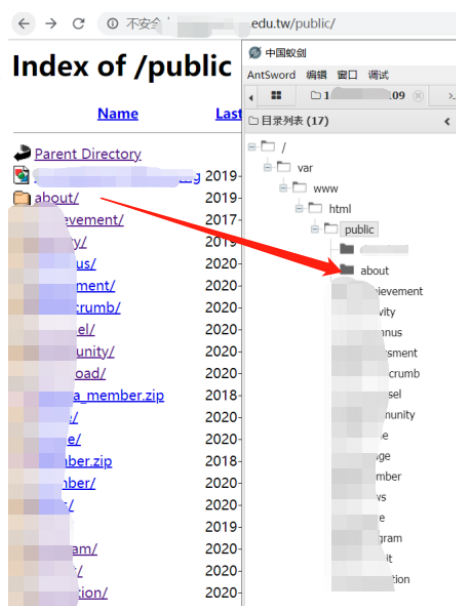
```
107 107
(*) 基础信息
当前路径: /usr/local/...
系统信息: FreeBSD ... 11.2-RELEASE FreeBSD 11.2-RELEASE #0 r335510: Fri Jun 22 04:32:14 UTC 2018
root@releng2: /usr/local/src/.../GENERIC amd64]
当前用户: www
(*) 输入 ashelp 查看本地命令
(www:/usr/local/www/...) $ cd /usr/local/...
(www:/usr/local/www/...) $ ip addr
/bin/sh: ip: not found
(www:/usr/local/www/...) $ ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether
hwaddr:
inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
nd6 options=29<PERFORMNUD, AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether
hwaddr:
inet 192.168.1.101 netmask 0xfffff00 broadcast 192.168.1.255
nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
lo0: flags=8049<UP, LOOPBACK, RUNNING, MULTICAST> metric 0 mtu 16384
options=600003<RXCSUM, TXCSUM, RXCSUM_IPV6, TXCSUM_IPV6>
inet6 ::1 prefixlen 128
inet6 fe80:: prefixlen 64 scopeid 0x3
inet 127.0.0.1 netmask 0xff000000
nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
groups: lo
```

5. 口罩大学公共研究所

存在列目录，得到网站备份。分析代码绕过上传。GETSHELL

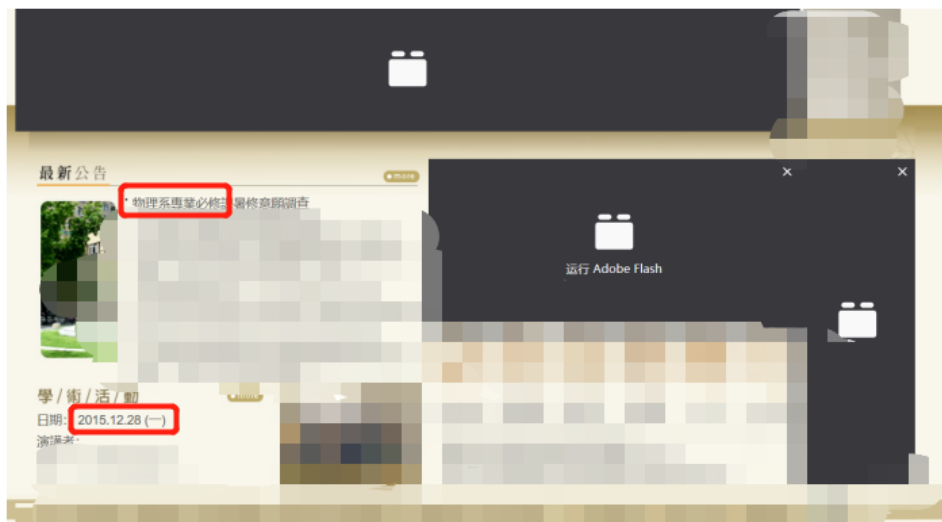
Index of /public

Name	Last modified	Size	Description
Parent Directory	-	-	-
9B4D22C7999CD.png	2019-02-21 18:19	598	
event/	2019-11-28 15:56	-	
ity/	2017-07-30 14:00	-	
ity/	2019-11-28 16:00	-	
inus/	2020-02-05 02:45	-	
ssment/	2020-02-05 02:45	-	
dcrumb/	2020-02-05 02:46	-	
usel/	2020-02-05 02:45	-	
munity/	2020-02-05 02:48	-	
nload/	2020-02-05 02:47	-	
pa_member.zip	2018-01-23 00:01	28M	
e/	2020-02-05 02:48	-	
le/	2020-02-05 02:48	-	
ber.zip	2018-01-23 21:35	1.2M	
ber/	2020-02-05 02:46	-	
/	2020-02-05 02:47	-	
/	2019-11-30 02:28	-	
ram/	2020-02-05 02:46	-	
it/	2020-02-05 02:47	-	
lation/	2020-02-05 02:46	-	

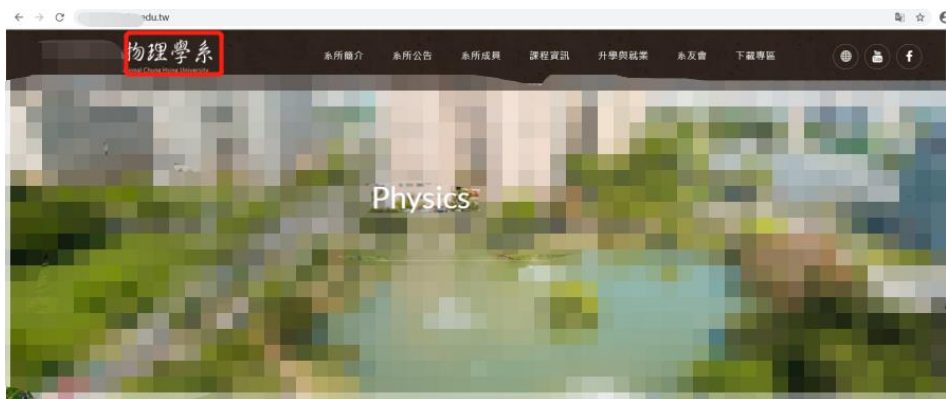


6. 口罩物理系主页

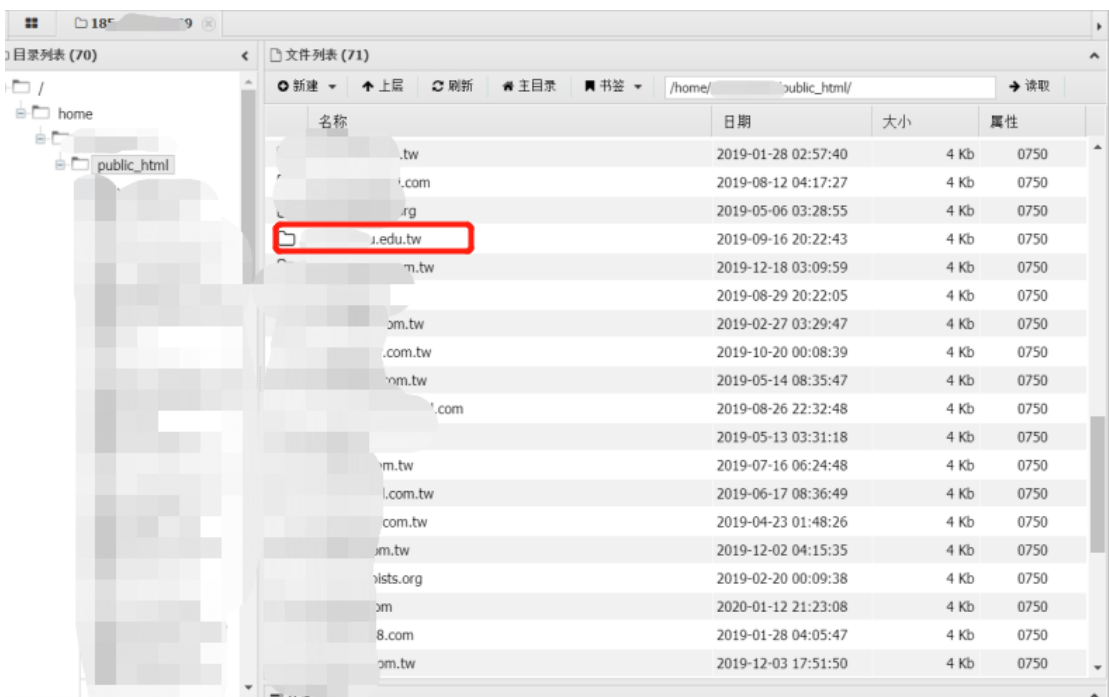
这是一个废弃了的主页，通过注入拿到了 3 个账号密码



但是死活找不到后台，后台通过谷歌语法找到了他新的主页。通过废弃网站的账号密码进入后台拿 SHELL。



登录 shell 发现这是一个 ww 的站群，网站数据库无价值，且其他旁站也不是这学校的。此 shell 无价值。



7.整理数据

通过港仔的渗透，我发现可以直接在大学主页处找到大部分和老师学生有关业务网站。



我在这里首先会去撞老师的平台，一般老师会上传材料什么的。拿 shell 拿重要数据，相对会比学生平台机会大一些。

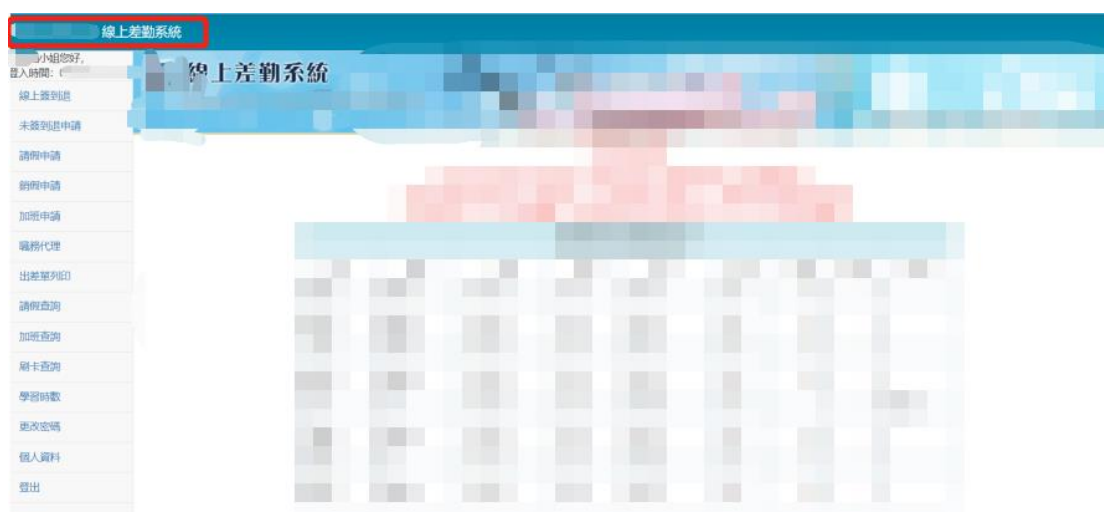
这里整理出 4 个文档，其中学生实习申请系统数据居多。

idpname.txt	2020/1/	文本文档	7 KB
idpasswd.txt	2020/1/	文本文档	5 KB
onepieceusername.txt	2020/1/	文本文档	6 KB
onepiecepasswd.txt	2020/1/	文本文档	5 KB

接下来就是每个接口去撞了。

8. 口罩大学教师服务器

成功撞入某个老师系统



在某处找到文件上传口，通过抓包找到文件位置。

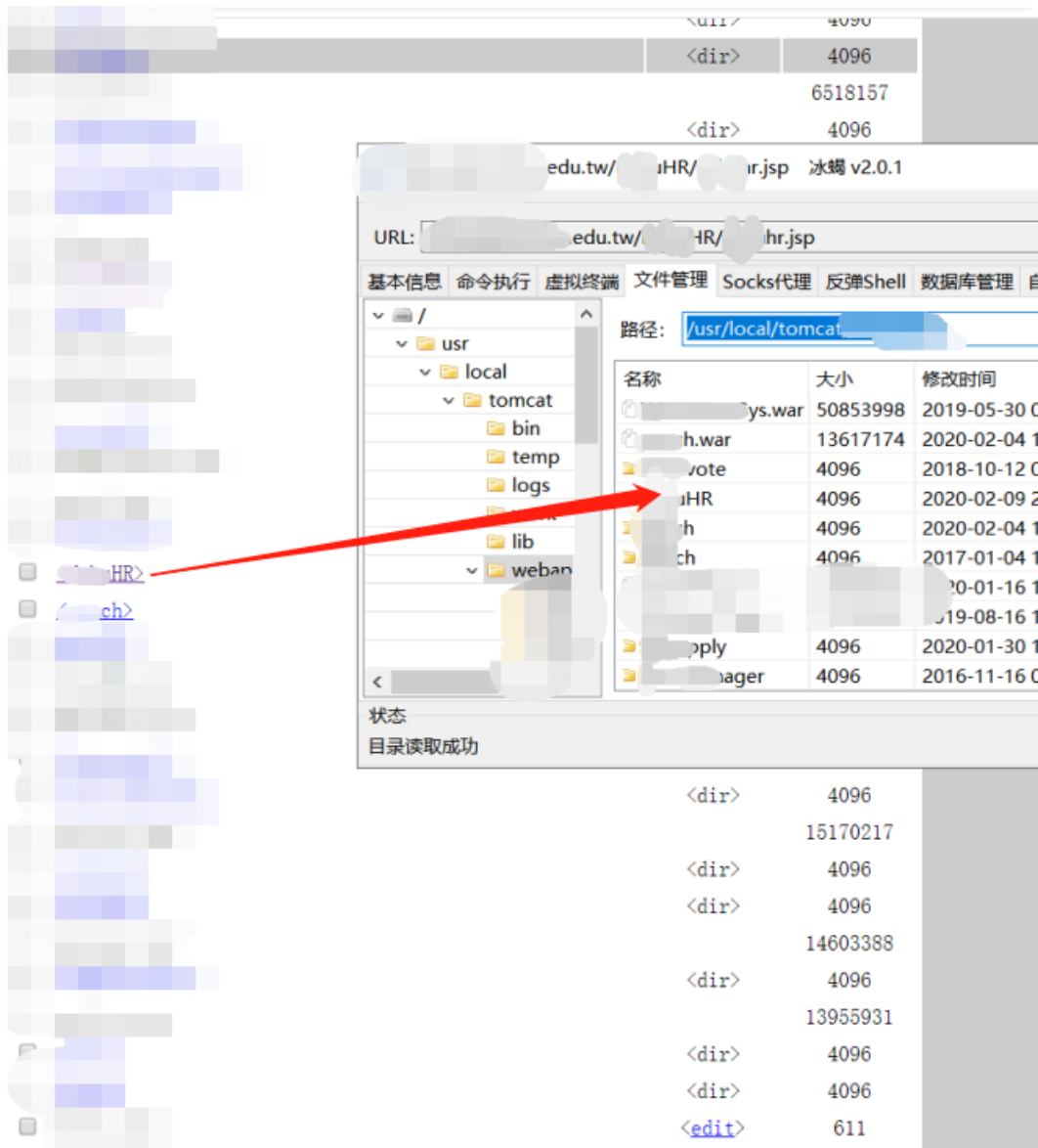


因为是 jsp 站，我又开心又担忧。担忧的是我的 shell 可能都连不上，尝试后都不行。后又花了一个多小时试了几十个 shell。

终于有个 shell 能用了，且是 root，很开心！



因为这个网页是单点登录的，shell 连接起来有点麻烦。所以又在服务器上找到了其他系统，且通过谷歌语法找到了 hr 系统的 url。成功通过 hr 系统连入，此服务器有七八个教师系统，照样的站库分离，拿到所有的连接 IP 账号密码。



总结经验：渗透就是信息搜集的过程。对于这种安全低档次的大学而言，可以尝试从与学生交互的平台入手。这样可以一下子拿到很多账号密码和邮箱。可以很快的去撞教师和服务生的服务接口，没有必要一开始就是啃那些 wordpress、joomla、drupal...这些网站的数据库

中可能只有网站管理员的账号密码，且撞接口成功率也不高。

个人疑问：1.找不到快速定位内网口的方法 2.大学 vpn 如何切入校园网 3.是否有其他更简单拿数据方法