BurpSuite 工具使用小经验

作者：mickey [54mickey_at_gmail.com]

一．使用代理做 WEB 渗透的好处

可以直观的看到客户端和 WEB 端的交互过程，比如下面的代码，如果是用浏览器直接查看，则不能看到"This is secret area"这些字符。

```
<?php
    $baseURL='http://pentestbox.com';
    Header("Location:$baseURL");
?>
<h1>This is Secret Area</h1>
```

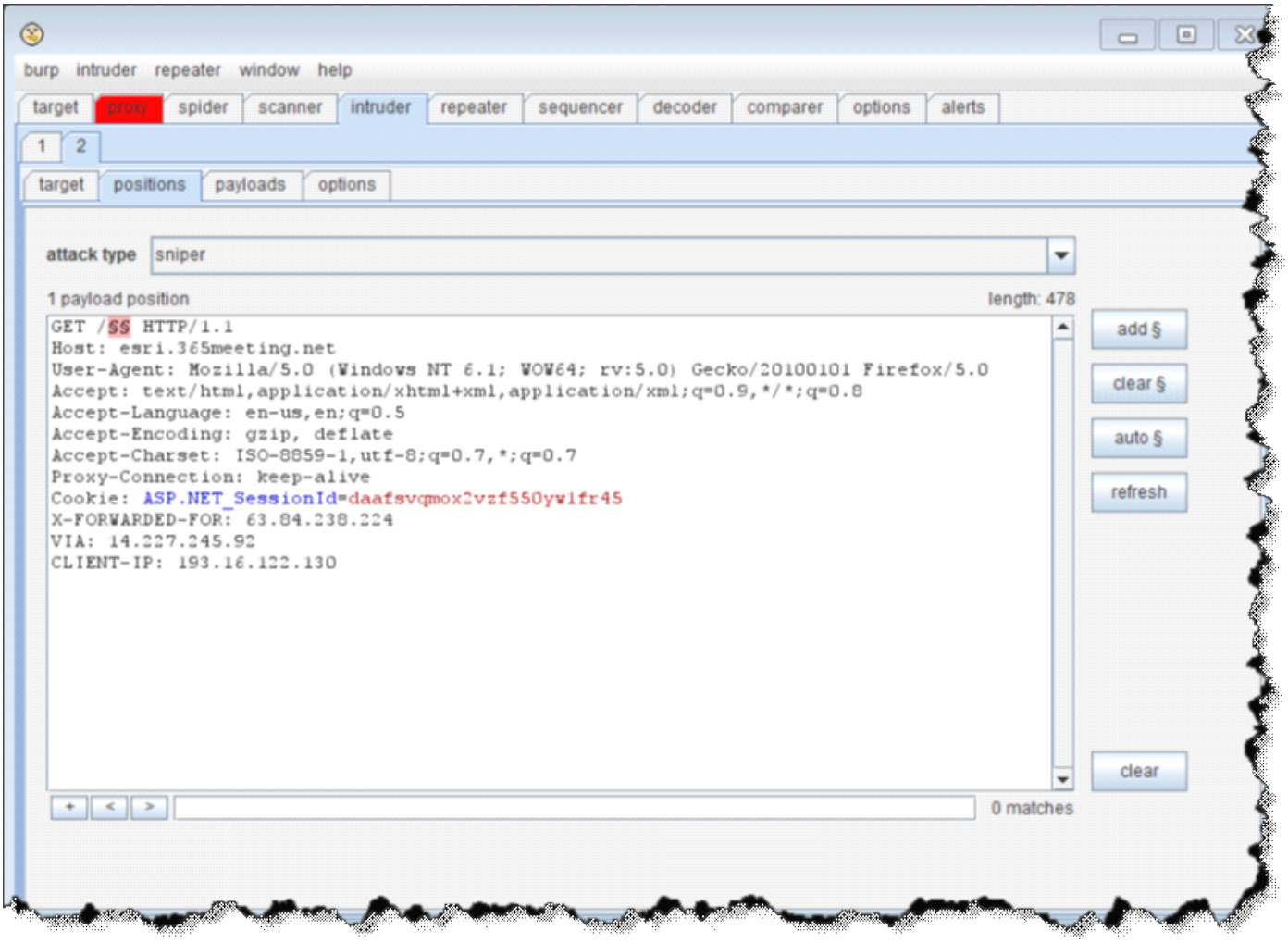
也可以自定义一些 HTTP 头，比如有一次我做测试，通过定义 User-Agent：为“Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)”，然后再 spider 站点，就爬出了许多原来没有看到的内容。

二．实际 WEB 渗透测试时用到的

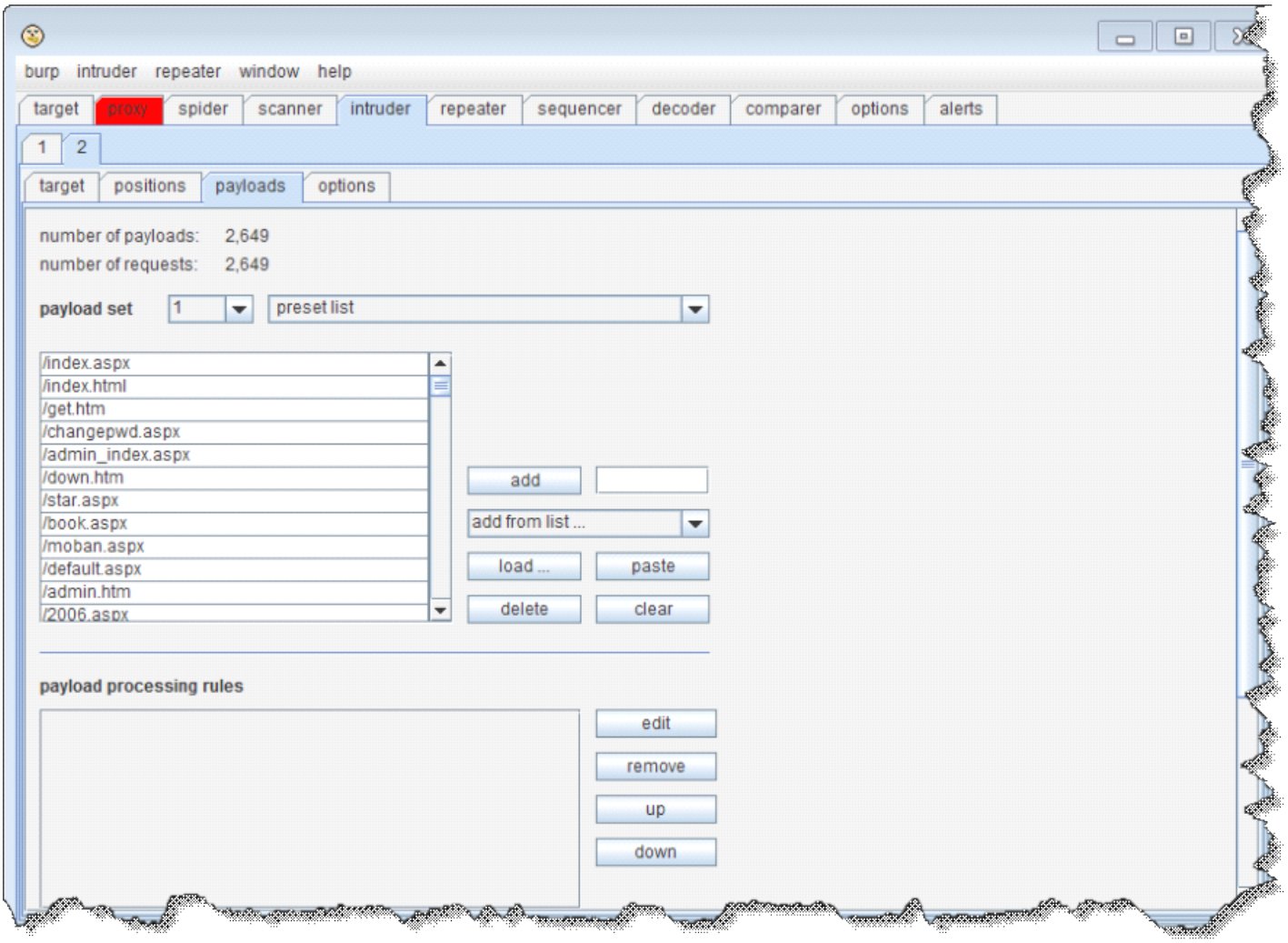
2.1 使用 burpsuite 的 intruder 的"Sniper"扫目录和文件(替代 Wfuzz 和 Dirbuster)

WEB 黑盒测试前，我都会扫描下网站的备份文件，日志文件和管理页面。首先设置 FireFox 的代理，推荐使用 FoxyProxy 插件来方便设置代理，然后浏览主站，当 BurpSuite 劫持到 Request 请求的时候，点击"Action"按钮，选择"Send to intruder"

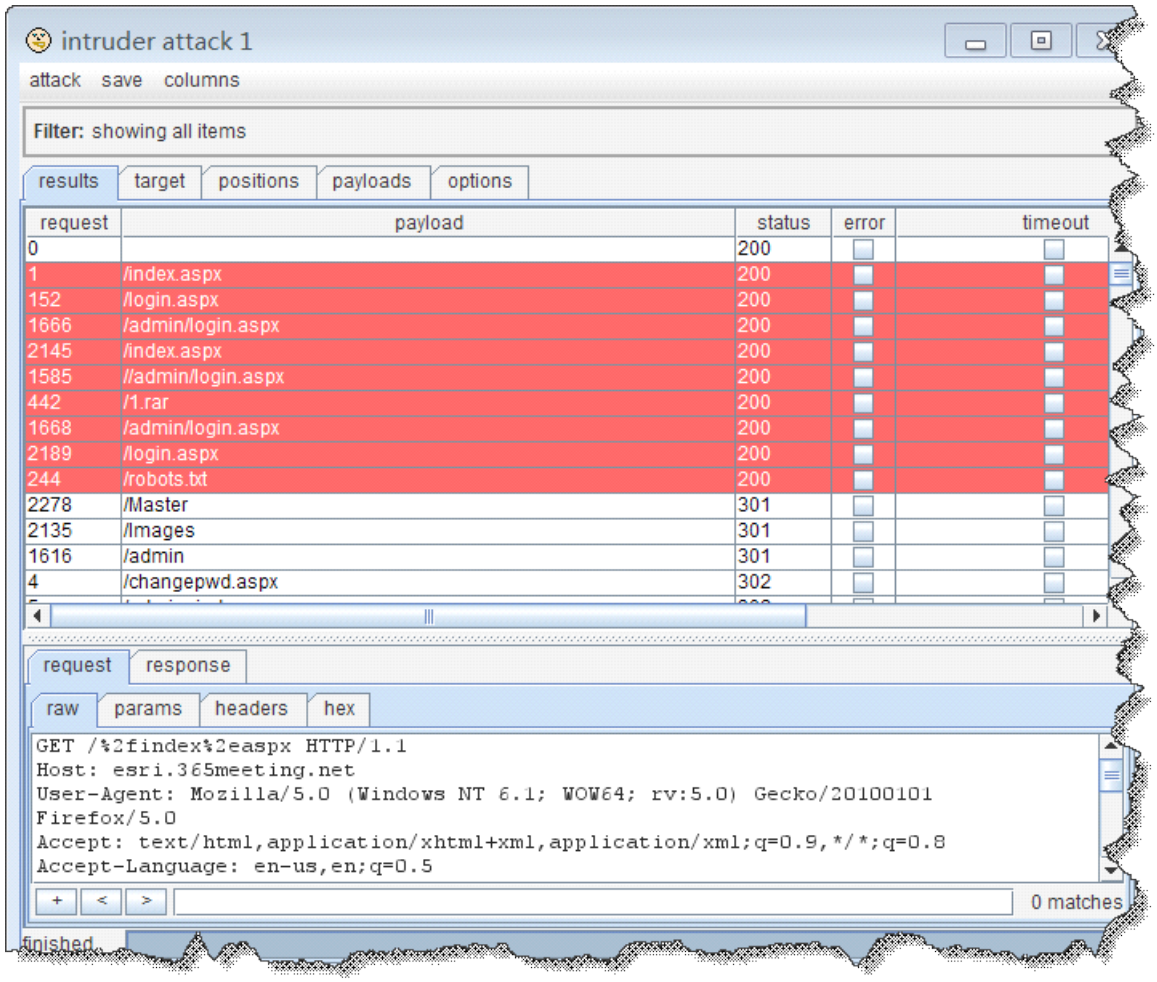
在"Intruder"标签下，"Attack type" 选择 "Sniper"，在 GET 后面的/添加$$，我这里因为是从根目录开始扫描的，所以选择了/，如果你是从其他特定目录开始扫，则自己做好相应的路径配置。具体配置下过如下图所示



来到 Payloads 标签下，选择"PreSet List" 载入字典文件，如果你的字典比较大，建议你选择"Runtime file"方式来载入字典，当然你也可以根据相应的选项来自己生成一个字典列表来跑，具体效果如下图所示：



然后就可以开始攻击了，可以根据 HTTP 的返回码来查看扫目录的结果，下图我用红色表示出来的就表示可以直接访问的目录



扩展思路：

1.可以根据 Apache 的 httpd.conf 里相应配置，来列举 LINUX 账户，类似 http://victim.org/~mickey

2.换一个思路，当使用一个低权限的用户登录后台后,利用 burpsuite 捕捉到的 cookies 来进一步扫目录，发现由于代码问题，可以直接访问的管理员文件。

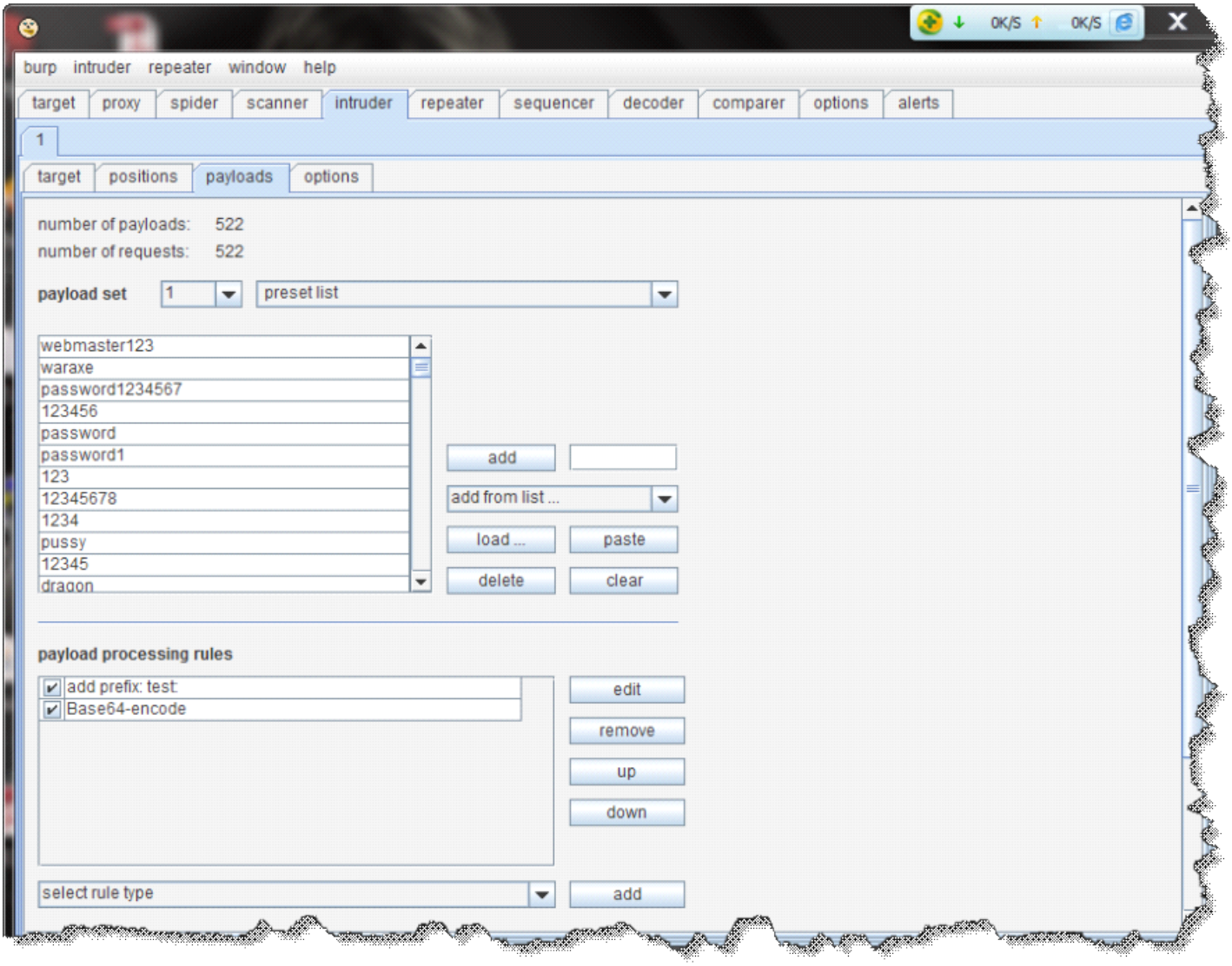
3.这里用来跑目录或者文件的字典，我通常选择的是 Wfuzz 和 Dirbruter 自带的字典

2.2 使用 burpsuite 的 intruder 的"Sniper"跑 HTTP 基本认证

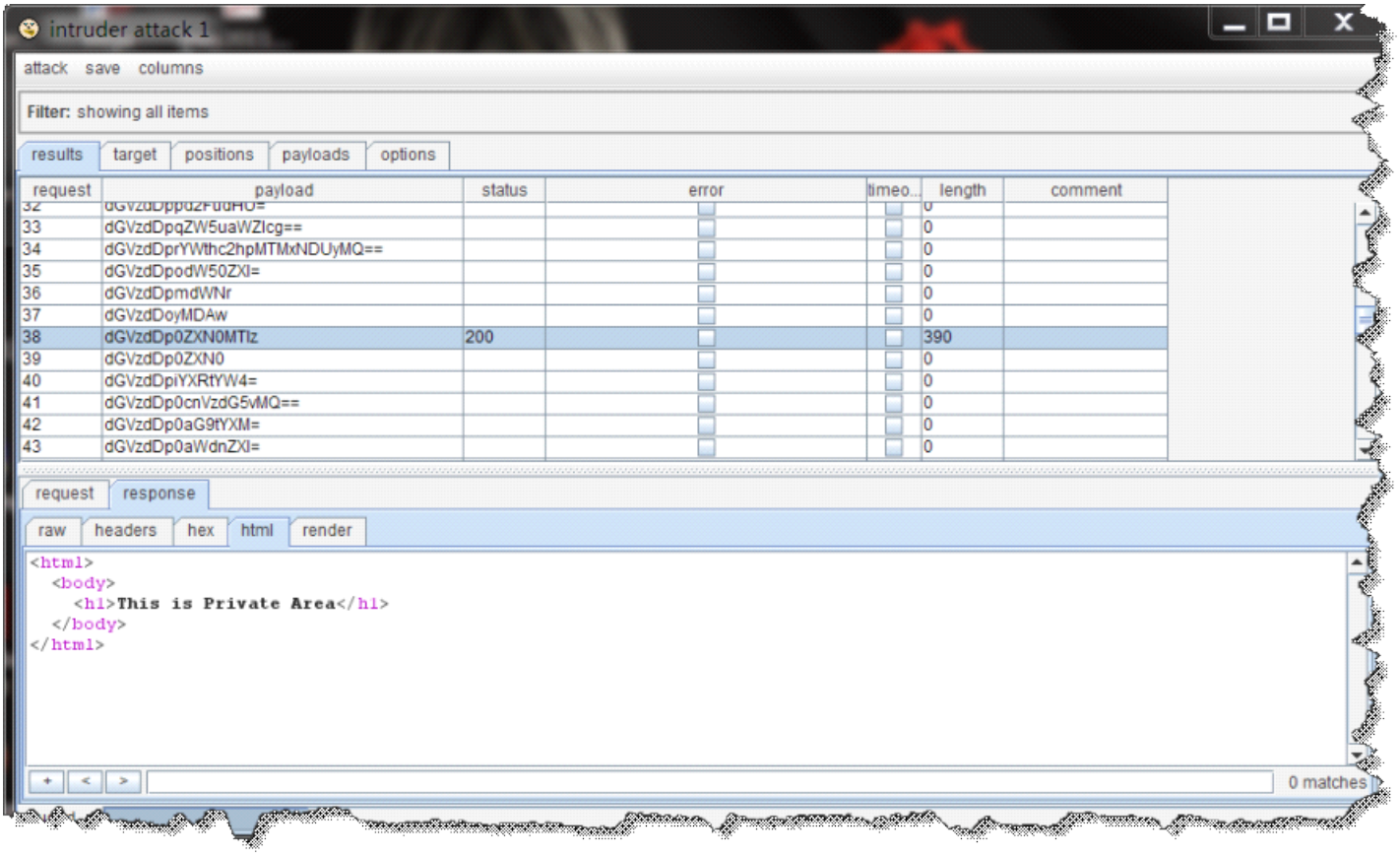
前几步的操作和前面一样，不同的是，需要在"Payload processing rules"做下设置，因为 HTTP 基本认证是采用 BASE64 编码的，所以我先添加一个规则，先来指定要跑的用户名，选择"add prefix"，添加用户名，我这里的案例用户名是"test"

然后指定"Encode"为"Base64-encode"

都配置好的效果图如下:



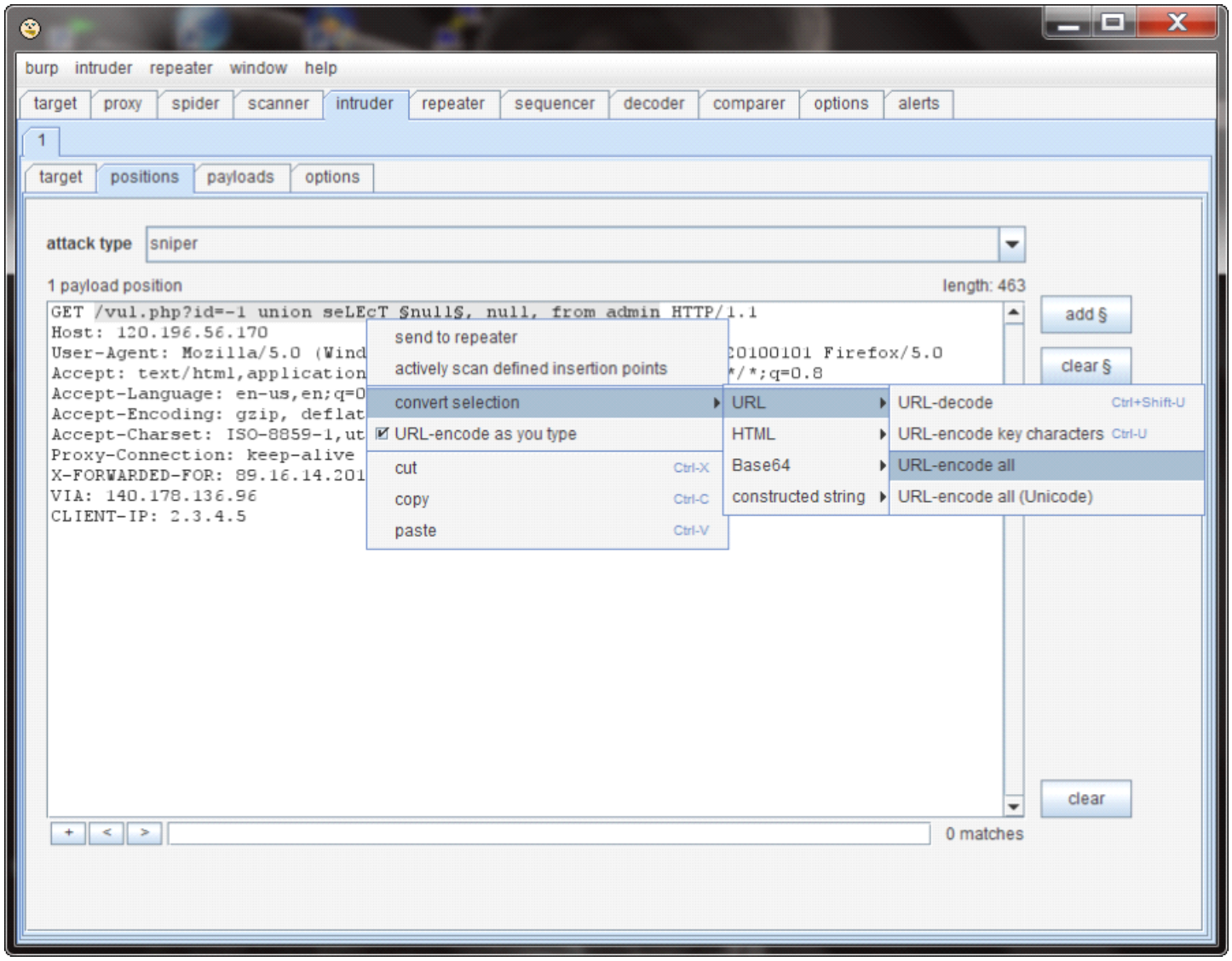
开始攻击，如果成功，HTTP 状态码通常会是 200，效果如下图



判断攻击结果是否成功，最常见的就是看"status"列和"length"列，可以根据 status 或 length 列的不同，来判断成功与失败。

2.3 使用 burpsuite 的 intruder 的"Sniper"一些其他的用处

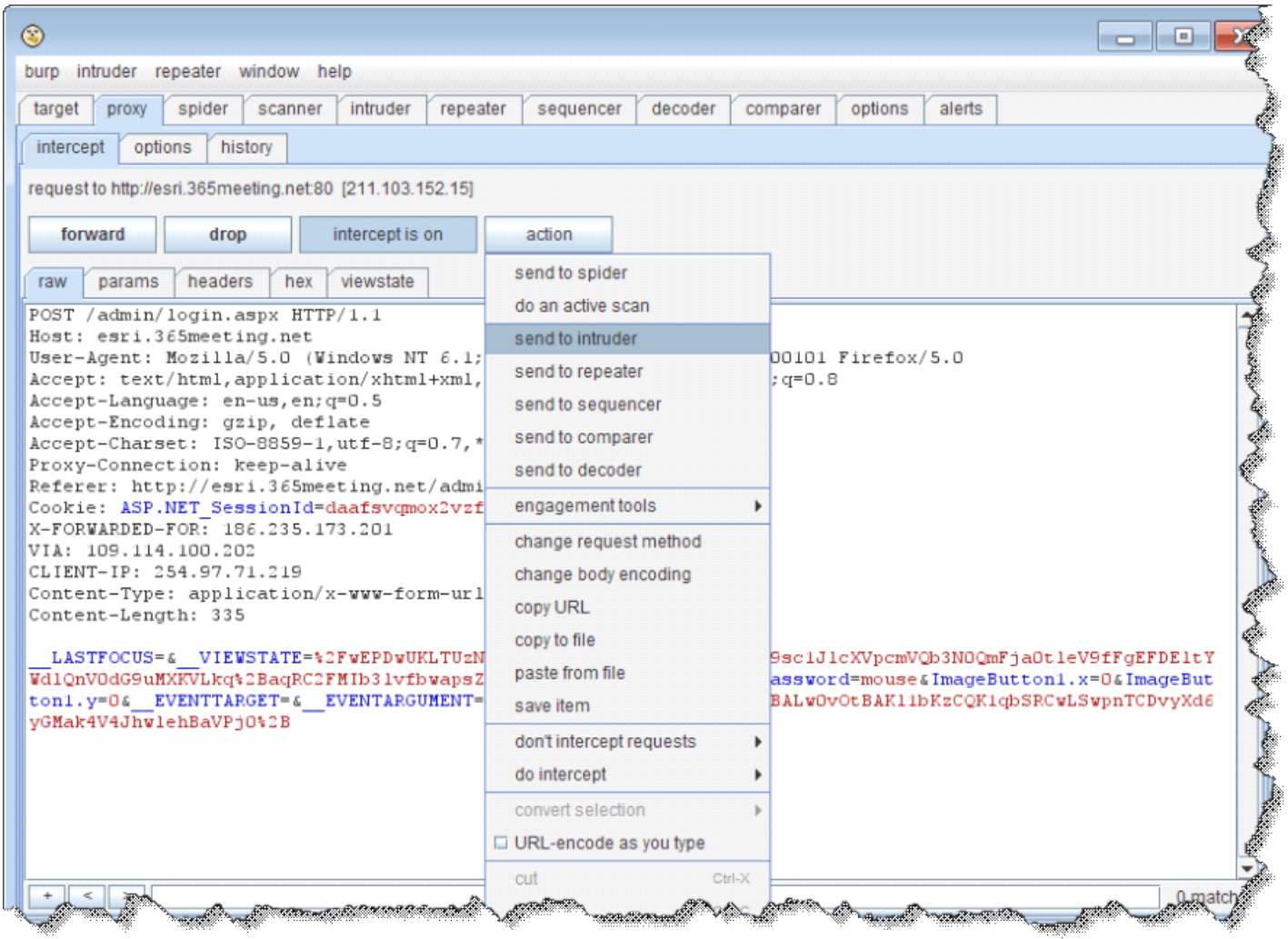
MYSQL4 注入的时候猜表名或者字段名，如果语句里有空格，还需要注意使用编码，否则不会成功，也可以通过使用不同的编码，来绕过简单的 WAF，效果如下图所示:

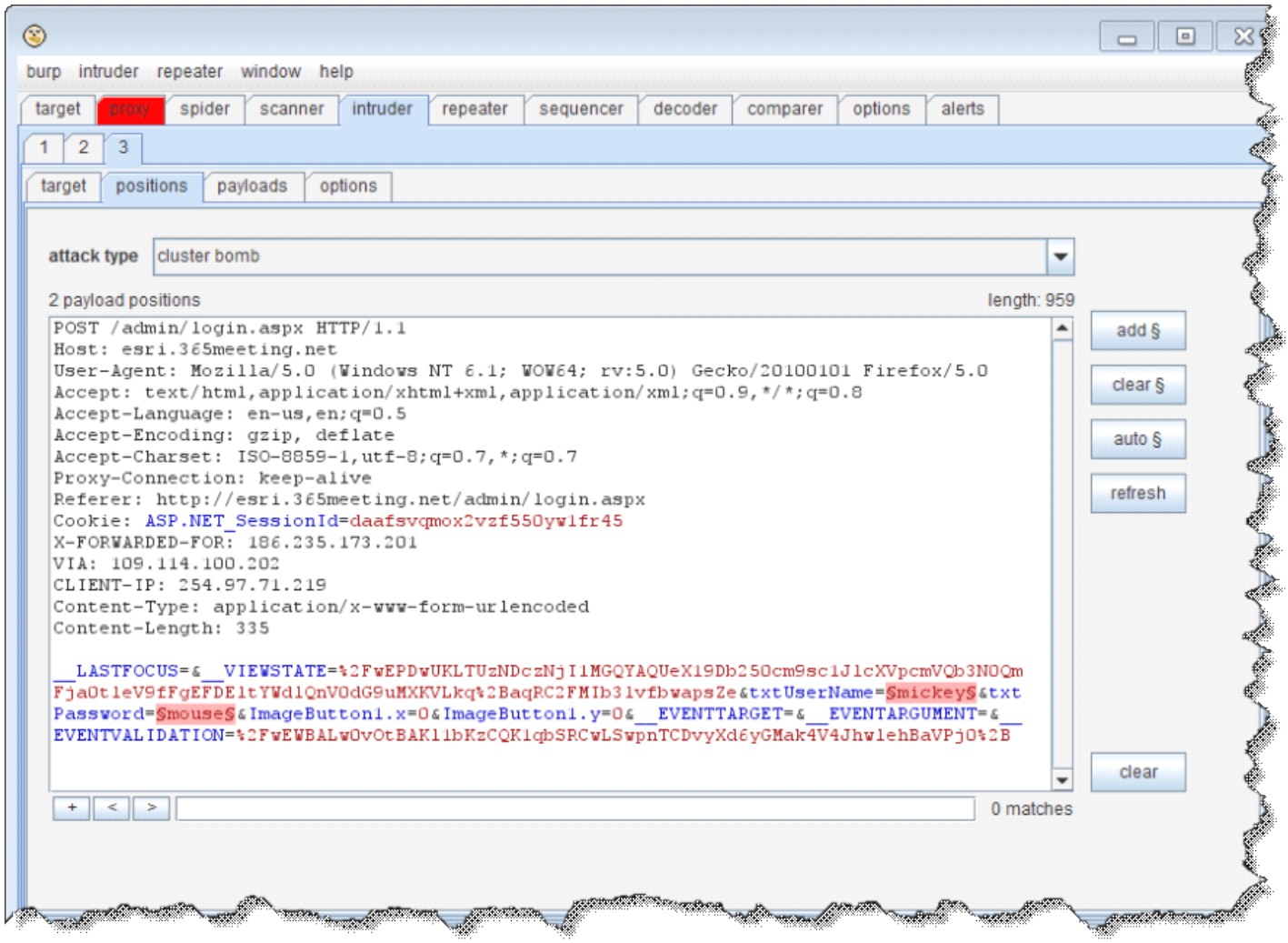


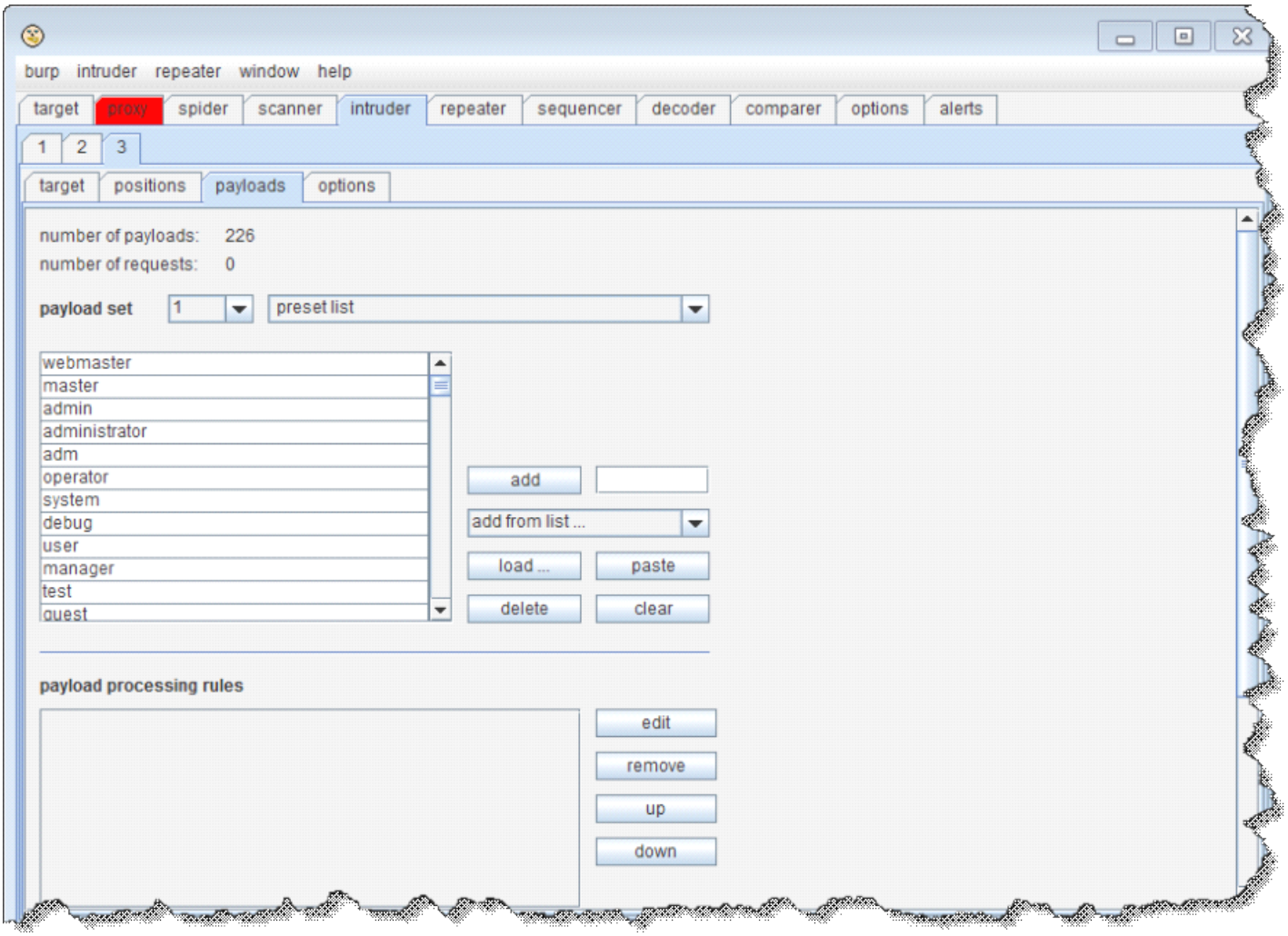
还可以使用 fuzzdb（code.google.com/p/fuzzdb/）里的 attack-payloads 文件夹下的文件，配合 burpsuite 的 intruder 的"Sniper"，来进行 XSS，blind sql inj，lfi 等测试，或者 FUZZ 一些其他的参数来发现漏洞。

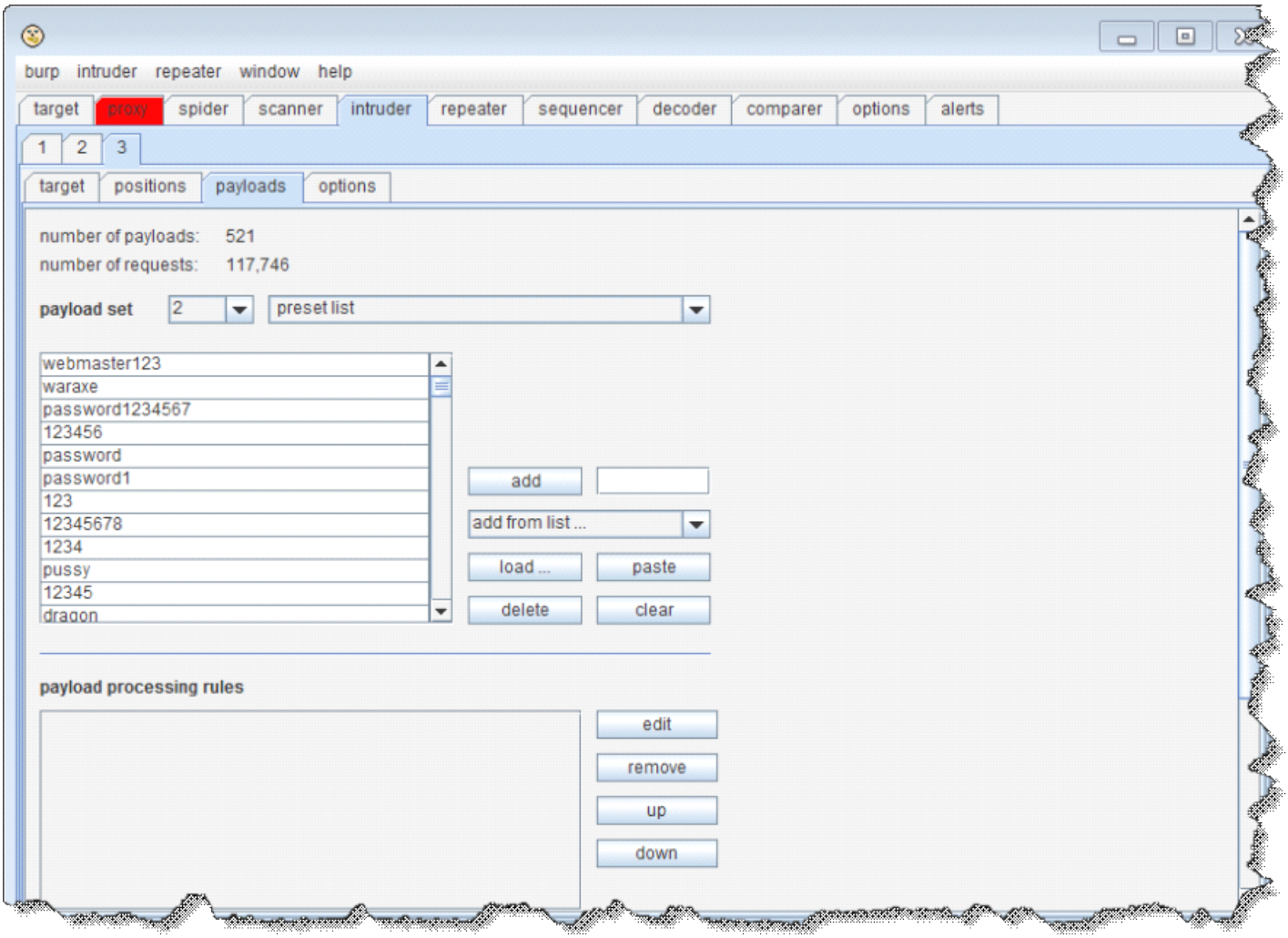
2.4 使用 burpsuite 的 intruder 的"Cluster Bomb"来破解后台登陆口

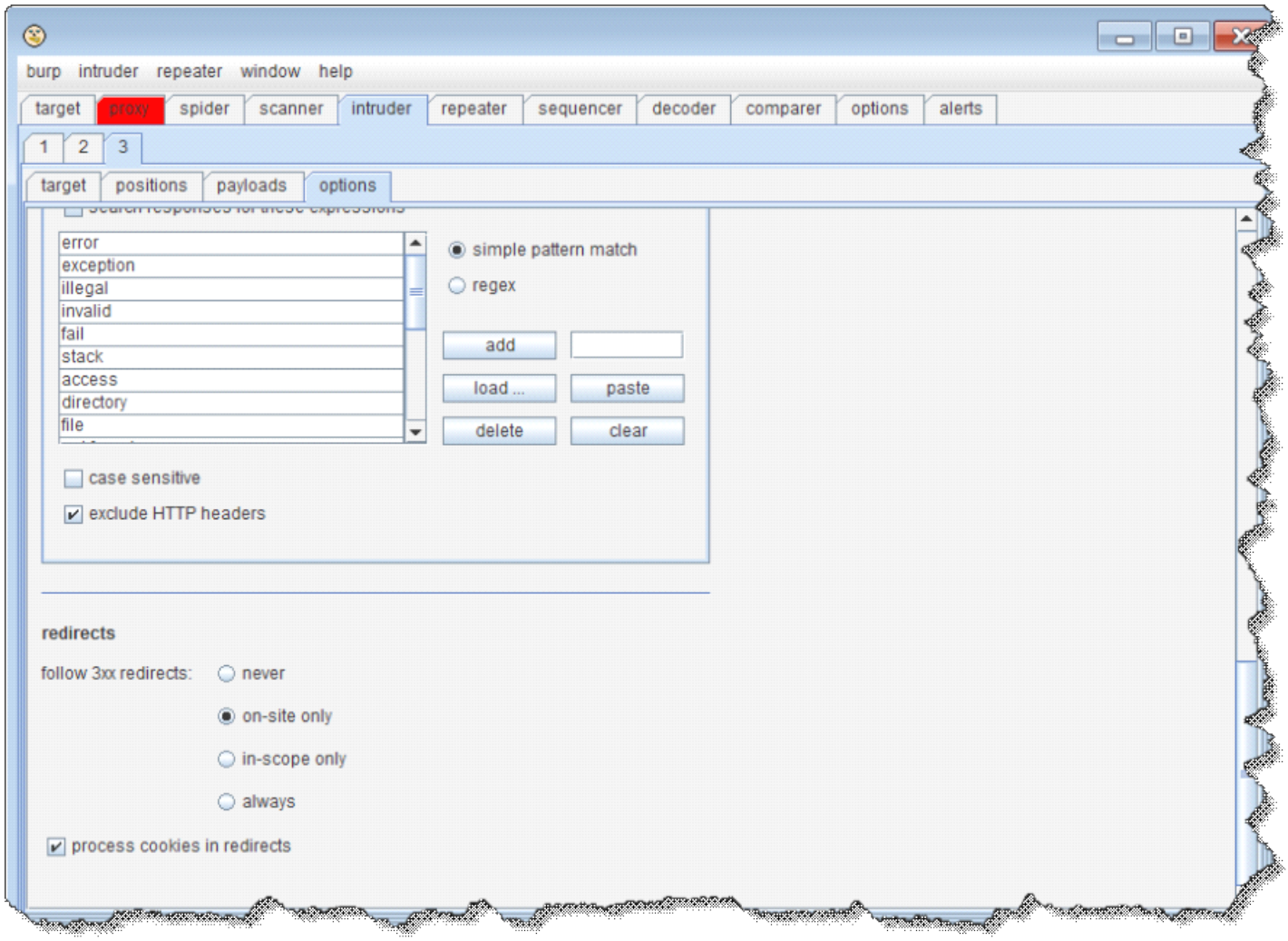
原来我都是用 GoldenEye 来破解没有验证码的 FORM 表单后台登陆口，不过最近在 PT007 给我的一个后台，GoldenEye 失效了，后来还是用 butpSuite 搞定的，当然用"wvs fuzzer"也可以，原理都差不多，比较懒了，我少打字，您多看图吧。

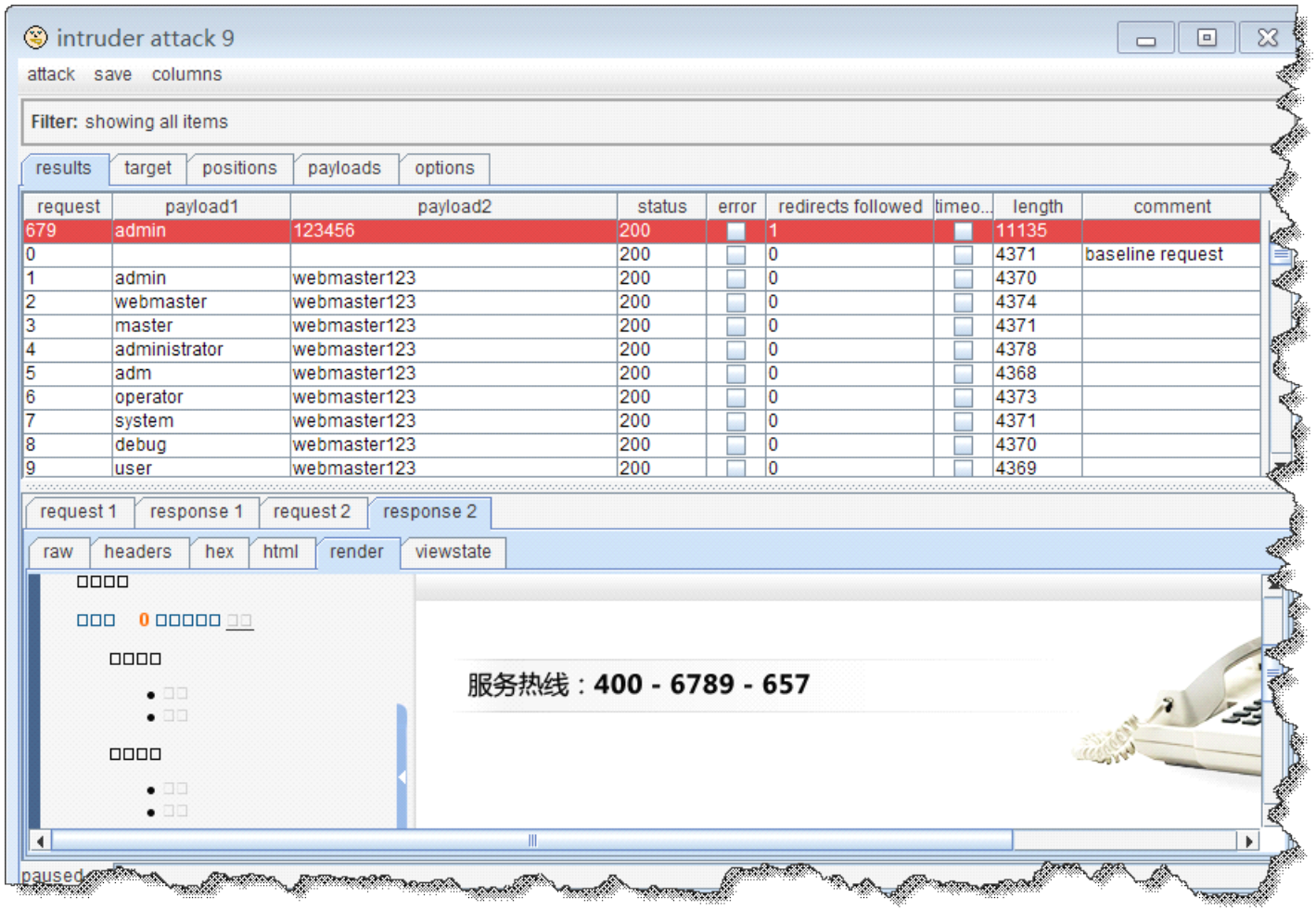

burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
request to http://esri.365meeting.net:80 [211.103.152.15]
forward drop intercept is on action
raw params headers hex viewstate
POST /admin/login.aspx HTTP/1.1
Host: esri.365meeting.net
User-Agent: Mozilla/5.0 (Windows NT 6.1;
Accept: text/html,application/xhtml+xml,
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*
Proxy-Connection: keep-alive
Referer: http://esri.365meeting.net/admi
Cookie: ASP.NET_SessionId=daafsvqmox2vzf
X-FORWARDED-FOR: 186.235.173.201
VIA: 109.114.100.202
CLIENT-IP: 254.97.71.219
Content-Type: application/x-www-form-url
Content-Length: 335
__LASTFOCUS=&__VIEWSTATE=%2FwEPDwUKLTUzN
WdlQnVOdG9uMXKVLkq%2BaqRC2FMIb3lvfbwapsZ
ton1.y=0&__EVENTTARGET=&__EVENTARGUMENT=
yGMak4V4JhwlehBaVPjO%2B
00101 Firefox/5.0
;q=0.8
9sc1JlcXVpcmVQb3NOQmFjaOtleV9fFgEFDEltY
assword=mouse&ImageButton1.x=0&ImageBut
BALwOvOtBAK1bKzCQK1qbSRCwLSwpnTCDvyXd6
send to spider
do an active scan
send to intruder
send to repeater
send to sequencer
send to comparer
send to decoder
engagement tools
change request method
change body encoding
copy URL
copy to file
paste from file
save item
don't intercept requests
do intercept
convert selection
URL-encode as you type
cut Ctrl-X
0 match


burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
1 2 3
target positions payloads options
attack type cluster bomb
2 payload positions
length: 959
POST /admin/login.aspx HTTP/1.1
Host: esri.365meeting.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Proxy-Connection: keep-alive
Referer: http://esri.365meeting.net/admin/login.aspx
Cookie: ASP.NET_SessionId=daafsvqmox2vzf550ywlfr45
X-FORWARDED-FOR: 186.235.173.201
VIA: 109.114.100.202
CLIENT-IP: 254.97.71.219
Content-Type: application/x-www-form-urlencoded
Content-Length: 335
__LASTFOCUS=&__VIEWSTATE=%2FwEPDwUKLTUzNDczNjI1MGQYAQUeX19Db250cm9sc1JlcXVpcmVQb3NOQm
FjaOtleV9fFgEFDEltYWdlQnV0dG9uMXKVLkq%2BaqRC2FMIb3lvfbwapsZe&txtUserName=$mickey$&txt
Password=$mouse$&ImageButton1.x=0&ImageButton1.y=0&__EVENTTARGET=&__EVENTARGUMENT=&__
EVENTVALIDATION=%2FwEWBALwOvOtBAK1lbKzCQK1qbSRCwLSwpnTCDvyXd6yGMak4V4JhwlehBaVPjO%2B
add §
clear §
auto §
refresh
clear
+ < >
0 matches


burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
1 2 3
target positions payloads options
number of payloads: 226
number of requests: 0
payload set 1
preset list
webmaster
master
admin
administrator
adm
operator
system
debug
user
manager
test
guest
add
add from list ...
load ...
paste
delete
clear
payload processing rules
edit
remove
up
down


burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
1 2 3
target positions payloads options
number of payloads: 521
number of requests: 117,746
payload set 2
preset list
webmaster123
waraxe
password1234567
123456
password
password1
123
12345678
1234
pussy
12345
dragon
add
add from list ...
load ...
paste
delete
clear
payload processing rules
edit
remove
up
down


burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
1 2 3
target positions payloads options
error
exception
illegal
invalid
fail
stack
access
directory
file
simple pattern match
regex
add
load ...
paste
delete
clear
case sensitive
exclude HTTP headers
redirects
follow 3xx redirects:
never
on-site only
in-scope only
always
process cookies in redirects

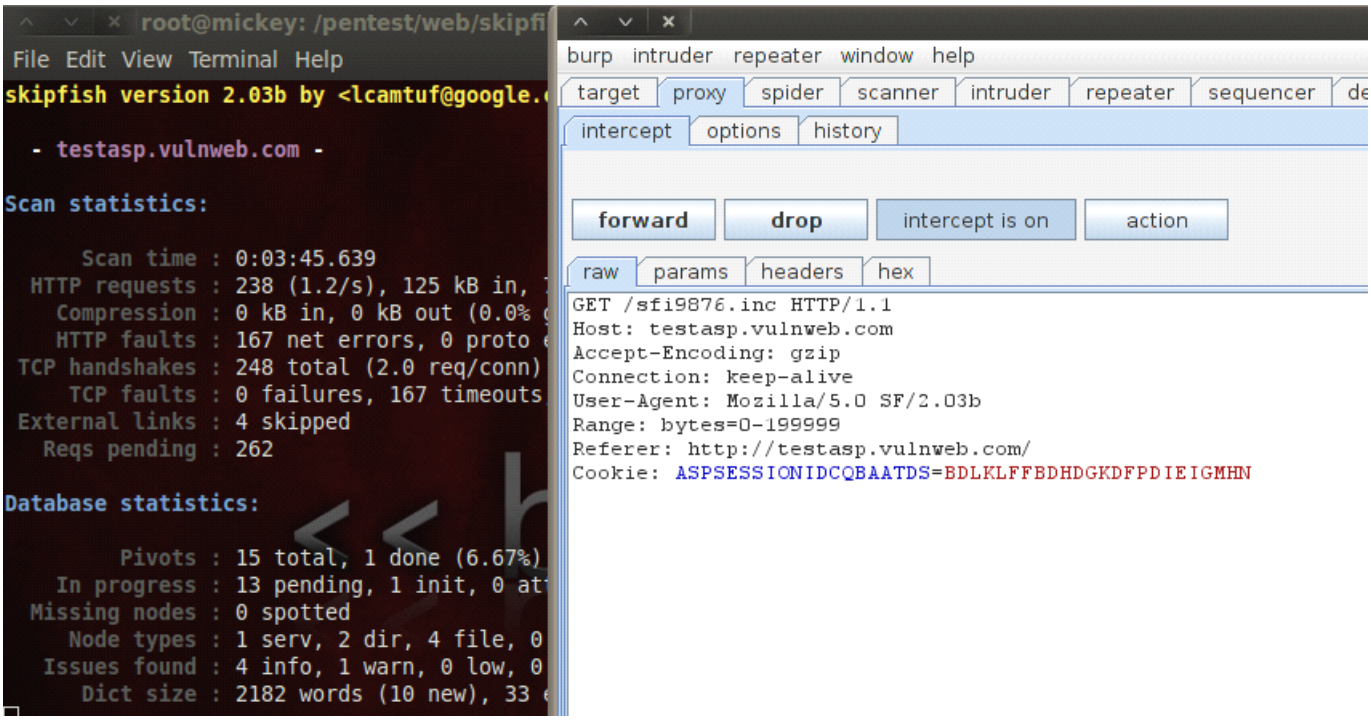


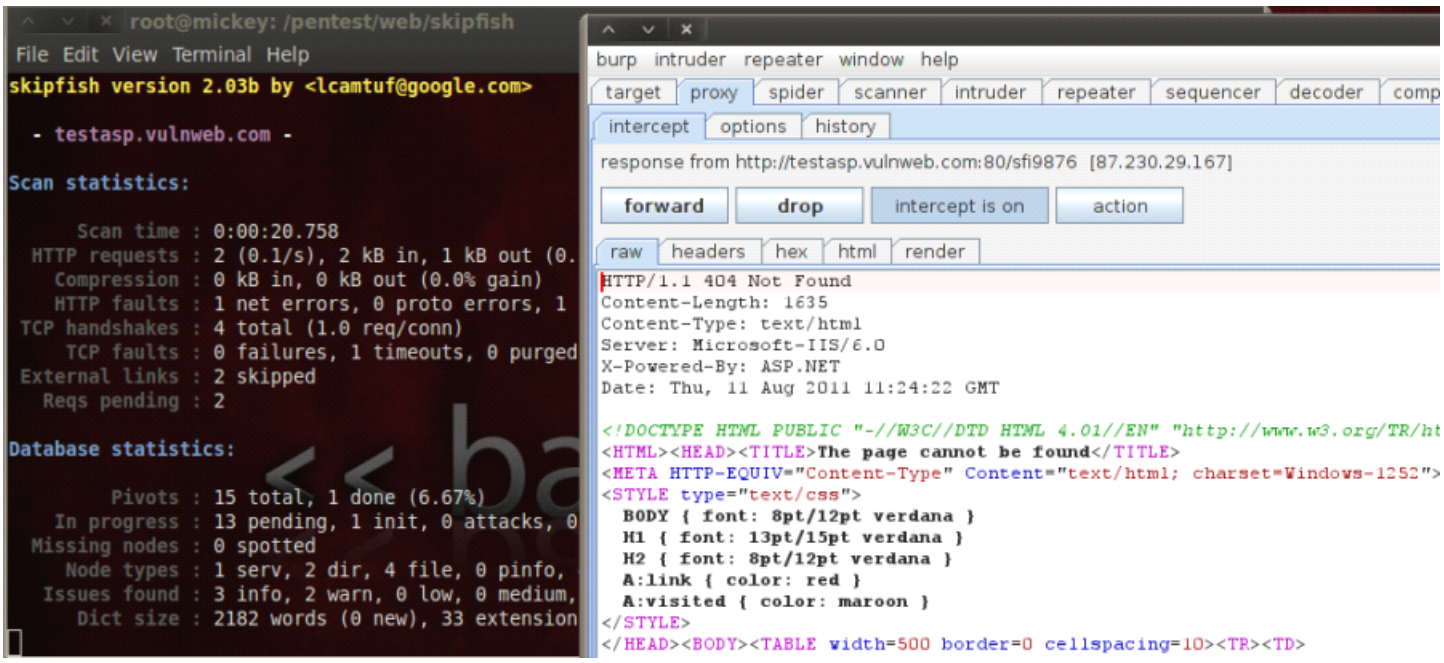
2.5 使用 burpsuite 来突破上传限制

这里我就不说了，Trace 牛的“Upload Shell with Burp Suite”写的比较详细了，我已经打包放在同目录了，而上传的种种绕过限制的方法，可以看 CasperKid 牛的“Bypass Upload Validation Framework V0.9”

2.6 使用 skipfish 配合 burpsuite

```
root@mickey:/pentest/web/skipfish# ./skipfish -F testasp.vulnweb.com=192.168.195.131 -o test_output
http://testasp.vulnweb.com/
```





三．结束语

可以用 burpSuite 自己本身的 Scanner 功能可以用来做自动扫描，扫一些常见的漏洞(分主动扫描和被动扫描,需要调节好线程数,以免程序假死)，扫描完成后，还能生成出一份不错的报告，具体使用比较简单了。可以看看官方的说明文档 http://portswigger.net/burp/help/scanner.html

手动测试方面，就是我上面列举的这些，替代 NC，来绕过上传限制，或者使用 intruder 的"Sniper"来进行扫目录，跑 HTTP 基本认证，FUZZ 参数，用 intruder 的"Cluster Bomb"来跑后台密码，当然每次的 WEB 黑盒的测试环境不同，BurpSuite 也要做相应的配置，比如 URL 编码，添加特殊的 HTTP 头等等。具体情况还给具体分析。文章写的比较简

单，就是起一个抛砖引玉的作用，欢迎喜欢渗透的朋友和我交流。