

Web 爆破攻击实战

1. Low 级别 Web 爆破攻击实战

1.1 暴力破解账户密码

步骤 1：设置安全级别为 Low，点击 Brute Force 按钮，进行暴力破解模块，发现是个用户登录的页面，随意输入用户名和密码，发现提示用户名或密码错误；同时发现输入的用户名和密码携带在了 URL 中，所以确认该页面提交方式为 GET，如图 1.1。

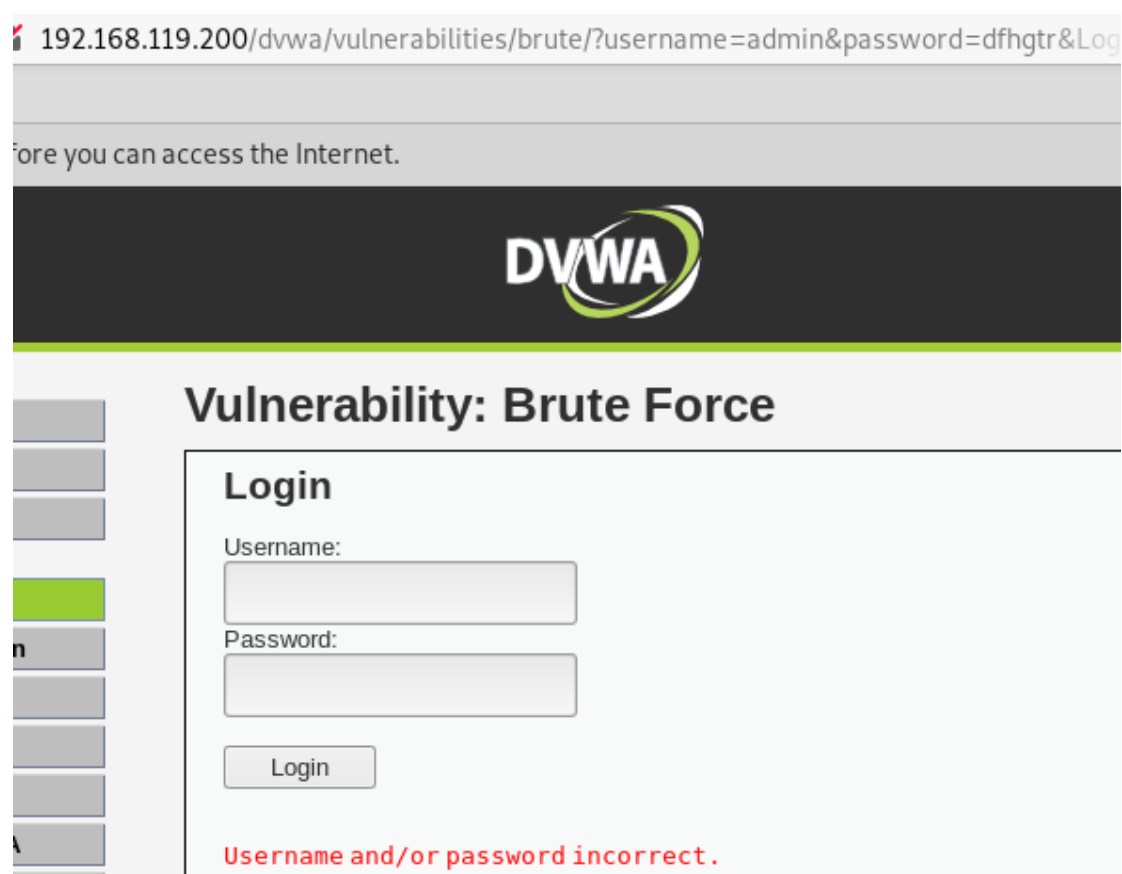


图 1.1

步骤 2：我们已经得知 DVWA 存在一个默认账户，用户名和密码为 admin/password，使用该账户登录，发现页面提示 Welcome to the password protected area admin，来说明登录成功，如图 1.2。



图 1.2

步骤 3：我们先自己构建一个字典文件，包含正确的密码信息 password，如图 1.3。

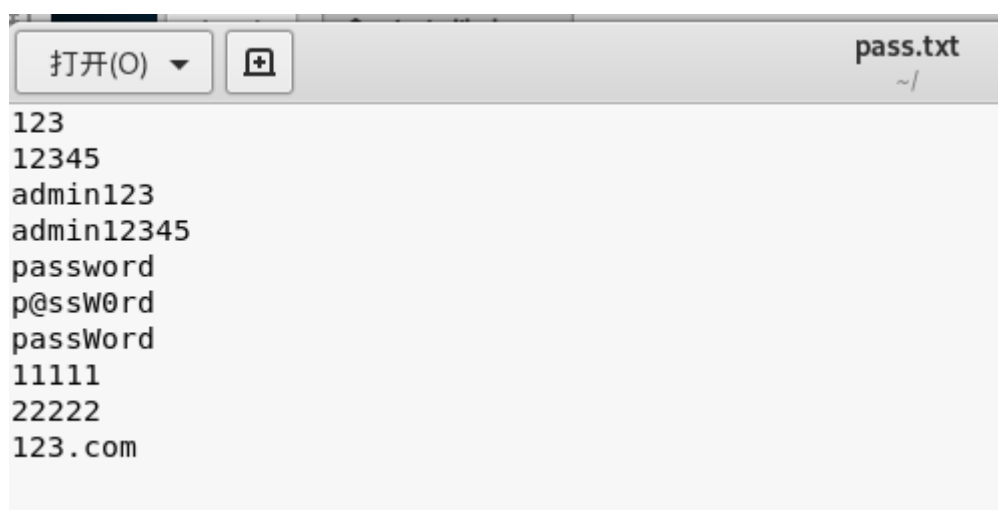


图 1.3

步骤 4：设置好 Burpsuite 和浏览器的代理，先随便输入一个用户名和密码，用 Burpsuite 抓包，如图 1.4。

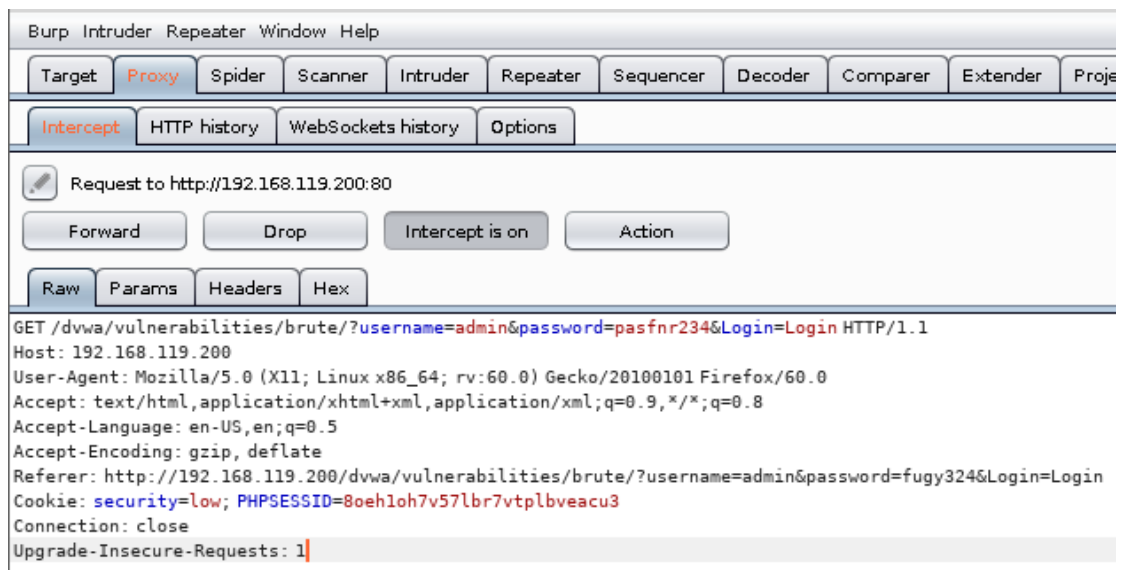


图 1.4

步骤 5: 点击 Action 按钮, 选择 Send to Intruder, 把数据包信息发送到暴力破解模块, 如图 1.5。

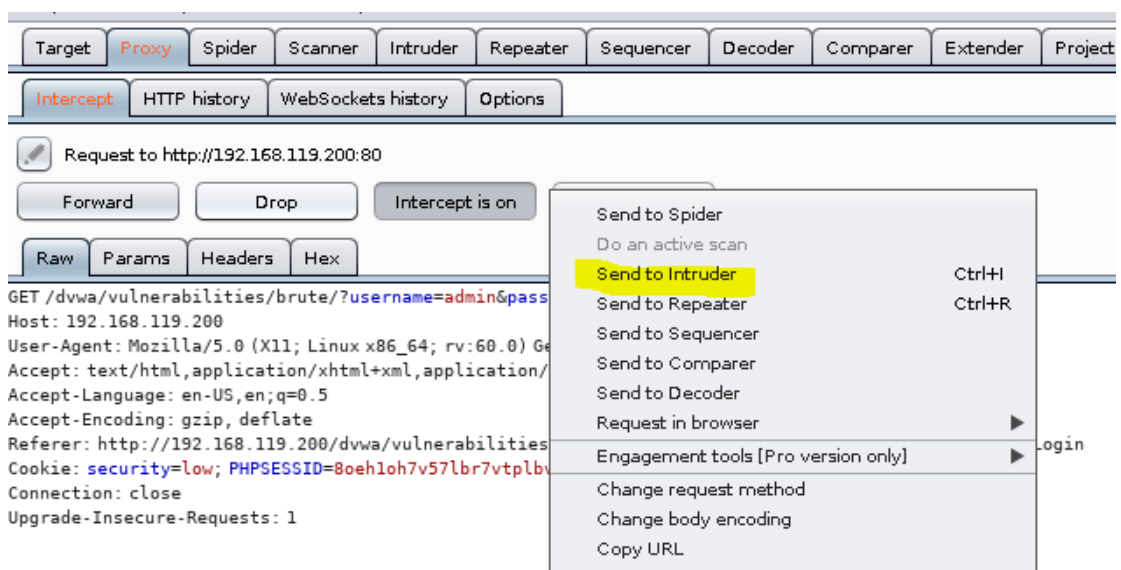


图 1.5

步骤 6: 点击 Intruder 模块, 选择 Positions 标签, 可以看到发送过来的数据包信息, 如图 1.6。

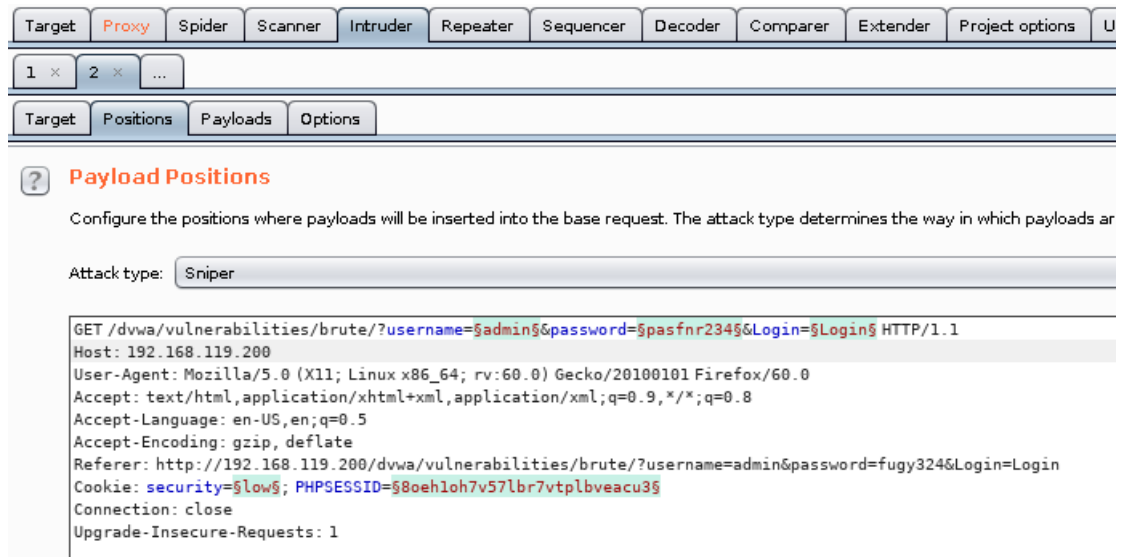


图 1.6

步骤 7: 点击 Clear \$ 按钮清除掉所有变量，如图 1.7。



图 1.7

步骤 8: 我们这里为了节省时间，假定已经得知了用户名为 admin，只猜解密码，所以选中之前随意输入的密码，点击 Add \$，把密码部分设置为要猜解的变量，如图 1.8。

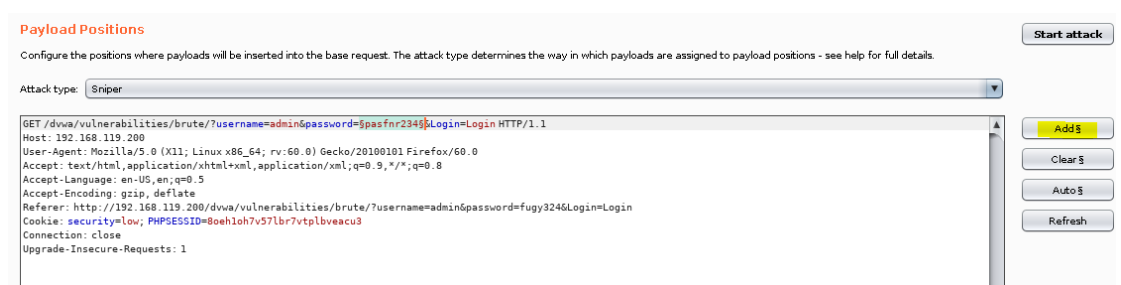


图 1.8

步骤 9: 切换到 Payloads 标签，在 Payload Option 处，点击 Load 按钮，选择之前构建的字典文件，如图 1.9。



图 1.9

步骤 10: 下拉到 Grep Match 处, 点击 Clear, 清除掉现有猜解成功匹配字符, 然后添加之前我们看到的 DVWA 中登录成功的提示字符 Welcome to the passowrd, 然后点击 Add。这样等到猜解成功后, 就会自动提示, 不用我们自己去比对回包长度和响应状态码来判断哪个是正确的密码, 如图 1.10。

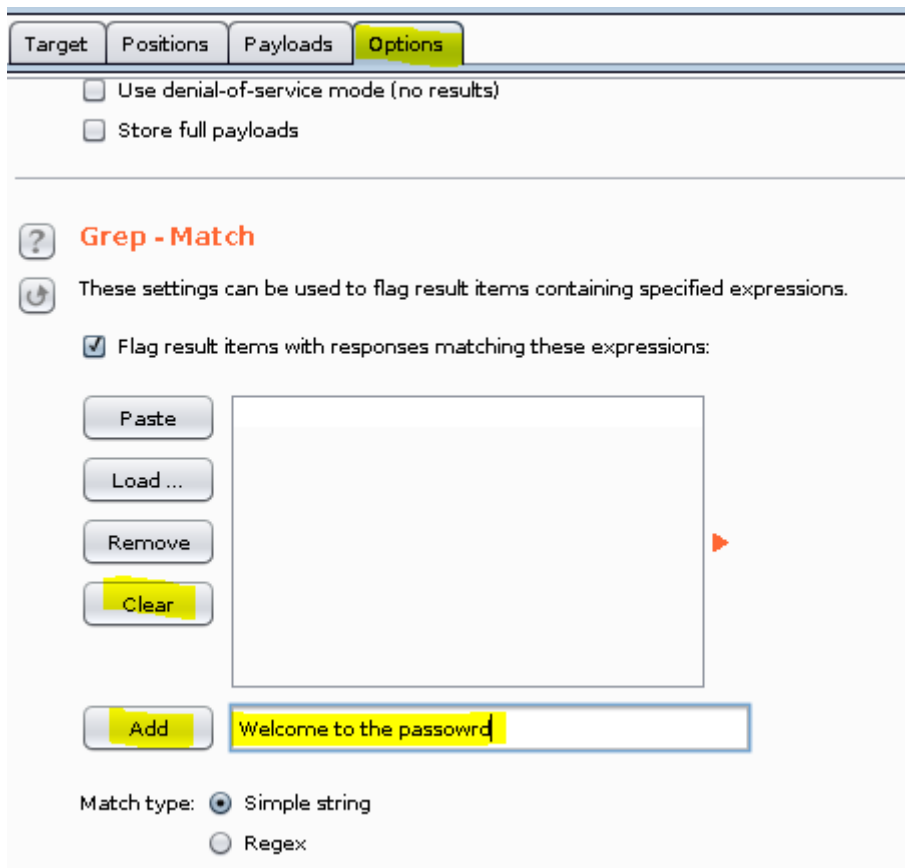


图 1.10

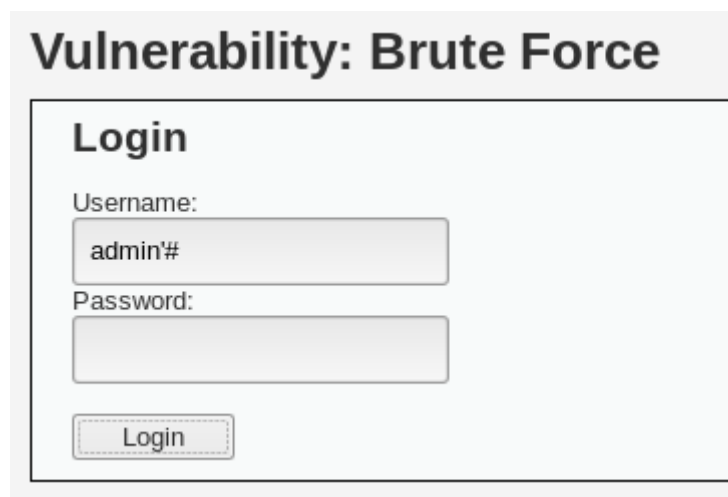
步骤 11: 点击 Start Attack 按钮, 开始爆破, 可以发现, 当猜解到 password 时, 回包长度与其他都不一致, 而且打钩提示该密码是正确的, 如图 1.11。

intruder attack 1							
Attack Save Columns							
Results Target Positions Payloads Options							
Filter: Showing all items							
Requ...	Payload	Status	Error	Timeo...	Length		Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
1	123	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
2	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
3	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
4	admin12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
5	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4738	<input checked="" type="checkbox"/>	
6	p@ssW0rd	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
7	passWord	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
8	11111	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
9	22222	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	
10	123.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	<input checked="" type="checkbox"/>	

图 1.11

1.2 SQL 注入破解账户密码

步骤 1：尝试使用 SQL 注入的方式登录，用户名输入 `admin' #`，密码留空登录，发现可以直接进入，如图 1.12，图 1.13。



The screenshot shows a web application interface with the title "Vulnerability: Brute Force". Below the title is a "Login" section. It contains two input fields: "Username:" and "Password:". The "Username:" field contains the text "admin'#". The "Password:" field is empty. Below the input fields is a "Login" button. The entire form is enclosed in a light gray border.

图 1.12



The screenshot shows the same web application interface as Figure 1.12, but with a successful login. The "Username:" field is now empty, and the "Password:" field is also empty. The "Login" button is still present. Below the input fields, a message reads: "Welcome to the password protected area admin'#". At the bottom left, there is a small icon of a document with a magnifying glass.

图 1.13

2. Medium 级别 Web 爆破攻击实战

步骤 1：安全级别设置为 Medium，进入 Web 爆破攻击页面，查看页面源码，发现对提交的用户名和密码内容使用了 `mysql_real_escape_string` 函数，对特殊字符进行转义，从而防止了以 SQL 注入的方式登录，如图 2.1。

同时，通过 `sleep(2)`，使登录失败后让页面延迟 2 秒响应，对暴力破解起到了一定的防御作用，如图 2.2。



图 2.1

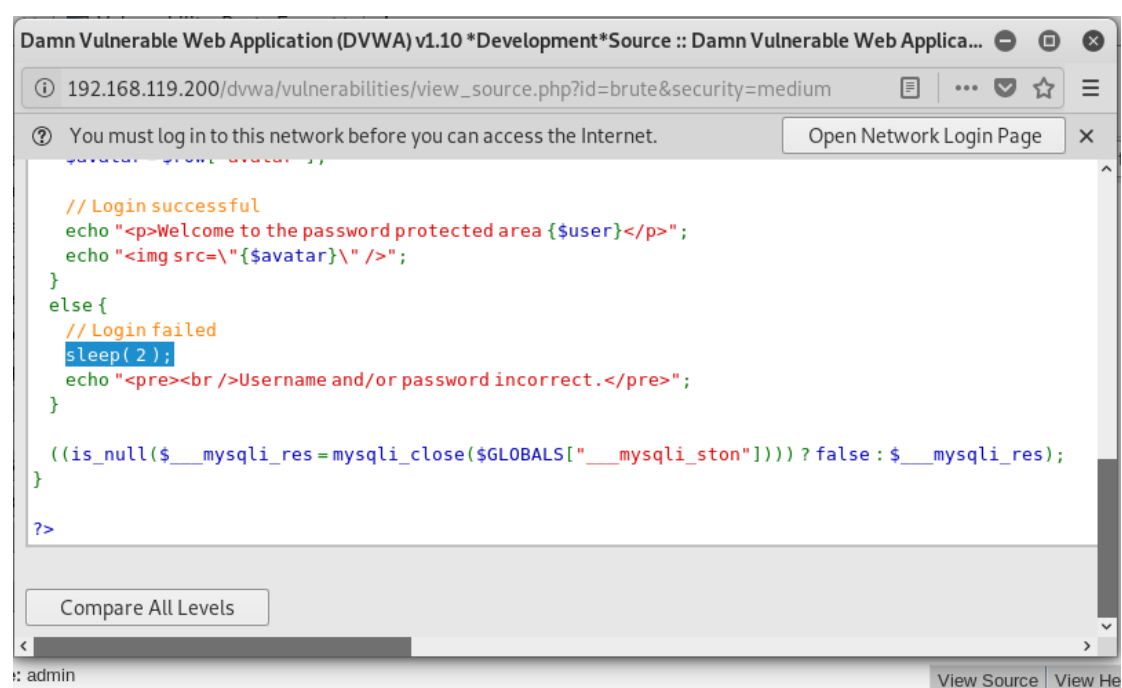


图 2.2

步骤 2：根据上述情况分析，防 SQL 注入并不能影响我们进行暴力破解，而登录失败的 2 秒延迟对暴力破解的影响也是微乎其微，所以我们这里直接使用 Low 级别的方式使用 Burpsuite 进行爆破即可。这里只展示最终结果，如图 2.3。

Attack Save Columns							
Results Target Positions Payloads Options							
Filter: Showing all items							
Requ... ▲	Payload	Status	Error	Timeo...	Length	Welco...	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
1	123	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
2	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
3	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
4	admin12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
5	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4747	<input type="checkbox"/>	
6	p@ssW0rd	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
7	passWord	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
8	11111	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
9	22222	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	
10	123.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4709	<input type="checkbox"/>	

图 2.3