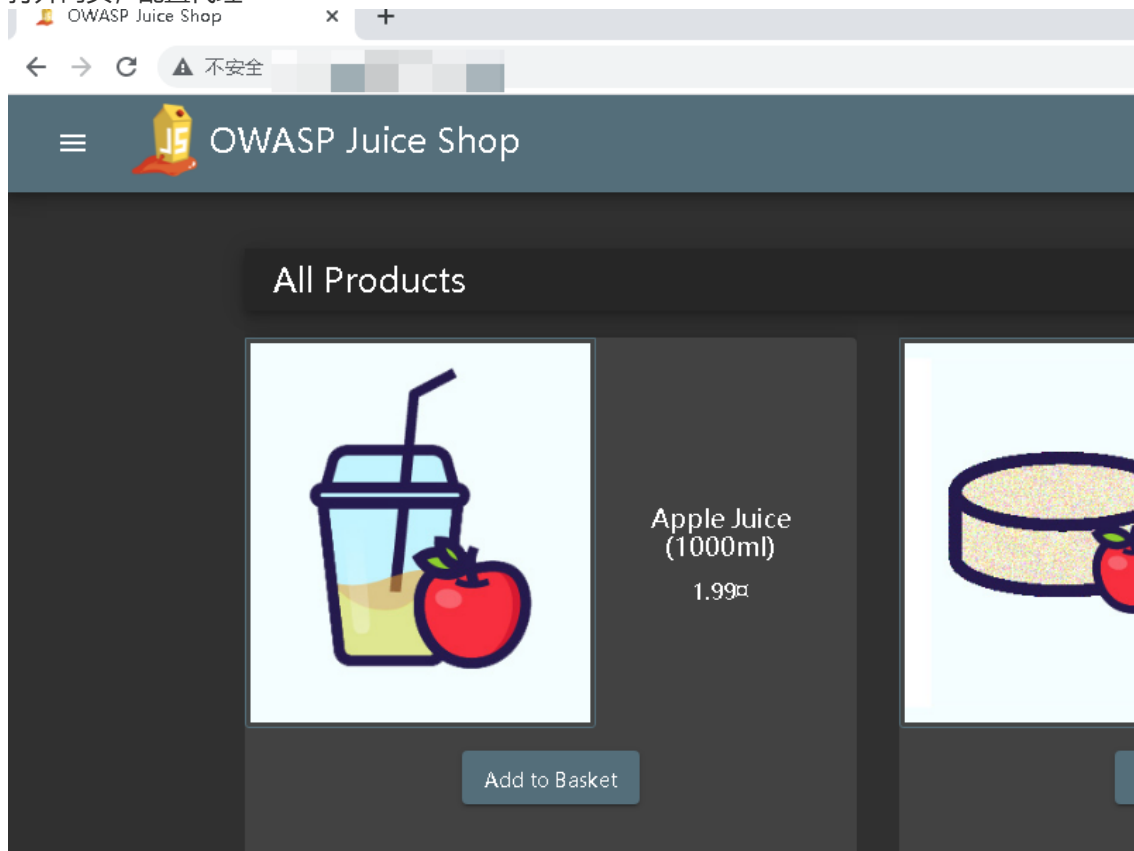


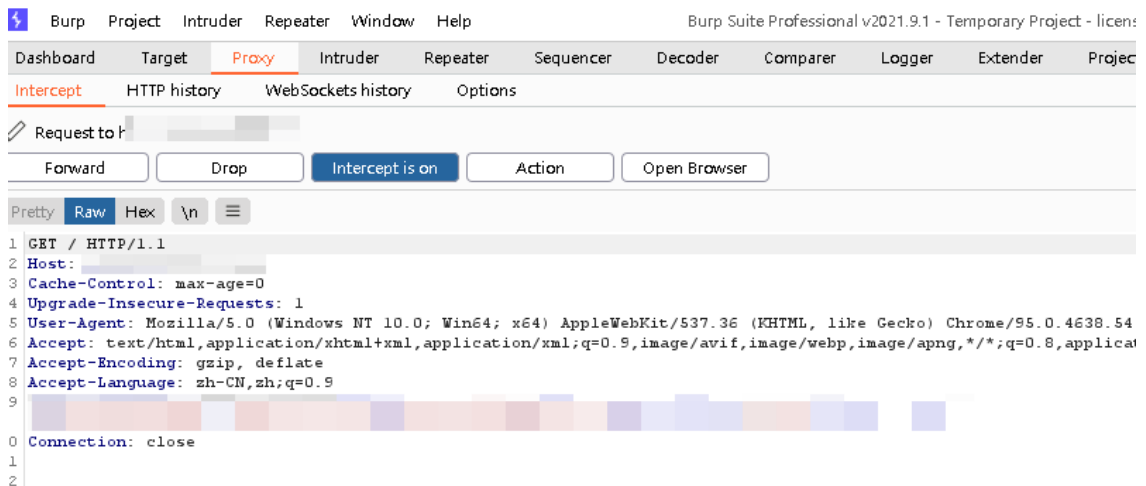
Intruder模块实战

sniper攻击方式

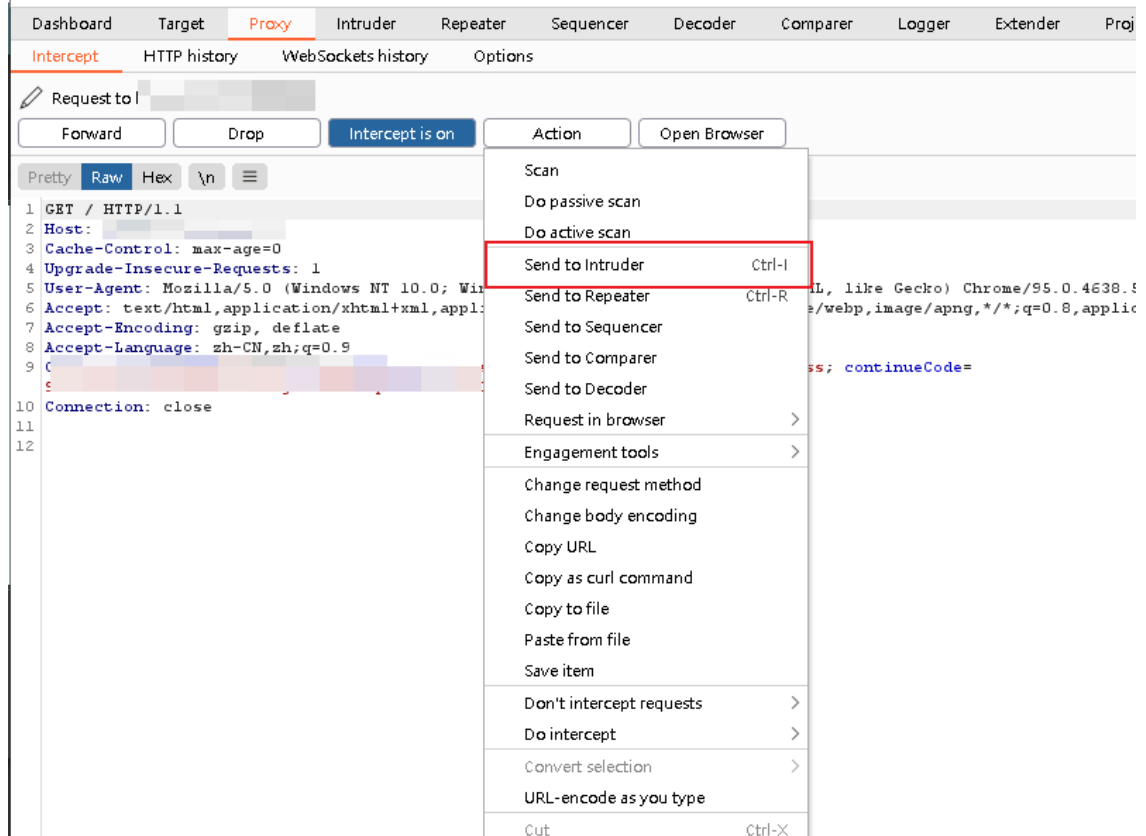
1. 打开网页，配置代理



2. 开启Proxy拦截，抓取刷新页面的数据包



3. 发送拦截数据包到Intruder模块



4. 设置Attack type攻击方式为Sniper，清除Burp自动设置的攻击标记位置，在GET请求的/后添加标记位置

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET / HTTP/1.1
2 Host:
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
  continueCode=
10 Connection: close
11
12
```

Add §

Clear §

Auto §

Refresh

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /$$ HTTP/1.1
2 Host:
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
  continueCode=
10 Connection: close
11
12
```

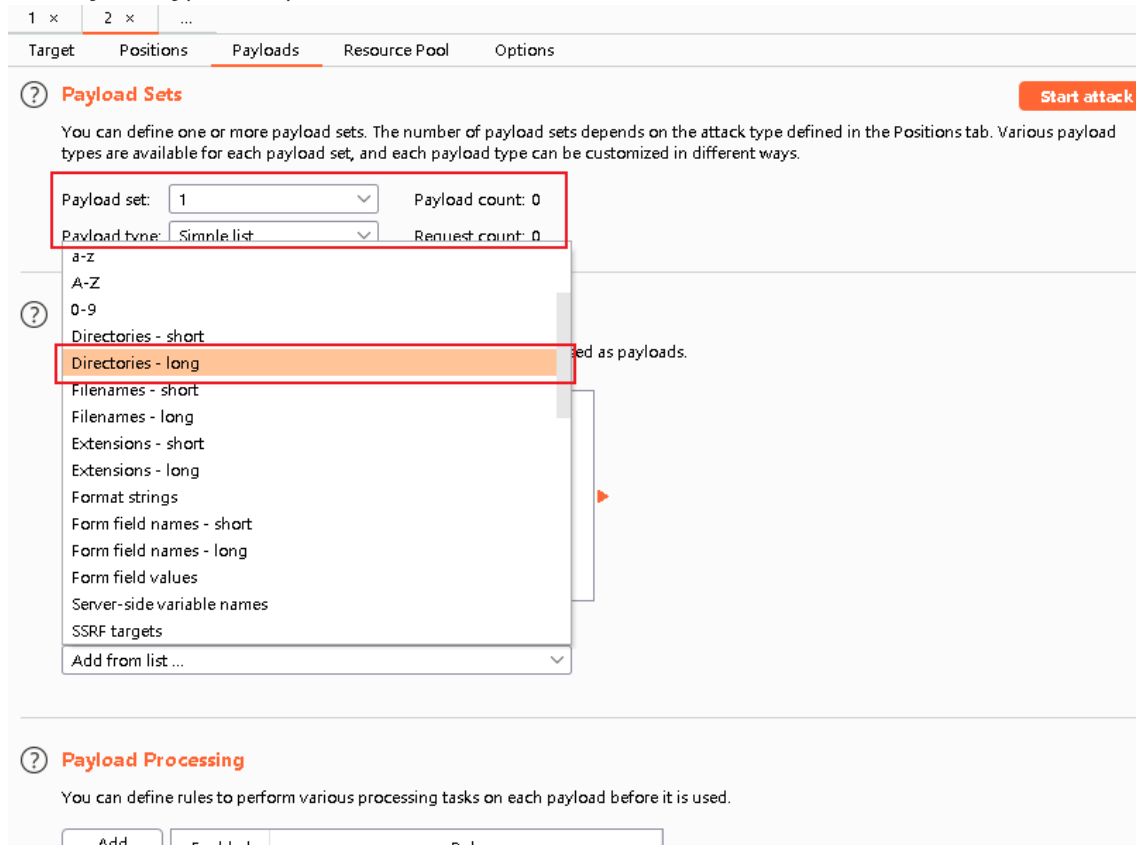
Add §

Clear §

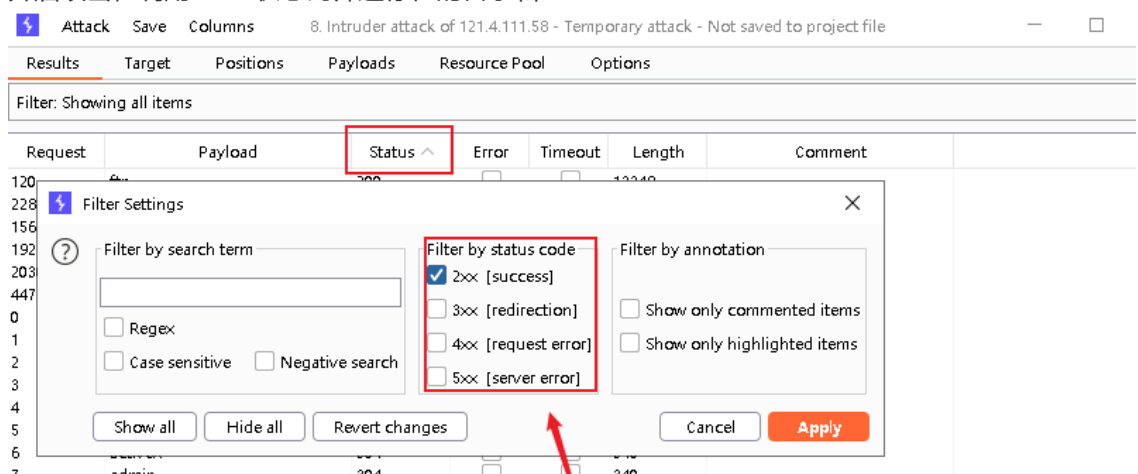
Auto §

Refresh

5. 设置Payload type为simple list，添加目录的密码字典



6. 开启攻击，利用HTTP状态码筛选存在的目录名

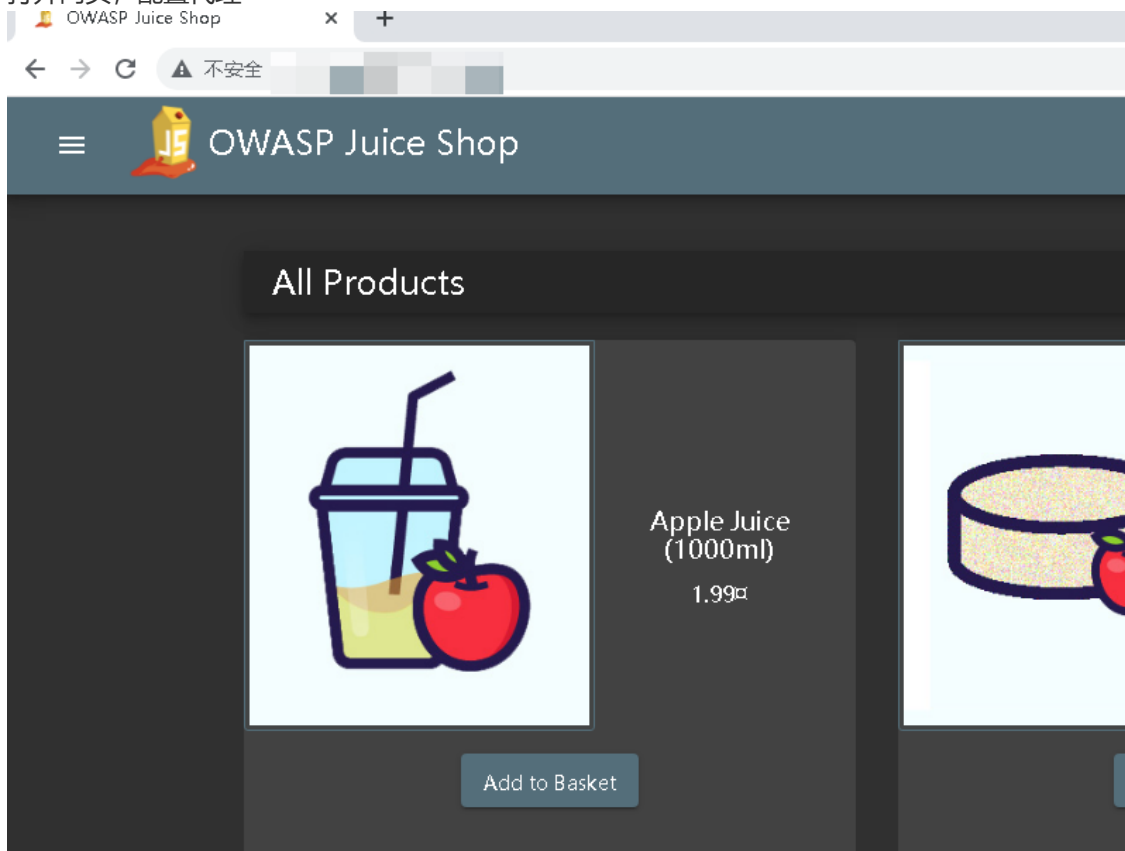


7. 成功爆破出服务器真实存在的目录

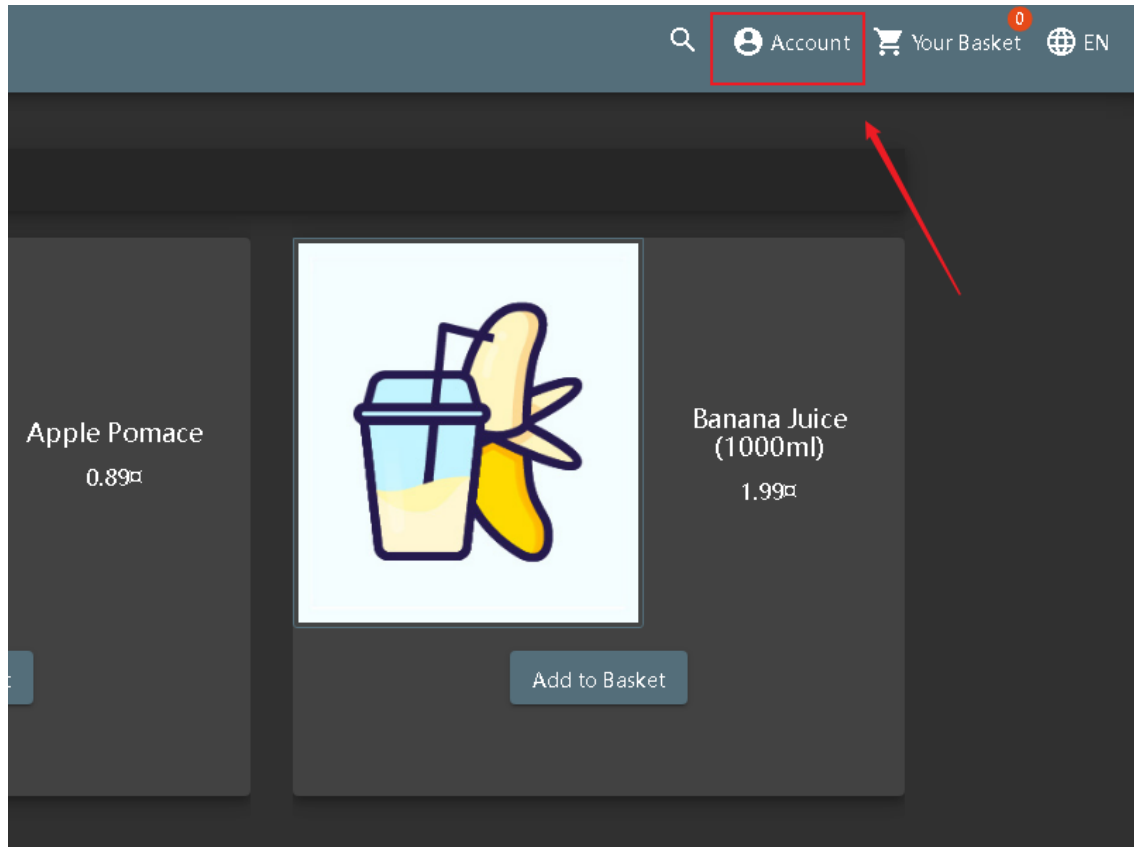
Attack Save Columns 8. Intruder attack of 121.4.111.58 - Temporary attack - Not saved to project file						
Results Target Positions Payloads Resource Pool Options						
Filter: Hiding 3xx, 4xx and 5xx responses						
Request	Payload	Status ^	Error	Timeout	Length	Comment
120	ftp	200	<input type="checkbox"/>	<input type="checkbox"/>	13349	
228	profile	200	<input type="checkbox"/>	<input type="checkbox"/>	6779	
1564	video	200	<input type="checkbox"/>	<input type="checkbox"/>	10075770	
1565	Video	200	<input type="checkbox"/>	<input type="checkbox"/>	10075770	
1922	ftp	200	<input type="checkbox"/>	<input type="checkbox"/>	13349	
2030	profile	200	<input type="checkbox"/>	<input type="checkbox"/>	6779	

Cluster bomb

1. 打开网页，配置代理



2. 点击Account尝试登陆



3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包

The screenshot displays the Burp Suite interface. At the top, a 'Login' form is visible with the following fields and controls:

- Email *: A text input field containing the value '1'.
- Password *: A password input field containing a single dot '.'.
- Forgot your password?: A link below the password field.
- Log in: A button with a right-pointing arrow icon.
- Remember me: A checkbox below the login button.
- Not yet a customer?: A link at the bottom of the form.

Below the login form, the Burp Suite toolbar is visible, with the 'Proxy' tab selected. The 'Intercept' sub-tab is active, showing the 'Request to h...' section. The 'Intercept is on' button is highlighted. The 'Request to h...' section shows the following details:

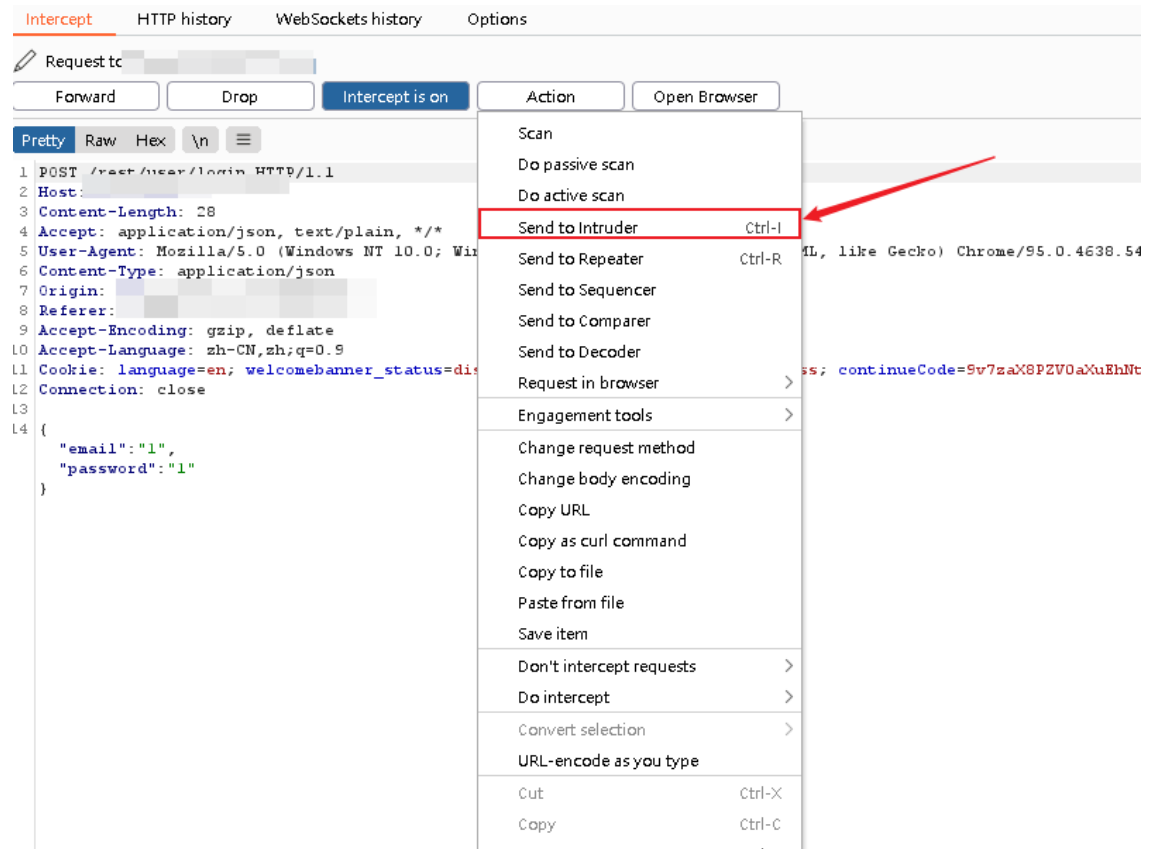
- Request to h...: A text input field.
- Forward: A button.
- Drop: A button.
- Intercept is on: A button.
- Action: A button.
- Open Browser: A button.

The 'Pretty' tab is selected in the request view, showing the following details:

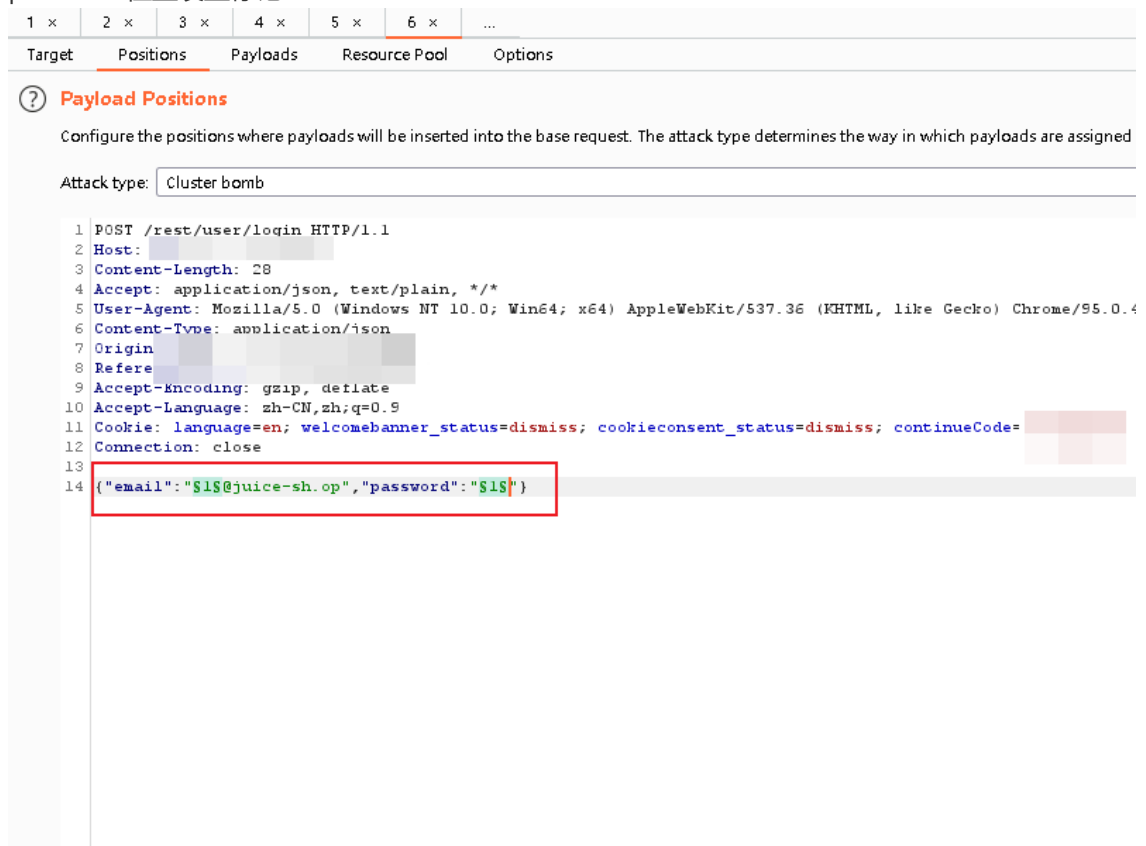
- 1 POST /rest/user/login HTTP/1.1
- 2 Host: [redacted]
- 3 Content-Length: 28
- 4 Accept: application/json, text/plain, */*
- 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.5
- 6 Content-Type: application/json
- 7 Origin: [redacted]
- 8 Referer: [redacted]
- 9 Accept-Encoding: gzip, deflate
- 10 Accept-Language: zh-CN,zh;q=0.9
- 11 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=9v7zaX8PZV0aXuEhN
- 12 Connection: close
- 13
- 14 {
- 15 "email": "1",
- 16 "password": "1"
- 17 }

The JSON body of the request is highlighted with a red box.

4. 发送到Intruder模块



5. 设置Attack type攻击方式为Cluster Bomb，清除Burp自动设置的攻击标记位置，在email和password位置设置标记



6. 在Payloads中设置第一个位置的Payload类型为simple list，添加用户名表

Target

Positions

Payloads

Resource Pool

Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types can be used as payloads.

Payload set: 1

Payload count: 8,894

Payload type: Simple list

Request count: 0

Add from list ...

Fuzzing - quick

Fuzzing - full

Username

Passwords

Short words

a-z

A-Z

0-9

Directories - short

Directories - long

Filenames - short

Filenames - long

Extensions - short

Extensions - long

Add from list ...

?

Payload Processing

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

Add

Enabled

Rule

Edit

在Payloads中设置第二个位置的Payload类型为simple list，添加密码表

1 x

2 x

3 x

4 x

5 x

6 x

...

Target

Positions

Payloads

Resource Pool

Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types can be used as payloads.

Payload set: 2

Payload count: 3,424

Payload type: Simple list

Request count: 30,453,056

Add from list ...

Fuzzing - quick

Fuzzing - full

Username

Passwords

Short words

a-z

A-Z

0-9

Directories - short

Directories - long

Filenames - short

Filenames - long

Extensions - short

Extensions - long

Add from list ...

?

Payload Processing

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

Add

Enabled

Rule

Edit

7. 或粘贴用户名和密码表

1 x
2 x
3 x
4 x
5 x
6 x
...

Target
Positions
Payloads
Resource Pool
Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available.

Payload set: 1

Payload count: 11

Payload type: Simple list

Request count: 1,100

? Payload Options (Simple list)

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ...

root

admin

test

guest

info

adm

mysql

user

administrator

Enter a new item

? Payload Processing

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

Add

Enabled

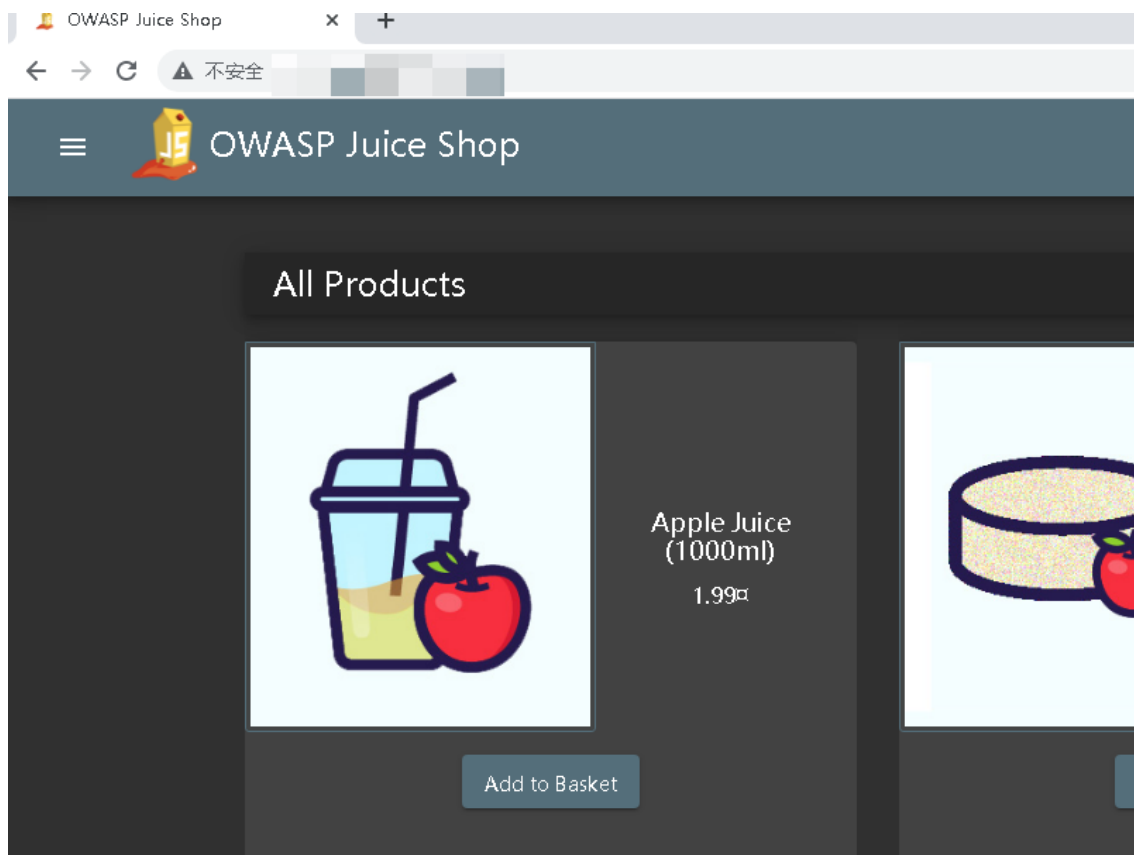
Rule

8. 开启攻击后利用HTTP状态码排序或Filter排序筛选账号名和密码

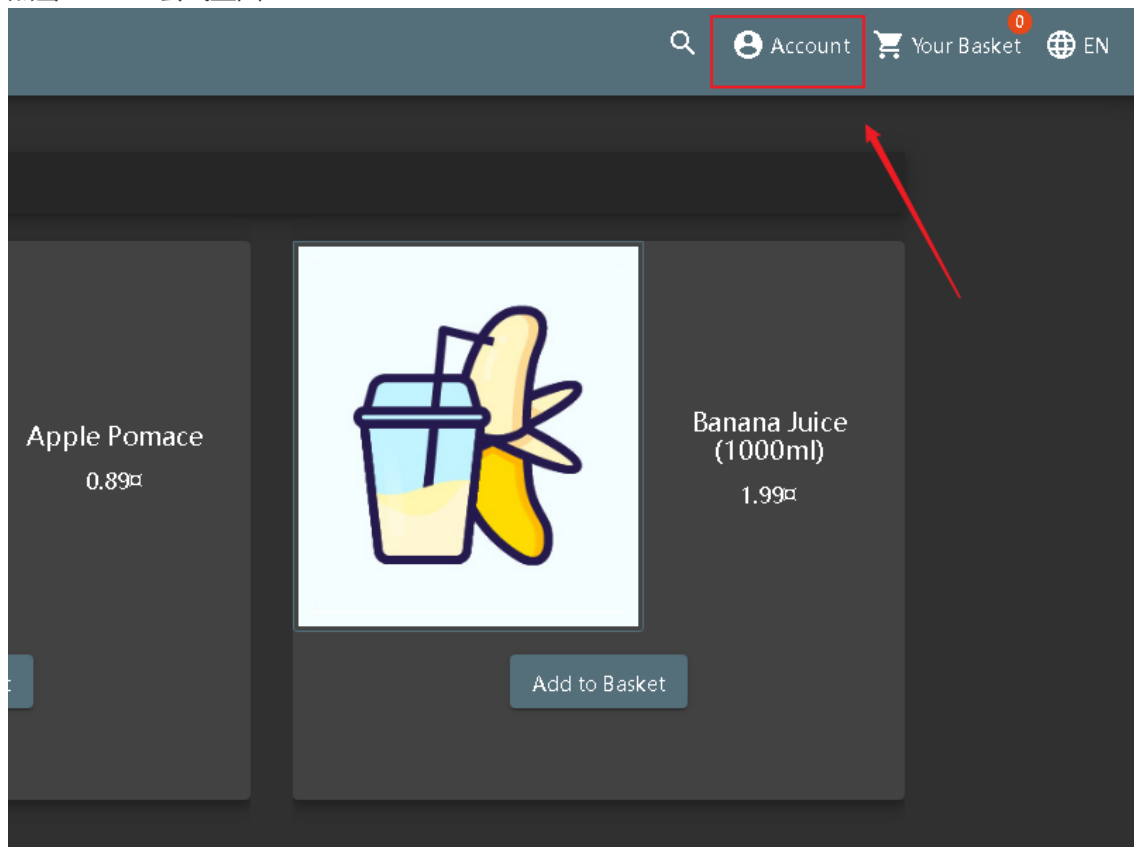
The screenshot displays the Burp Suite interface. At the top, the 'Filter' tab is active, showing a table with columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. A red box highlights the 'Status' column header, and a red arrow points to it. Below the table, a 'Filter Settings' dialog box is open. The dialog has three sections: 'Filter by search term' (with a search input field and checkboxes for 'Regex' and 'Case sensitive'), 'Filter by status code' (with checkboxes for '2xx [success]', '3xx [redirection]', '4xx [request error]', and '5xx [server error]'), and 'Filter by annotation' (with checkboxes for 'Show only commented items' and 'Show only highlighted items'). The '2xx [success]' checkbox is checked and highlighted with a red box. At the bottom of the dialog are buttons for 'Show all', 'Hide all', 'Revert changes', 'Cancel', and 'Apply'. The background shows a REST client request for 'http://bears1:401' with a 'Vary: Accept-Encoding' header and a JSON body containing authentication details.

Pitfork

1. 打开网页，配置代理，需先行注册账号保证后缀一致（如[1@mail.com](#)和[2@mail.com](#)或[1@t.com](#)和[2@t.com](#)）



2. 点击Account尝试登陆



3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包

The screenshot displays the Burp Suite interface. At the top, a 'Login' form is visible with the following fields and controls:

- Email ***: A text input field containing the value '1'.
- Password ***: A password input field containing a single dot '.'.
- Forgot your password?**: A link below the password field.
- Log in**: A button with a right-pointing arrow icon.
- Remember me**: A checkbox below the login button.
- Not yet a customer?**: A link at the bottom of the form.

Below the login form, the Burp Suite toolbar and HTTP history are visible. The 'Proxy' tab is selected, and the 'Intercept' sub-tab is active. The 'Request to h...' section shows the following details:

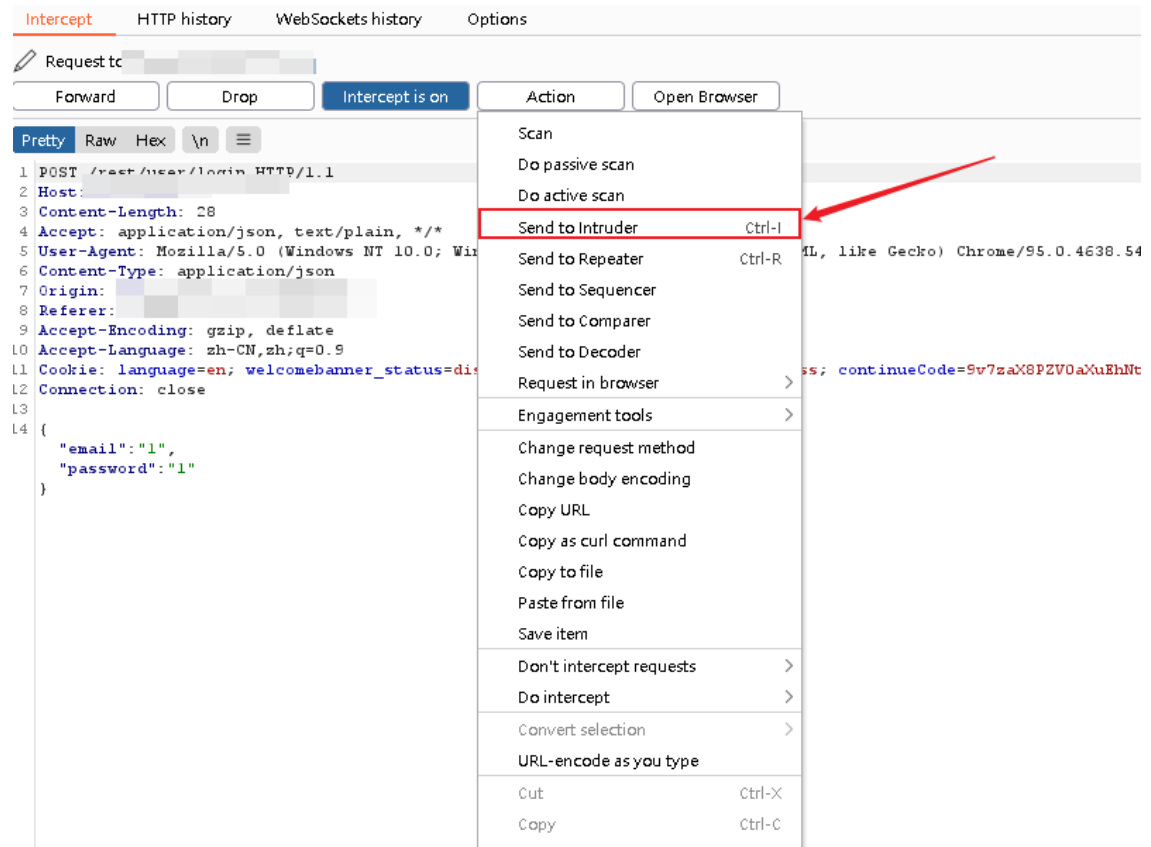
- Forward**, **Drop**, **Intercept is on**, **Action**, and **Open Browser** buttons.
- Pretty**, **Raw**, **Hex**, and **\n** tabs.

The intercepted request is a POST to `/rest/user/login` with the following headers and body:

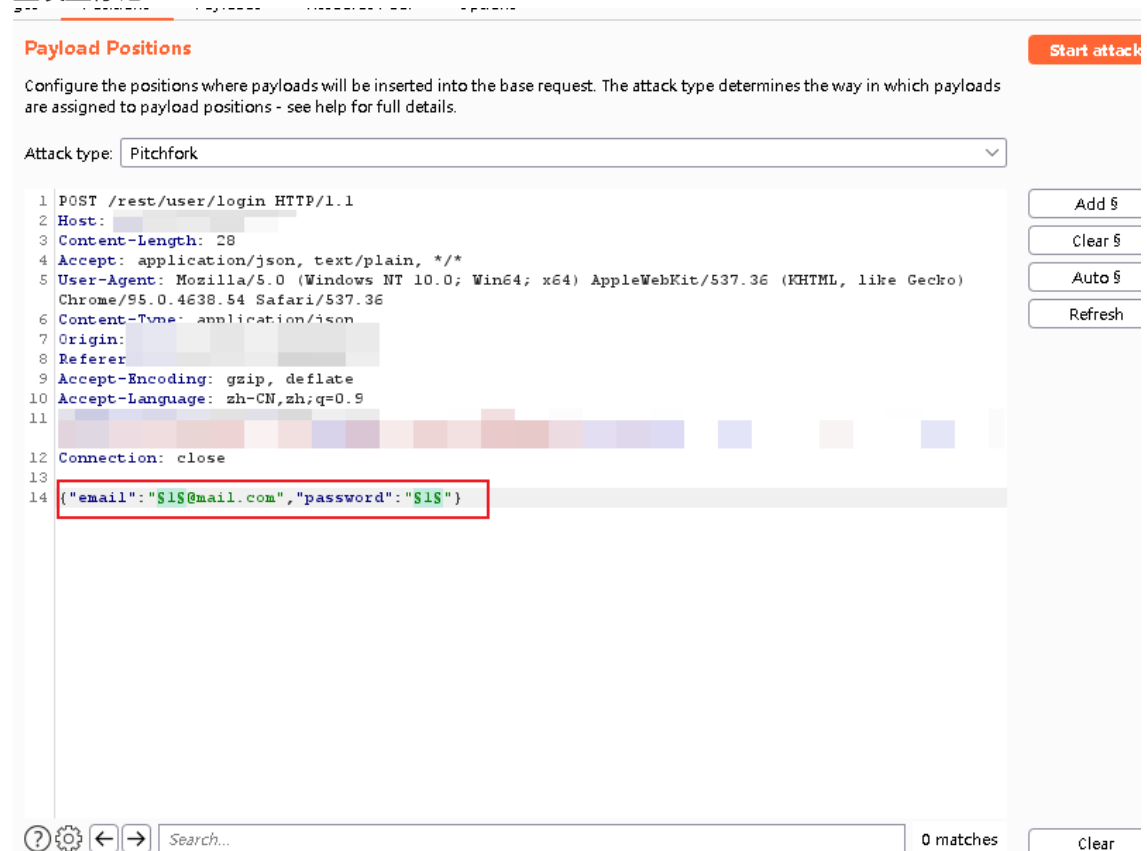
```
1 POST /rest/user/login HTTP/1.1
2 Host: [redacted]
3 Content-Length: 28
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
6 Content-Type: application/json
7 Origin: [redacted]
8 Referer: [redacted]
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=9v7zaX8PZV0aXuEhN
12 Connection: close
13
14 {
15   "email": "1",
16   "password": "1"
17 }
```

The JSON body is highlighted with a red box.

4. 发送到Intruder模块



5. 设置Attack type攻击方式为Pitfork，清除Burp自动设置的攻击标记位置，在email和password位置设置标记



6. 在Payload中粘贴用户名和密码

Target

Positions

Payloads

Resource Pool

Options

?

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

Payload count:

2

Payload type:

Simple list

Request count:

2

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

1

Load ...

2

Remove

Clear

Deduplicate

Add

Enter a new item

Add from list ...

?

Payload Processing

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

Add

Enabled

Rule

Target

Positions

Payloads

Resource Pool

Options

?

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

2

Payload count:

2

Payload type:

Simple list

Request count:

2

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

testtest

Load ...

testtest

Remove

Clear

Deduplicate

Add

Enter a new item

Add from list ...

?

Payload Processing

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

Add

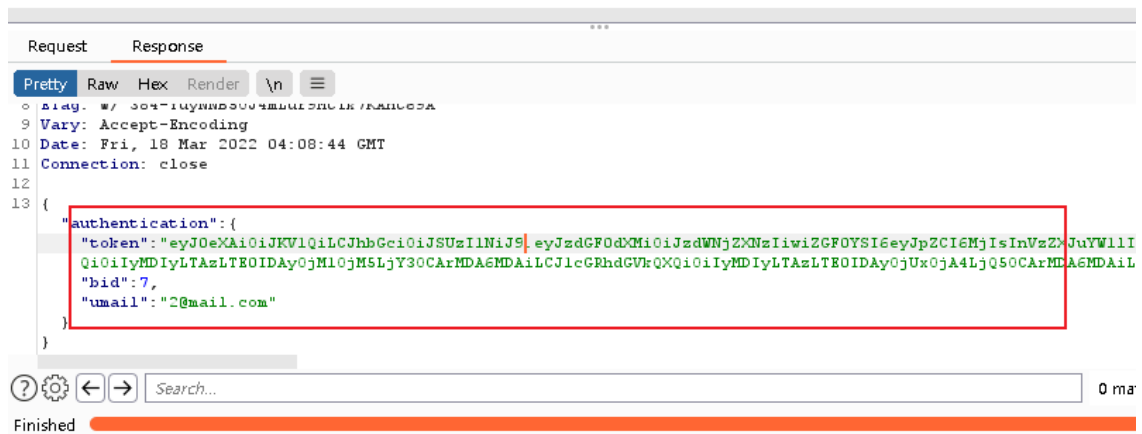
Enabled

Rule

Edit

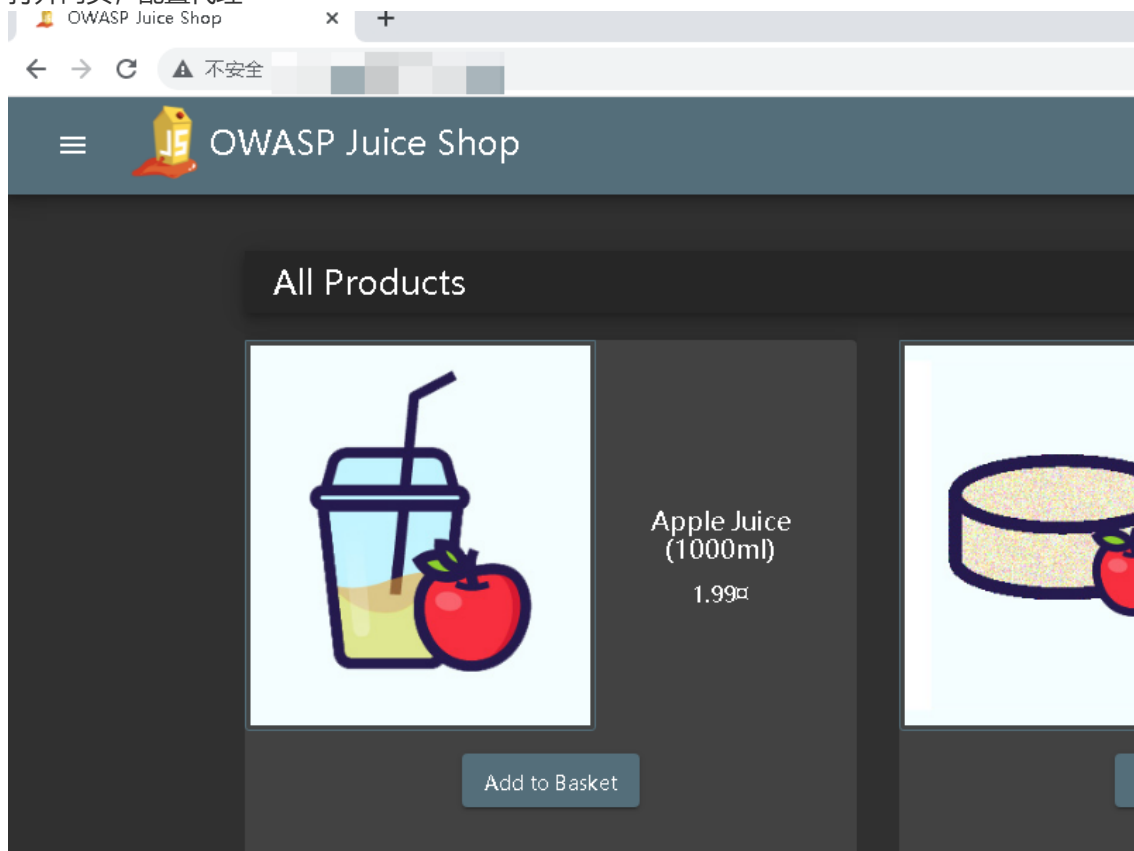
7. 开启攻击，成功返回

Results	Target	Positions	Payloads	Resource Pool	Options				
Filter: Showing all items									
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment		
0			401	<input type="checkbox"/>	<input type="checkbox"/>	362			
1	1	testtest	200	<input type="checkbox"/>	<input type="checkbox"/>	1240			
2	2	testtest	200	<input type="checkbox"/>	<input type="checkbox"/>	1235			

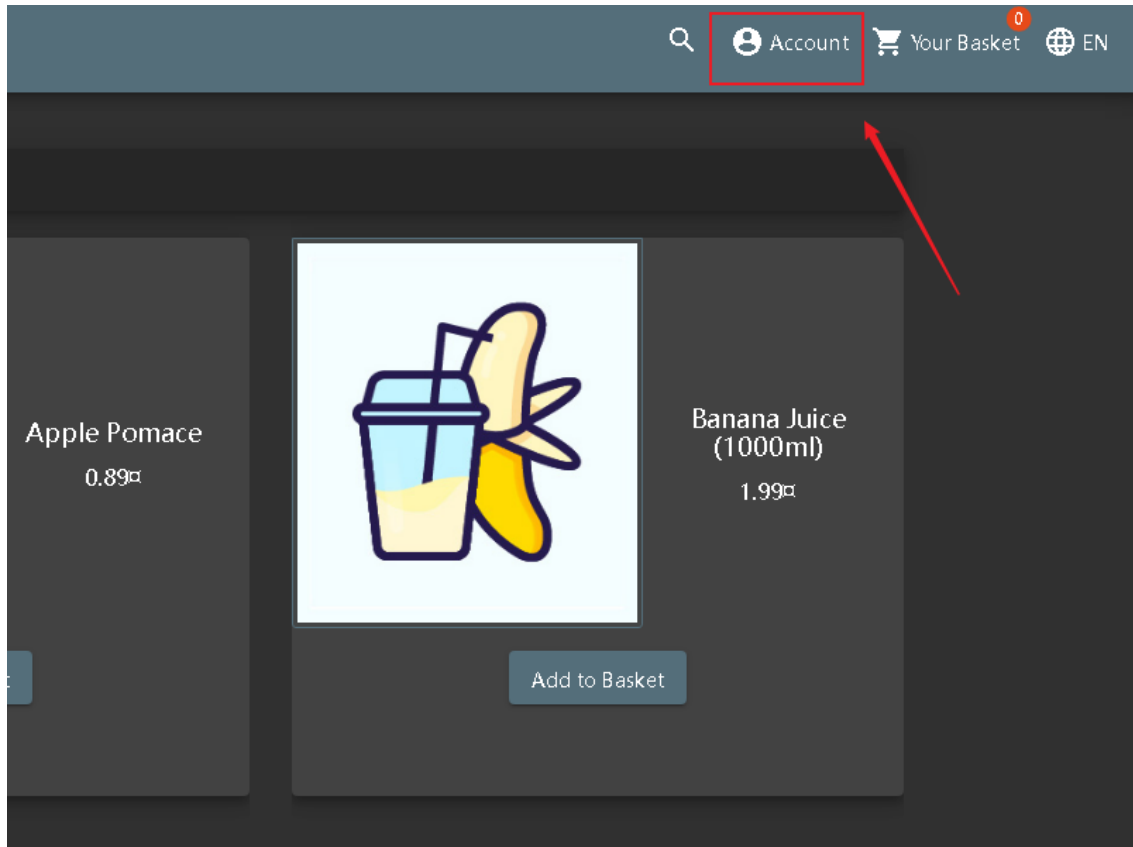


Battering ram

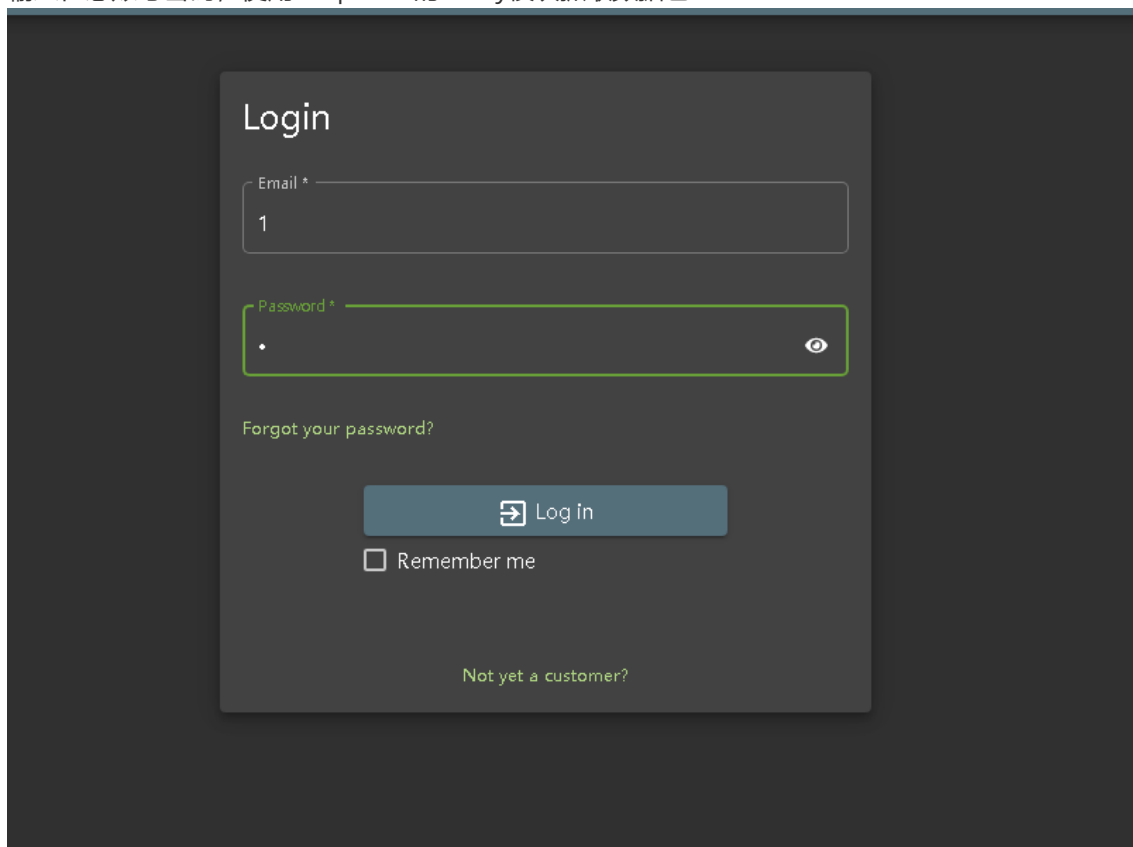
1. 打开网页，配置代理

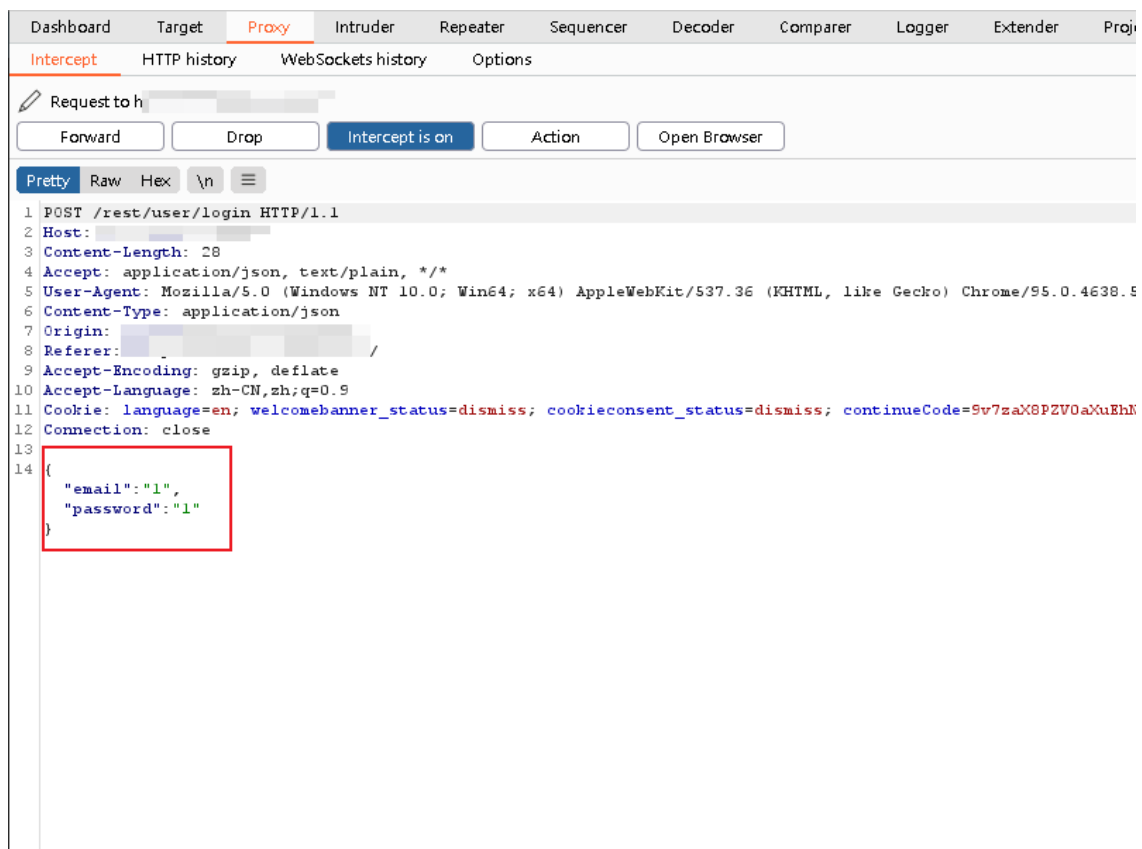


2. 点击Account尝试登陆

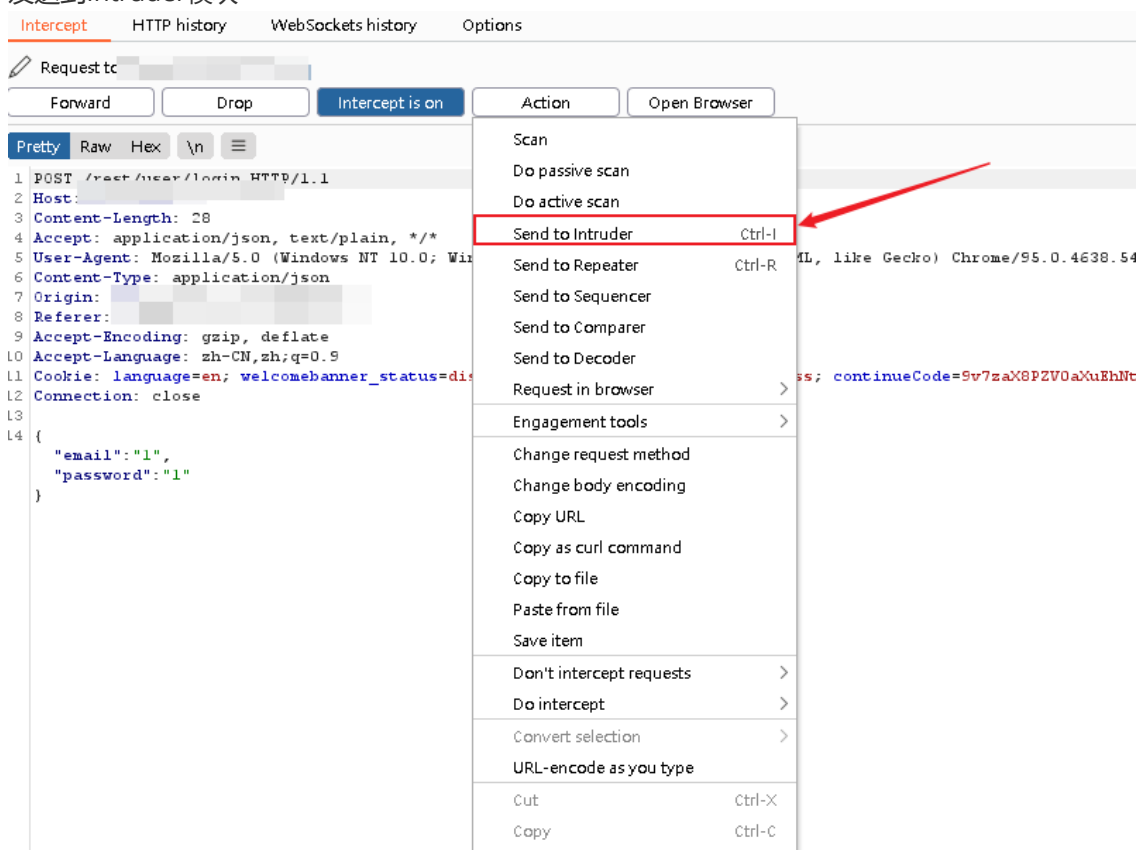


3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包





4. 发送到Intruder模块



5. 设置Attack type攻击方式为Battering ram，清除Burp自动设置的攻击标记位置，在email和password位置设置标记

Start attac

Attack type: **Battering ram**

Add 5

Clear 5

Auto 5

Refresh

0 matches

0 matches

Clear

1 x	2 x	...
-----	-----	-----

Target	Positions	Payloads	Resource Pool	Options
--------	-----------	----------	---------------	---------

Start at

Payload set: 1 Payload count: 11

Payload type: Simple list Request count: 11

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	root
-------	------

	admin
--	-------

test
quest

Remove

Clear

Deduplicate

administrator

Add

Add from list ...

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

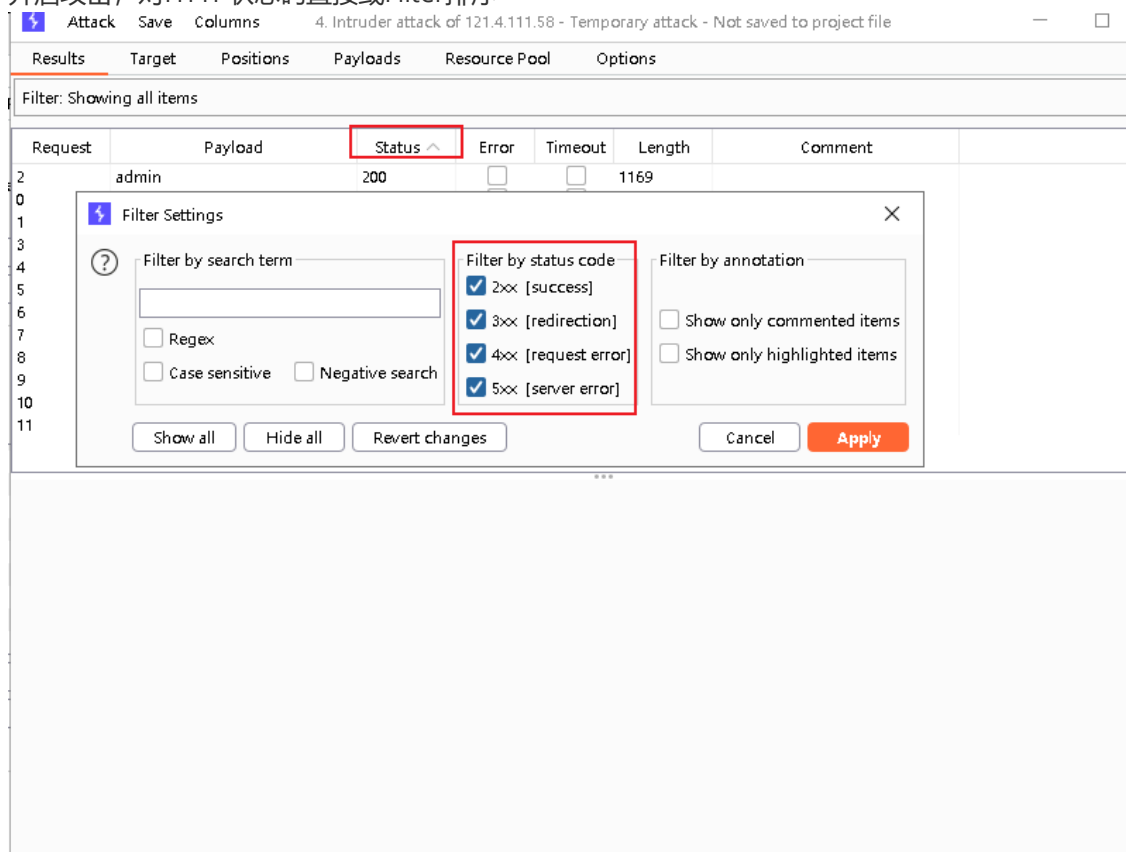
You can define rules to perform various processing tasks on each payload before it is used.

Add

Enabled

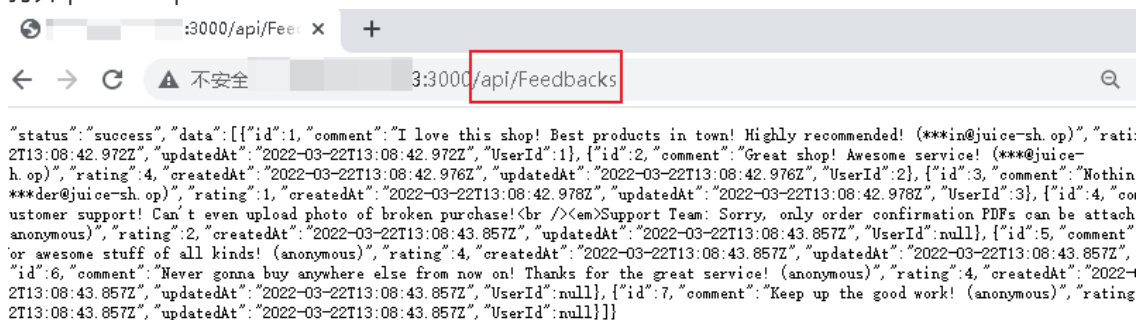
Rule

7. 开启攻击，对HTTP状态码直接或Filter排序

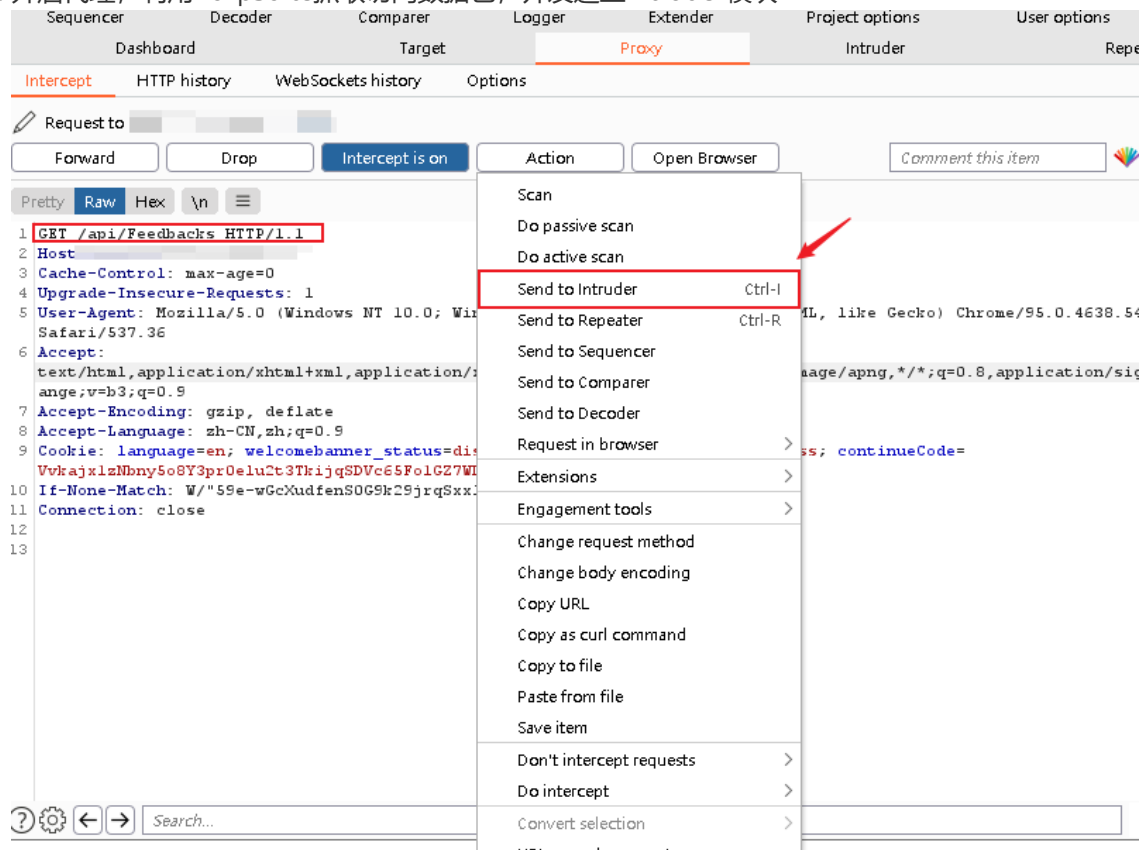


CAPTCHA Bypass

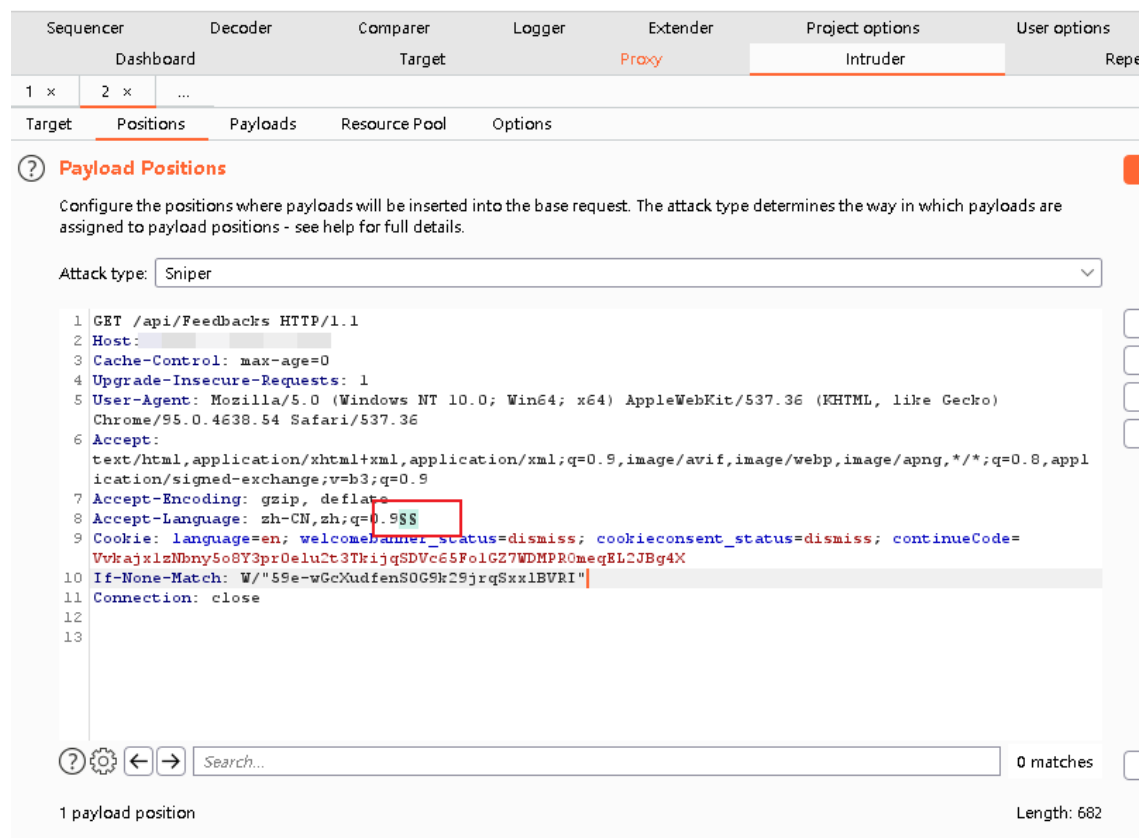
1. 打开ip:3000/api/Feedbacks/



2. 开启代理，利用BurpSuite抓取访问数据包，并发送至Intruder模块



3. 清除现有Positions，任意设置位置处为空Payload，攻击类型为Sniper



4. Payload type 设置为 Null payloads

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

Dashboard

Target

Proxy

Intruder

Repeat

1 x2 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Sets

Sta

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types available for each payload set, and each payload type can be customized in different ways.

Payload set:1

Payload count: 0

Payload type:Simple list

Request count: 0

?

Payload Options

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the unmodified.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ...

Character substitution

Case modification

Recursive grep

Illegal Unicode

Character blocks

Numbers

Dates

Brute forcer

Null payloads

Character frotter

Bit flipper

Username generator

ECB block shuffler

Extension-generated

Copy other payload

Simple list of strings that are used as payloads.

5. 设置发出10次请求

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

Dashboard

Target

Proxy

Intruder

Repeat

1 x2 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Sets

S

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types available for each payload set, and each payload type can be customized in different ways.

Payload set:1

Payload count: 10

Payload type:Null payloads

Request count: 10

?

Payload Options [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the unmodified.

☒ Generate10payloads

☐ Continue indefinitely

?

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

6. 开启攻击，完成CAPTCHA Bypass挑战