Host Header Injection

CHAMELEON

FOR OUR SMARTER WORLD

LEON NETTO

1. Executive Summary

This executive summary provides an overview of the findings from a penetration test conducted on the Chameleon and MOP websites, focusing on host header injection vulnerabilities. The test aimed to assess the security posture of both websites and determine the effectiveness of existing defences against such attacks.

Using Kali Linux and Burp Suite, attempts were made to manipulate the Host header and X-Forwarded-Host header to exploit potential vulnerabilities. However, the tests revealed that both websites appear to be well-secured, as the attacks were unsuccessful.

2. Purpose

The purpose of this penetration test was to identify and address potential vulnerabilities in the Chameleon and MOP websites, particularly focusing on host header injection attacks. By conducting controlled security assessments, the aim was to evaluate the effectiveness of existing security measures and identify any weaknesses that could be exploited by malicious actors. Ultimately, the goal was to enhance the overall security posture of both websites and mitigate the risk of unauthorised access or data breaches.

3. Scope

The scope of this penetration test encompassed the assessment of host header injection vulnerabilities on the Chameleon and MOP websites. The test specifically targeted the manipulation of the Host header and X-Forwarded-Host header to exploit potential weaknesses in the web applications' security defences.

The assessment included:

- Windows 11 workstation.
- Pentest on the MOP website hosted in GCP - https://react-test-6najyje5cq-uc.a.run.app/.
- Pentest on the Chameleon website hosted in GCP - https://sit374-2024-t1-chameleon.com/.
- Use of tools such as Kali Linux and Burp Suite to simulate real-world attack scenarios while adhering to ethical guidelines.

4. Findings

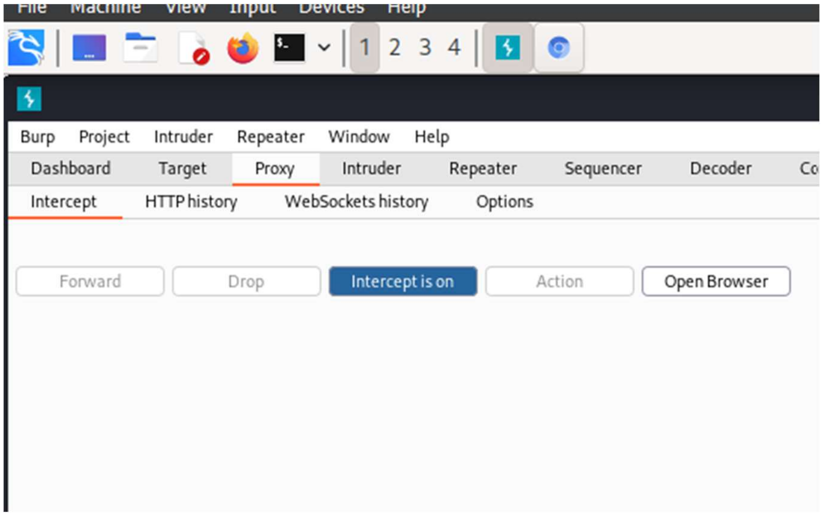
The findings of the penetration test indicate that both the Chameleon and MOP websites demonstrate a robust level of security against host header injection attacks. Despite attempts to manipulate the Host header and X-Forwarded-Host header using

Burp Suite, the attacks were unsuccessful. It appears that the websites have implemented effective security measures to validate and sanitise input, preventing unauthorised manipulation of HTTP headers.

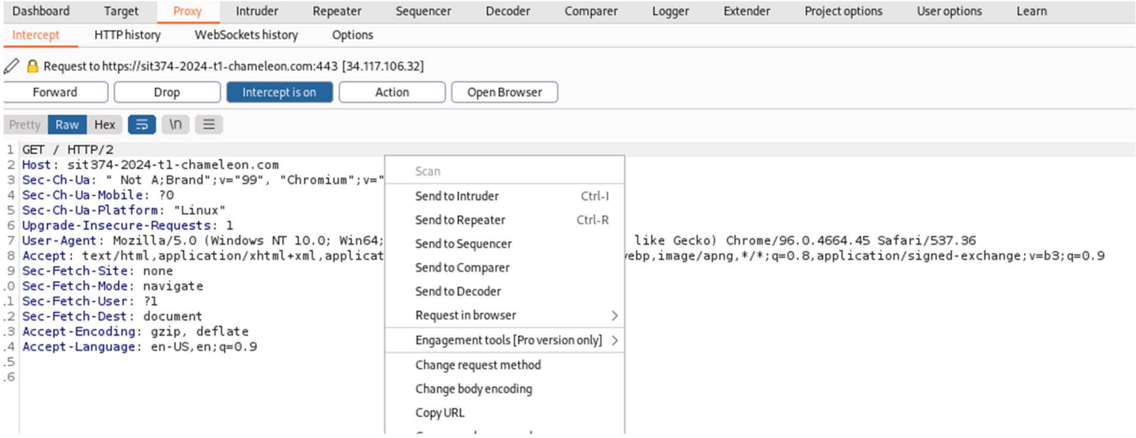
As a result, there is a low likelihood of successful exploitation of host header injection vulnerabilities on both websites. However, continuous monitoring and proactive security measures are recommended to maintain and further enhance the security posture of the Chameleon and MOP websites.

5. Host Header Attack on Chameleon Website – Steps and Results

Step 1 – Select Proxy in Burpe Suite and ensure Intercept. Select Open browser and navigate to the website.



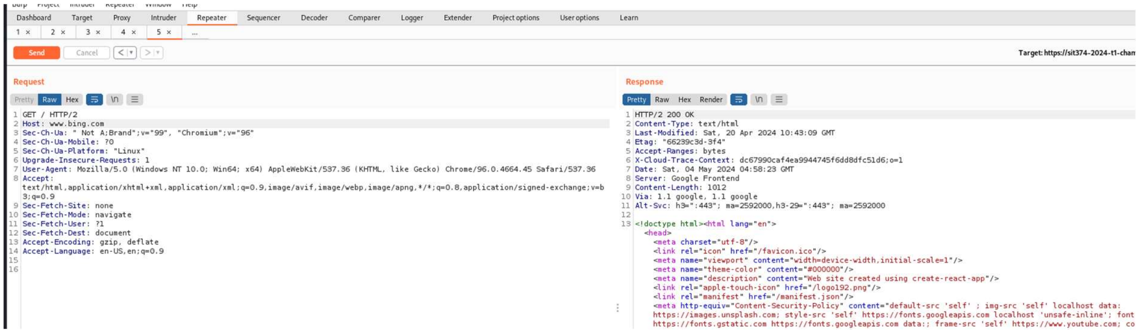
Step 2 – You will be directed back to the Intercept page. Right click on the Request header and select Send to Repeater.



Request to https://sit374-2024-t1-chameleon.com:443 [34.117.106.32]

```
GET / HTTP/2
Host: sit374-2024-t1-chameleon.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;                                like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,applicat                               ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Step 3 – Update Host to whatever address you like. In this scenario www.bing.com was entered. Click Send once complete.

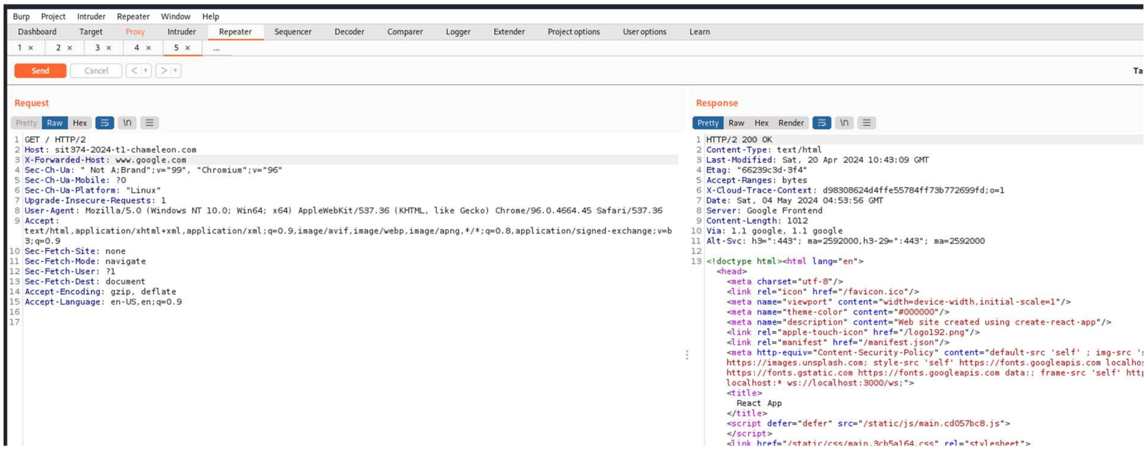


```
GET / HTTP/2
Host: www.bing.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Sat, 20 Apr 2024 10:43:09 GMT
Etag: "66239c3d-3f4"
Accept-Ranges: bytes
X-Cloud-Trace-Context: dc67990caf4ea9944745f6dd8dfc51d6;o=1
Date: Sat, 04 May 2024 04:58:23 GMT
Server: Google Frontend
Content-Length: 1012
Via: 1.1 google, 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!doctype html><html lang="en">
  <head>
    <meta charset="utf-8"/>
    <link rel="icon" href="/favicon.ico"/>
    <meta name="viewport" content="width=device-width,initial-scale=1"/>
    <meta name="theme-color" content="#000000"/>
    <meta name="description" content="Web site created using create-react-app"/>
    <link rel="apple-touch-icon" href="/logo192.png"/>
    <link rel="manifest" href="/manifest.json"/>
    <meta http-equiv="Content-Security-Policy" content="default-src 'self' ; img-src 'self' localhost data:
    https://images.unsplash.com; style-src 'self' https://fonts.googleapis.com localhost 'unsafe-inline'; font
    https://fonts.gstatic.com https://fonts.googleapis.com data:; frame-src 'self' https://www.youtube.com; co
```

To test the X-Forwaded-Host, enter a new line and enter the URL that you intend it to be forwarded to.

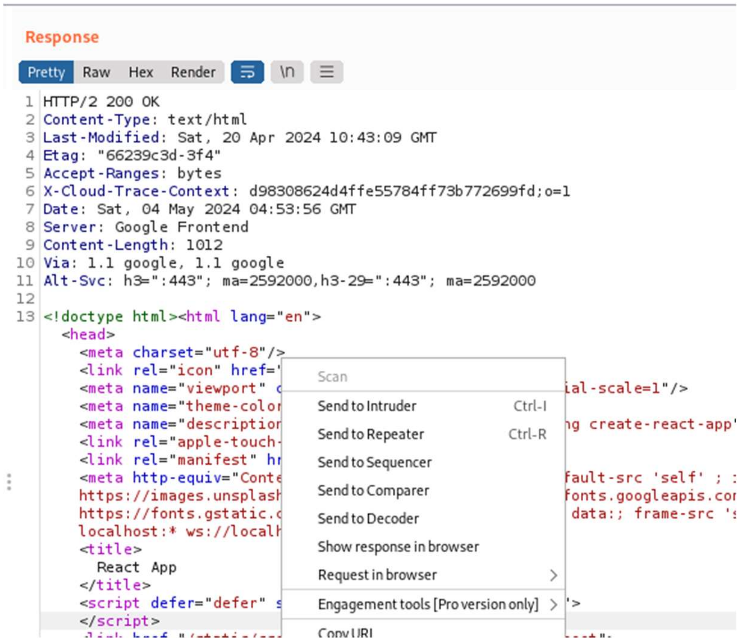


```
GET / HTTP/2
Host: sit374-2024-t1-chameleon.com
X-Forwarded-Host: www.google.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Sat, 20 Apr 2024 10:43:09 GMT
Etag: "66239c3d-3f4"
Accept-Ranges: bytes
X-Cloud-Trace-Context: d98308624d4ffe55784ff73b772699fd;o=1
Date: Sat, 04 May 2024 04:53:56 GMT
Server: Google Frontend
Content-Length: 1012
Via: 1.1 google, 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!doctype html><html lang="en">
  <head>
    <meta charset="utf-8"/>
    <link rel="icon" href="/favicon.ico"/>
    <meta name="viewport" content="width=device-width,initial-scale=1"/>
    <meta name="theme-color" content="#000000"/>
    <meta name="description" content="Web site created using create-react-app"/>
    <link rel="apple-touch-icon" href="/logo192.png"/>
    <link rel="manifest" href="/manifest.json"/>
    <meta http-equiv="Content-Security-Policy" content="default-src 'self' ; img-src ':
    https://images.unsplash.com; style-src 'self' https://fonts.googleapis.com localho:
    https://fonts.gstatic.com https://fonts.googleapis.com data:; frame-src 'self' htt
    localhost:* ws://localhost:3000/ws;">
    <title>
      React App
    </title>
    <script defer="defer" src="/static/js/main.cd057bc8.js">
    </script>
    <link href="/static/css/main.3cb5a164.css" rel="stylesheet">
```

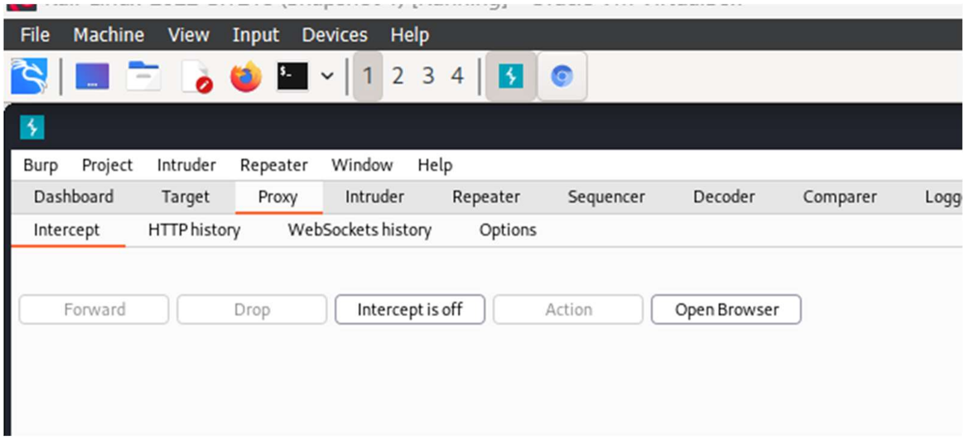
Step 4: Right click on the Response and select Open Response in Browser.



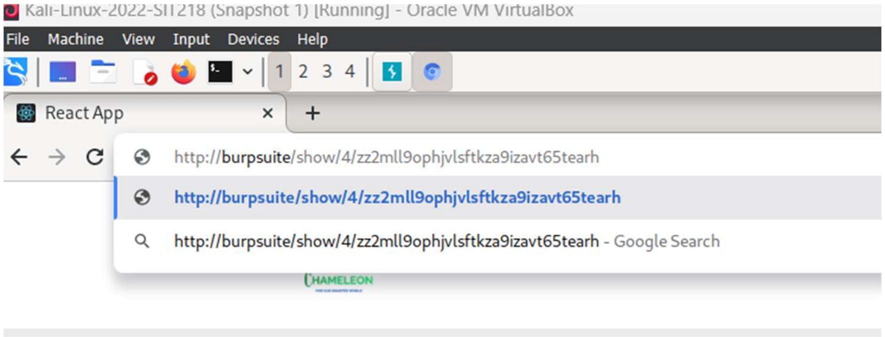
```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Sat, 20 Apr 2024 10:43:09 GMT
Etag: "66239c3d-3f4"
Accept-Ranges: bytes
X-Cloud-Trace-Context: d98308624d4ffe55784ff73b772699fd;o=1
Date: Sat, 04 May 2024 04:53:56 GMT
Server: Google Frontend
Content-Length: 1012
Via: 1.1 google, 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!doctype html><html lang="en">
  <head>
    <meta charset="utf-8"/>
    <link rel="icon" href="
    <meta name="viewport" c                              ial-scale=1"/>
    <meta name="theme-color
    <meta name="description                              g create-react-app'
    <link rel="apple-touch-
    <link rel="manifest" hr
    <meta http-equiv="Conte                              fault-src 'self' ; :
    https://images.unsplash                              fonts.googleapis.co
    https://fonts.gstatic.c                               data:; frame-src ':
    localhost:* ws://localh
    <title>
      React App
    </title>
    <script defer="defer" s                              '>
    </script>
```

Step 5: Select Proxy and ensure Intercept is off by selecting it.



Step 6: Navigate to the Burpe Suite browser and enter the website. In this scenario, the Chameleon website was entered.

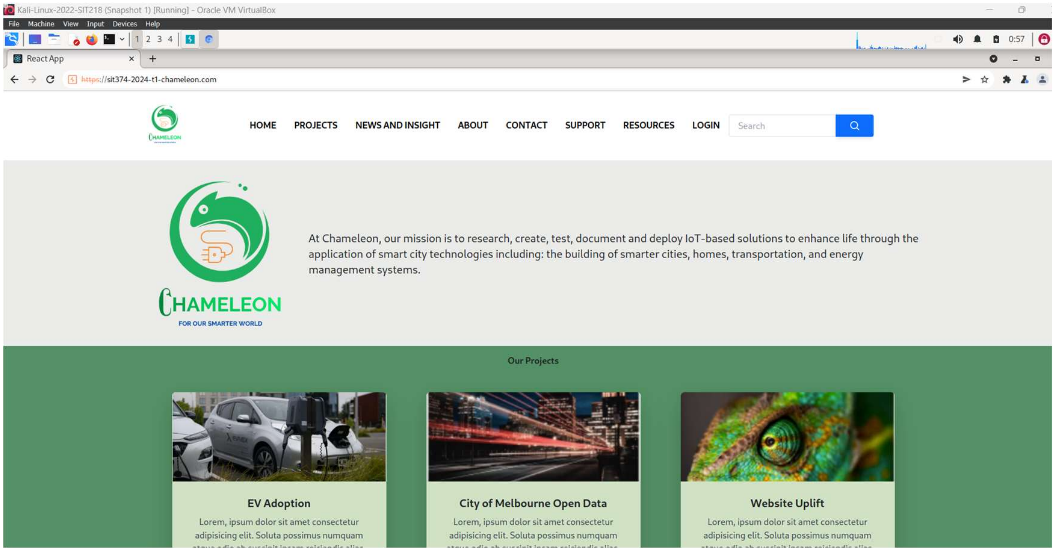

Kali-Linux-2022-SIT218 (Snapshot 1) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1 2 3 4
React App
CHAMELEON

http://burpsuite/show/4/zz2mll9ophjvlsftkza9izavt65tearh

http://burpsuite/show/4/zz2mll9ophjvlsftkza9izavt65tearh

http://burpsuite/show/4/zz2mll9ophjvlsftkza9izavt65tearh - Google Search

Step 7 – If the attack was successful, you would have been redirected to the website that was entered in the Response header. In this scenario, we can see the URL did not redirect when manipulating the Host and X-Forwarded-Host headers.



https://sit374-2024-t1-chameleon.com

At Chameleon, our mission is to research, create, test, document and deploy IoT-based solutions to enhance life through the application of smart city technologies including: the building of smarter cities, homes, transportation, and energy management systems.

Our Projects

EV Adoption

Lorem, ipsum dolor sit amet consectetur adipisicing elit. Soluta possimus numquam

City of Melbourne Open Data

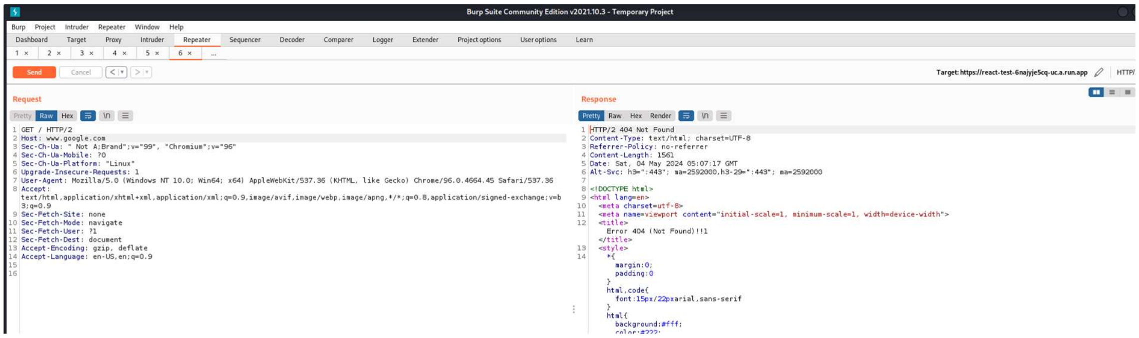
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Soluta possimus numquam

Website Uplift

Lorem, ipsum dolor sit amet consectetur adipisicing elit. Soluta possimus numquam

6. Host Header Attack on MOP Website – Steps and Results

Step 1: Changed the Host to www.google.com.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

Target: https://react-test-6najyje5cq-uc.a.run.app

Request:

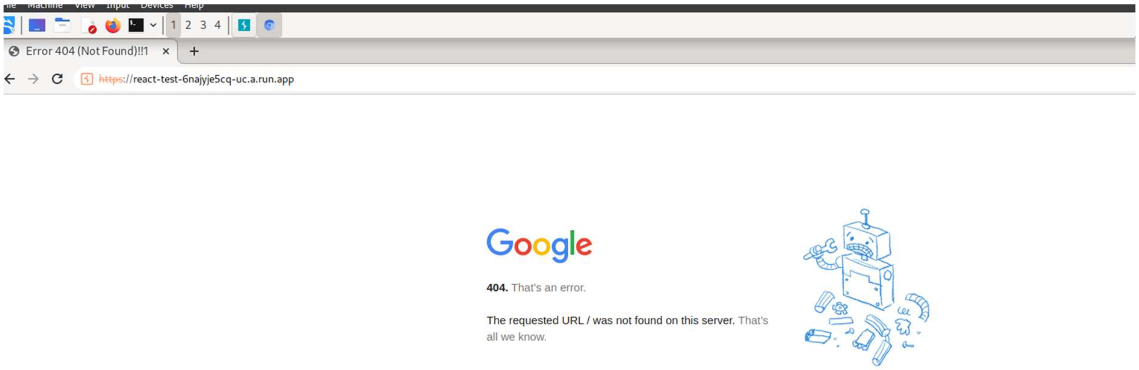
```
GET / HTTP/2
Host: www.google.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response:

```
HTTP/2 404 Not Found
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1561
Date: Sat, 04 May 2024 05:07:17 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>
    Error 404 (Not Found)!!1
  </title>
  <style>
    *{
      margin:0;
      padding:0
    }
    html,code{
      font:15px/22pxarial,sans-serif
    }
    html{
      background:#fff;
      color:#222;
```

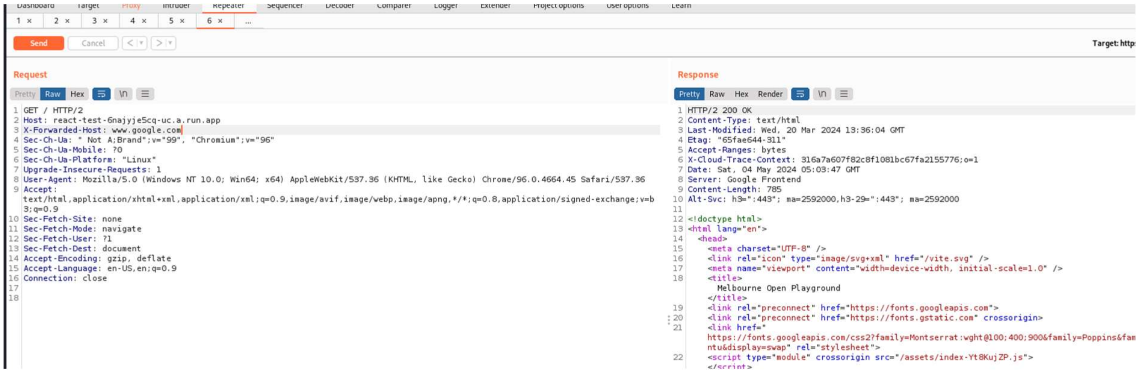
Step 2: 404 message appeared. It did not redirect and the attack was unsuccessful.


File Machine View Input Devices Help
1 2 3 4
Error 404 (Not Found)!!1
https://react-test-6najyje5cq-uc.a.run.app
Google

404. That's an error.

The requested URL / was not found on this server. That's all we know.

Step 3: Updated the X-Forwarded-Host header to www.google.com.


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: http
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

Request:

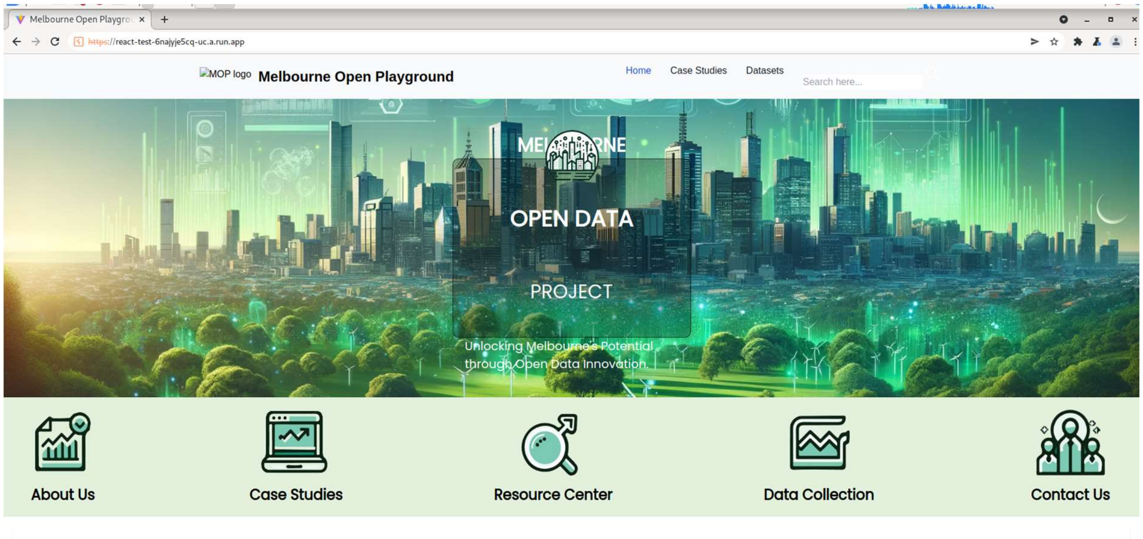
```
GET / HTTP/2
Host: react-test-6najyje5cq-uc.a.run.app
X-Forwarded-Host: www.google.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response:

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Wed, 20 Mar 2024 13:36:04 GMT
Etag: "65fae644-311"
Accept-Ranges: bytes
X-Cloud-Trace-Context: 316a7a607f82c8f1081bc67fa2155776;o=1
Date: Sat, 04 May 2024 05:03:47 GMT
Server: Google Frontend
Content-Length: 785
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!doctype html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml" href="/vite.svg" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>
      Melbourne Open Playground
    </title>
    <link rel="preconnect" href="https://fonts.googleapis.com">
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
    <link href="
    https://fonts.googleapis.com/css2?family=Montserrat:wght@100;400;900&family=Poppins&fam
    ntu&display=swap" rel="stylesheet">
    <script type="module" crossorigin src="/assets/index-Yt8KujZP.js">
    </script>
```

Step 4: It did not redirect and the attack was unsuccessful.


Melbourne Open Playgro
https://react-test-6najyje5cq-uc.a.run.app
MOP logo
Melbourne Open Playground
Home
Case Studies
Datasets
Search here...
MELBOURNE
OPEN DATA
PROJECT
Unlocking Melbourne's Potential through Open Data Innovation.
About Us
Case Studies
Resource Center
Data Collection
Contact Us