CYMOTIVE TECHNOLOGIES

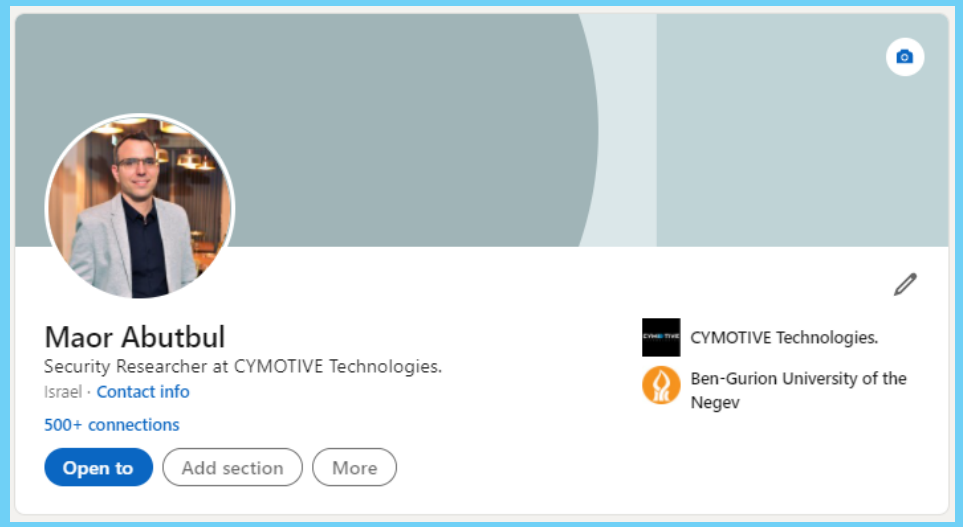
Web Security Workshop
מגשימים 2021

Maor Abutbul

24.11.2021

#whoami

מי אני



- רקע מקצועי
- לימודים

- Gamer
- Father
- Researcher
- Master ☺ (of science)

- חוקר אבטחה - סיימוטיב טכנולוגיות

https://il.linkedin.com/in/maor-abutbul

Agenda - תוכנית

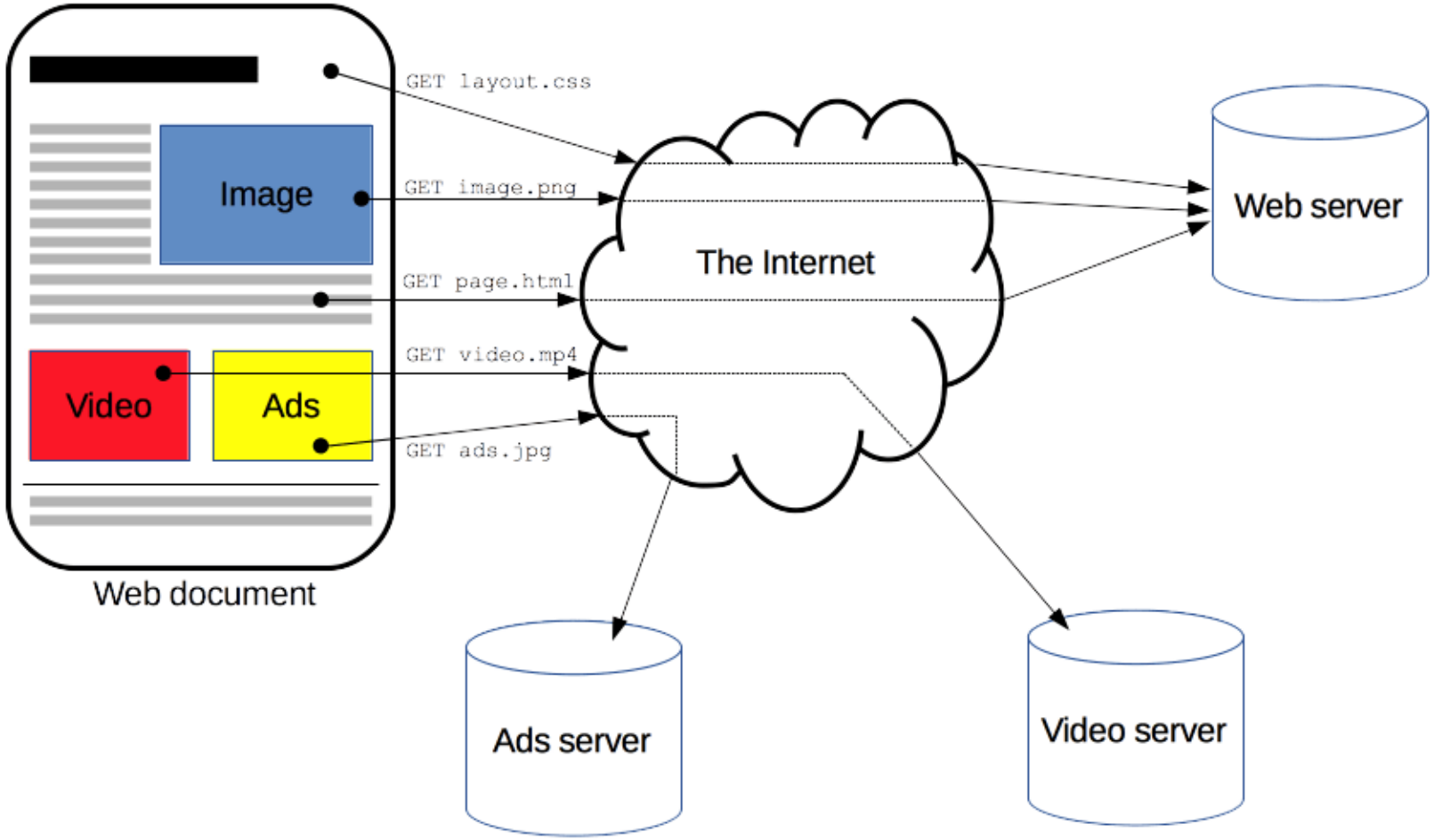
- חזרה רקע תיאורטי אבטחת מערכות ווב (בזריזות)
- Containers and Docker
- כלי פיתוח ומחקר (חזרה קצרה על Burp)
- היכרות עם חולשה בסיסית
- הדגמה +תרגול
  - הרצת מקומית של מכונה עם חולשה ידועה

סטטוס התקנה ?

פרוטוקול - HTTP

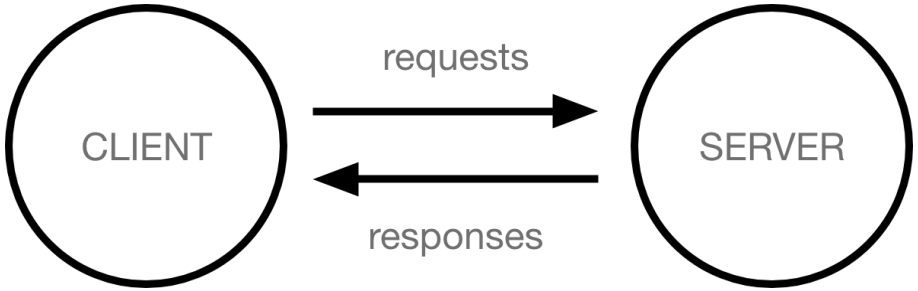
Hypertext Transfer Protocol (HTTP)

פרוטוקול HTTP



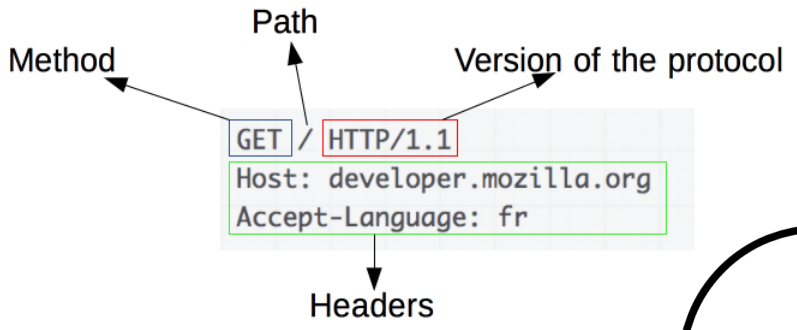
פרוטוקול HTTP - מודל שרת לקוח והודעות

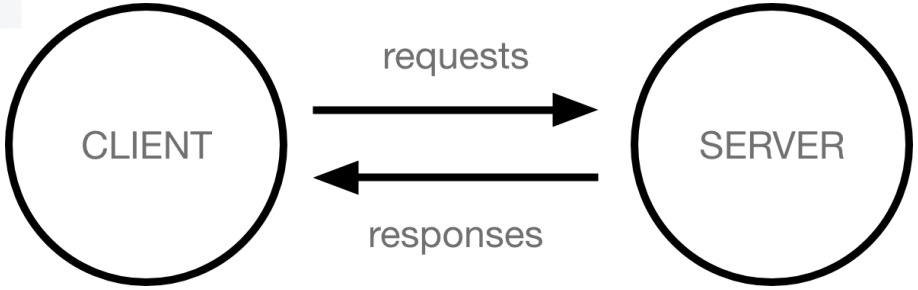
- מודל שרת-לקוח
- Stateless, but not Sessionless
- הודעות - בקשה תשובה \ תגובה

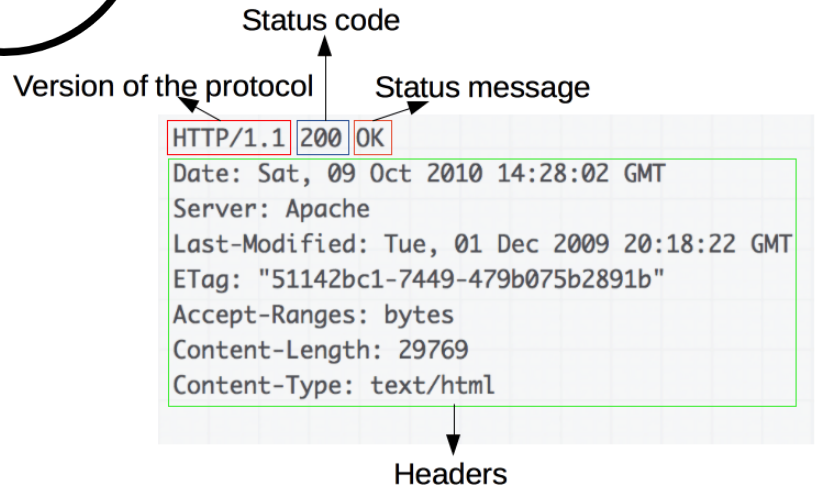


- https://developer.mozilla.org/en-US/docs/Web/HTTP/

פרוטוקול HTTP - מודל שרת לקוח והודעות



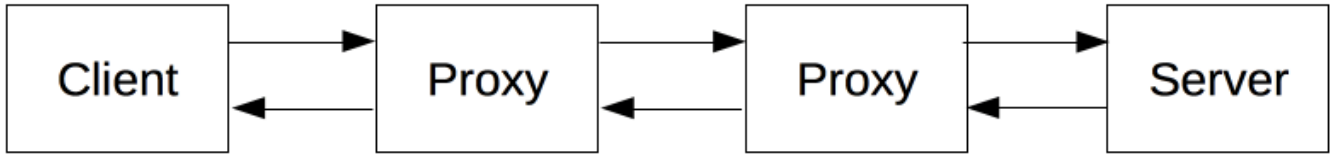




https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

רכיבי תקשורת ואבטחה - עבור פרוטוקול HTTP

- רכיבי תקשורת (ואבטחה) ללא התערבות ב-HTTP
  - Firewall
  - נתב (Router)
  - Load Balancer
  - ועוד



- רכיבים המנתחים תעבורת HTTP
  - רכיב פרוקסי (Proxy)
  - Load Balancer
  - Web Cache
  - WAF – Web Application Firewall
- שרת Web

- https://developer.mozilla.org/en-US/docs/Web/HTTP/

רגע לפני - אחריות – חוק המחשבים

- יש חוק בישראל
  - חוק המחשבים, התשנ"ה–1995
    - https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%94%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D
  - הסבר מתוך קורס של המרכז לחינוך סייבר
    - https://s3.eu-west-1.amazonaws.com/data.cyber.org.il/virtual_courses/websec/computer_law/%D7%97%D7%95%D7%A7%20%D7%94%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D.pdf
  - ובכל מקרה
    - חובה להשיג אישור (בכתב!) של בעל הנכס.
    - לשים לב שלא חורגים מהנכסים שהוגדרו לנו.
      - לדוגמא:
      - שרתים משותפים.
      - שירותי אחסון.

Containers and Docker

Background - רקע

Docker

Some Docker vocabulary

Containers	Images
How you **run** your application	How you **store** your application

Docker Image

The basis of a Docker container. Represents a full application

Docker Container

The standard unit in which the application service resides and executes

Docker Engine

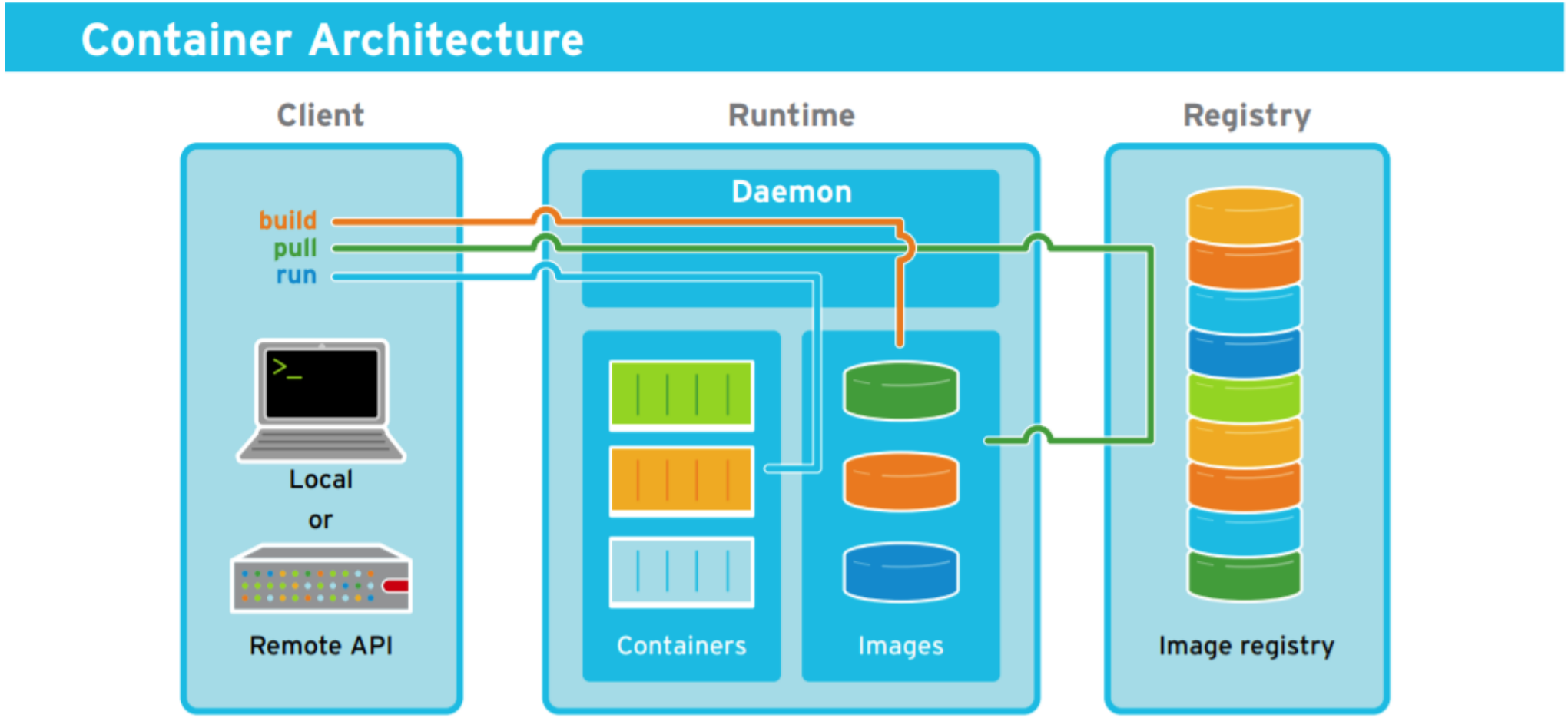
Creates, ships and runs Docker containers deployable on a physical or virtual, host locally, in a datacenter or cloud service provider

Registry Service (Docker Hub or Docker Trusted Registry)

Cloud or server based storage and distribution service for your images

- Source: https://dockerlabs.collabnix.com/docker/Docker_VIT_Intro/Docker_VIT_Intro.html

Containers Architecture



- Source Red Hat

Docker

- DockerHub

- Docker CLI
  - docker pull httpd
  - docker images
  - docker ps
  - docker run -d --name docker-apache -p 80:80 -d httpd
  - docker stop <container_id_or_name>
  - docker exec -it <container_id_or_name> echo "I'm inside the container!“
  - https://dockerlabs.collabnix.com/docker/cheatsheet/

- Dockerfile
  - docker build

Install docker

- # Set up the repository
  - sudo apt-get update
  - sudo apt-get install ca-certificates curl gnupg lsb-release
  - curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
  - echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
- # Install Docker Engine
  - sudo apt-get update
  - sudo apt-get install docker-ce docker-ce-cli containerd.io
- # Verify that Docker Engine is installed correctly by running the hello-world image.
  - sudo groupadd docker
  - sudo usermod -aG docker $USER
    - Logoff !
  - docker run hello-world

זמן להתקין

End Goal: docker run hello-world

Docker Images for Web Security Practice

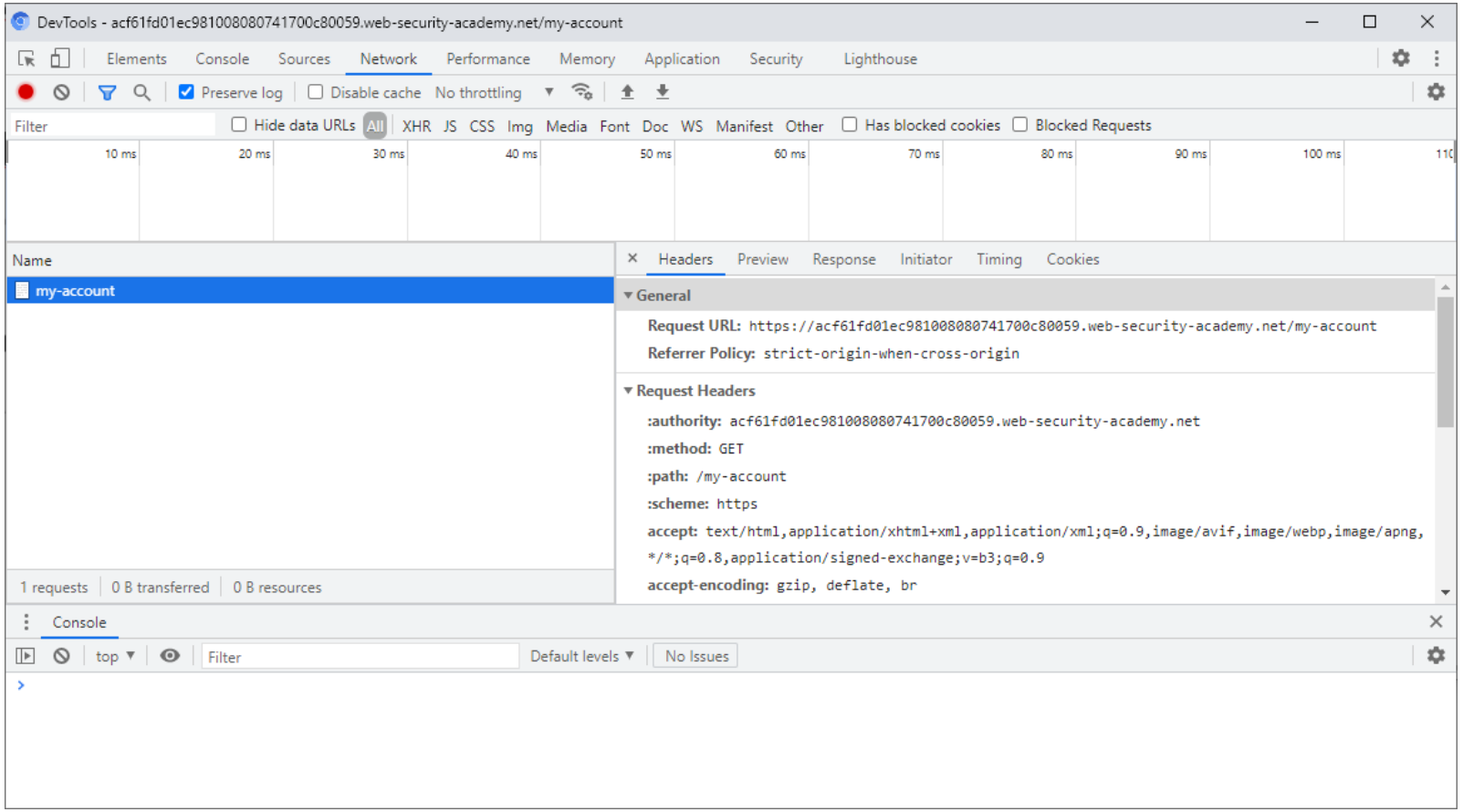
- https://hub.docker.com/r/webgoat/goatandwolf
  - Run
    - docker run -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 webgoat/goatandwolf
  - Browse to http://127.0.0.1:8080/WebGoat

- https://hub.docker.com/r/bkimminich/juice-shop#docker-container
  - Run
    - docker pull bkimminich/juice-shop
  - Run
    - docker run --rm -p 3000:3000 bkimminich/juice-shop
  - Browse to http://localhost:3000

כלי פיתוח ומחקר (חזרה) – Tools

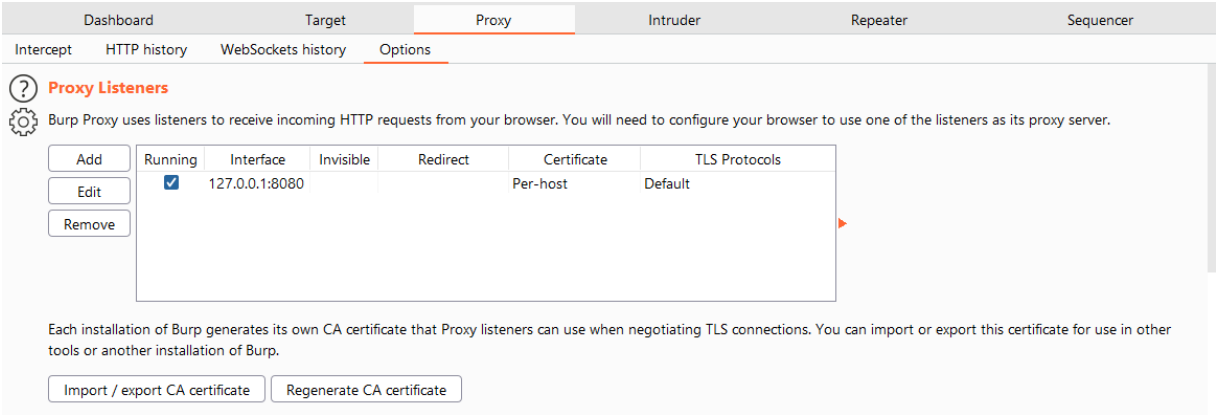
DevTools

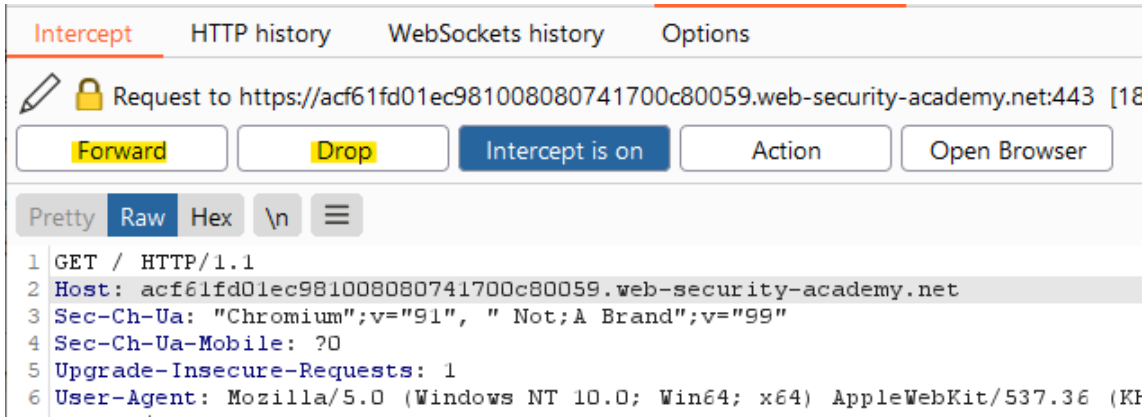
- Elements
- Console
  - Page interaction
- Sources
  - Debug
- Network
  - Copy As
  - (fetch + console)



Tools - Burp Suite (Community)

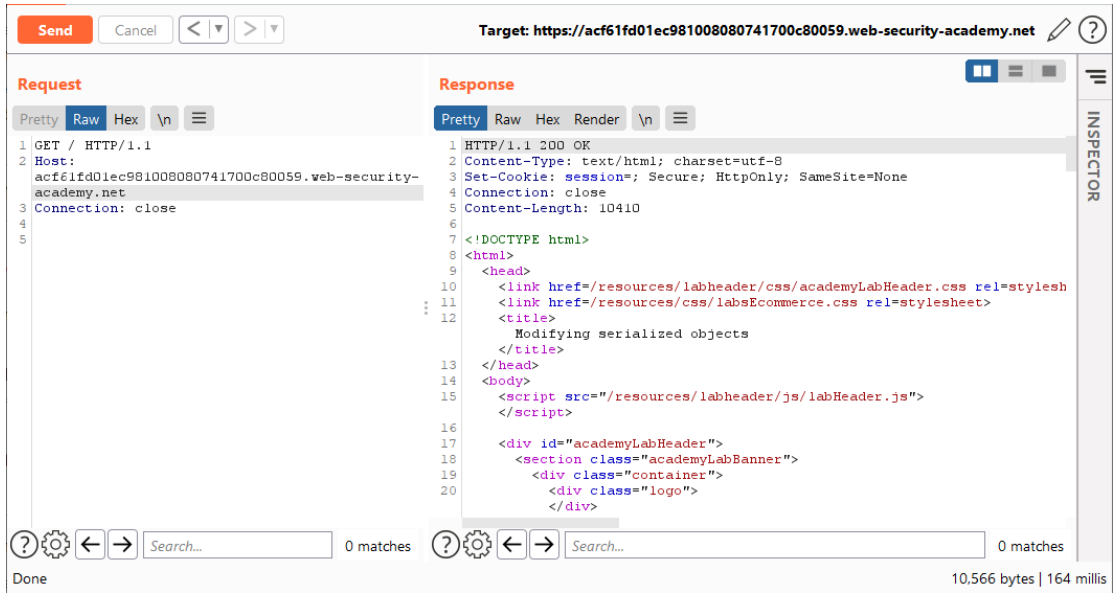
- Dashboard
- Target
- Proxy
  - Intercept
  - HTTP History
  - Options

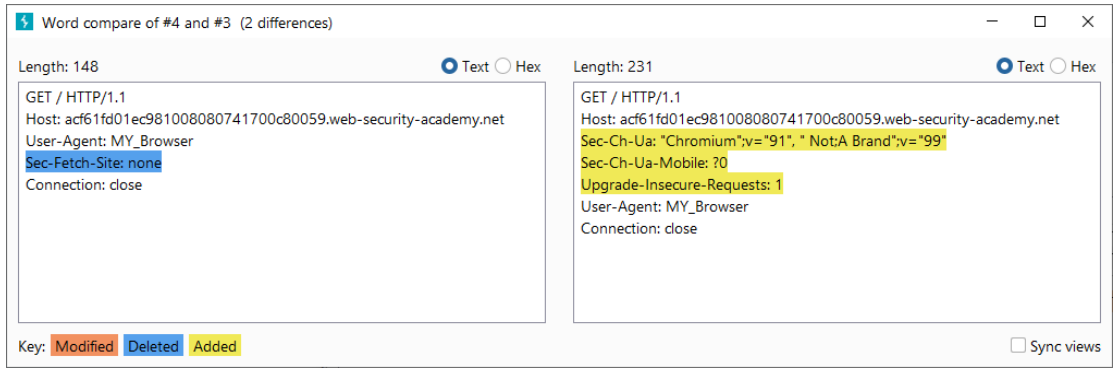




Burp Suite Cont’

- Repeater (Ctrl + R)
  - עריכה ושליחה ידנית
- Intruder (Ctrl + I)
  - הגדרת "משתנים" וערכים (Payloads) לשליחה אוטומטית
- Decoder
  - פענוח קידודים
- Comparer
  - השוואה בין בקשות
- Extender
  - הורדת וניהול "הרחבות"





Web Vulnerability Self Study + Lab Time

Directory Traversal Vulnerability

- https://portswigger.net/web-security/file-path-traversal
  - חולשה המאפשרת קריאת קבצים "אקראיים" מהשרת (ממערכת הקבצים של השרת)
  - ייתכן ויתאפשר לנו לקרוא קבצים רגישים כמו קבצי סיסמאות או קוד המקור של האפליקציה.
  - במקרים מסוימים תוקף יוכל לכתוב קבצים לשרת
    - וזה בתורו יאפשר לשנות מידע או התנהגות של אפליקציה ואף להשתלט לגמרי על השרת

- Lab
  - https://portswigger.net/web-security/file-path-traversal/lab-simple

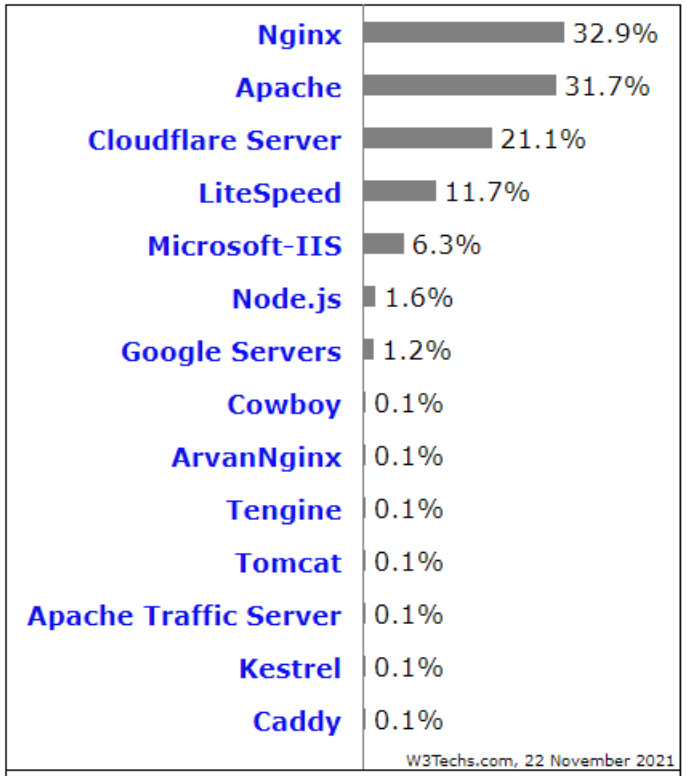
Self Study + Lab Time

Goal: Finish Lab

Apache (httpd) Web Server

Apache (httpd) Web Server

- https://httpd.apache.org/
- Open-source HTTP server.
- To provide a secure, efficient and extensible server that provides HTTP services
- The Apache HTTP Server ("httpd") was launched in 1995.



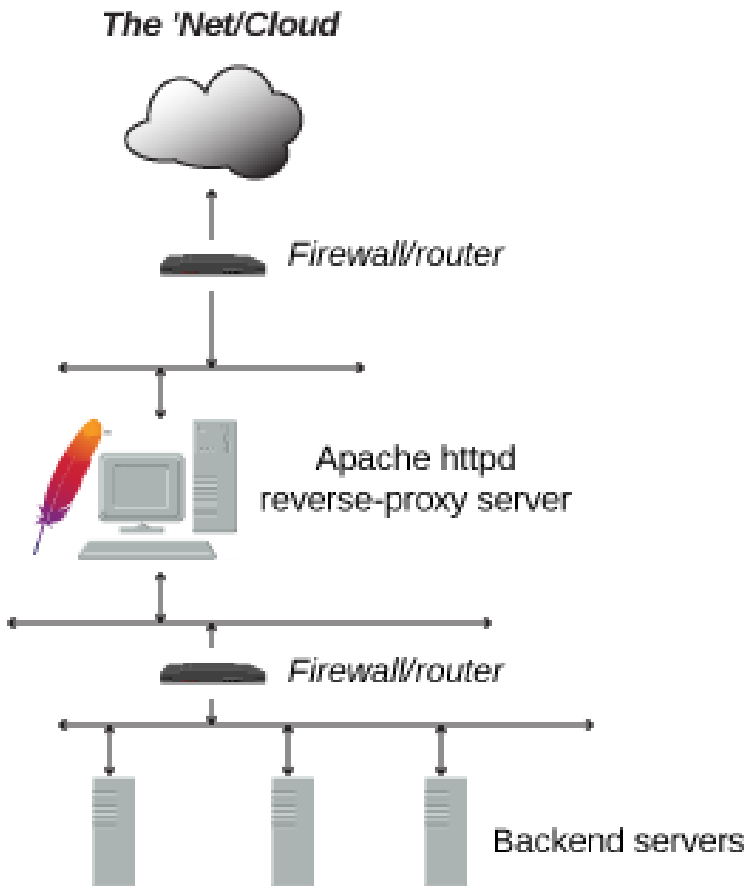
Percentages of websites using various web servers
Note: a website may use more than one web server

Apache (httpd) Web Server

- Getting Started
  - http://httpd.apache.org/docs/2.4/getting-started.html
- Config Files
  - http://httpd.apache.org/docs/current/configuring.html

- Apache on Docker
  - https://hub.docker.com/_/httpd
  - docker run -it --name my-apache-app -p 8080:80 -v "$PWD":/usr/local/apache2/htdocs/ httpd:2.4

- Example module: Reverse Proxy
  - https://httpd.apache.org/docs/2.4/images/reverse-proxy-arch.png



Real World CVE

Real World CVE + Practice

- https://cve.mitre.org/
- https://www.cve.org/

- git clone https://github.com/m2a2/magshimim_workshop_2021

Real World CVE

Goal: Run the Container, explore using Burp, find the vulnerability

Apache CVEs References

- https://blog.qualys.com/vulnerabilities-threat-research/2021/10/27/apache-http-server-path-traversal-remote-code-execution-cve-2021-41773-cve-2021-42013

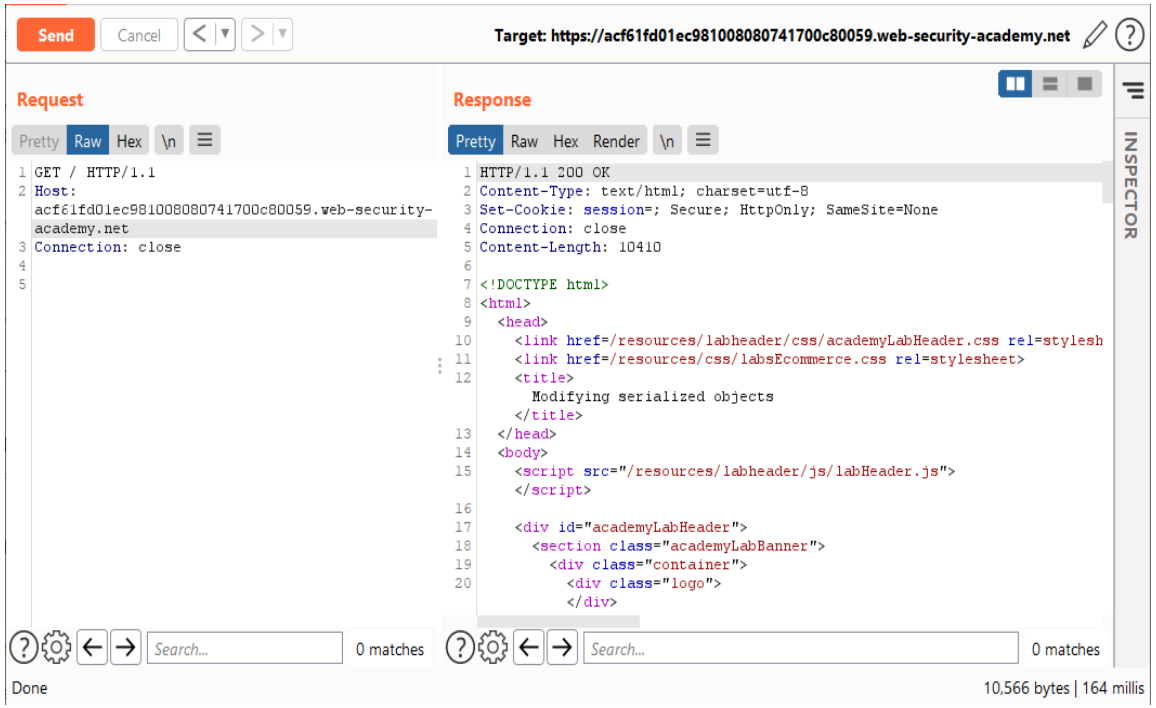
- https://appcheck-ng.com/apache-path-traversal-vulnerability-cve-2021-41773/#

Vulnerable Docker Images

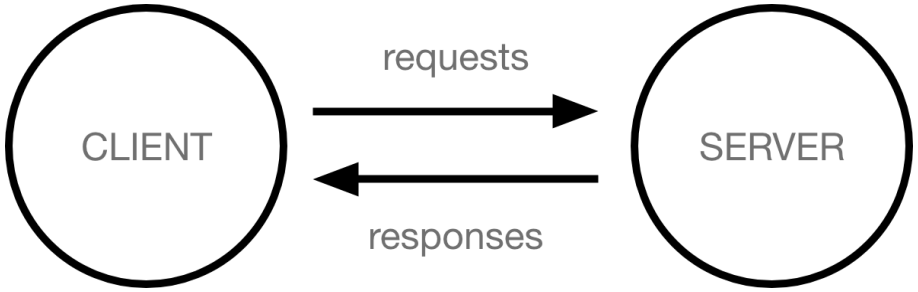
- https://github.com/vulhub/vulhub

Summary

סיכום



- חזרה רקע תיאורטי אבטחת מערכות ווב
  - Containers and Docker
    - הרצנו Image לתרגול מקומי
- כלי פיתוח ומחקר (חזרה קצרה על Burp)
- Directory traversal Vulnerability
- תרגול + Real World CVE



Questions ?

Thank You!

Contact At:
https://il.linkedin.com/in/maor-abutbul

CYMOTIVE
TECHNOLOGIES