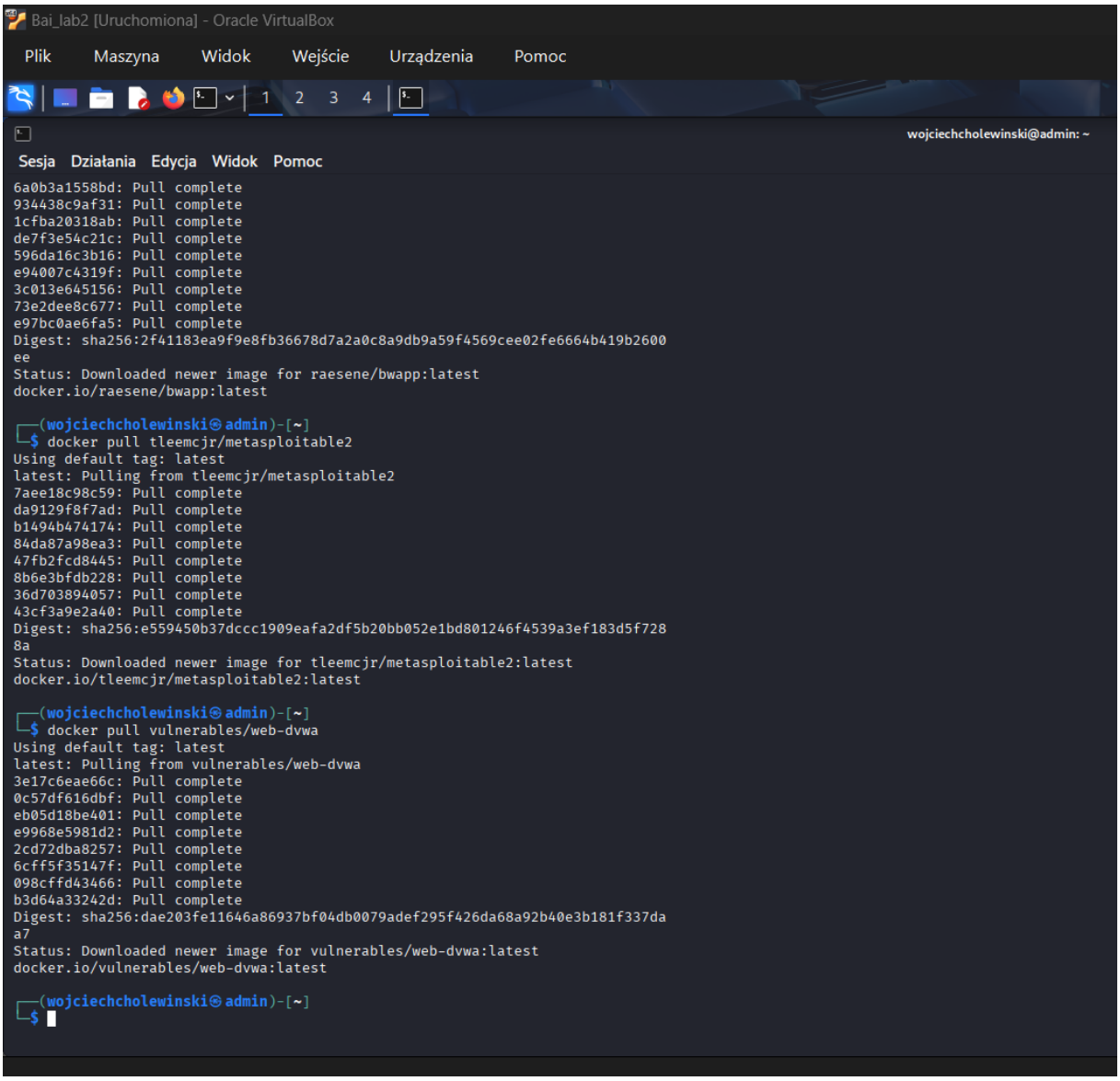
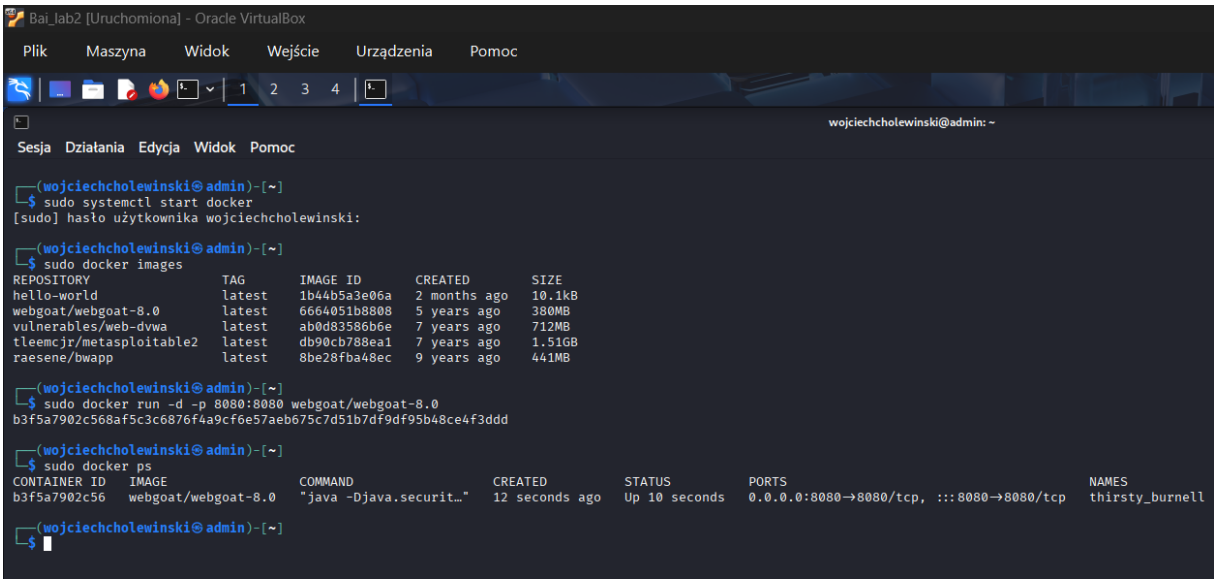
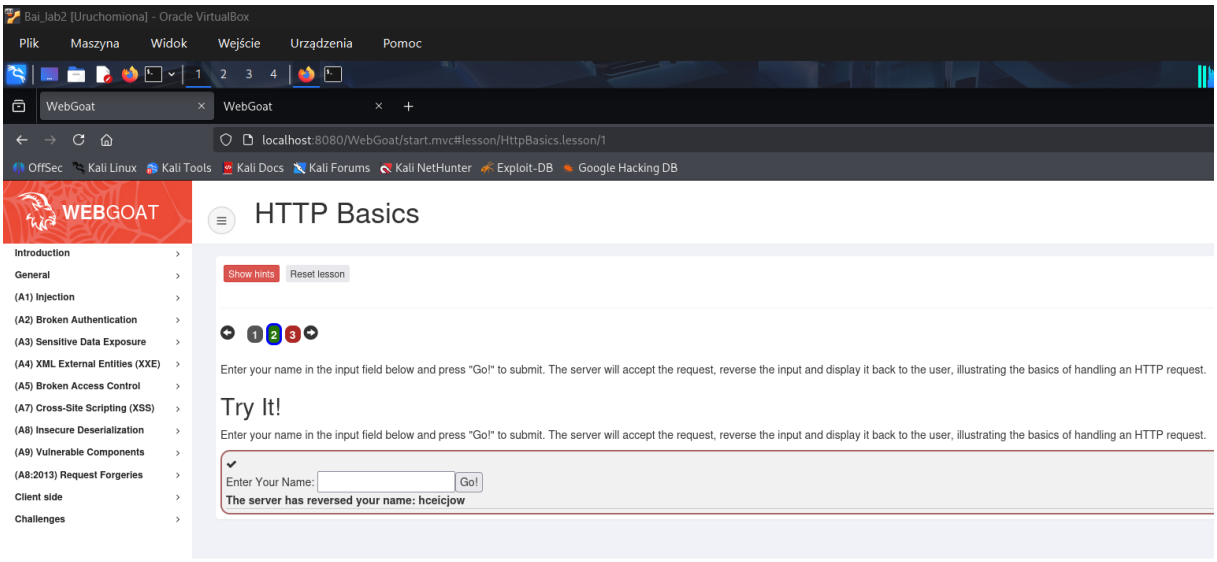
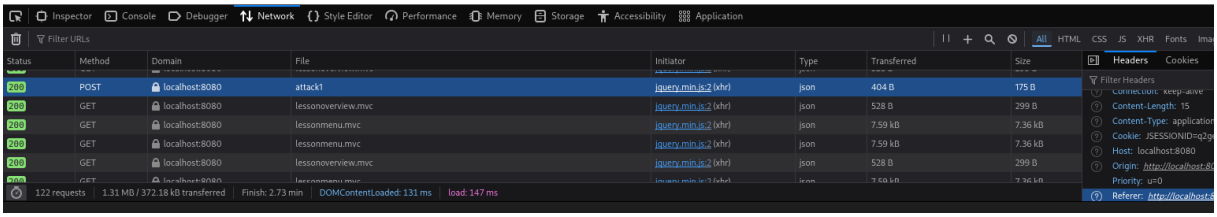

Bai_lab2 [Uruchomiona] - Oracle VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
1 2 3 4
wojciechcholewinski@admin: ~
Sesja Działania Edycja Widok Pomoc
6a0b3a1558bd: Pull complete
934438c9af31: Pull complete
1cfba20318ab: Pull complete
de7f3e54c21c: Pull complete
596da16c3b16: Pull complete
e94007c4319f: Pull complete
3c013e645156: Pull complete
73e2dee8c677: Pull complete
e97bc0ae6fa5: Pull complete
Digest: sha256:2f41183ea9f9e8fb36678d7a2a0c8a9db9a59f4569cee02fe6664b419b2600
ee
Status: Downloaded newer image for raesene/bwapp:latest
docker.io/raesene/bwapp:latest
(wojciechcholewinski㉿admin)-[~]
$ docker pull tleemcjr/metasploitable2
Using default tag: latest
latest: Pulling from tleemcjr/metasploitable2
7aee18c98c59: Pull complete
da9129f8f7ad: Pull complete
b1494b474174: Pull complete
84da87a98ea3: Pull complete
47fb2fcd8445: Pull complete
8b6e3bfdb228: Pull complete
36d703894057: Pull complete
43cf3a9e2a40: Pull complete
Digest: sha256:e559450b37dccc1909eafa2df5b20bb052e1bd801246f4539a3ef183d5f728
8a
Status: Downloaded newer image for tleemcjr/metasploitable2:latest
docker.io/tleemcjr/metasploitable2:latest
(wojciechcholewinski㉿admin)-[~]
$ docker pull vulnerables/web-dvwa
Using default tag: latest
latest: Pulling from vulnerables/web-dvwa
3e17c6eae66c: Pull complete
0c57df616dbf: Pull complete
eb05d18be401: Pull complete
e9968e5981d2: Pull complete
2cd72dba8257: Pull complete
6cff5f35147f: Pull complete
098cffd43466: Pull complete
b3d64a33242d: Pull complete
Digest: sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337da
a7
Status: Downloaded newer image for vulnerables/web-dvwa:latest
docker.io/vulnerables/web-dvwa:latest
(wojciechcholewinski㉿admin)-[~]
$


Bai_lab2 [Uruchomiona] - Oracle VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
1 2 3 4
wojciechcholewinski@admin: ~
Sesja Działania Edycja Widok Pomoc
(wojciechcholewinski㉿admin)-[~]
$ sudo systemctl start docker
[sudo] hasło użytkownika wojciechcholewinski:
(wojciechcholewinski㉿admin)-[~]
$ sudo docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
hello-world latest 1b44b5a3e06a 2 months ago 10.1kB
webgoat/webgoat-8.0 latest 6664051b8808 5 years ago 380MB
vulnerables/web-dvwa latest ab0d83586b6e 7 years ago 712MB
tleemcjr/metasploitable2 latest db90cb788ea1 7 years ago 1.51GB
raesene/bwapp latest 8be28fba48ec 9 years ago 441MB
(wojciechcholewinski㉿admin)-[~]
$ sudo docker run -d -p 8080:8080 webgoat/webgoat-8.0
b3f5a7902c568af5c3c6876f4a9cf6e57aeb675c7d51b7df9df95b48ce4f3ddd
(wojciechcholewinski㉿admin)-[~]
$ sudo docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
b3f5a7902c56 webgoat/webgoat-8.0 "java -Djava.securit…" 12 seconds ago Up 10 seconds 0.0.0.0:8080→8080/tcp, :::8080→8080/tcp thirsty_burnell
(wojciechcholewinski㉿admin)-[~]
$


Bai_lab2 [Uruchomiona] - Oracle VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
WebGoat
WebGoat
localhost:8080/WebGoat/start.mvc#lesson/HttpBasics.lesson/1
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
WEBGOAT
HTTP Basics
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Show hints
Reset lesson
Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.
Try It!
Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.
Enter Your Name:
Go!
The server has reversed your name: hceicjow


Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts
Status Method Domain File Initiator Type Transferred Size
200 POST localhost:8080 attack1 jquery.min.js:2 (xhr) json 404 B 175 B
200 GET localhost:8080 lessonoverview.mvc jquery.min.js:2 (xhr) json 528 B 299 B
200 GET localhost:8080 lessonmenu.mvc jquery.min.js:2 (xhr) json 7.59 kB 7.36 kB
200 GET localhost:8080 lessonmenu.mvc jquery.min.js:2 (xhr) json 7.59 kB 7.36 kB
200 GET localhost:8080 lessonoverview.mvc jquery.min.js:2 (xhr) json 528 B 299 B
122 requests 1.31 MB / 372.18 kB transferred Finish: 2.73 min DOMContentLoaded: 131 ms load: 147 ms
Headers Cookies
Filter Headers
Content-Length: 15
Content-Type:
Cookie: JSESSIONID=
Host: localhost:8080
Origin:
Priority: u=0
Referer: