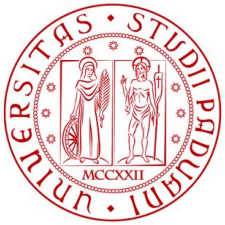
CyberSecurity: Principle and Practice

BSc Degree in Computer Science
2024-2025

Lesson 7: Introduction to Web Vulnerabilities

Prof. Mauro Conti
Department of Mathematics
University of Padua
conti@math.unipd.it
http://www.math.unipd.it/~conti/

Teaching Assistants
Tommaso Bianchi
tommaso.bianchi@phd.unipd.it
Riccardo Preatoni
riccardo.preatoni@studenti.unipd.it



UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

Introduction

Introduction

- What does hacking mean?
- What is the goal of an attacker?
- Why is doing it?
- Who can be an hacker?

Stereotypes

“A computer hacker is any skilled computer expert who uses his technical knowledge to overcome a problem.”

_cit Wikipedia

Stereotypes

The attacker is **often** seen as... “super skilled”

...is it really/always the case?

Stereotypes

The attacker is **often** seen as... “super skilled”

...is it really/always the case?

- probably yes, if he attacks “super secure” systems (e.g., NASA)

Confirmed: **NASA** Has Been **Hacked**
Forbes - Jun 20, 2019
The U.S. National Aeronautics and Space Administration (**NASA**) this week confirmed that its Jet Propulsion Laboratory (JPL) has been **hacked**.

NASA hacked because of unauthorized Raspberry Pi ...
ZDNet - Jun 21, 2019

View all

Stereotypes

The attacker is **often** seen as... “super skilled”

...is it really/always the case?

- **probably yes**, if he attacks “super secure” systems (e.g., NASA)
- **probably no**, if he attacks “normal” systems

Aveva violato la piattaforma "**Rousseau**" del Movimento 5 ...
PadovaOggi - Feb 6, 2018
L'**hacker**, intervistato a suo tempo anche **da** alcune testate dopo l'incursione, ... E proprio Matematica studierebbe all'Università di **Padova**.
Rousseau, preso l'**hacker**. Cos'è e come funziona la ...
In-Depth - Quotidiano.net - Feb 6, 2018

Stereotypes

- A **fundamental** consideration is:
  - who am I (the hacker) fighting against?

- The **defender**, the one that developed a target system:
  - is usually a **normal** guy, like you
    - maybe with more experience
  - might not be a security expert

- What **often** happen is that who develop a system do not focus on its security, but has a priority on:
  - **functionality**: the system does what it has to do
  - **performance**: the system is efficient

Sad but true …

When security aspects are ***secondary*** in a system…
troubles start

you

vs

target

How can we proceed?

How can we proceed?

- Gather **as much info as possible** about the target
  - e.g., OS, program language, type of services, protocols …the more we now about the target, the better!

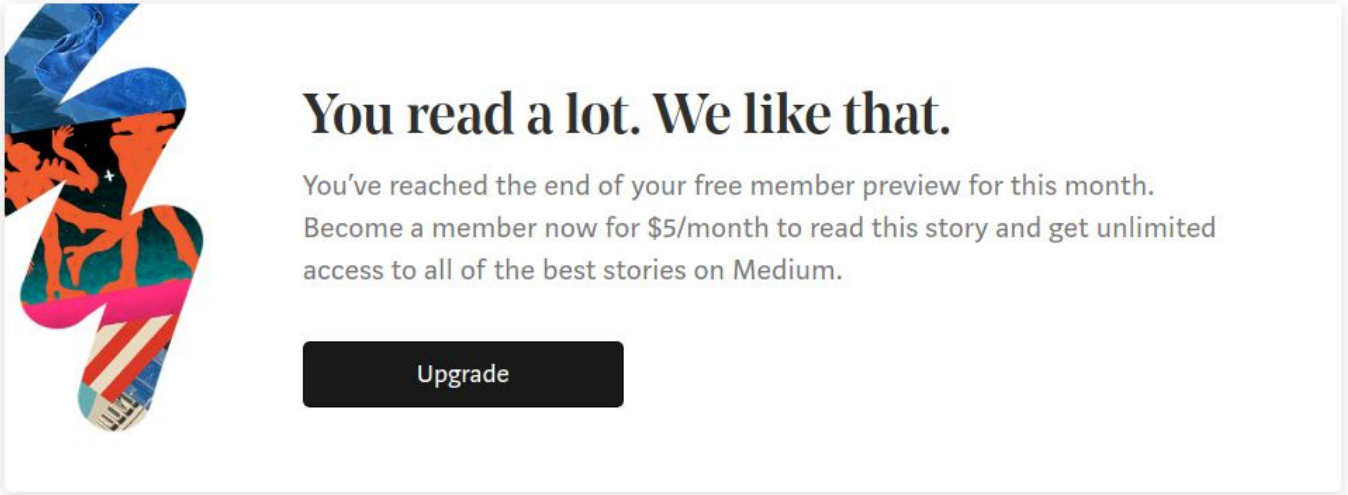
- **for each component** we can find (on the web), the **vulnerabilities**
  - search on the web: this is not an exam; the victims won't complain this leak of "fairness" -- hacking is not a sport
  - e.g., for a programming language there are some common and well known vulnerabilities
  - if you know what you want, you can easily understand if these vulnerabilities are useful

- Look online for **tools** that can help you

Hacking in practice

Example 1

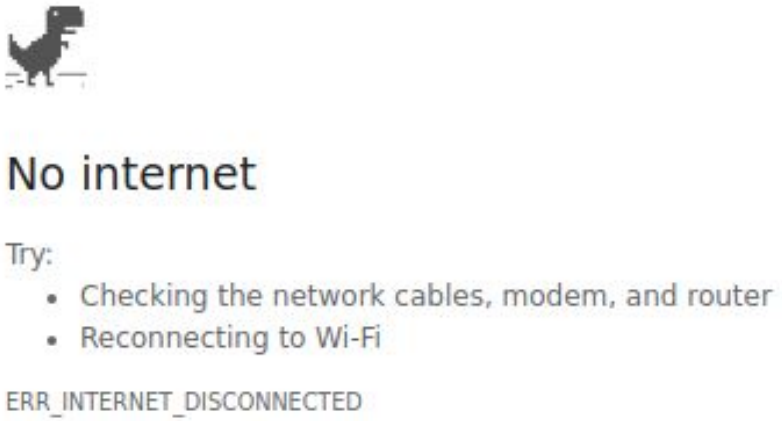
- **Target**: Toward Data Science
- **System Type**: scientific journal, web app
- **Problem**: After reading for free few articles, the system ask you to upgrade your account
- **Attacker Goal**: infinite free access to the contents



Hacking in practice

Example 2

- **Target:** T-Rex Game (chrome://dino/)
- **System Type: web game**
- **Problem:** the game is way too difficult
- **Attacker Goal**: show to my friends how good am I in this game



Hacking in practice

Example 2

- **Target:** T-Rex Game (chrome://dino/)
- **System Type: web game**
- **Problem:** the game is way too difficult
- **Attacker Goal**: show to my friends how good am I in this game

Exercises

- Today exercises focus on the *inspect* section of your browser
- Let's play a bit

Exercises

- Exercise 1:
  - Javascript is checking the login password off of an ajax call, The verification is being done on the client side. Making a direct call to the ajax page will return the expected password
- Exercise 2:
  - You control the browser
- Exercise three
  - You control the browser

Questions? Feedback? Suggestions?