

WORKSHOP 1 OF 3 • FOUNDATIONS

The Attacker's Mindset

The basics, and everything you'll need for Tuesday and Thursday.

Mohamed Medjahdi, Cybersecurity Engineer

7-77 Digital Skills Programme • Algérie Télécom SkillsCenter, Saïda

Three sessions, one journey.

TODAY

Sunday · theory

Understand

The basics, the words, and how attacks work.
Today you just listen and absorb.

Tuesday · hands-on

Do it

Bring a laptop. We set up a safe lab and find a real vulnerability together.

Thursday · challenge

Compete

A friendly challenge. Everything in it, you will already have seen this week.

Everything you use runs on a system.

Your phone, your bank, social media, this centre. **Cybersecurity is the job of protecting all of it** from people who try to break in or steal. It's one of the biggest and best paid fields in the world today.

The field has two teams.



THE DEFENDERS

Blue Team

Watches, detects, and stops attacks. The guard on duty.

example: SOC analyst



THE ATTACKERS, LEGALLY

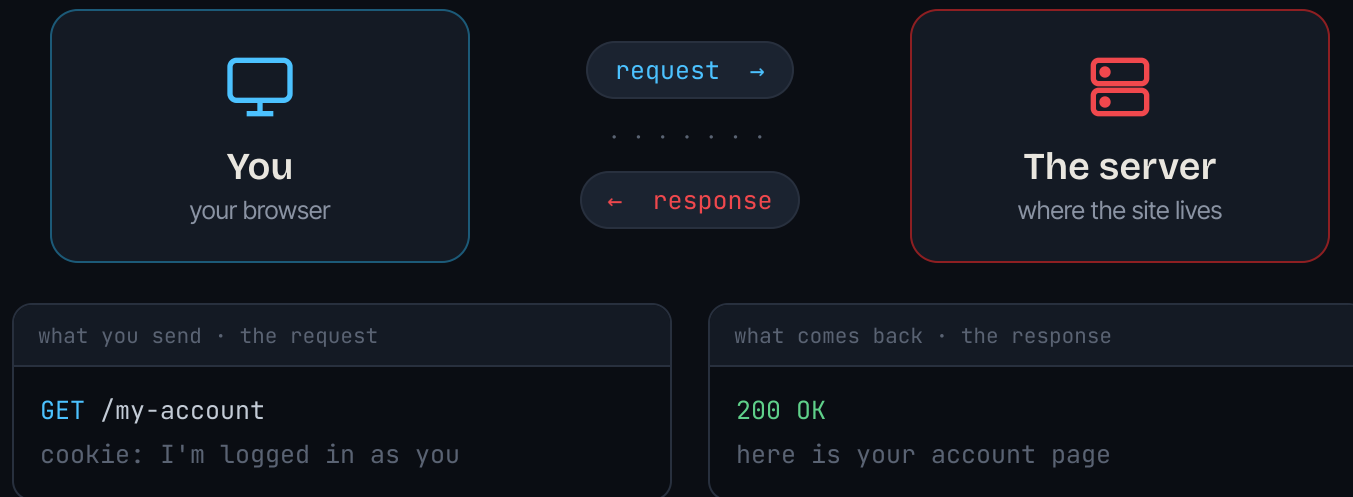
Red Team

Breaks in on purpose, with permission, to find the holes first.

= offensive security = us

We learn the red side, because **you can't defend against what you don't understand.**

A website is a conversation: you ask, it answers.



Every click is a request. The server reads it and decides what to answer. **An attack is just a request the server didn't expect.**

Two words people always mix up.



AUTHENTICATION

Who are you?

Proving your identity, logging in with a password or a code. **Like showing your ID at the door.**



AUTHORIZATION

What are you allowed to do?

Your permissions once you're inside. **Like a ticket that decides which rooms you can enter.**

Many bugs come from broken authorization: you're logged in, but you can still reach someone else's data. (That's OWASP A01.)

The words you'll hear all week.

Vulnerability

A weakness, a mistake left in a system.

Exploit

The trick that abuses that weakness.

Payload

The thing you send to make it happen.

Reconnaissance

Looking around the target first.

Privilege escalation

Going from normal user to full control.

CVE

A public ID for a known vulnerability.

The OWASP Top 10: the weaknesses attackers hunt.

A01 Broken Access Control
reaching data that isn't yours

A03 **Injection**
untrusted input runs as code (this is XSS)

A05 Security Misconfiguration
unsafe settings or defaults

A07 Auth Failures
weak logins and sessions

A09 Logging Failures
attacks go unseen

A02 Cryptographic Failures
weak or missing encryption

A04 Insecure Design
the flaw is in the design itself

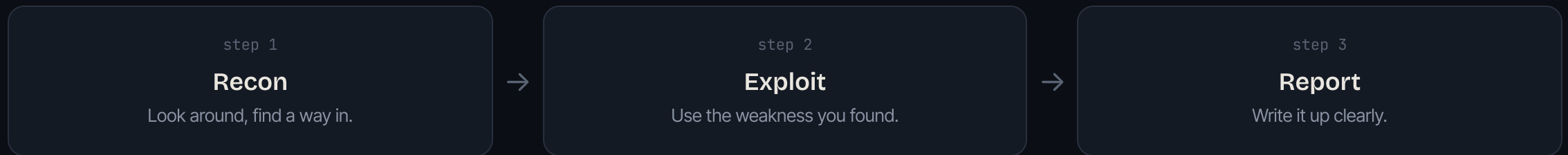
A06 Vulnerable Components
old libraries with known holes

A08 Data Integrity Failures
trusting unverified code

A10 Server-Side Request Forgery
the server tricked into requests

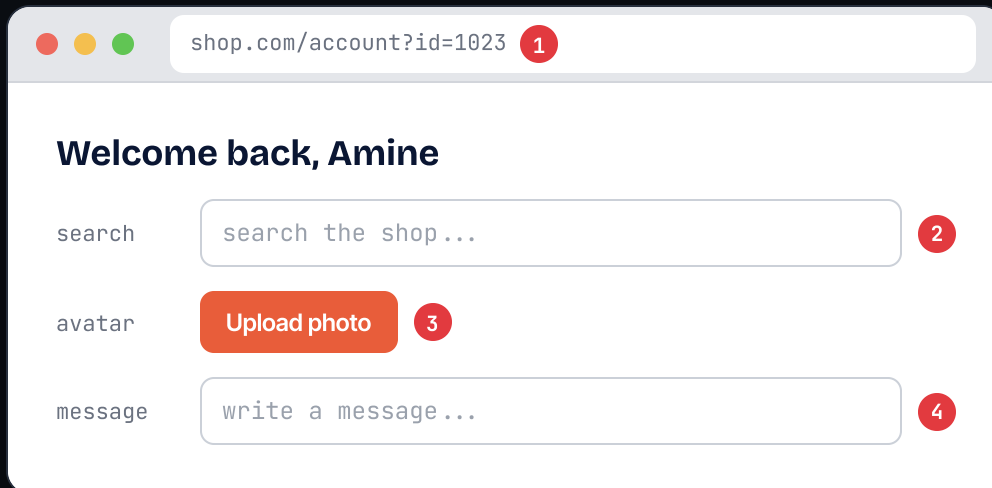
The one we'll do together is **A03: Injection**, better known as XSS.

Not random. The same three steps, every time.



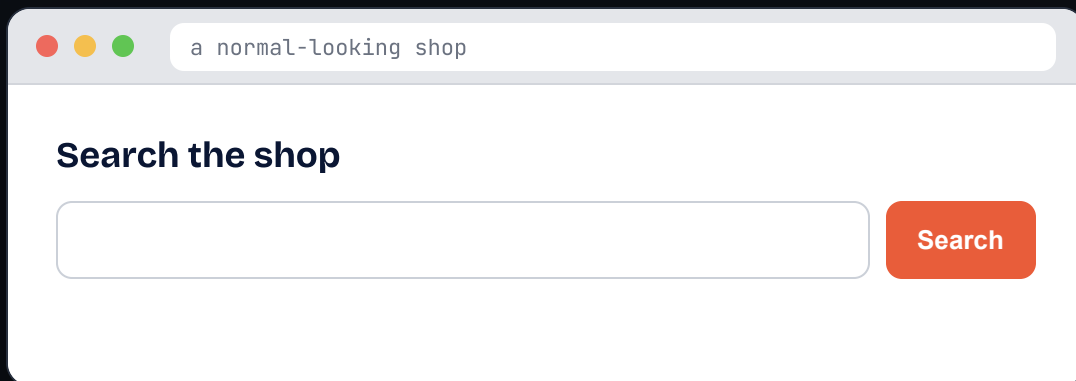
This is exactly what you'll do Tuesday, and compete with Thursday.

Look at any normal page and ask: where could this break?



- 1 The address bar. It says id=1023. What if I change it to 1024, do I see someone else's account?
- 2 The search box. What if I type code in here instead of a word?
- 3 The upload. What if I upload something that isn't really an image?
- 4 The message box. Where does my text show up, and does the site trust it?

That's the whole mindset: **don't just use the page, question it.**



A PREVIEW OF WHAT YOU'LL DO

This box was built to search. Watch what it does instead.

We put a little code in the search box, and the website **ran it**. That's a real attack, and on Tuesday you'll do it with your own hands.

The tools we'll use. Just know the names for now.

PRACTICE TARGET

OWASP Juice Shop

A safe website, made to be hacked legally.

WEB TOOL

Burp Suite

Lets you see and change what your browser sends.

FINDING TOOL

dirsearch

Finds hidden pages a site doesn't link to.

| All free. We install them together, or you set them up beforehand from the resources page.

What machine do you need? The one you already have.



WINDOWS

Use WSL

Install **WSL** (Windows Subsystem for Linux) to get Linux tools inside Windows. A VM also works.



MAC

Nothing to change

It runs everything you need already. Want Kali Linux? Just add a **VM**.



LINUX

You're set

Run the tools directly, or keep them tidy in a **VM** like Kali.

| A **VM** (VirtualBox, UTM, VMware) is just a second computer running safely inside your own. We'll keep it simple on Tuesday.

Finding a bug is half the job. Writing it up is the other half.

A company doesn't pay for a popup. It pays for a clear report: what you found, how to repeat it, why it matters, and how to fix it. On Thursday you'll write one, and AI can help you draft it fast.

XSS in search

HIGH

what

Search runs injected code

steps

1. open search 2. enter payload 3. it runs

impact

Attacker code runs in the victim's browser

fix

Clean the input before showing it

In this field, you get known by what you show.



SHOW YOUR CODE

GitHub

Put your scripts and tools there. Keep it alive.



EXPLAIN WHAT YOU DID

Write-ups

Solve something, then write how. A blog or your site.



GET SEEN

Build a name

A public record is what gets you hired or gets you clients.

Only ever test what you **own or are allowed to.**

Everything we do this week is on safe practice labs built for it. Attacking a real site without permission is a crime in Algeria (**Penal Code 394 bis**). The skill is the same, the only difference is permission, and that's the difference between a career and a criminal record.

You're ready. Two small things before Tuesday.

- 1 **Bring a laptop** on Tuesday if you can. No laptop? You'll pair up, nobody is left out.
 - 2 **Optional, but it helps:** set up the tools beforehand with the simple guide on the resources page.
- + Free slides and a full roadmap live at medjahdi.dev/src/roadmap-red.



[medjahdi.dev/src
/roadmap-red](https://medjahdi.dev/src/roadmap-red)

THAT'S THE FOUNDATIONS

Now you think like an **attacker.**

Questions? Ask me anything.