# Penetration Testing Practice Seminar

PA211 Advanced Topics of Cyber Security

October 18, 2022

**Ádám Ruman,** Jan Vykopal

# Agenda

- Response to the Exit Ticket from Last Week
- Solution of Homework 1
- Tools for Penetration Testing
- Penetration Testing Practice in a Team

# Exit tickets from last week

- **Q: How should we have approached this website vulnerability finding?**
- **A:** Optimally, choose a methodology (OWASP) and follow its steps. An excellent checklist excel table can be found here.

- **Q: Do pentesting tools entirely replace manual checks?**
- **A:** Some tools are just convenience wrappers; thus, I would count using them as manual checking. If you mean autonomous tools, those are not complete replacements. They can cover much ground, find common vulnerabilities, and exploit them – they are a great starting point.

# Solution of Homework 1

- Presented only in class.

# Goals of this seminar

- **Do the actual penetration testing**.
- **Share your findings** with your team members.
- **Store your findings** in a shared document.

# Penetration Testing Practice

**Start your sandbox using steps from the last week.**

**Update from last week:**

It seems that an older version of VirtualBox at nymfe was a root cause of instable virtual machines in sandboxes. VirtualBox has been updated to a newer version. Please report us any issues.

# Tools for Penetration Testing

# Tooling Overview

- Network Scanning Tools
- WEB
  - Recon
  - Enumeration and Crawling
  - Vulnerability Scanning
  - Proxying
- MSF

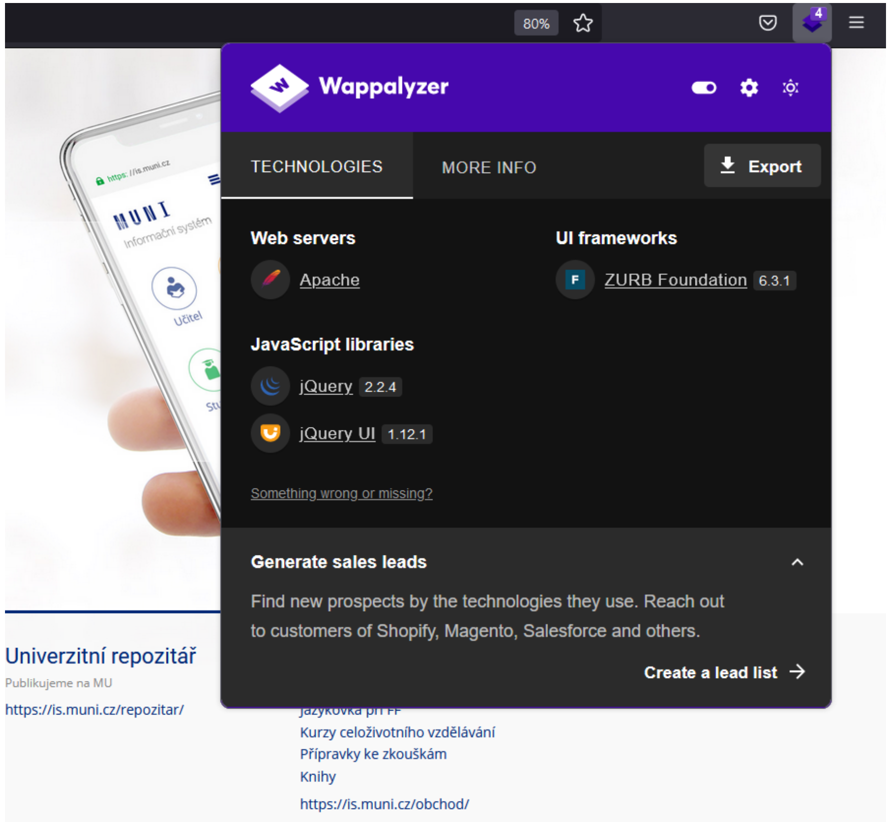
# Network Scanning Tools

- Nmap, RustScan
- To find open ports, identify services, and scan vulnerabilities.

# WEB – Browsers

- Browser developer tools are the most available and basic web penetration testing tools.

# WEB – Technology Reconnaissance



Web servers
Apache

UI frameworks
ZURB Foundation 6.3.1

JavaScript libraries
jQuery 2.2.4
jQuery UI 1.12.1

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

Univerzitní repozitář
Publikujeme na MU
https://is.muni.cz/repozitar/

Jazykovka při FF
Kurzy celoživotního vzdělávání
Přípravky ke zkouškám
Knihy
https://is.muni.cz/obchod/

– WhatWeb

– Wappalyzer

– For enumerating web technologies.

# WEB – Crawling and Enumeration

- Gather and follow linked pages.
  - OWASP ZAP
  - Burp Suite Pro

- Enumerating pages with brute-force or wordlists:
  - Fuff, dirb, Dirbuster, gobuster, Nikto

# WEB – Vulnerability Scanning

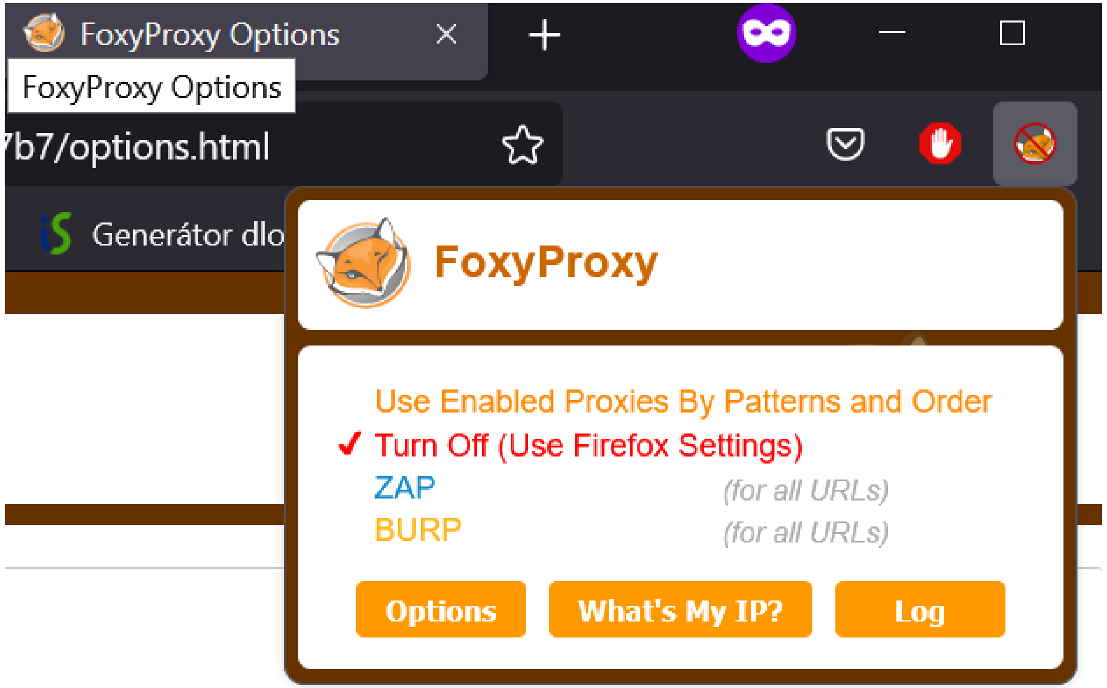
- Nikto
- Burp Suite Pro
- OWASP ZAP

# WEB – Proxies

- Intercepts web data between your browser and the website.
- Allows changing data and headers – thus bypassing browser and client-side limitations.
- Other convenience features – repeating, encoder/decoder, HTTP history registry.
- Scriptability.
- Burp (Community or Pro), OWASP ZAP

# WEB – Proxies: Convenience

- [FoxyProxy]
- Convenience tool that saves you the trouble of setting up and changing proxies.



Use Enabled Proxies By Patterns and Order
✓ Turn Off (Use Firefox Settings)
ZAP (for all URLs)
BURP (for all URLs)

# Metasploit Framework

- The “Swiss army knife” of penetration testing:
  - Vulnerability scanners.
  - Exploits.
  - Payloads.
  - Post-exploitation tools.

# Penetration Testing Practice

# Your task for today

- **Work in a team, and share what you find with other team members.**
- **Refresh the rules** of engagements and **scope** of the test (see last week).
- Next week: **Report** your results, including **homework**.

- From now on, we are here for **consultations** till the end of the seminar.
- Take a break any time you need.
- Feel free to leave when you are done.

# Scoping matters – real-life example

- Police Presidium hired 3rd party to run penetration testing on their systems.
- Ministry of Interior was unaware of these tests and accused the 3rd party of intruding on their systems and manipulating data.
- Source: https://denikn.cz/986275/zadrzeni-sefa-cermatu-inspekce-resi-prolomeni-systemu-ministerstva-vnitra/ (paywall, in Czech)

# How was it today?

And **what is your progress?**

Please fill in an **anonymous** exit ticket:

**https://muni.cz/go/pa211-22-06**

MUNI
FI