

## Session 04

Exploiting. Part 2: Web & OS & Hardware

Security of Information Systems (SIS)

Computer Science and Engineering Department

October 25, 2023

- ▶ Linux Kernel Vulnerabilities: State-of-the-Art Defenses and Open Problems (APSys'11)
- ▶ Securing Web Applications from Injection and Logic Vulnerabilities: Approaches and Challenges (Information & Software Technology, Volume 74, 2016)

1 / 33

2 / 33

## Web App architecture

- ▶ front end
- ▶ back end
- ▶ database

## Common Targets

- ▶ hosting web server
- ▶ other web servers
- ▶ privileged users
- ▶ other users

4 / 33

5 / 33

## Attack Vectors

- ▶ HTTP protocol
- ▶ URL
  - ▶ GET
  - ▶ POST
- ▶ file upload
- ▶ other users

## Common Web Vulnerabilities 2017

- ▶ OWASP 2017 TOP 10
- ▶ Injection
- ▶ Broken Authentication and Session Management
- ▶ Sensitive Data Exposure
- ▶ XML External Entity XXE
- ▶ Broken Access Control
- ▶ Security Misconfiguration
- ▶ Cross-Site Scripting XSS
- ▶ Insecure Deserialization
- ▶ Components with known vulnerabilities

6 / 33

7 / 33

## Injection

- ▶ SQL
- ▶ OS
- ▶ LDAP

## Broken Authentication Vulnerabilities

- ▶ compromise / steal
  - ▶ passwords
  - ▶ keys
  - ▶ session Tokens
- ▶ assume other users identities

8 / 33

9 / 33

## Sensitive Data Exposure

- ▶ data in transit
- ▶ data at rest

10 / 33

## XML External Entities (XXE)

- ▶ Extensible Markup Language (XML)
- ▶ Document Type Definition (DTD)
- ▶ billion laughs attack

11 / 33

## Broken Access Control

- ▶ bypass access control checks
- ▶ metadata manipulation
- ▶ browsing to authenticated pages as unauthenticated user

12 / 33

## Security Misconfiguration

- ▶ unnecessary features
- ▶ debug mode
- ▶ obsolete backward compatibility

13 / 33

## Cross-Site Scripting (XSS)

- ▶ reflected XSS
- ▶ stored XSS
- ▶ DOM XSS

14 / 33

## Insecure Deserialization

- ▶ Java object serialization
- ▶ JSON
- ▶ COAP

15 / 33

## Components with Known Vulnerabilities

- ▶ direct components
- ▶ nested dependencies
- ▶ 3rd party software

16 / 33

## Bonus: CSRF & SSRF

- ▶ same-origin policy
- ▶ Cross Site Request Forgery
- ▶ Server Side Request Forgery

17 / 33

## Common tools

- ▶ Dirb
- ▶ Burp
- ▶ Acunetix
- ▶ BeEF
- ▶ sqlmap
- ▶ Metasploit

18 / 33

## OS Exploiting

- ▶ information leak
- ▶ local privilege escalation
- ▶ remote command execution
- ▶ resource exhaustion

20 / 33

## Linux Kernel CVEs So far

- ▶ [https://www.cvedetails.com/vulnerability-list/vendor\\_id-33/product\\_id-47/cvssscoremin-7/cvssscoremax-7.99/Linux-Linux-Kernel.html](https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/cvssscoremin-7/cvssscoremax-7.99/Linux-Linux-Kernel.html)

21 / 33

## Common tools

- ▶ exploitdb: <https://github.com/offensive-security/exploitdb>
- ▶ LES (Linux Exploit Suggester): <https://github.com/mzet-/linux-exploit-suggester>
- ▶ Metasploit: <https://www.metasploit.com/>

22 / 33

## Hardware Flaws

- ▶ side channel + microarchitectural attacks
- ▶ undocumented instructions
- ▶ hardware synchronization issues (due to speed / performance updates)

24 / 33

## Side Channel Attacks

- ▶ cache attacks
- ▶ microarchitectural attacks

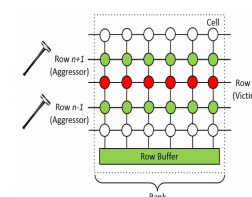
25 / 33

## Rowhammer

- ▶ <http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf>

26 / 33

## Rowhammer



<https://medium.com/baidulab/>

pc-security-facing-another-heavy-hammer-baidu-security-discovers-a-new-rowhammer-attack-be3dce8d1e92

27 / 33

## Meltdown & Spectre

- ▶ <https://meltdownattack.com/>
- ▶ Meltdown:  
<https://www.cve.org/CVERecord?id=CVE-2017-5754>
- ▶ bypass checks, cache side-channel attack
- ▶ Spectre:  
<https://www.cve.org/CVERecord?id=CVE-2017-5753>,  
<https://www.cve.org/CVERecord?id=CVE-2017-5715>
- ▶ speculative execution
- ▶ arbitrary memory access

28 / 33

## Sandsifter

- ▶ <https://github.com/xoreaxeaxeax/sandsifter>
- ▶ fuzzing of CPU instructions

29 / 33

## Summary

- ▶ TODO
- ▶ TODO
- ▶ TODO

31 / 33

## Keywords

- ▶ web application
- ▶ injection
- ▶ broken access control
- ▶ XEE
- ▶ XSS
- ▶ CSRF
- ▶ exploitdb
- ▶ Metasploit
- ▶ rowhammer
- ▶ Meltdown
- ▶ Spectre
- ▶ Sandsifter

32 / 33

## Resources

- ▶ TODO
- ▶ TODO
- ▶ TODO

33 / 33