AEV
Analysis and Exploration of Vulnerabilities

JOÃO PAULO BARRACA

Overall objectives

Understand key concepts around popular vulnerabilities and its exploitation

Experience with key techniques to exploit or defend software systems

Experience with relevant tools to conduct assessments and attacks

Identify, defend and recover from attacks

Approach

Explore the security landscape and actors

Explore attack vectors and enumeration

Explore specific vulnerabilities focusing on what, how, why

Explore how to reduce impact or recover from disaster

Document everything

Collaboration Tools

Discussion @ MS Teams: #OP_AEV_2223

- General discussion and instant collaboration
- Some course contents (snippets, confs, instructions)
- Grading and Assignments

Lecture Notes @ https://joao.barraca.pt/course/aev-2223

CTF Team @ UAC

- Discord link to be provided in class

Email: jpbarraca@ua.pt

Laboratory tools

Crafted exercises for each topic

Linux VMs and Docker Containers

- Debian/Ubuntu based
- Virtualbox disk format

Python, PHP and C languages

Other software: wireshark, nmap, gdb, ghidra, ZAP, openvas, john, metasploit, etc…

Home
My Profile
My Team
Labs
Rankings
Battlegrounds
Academy
Careers
Universities
Social
Enterprise
Customer Support
v 3.18.0

universidade de aveiro

University of Aveiro

DESCRIPTION

The University of Aveiro (UA) is a public foundation under private law whose mission is to contribute to and develop graduate and postgraduate education and training, research and cooperation with society.
Mission The UA's mission is to create, share and apply knowledge, involving the whole community through teaching, research and cooperation with the surrounding environment, in order to make a clear difference for individuals and society. This is a global project based on:

- innovative and lifelong learning, based on critical and independent thinking, which provides high quality education that is accessible to all
- influential research in creative ventures that provide meaningful local and global contributions to knowledge
- cooperation with society
- internationalisation linked to its diverse activities
- an academic welcoming and rewarding work environment for students, teachers, researchers and technical, administrative and management personnel

Vision To create and transmit knowledge in order to transform lives, communities and society in general, by promoting training for citizenship, in respecting the freedom, equality and dignity of the human person.
Organization The organisation of the UA is based on a matrix structure, which integrates the subsystems of both the university and polytechnic institutions, and involves permanent interaction between units, services and other structures. Interdisciplinarity and flexibility are the principal features as well as organisation and management by activities and objectives, plus an open-door approach with society and close links to the surrounding business environment.

Topics

Vulnerabilities

- CIA triad
- Tracking: CVE, NVD, CVSS

Vulnerability management

- Assessment
- Scope
- Auditing, SCAP
- Open acess platforms, crowdsourced Bug Hunting

Topics

Enumeration and System Analysis

- Attack surface
- Information sources (OSINT)
- Network protocols, APIs
- Software/system analysis
- Cyber Kill Chain, MITRE ATT&CK

Topics

Assessment and Exploitation of Vulnerabilities

- OWASP top 10, IEEE CSD top 10, 7 Pernicious Kingdoms

- Authentication: Cookies, JWT, Password Security, Enumeration
- XML External Entities (XXE)
- Cross Site Scripting: CSS, CSRF, Policies
- Deserialization: XML, JSON, WAF Bypassing
- Injection: SQL, Buffer Overflows, ROP
- Insecure direct object references and Authorization
- Environment: PATH, Preloading, Interception

Prevention and Detection

- Firewalls and WAF
- Logging
- Throttling

Incident Response: DFIR

Grading – 0 to 20 - 9.50 points required

10 points: practical assignments

- 1pt Group Assignment – CTF participation (2 students)
- 2pt Group Assignment – Challenge creation (2 students)
- 7pt Group Assignment – Software Audit (4 students)

10 points: theoretical exam

- Optionally split in two tests (November and January)
  - Same content, same difficulty, but split in two sessions

up to -20: Exploitation of UA/professors/students/out of scope entities or cheating/plagiarism

- UA internal regulation and Portuguese Legal Framework will be followed