Poznan University of Technology
Faculty of Computing and Telecommunications

michal.apolinarski[at]put.poznan.pl

Course: Application Security – laboratories

Lecturer: Michał Apolinarski, Ph.D.

Topic: Websites recon

Duration (on site): 180 min.

PREREQUISITES:

Knowledge of computer networks, operating systems and web apps.

GOALS:

- The aim of the class is to familiarize students with the OSINT (**O**pen **S**ource **Int**elligence) targeted on websites.
- Preparing a report of the performed tasks.

INSTRUCION (tasks for 1 person):

1. You can't perform any type of attacks, it's only a RECON.
2. Remember that you should base on and use only public information accessible legally. You may use for example:
    a. web browsers (view source, devtools, inspectors, debuggers, add-ons),
    b. operating systems network tools, Wireshark, etc.
    c. online tools like: dnschecker.org, whois, etc.
    d. bing, google (google dorks aka Google Hacking):
3. Visit sites:
    a. https://www.put.poznan.pl/
    b. https://www.b-tu.de/
    c. https://web.unican.es/
    d. https://web.umons.ac.be/en/
    e. https://www.uphf.fr/

f. https://www.uwasa.fi/fi

g. ... (your idea ☺)

4. For at least 3 of above sites try find as much as possible about technical issues like (the more the better):

   a. website tech stack,

   b. IP addresses, DNS records, domain history / registrar, web server info, subdomains,

   c. developers and used CMS, dependencies and frameworks – check for known vulnerabilities,

   d. check web browser consol log, requests,

   e. details about SSL (type, validation, CA, expire date), check if there is any unencrypted traffic,

   f. contents of /robots.txt file

   g. check Google Dorks (indexed urls) like:

      i. publicly exposed documents[1],

      ii. directory listing vulnerabilities[2],

      iii. configuration / database / log files exposed,

      iv. backup and old files,

      v. login / signup pages,

      vi. sql errors,

      vii. php errors / warning,

      viii. find subdomains / sub-subdomains,

      ix. search in github / gitlab / wayback machine,

   h. and so on…

5. Prepare and send to the lecturer a report of performed tasks (positive and false) with your results and analysis. Describe used tools and steps.

REPORT:

- Should include a title page with full details of the student, course and exercise being reported.
- Should be carefully edited and provide evidence of the completion of all exercises confirmed by screenshots, answers and conclusions.
- Complete report should be send to the lecturer.

[1] example: site:***domain*** ext:***doc*** | ext:***docx*** | ext:***odt*** | ext:***rtf*** | ext:***sxw*** | ext:***psw*** | ext:***ppt*** | ext:***pptx*** | ext:*pps* | ext:***csv***

[2] example: site:***domain*** intitle:***index.of***