CSTCE
Cyber Security Training Centre of Excellence

Efectuarea Testelor de Penetrare asupra Aplicațiilor de tip Web

Ce este Web Penetration Testing?

- Testarea unei aplicatii de tip web (website) pentru a identifica vulnerabilitati
- Testele sunt efectuate atat automat cat si manual
- Vulnerabilitatile identificate sunt verificate prin incercarea de exploatare a acestora

CSTCE
Cyber Security Training
Centre of Excellence

Metodologie - Web Pentest

1. Planificare
2. Recunoastere si Enumerare
3. Scanare
4. Exploatare
5. Raportare
6. Retestare

CSTCE
Cyber Security Training
Centre of Excellence

Planificare

- Se stabileste scopul testelor - SoW (Statement of Work)
- Se stabilesc regulile testelor - RoE (Rules of Engagement)
- Se stabileste mediul de test

CSTCE
Cyber Security Training Centre of Excellence

Planificare: SoW

- “Statement of Work”
- Ce aplicatii web?
- Care sunt asteptarile?
- Deadline, program de executie, preturi
- Rol de contract

CSTCE
Cyber Security Training
Centre of Excellence

Planificare: NDA

- “Non-Disclosure Agreement”
- Acord legal de protejare a informatiilor confidentiale

Planificare: RoE

- “Rules of Engagement”
- Instructiuni si reguli de desfasurare a testului de penetrare
- Restrictii de anumite teste, ore/zile de testare, reguli de comunicare, detalii despre testeri, etc.

CSTCE
Cyber Security Training Centre of Excellence

Planificare: Pregatirea mediului

- Recomandari:
  - Mediul de test trebuie sa fie **diferit** si **izolat** fata de mediul de productie!
  - Mediul de test sa contina date “dummy”
  - Abilitatea de a fi resetat cu usurinta

CSTCE
Cyber Security Training Centre of Excellence

Planificare: Tipuri de Testare

1. Blackbox Testing:
    a. Pentester-ul cunoaste doar adresa website-ului
2. Graybox Testing:
    a. Pentester-ul cunoaste adresa si are access la conturi in website (optional si documentatie)
3. Whitebox Testing:
    a. Pentester-ul cunoaste adresa, are access la conturi in website (optional si documentatie), dar si la cod sursa

CSTCE
Cyber Security Training Centre of Excellence

Recunoastere si Enumerare

In principal se auditeaza urmatoarele aspecte:

- Foldere, Fisiere si Pagini
- Endpoint-uri
- Cod Sursa (Client-Side)
- Librarii si Tehnologii folosite de website (incl. versiunile acestora)
- Mesaje de eroare
- Functionalitati ale website-ului
- Configurari de securitate (headers, cookie-uri, SSL/TLS, etc.)
- Redirectionari catre alte pagini
- Formatul numelui de utilizator si validarea celor existenti
- Mecanisme de securitate in functiune - WAF, Rate-Limiting, Password Policy, etc.

CSTCE
Cyber Security Training Centre of Excellence

Scanare

- “Vulnerability Scanning”
- Se folosesc atat instrumente automate de identificare a vulnerabilitatilor cat si teste manuale

CSTCE
Cyber Security Training Centre of Excellence

Exploatare

- Reprezinta procesul de validare a vulnerabilitatiilor identificate in pasul anterior
- Se realizeaza in mod manual in majoritatea timpului
- Multiple vulnerabilitati se pot “lega” pentru a realiza un impact mai mare (corelare)

CSTCE
Cyber Security Training
Centre of Excellence

Raportare

- Se finalizeaza raport-ul de Web Penetration Testing
- Acesta reprezinta “ceea ce vede clientul” (produsul final - livrabilul)
- Contine toate detaliile despre vulnerabilitatiile identificate si recomandari de remediere

CSTCE
Cyber Security Training Centre of Excellence

Retestare

- Procesul de testare a remedierilor propuse
- Totodata, se testeaza eficacitatea solutiilor implementate, prin incercarea de evaziune a acestora
- Deobicei, se emite un raport de retestare la final

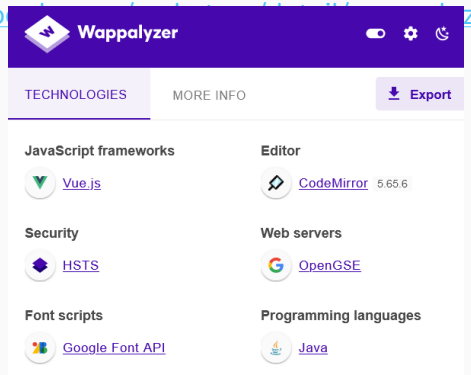
CSTCE
Cyber Security Training
Centre of Excellence

OWASP TOP 10 - Web

CSTCE
Cyber Security Training Centre of Excellence

Enumerarea Tehnologiilor Folosite

- Wappalyzer - extensie in browser pentru identificarea librariilor, tehnologiilor, si versiunilor acestora
  - Firefox: https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/
  - Chrome: https://chrome.go[illegible]zer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg



CSTCE
Cyber Security Training Centre of Excellence

Enumerare Foldere si Fisiere

- Instrumente de enumerare foldere si fisiere:
  - dirb
  - dirbuster
  - gobuster
  - gospider

CSTCE
Cyber Security Training
Centre of Excellence

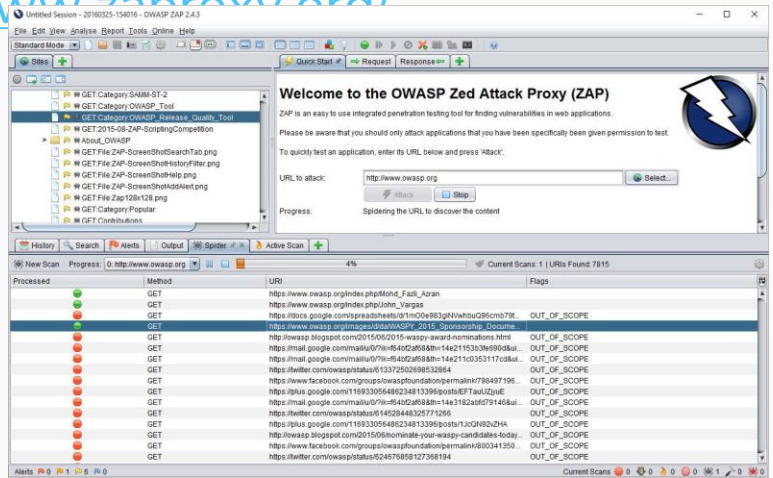
Parameter Fuzzing

- Procesul de introducere a datelor aleatorii pentru a identifica parametrii acceptati de catre website
- Acestia pot contine vulnerabilitati “ascunse” de catre dezvoltatori
- ffuf: https://github.com/ffuf/ffuf

CSTCE
Cyber Security Training Centre of Excellence

OWASP ZAP

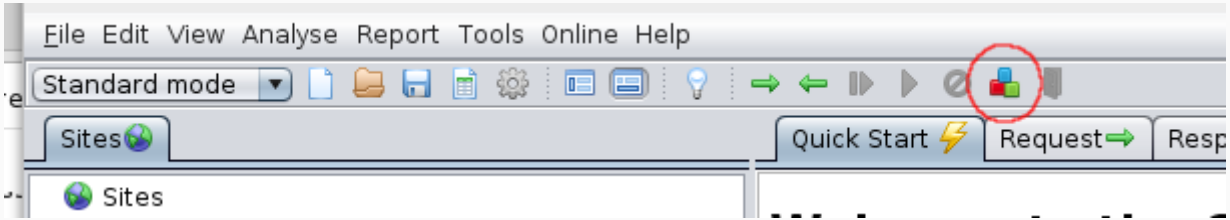
- Instrument de scanare automata de vulnerabilitati in aplicatii web (web vulnerability scanning)
- https://www.zaproxy.org/



CSTCE
Cyber Security Training Centre of Excellence

OWASP ZAP - Extensii

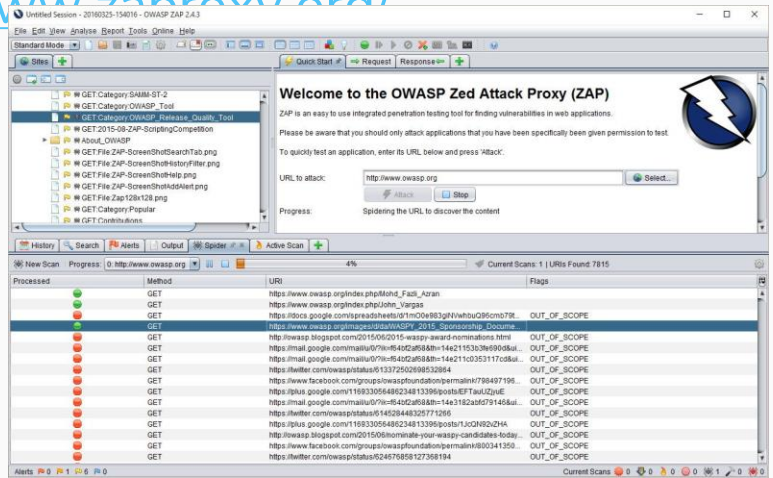
- Pachete de module suplimentare care se pot importa in OWASP ZAP pentru a rula mai multe teste aditionale
- https://github.com/zaproxy/zap-extensions



CSTCE
Cyber Security Training Centre of Excellence

OWASP ZAP

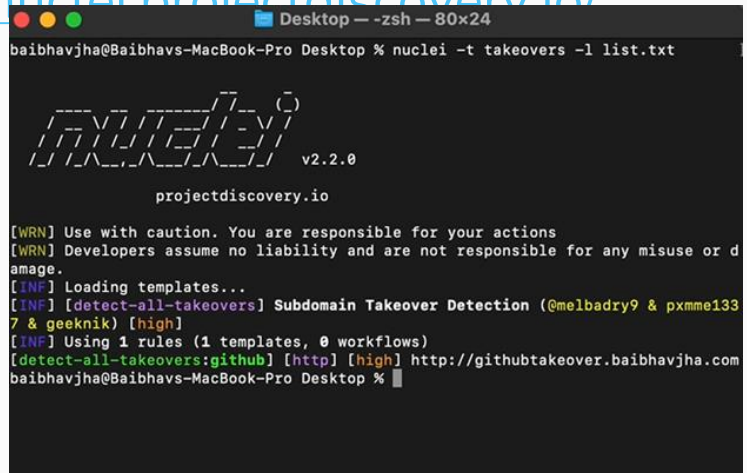
- Instrument de scanare automata de vulnerabilitati in aplicatii web (web vulnerability scanning)
- https://www.zaproxy.org/



CSTCE
Cyber Security Training Centre of Excellence

Nuclei

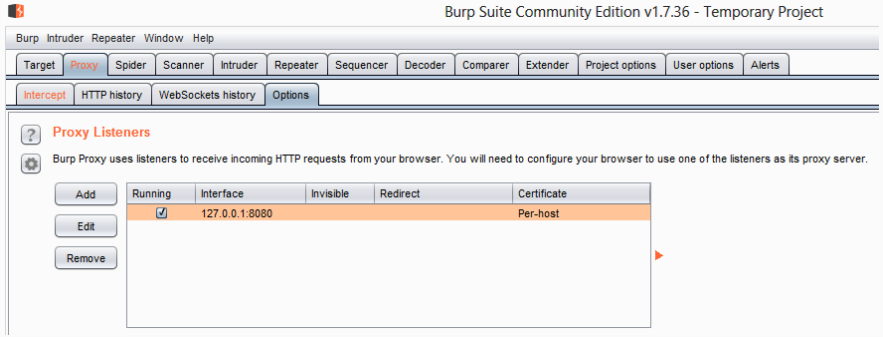
- Instrument de scanare automata de vulnerabilitati in aplicatii web (web vulnerability scanning)
- https://nuclei.projectdiscovery.io/



CSTCE
Cyber Security Training Centre of Excellence

Burp Suite Community

- Instrument ce contine o colectie de module si utilitati pentru testarea manuala a securitatii aplicatiilor web
  - https://portswigger.net/burp



CSTCE
Cyber Security Training Centre of Excellence

Burp Suite Community

Utilizari:

- Identificarea manuala a vulnerabilitatiilor
- Interceptarea, manipularea si modificarea request-urilor catre aplicatiile web
- Simularea controlata actiuni

CSTCE
Cyber Security Training
Centre of Excellence

Disclaimer

- “Nu ne asumam daca se va intampla ceva pe viitor”
- “The vulnerabilities in this report reflect the conditions found during our testing and do not necessarily reflect current conditions.”
- Foarte important din punct de vedere legal !!!

CSTCE
Cyber Security Training
Centre of Excellence

Invata din Exemple!

- Rapoarte publice de Penetration Testing:

https://github.com/juliocesarfort/public-pentesting-reports

CSTCE
Cyber Security Training
Centre of Excellence

Q&A