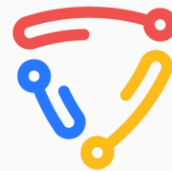


# Efectuarea Testelor de Penetrare asupra Aplicațiilor de tip Web

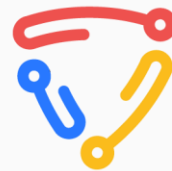
# Ce este Web Penetration Testing?

- 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



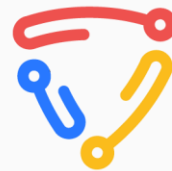
# Metodologie - Web Pentest

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



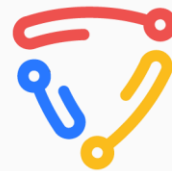
# Planificare

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



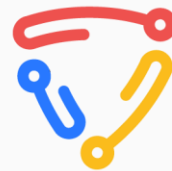
# Planificare: SoW

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



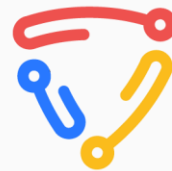
# Planificare: NDA

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



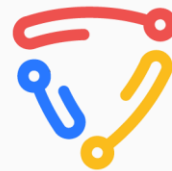
# Planificare: RoE

- “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.



# 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





# Planificare: Tipuri de Testare

## 1. Blackbox Testing:

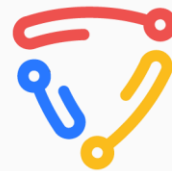
- a. Pentester-ul cunoaste doar adresa website-ului

## 2. Graybox Testing:

- a. Pentester-ul cunoaste adresa si are access la conturi in website (optional si documentatie)

## 3. Whitebox Testing:

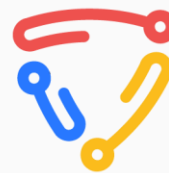
- a. Pentester-ul cunoaste adresa, are access la conturi in website (optional si documentatie), dar si la cod sursa



# Recunoastere si Enumerare

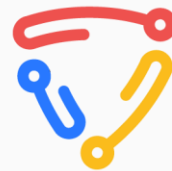
In principal se auditeaza urmatoarele aspecte:

- 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.



# Scanare

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



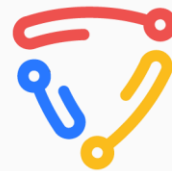
# Exploatare

- Reprezinta procesul de validare a vulnerabilitatilor 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)



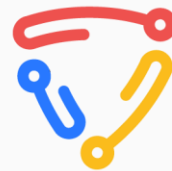
# Raportare

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



# 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



# OWASP TOP 10 - Web

## The 2021 OWASP Top 10 list

### **A01:2021**

Broken  
Access Control

### **A02:2021**

Cryptographic  
Failures

### **A03:2021**

Injection

### **A04:2021**

Insecure Design

### **A05:2021**

Security  
Misconfiguration

### **A06:2021**

Vulnerable  
and Outdated  
Components

### **A07:2021**

Identification  
and Authentication  
Failures

### **A08:2021**

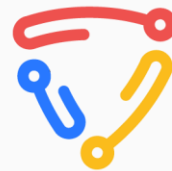
Software and  
Data Integrity  
Failures

### **A09:2021**

Security Logging  
and Monitoring  
Failures

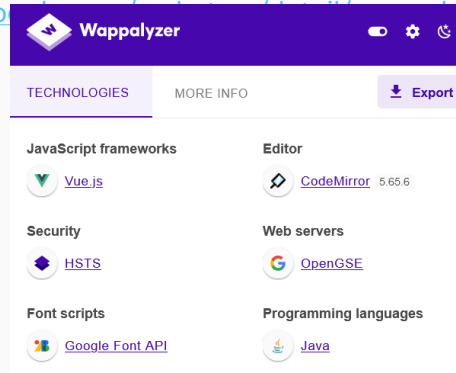
### **A10:2021**

Server-Side  
Request Forgery



# Enumerarea Tehnologiilor Folosite

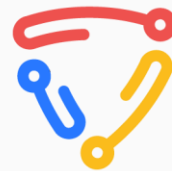
- Wappalyzer - extensie in browser pentru identificarea librariilor, tehnologiilor, si versiunilor acestora
- Firefox: <https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/>
- Chrome: <https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfblamg>





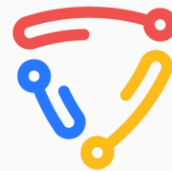
# Enumerare Foldere si Fisiere

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



# Parameter Fuzzing

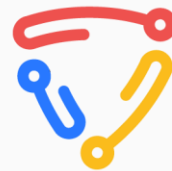
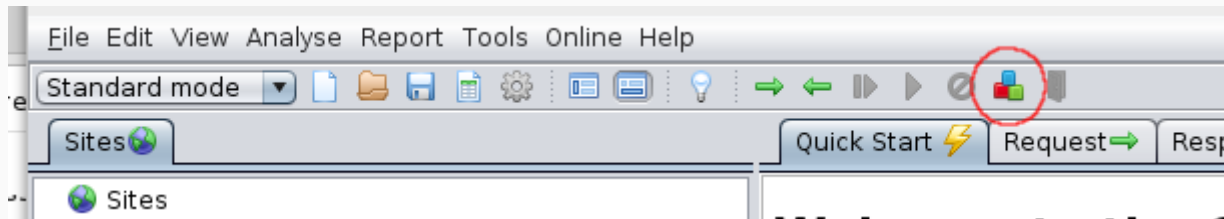
- Procesul de introducere a datelor aleatorii pentru a identifica parametrii acceptati de catre website
- Acestia pot contine vulnerabilitati “ascunse” de catre dezvoltatori
- ffuf: <https://github.com/ffuf/ffuf>





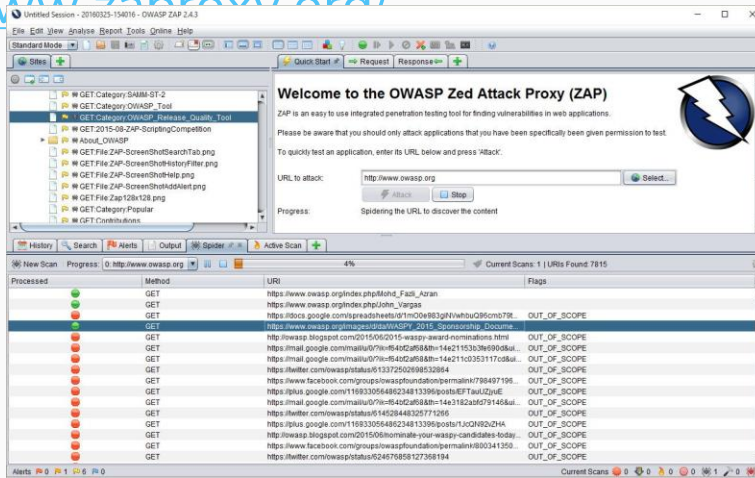
# OWASP ZAP - Extensii

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



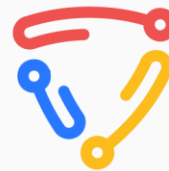
# OWASP ZAP

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



The screenshot displays the OWASP Zed Attack Proxy (ZAP) interface. The main window shows a 'Welcome to the OWASP Zed Attack Proxy (ZAP)' message with instructions on how to use the tool. Below the message, there is a text input field for the URL to attack, set to 'http://www.owasp.org', and buttons for 'Attack' and 'Stop'. The 'Progress' bar indicates 'Spidering the URL to discover the content'. The bottom pane shows a table of discovered URIs and their corresponding methods.

Method	URI	Flags
GET	https://www.owasp.org/index.php/Muhj_Fadl_Azran	
GET	https://www.owasp.org/index.php/ohrj_1vrgzq	
GET	https://sites.google.com/view/owasp-2015-08-zap-scanning/completion	OUT_OF_SCOPE
GET	https://www.owasp.org/images/OWASPSP_2015_Sponsorship_Docume...	OUT_OF_SCOPE
GET	http://www.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
GET	https://mail.google.com/mail/u/0/wi-fi-40249884m-144211033511708ku...	OUT_OF_SCOPE
GET	https://mail.google.com/mail/u/0/wi-fi-40249884m-144211033511708ku...	OUT_OF_SCOPE
GET	https://www.facebook.com/groups/owasp/attachements/permalink/798437198...	OUT_OF_SCOPE
GET	https://plus.google.com/116933056486234813396/posts/EFTTAuZUe...	OUT_OF_SCOPE
GET	https://mail.google.com/mail/u/0/wi-fi-40249884m-1443102a3d79146ku...	OUT_OF_SCOPE
GET	https://www.owasp.org/images/1492844830711266	OUT_OF_SCOPE
GET	https://plus.google.com/116933056486234813396/posts/1uQNR9Zq4H...	OUT_OF_SCOPE
GET	http://www.blogspot.com/2015/06/nominate-your-waspy-candidates-today...	OUT_OF_SCOPE
GET	https://www.facebook.com/groups/owasp/attachements/permalink/800341350...	OUT_OF_SCOPE
GET	https://www.owasp.org/images/824676858127368194	OUT_OF_SCOPE



# Nuclei

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

```
baibhavjha@Baibhavs-MacBook-Pro Desktop % nuclei -t takeovers -l list.txt

nuclei v2.2.0
projectdiscovery.io

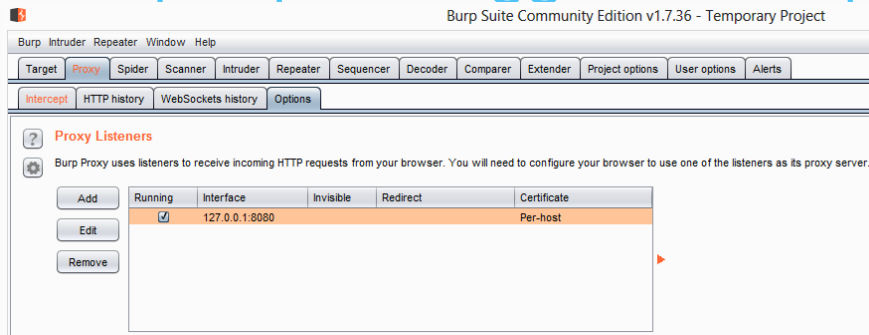
[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[INF] Loading templates...
[INF] [detect-all-takeovers] Subdomain Takeover Detection (@melbadry9 & pxmme1337 & geeknik) [high]
[INF] Using 1 rules (1 templates, 0 workflows)
[detect-all-takeovers:github] [http] [high] http://githubtakeover.baibhavjha.com
baibhavjha@Baibhavs-MacBook-Pro Desktop %
```



# Burp Suite Community

- Instrument ce contine o colectie de module si utilitati pentru testarea manuala a securitatii aplicatiilor web

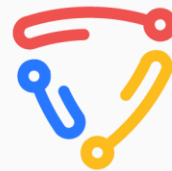
○ <https://portswigger.net/burp>



# Burp Suite Community

Utilizari:

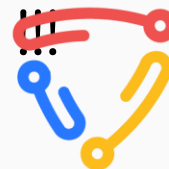
- Identificarea manuala a vulnerabilitatilor
- Interceptarea, manipularea si modificarea request-urilor catre aplicatiile web
- Simularea controlata actiuni





# Disclaimer

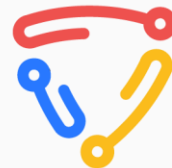
- “Nu ne asumam daca se va intampla ceva pe viitor”
- “The vulnerabilities in this report reflect the conditions found during our testing and do not necessarily reflect current conditions.”
- Foarte important din punct de vedere legal !!!



# Invata din Exemple!

- Rapoarte publice de Penetration Testing:

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





**CSTCE**  
Cyber Security Training  
Centre of Excellence

# Q&A

