CyberSecurity Summer School

Lector dr. Dorin IORDACHE

26-30.06.2023
Facultatea de Matematică și Informatică

Atacuri asupra aplicațiilor Web

Agenda

01 Amprenta server web

02 OSINT – Open Source Intelligence

03 Open Web Application Security Project -OWASP

04 Exercițiu SQL injection

01 Introducere

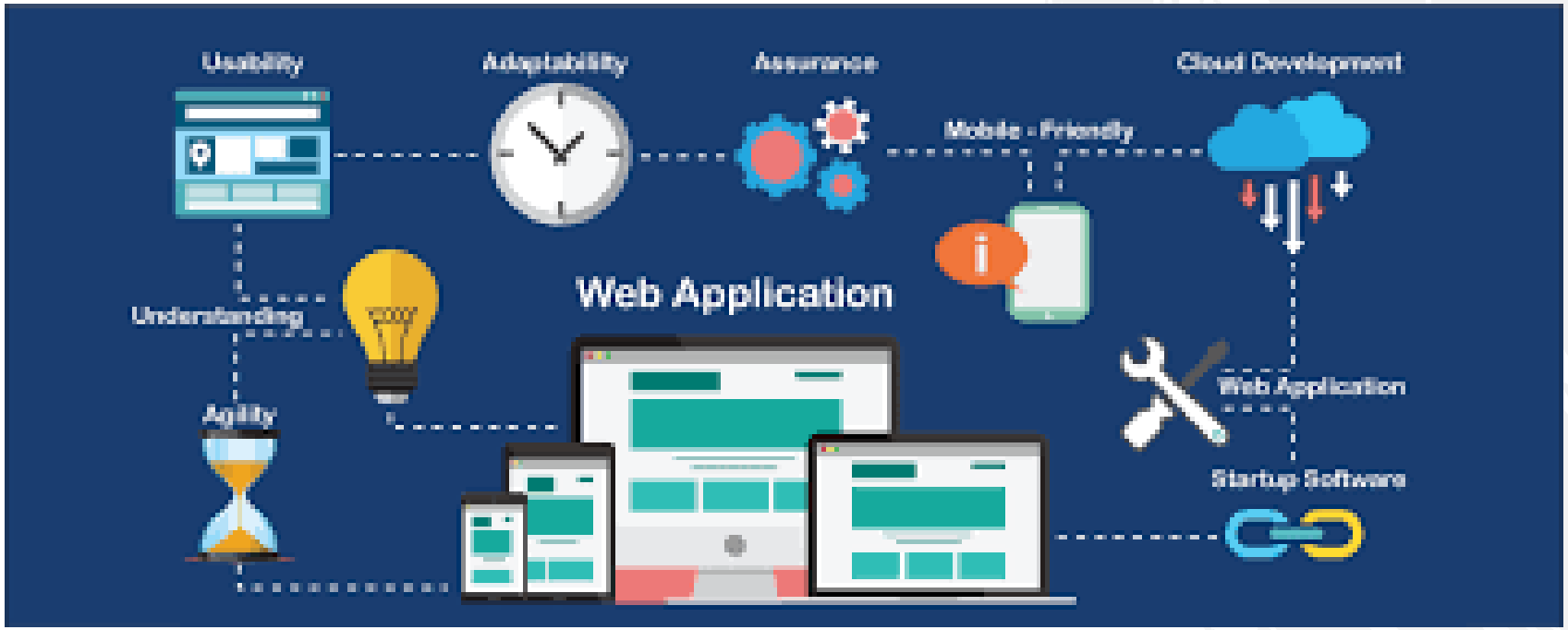
Avertisment

Ca și în alte cursuri, este posibil să întâlniți exemple de instrumente și tehnici aplicate unor adrese IP și resurse web reale.

Nu executați niciodată niciunul dintre aceste instrumente și tehnici împotriva acestora!!!!!

Aplicații web

Aplicațiile web folosesc tehnologii și paradigme de programare diferite în comparație cu aplicațiile desktop.
Din acest motiv, testarea aplicațiilor web, de la culegerea de informații tehnice până la faza de exploatare web, este importantă.



Imagine: https://www.javatpoint.com/web-application/

Aplicații web

Aplicațiile web reprezintă adesea marea majoritate a suprafeței de atac a Internetului.

Aplicațiile web rulează pe servere web, așa că testarea dacă un server web este protejat de atacurile externe sau interne este importantă.

Un server web configurat greșit poate fi o ușă deschisă către întreaga infrastructură.

Amprenta web

Amprentarea unui server web înseamnă detectarea:

- Platforma serviciului web: Apache, IIS, nginx, etc.
- Versiunea serverului web
- Sistemul de operare al serverului.

02 OSINT – Open Source Intelligence

OSINT – OpenSource Intelligence

Mai noi, OSINT este mai eficient, prin:

- Exploatarea informațiilor disponibile în:
  - Rețelele sociale;
  - Situri publice
  - Siturile web ale țintelor

OSINT – OpenSource Intelligence

- Colectarea de informații din Rețelele sociale:
  - Identificarea verigii slabe din lanțul de securitate: **omul!**

  Personalul interacționează activ cu sistemele și serviciile organizației, prin urmare securitatea personalului, când interacționează în Internet, influențează gradul de securitate al organizației.

OSINT

Atacatorii (hacker) acum pot accesa informații despre persoane și produse care cu greu puteau fi obținute în trecut.

în Mediul criminal actual atacatorii pot exploata aceste informații valoroase pentru a executa **atacuri sofisticate**.

Informații

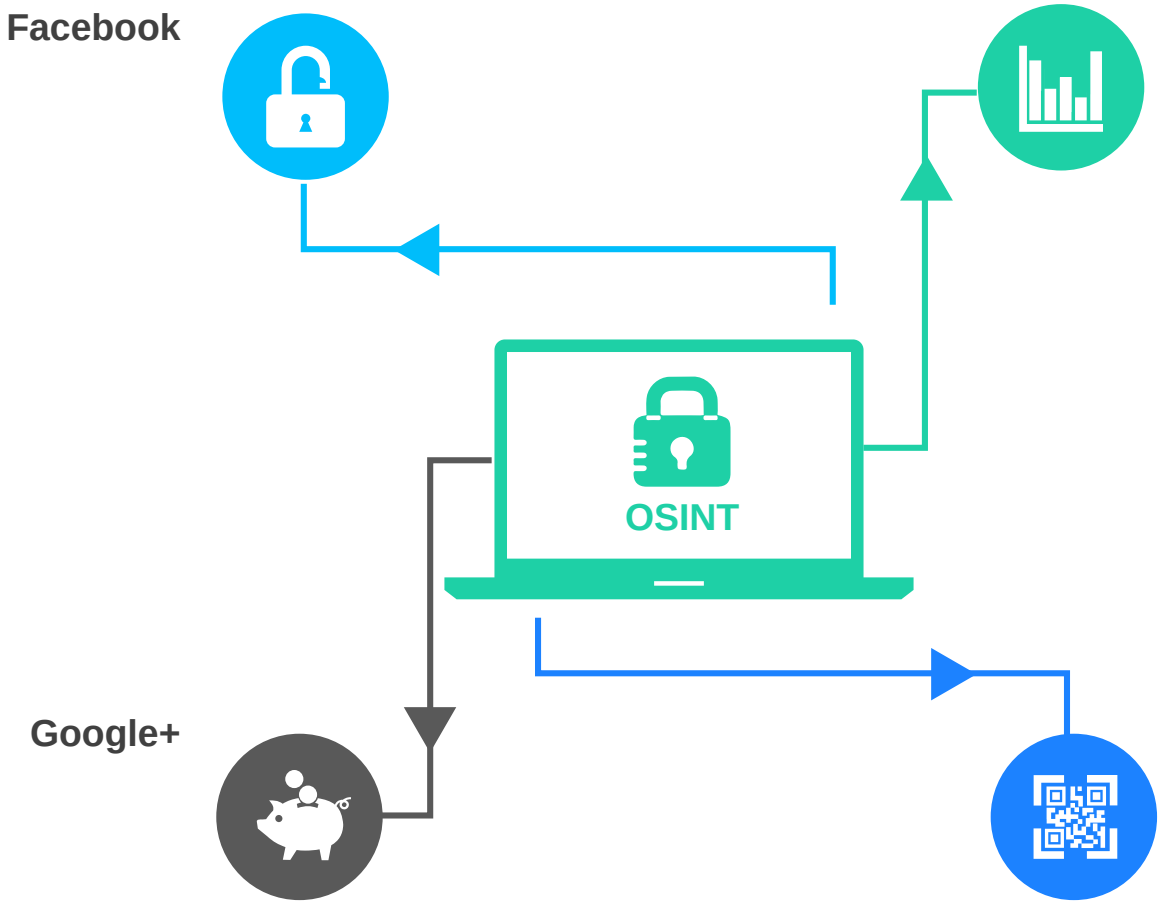
Nontehnice

Proiecte în lucru
Excursii la conferințe
Numere de telefon
Adrese de email și conturi rețele sociale.

Tehnice

Adrese de rețea
Situri web
Locații infrastructură
Sisteme de operare

Crearea imaginii sistemelor și tehnologiilor organizației



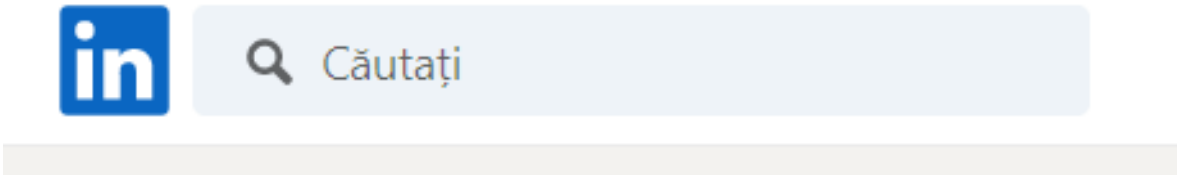
Exemplu:
Instagram ar fi util de investigat dacă organizația activează în domeniul publicității

Având în vedere gama largă de rețele sociale alegerea elementelor de investigat se realizează în funcie de specificul organizației:
While LinkedIn, Twitter și Facebook sunt utilizate în ”*scop general*”

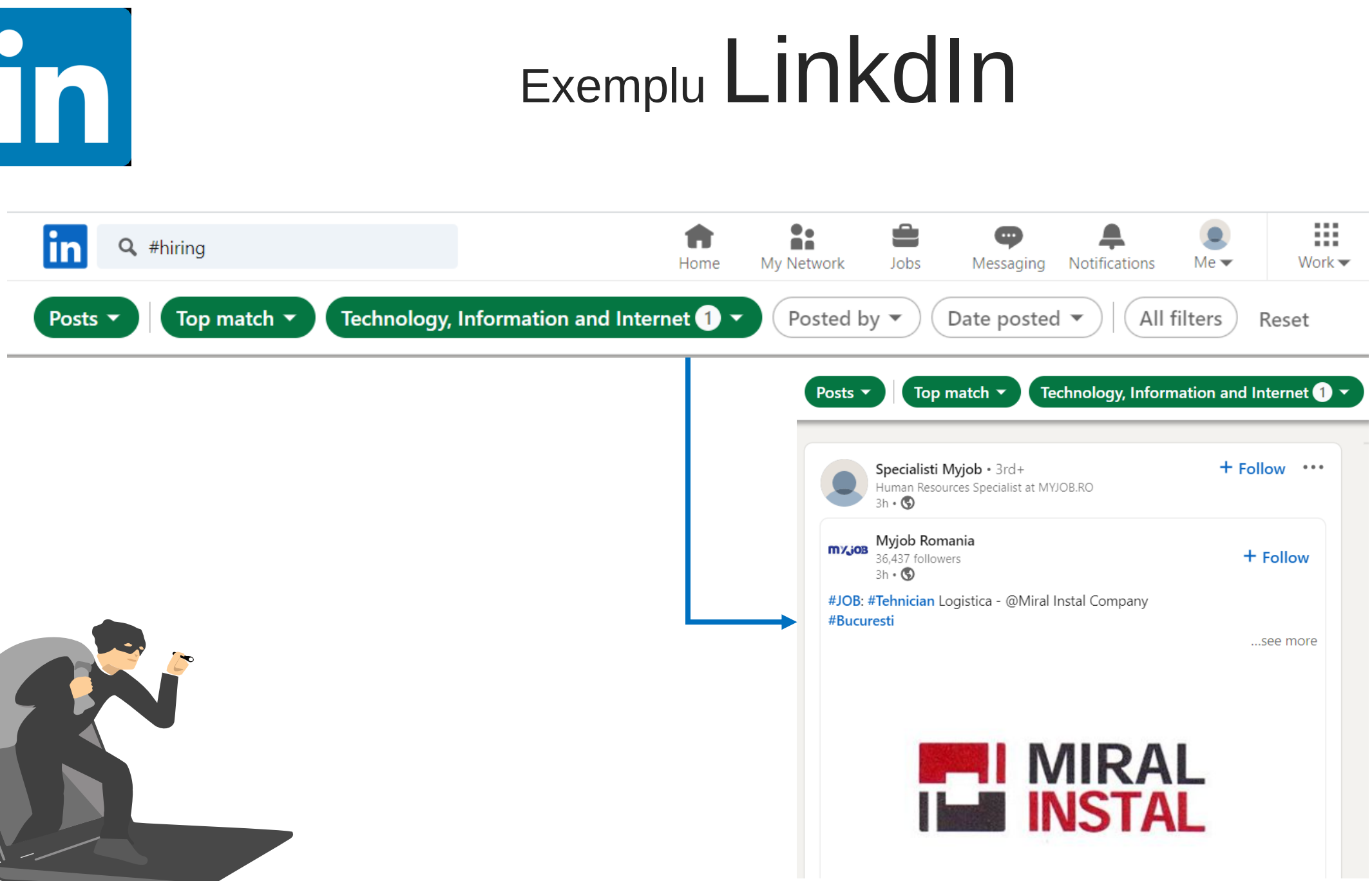
Exemplu LinkdIn

Utilizare căutare avansată LinkedIn pentru a regăsi anunțuri după diferite criterii:

După logarea în cont din fereastra de căutare, ca în imaginea de mai jos:

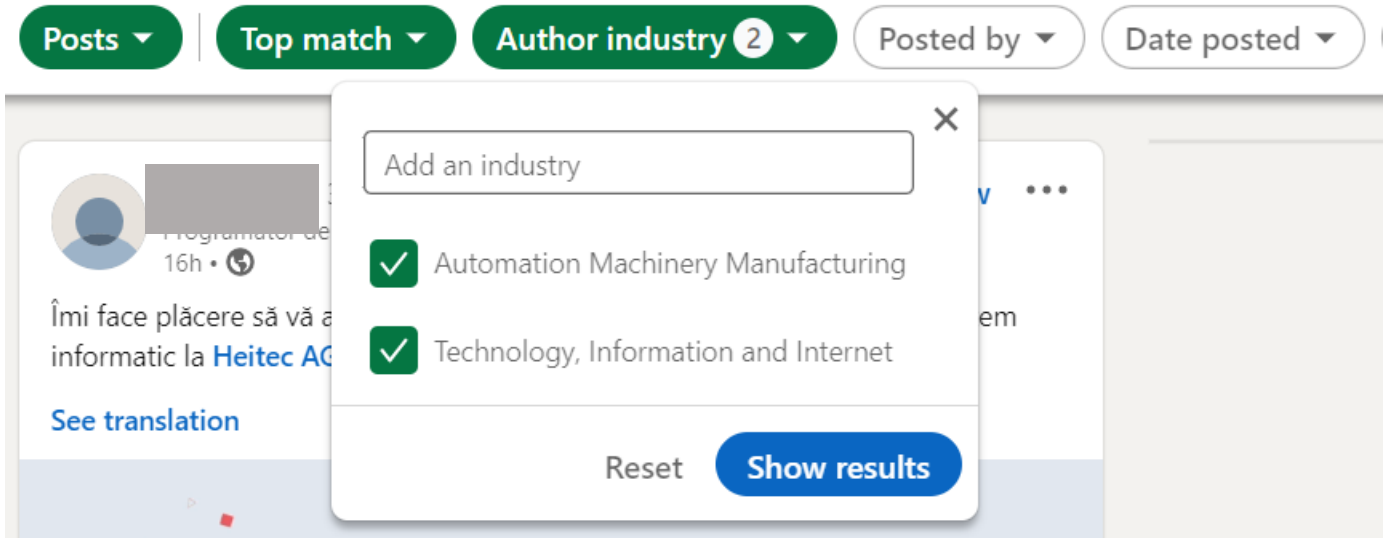


Exemplu LinkdIn



Exemplu LinkdIn

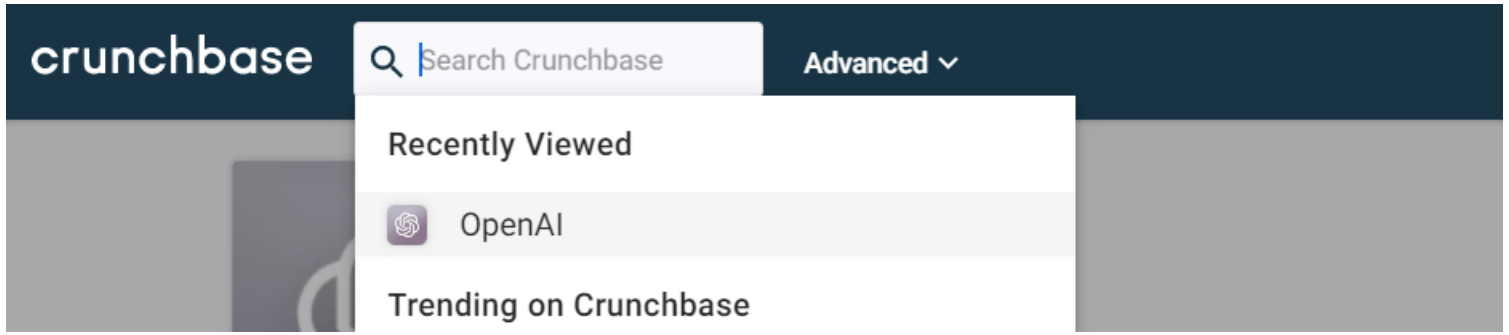
Multe conturi LinkedIn au și informații personale, **numere de telefon** sau **adrese de email**, ce pot fi exploatate.



Diferite platforme de rețele sociale pot fi integrate în scopul *rafinării* datelor colectate (creșterea gradului de certitudine).
Spre exemplu, LinkdIn corelat cu Twitter pentru a găsi eventualele informații lipsă, dintr-o rețea.

Exemplu CrunchBase

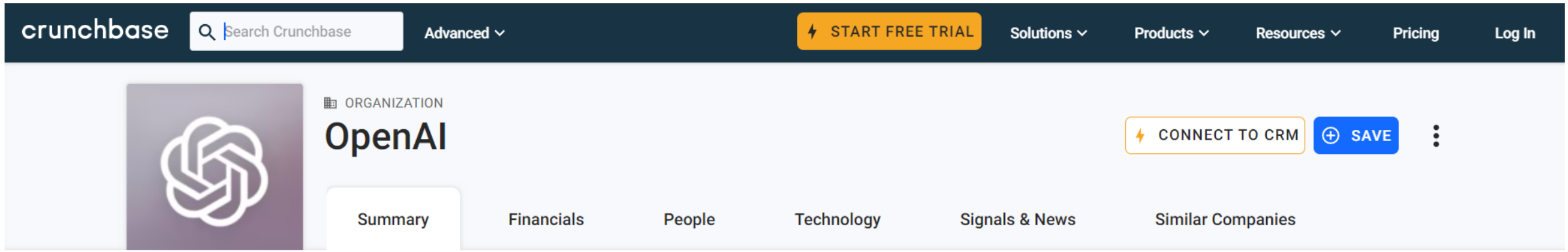
Crunchbase este o companie ce furnizează o bază de date care stochează informații detaliate despre fondatori, investitori, angajați, răscumpărări și achiziții.



https://www.crunchbase.com/

Exemplu: CrunchBase

crunchbase



About

OpenAI is an AI research and deployment company that aims to ensure that artificial general intelligence benefits all of humanity.

- San Francisco, California, United States
- 251-500
- Corporate Round
- Private
- www.openai.com

Highlights

Investments 2	Total Funding Amount $11B
Contacts 104	Employee Profiles 27
Investors 9	Similar Companies 9

Recent News & Activity

News • Jan 30, 2023
exchangewire.com — Microsoft, GitHub & OpenAI Appeal to Dismiss Lawsuit; UK Homes Cancel 2 Million Streaming Services

News • Jan 30, 2023
The Information — OpenAI Dangles Perks and Early Access to Win Investments in AI Startups

News • Jan 30, 2023
pcgamer — CEO of OpenAI says misuse of artificial intelligence could be 'lights out for all'

VIEW ALL

https://www.crunchbase.com/

Exemplu: Whois

O altă resursă este baza de date Whois. Se pot obține informații cu privire la:

- Numele proprietarului
- Adresa de corespondență
- Adresa de email
- Date de contact tehnice

cu privire la un domeniu Internet (atât timp cât aceste informații sunt publice), astfel:

```
root@debian:/home/dorin# whois tesla.com
   Domain Name: TESLA.COM
   Registry Domain ID: 187902_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2022-10-02T09:36:05Z
   Creation Date: 1992-11-04T05:00:00Z
   Registry Expiry Date: 2024-11-03T06:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
bited
```

Exemplu: Whois

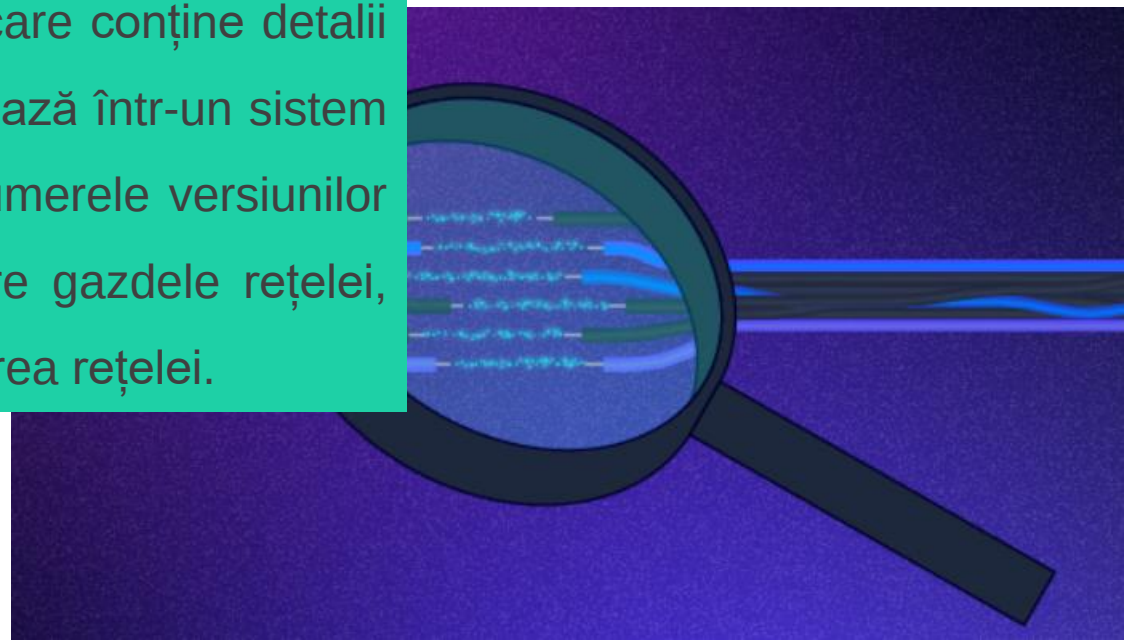
Informații tehnice:

```
Admin Fax Ext:
Admin Email: admin@dnstinations.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: DNStination Inc.
Tech Street: 3450 Sacramento Street, Suite 405
Tech City: San Francisco
Tech State/Province: CA
Tech Postal Code: 94118
Tech Country: US
Tech Phone: +1.4155319335
Tech Phone Ext:
Tech Fax: +1.4155319336
Tech Fax Ext:
Tech Email: admin@dnstinations.com
Name Server: a1-12.akam.net
Name Server: edns69.ultradns.com
Name Server: a9-67.akam.net
Name Server: a12-64.akam.net
Name Server: a28-65.akam.net
Name Server: edns69.ultradns.net
Name Server: edns69.ultradns.org
Name Server: a7-66.akam.net
Name Server: edns69.ultradns.biz
```

Banner Grabbing

banner grabbing:

- este o tehnică folosită de hackeri și echipele de securitate pentru a obține informații despre un sistem informatic dintr-o rețea și despre serviciile care rulează pe porturile sale deschise. Un banner este un text afișat de un server gazdă care conține detalii precum tipul software-ului și versiunea care rulează într-un sistem sau server. Ecranele de întâmpinare divulgă numerele versiunilor software și alte informații despre sistem despre gazdele rețelei, oferind infractorilor cibernetici un avans în atacarea rețelei.



Banner Grabbing

Instrumente:

Telnet: client clasic multiplatformă ce permite hackerilor și pen-testerilor să interacționeze cu serviciile de la distanță pentru preluarea de bannere. Pen-testerii și atacatorii pot executa telnet la gazde pe portul telnet implicit (portul TCP 23) pentru a descoperi informații relevante. Atacurile pot accesa alte porturi utilizate în mod obișnuit, cum ar fi SMTP, HTTP și POP3. Majoritatea sistemelor de operare pot stabili sesiuni Telnet, permițând utilizatorilor să efectueze preluarea bannerelor

Whatweb: instrument ce recunoaște site-urile web, ajutând hackerii și analiștii de securitate să determine bannerul aplicațiilor web prin dezvăluirea informațiilor despre server, cum ar fi adresa IP, versiunea, titlul paginii web și sistemul de operare care rulează

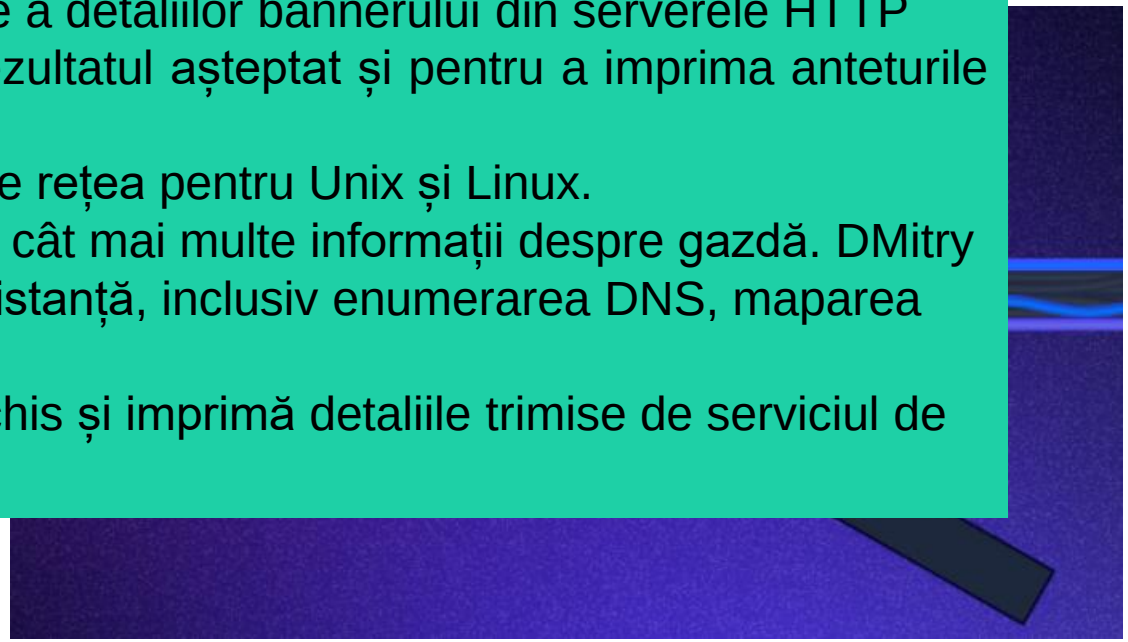
cURL: instrumentul care include funcționalitatea de preluare a detaliilor bannerului din serverele HTTP

Wget: Wget folosește un script simplu pentru a suprima rezultatul așteptat și pentru a imprima anteturile trimise de serverul HTTP

Netcat: este unul dintre cele mai vechi și populare utilitare de rețea pentru Unix și Linux.

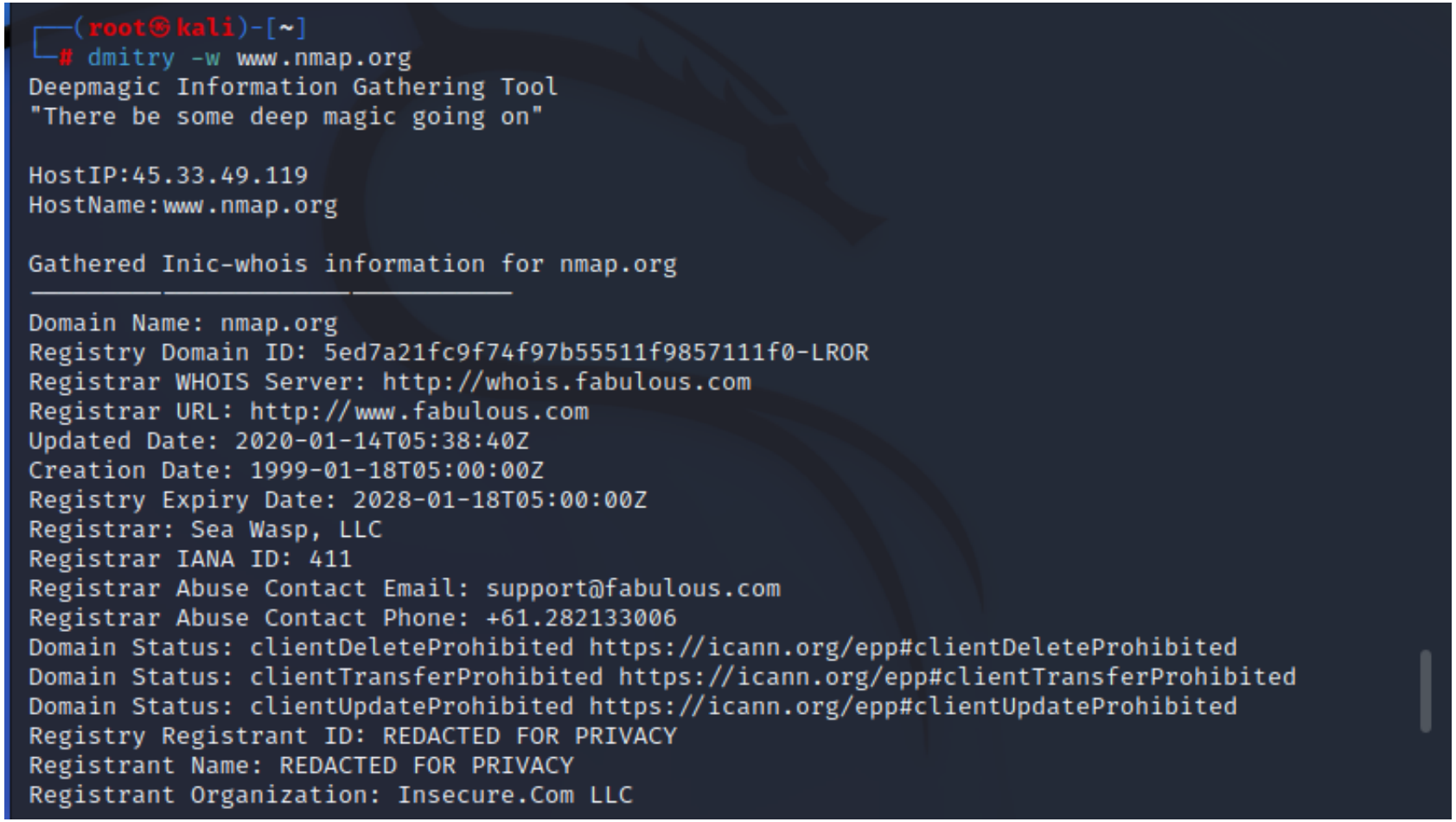
DMitry: Deepmagic Information Gathering Tool poate aduna cât mai multe informații despre gazdă. DMitry permite atacatorilor să obțină toate datele de la o gazdă la distanță, inclusiv enumerarea DNS, maparea subdomeniilor, porturile deschise și multe altele.

Nmap: grabb banner ce se conectează la un port TCP deschis și imprimă detaliile trimise de serviciul de ascultare în câteva secunde



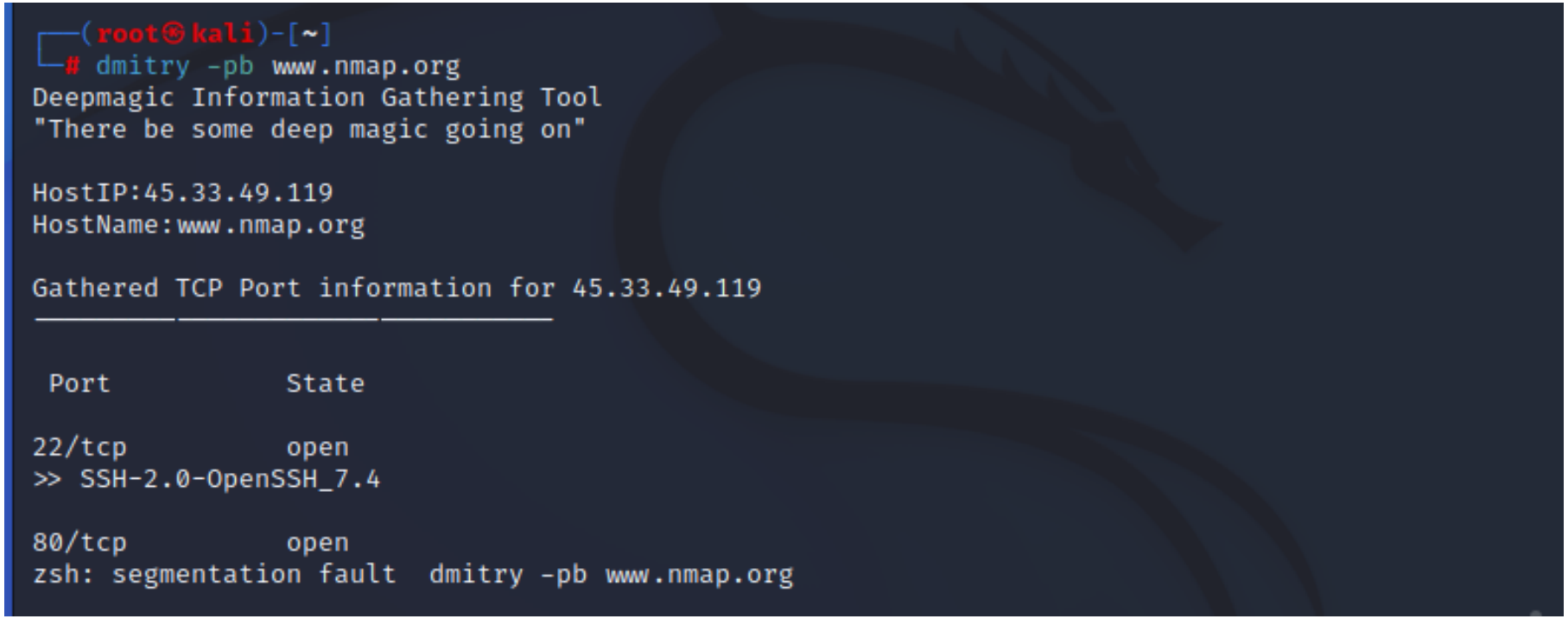
Banner Grabbing

dmitry -w www.nmap.org



Banner Grabbing

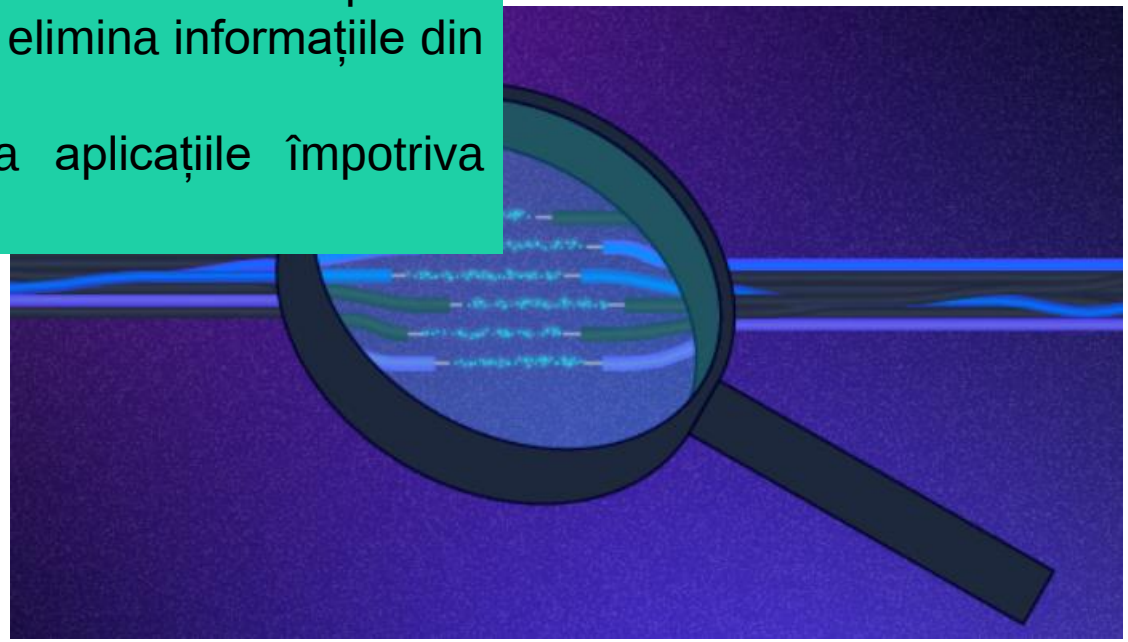
dmitry -pb www.nmap.org



Banner Grabbing

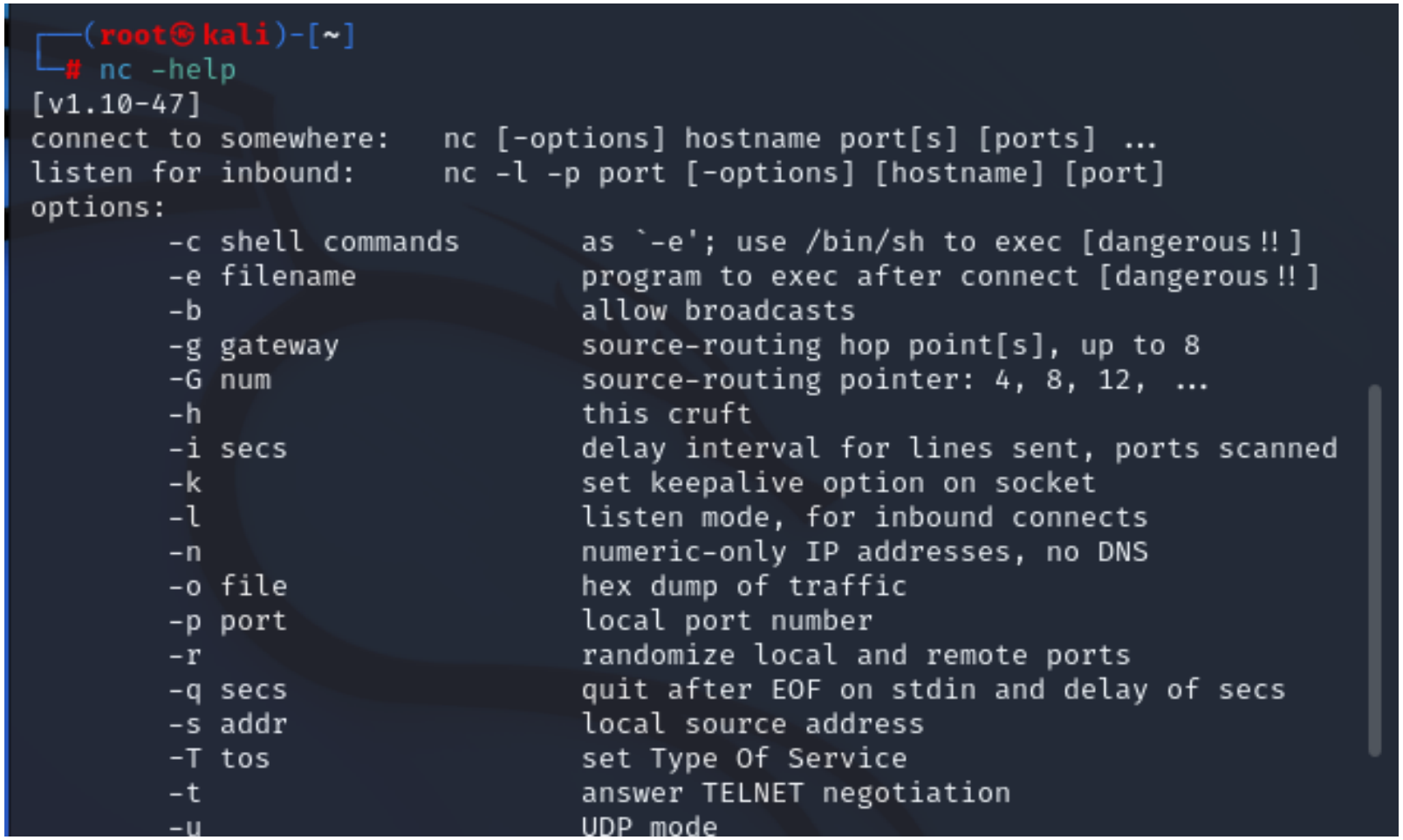
Prevenire

- Restricționarea accesului la serviciile din rețea
- Închiderea serviciilor neutilizate sau inutile care rulează pe gazdele de rețea
- Suprascrierea comportamentului standard de banner al serverului dvs. pentru a ascunde informațiile despre versiune. Administratorii de sistem pot personaliza bannerele implicite, pot configura aplicația sau sistemul de operare al gazdei de rețea pentru a dezactiva bannerele sau pot elimina informațiile din bannere care ar putea oferi atacatorului un avans.
- Update server și sisteme la zi pentru a securiza aplicațiile împotriva exploatărilor de server cunoscute



netcat – un instrument util

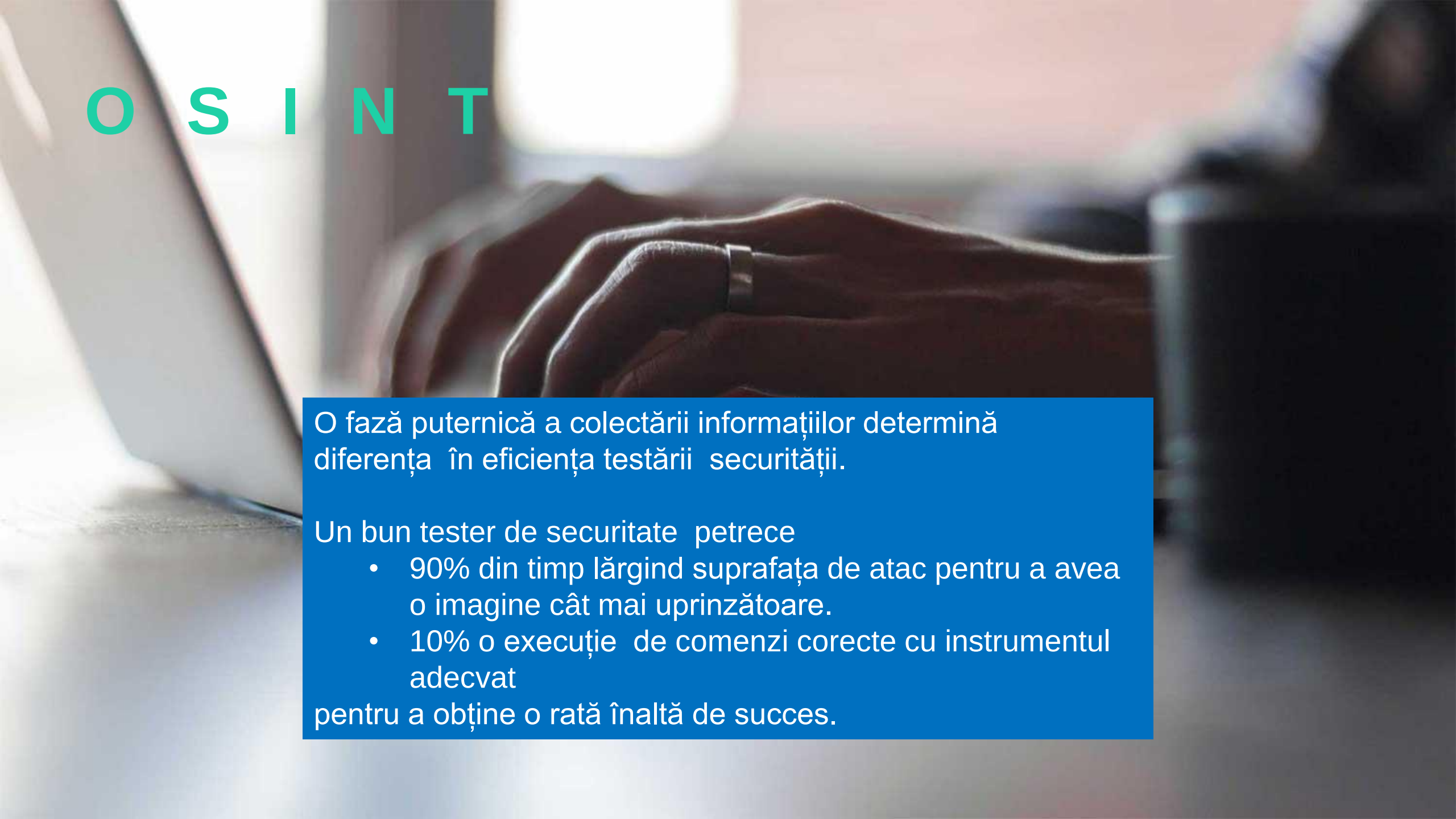
$ **nc -help**



$ **nc**<adresa IP a serverului web țintă > 80

De obicei portul serverului web este 80

O S I N T



O fază puternică a colectării informațiilor determină diferența în eficiența testării securității.

Un bun tester de securitate petrece

- 90% din timp lărgind suprafața de atac pentru a avea o imagine cât mai uprinzătoare.
- 10% o execuție de comenzi corecte cu instrumentul adecvat

pentru a obține o rată înaltă de succes.

OSINT

Rețelele sociale, site-urile publice și serviciile whois fiecare oferă informații fragmentate care prin corelare putem înțelege mai bine afacerea organizației de interes

Colectare de informații

Mai multe aruncări într-o țintă mică, sau
o aruncare într-o tintă mare?

O S I N T

Procesul OSINT este ciclic,
la fiecare iterație colectând informații din ce în ce mai multe și mai rafinate, astfel încât imaginea origanizației de interes devine mai complexă și mai completă, oferind țintele de atac și totodată modalitățile de blocare ale acestor eventuale vulnerabilități.

03

Open Web Application Security Project -OWASP

Top 10 OWASP

1. Injection exploit
    a) SQL, XPATH, etc
2. Cross-Site Scripting (XSS)
3. Broken Authentication and Session Management
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Mai multe aici: https://owasp.org/www-project-top-ten/

Cross-Site Scripting (XSS) Attacks

- Codul *rău intenționat* poate schimba aspectul și funcțile unei aplicații web legitime:
  - Provine din vechile atacuri de phishing, dar mai puțin evidente și mai periculoase pentru utilizator/victimă
  - Mai răspândită, datorită trecerii la aplicații Internet ce folosesc conținut dinamic și JavaScript cu una din cele mai recente tendințe AJAX
- O resursă XSS importantă pentru studiu
  - OWASP Cross-site Scripting (XSS)

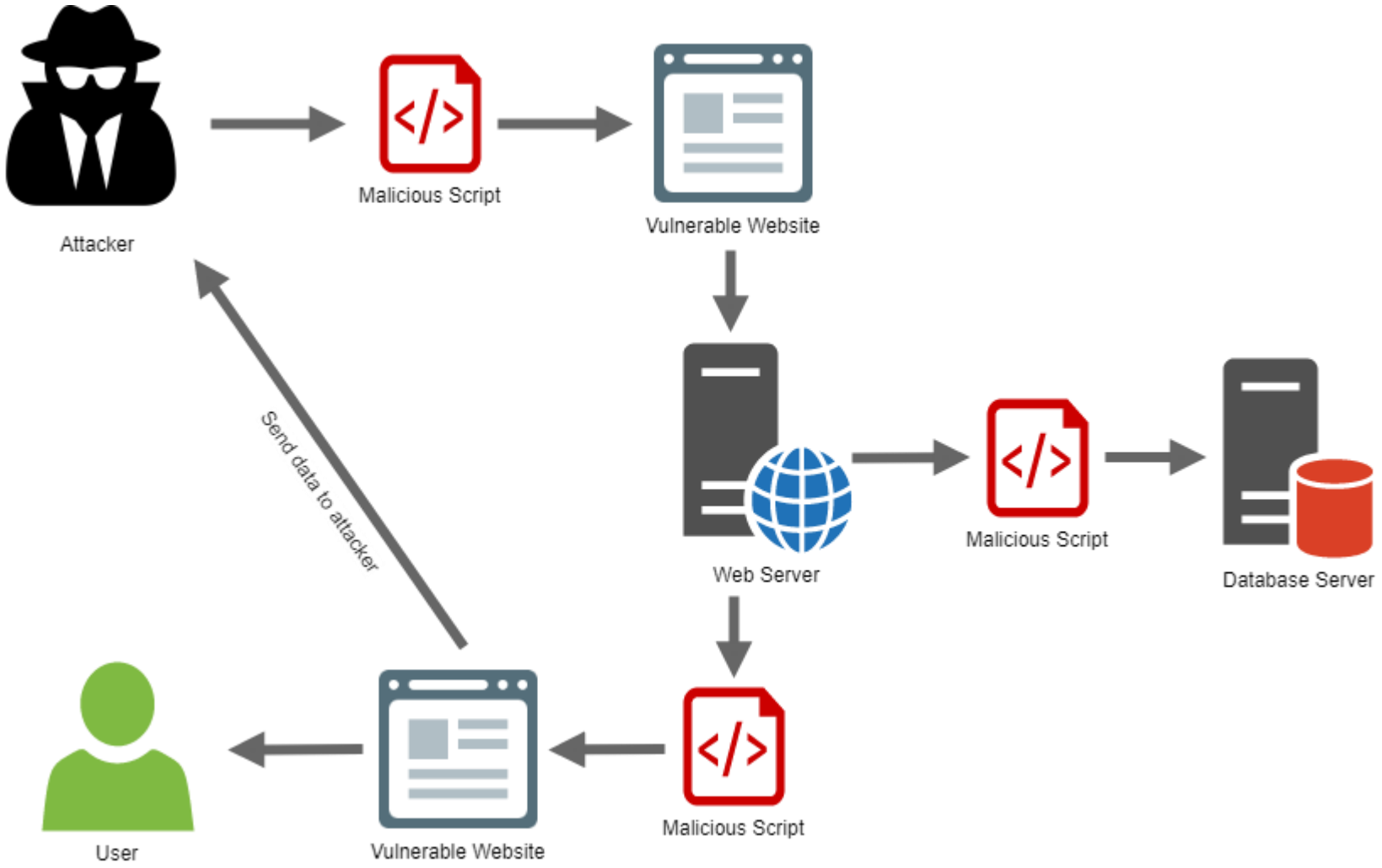
Websites XSS’d

Exemplu:

- Un hacker a reușit să introducă cod JavaScript în secțiunea blogului comunității Obama
  - JavaScript redirecționa utilizatorii către site-ul web Hillary Clinton
    - https://news.netcraft.com/archives/2008/04/21/hacker_redirects_barack_obamas_site_to_hillaryclintoncom.html

O platforma de teste buna este DVWA ce poate fi instalata local.

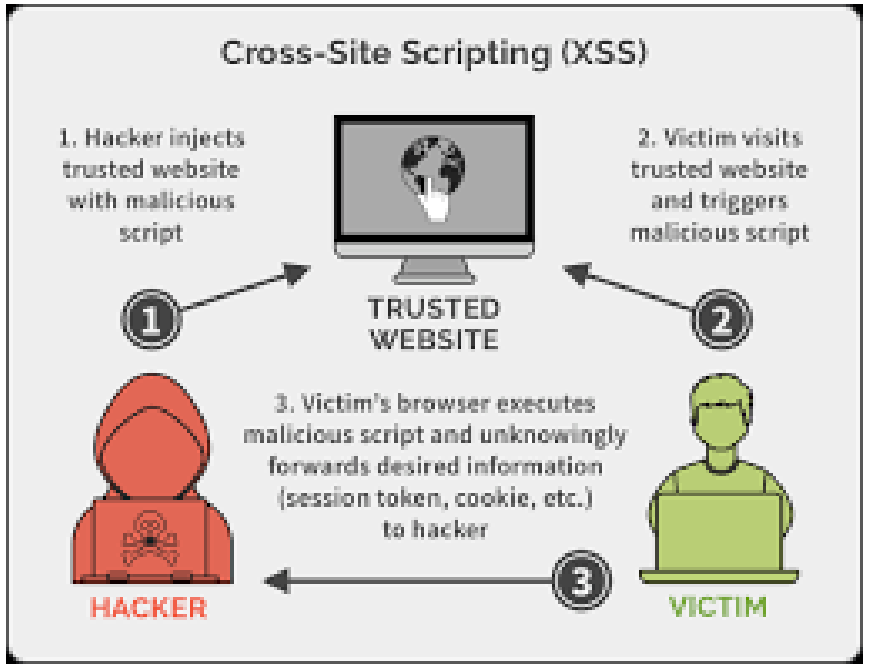
Cross-Site Scripting (XSS) - atac



Imagine: https://dejanstojanovic.net/aspnet/2018/march/handling-cross-site-scripting-xss-in-aspnet-mvc/

Impact XSS

- Datele care se află pe pagina web pot fi trimise oriunde
  - Inclusiv cookie-uri!
- Facilitează multe alte tipuri de atacuri
  - Falsificarea cererilor între site-uri (CSRF), atacuri de sesiune
- Comportamentul site-ului poate fi deturnat



Prevenire atac XSS

- Controlul toturor intrărilor utilizatorului când acestea sunt afișate (Escape)
- Controlul are ca scop convertirea rezultatului în entități html inofensive (termen Escaping)
    - <*script*> devine *<script>*
    - dar va fi afișat ca <*script*>
  - Metode:
    - OWASP ESAPI
    - Java Standard Tag Library (JSTL) <*c:out/*>
- Mai multe aici:

  OWASP XSS Prevention Cheat Sheet

Prevenire atac XSS

- Asigurați-vă că filtrul folosește o abordare pe *lista albă*
  - Filtrele bazate pe *blacklisting* istoric sunt viciate
    - ex: PHP, Ruby on Rails sanitize method
  - Noile scheme de codare pot ocoli cu ușurință filtrele care utilizează o abordare pe lista neagră
- Nu acceptați și afișați intrările nesolicitate
  - Verificarea fiecărui parametru pentru paginile de confirmare
  - Afișarea parametrilor de sesiune/cerere în paginile de eroare

- XSS tutorial: https://www.hacking-tutorial.com/hacking-tutorial/basic-hacking-via-cross-site-scripting-xss-the-logic/

Tutorial:
https://owasp.org/www-pdf-archive/OWASP_-_WebGoat_-_Introduction_to_XSS.pdf

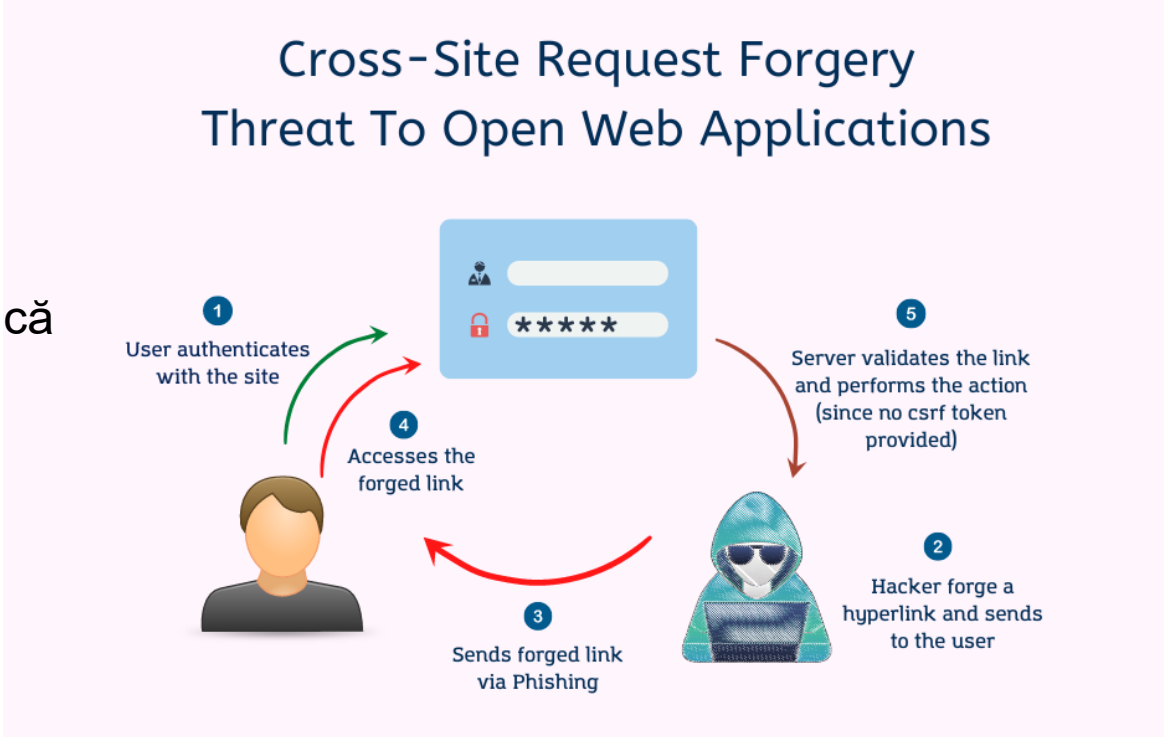
Cross Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) = atac care forțează un utilizator final să execute acțiuni nedorite pe o aplicație web în care este autentificat.
Cu puțin ajutor de inginerie socială (cum ar fi trimiterea unui link prin e-mail sau chat), un atacator poate păcăli utilizatorii unei aplicații web să execute acțiuni alese de atacator. Dacă victima este un utilizator normal, un atac CSRF de succes îl poate forța pe utilizator să efectueze solicitări de schimbare a stării, cum ar fi transferul de fonduri, schimbarea adresei de e-mail și așa mai departe. Dacă victima este un cont administrativ, CSRF poate compromite întreaga aplicație web.

https://owasp.org/www-community/attacks/csrf

Cross Site Request Forgery (CSRF)

- Apare atunci când un utilizator autentificat inițiază, fără să știe, o solicitare
- Solicitarea este tratată ca și cum ar fi intenționată
  - De obicei, se întâmplă fără ca utilizatorul să fie conștient!
- Atacurile CSRF sunt dificil de urmărit
  - Comenzile sunt executate în contextul victimei
  - Solicitarea vine de la adresa IP a utilizatorului, așa că este dificil să vânezi hackerul
- Hackerului i se acordă în esență toate privilegiile utilizatorului
- XSS facilitează CSRF prin „Link Injection”



Imagine: https://www.atatus.com/blog/cross-site-request-forgery-a-threat-to-open-web-applications/

Exempu CSRF

- Un hacker postează pe un panou de mesaje care conține o etichetă de imagine
- <img src= „http://yourbank.com/transfer?to_account=my_account_number&amount=all_of_your_money>

- Un utilizator care nu bănuiește se conectează la yourbank.com și se autentifică

- Apoi utilizatorul vizitează mesajul respectiv

- O solicitare este emisă din browserul victimei către site-ul web al băncii

- Site-ul web al băncii transferă banii utilizatorului în contul hackerului

Exempu CSRF

Here is a GET request for ordering a product in `mybank.com`.

```
GET https://mybank.com/api/send?beneficiary_account=45047580936&amount=100000
```

The request can be embedded into an innocent-looking hyperlink:

```
<a href="https://mybank.com/api/send?beneficiary_account=45047580936&amount=100000"
```

```
<h1> Hurry Up and grab your offer worth $250! </h1>

<form name="auto-submit-form" id="auto-submit-form" action="https://mybank.com/api/

    <input type="hidden" name="beneficiary_account" value="45047580936" />

    <input type="hidden" name="amount" value="100000" />

</form>

<script type="text/javascript">
    window.onload = function() {
        setTimeout(function() {
            submitForm();
        }, 100);

        function submitForm() {
            document.forms["auto-submit-form"].submit();
        }
    }
</script>
```

https://www.atatus.com/blog/cross-site-request-forgery-a-threat-to-open-web-applications/

Prevenire atac CSRF

- Adăugați un mecanism de autentificare secundar
  - Cum ar fi un simbol imposibil/greu de ghicit
- Solicitați o pagină de confirmare înainte de a executa acțiuni potențial periculoase
- Eliminați vulnerabilitățile XSS
- Utilizați POST ca acțiune de formular și acceptați numai cereri POST pe server pentru date sensibile!
  - Solicitările CSRF primite vor eșua, deoarece parametrul se află în adresa URL și nu în corpul postării
- Vă puteți proteja cu Request Policy (extensia Firefox)

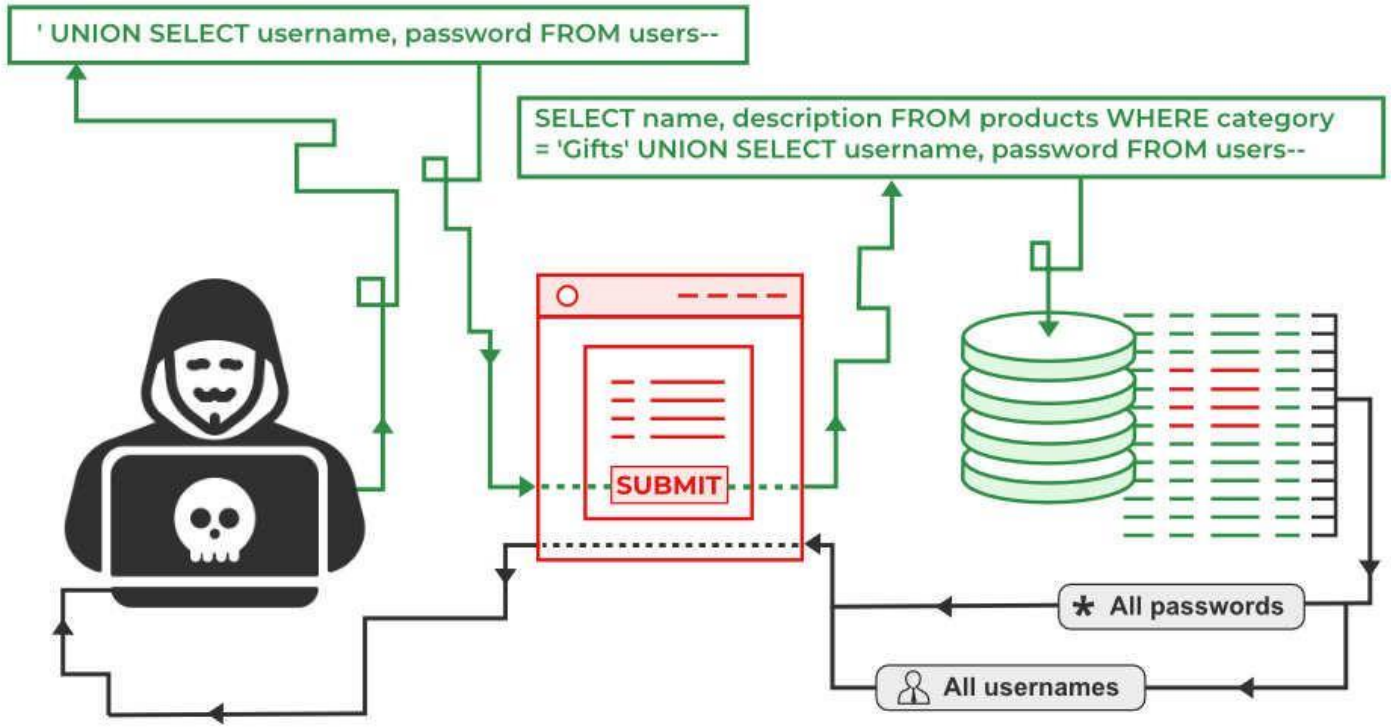
SQL injection

Un atac SQL injection = inserarea sau „injectarea" unei interogări SQL prin datele de intrare de la client în aplicație.
Un exploit SQL de succes poate:

- citi date sensibile din baza de date
- modifica datele bazei de date (Inserare/Actualizare/Ștergere)
- executa operațiuni de administrare pe baza de date (cum ar fi închiderea SGBD)
- recupera conținutul unui anumit fișier prezent în fișierul SGBD
- în unele cazuri, emite comenzi către sistemul de operare.

Atacurile SQL injection = tip de atac de injecție, în care comenzile SQL sunt injectate în intrarea în planul de date pentru a afecta execuția comenzilor SQL predefinite

https://owasp.org/www-community/attacks/SQL_Injection



https://www.geeksforgeeks.org/sql-injection/

SQL Injection

“**SQL injection** tip de atac de injecție, în care comenzile SQL sunt injectate în intrarea în planul de date pentru a afecta execuția comenzilor SQL predefinite.

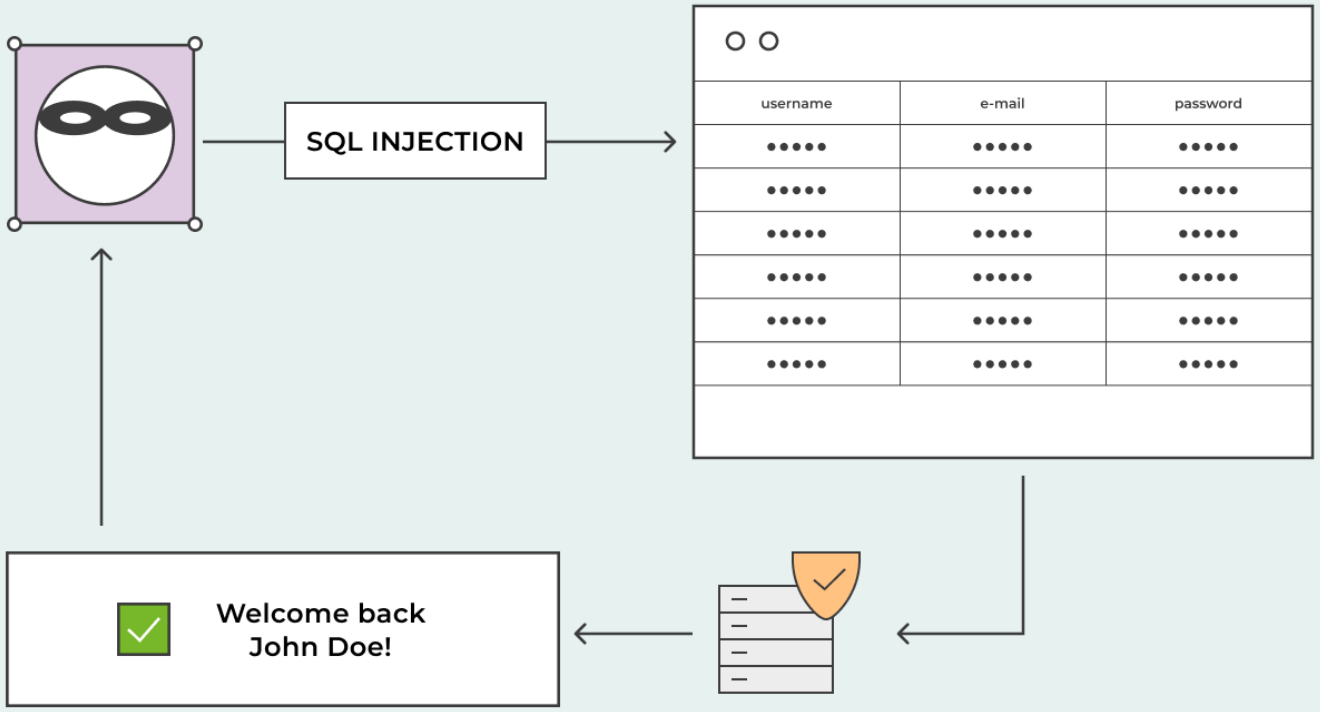


Image: https://www.one.com/en/website-security/what-is-sql-injection

Impact SQL Injection

- În cel mai fericit caz: scurgere de informații
- În funcție de configurație, un hacker poate:
  - Șterge, modifica sau crea date
  - Acorda acces direct hacker-ului
  - Căpăta privilegii sporite și chiar preluare control asupra SO (Sistem de Operare)

SQL Injection

- Login
  - Text albastru = cod utilizator SQL, Text roșu cod extern(injectat), text negru este codul aplicației
  - Login:  Parola: 
- SQL String autentificare, generat dinamic:
  - “SELECT * FROM users WHERE login = ‘” + userName + “’ and password= ‘” + password + “‘”;
- Hacker se loghează ca: **‘ or ‘’ = ‘’; --**
  - SELECT * FROM users WHERE login = ‘’ **or ‘’ = ‘’; --**‘ and password=‘’

SQL Injection

- Hacker-ul crează un cont Windows:
  - SELECT * FROM users WHERE login = ‘’**; exec master..xp_cmdshell 'net users username password /add';--**’ and password= ’’
- Își adaugă drepturi de *administrator*:
  - SELECT * FROM users WHERE login = ‘**'; exec master..xp_cmdshell 'net localgroup Administrators username /add';--**’ and password= ‘’
- Exemple SQL Injection:
  - **https://www.cisa.gov/uscert/sites/default/files/publications/sql200901.pdf**
  - **http://www.unixwiz.net/techtips/sql-injection.html**

Prevenire SQL Injection

- Utilizați secvențe de prevenire (aka Parameterized Queries)
  $id=1234
  “select * from accounts where id = “ + $id
  vs
  “select * from accounts where id =1234”
- Validate intrări (input)
  - Puternică
    - Dacă parametrul *id* este un *număr*, atunci este necesar să verificați dacă intrarea este un număr întreg
  - Validarea logicii
- Evitarea caracterelor (ticks, --, semi-colon, brackets, etc.)

Minimizare impact SQL Injection

- Test:
  Rularea unei aplicații web utilizand un cont „*sa*” (System Administrator) de administrator al sistemului de baze de date este o practică bună?

- Aplicați principiul ***cel mai mic privilegiu***

- Dacă interogarea citește baza de date, nu rulați interogarea cu un cont de utilizator cu permisiuni de actualizare (**dbo, drop** etc.)

Injection mai mult decât SQL

- “Injection Flaw” = termen lipsit de conținut (în sine)
- SQL Injection cel mai des întâlnit
- Alte forme:
  - XPath Injection
  - Command Injection
  - LDAP (Lightweight Directory Access Protocol) Injection
  - DOM (Document Object Model) Injection
  - JSON (Javascript Object Notation) Injection
  - Log Spoofing

și altele …

Exemple SQL atacuri injection

- **Heartland Payment Systems (2008)**: An SQL Injection attack compromised 130 million credit and debit card numbers, making it one of the largest breaches in history.
- **Sony Pictures (2011)**: An SQL Injection vulnerability was used in an attack that led to the leak of thousands of confidential documents, emails, and unreleased films.
- **Yahoo! (2012)**: An SQL Injection attack resulted in a breach of 450,000 Yahoo! user credentials.
- **Drupal (2014)**: A vulnerability in the popular content management system Drupal allowed an SQL Injection attack that potentially affected millions of websites.
- **TalkTalk (2015)**: A British telecom company suffered a major breach with 157,000 customers' details accessed, including bank account numbers, due to an SQL Injection attack.
- **Estonian Central Health Database (2020)**: A massive SQL Injection attack potentially compromised the health records of nearly all of Estonia's citizens.

https://softwarelab.org/blog/sql-injection-examples/

CrunchBase http://www.crunchbase.com/

Facebook https://www.facebook.com/

LinkedIn https://www.linkedin.com/

Twitter https://twitter.com/

Whois https://www.kali.org/tools/whois/

DNSdumpster.com https://dnsdumpster.com/

Sublist3r https://github.com/aboul3la/Sublist3r

SAM: System for Award Management

https://www.sam.gov/

Referințe

Mulțumesc pentru atenție !

dorin.iordache@365.univ-ovidius.ro