

# **UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREȘTI**

Facultatea de Științe Aplicate  
Teoria Codării și Stocării Informației



Tema proiect

Aplicație mobilă pentru filtrarea traficului web  
pe dispozitive mobile (Android)

Masterand

Sergiu-Ionuț-Andrei GHERMAN

București 2026

# Cuprins

1.	Introducere .....	4
1.1.	Contextul securității aplicațiilor web .....	4
1.2.	Prezentarea aplicației WebGoat.....	4
2.	Fundamente teoretice privind securitatea web .....	4
2.1.	Principii generale de securitate .....	4
	2.2.Modelul OWASP și importanța sa .....	4
	2.3.Cele mai comune vulnerabilități web (OWASP Top 10).....	4
	• SQL Injection.....	4
	• Cross-Site Scripting (XSS) .....	4
	• Broken Authentication .....	4
	• Broken Access Control .....	4
	• Security Misconfiguration .....	4
	• Alte vulnerabilități relevante.....	4
3.	Descrierea mediului de lucru .....	4
3.1.	Instalarea și configurarea WebGoat .....	4
3.2.	Instrumente utilizate în testare (Burp Suite, OWASP ZAP, browser tools etc.).....	4
3.3.	Setări și arhitectura aplicației .....	4
4.	Analiza vulnerabilităților identificate în WebGoat.....	4
4.1.	Metodologia de testare .....	4
4.2.	Demonstrații practice ale vulnerabilităților.....	4
	• SQL Injection – scenariu, exploatare, remediere .....	4
	• Cross-Site Scripting (XSS) – scenariu, exploatare, remediere .....	4
	• Broken Authentication – scenariu, exploatare, remediere .....	5
	• Insecure Deserialization.....	5
	• Directory Traversal .....	5
	• Alte vulnerabilități testate .....	5
4.3.	Impactul potențial al vulnerabilităților .....	5
5.	Recomandări și bune practici de securitate .....	5
5.1.	Prevenirea atacurilor web .....	5
5.2.	Configurarea corectă a aplicațiilor.....	5
5.3.	Utilizarea instrumentelor automate de audit .....	5
5.4.	Implementarea unui proces de securitate continuă .....	5
6.	Concluzii .....	5
6.1.	Rezumatul rezultatelor .....	5
6.2.	Lecții învățate.....	5
6.3.	Directive viitoare de îmbunătățire .....	5
7.	Bibliografie.....	5

## 1. Introducere

Dezvoltarea accelerată a tehnologiilor mobile și creșterea semnificativă a numărului de aplicații utilizate zilnic pe smartphone-uri au determinat apariția unor noi provocări în domeniul securității informaticе. Dispozitivele mobile sunt permanent conectate la internet, folosind atât rețele Wi-Fi publice, cât și conexiuni mobile, ceea ce le expune riscurilor precum accesarea de site-uri malicioase, atacuri de tip phishing, colectarea neautorizată de date personale sau comunicarea excesivă a unor aplicații cu servere externe necunoscute.

Pentru desktop-uri există instrumente mature pentru analiză și diagnosticare a traficului de rețea, cum ar fi Wireshark, tcpdump sau firewall-uri avansate. În schimb, pe platforma Android accesul la traficul de rețea este limitat de politicile de securitate ale sistemului de operare, iar utilizatorii obișnuiți nu pot intercepta pachetele fără drepturi speciale (root).

Scopul acestui proiect este realizarea unei aplicații Android care simulează, într-o manieră sigură și controlată, un mecanism de monitorizare și filtrare a traficului web, folosind un VPN local software. Aplicația permite utilizatorului să observe cererile DNS generate de dispozitiv și să blocheze accesul către anumite domenii web prin intermediul unei liste de tip blacklist. Această abordare este realistă și utilizată inclusiv în soluții comerciale de tip parental control, ad-blocking sau protecție împotriva malware-ului.

## 2. Obiectivul proiectului

Obiectivul general al proiectului este proiectarea și implementarea unei aplicații mobile funcționale care demonstrează concepe fundamentale de rețelistică, urmărirea traficului de date și programare Android.

Obiectivele specifice sunt:

- Implementarea unui serviciu VPN local care să permită interceptarea controlată a traficului de rețea.
- Identificarea și procesarea pachetelor DNS pentru extragerea numelor de domenii accesate.
- Realizarea unui mecanism de blocare a domeniilor bazat pe o listă configurabilă de domenii blocate.
- Afisarea în timp real a evenimentelor de rețea și a cererilor.

## 3. Tehnologii utilizate

Aplicația este dezvoltată folosind Android Studio și limbajul Java. Android SDK oferă clasele necesare pentru gestionarea activităților, serviciilor, permisiunilor și interacțiunii cu rețea.

Interceptarea traficului este realizată prin clasa VpnService, care creează un tun virtual de rețea. Pachetele sunt analizate la nivel IPv4 și UDP, fiind urmărite în special cererile DNS (port 53). Serverul DNS public Google (8.8.8.8) este utilizat pentru forward-ul cererilor valide. Setările aplicației, precum lista domeniilor blocate sunt salvate folosind "SharedPreferences", asigurând păstrarea configurațiilor între sesiuni.

## 4. Arhitectura aplicației

Aplicația este structurată modular, având două componente principale:

- **MainActivity** – responsabilă pentru interfața utilizator și gestionarea interacțiunilor.
- **CaptureVpnService** – serviciul care creează VPN-ul și procesează traficul.

Fluxul aplicației:

Utilizatorul pornește VPN-ul din interfață-telefonul solicită permisiunea (la prima rulare)-VPN-ul pornește-Cererile DNS sunt interceptate-domeniile sunt afișate. După introducerea unui domeniu în blocked list acestea sunt afișate în interfață, iar dacă se încearcă accesarea unui domeniu blocat pagina web nu se încarcă, iar în log-uri apare numele domeniului blocat însoțit de un mesaj.

## 5. Funcționarea VPN-ului local

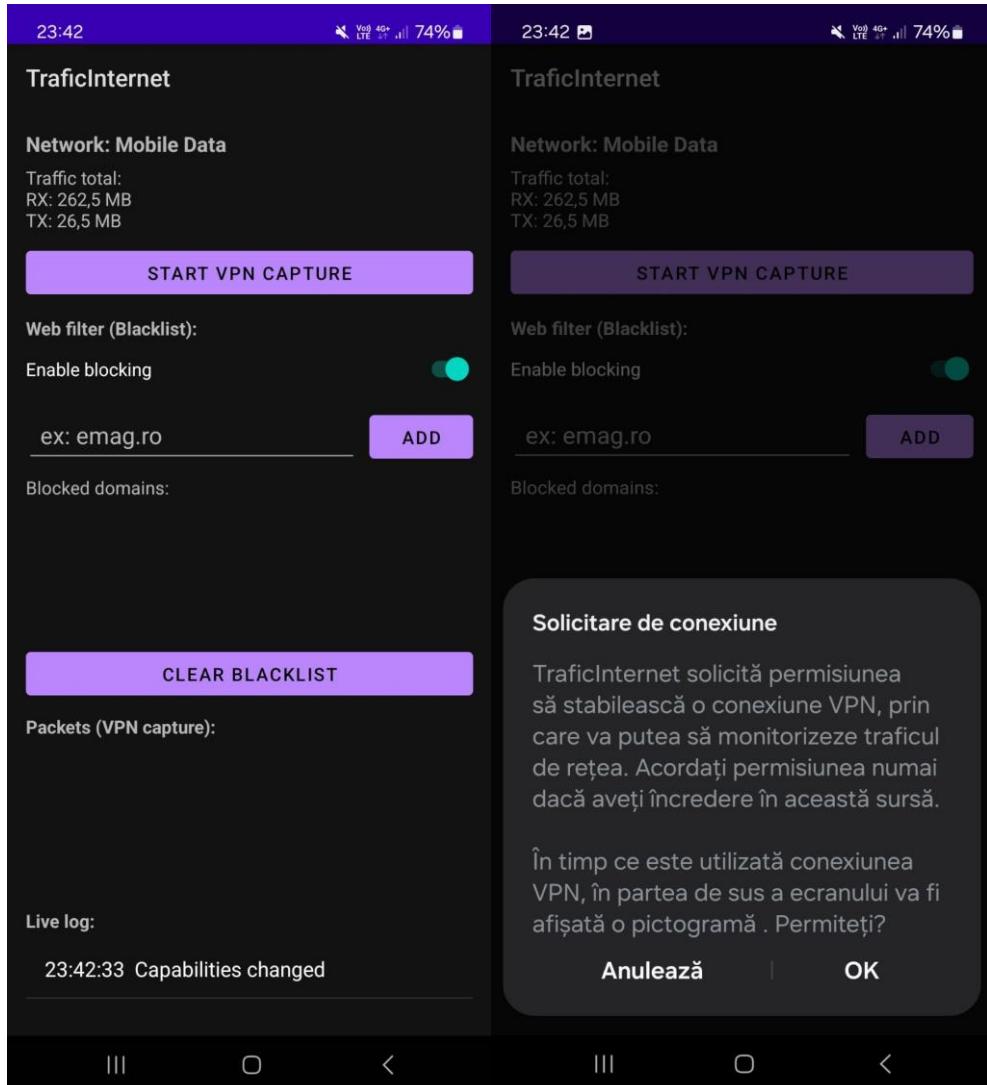
Prin intermediul clasei VpnService, aplicația creează o interfață virtuală de rețea cu o adresă IP internă. Dispozitivul direcționează cererile DNS prin acest tunel, permitând aplicației să analizeze pachetele înainte ca acestea să ajungă la serverul DNS extern.

Doar traficul DNS este redirecționat prin VPN, în timp ce restul traficului de internet circulă normal. Această abordare minimizează impactul asupra performanței și evită întreruperea accesului la internet.

La recepționarea unui pachet DNS, aplicația extrage numele domeniului din structura protocolului DNS. Domeniul este normalizat și verificat în lista de domenii blocate. Dacă domeniul se află în blacklist, aplicația construiește un răspuns DNS de tip NXDOMAIN, indicând că domeniul nu există. Browser-ul sau aplicația nu va putea rezolva adresa IP și accesul va fi blocat. Dacă domeniul nu este blocat, cererea este forwardată către serverul DNS public, iar răspunsul este retransmis către dispozitiv.

## 6. Interfața utilizatorului

La lansarea aplicației se apasă butonul “Start VPN capture”, după care apare notificarea pe care apăsăm “Ok”



Se pornește serviciul VPN, cum se observă și în log-uri. Dacă se încearcă accesarea paginii Emag totul funcționează normal.

The image consists of three vertically stacked screenshots from a mobile application, likely a browser or a specialized tool, displayed on a dark-themed interface.

**Screenshot 1 (Top): TraficInternet**

- Network:** Mobile Data
- Traffic total:** RX: 262,5 MB TX: 26,5 MB
- START VPN CAPTURE** button (purple)
- Web filter (Blacklist):**
  - Enable blocking (switch is on)
  - Text input: ex: emag.ro
  - ADD** button (purple)
- Blocked domains:** (empty)
- CLEAR BLACKLIST** button (purple)
- Packets (VPN capture):**
  - TCP 10.0.0.2:37514 -> 10.0.0.1:853 (60B)
  - DNS query: mtalk.google.com
  - DNS query: matt-mini.facebook.com
- Live log:** 23:43:01 VPN started

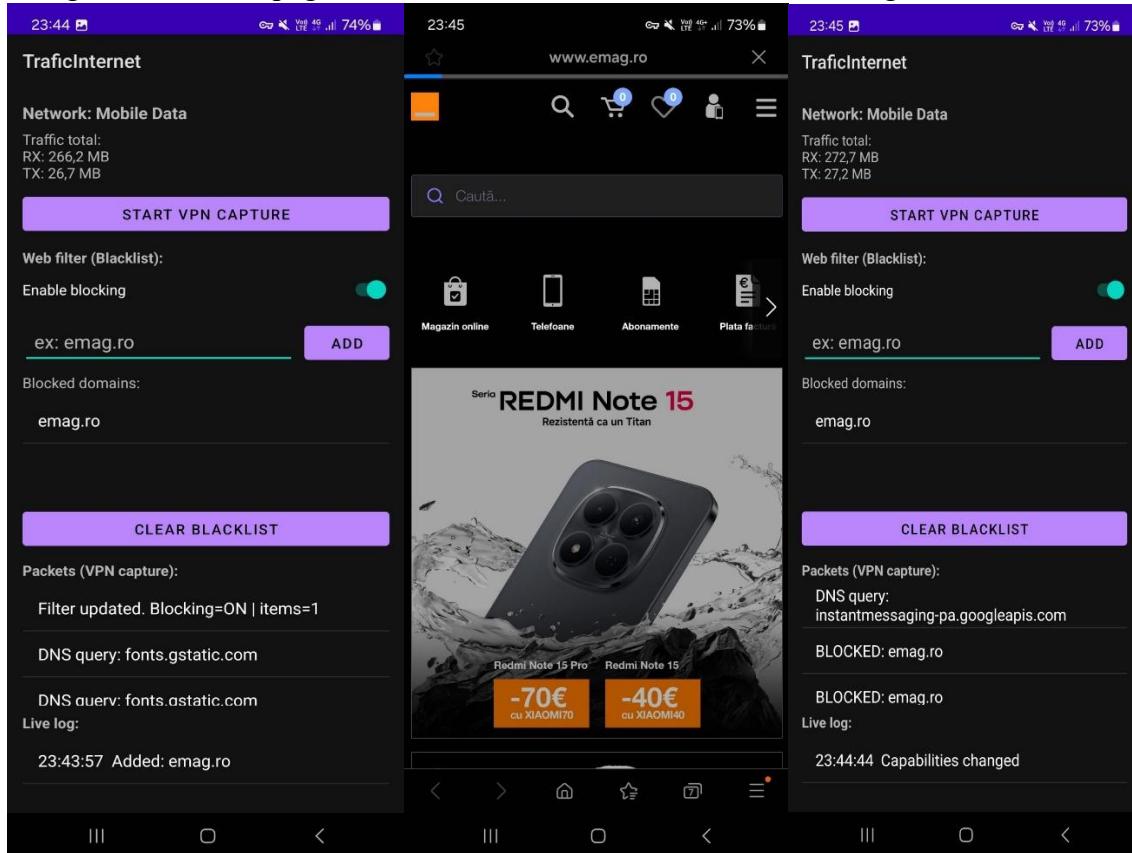
**Screenshot 2 (Middle): www.google.com**

- Search bar: emag
- Navigation tabs: Modul AI, Toate, Produse, Site-uri cu produse, Locații
- Filters: Data postării, Tipul locului de muncă, Deschis
- Location: București · Alege zona
- Result: eMAG (https://www.emag.ro)
  - Thumbnail: eMAG logo
  - Text: Ai libertatea sa alegi din milioane de produse IT, electronice si electrocasnice, gadgeturi, jucarii, imbracaminte si incaltaminte la Super Pret sau cu ...
- Category links:
  - Electronice & Electrocasnice
  - Toate departamentele
  - Haine & Accesorii
  - Casa & Gradina
  - Telefoane Mobile. Afla Preturile!

**Screenshot 3 (Bottom): www.emag.ro**

- Header: -50 lei la prima comandă în app
- Logo: eMAG
- Search bar: Începe o nouă căutare
- Banner: #MultiDeals, Oferte ai combinat, EXTRA ai activat, până la -20% extra
- Navigation: Ofertele eMAG, Genius, Easy BuyBack, Genius D...
- Category icons: Ofertele eMAG, Resigilate, IT, Mobile & Gaming, Electronice & ..., Casa & Gradina
- Cookie consent banner:
  - Salut! Noi, la eMAG, dorim să îți oferim o experiență cât mai plăcută.
  - Folosim cookie-uri și tehnologii similare pentru:
    - funktionarea corectă a site-ului,
  - Accept toate**
  - Refuză toate**
  - Administrează preferințele**

Se introduce în blacklist domeniul Emag (emag.ro) și încercăm să accesăm iar pagina de la Emag, observând că pagina nu se mai încarcă, lucru observat și în log-uri.



O limitare a aplicației nu poate intercepta conținutul criptat HTTPS și nu poate identifica aplicația care generează traficul. Blocarea este realizată exclusiv la nivel DNS. Aceasta ar poate fi extinsă prin adăugarea unor funcționalități precum export de loguri, whitelist și filtrare avansată.