

SAÉ 3.02 - Développer des applications communicantes

Mohamed Droussi
Johan Abdallah
Nicolas Nonnenmacher
Mathis Desmet

Sommaire

- Définition Du Problème
- Gestion du projet
- Outils utilisés
- Présentation de notre solution
- Démonstration

Définition du problème

Concevoir un système capable de :

- **Scanner** les failles d'un réseau.
- **Visualiser** les résultats sur un tableau de bord Web.
- **Consulter** ses informations via une application Android.

Gestion Du projet

Mise en place d'un RACI pour se répartir les taches

SAE 302	MOHAMED	MATHIS	JOHAN	NICOLAS
Squelette du programme java	A	I	R	C
Maquette de l'app Android	C	I	A	R
Maquette Site Web	I	R	A	C
Schema Base de Données	A	I	R	A
Communication web <-> android	R	C	A	I
Creation App Android java	R	C	A	I
Creation Site Web	C	I	R	A
Importation Base de Données	C	A	R	I
Creatopn App Java pour recherche failles (kali)	A	I	R	C

Outils utilisées



Frontend Mobile

- › **Android Studio** Environnement de développement et compilation.
- › **Java (Android)** Logique métier, Intents et Adaptateurs.
- › **XML** Design des interfaces (Layouts, CardViews).



Réseau & Sécurité

- › **Nmap** Moteur de scan de ports et vulnérabilités.
- › **HTTP / JSON** Protocole d'échange App ↔ Serveur.
- › **SHA-256** Hachage sécurisé des mots de passe.



Backend & Données

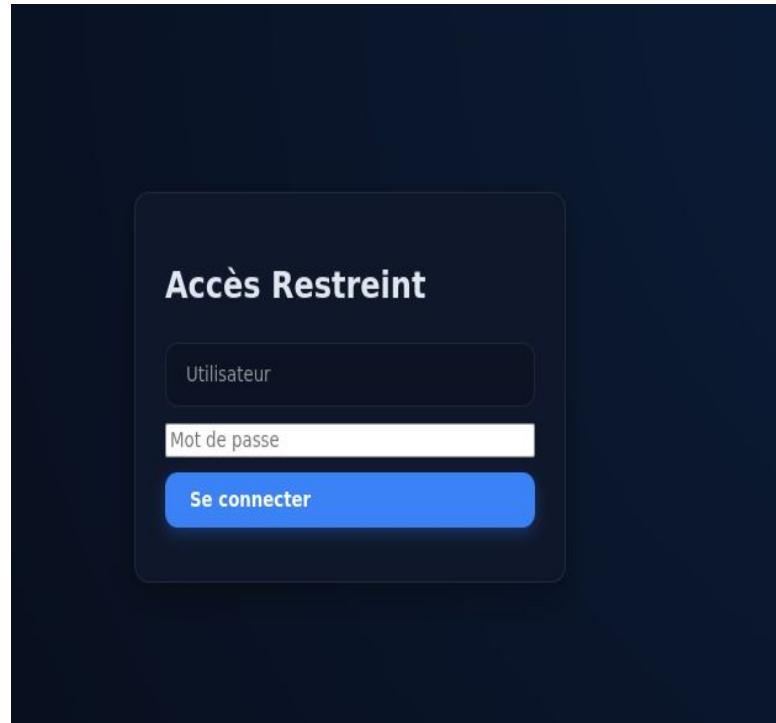
- › **Serveur Java** Pont entre le mobile et le système (Port 8080).
- › **SQLite** Base de données locale (Fichier bd .db).
- › **JDBC** API de connexion Java vers SQLite.



Administration Sys.

- › **VM Debian** Environnement d'hébergement du scanner.
- › **Apache** Serveur Web et redirection de flux.
- › **HTML / CSS** Interface Web d'administration.

Présentation de notre solution



Page accueil site

The screenshot shows a dark-themed web application interface. At the top left is a blue rounded square icon containing the letters "SZ". To its right is the title "Scanner vulnérabilités" in white. Further to the right is a red rectangular button labeled "Déconnexion". Below the title, the text "Connecté en tant que admin" is displayed. In the center, there is a search bar with the placeholder "Ex: 192.168.1.10" and two blue buttons: "Lancer le scan" and "Voir vulnérabilités". A note below the search bar says "Tape l'IP puis clique sur Lancer le scan.". At the bottom left, the text "Projet SAE302 — interface simple" is visible.

Scanner vulnérabilités

Connecté en tant que **admin**

Ex: 192.168.1.10

Lancer le scan Voir vulnérabilités

Tape l'IP puis clique sur **Lancer le scan**.

Projet SAE302 — interface simple

Listes des vulnérabilités

10.11.10.27:22

HIGH

Date du scan : 2026-01-03 17:58:49

| CVE-2025-61984 3.6 https://vulners.com/cve/CVE-2025-61984

10.11.10.27:80

LOW

Date du scan : 2026-01-03 17:58:49

B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150 3.6 https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150

EXPLOIT

4C6E2182-0E99-5626-83F6-1646DD648C57 3.6 https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-1646DD648C57

EXPLOIT

- PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*

Détails du scan

SZ Scanner vulnérabilités

Connecté en tant que **admin**

Déconnexion

Vulnérabilités

Récupère les dernières vulnérabilités depuis la base

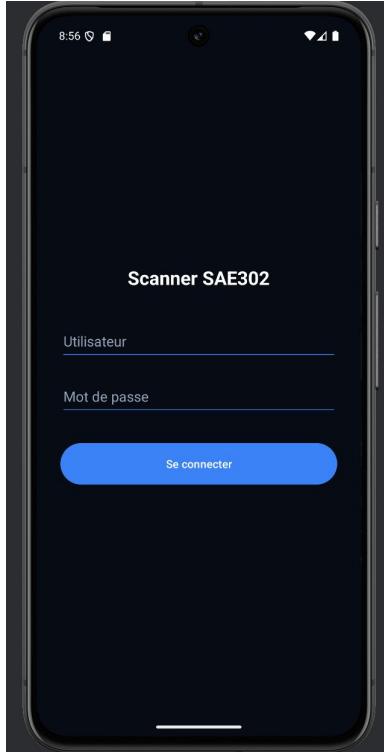
Rafraîchir **Lancer un scan**

10.11.10.27:22 HIGH

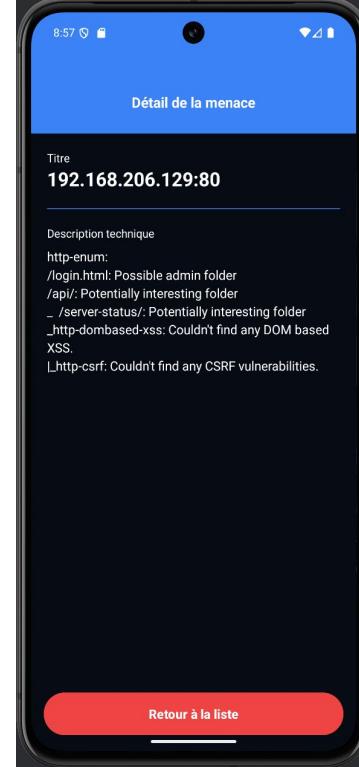
Date du scan : 2026-01-03 17:58:49

```
vulners:  
cpe:/a:openbsd:openssh:9.2p1:  
PACKETSTORM:179290 10.0 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT*  
1EEC8894-D2F7-547C-827C-915BE866875C 10.0 https://vulners.com/githubexploit/1EEC8894-  
D2F7-547C-827C-915BE866875C *EXPLOIT*  
PACKETSTORM:173661 9.8 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*  
F0979183-AE88-53B4-86CF-3AF0523F3807 9.8 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  
*EXPLOIT*  
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
```

Interface Android



Scanner réseau		
192.168.206.129:80		High
2026-01-03 15:40:23		
192.168.206.129:80		High
2026-01-03 15:40:23		
192.168.206.129:80		High
2026-01-03 15:40:23		
192.168.206.129:80		High
2026-01-03 15:40:23		
192.168.206.129:80		High
2026-01-03 15:40:23		
192.168.206.129:80		Low
2026-01-03 15:40:23		
192.168.206.129:8080		High
2026-01-03 15:40:23		
192.168.206.129:8080		High
2026-01-03 15:40:23		
192.168.206.129:8080		Low



Démonstration