Pen-test

1. Introduction

Date du test d'intrusion : 27/10/2024

Client : Gothime Manager

Testeurs : MAR_10

Objet du test : Ce test d'intrusion vise à évaluer la sécurité du site web et de l'API associée afin d'identifier et de documenter les vulnérabilités existantes et d'orienter les recommandations de sécurité.

2. Résumé Exécutif

Le test d'intrusion a permis de détecter plusieurs vulnérabilités dans l'application web et l'API. Ces vulnérabilités peuvent permettre des accès non autorisés, des manipulations de données sensibles, ou une compromission du système.

Voici un résumé des résultats :

Vulnérabilités critiques :

- Aucune détection de brute-force
- Informations envoyées en clairs lors des requêtes

Vulnérabilités majeures :

- La base de donnée hébergée sur la même machine que le web
- Lors d'une authentification, les identifiants en clairs sont envoyées au serveur

Vulnérabilités modérées :

- Aucun filtre lors du scan des QRCode

Les principales recommandations incluent l'amélioration de la validation des entrées, la sécurisation des configurations serveur, et la mise à jour des composants logiciels.

3. Méthodologie

Les tests ont été réalisés selon les méthodes d'analyse suivantes :

1. **Reconnaissance passive et active :** Collecte d'informations sur le site et l'API.
2. **Scan de vulnérabilités :** Analyse des vulnérabilités connues.
3. **Exploitation des vulnérabilités :** Tentative d'exploitation des faiblesses détectées.
4. **Post-exploitation :** Test de persistance et d'escalade de privilèges.
5. **Rapport et recommandations :** Documentation des vulnérabilités et recommandations de sécurité.

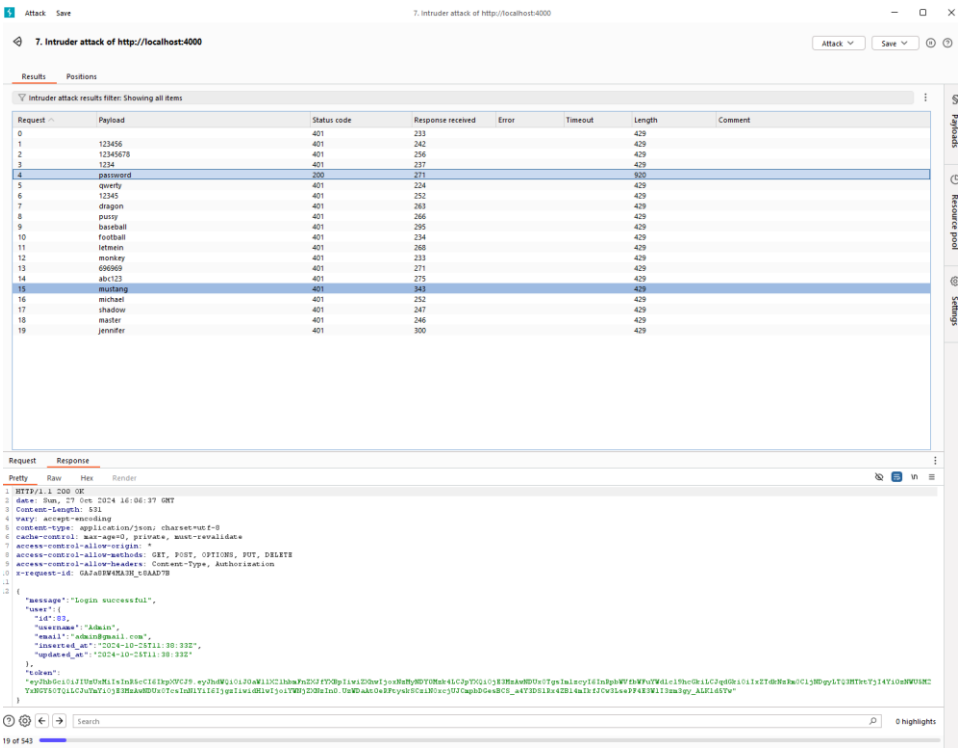
4. Détails des Vulnérabilités

4.1 Vulnérabilités Critiques

4.1.1 Absence de détection de force brute

Description : L'application ne détecte pas les tentatives de force brute,

permettant la récupération non autorisée des identifiants administrateurs

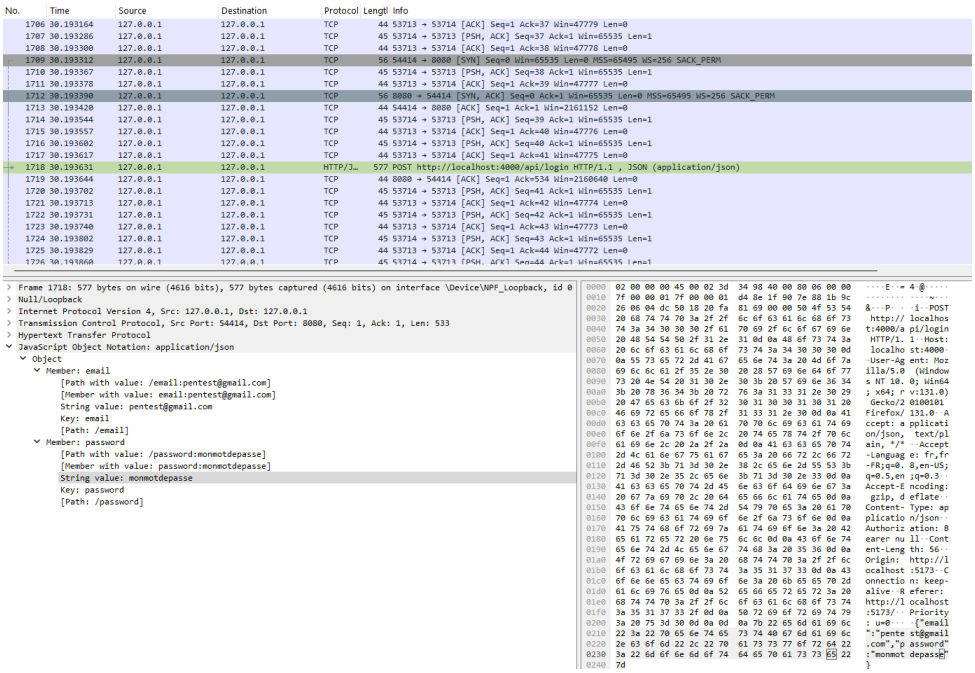


Impact : Risque élevé d'accès non autorisé aux comptes administrateurs et aux données sensibles.

Recommandation : Mettre en place un système de détection et de blocage des tentatives de force brute, ainsi qu'une politique de mots de passe robuste.

4.1.2 Les requêtes d'authentification sont envoyées en clairs

Description : Lors de l'authentification, la requête de login est envoyé en clair, avec les identifiants sans aucune obfuscation.



Impact : Risque élevé de sniffing du réseau et de récupération des identifiants.

Recommandation : Mettre en place un système directement dans le front-end qui obfusque (ou hashage) les identifiants avant de les envoyées au serveur web.

4.1.2 Authentification Insecure

Description : Le mécanisme d'authentification de l'API permet la réutilisation des jetons expirés, ce qui peut permettre un accès non autorisé.

Impact : Risque d'accès non autorisé aux comptes d'utilisateurs et aux données sensibles.

Recommandation : Utiliser des jetons avec un délai d'expiration court et activer

le renouvellement sécurisé des jetons

4.2 Vulnérabilités Majeures

4.2.1 Base de données hébergée sur la même machine que le serveur web

Description : La base de données et le serveur web sont hébergés sur la même machine, ce qui compromet la sécurité, l'isolation des données, mais compromet aussi la performance et la disponibilité de l'application web.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.5 -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 11:3
Nmap scan report for xps (192.168.1.5)
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
4000/tcp open  http-proxy Ncat http proxy (Nmap 4.85BETA1 or
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later
8081/tcp open  http       PHP cli server 5.5 or later (PHP 7.
SF-Port5432-TCP:V=7.94SVN%I=7%D=10/27%Time=671E5D96%P=x86_64-
SF:r(SMBProgNeg,90,"E\0\0\0\x8fSFATAL\0VFATAL\0C0A000\0Munsup
SF:ntend\x20protocol\x2065363\.19778:\x20server\x20supports\x
SF:x203\.0\0Fbackend_startup\.c\0L679\0RProcessStartupPacket\

Nmap done: 1 IP address (1 host up) scanned in 180.26 seconds
```

Impact : Risque accru de compromission totale du système en cas d'intrusion.

Recommandation : Séparer physiquement la base de données du serveur web et mettre en place un réseau segmenté pour isoler les composants critiques.

4.3 Vulnérabilités Modérées

4.3.1 Absence de filtrage lors du scan du QRCode

Description : L'application ne filtre pas les données lors du scan des QR codes, ce qui peut permettre l'injection de contenu malveillant.

Impact : Risque d'exécution de code arbitraire ou d'accès non autorisé aux données.

Recommandation : Implémenter une validation stricte des données issues des QR codes et limiter les actions possibles après un scan.

5. Recommandations Générales

- **Renforcer l'authentification :** Activer une authentification multi-facteurs pour les comptes utilisateurs.
- **Chiffrer les données sensibles :** Utiliser HTTPS et chiffrer les données sensibles lors de leur transport (requête client → serveur & serveur → client)
- **Surveillance et Alertes :** Mettre en place un système de détection d'intrusion pour surveiller les comportements anormaux et détecter rapidement toute tentative d'intrusion.

6. Conclusion

Le test d'intrusion a révélé plusieurs faiblesses de sécurité qui nécessitent une action immédiate pour protéger les données des utilisateurs et maintenir la sécurité de l'application. Les correctifs recommandés devraient être appliqués rapidement, et un suivi de sécurité périodique est conseillé pour détecter d'éventuelles nouvelles vulnérabilités.

7. Annexes

Liste des outils utilisés

- Burp Suite
- Wappalazer
- OWASP ZAP
- Nmap
- Dirbuster & Gobuster
- Metasploit