



Information Entreprise

Adresse

Tel

LOGO CLIENT

CLIENT

CONTEXTE

DATE

Rapport d'Audit Sécurité

EvilCorp - Application Web

Référence : NUXIA/XXXX/Pentest/2020/06

Auteurs : Nuxia - Consultant

Dernière maj : 15/03/2021

Classification : **Strictement Confidentiel**

Informations du document

Rapport d'audit sécurité	
Version	1.0
Référence	ALPHORM/XXXX/Pentest/2021/06
Dernière modification	XX/XX/XXXX
Auteurs	Alphorm
Relecteurs	Alphorm
Validateurs	XXXXXXXX

Versions du document

Version	Date	Description	Auteurs
0.1	26/05/2020	Première version	Alphorm
0.2	29/05/2020	Listing des vulnérabilités	Alphorm
1.0	07/06/2020	Version finale	Alphorm

Table des matières

1. Contexte et objectif	4
1.1. Introduction	4
1.2. Objectif	4
1.3. Périmètre et prérequis de tests.....	4
1.3.1. Périmètre	4
1.3.2. Prérequis	4
2. Synthèse managériale	5
3. Synthèse technique	6
3.1. Inventaire des vulnérabilités.....	6
3.2. Matrice de risque	6
4. Identification et exploitation des vulnérabilités.....	8

1. Contexte et objectif

1.1. Introduction

Ce document représente le rapport d'audit effectué sur l'application **XXXX**. Il décrit les tests d'intrusion réalisés, les différentes vulnérabilités identifiées, pour enfin conclure avec les recommandations de sécurité à prendre en compte pour améliorer le niveau de sécurité de l'application.

1.2. Objectif

L'objectif principal est de faire un contrôle de l'état de sécurité actuel et de vérifier le niveau de criticité et d'exploitabilité des vulnérabilités identifiées.

1.3. Périmètre et prérequis de tests

1.3.1. Périmètre

Le périmètre **XXXXX** testé regroupe les composants suivants :

Application	URL concernée
Console d'administration	XXXX
Plateforme utilisateur	XX
Web Services	XXXX

1.3.2. Prérequis

Ci-dessous, les prérequis utilisés pour interagir avec l'application audité.

- 1 comptes utilisateur.
- 1 comptes administrateurs.

2. Synthèse managériale

L'audit du périmètre **XXXX** a été mené par l'équipe ALPHORM du XX Avril XX au XX Septembre XXX.

Les différents tests réalisés ont permis d'exploiter des vulnérabilités critiques permettant d'accéder à des informations sensibles. Au total, **15 vulnérabilités** ont été identifiées dont **10 critiques**, **2 majeures** et **3 moyennes**. Cela est causé principalement par :

- XXX
- XXX
- XX

Néanmoins, plusieurs points positifs ont été constaté lors de cet audit :

- XXXX
- XXXX
- XXX
- XXX

Le tableau ci-dessous récapitule le nombre et la criticité des vulnérabilités identifiées :

				RISQUE
EFFORT DE REMEDIATION	Faible			Critique
				Majeur
				Moyen
				Faible
	10			
	2			
	2	1		

3. Synthèse technique

3.1. Inventaire des vulnérabilités

Réf.	Vulnérabilité	Niv. de risque	Recommandation
#1	Exposition des adresses XXX	Critique	<p>Il est fortement recommandé de vérifier de l'exactitude des adresses mail et mot de passe recueillis et d'essayer de mettre à jour le plus rapidement possible les comptes compromis.</p> <p>Mettre en place un système de renouvellement de mot de passe tous les X temps.</p>
#2	Référence directe non sécurisée à un objet (IDOR)	Critique	<p>Implémenter des contrôles d'accès à toutes les ressources. L'utilisateur doit être autorisé pour accéder aux informations souhaitées avant que le serveur ne les lui fournisse.</p> <p>Il est également recommandé d'utiliser des hashes (qui sont plus difficile à énumérer) comme référence au lieu des entiers incrémenté.</p>
#3	Téléchargement de fichier malveillant sur le serveur	Majeur	Renforcer les mécanismes de vérifications des fichiers téléchargés sur le serveur du côté serveur en plus de la sécurité mis en place du côté client.
#4	Falsification des requêtes intersites (CSRF)	Majeur	L'application doit implémenter des jetons anti-CSRF dans toutes les demandes qui effectuent des actions qui modifient l'état de l'application ou qui ajoutent/modifient/suppriment du contenu.
#5	Exposition d'interfaces sensibles	Moyen	Supprimer les interfaces non utilisées (ex. phpinfo.php) et limiter l'accès aux autres (back office) uniquement pour les machines autorisées (whitelisting de ces machines).
#6	Utilisation de composants avec des vulnérabilités connues	Moyen	Il est fortement recommandé de lister les composants tiers utilisés et de maintenir un système de veille afin de détecter la publication de vulnérabilités critiques les impactant et de pouvoir les mettre à jour.

3.2. Matrice de risque

Tout au long du rapport, chaque vulnérabilité ou risque identifié sera étiqueté et classé comme suit :

Niveau de risque	Description
Faible	Les risques ont un impact minimal.
Moyen	Les risques ont un impact moyen et doivent être traités.
Majeur	Les risques ont un impact fort et doivent absolument être traitée.
Critique	Les risques ont un impact critique et doivent être traités le plus rapidement possible.

Le niveau de risque des vulnérabilités identifiées est calculé en se basant sur deux éléments essentiels :

- La probabilité de l'attaque : Facilité de découverte et d'exploitation.
- L'impact business : Des pertes financières, d'image, de non-conformité ou de violation de vie privée.

Sévérité globale du risque					
Impact Métier	Critique	#X	#X		
	Fort		#X		#X
	Moyen			#X	
	Faible				
		Certaine	Forte	Moyenne	Faible
		Probabilité			

4. Identification et exploitation des vulnérabilités

[illegible]

#2		Référence directe non sécurisée à un objet (IDOR)				
Technique	🔴	Image	🔴	Occurrences	+3	<div><div><div>3</div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>€</div><div>€€€</div><div>Effort remédiation</div></div> <div>RISQUE</div>
Financier	🔴	Juridique	🔴			
Description : Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel qu'un fichier, un dossier, un enregistrement de base de données, ou une clef, comme paramètre d'URL ou de formulaire. Les attaquants peuvent manipuler ces références pour avoir accès à d'autres objets sans autorisation.						
Composants vulnérables : Plateforme utilisateur.				Conditions : Avec compte utilisateur.		
Risque : Un attaquant ayant un compte créé sur la plateforme a la possibilité d'accéder à des informations des autres utilisateurs et d'exécuter des actions sur leurs comptes (Désactivation de mandats, réalisation de paiement...).						
Recommandations : Implémenter des contrôles d'accès à toutes les ressources. L'utilisateur doit être autorisé pour accéder aux informations souhaitées avant que le serveur ne les lui fournisse. Il est également recommandé d'utiliser des hashes (qui sont plus difficile à énumérer) comme référence au lieu des entiers incrémenté.						
Référence : https://owasp.org/www-chapter-ghana/assets/slides/IDOR.pdf						
Auditeur	Alphorm		Propriétaire		Client	
Date d'identification	XXXX		Niveau de confiance		Certain	
Preuves : XXXX						