Rapport de Test d'Intrusion

OWASP Juice Shop

Propriété	Valeur
Préparé par:	Clemence Chopin
Version du document:	1.0
Date:	7 mars 2025
Client:	OWASP Juice Shop
Classification:	Confidentiel

Sommaire

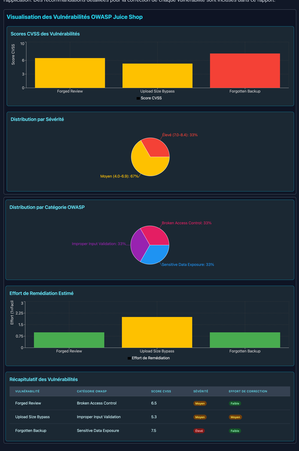
Résumé Exécutif

Ce rapport présente les résultats d'un test d'intrusion ciblé sur l'application web OWASP Juice Shop. L'objectif était d'identifier et d'exploiter trois vulnérabilités spécifiques dans l'application.

Nous avons découvert et exploité avec succès les trois vulnérabilités suivantes:

Vulnérabilité	Sévérité	Impact Principal
Forged Review	CVSS 6.5 (Moyen)	Usurpation d'identité
Upload Size Validation Bypass	CVSS 5.3 (Moyen)	Déni de service potentiel
Forgotten Developer Backup	CVSS 7.5 (Élevé)	Fuite de données sensibles

Ces vulnérabilités représentent des risques significatifs pour l'intégrité des données, la confidentialité et la réputation de l'application. Des recommandations détaillées pour la correction de chaque vulnérabilité sont incluses dans ce rapport.



Méthodologie

Pour ce test d'intrusion, nous avons utilisé une approche ciblée pour identifier et exploiter spécifiquement trois vulnérabilités connues dans l'application OWASP Juice Shop.

Phase	Description
Reconnaissance	Exploration de l'application pour comprendre sa structure et ses fonctionnalités
Analyse	Identification des points d'entrée potentiels et des mécanismes de sécurité
Exploitation	Développement et exécution d'exploits pour confirmer les vulnérabilités
Documentation	Enregistrement détaillé des méthodes d'exploitation et des impacts potentiels

Outils utilisés:

- Burp Suite Community Edition
- Scripts Python personnalisés
- Navigateurs web (Firefox, Chrome)
- Encodeurs/décodeurs URL
- Exegol
- Gobuster

Résultats et Découvertes

Vulnérabilité 1: Forged Review (Broken Access Control)

Propriété	Détail
Catégorie OWASP Top 10	A01:2021 - Broken Access Control
Sévérité	Moyenne (CVSS 6.5)
URL Affectée	http://p10-36-82-5-cv5j34wsk3i111osqa7g-3000.direct.labs.cyberini.com/#/contact

Description

L'application permet aux utilisateurs d'ajouter des commentaires via la fonctionnalité de feedback client. Cependant, une vulnérabilité de contrôle d'accès permet à un attaquant de soumettre des commentaires au nom d'autres utilisateurs sans authentification appropriée.

Reproduction

1. Accéder à la page de commentaires clients : `/#/contact`
2. Intercepter la requête avec Burp Suite lorsqu'un commentaire est soumis
3. Observer que l'ID de l'utilisateur est transmis en clair dans la requête
4. Modifier l'ID utilisateur dans la requête pour usurper l'identité d'un autre utilisateur
5. Transmettre la requête modifiée

Preuve d'Exploitation

L'attaquant peut soumettre un commentaire qui apparaîtra comme s'il avait été écrit par n'importe quel autre utilisateur du système, ce qui permet de manipuler la réputation et potentiellement de propager de fausses informations.

Impact

- Usurpation d'identité des utilisateurs
- Atteinte à la réputation des utilisateurs
- Possibilité de diffuser des informations trompeuses au nom d'autres utilisateurs

Recommandations

1. Implémenter une vérification côté serveur de l'identité de l'utilisateur lors de la soumission des commentaires
2. Utiliser des identifiants de session pour associer les commentaires aux utilisateurs authentifiés
3. Mettre en œuvre des mécanismes de journalisation pour détecter les tentatives d'usurpation d'identité

Vulnérabilité 2: Upload Size Validation Bypass (Improper Input Validation)

Propriété	Détail
Catégorie OWASP Top 10	A03:2021 - Injection
Sévérité	Moyenne (CVSS 5.3)
URL Affectée	http://p10-36-82-5-cv5j34wsk3i111osqa7g-3000.direct.labs.cyberini.com/#/photo-wall

Description

L'application impose une limite de taille sur les fichiers téléversés, mais cette vérification peut être contournée en interceptant et modifiant la requête. Cette vulnérabilité peut conduire à des attaques de déni de service ou au téléversement de contenus malveillants de grande taille.

Reproduction

1. Accéder à la page d'ajout de photos : `/#/photo-wall`
2. Tenter d'ajouter une photo classique
3. Intercepter la requête avec Burp Suite
4. Générer une image de grande taille (plus de 100 Ko) en utilisant un script Python
5. Utiliser l'encodage base64 pour l'image générée
6. Remplacer le code de l'image d'origine dans le répéteur de Burp Suite
7. Envoyer la requête modifiée

Script utilisé pour générer l'image:

```
from PIL import Image
import numpy as np

# Créer une image de taille suffisante pour atteindre 50 Mo
# Une image RGB non compressée a 3 octets par pixel
width = 4096
height = 4096  # Environ 48 Mo (4096*4096*3 = 50,3 Mo)

# Créer une image avec des valeurs aléatoires
data = np.random.randint(0, 256, (height, width, 3), dtype=np.uint8)
img = Image.fromarray(data, 'RGB')

# Sauvegarder en format BMP (non compressé)
img.save('image_50mb.bmp')
```

Preuve d'Exploitation

Nous avons réussi à téléverser une image de plus de 50 Mo alors que la limite configurée dans l'application est de 100 Ko.

Impact

- Risque de déni de service par la consommation excessive d'espace disque
- Possibilité de téléverser des fichiers malveillants volumineux
- Consommation excessive de bande passante

Recommandations

1. Implémenter des vérifications de taille côté serveur qui ne peuvent pas être contournées
2. Utiliser des validations côté serveur et client pour la taille des fichiers
3. Mettre en place des quotas d'utilisation par utilisateur
4. Implémenter des mécanismes de contrôle des types MIME réels des fichiers

---

Vulnérabilité 3: Forgotten Developer Backup (Sensitive Data Exposure)

Propriété	Détail
Catégorie OWASP Top 10	A02:2021 - Cryptographic Failures
Sévérité	Élevée (CVSS 7.5)
URL Affectée	http://p10-36-86-5-cv5nu8b6xb3111osqae0-3000.direct.labs.cyberini.com/ftp/

Description

L'application expose un répertoire FTP contenant des fichiers de sauvegarde sensibles. Bien que l'application tente de restreindre l'accès aux seuls fichiers *.md et *.pdf, cette restriction peut être contournée en utilisant une technique d'injection de byte nul (Null Byte Injection).

Reproduction

1. Accéder au répertoire FTP exposé : `/ftp/`
2. Observer que le serveur HTTP renvoie une erreur 403 si l'on tente de télécharger des fichiers .bak directement

```
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
```

3. Utiliser une injection de byte nul encodée en URL pour contourner cette restriction
4. Construire une URL comme suit : `/ftp/package.json.bak%2500.md`
5. Accéder à cette URL pour télécharger le fichier de sauvegarde

Preuve d'Exploitation

Nous avons pu accéder aux fichiers suivants:

- `http://p10-36-86-5-cv5nu8b6xb3111osqae0-3000.direct.labs.cyberini.com/ftp/package.json.bak%2500.md`
- `http://p10-36-86-5-cv5nu8b6xb3111osqae0-3000.direct.labs.cyberini.com/ftp/coupons_2013.md.bak%2500.md`

Impact

- Accès à des données sensibles de développement
- Possibilité de découvrir des informations sur la structure interne de l'application
- Exposition potentielle de secrets, mots de passe ou clés API

Recommandations

1. Supprimer tous les fichiers de sauvegarde des environnements de production
2. Mettre en place un contrôle d'accès approprié pour les répertoires sensibles
3. Corriger la validation des extensions de fichiers pour empêcher les techniques d'injection de byte nul
4. Implémenter la validation côté serveur des chemins de fichiers complets, et pas seulement des extensions

---

Synthèse des Risques

#	Vulnérabilité	Catégorie OWASP	Sévérité CVSS	Impact	Complexité de correction
1	Forged Review	A01 - Broken Access Control	6.5 (Moyen)	Moyen	Faible
2	Upload Size Validation Bypass	A03 - Injection	5.3 (Moyen)	Moyen	Moyenne
3	Forgotten Developer Backup	A02 - Cryptographic Failures	7.5 (Élevé)	Élevé	Faible

Conclusion

Ce test d'intrusion a démontré la présence de trois vulnérabilités significatives dans l'application OWASP Juice Shop. Ces vulnérabilités exposent l'application à divers risques, notamment l'usurpation d'identité, les attaques par déni de service et l'exposition de données sensibles.

Les recommandations fournies dans ce rapport devraient être mises en œuvre dans les plus brefs délais pour renforcer la posture de sécurité de l'application. En particulier, la vulnérabilité "Forgotten Developer Backup" représente le risque le plus élevé et devrait être corrigée en priorité.

Nous recommandons également de réaliser un test d'intrusion complet pour identifier d'autres vulnérabilités potentielles qui pourraient exister dans l'application.

Annexes

Glossaire

- **CVSS**: Common Vulnerability Scoring System
- **OWASP**: Open Web Application Security Project
- **Broken Access Control**: Défaillance dans les mécanismes de contrôle d'accès
- **Injection de byte nul**: Technique d'exploitation utilisant le caractère NULL (%00) pour tromper les systèmes de validation

Références

- OWASP Top 10 2021: https://owasp.org/Top10/
- CVSS v3.1: https://www.first.org/cvss/
- NULL Byte Injection: https://owasp.org/www-community/attacks/Null_Byte_Injection