Rapport d’audit de sécurité

V 1.0

- Breizh CTF 2023 –



Table des matières

[Contexte 2](#_Toc121237419)

[Périmètre d’audit 2](#_Toc121237420)

[Synthèse 3](#_Toc121237421)

[Détails des vulnérabilités 4](#_Toc121237422)

[Référentiels 5](#_Toc121237423)

# Contexte

La société BreizhCTF a souhaité évaluer le niveau de sécurité de sa plateforme par la réalisation de tests d'intrusion depuis Internet. Les tests ont été menés en suivant une approche de type « boîte grise ».

Les objectifs de ce test d'intrusion étaient :

* d'identifier les vulnérabilités présentes au sein de l'application ;
* d'exploiter les vulnérabilités présentes afin d'évaluer les risques de compromission ;
* de fournir les recommandations adéquates permettant de réduire ces niveaux de risques.

# Périmètre d’audit

L’audit de sécurité s’est déroulé sur la période suivante :

|  |  |
| --- | --- |
| ACTIVITÉ D’AUDIT | DATE |
| Test d’intrusion externe | Du 10/01/2023 au 17/01/2023 |

Le périmètre du test d'intrusion réalisé par Cybeur-salé incluait les serveurs suivants :

* app.breizh.ctf

Les comptes suivants ont été fournis :

* un compte admin;
* un compte utilisateur.

Toutes les données collectées pendant l’audit seront transmises à leur propriétaire sur demande et/ou détruites à l’issue de la mission.

# Synthèse

|  |  |
| --- | --- |
| Score : |  |

En premier lieu, on observe une hétérogénéité des technologies de l’application web ce qui augmente la surface d'attaque, notamment par le biais de bugs logiciels dont la correction est plus complexe à coordonner.

Des mesures de protection (WAF et pare-feu) sur le périmètre externe sont efficaces mais ne sont pas généralisées à toutes les routes de l’application.

Par conséquents plusieurs vulnérabilités majeurs et une vulnérabilité critique ont été identifiée sur le périmètre. Il est en effet possible d’accéder aux informations des utilisateurs du BreizhCTF

# Détails des vulnérabilités

|  |  |  |
| --- | --- | --- |
| Vuln-001 | | |
| Titre | Remote Flag Execution | CVSS 10 |
| Cible | breizh.ctf |
| Description | En sécurité informatique, l'exécution de code arbitraire est la capacité d'un attaquant à exécuter n'importe quelle commande ou code de son choix sur une machine cible ou dans un processus cible. | |
| Preuve | **BZHCTF{CryptoKnownFiles !}** | |

# Référentiels

* CVSS 3.1 - Annexe cvss-v31-specification\_r1.pdf
* OWASP - Annexe 20211216\_OWASP-MSP\_OWASP\_Top\_Ten\_2021.pdf