# SECS1024 - Projet Application web Wordpress

not´e 20 points - 25% de la note finale

a` rendre pour le 10 avril

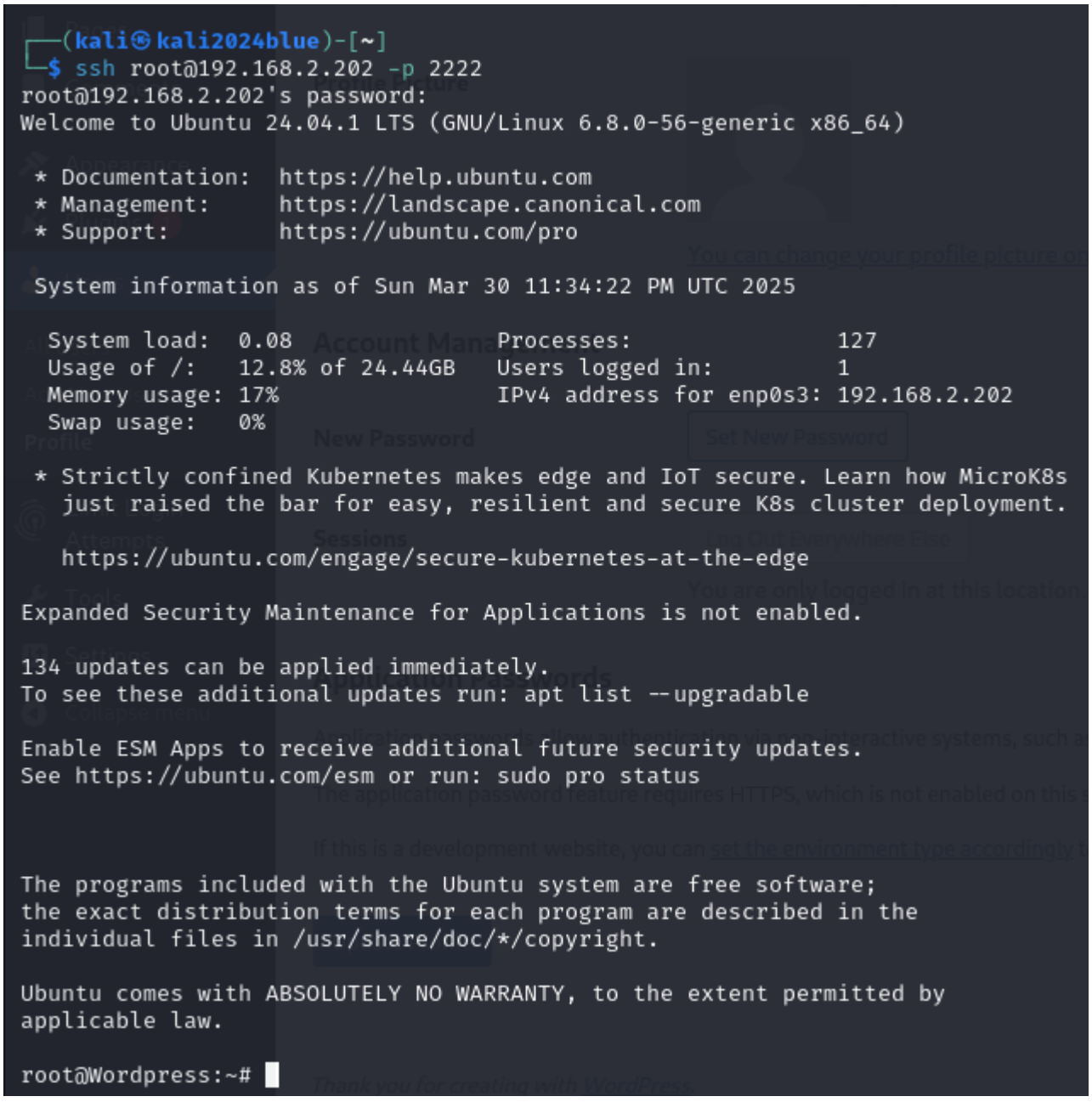
Objectif : S´ecuriser une application web wordpress.

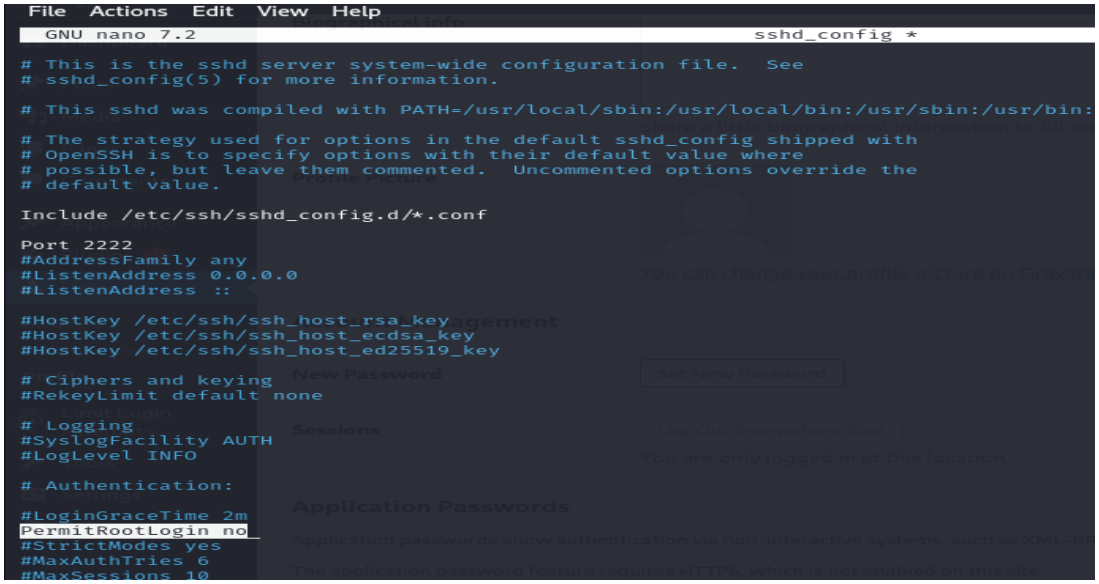
Machine utiliser kali linux et wordpress

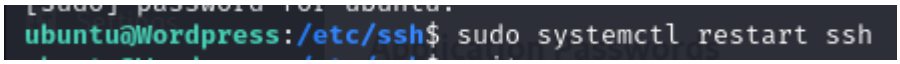
## 1 S´ecurisation du serveur web (6 points)

(3 points) Expliquez au moins 3 protections que vous avez mises en place pour s´ecuriser le serveur et les applications autres que l'application web (compte root, ssh, pare-feu). Documentez vos r´eponses par des explications textuelles et des captures ´ecran. (2 points par protection)

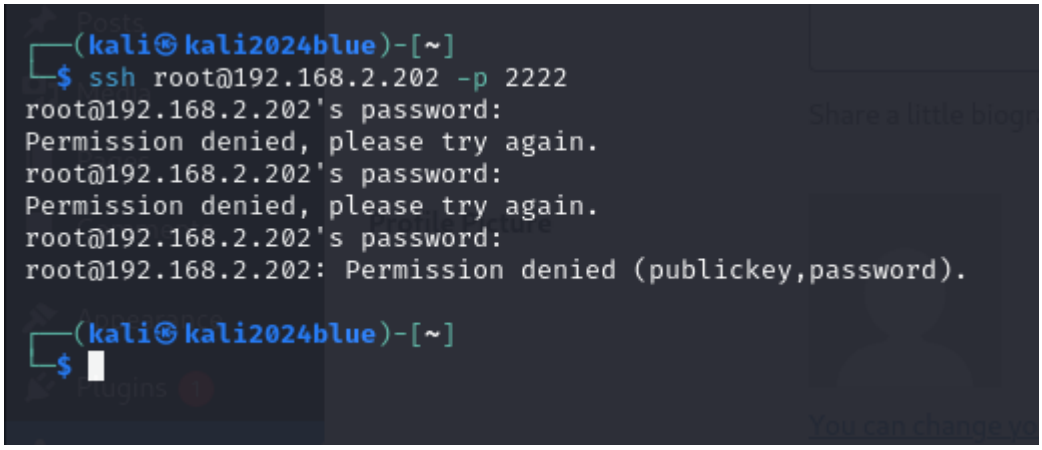
Empêcher le root login



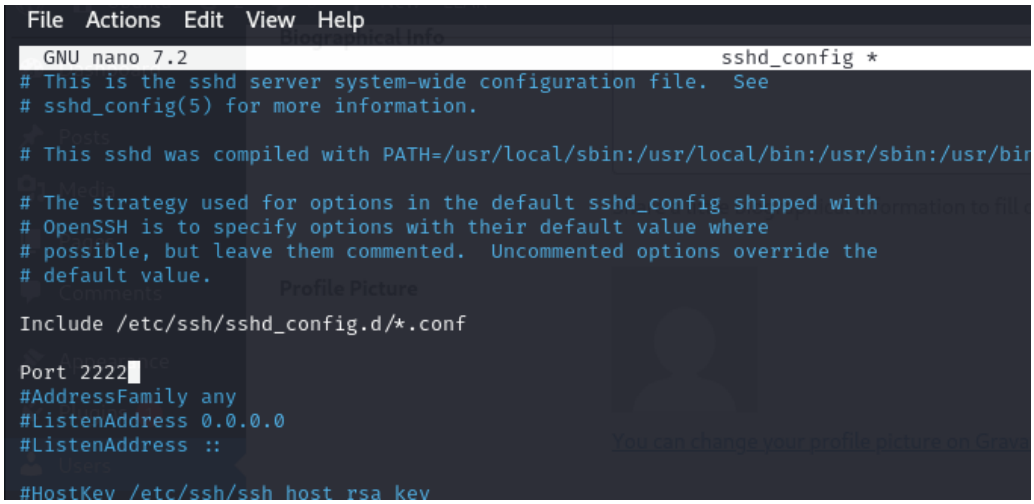



Même si j'ai le bon mot de passe ca ne me laisse pas entrer



Changement du port ssh





```
┌──(kali㉿kali2024blue)-[~]
└─$ ssh ubuntu@192.168.2.202 -p 2222
ubuntu@192.168.2.202's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-56-generic x86_64)

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

 System information as of Sun Mar 30 11:09:55 PM UTC 2025

  System load:  0.11               Processes:               124
  Usage of /:   12.8% of 24.44GB   Users logged in:         1
  Memory usage: 17%                IPv4 address for enp0s3: 192.168.2.202
  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.

134 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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


Last login: Sun Mar 30 23:06:54 2025 from 192.168.2.204
ubuntu@Wordpress:~$
```

Règle firewall qui empêche les autres de rentrer par ssh mais de seulement laisser une adresse ip

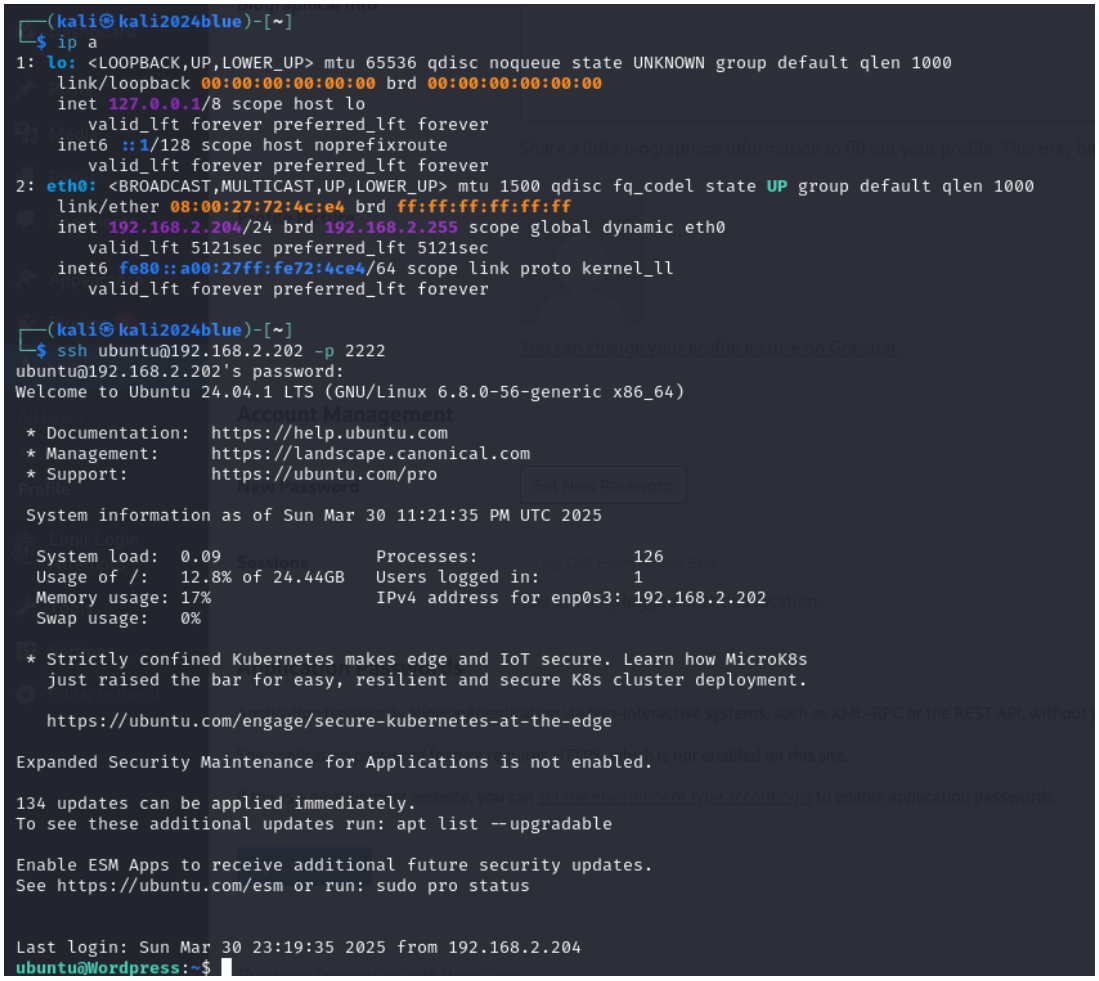
```
 GNU nano 7.2                                                    hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
sshd: 192.168.2.204
#                See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
```

```
To                         Action      From
--                         ------      ----
2222                       ALLOW       192.168.2.204
2222                       DENY        Anywhere
80                         ALLOW       Anywhere
2222 (v6)                  DENY        Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)

ubuntu@Wordpress:~$
```

```
┌──(kali㉿kali2024)-[~]
└─$ ip a
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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:01:71:cc brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.203/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
       valid_lft 5157sec preferred_lft 5157sec
    inet6 fe80::a00:27ff:fe01:71cc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali2024)-[~]
└─$ ssh ubuntu@192.168.2.202 -p 2222
```




# 2 Application Web Wordpress

## 2.1 S´ecurisation de l'application Web (10 points)

Expliquez au moins 5 protections que vous avez mises en place pour s´ecuriser l'application Wordpress dont au moins les protections suivantes : acc`es au compte admin, acc`es a` l'API wordpress, protection HTTPS, protection WAF. (2 points par protection)

Documentez votre r´eponse par des explications textuelles et des captures ´ecran.

WAF :

```
File  Actions  Edit  View  Help
ubuntu@Wordpress:~$ sudo apt install libapache2-mod-security2 -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  liblua5.1-0 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 libyajl2 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 147 not upgraded.
Need to get 542 kB of archives.
After this operation, 2,481 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 liblua5.1-0 amd64 5.1.5-9build2 [120 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libyajl2 amd64 2.1.0-5build1 [20.2 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 libapache2-mod-security2 amd64 2.9.7-1build3 [260 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 modsecurity-crs all 3.3.5-2 [143 kB]
Fetched 542 kB in 0s (1,817 kB/s)
Selecting previously unselected package liblua5.1-0:amd64.
(Reading database ... 87204 files and directories currently installed.)
Preparing to unpack .../liblua5.1-0_5.1.5-9build2_amd64.deb ...
Unpacking liblua5.1-0:amd64 (5.1.5-9build2) ...
Selecting previously unselected package libyajl2:amd64.
Preparing to unpack .../libyajl2_2.1.0-5build1_amd64.deb ...
Unpacking libyajl2:amd64 (2.1.0-5build1) ...
Selecting previously unselected package libapache2-mod-security2.
Preparing to unpack .../libapache2-mod-security2_2.9.7-1build3_amd64.deb ...
Unpacking libapache2-mod-security2 (2.9.7-1build3) ...
Selecting previously unselected package modsecurity-crs.
Preparing to unpack .../modsecurity-crs_3.3.5-2_all.deb ...
Unpacking modsecurity-crs (3.3.5-2) ...
Setting up libyajl2:amd64 (2.1.0-5build1) ...
Setting up modsecurity-crs (3.3.5-2) ...
Setting up liblua5.1-0:amd64 (5.1.5-9build2) ...
Setting up libapache2-mod-security2 (2.9.7-1build3) ...
apache2_invoke: Enable module security2
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@Wordpress:~$
```

```
ubuntu@Wordpress:~$ sudo a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
```

```
  GNU nano 7.2                                    modsecurity.conf
# -- Rule engine initialization ----------------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On


# -- Request body handling ---------------------------------------------------

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On


# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "^(?:application(?:/soap\+|/)|text/)xml" \
     "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

# Enable JSON request body parser.
```

```
ubuntu@Wordpress:/etc/modsecurity$ sudo apt install git
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
git is already the newest version (1:2.43.0-1ubuntu7.2).
git set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 147 not upgraded.
ubuntu@Wordpress:/etc/modsecurity$ sudo rm -rf /usr/share/modsecurity-crs
ubuntu@Wordpress:/etc/modsecurity$ sudo git clone https://github.com/coreruleset/coreruleset /usr/share/modsecurity-
crs
Cloning into '/usr/share/modsecurity-crs' ...
remote: Enumerating objects: 35133, done.
remote: Counting objects: 100% (142/142), done.
remote: Compressing objects: 100% (76/76), done.
remote: Total 35133 (delta 120), reused 66 (delta 66), pack-reused 34991 (from 3)
Receiving objects: 100% (35133/35133), 10.24 MiB | 13.62 MiB/s, done.
Resolving deltas: 100% (27801/27801), done.
ubuntu@Wordpress:/etc/modsecurity$ sudo mv /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modsecurity-
crs/crs-setup.conf
ubuntu@Wordpress:/etc/modsecurity$ sudo mv /usr/share/modsecurity-crs/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.c
onf.example /usr/share/modsecurity-crs/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf
ubuntu@Wordpress:/etc/modsecurity$
```

File Actions Edit View Help

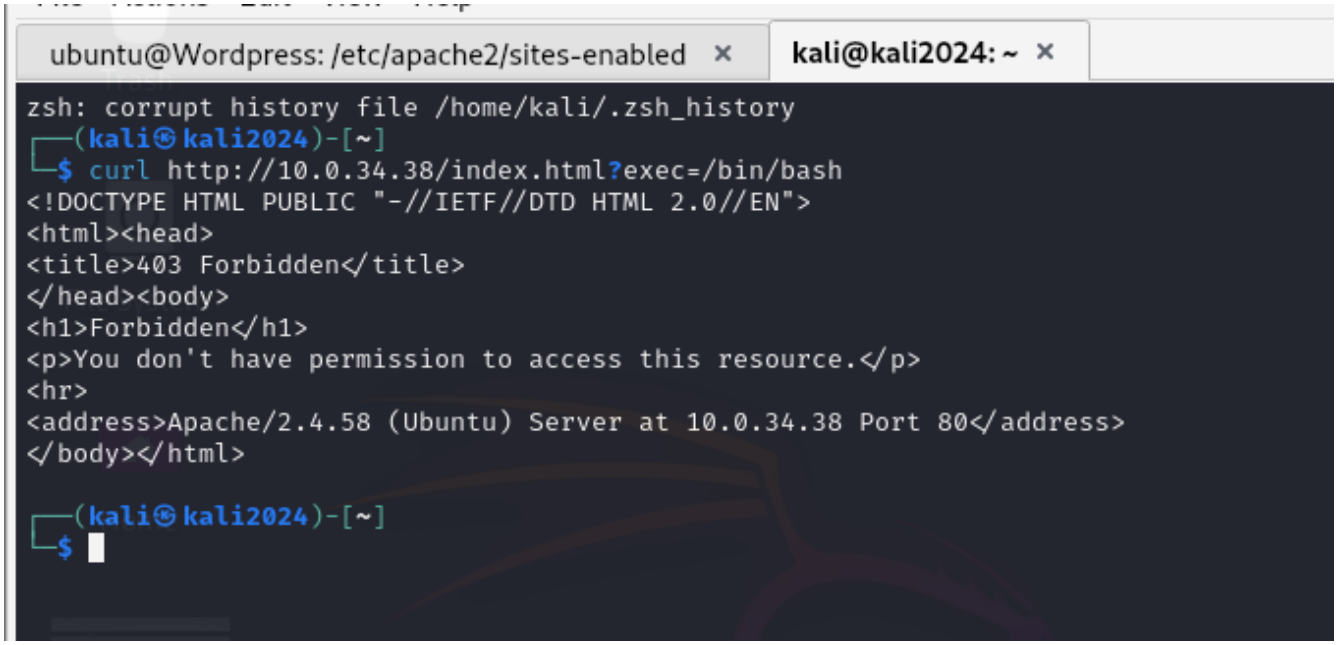
```
 GNU nano 7.2                          /etc/apache2/mods-available/security2.conf *
<IfModule security2_module>
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity
        Include /usr/share/modsecurity-crs/crs-setup.conf
        Include /usr/share/modsecurity-crs/rules/*.conf
        # Include all the *.conf files in /etc/modsecurity.
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf

        # Include OWASP ModSecurity CRS rules if installed
        IncludeOptional /usr/share/modsecurity-crs/*.load
</IfModule>
```

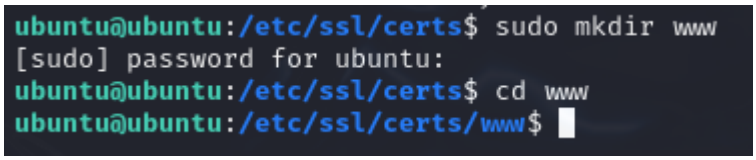
File Actions Edit View Help

```
 GNU nano 7.2                                                wordpress.conf
<VirtualHost *:80>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
        ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SecRuleEngine On
</VirtualHost>
```


ubuntu@Wordpress: /etc/apache2/sites-enabled
kali@kali2024: ~
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali2024)-[~]
$ curl http://10.0.34.38/index.html?exec=/bin/bash
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
You don't have permission to access this resource.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 10.0.34.38 Port 80</address>
</body></html>
(kali㉿kali2024)-[~]
$

HTTPS :


ubuntu@ubuntu:/etc/ssl/certs$ sudo mkdir www
[sudo] password for ubuntu:
ubuntu@ubuntu:/etc/ssl/certs$ cd www
ubuntu@ubuntu:/etc/ssl/certs/www$

```
ubuntu@ubuntu:/etc/ssl/certs/www$ sudo openssl req -x509 -newkey rsa:4096 -keyout private_key.key -out certificate.
pem -days 365
...+.............+.........+.+...+...+...+.............+...+.........+.............+...+..+.......+..+...+.+..
...+.......+........+.+.....+......+.......+......+.................+.......+......++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++*...+.....+.+...+........+........+.............+.+..+...+.......+.....+.......
..............+........+.+............+...+..+....+.....+......++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++*.................+.+...+..+.+.............+........+.........+......+.....................+....
..+....+.....+............+.................+.............+..+.......+..+...+.......+.....+....+..+.......+....
....+...+..............+.....+......+.........+..+...+........+..+....+.........+.....+...+..........+...
..............+......+.........+....+..+...+.+.....+......+............+.....+......+...+.........+.........
.........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
...+.....+.........+.........+.......+...+..+..+............+..+...+....++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++*.+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+...+.....+..
.......+....+..+............+...+.................+.........+.+.....+......+.........+....+........+...+......+.+.
.......+......+....+...........+...+.+..+.........+...+...........+........+.............................+.+....
..+........+.......+............+........+....+...+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
ubuntu@ubuntu:/etc/ssl/certs/www$ ls
certificate.pem  private_key.key
ubuntu@ubuntu:/etc/ssl/certs/www$
```

```
ubuntu@ubuntu:/etc/ssl/certs/www$ openssl x509 -inform PEM -in certificate.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            63:95:39:6a:f4:66:fd:65:2c:6a:de:3c:19:e9:d0:51:95:d9:36:aa
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Feb 18 13:56:09 2025 GMT
            Not After : Feb 18 13:56:09 2026 GMT
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:c8:16:45:53:a2:5c:66:39:2d:5a:e9:c5:59:
                    e0:45:fd:c6:b0:4b:a3:a4:94:13:30:3c:47:9e:ff:
                    97:1d:84:aa:31:5b:df:bf:4d:73:aa:60:bf:2d:d8:
                    cb:f2:09:1d:75:02:63:2f:e0:3d:b0:9c:e2:0e:83:
                    da:06:0d:63:61:b9:1b:5b:f8:e2:10:fa:a7:ab:bc:
                    ed:7a:aa:9c:80:39:2d:a0:7f:27:34:ca:7b:c9:3a:
                    ff:2b:9a:ca:3c:53:7c:b6:66:c3:05:a2:9c:7b:58:
                    60:3e:c2:6f:5c:ca:fe:0c:b2:06:41:01:a6:69:a1:
                    c4:dc:6a:8f:c0:ec:ec:a4:81:e7:de:01:6a:70:75:
                    6c:d8:aa:2d:ef:8a:78:db:83:5a:03:9f:1f:82:0a:
                    e8:5a:6d:50:dd:64:e3:c6:82:62:f6:df:eb:92:a3:
                    0a:20:79:2b:43:25:df:e0:0a:ac:b7:e4:4a:1b:6b:
                    55:d5:74:9b:2a:52:51:7c:01:66:90:2d:94:fc:fe:
                    22:2d:b4:5f:75:22:c7:df:b4:99:e1:0f:79:84:fc:
                    f2:bc:a8:8b:45:92:88:c8:86:74:a6:ce:11:87:29:
                    30:c0:67:ab:a0:b5:1c:4a:05:36:f2:a2:c0:8a:b9:
                    60:07:df:e8:76:d0:71:83:54:fb:2b:14:25:9c:6d:
                    a2:16:2e:0c:1e:85:56:9f:a5:ea:f2:c9:6f:9e:32:
                    48:ec:e8:89:a1:e8:fd:44:53:7c:0c:b0:b0:b9:c5:
                    f6:ca:70:d1:45:bf:a3:7f:c4:ab:fa:6d:b1:c4:7d:
                    87:0e:b2:fc:2b:98:82:1c:f7:c8:59:1f:bc:10:3c:
                    b8:86:8e:87:40:4d:37:ad:f7:47:e0:46:a5:9e:e4:
                    db:53:70:5f:39:78:7c:ad:09:8e:85:70:a4:1e:95:
                    c6:4e:74:4b:c9:70:f7:5b:f5:5d:0e:25:49:86:15:
                    66:c1:6f:99:94:19:99:c5:b4:83:ed:c6:ac:71:d5:
                    57:c6:61:51:28:20:73:71:0e:96:78:dc:6d:cf:ac:
                    38:bc:d3:31:b0:4a:bd:74:75:e1:15:43:b6:98:8a:
                    db:7d:14:52:28:18:6a:9d:e0:47:e4:a9:f0:7b:41:
                    c4:28:e0:8b:52:fd:0b:19:be:7b:19:dd:74:c9:ff:
                    47:c6:b0:48:6a:d4:6e:cd:9c:69:65:1e:28:ee:af:
                    70:20:32:a5:86:ef:55:07:55:4e:6d:3c:f6:52:86:
                    42:ef:4c:84:3c:44:a7:64:a4:86:ac:35:bf:75:d4:
                    2d:af:8c:30:d7:3b:5d:cb:a0:30:5d:e7:14:0d:0f:
                    f8:04:52:68:38:88:35:8a:64:47:20:7d:93:70:1a:
                    26:62:fb
                Exponent: 65537 (0x10001)
```

```
            26:62:fb
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            E9:75:9D:09:2C:3D:2D:CE:23:C4:15:EE:D9:C9:43:EF:88:1C:7D:99
        X509v3 Authority Key Identifier:
            E9:75:9D:09:2C:3D:2D:CE:23:C4:15:EE:D9:C9:43:EF:88:1C:7D:99
        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
    67:ce:ab:c0:38:79:67:b1:dc:13:94:9d:fe:a0:f1:7d:9e:df:
    c9:89:74:23:4d:2c:0e:27:64:ff:ad:da:f2:09:24:7e:53:be:
    a1:36:8f:03:2f:21:c4:b5:ca:54:71:8e:5b:90:fa:b5:f2:a8:
    ac:5f:67:2a:b3:5b:fa:ab:8e:a3:7f:8a:0b:a1:66:8d:79:a9:
    64:f0:25:4f:e7:ad:15:3d:34:41:80:5a:f5:2e:25:df:e4:48:
    89:f2:c5:25:95:9f:4e:b1:91:ef:d8:aa:c7:be:58:db:7c:54:
    e2:88:dc:cd:6e:fe:63:8b:1f:98:bf:98:2e:9e:cd:8a:71:b4:
    2a:61:79:f7:c0:14:ca:96:4e:86:41:60:1f:07:3a:ca:52:8a:
    5a:c4:17:d4:24:bd:39:32:6d:dd:8a:d6:b4:e4:dc:93:68:41:
    8f:6c:e2:c4:01:4f:d7:b5:9f:c9:b9:fa:37:00:25:7b:7f:ee:
    89:65:ac:c0:00:97:aa:73:14:ea:a5:f2:2b:6b:a6:05:4b:16:
    bf:24:c1:ac:a0:6c:e9:e7:5f:8d:09:89:5b:4f:9b:ed:fb:a9:
    81:02:c0:69:2d:c9:f2:4f:85:f2:af:d7:b2:47:27:09:cf:d4:
    f4:fa:bf:1c:0b:75:b8:3b:c0:da:a6:27:5e:48:31:51:4d:c1:
    d8:c3:af:d2:bd:11:6e:e9:65:56:2a:3d:44:d3:26:4e:52:4e:
    0f:4a:00:82:c0:b6:2c:dd:4c:5b:d7:ad:06:66:19:c6:4b:0b:
    be:1f:c2:5c:76:88:3d:25:9f:0e:52:bc:ef:23:49:15:b2:fe:
    9b:54:0b:02:f2:b6:36:7e:52:e9:38:4d:0f:23:fb:20:a8:96:
    49:17:0b:dd:af:16:1c:5f:87:1d:85:32:ac:1d:13:a4:48:8f:
    64:a0:d0:1c:51:74:76:1b:e8:3c:1c:63:a5:29:2d:60:67:1e:
    d2:4a:af:dd:a5:97:6c:ff:82:74:c3:91:d2:bb:6c:37:a3:09:
    07:06:e5:9e:b7:34:63:7b:49:62:b0:92:9a:ca:e6:b4:c3:04:
    5b:f5:40:97:d5:4f:b2:fc:a7:6f:f1:f4:aa:6d:e5:1f:2b:fd:
    89:0b:c1:3d:1a:08:0a:ee:6e:32:15:2c:0b:7e:ae:b8:d2:46:
    ee:5e:38:e4:91:94:e5:2c:92:6c:c7:8d:ad:8c:9c:b8:96:cd:
    26:fd:ee:5c:3b:4a:9b:41:da:ed:e8:97:97:4c:02:44:a8:11:
    99:3f:03:ef:39:a0:d6:a2:02:eb:59:d8:d3:42:80:35:03:e9:
    a7:8c:2c:f9:e6:b8:71:3e:74:88:54:93:8f:ed:46:e5:66:28:
    a3:61:65:cf:77:b3:42:02
```

```
ubuntu@ubuntu:/etc/ssl/certs/www$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
ubuntu@ubuntu:/etc/ssl/certs/www$ sudo systemctl restart apache2
ubuntu@ubuntu:/etc/ssl/certs/www$
```

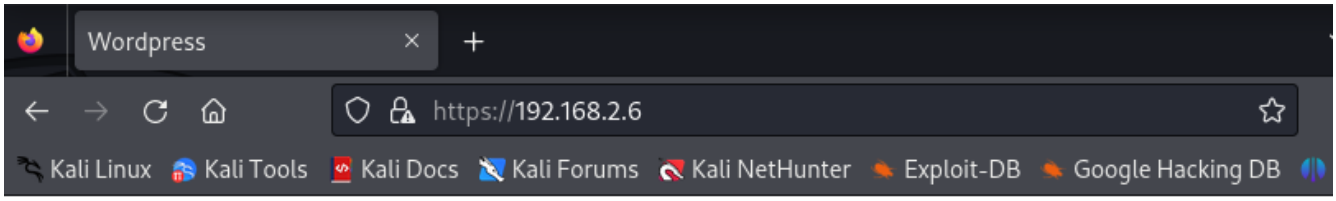
```
  GNU nano 7.2                                          wordpress
<VirtualHost *:80>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>
<VirtualHost *:443>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
SSLEngine on
SSLCertificateFile /etc/ssl/certs/www/certificate.pem
SSLCertificateKeyFile /etc/ssl/certs/www/private_key.key
</VirtualHost>
```

```
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo a2ensite wordpress.conf
Site wordpress already enabled
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo systemctl restart apache2
🔐 Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA): (press TAB for no echo)
Broadcast message from root@ubuntu (Tue 2025-02-18 14:18:10 UTC):

Password entry required for 'Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA):' (PID 1601).
Please enter password with the systemd-tty-ask-password-agent tool.

......
ubuntu@ubuntu:/etc/apache2/sites-available$
```

```
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo ss -tuln
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:*
udp        UNCONN     0          0             192.168.2.6%enp0s3:68              0.0.0.0:*
tcp        LISTEN     0          151                  127.0.0.1:3306              0.0.0.0:*
tcp        LISTEN     0          4096             127.0.0.53%lo:53                0.0.0.0:*
tcp        LISTEN     0          70                   127.0.0.1:33060             0.0.0.0:*
tcp        LISTEN     0          4096                127.0.0.54:53                0.0.0.0:*
tcp        LISTEN     0          511                        *:80                      *:*
tcp        LISTEN     0          4096                       *:22                      *:*
tcp        LISTEN     0          511                        *:443                     *:*
```




API REST :

```
┌──(kali㉿kali2024blue)-[~]
└─$ curl -X GET -i http://10.0.67.244/wp-json/wp/v2/users
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 17:53:40 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
X-WP-Total: 2
X-WP-TotalPages: 1
Allow: GET
Vary: Origin
Content-Length: 1243
Content-Type: application/json; charset=UTF-8

[{"id":2,"name":"Jean-Marc Solution","url":"","description":"","link":"http:\/\/10.0.67.244\/author\/jean-marc\/","slug":"jean-marc","avatar_urls":{"24":"https:\/
\/secure.gravatar.com\/avatar\/09c9f88de7f4b5f1665c4bffb8eac9fc?s=24&d=mm&r=g","48":"https:\/\/secure.gravatar.com\/avatar\/09c9f88de7f4b5f1665c4bffb8eac9fc?s=48&
d=mm&r=g","96":"https:\/\/secure.gravatar.com\/avatar\/09c9f88de7f4b5f1665c4bffb8eac9fc?s=96&d=mm&r=g"},"meta":[],"_links":{"self":[{"href":"http:\/\/10.0.67.244\
/wp-json\/wp\/v2\/users\/2","targetHints":{"allow":["GET"]}}],"collection":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/users"}]}},{"id":1,"name":"Ubuntu","ur
l":"http:\/\/10.0.67.244","description":"","link":"http:\/\/10.0.67.244\/author\/ubuntu\/","slug":"ubuntu","avatar_urls":{"24":"https:\/\/secure.gravatar.com\/ava
tar\/2672049e12d6caf8633f13a917b22fae?s=24&d=mm&r=g","48":"https:\/\/secure.gravatar.com\/avatar\/2672049e12d6caf8633f13a917b22fae?s=48&d=mm&r=g","96":"https:\/\/
secure.gravatar.com\/avatar\/2672049e12d6caf8633f13a917b22fae?s=96&d=mm&r=g"},"meta":[],"_links":{"self":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/users\/1
","targetHints":{"allow":["GET"]}}],"collection":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/users"}]}}]

┌──(kali㉿kali2024blue)-[~]
└─$
```

```
┌──(kali㉿kali2024blue)-[~]
└─$ curl -X GET -i http://10.0.67.244/wp-json/wp/v2/posts
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 17:57:40 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
X-WP-Total: 2
X-WP-TotalPages: 1
Allow: GET
Vary: Origin
Content-Length: 3666
Content-Type: application/json; charset=UTF-8

[{"id":8,"date":"2025-01-30T17:53:14","date_gmt":"2025-01-30T17:53:14","guid":{"rendered":"http:\/\/10.0.67.244\/?p=8"},"modified":"2025-01-30T17:53:14","modified
_gmt":"2025-01-30T17:53:14","slug":"pierre-jean-pour-vous-aider","status":"publish","type":"post","link":"http:\/\/10.0.67.244\/2025\/01\/30\/pierre-jean-pour-vou
s-aider\/","title":{"rendered":"Pierre-jean pour vous aider"},"content":{"rendered":"\n<p>salut les amis<\/p>\n","protected":false},"excerpt":{"rendered":"<p>salu
t les amis<\/p>\n","protected":false},"author":2,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard",
"meta":{"footnotes":""},"categories":[1],"tags":[],"class_list":["post-8","post","type-post","status-publish","format-standard","hentry","category-uncategorized"]
,"_links":{"self":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/8","targetHints":{"allow":["GET"]}}],"collection":[{"href":"http:\/\/10.0.67.244\/wp-jso
n\/wp\/v2\/posts"}],"about":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/types\/post"}],"author":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp
\/v2\/users\/2"}],"replies":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/comments?post=8"}],"version-history":[{"count":2,"href":"http:\/\/1
0.0.67.244\/wp-json\/wp\/v2\/posts\/8\/revisions"}],"predecessor-version":[{"id":11,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/8\/revisions\/11"}],"wp:
attachment":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/media?parent=8"}],"wp:term":[{"taxonomy":"category","embeddable":true,"href":"http:\/\/10.0.67.244\/w
p-json\/wp\/v2\/categories?post=8"},{"taxonomy":"post_tag","embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/tags?post=8"}],"curies":[{"name":"wp",
"href":"https:\/\/api.w.org\/{rel}","templated":true}]}},{"id":1,"date":"2025-01-23T17:34:16","date_gmt":"2025-01-23T17:34:16","guid":{"rendered":"http:\/\/10.0.6
7.244\/?p=1"},"modified":"2025-01-23T17:34:16","modified_gmt":"2025-01-23T17:34:16","slug":"hello-world","status":"publish","type":"post","link":"http:\/\/10.0.67
.244\/2025\/01\/23\/hello-world\/","title":{"rendered":"Hello world!"},"content":{"rendered":"\n<p>Welcome to WordPress. This is your first post. Edit or delete i
t, then start writing!<\/p>\n","protected":false},"excerpt":{"rendered":"<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!<
\/p>\n","protected":false},"author":1,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"fo
otnotes":""},"categories":[1],"tags":[],"class_list":["post-1","post","type-post","status-publish","format-standard","hentry","category-uncategorized"],"_links":{
"self":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1","targetHints":{"allow":["GET"]}}],"collection":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/
posts"}],"about":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/types\/post"}],"author":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/users
\/1"}],"replies":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/comments?post=1"}],"version-history":[{"count":0,"href":"http:\/\/10.0.67.244\
/wp-json\/wp\/v2\/posts\/1\/revisions"}],"wp:attachment":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/media?parent=1"}],"wp:term":[{"taxonomy":"category","emb
eddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/categories?post=1"},{"taxonomy":"post_tag","embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/w
p\/v2\/tags?post=1"}],"curies":[{"name":"wp","href":"https:\/\/api.w.org\/{rel}","templated":true}]}]]

┌──(kali㉿kali2024blue)-[~]
└─$
```

WordPress REST API Authentication

By miniOrange

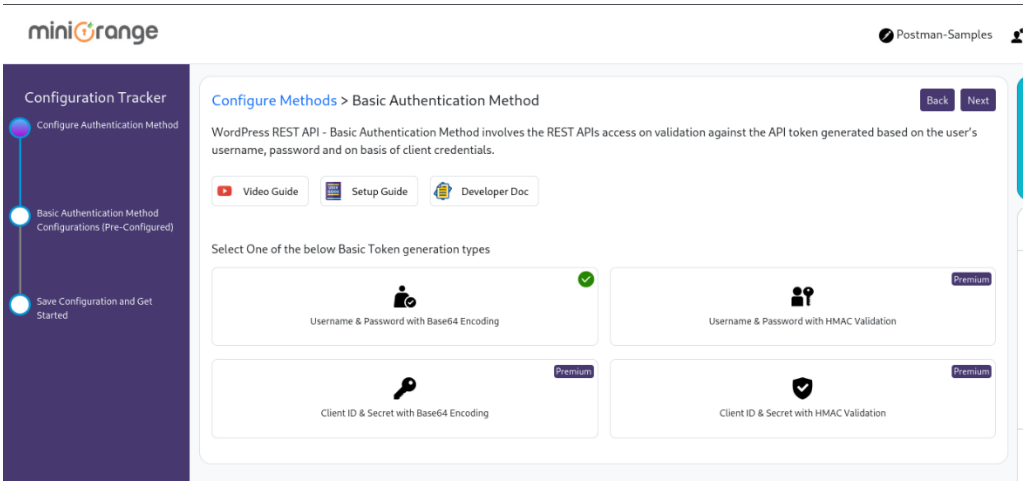
Download

Details | Reviews | Installation | Development | Support

Add Plugins Upload Plugin

If you have a plugin in a .zip format, you may install or update it by uploading it here.

Browse... wp-rest-api-authentication.3.6.2.zip Install Now




Token Encryption Type Type: **Base 64 Encoding**

Test Configuration

ubuntu

password

REST API Endpoint:

GET http://10.0.67.244/wp-json/wp/v2/posts

Test Configuration

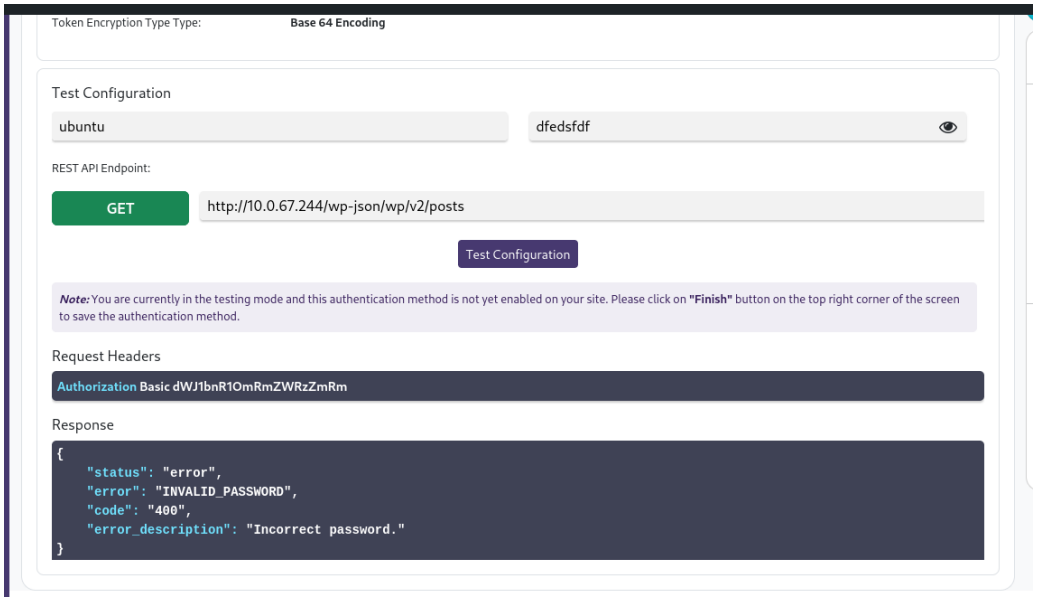
***Note:*** The Test has been done successfully. Please click on **"Finish"** button on the top right corner of the screen to save the authentication method.

Request Headers

```
Authorization Basic dWJ1bnR1OnBhc3N3b3Jk
```

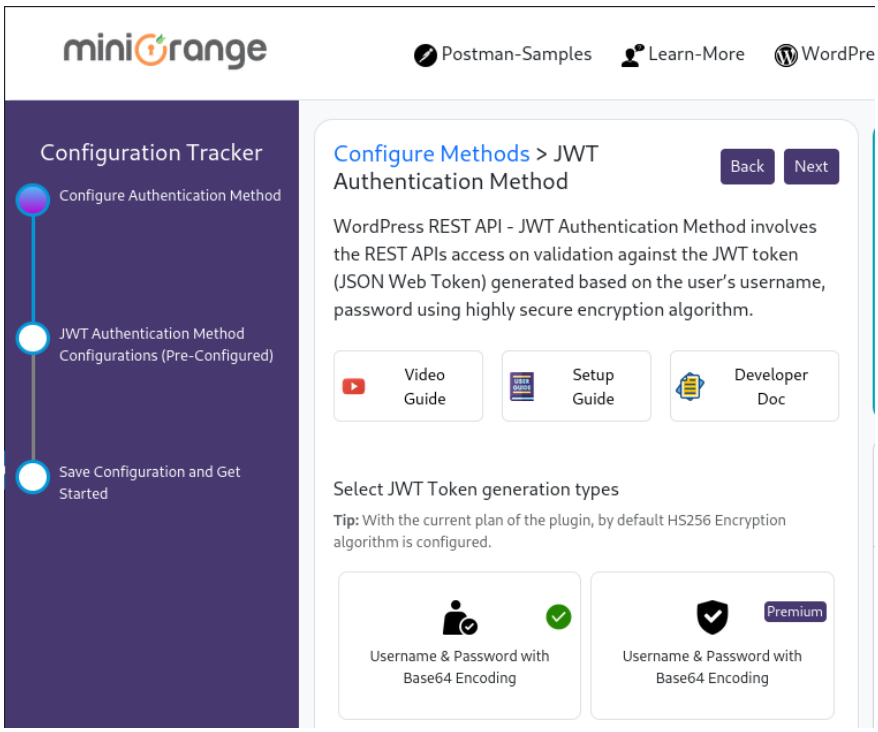
Response

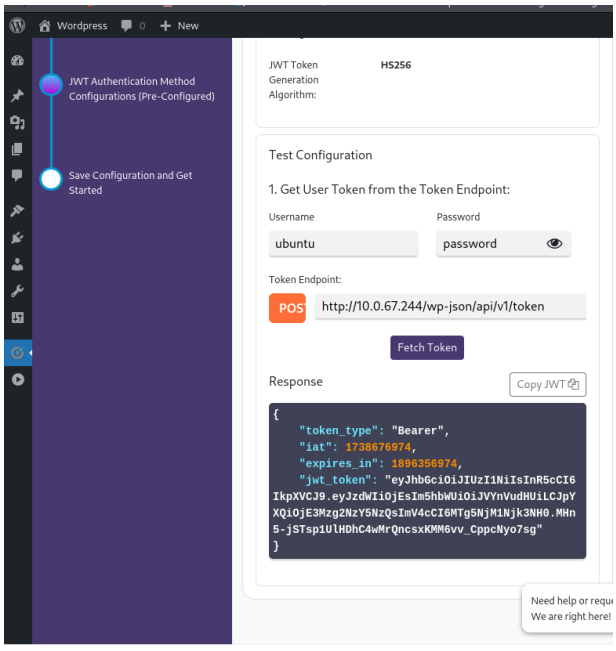

```
[
    {
        "id": 8,
        "date": "2025-01-30T17:53:14",
        "date_gmt": "2025-01-30T17:53:14",
        "guid": {
            "rendered": "http://10.0.67.244/?p=8"
```

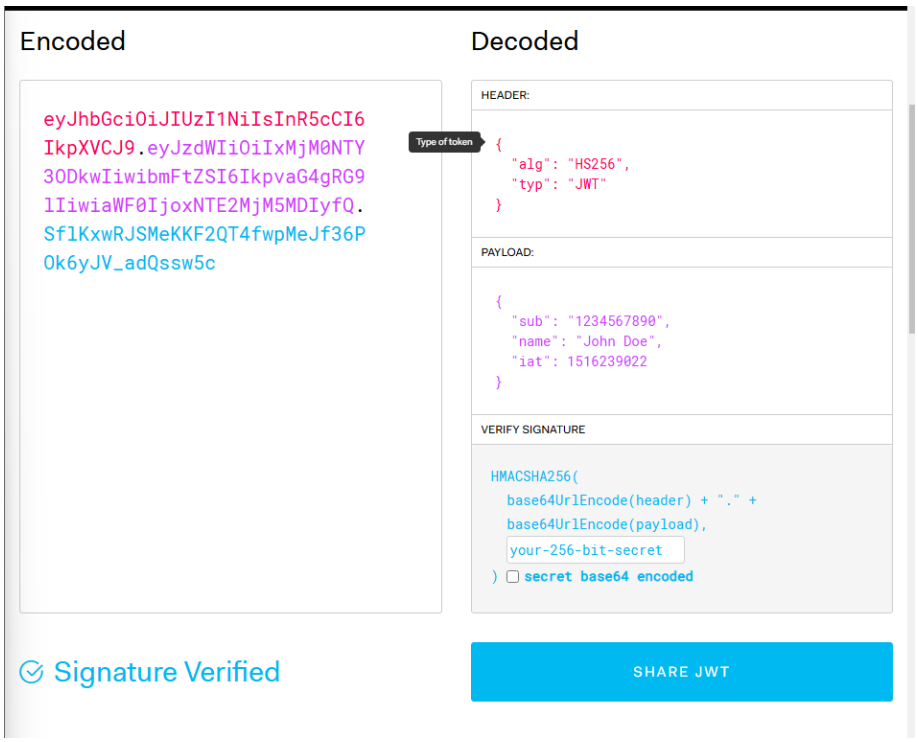


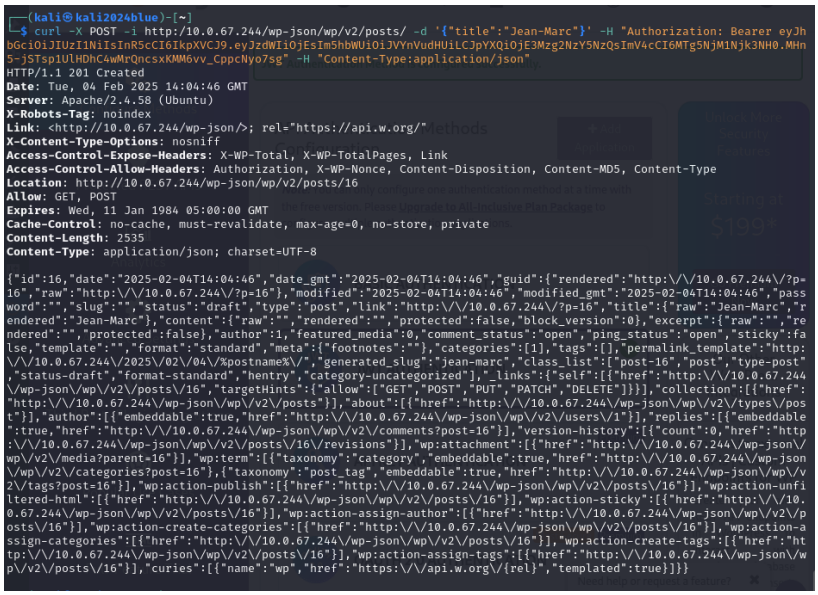

```
┌──(kali㉿kali2024blue)-[~]
└─$ curl -X POST -i http:/10.0.67.244/wp-json/wp/v2/posts/1 -d '{"title":"piere-jean"}' --user ubuntu:password -H "Content-Type:application/json"
HTTP/1.1 200 OK
Date: Tue, 04 Feb 2025 13:37:07 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
Allow: GET, POST, PUT, PATCH, DELETE
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private
Content-Length: 2996
Content-Type: application/json; charset=UTF-8

{"id":1,"date":"2025-01-23T17:34:16","date_gmt":"2025-01-23T17:34:16","guid":{"rendered":"http:\/\/10.0.67.244\/?p=1","raw":"http:\/\/10.0.67.244\/?p=1"},"modified":"2025-02-04T13:37:07","modified_gmt":"2025-02-04T13:37:07","password":"","slug":"hello-world","status":"publish","type":"post","link":"http:\/\/10.0.67.244\/2025\/01\/23\/hello-world\/","title":{"raw":"piere-jean","rendered":"piere-jean"},"content":{"raw":"<!-- wp:paragraph -->\n<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!<\/p>\n<!-- \/wp:paragraph -->","rendered":"\n<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!<\/p>\n","protected":false,"block_version":1},"excerpt":{"raw":"","rendered":"<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!<\/p>\n","protected":false},"author":1,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"footnotes":""},"categories":[1],"tags":[],"permalink_template":"http:\/\/10.0.67.244\/2025\/01\/23\/%postname%\/","generated_slug":"piere-jean","class_list":["post-1","post","type-post","status-publish","format-standard","hentry","category-uncategorized"],"_links":{"self":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1","targetHints":{"allow":["GET","POST","PUT","PATCH","DELETE"]}}],"collection":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts"}],"about":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/types\/post"}],"author":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/users\/1"}],"replies":[{"embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/comments?post=1"}],"version-history":[{"count":2,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1\/revisions"}],"predecessor-version":[{"id":14,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1\/revisions\/14"}],"wp:attachment":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/media?parent=1"}],"wp:term":[{"taxonomy":"category","embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/categories?post=1"},{"taxonomy":"post_tag","embeddable":true,"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/tags?post=1"}],"wp:action-publish":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-unfiltered-html":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-sticky":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-assign-author":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-create-categories":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-assign-categories":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-create-tags":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"wp:action-assign-tags":[{"href":"http:\/\/10.0.67.244\/wp-json\/wp\/v2\/posts\/1"}],"curies":[{"name":"wp","href":"https:\/\/api.w.org\/{rel}","templated":true}]}}
```

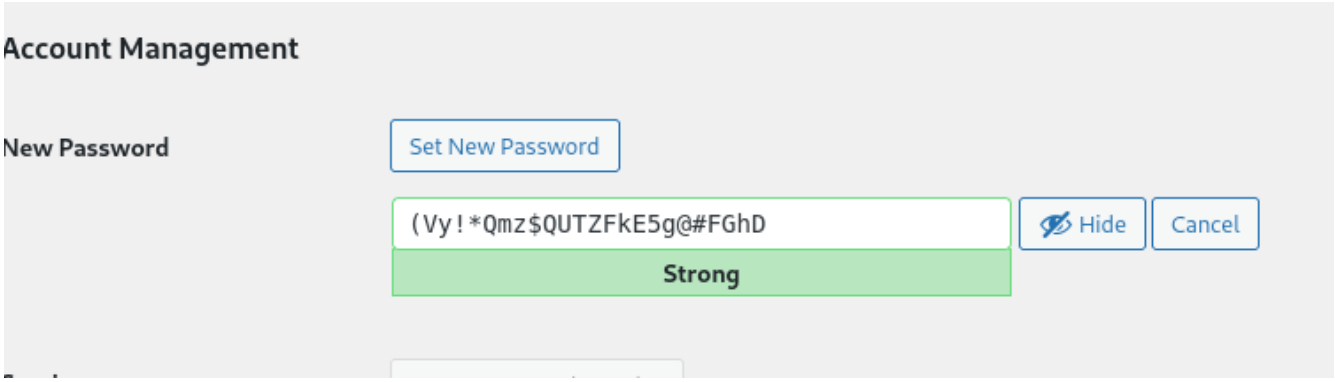

miniOrange
Postman-Samples
Learn-More
WordPre
Configuration Tracker
Configure Authentication Method
JWT Authentication Method Configurations (Pre-Configured)
Save Configuration and Get Started
Configure Methods > JWT Authentication Method
Back
Next
WordPress REST API - JWT Authentication Method involves the REST APIs access on validation against the JWT token (JSON Web Token) generated based on the user's username, password using highly secure encryption algorithm.
Video Guide
Setup Guide
Developer Doc
Select JWT Token generation types
Tip: With the current plan of the plugin, by default HS256 Encryption algorithm is configured.
Username & Password with Base64 Encoding
Premium
Username & Password with Base64 Encoding


Wordpress
New
JWT Authentication Method Configurations (Pre-Configured)
Save Configuration and Get Started
JWT Token Generation Algorithm:
HS256
Test Configuration
1. Get User Token from the Token Endpoint:
Username
ubuntu
Password
password
Token Endpoint:
POST
http://10.0.67.244/wp-json/api/v1/token
Fetch Token
Response
Copy JWT
{
"token_type": "Bearer",
"iat": 1738676974,
"expires_in": 1896356974,
"jwt_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsIm5hbWUiOiJVYnVudHUiLCJpYXQiOjE3Mzg2NzY5NzQsImV4cCI6MTg5NjM1Njk3NH0.MHn5-jSTsp1UlHDhC4wMrQncsxKMM6vv_CppcNyo7sg"
}
Need help or requ
We are right here!

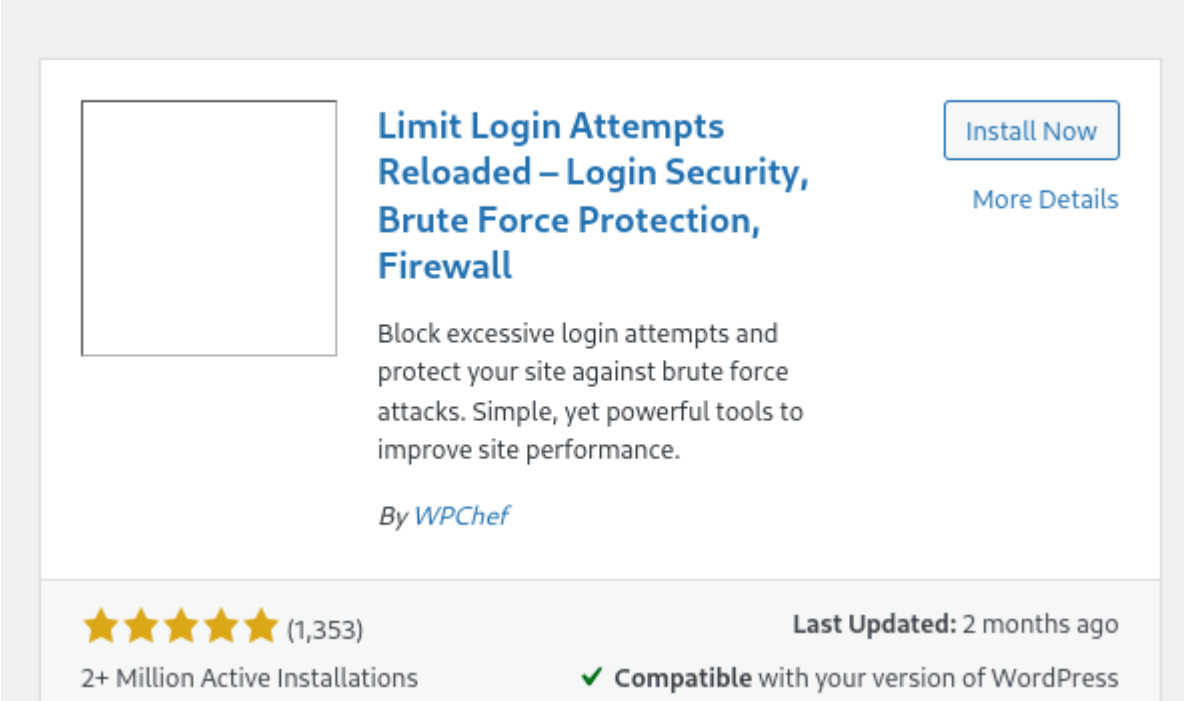


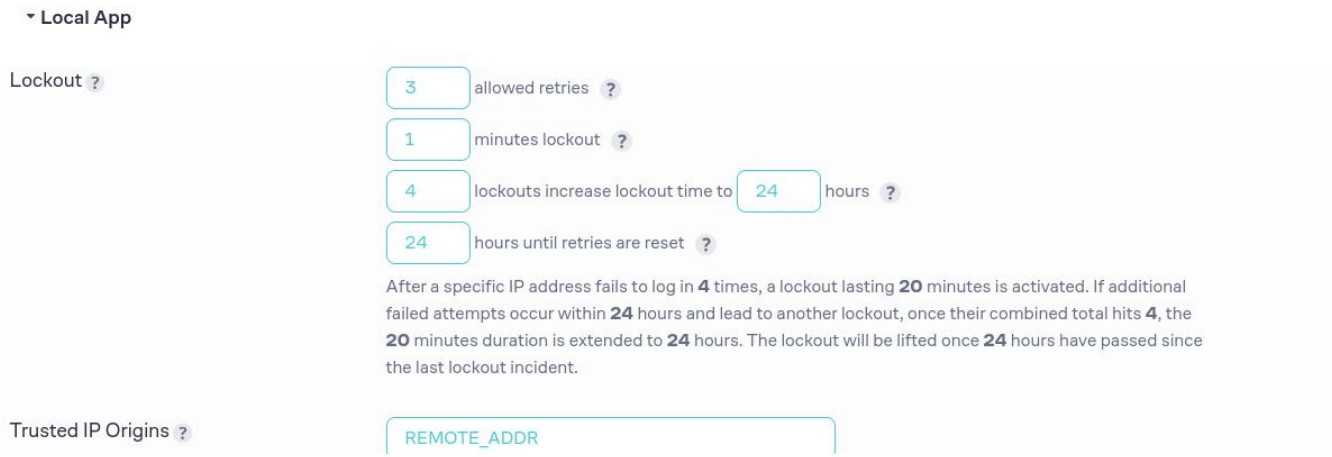




Mot de passe Fort :



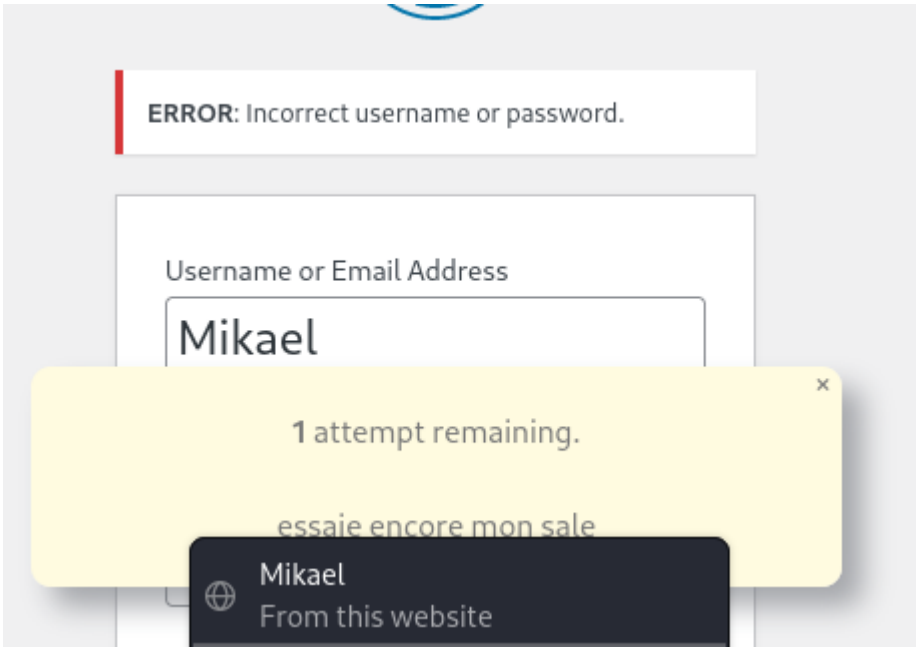

Limitation de connexion échoué

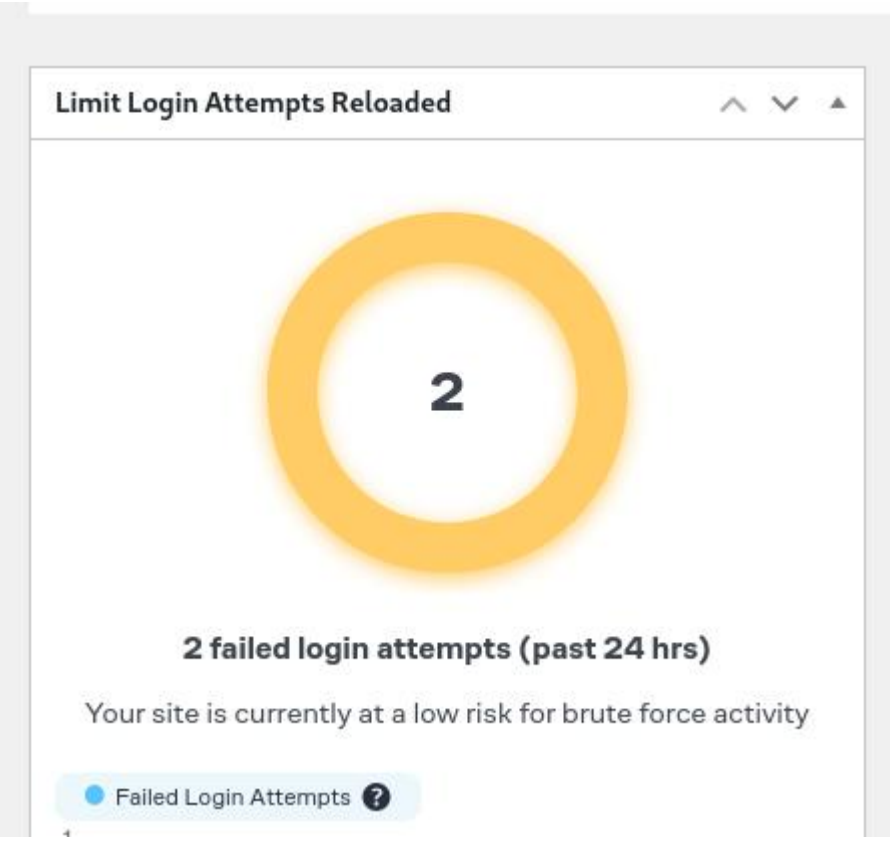


Custom Login Error Message ?

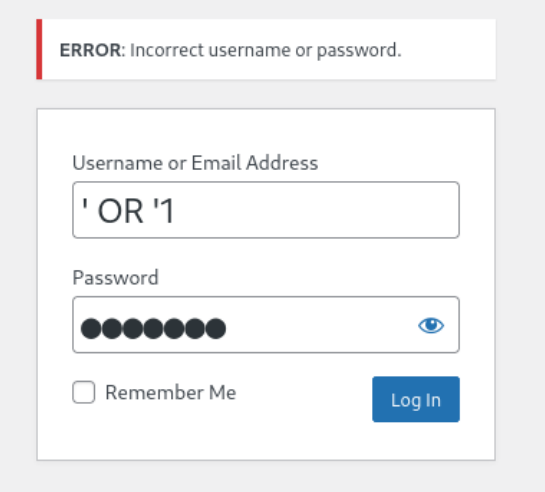
essaie encore mon sale

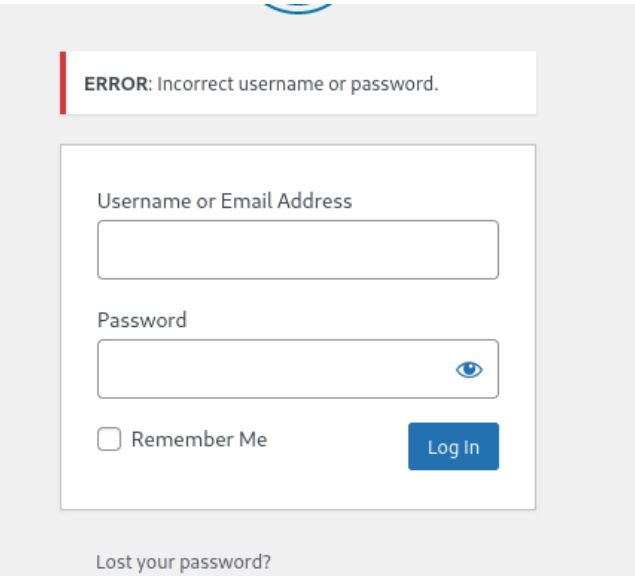





## 2.2 D´emonstration (4 points)

D´emontrez l'efficacit´e de vos protections en effectuant deux attaques (sql injection et hydra par exemple) contr´ees par vos protections.


ERROR: Incorrect username or password.
Username or Email Address
' OR '1
Password
Remember Me
Log In


ERROR: Incorrect username or password.
Username or Email Address
Password
Remember Me
Log In
Lost your password?

Hydra :

Comme l’on peut voir il trouve un mot de passe mais le mot de passe n’est pas valide donc c’est bien, il ne trouve pas un bon mot de passe