WordPress on EC2

Group: Cloudlet
Members: Sahana Nagaraj, Rona Shaji, Pallavi Karunakar Salian
ID: 23325704, 23292709, 23267381

CONTENTS

Video Link: https://www.youtube.com/watch?v=AuO-JP41B28

1. INTRODUCTION

The goal of this project is to build a WordPress site on an EC2 instance on the Amazon Web Services (AWS) platform that is set up with the LAMP stack (Linux, Apache, MySQL, PHP) and to secure both the website and the infrastrcture. Even while AWS offers a secure cloud infrastructure, the WordPress application and virtual machine instance's default settings could nevertheless leave them open to online dangers like malware infections, brute-force attacks, SQL injection, and illegal access. Different security hardening strategies are used at the infrastructure and application levels to mitigate these risks.

To protect data in transit and at rest, this entails limiting SSH access, setting up firewalls and security groups, implementing encryption techniques, and enforcing robust authentication procedures. To further reduce web-based risks, WordPress security features like role-based access control, security plugins, Multi-Factor Authentication (MFA), and automatic upgrades are used.

Following the implementation of these security measures, thorough testing is done to confirm the controls' efficacy. This entails using tools for penetration testing and vulnerability assessment, such as Wireshark for traffic analysis, Nessus for vulnerability identification, and Nmap for network scanning. With the aid of these tools, possible system flaws including open ports, out-of-date software, and unsafe configurations can be quickly fixed. Additionally, AWS CloudWatch, GuardDuty, and third-party security solutions are integrated with continuous monitoring and logging systems to identify and address security events instantly.

2. APPROACH AND PROJECT PLANNING

We began by starting an AWS EC2 instance, which is effectively a Linux-based virtual computer that is set up in the cloud. But we soon discovered that it was not by default secure, leaving it open to possible intrusions. We first used SSH (Secure Shell) to connect to our instance from our local computer in order to secure it. After connecting, we set up a LAMP stack (Linux, Apache, MySQL, PHP), which offers the necessary building blocks for hosting a website. We set up MariaDB, the database system that runs WordPress, and Apache, a popular web server. We discovered that our server was missing crucial security protections after verifying that it was operating correctly by using a web browser to view its public IP address. We set up SSL/TLS encryption to solve this, guaranteeing that all user-to-website data exchanges are safe and secured.

In order for customers to access the website using a memorable domain name rather than an IP address, we then connected a custom domain with our instance. After WordPress was set up, we concentrated on protecting it by putting in place a number of security measures. We started by hiding the normal WordPress admin login page so that attackers and automated bots couldn't discover it with ease. In order to lower the possibility of unwanted access, we additionally configured AWS security groups to limit SSH access to only particular IP ranges and regulate access to our EC2 instance. We added an additional layer of security by installing the Wordfence security plugin within WordPress, which enabled Two-Factor Authentication (2FA) for administrator and user logins. We set up Wordfence to automatically block IP addresses following several unsuccessful login attempts in order to guard against brute-force attacks. To further improve security, we also maintained IP whitelists and blacklists based on real-time threat intelligence.

Using the Wordfence plugin, we configured a Web Application Firewall (WAF) to bolster our defenses against web-based threats. This firewall allowed us to take proactive mitigation actions by continuously monitoring and recording security incidents, which gave us important insights into possible intrusions. After implementing all security improvements, we used tools like Nmap, Nessus, and Wireshark to do penetration testing in order to find weaknesses in the WordPress system and cloud architecture. By these efforts, we were able to successfully turn a cloud instance that was once susceptible into a safe, well-defended online environment that complies with cybersecurity best practices.

3. CLOUD PLATFORM SELECTION

The top global cloud service provider, Amazon Web Services (AWS), provides a variety of services, such as databases, networking, storage, computation, and artificial intelligence (AI)/machine learning (ML). AWS offers versatile, scalable, and reasonably priced solutions for companies of all sizes, from start-ups to major corporations. AWS is the leading company in the cloud computing sector, with a market share of more than 40% and a reputation for dependability and creativity. Since its debut in 2006, AWS has consistently delivered cutting-edge services like S3 for safe storage and EC2 for scalable computing, completely changing how companies create, test, and implement applications. Its pay-as-you-go pricing structure enables businesses to save expenses without sacrificing availability or performance. With its several regions and availability zones, AWS's global architecture guarantees minimal latency and uninterrupted business operations everywhere.

Furthermore, AWS offers strong security and compliance capabilities that guarantee compliance with regulations such as GDPR and HIPAA. Organizations may improve governance and security by utilizing tools like AWS CloudTrail for activity tracking and AWS IAM for access management. All things considered, AWS is the preferred platform for digital transformation because it enables companies to streamline operations, spur innovation, and grow with ease.

Secure: To safeguard client data, AWS has a thorough, end-to-end security strategy that includes operational, technical, and physical security measures. To guarantee the greatest levels of protection across all of its cloud services, this includes network security, identity and access management, data encryption, and frequent compliance assessments. Visit the AWS Security Center to learn more.

Global presence: With a 31% market share and a global footprint spanning 16 geographical regions and 44 Availability Zones (AZs), AWS is a major player in the cloud computing industry. Applications are kept robust and available even in the event of failures in designated zones thanks to the numerous AZs—separate data centers built for fault tolerance and high availability—that make up each region.

Businesses can select locations near their user base thanks to this global infrastructure, which reduces latency and improves performance. By facilitating the replication of data and services across geographical boundaries, AWS's architecture also aids in disaster recovery by guaranteeing business continuity. With this vast network, AWS gives users the freedom to create scalable, low-latency applications while satisfying local data residency requirements.

Scalable and high performance: The Auto Scaling and Elastic Load Balancing features of AWS dynamically modify resources to manage fluctuating traffic volumes, guaranteeing peak performance while preserving cost effectiveness. When you have access to Amazon's extensive worldwide infrastructure, you can swiftly scale apps to accommodate surges in traffic or reduce them when demand is low without sacrificing functionality.

Cost-Effective: Because of AWS's pay-as-you-go pricing model, companies may only pay for the resources they utilize, which lowers operating expenses and increases budget flexibility. Because there are no upfront fees or long-term agreements, businesses can adjust their usage to meet demand and maintain cost effectiveness throughout. To learn more about how much AWS costs compared to other hosting options, visit the AWS Economics Center.

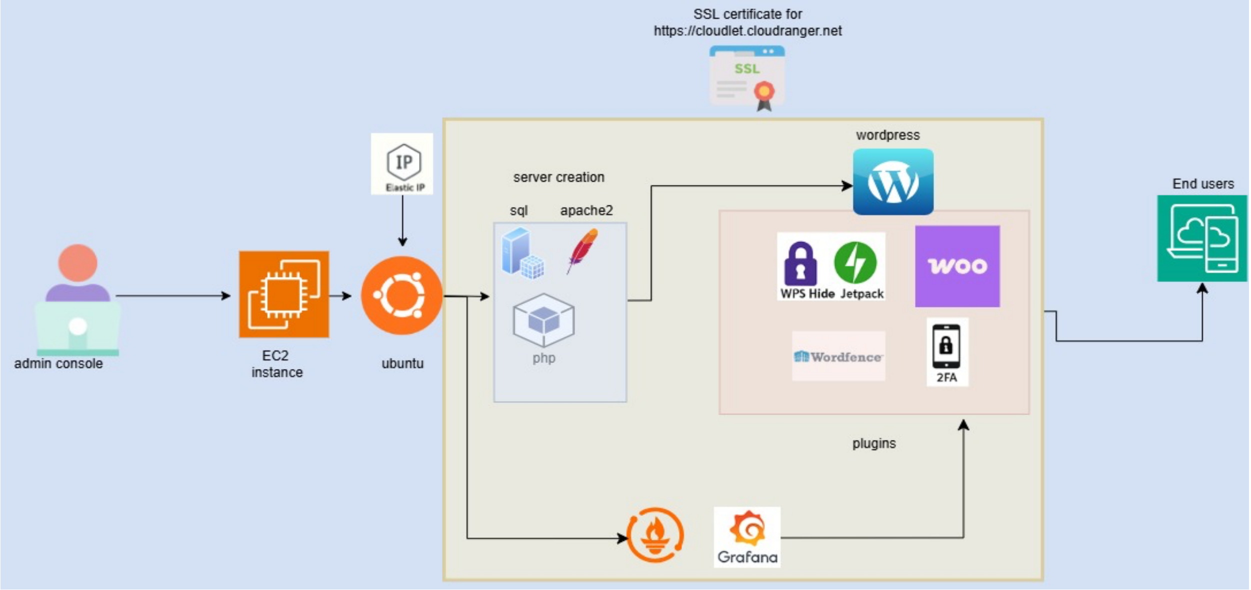


Figure 1: Security Architecture

4. TOOLS, METHODOLOGIES, FRAMEWORKS AND BENCHMARKING

Lamp Stack: A foundation for the environment requires the installation of LAMP stack because it is compatible with WordPress and provides straightforward installation on Ubuntu OS. An organization requires server infrastructure that operates reliably when running WordPress.

WordPress: WordPress functions as the chosen content management system (CMS) because of its adaptable features which provide users with easy-to-utilize tools to run their sites. Its selection focuses on finding a platform which enables customization through plugins and theme options to establish secure online presence development.

Certbot: The setup relies on Certbot to create SSL/TLS certificates which secure HTTPS transmission between server users. Protecting communication is possible through this mechanism which prevents interception and eavesdropping incidents.

Wordfence: Wordfence received selection because it delivers dedicated WordPress website security through its features for authentication and force protection alongside IP moderation capabilities. This security plugin helps WordPress to become more resilient to potential risks through its vulnerability detection system.

Jetpack: Jetpack provides users with Automatic’s versatile plugin that includes security features as well as performance and site management abilities. With real-time backup tools together with malware scanning and spam protection and site stats this system makes possible an extensive set of features. Jetpack stands out as an excellent tool which extends functionality to your WordPress website[1].

UpdraftPlus: WordPress users benefit from UpdraftPlus as their preferred backup solution along with their migration requirements. The plugin provides backup scheduling functionality together with site restoration capabilities and domain and host migration features. The plugin allows users to connect their storage to Dropbox, Google Drive and Amazon S3 and many other options[2].

Inactive Logout : This plugin implements automatic user logout when users become inactive thus protecting site security. Lazy administrators can prevent unauthorized access by using this plugin to terminate idle sessions while still having control of basic settings through time-out options and custom logout text[3].

WPS Hide Plugin: The WPS Hide Login plugin serves as a lightweight tool which lets users modify their WordPress login page address for enhanced security purposes. The default login page becomes inaccessible by using this plugin which also works with most WordPress environments[4].

Prometheus: Prometheus depends on exporters and integrations to increase its operational range. These systems transform information from external third-party programs so Prometheus can extract it which facilitates data collection. The third-party database exporters MySQL and PostgreSQL together with hardware measurement tools and messaging system RabbitMQ comprise examples of Prometheus exporters[5].
Prometheus establishes integration capabilities by working with third-party solutions that detect services and provide storage facilities and alert detection systems. The tool enables compatibility with Kubernetes service and offers support for Grafana Mimir along with Alert manager integration. Strong customization features of these tools enable them to function powerfully for observability tasks. Inform me if you prefer a detailed analysis on any particular plugin or feature within the system.

Grafana: Grafana utilizes three principal plugin categories. The Panel Plugins functionality lets you develop specific visual components for dashboard display. The plugin collection for Grafana includes bar charts together with heatmaps and geomaps2[6].
Graphic information sources through these plugins allow Grafana to retrieve data from different operational systems such as database collections and application programming interfaces and logging systems. The platform offers plugins which connect it to Google Sheets and Elasticsearch together with MongoDB3.
App Plugins: These bundle data source, panels, and dashboards into a cohesive experience. With its Zabbix app plugin users receive a specialized monitoring interface for their needs.

5. TECHNICAL TESTING

The evaluation of cloudlet.cloudranger.net used industrial standard applications to measure performance together with security weaknesses and encryption strengths and web application integrity. The selection of tools followed their unique ability to reveal system weaknesses together with practical recommendations.

Google Page Speed Insights:

The primary duty of Google PageSpeed Insights involves evaluation of website loading speed together with rendering efficiency while assessing user experience quality. The evaluation tool analyses two key performance indicators which include First Contentful Paint (FCP) that measures initial page element load time and Largest Contentful Paint (LCP) that evaluates main content rendering duration. The metrics

Speed Index and Total Blocking Time (TBT) and Cumulative Layout Shift (CLS) form part of the additional assessment tools used to guarantee frictionless user interaction.
The tool should offer performance scores which would depict optimization zones including JavaScript trimming and caching implementation as well as image file optimization. A rating above 90 suggests good outcome but results between 50–90 show potential growth points.

Nmap (Network Mapper):
Nmap serves as a discovery tool that discovers network ports which are open along with active services and reveals firewall information and system specifications. The application sends unaltered IP packets to examine network host devices while searching for possible security weaknesses throughout the infrastructure. Nmap provides broad port and service scans which help organizations detect potential threats that attackers might utilize.
The test goal consisted of identifying presently accessible ports alongside running services and networking configuration problems that needed security enhancements. The protection of a system depends on having few unnecessary exposed ports and the latest software installations which minimize attack possibilities.

Nikto (Web Server Vulnerability Scanner):
The web server scanner Nikto serves the purpose of discovering web server misconfigurations coupled with outdated software versions and files containing security vulnerabilities. Nikto conducts standard security assessments alongside tests which focus on specific web server requirements enabling it to identify exclusive server vulnerabilities. The web server scanner Nikto displays received cookies during its operation which helps evaluate session protection.
The security analysis sought to detect outdated software modules together with unsecured system directories and improper HTTP header configurations which create potential security risks. The correct configuration of a web server is needed to prevent both the disclosure of important files and its deployment of out-of-date versions of server applications.

Wireshark (Network Packet Analyzer):
Wireshark functions as an online traffic analysis software system which instantly tracks data packets during active networks. The tool allows users to analyse device-server communication in depth for revealing unsecure data communications while identifying encryption issues along with unauthorized data transfers.
The assessment checked the SSL/TLS encryption of the website and investigated if any unencrypted network traffic data appeared. Protected systems need to operate with encrypted data transfer while every sensitive piece of information needs to stay hidden from view.

WPScan (WordPress Security Scanner):
WPScan represents a security scanning utility that identifies WordPress-based vulnerabilities along with plugin issues and configuration errors as well as backup exposure and outdated WordPress installations. Due to its high adoption rate numerous security threats attack the vulnerabilities found in WordPress theme and plugin systems together with core files.
This security test was expected to detect plugin vulnerabilities in addition to theme and core WordPress component flaws as well as reveal any publicly accessible admin panels or backup files. A properly secured WordPress website must have recently updated plugins/themes together with restricted access to the admin panel.
This tool is needed to detect both authentication weakness and incorrect cookie

management and input validation issues that attackers might exploit. A secure application must correctly authenticate users and block dangerous input and stop unauthorized system access.

Qualys SSL Labs (SSL/TLS Security Assessment):
Qualys SSL Labs serves as an SSL/TLS configuration security assessment tool which evaluates certificate strength while examining encryption protocols as well as cipher suite integrity. Security in communication depends on proper SSL/TLS implementation because it ensures both confidentiality and trustworthiness between networked devices.
The test evaluated SSL/TLS configuration practices to determine correct implementation of strong encryption methods and valid certificates and secure cipher suites. High-grade SSL configurations need to eliminate both weak encryption protocols and to avoid risks of invalidation or expiration of certificates.
These security and performance tools helped achieve a comprehensive evaluation which confirmed both security and operational efficiency of the website. The evaluation results from these individual tools give complete knowledge about web application security and network integrity and website optimization.

6. FINDINGS AND RISK RATING

Nmap:
Nmap scan was run on the instance to identify the open ports, detect active services and security threats. The scan identified four accessible ports: 22/ssh, 80,https, 443 https/ssl and 3000/tcp. The SSH port(22) is configured to allow only the host ip using the keypair. It uses the version 8.7 and the restriction prevents unauthorized remote access reducing the risks from brute force attacks and unapproved login attempts. The web traffic security system runs via Apache HTTP and HTTPS (version 2.4.62) on Amazon Linux with OpenSSL 3.0.8 through ports 80 and 443. The system contains Grafana login page which operates through port 3000. More security features should be implemented on the public login page because it remains accessible without authorization thus presenting a risk of unauthorized access.

Security headers present in the scan reveal important protective measures that include deny options through X-Frame-Options and block-level security enabled by X-XSS-Protection. These headers work together with mandatory encryption standards to develop secure internet connections.
This scan had its main goal to detect running applications and check operating system versions and application software levels and locate vulnerable security areas. The infrastructure demonstrates comprehensive protection because SSH has proper restrictions and Apache and Grafana exist under secure conditions and necessary security headers are implemented. The system requires ongoing monitoring along with routine software maintenance updates and additional security features to stay protected from new threats in the medium and long term.

Google Page Speed:
Google Page Speed Insights examined "https://cloudlet.cloudranger.net/ " to evaluate various elements of site performance, accessibility and standard practices as well as search engine optimization. The evaluation analysed potential areas of improvement for faster loading speed as well as better user experience and modern web standard compliance.
The website reached a performance score of 87 which indicates it has generally fast load times but still presents a few areas for improvement. First Contentful Paint (FCP) reached 0.8 seconds thus delivering a fast but smooth viewing experience of the

website. The main content displayed efficiently due to a Largest Contentful Paint score of 1.7 seconds. Speed Index reached a rating of 2.6 seconds meaning the website loads its visible content quickly. The Total Blocking Time measurement for this site showed 0ms which indicates fast JavaScript execution did not delay users from continuous interaction. The page elements kept their positions steady during the measurement period because the recorded Cumulative Layout Shift value was 0. In addition to performance testing the evaluation checked the usability elements and consistency with best practices requirements. Users with disabilities experience smooth navigation through all interfaces because the site achieved a 96-accessibility score. Modern development standards and security configurations and responsive design principles were fully implemented according to the best practice evaluation which awarded it a precision 100 score.

An SEO score of 83 indicates the website shows effective optimization for its structure but more improvements are needed specifically for metadata optimization and structural data implementation and index optimization. The evaluation process focused on identifying ways to improve website speed rates together with UX standards and search engine discoverability metrics. The site performs well but additional efficiency gains would develop by optimizing SEO elements and by reducing render-blocking resources and through image format refinement.

Qualys SSL labs:

The security of SSL/TLS configuration for cloudlet.cloudranger.net (34.230.235.225) received evaluation through Qualys SSL Labs. The platform evaluates multiple core security characteristics from certificate lifespan to protocol compatibility along with key negotiation methods and cryptographic option power to generate a global safety measure.

The certificate received grade "A" on the evaluation signifying that it has high level of security standards. TLS 1.3 operates on the server to provide the latest and most secure encryption protocol that ensures powerful data transmission confidentiality. The security rating demonstrated strong performance in key exchange and cipher strength measures because these parameters enhance encryption resistance against security risks.

The main purpose of this evaluation was to ensure the best security protocols were followed and to find potential enhancements needed. Secure encryption reliability and data integrity with user trust benefits arise from an SSL/TLS setup which is correctly configured. Continuous support of encryption standards combined with certificate expiration tracking and refined protocol setup methods help organizations maintain high security levels.

WPSC Scan:

A WPScan was run on the domain to assess the security of the Wordpress core, plugin, themes and configurations. The scan used WPScan’s latest vulnerability database for accurate results. By entering the website address, WPScan examined important parts of the WordPress setup. It found exposed areas, checked security tags, and reviewed active plugins to identify potential weaknesses that hackers might exploit.

During the check, it was confirmed that WordPress version 6.7.2 is used, which is the latest, ensuring the core system is up to date. The WooCommerce plugin version 9.7.1 is also the latest stable release. While updating plugins helps reduce risks, other concerns were found. The file named robots.txt is public and reveals restricted directories like /wp-content/uploads/wc-logs/, /wp-content/uploads/woocommerce_transient_files/, and /wp-admin/admin-ajax.php, which might disclose sensitive site information. This should not be an issue since directory listing has been disabled by adding disabling query into the configuration

file. Another security issue would be that XML-RPC is turned on, which is often used by hackers for brute-force login attempts, which is also tackled as we have brute force protection offered by wordfence. The presence of an external WP-Cron was also noted; if it's not set up properly, it can make the site vulnerable to DDoS attacks because it can allow too many automated requests. Also, the WordPress readme file is publicly accessible. This file unintentionally might disclose version details, which would aid the attackers in targeting known vulnerabilities.
The aim of this check was to see if the website follows WordPress security best practices. The main systems and plugins seem to be up to date there are areas for improvement to increase the site's protection. XML-RPC should be turned off, restrict access to robots.txt and readme.html, and monitor WP-Cron activity could minimize potential security risks. Taking these actions would make the WordPress site much safer, reducing exposure to common attack methods and ensuring it remains stable in the long run.

Wireshark:
We used Wireshark to examine the WordPress login traffic. This analysis confirmed that login details were securely encrypted with TLS 1.3. The Client Hello and Change Cipher Spec packets confirmed a correct handshake process. The Application Data was fully encrypted, so login details were never exposed as plain text. We found no immediate security issues with how the login information was transmitted.

Nikto Scanning:
Nikto tried to find security weaknesses by sending lots of requests, but the Wordfence firewall blocked these attempts. This action stopped Nikto from fully checking the website's security. Wordfence proved its effectiveness at detecting and stopping automated scans, showing its strength in protection. However, this limits the ability to test for weaknesses properly. For a complete security check, we need to change the firewall settings or temporarily allow the use of scanning tools.

7. CHALLENGES & LIMITATIONS IN SECURITY TESTING

Challenges in Securing the System

- Our limited ability to customize IAM role restricted our security aspect.
- We use free versions of the security plugins which offer only basic protection causing restrictions on them.
- We had limited access to advanced AWS security services due to budget constraints.
- We realized that failure to update WordPress themes and plugins regularly can introduce security risks at any point in time.
- We made a lot of manual changes; this would lead way to errors.
- Our EC2 instance does not make use of any backup, so there is risk of downtime, however the db and websites have backups.
- Lack of dedicated DDoS protection leaves websites open to large-scale attacks.

Evaluating Security

- Wireshark confirms that the credentials are encrypted, but more analysis of security headers is necessary.
- Nikto and WPScan found known security issues but they may fail to detect new, undiscovered ones.

- Although Wordfence blocks harmful traffic, it can mistakenly identify real users, so rule adjustments are necessary.
- Very strict firewalls may prevent access for legitimate users and automated services as in our case when conducting nikto scans.

8. SG GOALS

Cloud computing extends its innovative powers beyond technological boundaries, so it serves as a vital instrument for the United Nations to achieve Sustainable Development Goals (SDGs). This project aims to construct a secure cloud infrastructure on AWS which provides scalability as well as reliability. The goal for building reliable infrastructure and fostering sustainable industrial development stands parallel to UN SDGs 9 and 12 which address innovation promotion and sustainable production patterns. Establishing resistant infrastructure and developing inclusive industrial operations and launching innovative solutions thus stands as a central priority.

9. SUMMARY

This project gave us insights to both the advantages and disadvantages of setting up a website on AWS. The Wireshark packet capture showed that our login data is safely encrypted to protect against interception while Nikto scanning and Wordfence logs identified potential attacks, underlining the importance of monitoring firewalls and securing plugins and keeping them updated at all times. We also had to deal with issues like IAM restrictions, financial limitations, and worries about the scalability of free-tier EC2 instances which directly impacted the overall security. To enhance security, we recognized the need to optimize IAM policies, improve firewall settings, adopt modern TLS protocols, conduct regular vulnerability scans, and keep everything updated to the latest version. Ultimately, we understood the importance of maintaining a balance between security, performance, and usability to ensure the website remains protected over time. Balancing these elements is essential for the site's long-term safety and functionality.

Contribution

Member	Report
Sahana	1,2,3
Rona	5,6,9
Pallavi	4,7,8

The practical part was a joined effort and everyone had equal contributions.

10. REFERENCE

[1] T. EMB, “The Ultimate Guide to Jetpack Plugins for WordPress.” Accessed: Apr. 03, 2025. [Online]. Available: https://blog.emb.global/jetpack-plugins-for-wordpress/?form=MG0AV3

[2] “UpdraftPlus home,” TeamUpdraft. Accessed: Apr. 03, 2025. [Online]. Available: https://teamupdraft.com/updraftplus/

[3] Deepen, “Inactive Logout,” WordPress.org. Accessed: Apr. 03, 2025. [Online]. Available: https://wordpress.org/plugins/inactive-logout/

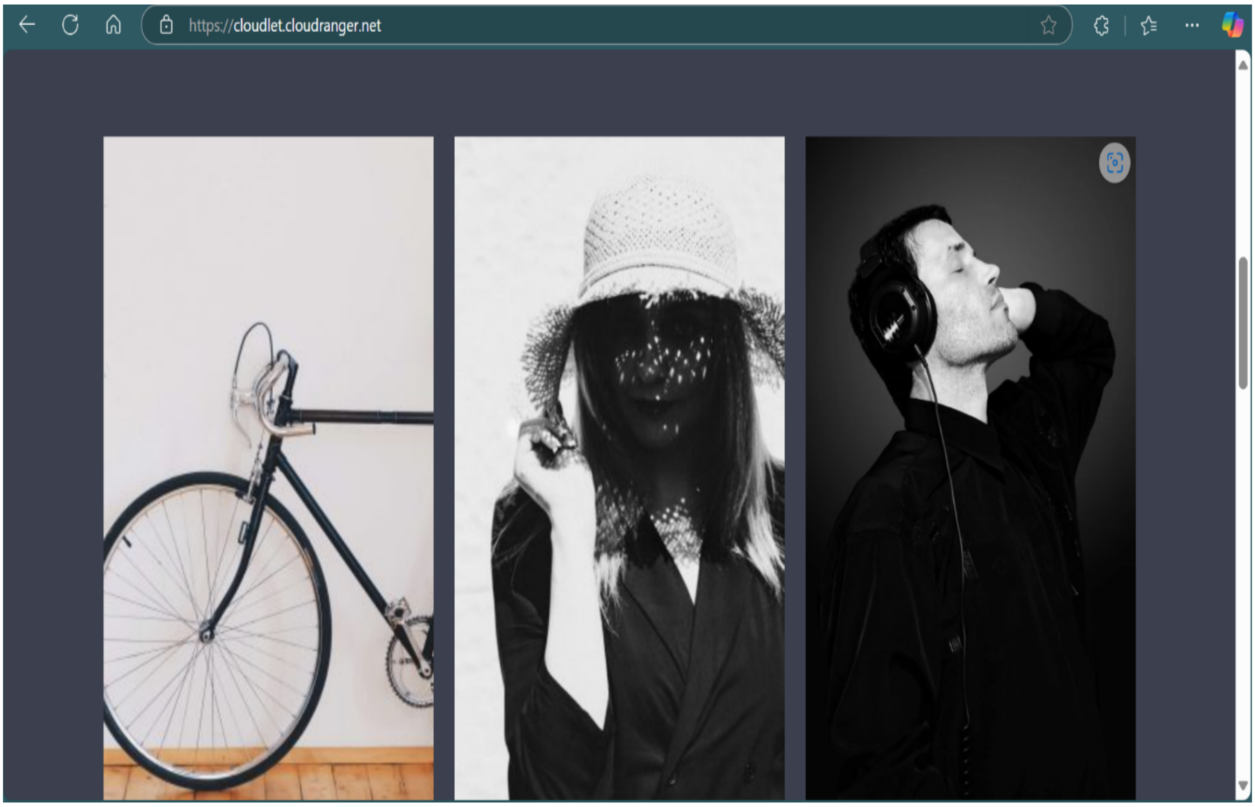
[4] R. Giaquinto, “How to Use WPS Hide Login to Protect the WordPress Admin Page,” GreenGeeks. Accessed: Apr. 03, 2025. [Online]. Available: https://www.greengeeks.com/tutorials/use-wps-hide-login/

[5] Prometheus, "Exporters and integrations | Prometheus." Accessed: Apr. 03, 2025. [Online]. Available: https://prometheus.io/docs/instrumenting/exporters/?form=MG0AV3&form=MG0AV3

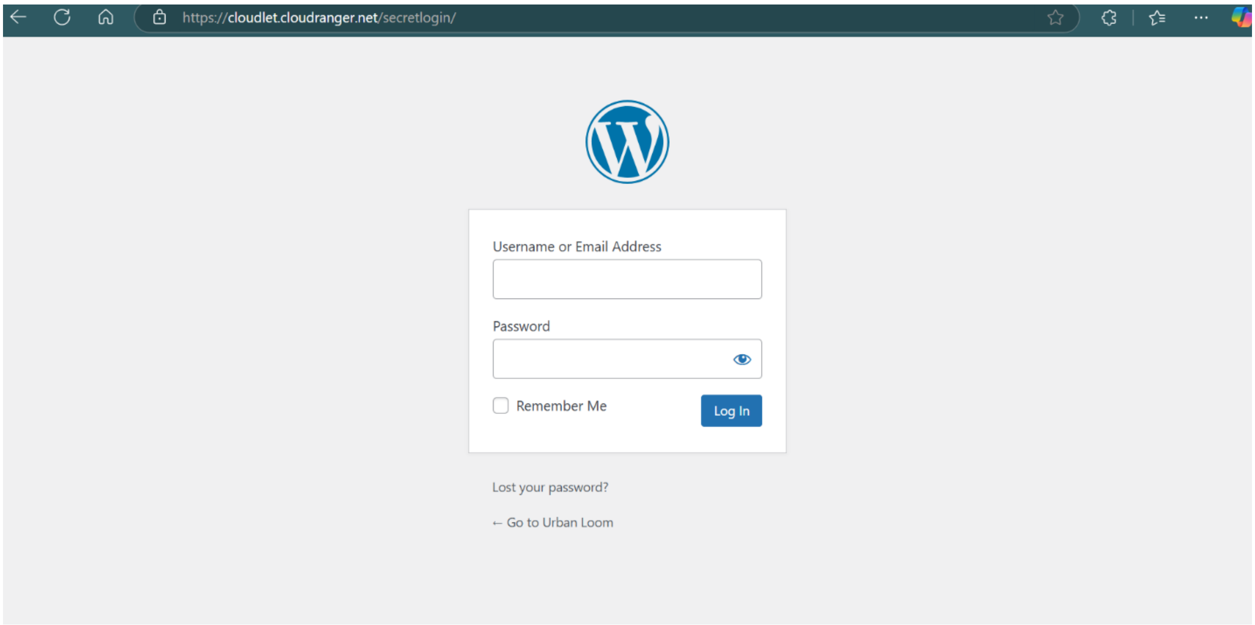
[6] "Grafana Plugins - extend and customize your Grafana," Grafana Labs. Accessed: Apr. 03, 2025. [Online]. Available: https://grafana.com/grafana/plugins/

APPENDIX

Website:



Login page:



Username or Email Address

Password

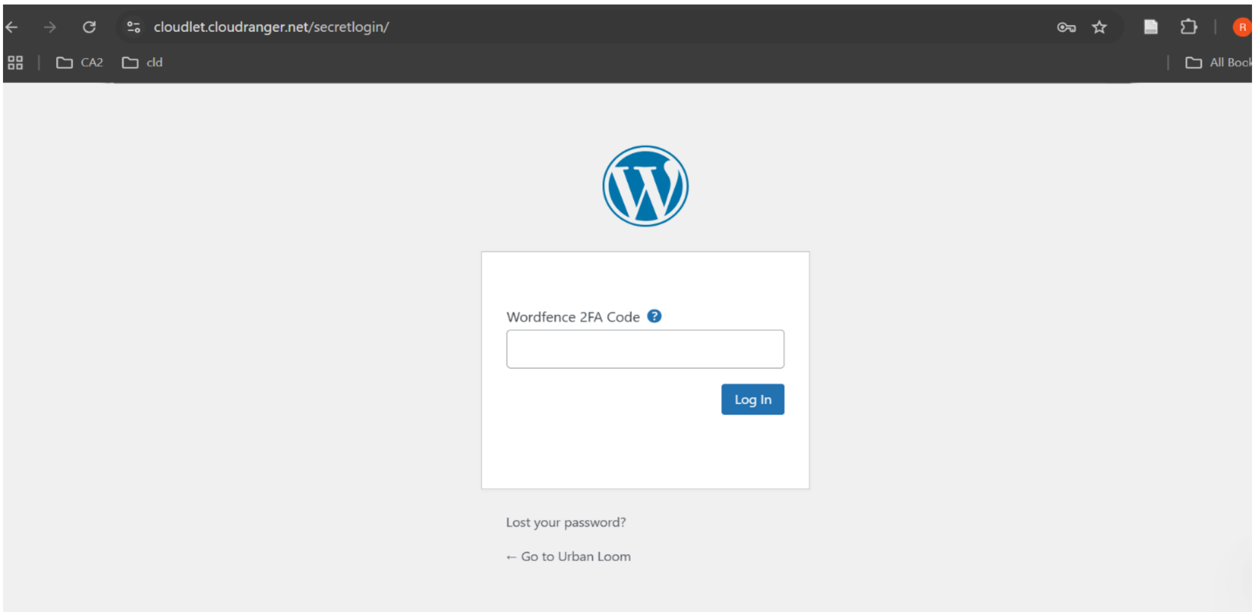
□ Remember Me

Log In

Lost your password?

← Go to Urban Loom

2FA:



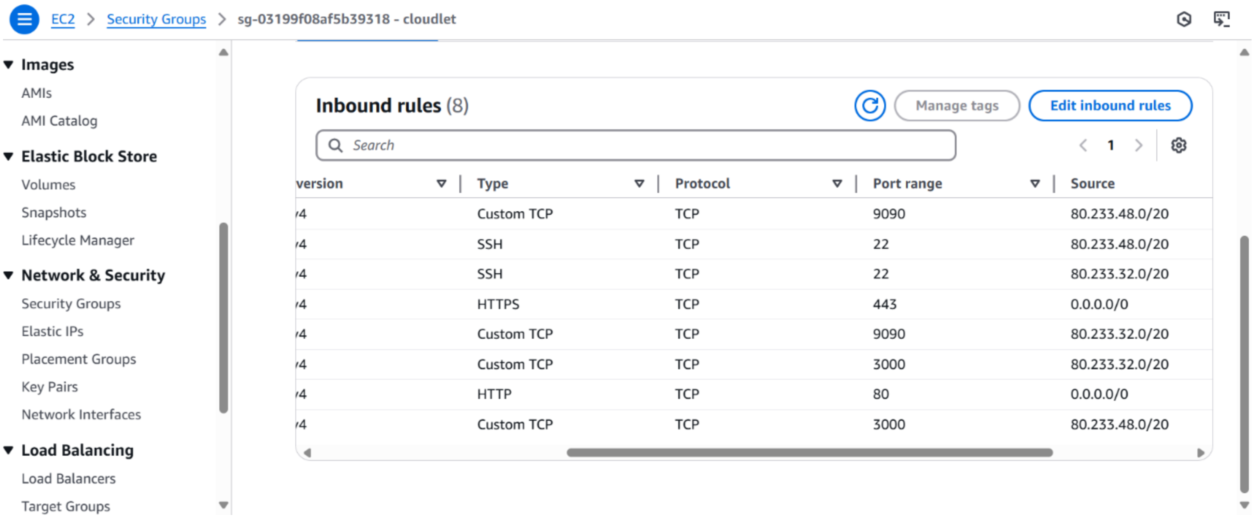
cloudlet.cloudranger.net/secretlogin/

Wordfence 2FA Code

Lost your password?

← Go to Urban Loom

Security Group:

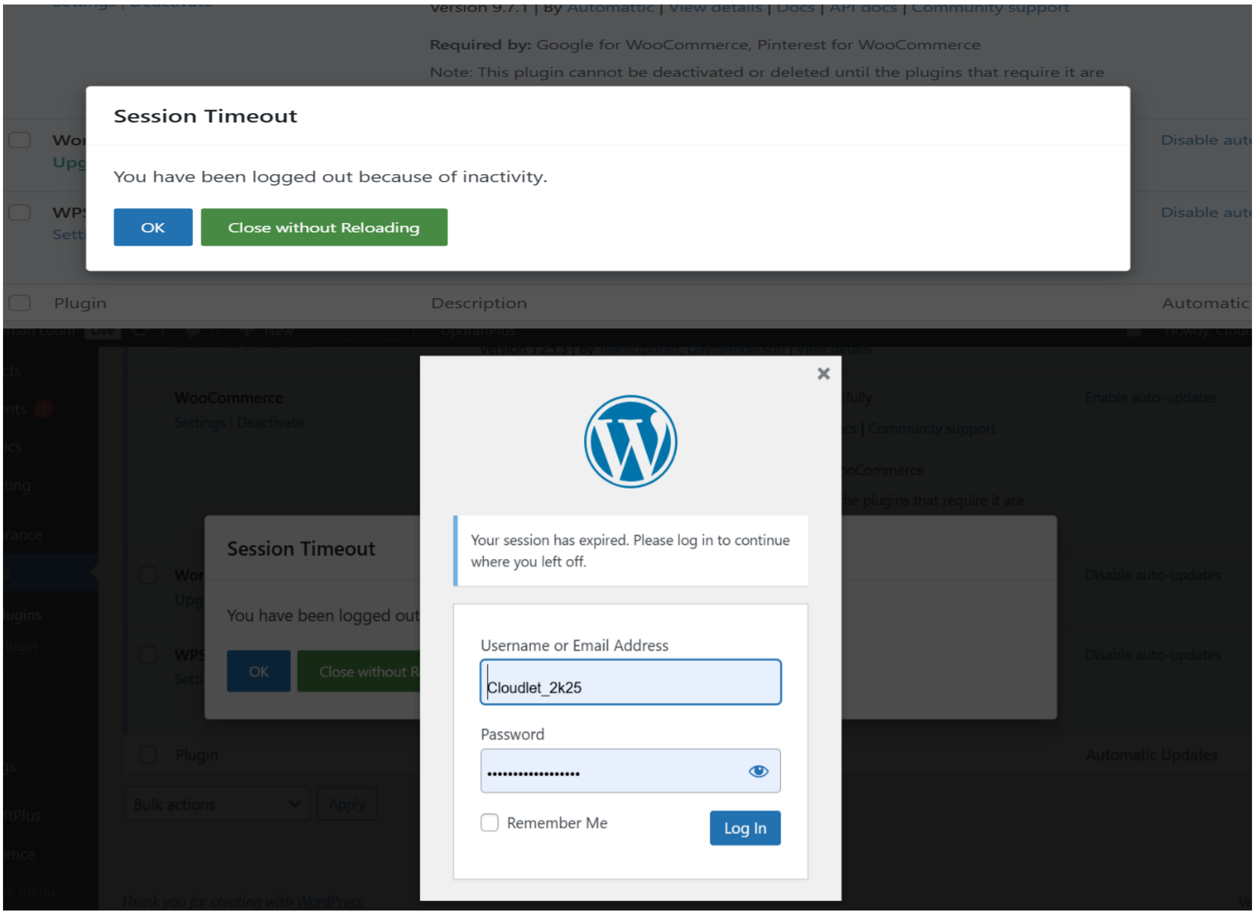


EC2 > Security Groups > sg-03199f08af5b39318 - cloudlet

Inbound rules (8)

version	Type	Protocol	Port range	Source
4	Custom TCP	TCP	9090	80.233.48.0/20
4	SSH	TCP	22	80.233.48.0/20
4	SSH	TCP	22	80.233.32.0/20
4	HTTPS	TCP	443	0.0.0.0/0
4	Custom TCP	TCP	9090	80.233.32.0/20
4	Custom TCP	TCP	3000	80.233.32.0/20
4	HTTP	TCP	80	0.0.0.0/0
4	Custom TCP	TCP	3000	80.233.48.0/20

Timeout:



Version 9.7.1 | By Automattic | View details | Docs | API docs | Community support

Required by: Google for WooCommerce, Pinterest for WooCommerce

Note: This plugin cannot be deactivated or deleted until the plugins that require it are

Session Timeout

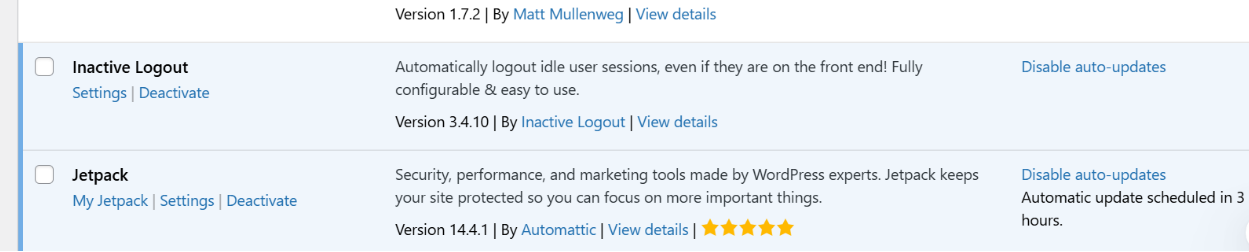
You have been logged out because of inactivity.

Your session has expired. Please log in to continue where you left off.

Username or Email Address: Cloudlet_2k25

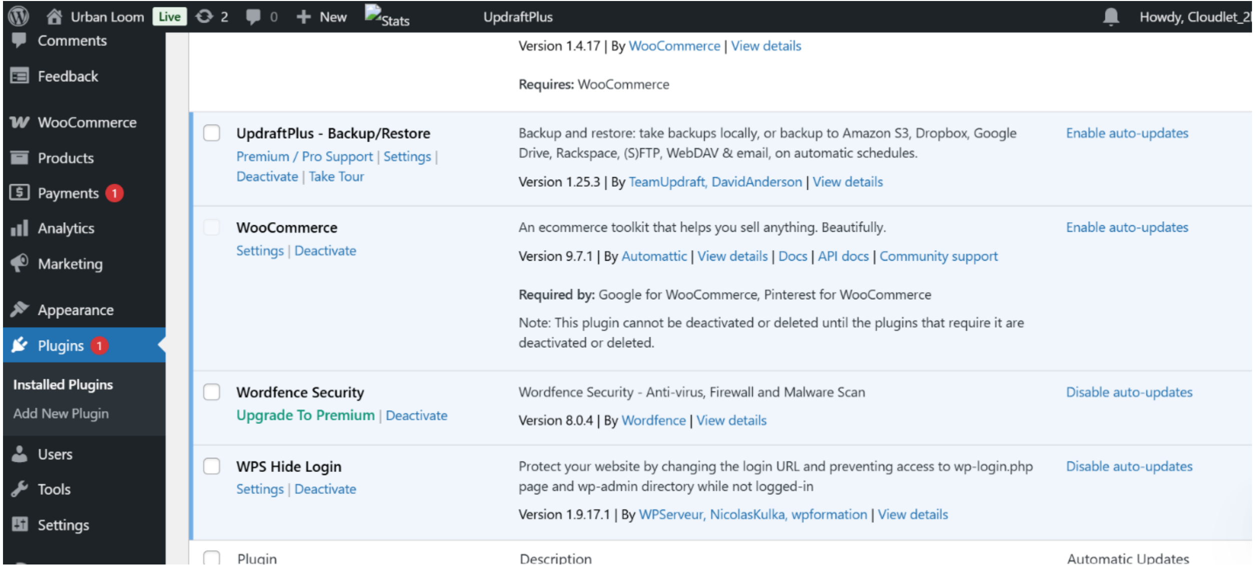
Password: ••••••••••••••••••

Plugins:



Version 1.7.2 | By Matt Mullenweg | View details

□ **Inactive Logout** Settings | Deactivate	Automatically logout idle user sessions, even if they are on the front end! Fully configurable & easy to use. Version 3.4.10 | By Inactive Logout | View details	Disable auto-updates
□ **Jetpack** My Jetpack | Settings | Deactivate	Security, performance, and marketing tools made by WordPress experts. Jetpack keeps your site protected so you can focus on more important things. Version 14.4.1 | By Automattic | View details | ★★★★★	Disable auto-updates Automatic update scheduled in 3 hours.

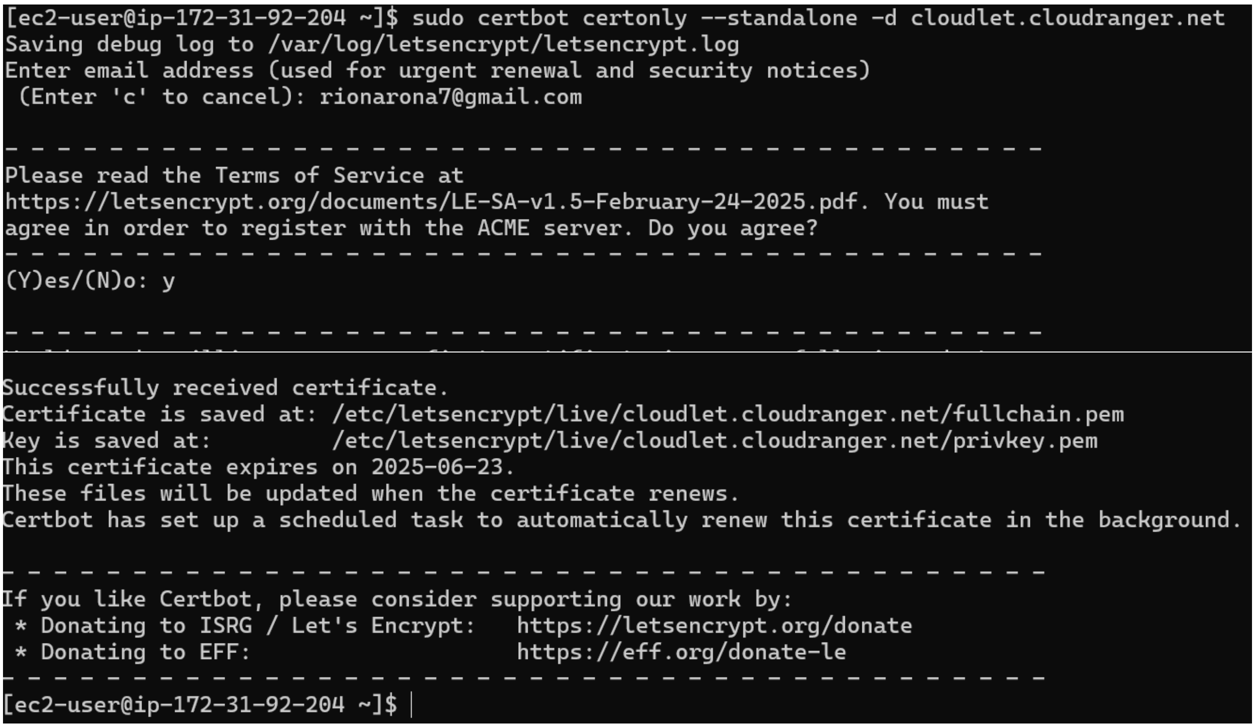


Version 1.4.17 | By WooCommerce | View details

Requires: WooCommerce

Plugin	Description	Automatic Updates
□ **UpdraftPlus - Backup/Restore** Premium / Pro Support | Settings | Deactivate | Take Tour	Backup and restore: take backups locally, or backup to Amazon S3, Dropbox, Google Drive, Rackspace, (S)FTP, WebDAV & email, on automatic schedules. Version 1.25.3 | By TeamUpdraft, DavidAnderson | View details	Enable auto-updates
□ **WooCommerce** Settings | Deactivate	An ecommerce toolkit that helps you sell anything. Beautifully. Version 9.7.1 | By Automattic | View details | Docs | API docs | Community support Required by: Google for WooCommerce, Pinterest for WooCommerce Note: This plugin cannot be deactivated or deleted until the plugins that require it are deactivated or deleted.	Enable auto-updates
□ **Wordfence Security** Upgrade To Premium | Deactivate	Wordfence Security - Anti-virus, Firewall and Malware Scan Version 8.0.4 | By Wordfence | View details	Disable auto-updates
□ **WPS Hide Login** Settings | Deactivate	Protect your website by changing the login URL and preventing access to wp-login.php page and wp-admin directory while not logged-in Version 1.9.17.1 | By WPServeur, NicolasKulka, wpformation | View details	Disable auto-updates

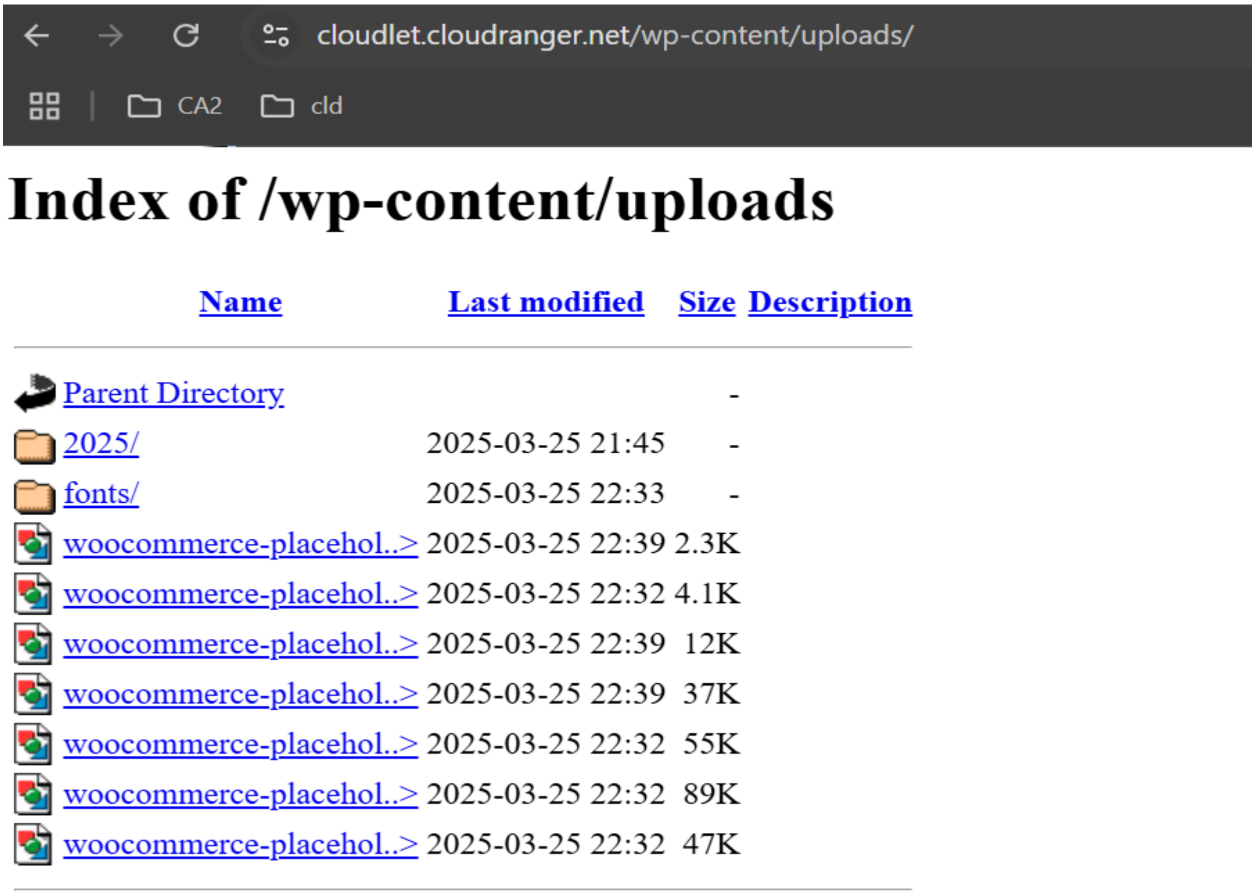
SSL:



```
[ec2-user@ip-172-31-92-204 ~]$ sudo certbot certonly --standalone -d cloudlet.cloudranger.net
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): rionarona7@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.5-February-24-2025.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

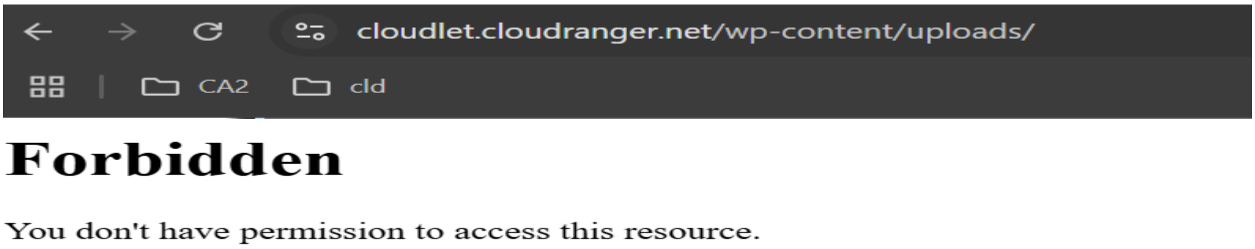
```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/cloudlet.cloudranger.net/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/cloudlet.cloudranger.net/privkey.pem
This certificate expires on 2025-06-23.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[ec2-user@ip-172-31-92-204 ~]$ 
```

Disabling access to directory:



Index of /wp-content/uploads

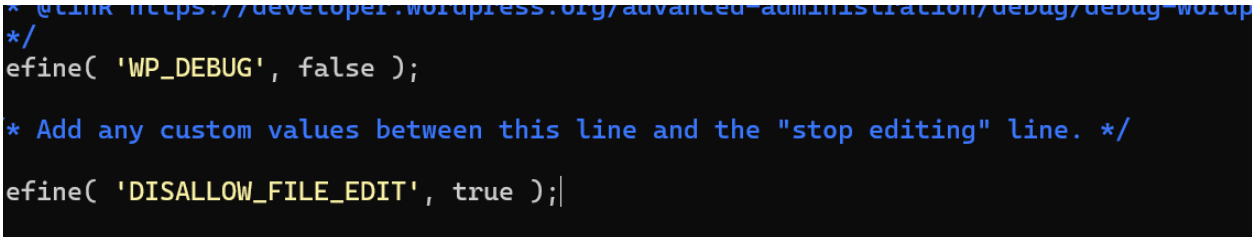
Name	Last modified	Size	Description
Parent Directory		-	
2025/	2025-03-25 21:45	-	
fonts/	2025-03-25 22:33	-	
woocommerce-placehol..>	2025-03-25 22:39	2.3K	
woocommerce-placehol..>	2025-03-25 22:32	4.1K	
woocommerce-placehol..>	2025-03-25 22:39	12K	
woocommerce-placehol..>	2025-03-25 22:39	37K	
woocommerce-placehol..>	2025-03-25 22:32	55K	
woocommerce-placehol..>	2025-03-25 22:32	89K	
woocommerce-placehol..>	2025-03-25 22:32	47K	



Forbidden

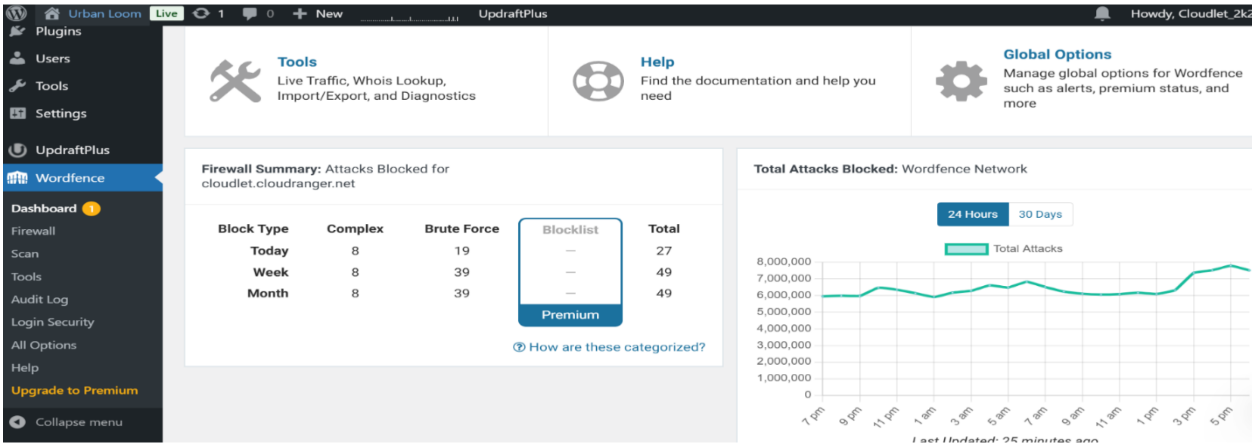
You don't have permission to access this resource.

Disabling file edit:



```
* @link https://developer.wordpress.org/advanced-administration/debug/debug-wordp
*/
efine( 'WP_DEBUG', false );

* Add any custom values between this line and the "stop editing" line. */

efine( 'DISALLOW_FILE_EDIT', true );
```

Wordfence:



Tools
Live Traffic, Whois Lookup, Import/Export, and Diagnostics

Help
Find the documentation and help you need

Global Options
Manage global options for Wordfence such as alerts, premium status, and more

Firewall Summary: Attacks Blocked for cloudlet.cloudranger.net

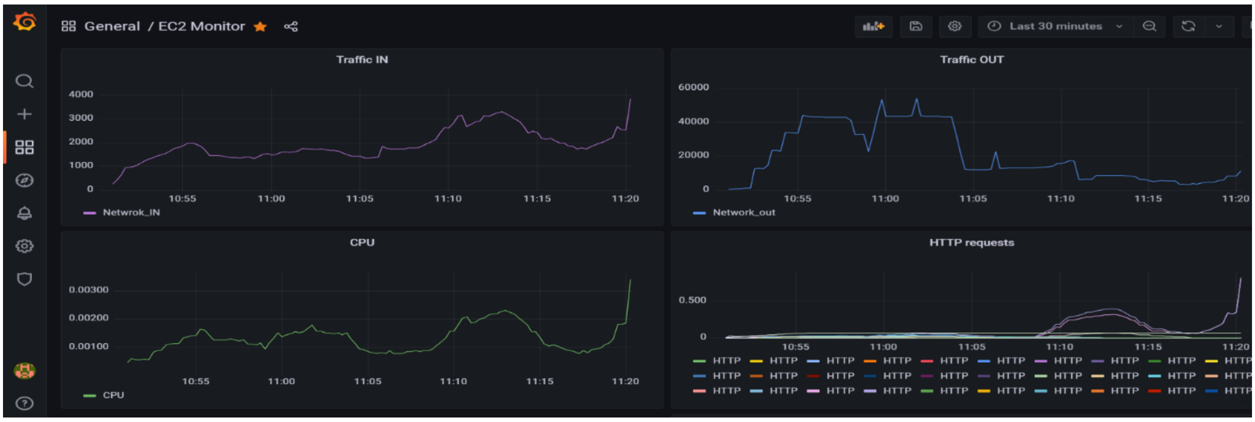
Block Type	Complex	Brute Force	Blocklist	Total
Today	8	19	–	27
Week	8	39	–	49
Month	8	39	–	49
			Premium	

How are these categorized?

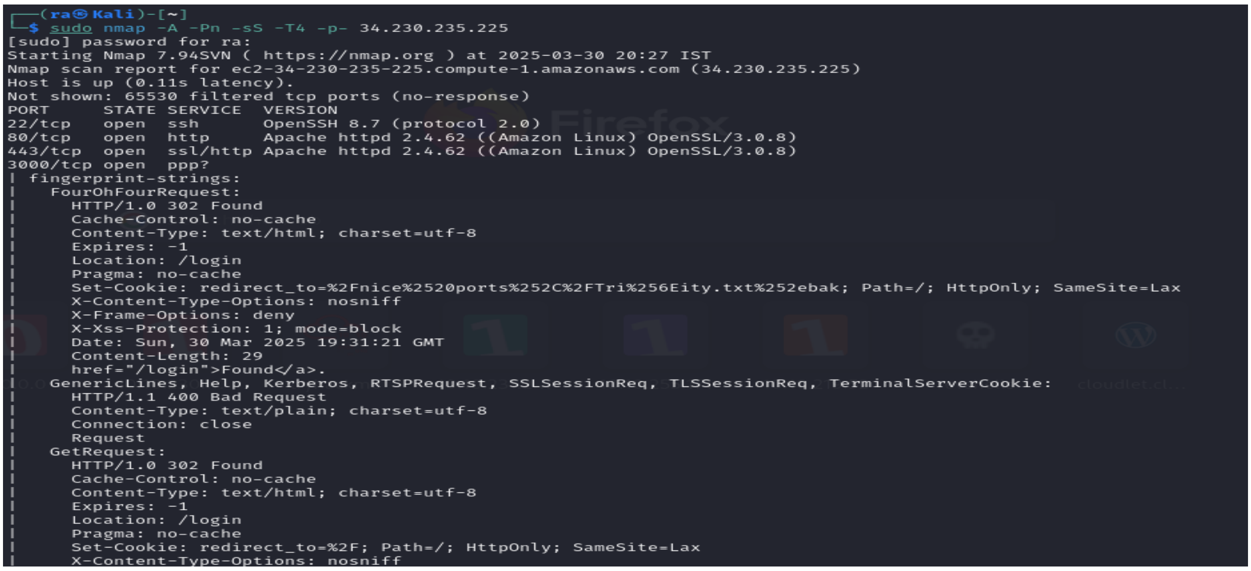
Total Attacks Blocked: Wordfence Network

Last Updated: 25 minutes ago

Garfana monitoring:

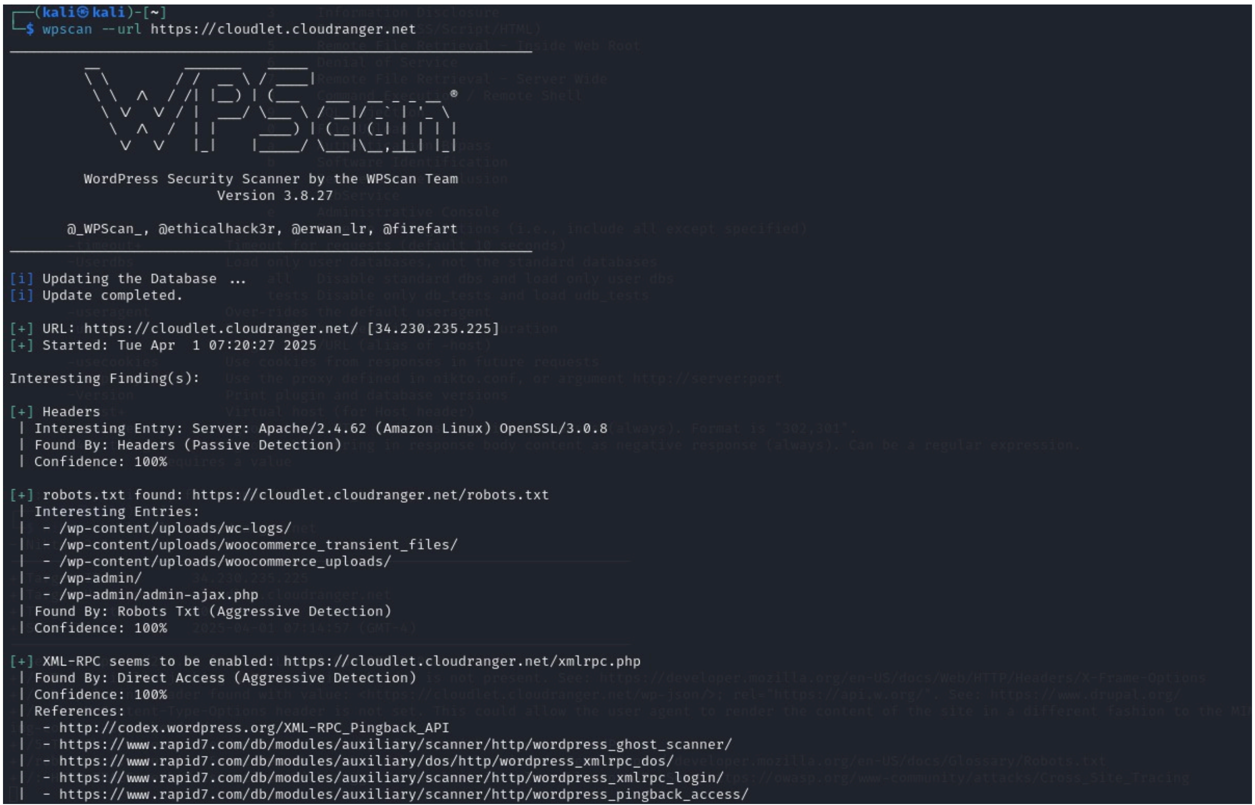


Nmap:

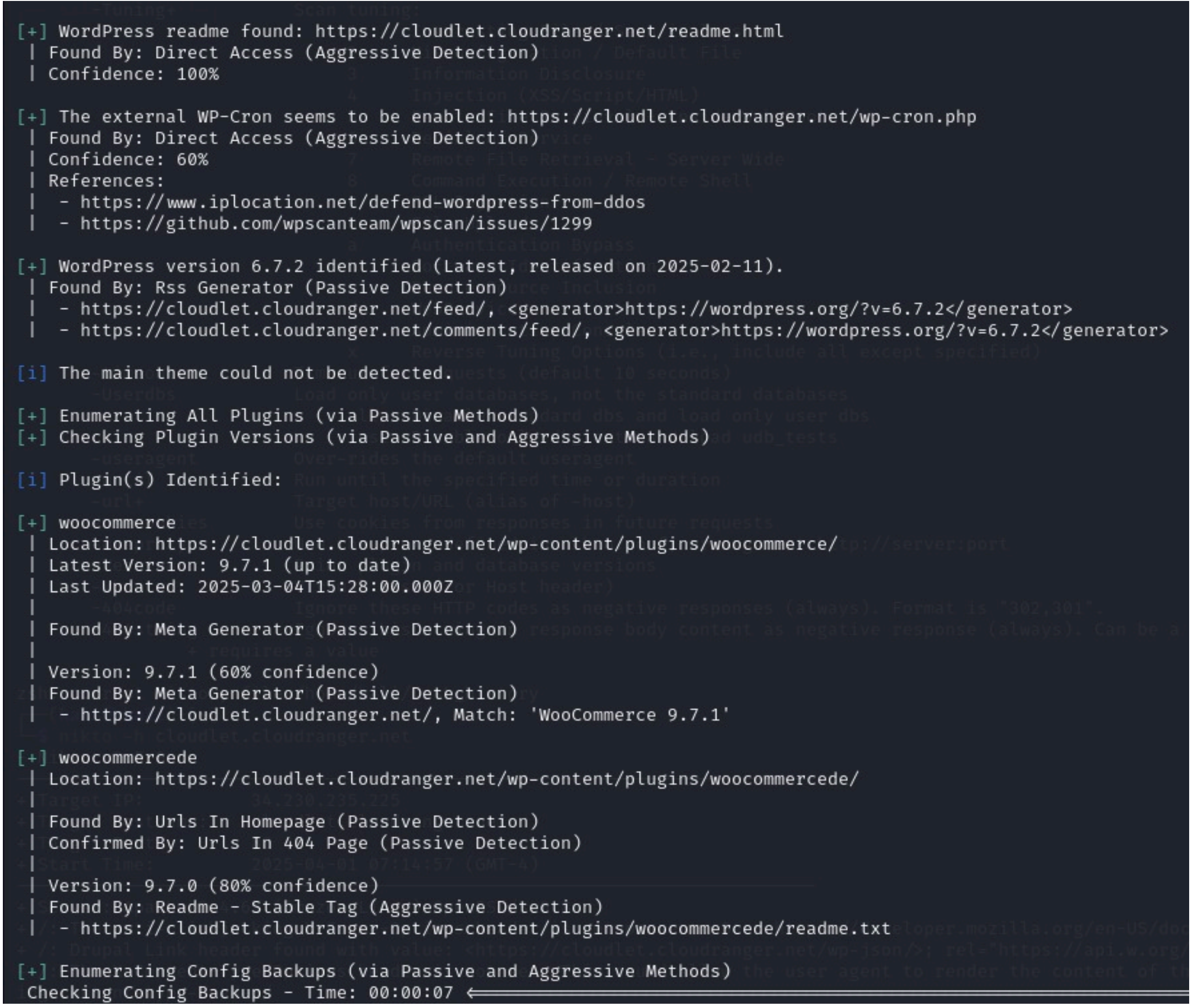


```
┌──(ra㉿Kali)-[~]
└─$ sudo nmap -A -Pn -sS -T4 -p- 34.230.235.225
[sudo] password for ra:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-30 20:27 IST
Nmap scan report for ec2-34-230-235-225.compute-1.amazonaws.com (34.230.235.225)
Host is up (0.11s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.7 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.62 ((Amazon Linux) OpenSSL/3.0.8)
443/tcp  open  ssl/http Apache httpd 2.4.62 ((Amazon Linux) OpenSSL/3.0.8)
3000/tcp open  ppp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie: redirect_to=%2Fnice%2520ports%252C%2FTri%256Eity.txt%252ebak; Path=/; HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: deny
|     X-Xss-Protection: 1; mode=block
|     Date: Sun, 30 Mar 2025 19:31:21 GMT
|     Content-Length: 29
|     href="/login">Found</a>.
|   GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
```

WPScan:

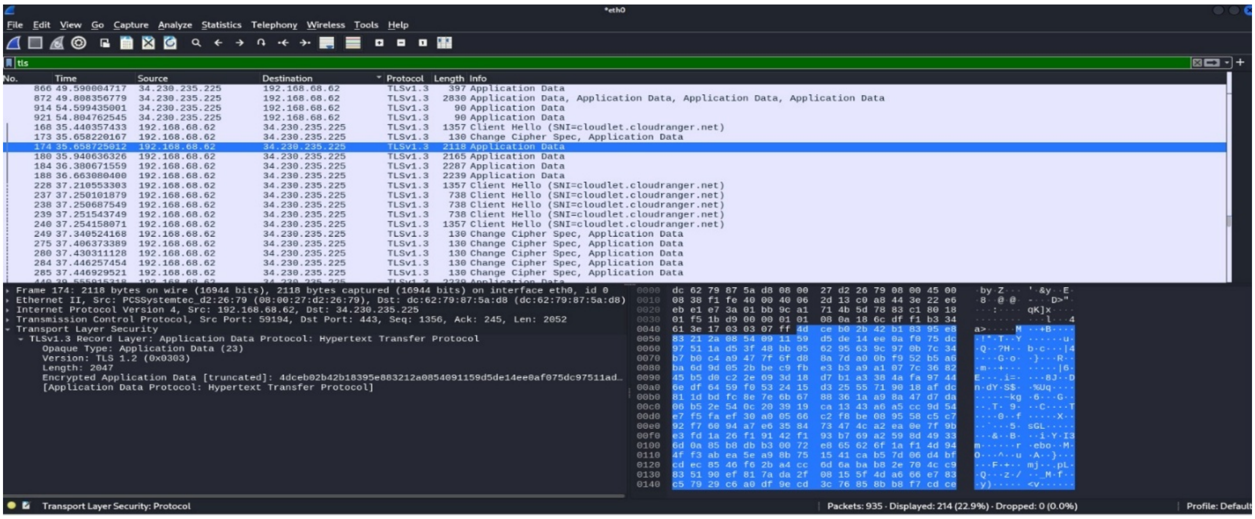


```
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://cloudlet.cloudranger.net
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: https://cloudlet.cloudranger.net/ [34.230.235.225]
[+] Started: Tue Apr  1 07:20:27 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.62 (Amazon Linux) OpenSSL/3.0.8
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://cloudlet.cloudranger.net/robots.txt
 | Interesting Entries:
 |  - /wp-content/uploads/wc-logs/
 |  - /wp-content/uploads/woocommerce_transient_files/
 |  - /wp-content/uploads/woocommerce_uploads/
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://cloudlet.cloudranger.net/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: https://cloudlet.cloudranger.net/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://cloudlet.cloudranger.net/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 6.7.2 identified (Latest, released on 2025-02-11).
 | Found By: Rss Generator (Passive Detection)
 |  - https://cloudlet.cloudranger.net/feed/, <generator>https://wordpress.org/?v=6.7.2</generator>
 |  - https://cloudlet.cloudranger.net/comments/feed/, <generator>https://wordpress.org/?v=6.7.2</generator>

[i] The main theme could not be detected.

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

[i] Plugin(s) Identified:

[+] woocommerce
 | Location: https://cloudlet.cloudranger.net/wp-content/plugins/woocommerce/
 | Latest Version: 9.7.1 (up to date)
 | Last Updated: 2025-03-04T15:28:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 9.7.1 (60% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - https://cloudlet.cloudranger.net/, Match: 'WooCommerce 9.7.1'

[+] woocommercede
 | Location: https://cloudlet.cloudranger.net/wp-content/plugins/woocommercede/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 9.7.0 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://cloudlet.cloudranger.net/wp-content/plugins/woocommercede/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:07 <=========================================
```

Wireshark:



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.   Time          Source           Destination      Protocol Length Info
  866 49.590004717  34.230.235.225   192.168.68.62    TLSv1.3   397 Application Data
  872 49.808356779  34.230.235.225   192.168.68.62    TLSv1.3  2830 Application Data, Application Data, Application Data, Application Data
  914 54.599435001  34.230.235.225   192.168.68.62    TLSv1.3    90 Application Data
  921 54.804762545  34.230.235.225   192.168.68.62    TLSv1.3    90 Application Data
  168 35.440357433  192.168.68.62    34.230.235.225   TLSv1.3  1357 Client Hello (SNI=cloudlet.cloudranger.net)
  173 35.658220167  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
  174 35.658725012  192.168.68.62    34.230.235.225   TLSv1.3  2118 Application Data
  180 35.940636326  192.168.68.62    34.230.235.225   TLSv1.3  2165 Application Data
  184 36.380671559  192.168.68.62    34.230.235.225   TLSv1.3  2287 Application Data
  188 36.663080400  192.168.68.62    34.230.235.225   TLSv1.3  2239 Application Data
  228 37.210553303  192.168.68.62    34.230.235.225   TLSv1.3  1357 Client Hello (SNI=cloudlet.cloudranger.net)
  237 37.250101879  192.168.68.62    34.230.235.225   TLSv1.3   738 Client Hello (SNI=cloudlet.cloudranger.net)
  238 37.250687549  192.168.68.62    34.230.235.225   TLSv1.3   738 Client Hello (SNI=cloudlet.cloudranger.net)
  239 37.251543749  192.168.68.62    34.230.235.225   TLSv1.3   738 Client Hello (SNI=cloudlet.cloudranger.net)
  240 37.254158071  192.168.68.62    34.230.235.225   TLSv1.3  1357 Client Hello (SNI=cloudlet.cloudranger.net)
  249 37.340524168  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
  275 37.406373389  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
  280 37.430311128  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
  284 37.446257454  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
  285 37.446929521  192.168.68.62    34.230.235.225   TLSv1.3   130 Change Cipher Spec, Application Data
```

```
▸ Frame 174: 2118 bytes on wire (16944 bits), 2118 bytes captured (16944 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d2:26:79 (08:00:27:d2:26:79), Dst: dc:62:79:87:5a:d8 (dc:62:79:87:5a:d8)
▸ Internet Protocol Version 4, Src: 192.168.68.62, Dst: 34.230.235.225
▸ Transmission Control Protocol, Src Port: 59194, Dst Port: 443, Seq: 1356, Ack: 245, Len: 2052
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 2047
      Encrypted Application Data [truncated]: 4dceb02b42b18395e883212a0854091159d5de14ee0af075dc97511ad…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

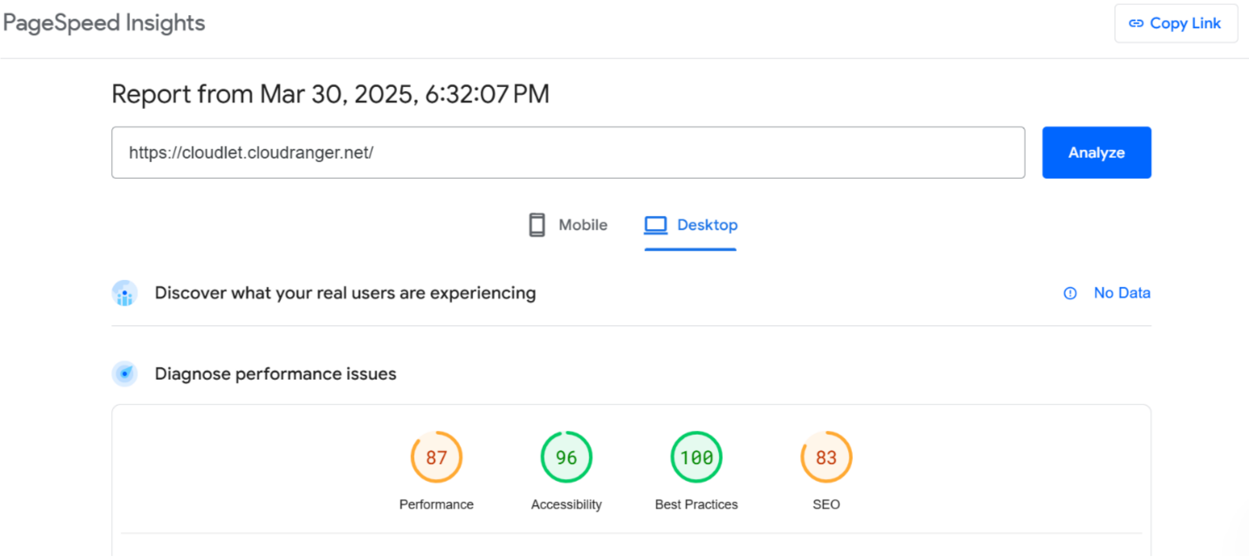
```
0000  dc 62 79 87 5a d8 08 00  27 d2 26 79 08 00 45 00   ·by·Z···  '·&y··E·
0010  08 38 f1 fe 40 00 40 06  2d 13 c0 a8 44 3e 22 e6   ·8··@·@·  -···D>"·
0020  eb e1 e7 3a 01 bb 9c a1  71 4b 5d 78 83 c1 80 18   ···:····  qK]x····
0030  01 f5 1b d9 00 00 01 01  08 0a 18 6c df f1 b3 34   ········  ···l···4
0040  61 3e 17 03 03 07 ff 4d  ce b0 2b 42 b1 83 95 e8   a>·····M  ··+B····
0050  83 21 2a 08 54 09 11 59  d5 de 14 ee 0a f0 75 dc   ·!*·T··Y  ······u·
0060  97 51 1a d5 3f 48 bb 05  62 95 63 9c 97 0b 7c 34   ·Q··?H··  b·c···|4
0070  b7 b0 c4 a9 47 7f 6f d8  8a 7d a0 0b f9 52 b5 a6   ····G·o·  ·}···R··
0080  ba 6d 9d 05 2b be c9 fb  e3 b3 a9 a1 07 7c 36 82   ·m··+···  ·····|6·
0090  45 b5 d0 c2 2e 69 3d 18  d7 b1 a3 38 4a fa 97 44   E···.i=·  ···8J··D
00a0  6e df 64 59 f0 53 24 15  d3 25 55 71 90 18 af dc   n·dY·S$·  ·%Uq····
00b0  81 1d bd fc 8e 7e 6b 67  88 36 1a a9 8a 47 d7 da   ·····~kg  ·6···G··
00c0  06 b5 2e 54 0c 20 39 19  ca 13 43 a6 a5 cc 9d 54   ··.T· 9·  ··C····T
00d0  e7 f5 fa ef 30 a0 05 66  c2 f8 be 08 95 58 c5 c7   ····0··f  ·····X··
00e0  92 f7 60 94 a7 e6 35 84  73 47 4c a2 ea 0e 7f 9b   ··`···5·  sGL·····
00f0  e3 fd 1a 26 f1 91 42 f1  93 b7 69 a2 59 8d 49 33   ···&··B·  ··i·Y·I3
0100  6d 0a 85 b8 db b3 00 72  e8 65 62 6f 1a f1 4d 94   m······r  ·ebo··M·
0110  4f f3 ab ea 5e a9 8b 75  15 41 ca b5 7d 06 d4 bf   O···^··u  ·A··}···
0120  cd ec 85 46 f6 2b a4 cc  6d 6a ba b8 2e 70 4c c9   ···F·+··  mj··.pL·
0130  83 51 90 ef 81 7a da 2f  08 15 5f 4d a6 66 e7 83   ·Q···z·/  ··_M·f··
0140  c5 79 29 c6 a0 df 9e cd  3c 76 85 8b b8 f7 cd ce   ·y)·····  <v······
```

Transport Layer Security: Protocol

Packets: 935 · Displayed: 214 (22.9%) · Dropped: 0 (0.0%)

Profile: Default

Google Speed Insights:



Report from Mar 30, 2025, 6:32:07 PM

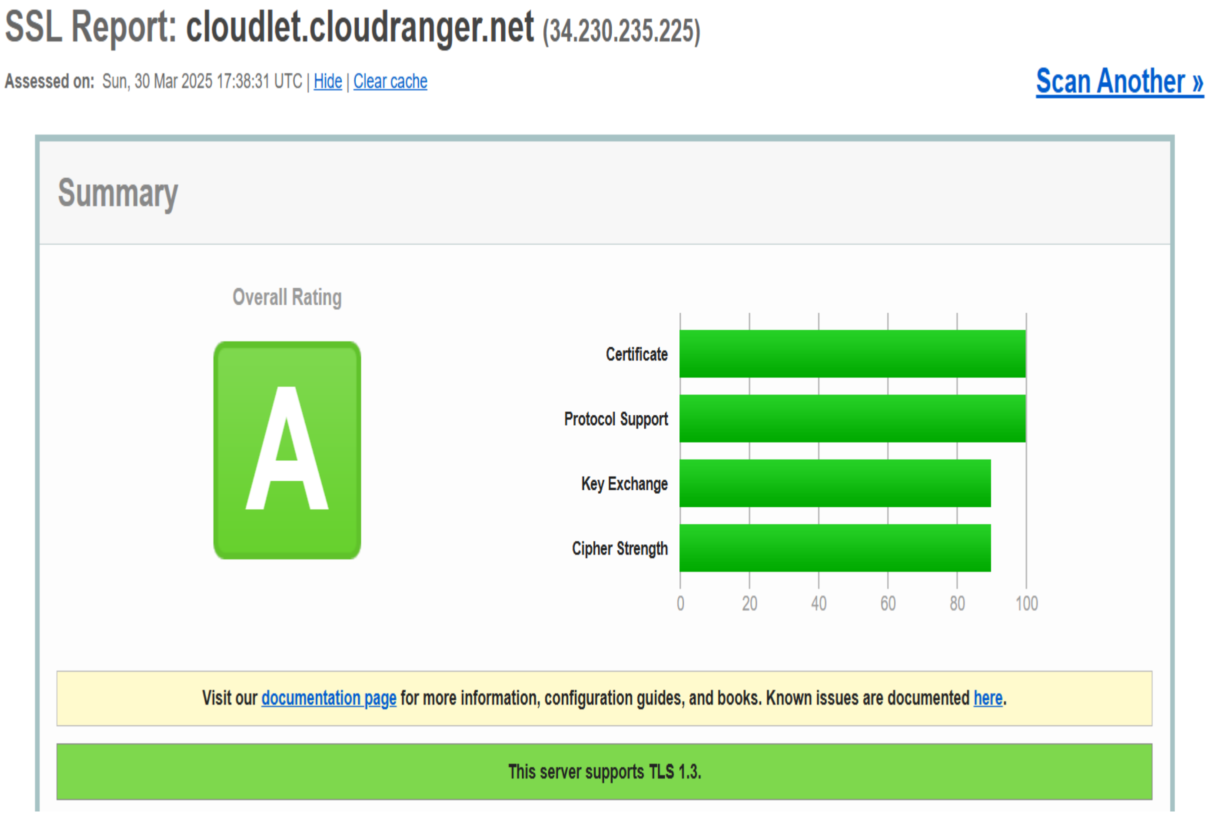
https://cloudlet.cloudranger.net/

Discover what your real users are experiencing — No Data

Diagnose performance issues

Performance	Accessibility	Best Practices	SEO
87	96	100	83

SSL Lab:



SSL Report: cloudlet.cloudranger.net (34.230.235.225)

Assessed on: Sun, 30 Mar 2025 17:38:31 UTC | Hide | Clear cache

Scan Another »

Summary

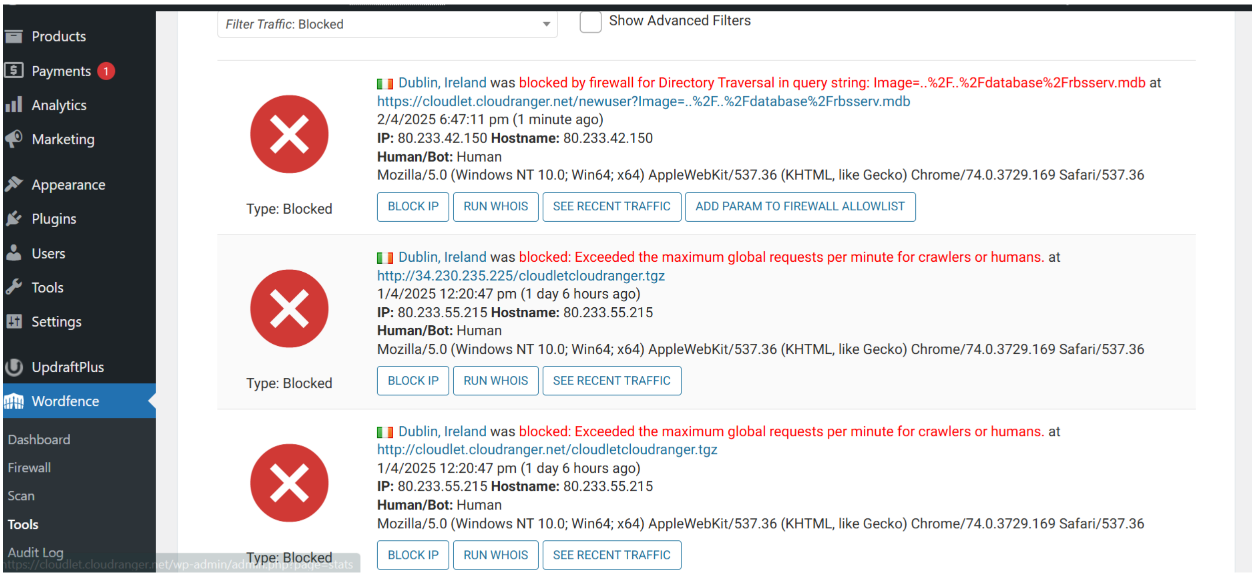
Overall Rating

A

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

Result of running a nikto scan, blocked IP as a result of sending too many requests:



Filter Traffic: Blocked

□ Show Advanced Filters

Dublin, Ireland was blocked by firewall for Directory Traversal in query string: Image=..%2F..%2Fdatabase%2Frbsserv.mdb at https://cloudlet.cloudranger.net/newuser?Image=..%2F..%2Fdatabase%2Frbsserv.mdb
2/4/2025 6:47:11 pm (1 minute ago)
IP: 80.233.42.150 **Hostname:** 80.233.42.150
Human/Bot: Human
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

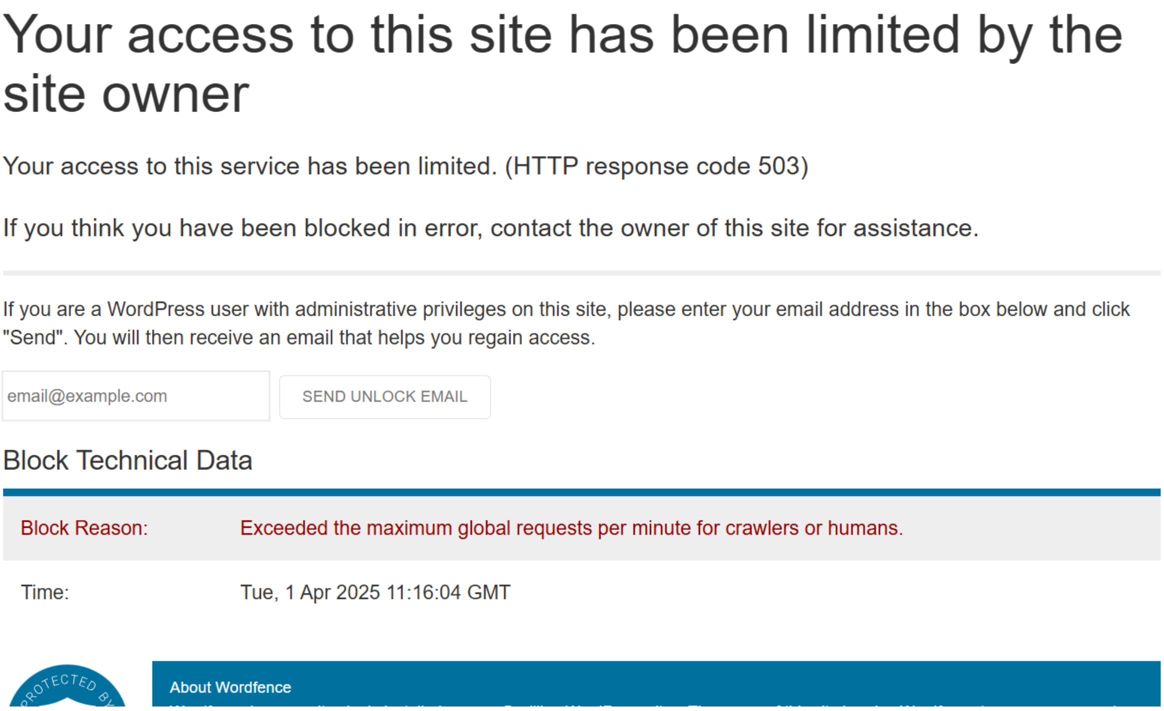
Type: Blocked

Dublin, Ireland was blocked: Exceeded the maximum global requests per minute for crawlers or humans. at http://34.230.235.225/cloudletcloudranger.tgz
1/4/2025 12:20:47 pm (1 day 6 hours ago)
IP: 80.233.55.215 **Hostname:** 80.233.55.215
Human/Bot: Human
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

Type: Blocked

Dublin, Ireland was blocked: Exceeded the maximum global requests per minute for crawlers or humans. at http://cloudlet.cloudranger.net/cloudletcloudranger.tgz
1/4/2025 12:20:47 pm (1 day 6 hours ago)
IP: 80.233.55.215 **Hostname:** 80.233.55.215
Human/Bot: Human
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

Type: Blocked



Your access to this site has been limited by the site owner

Your access to this service has been limited. (HTTP response code 503)

If you think you have been blocked in error, contact the owner of this site for assistance.

If you are a WordPress user with administrative privileges on this site, please enter your email address in the box below and click "Send". You will then receive an email that helps you regain access.

Block Technical Data

Block Reason:	Exceeded the maximum global requests per minute for crawlers or humans.
Time:	Tue, 1 Apr 2025 11:16:04 GMT

About Wordfence