WPGateway Secure

A comprehensive, easy to use, stable and well supported WordPress plugin. WordPress itself is a secure platform.

However, this plugin adds some extra security **AND** firewall to your WordPress website. It makes your website more secure against hackers.

WPGateway Secure scans your website for the key points to hide your WordPress website from spammers.

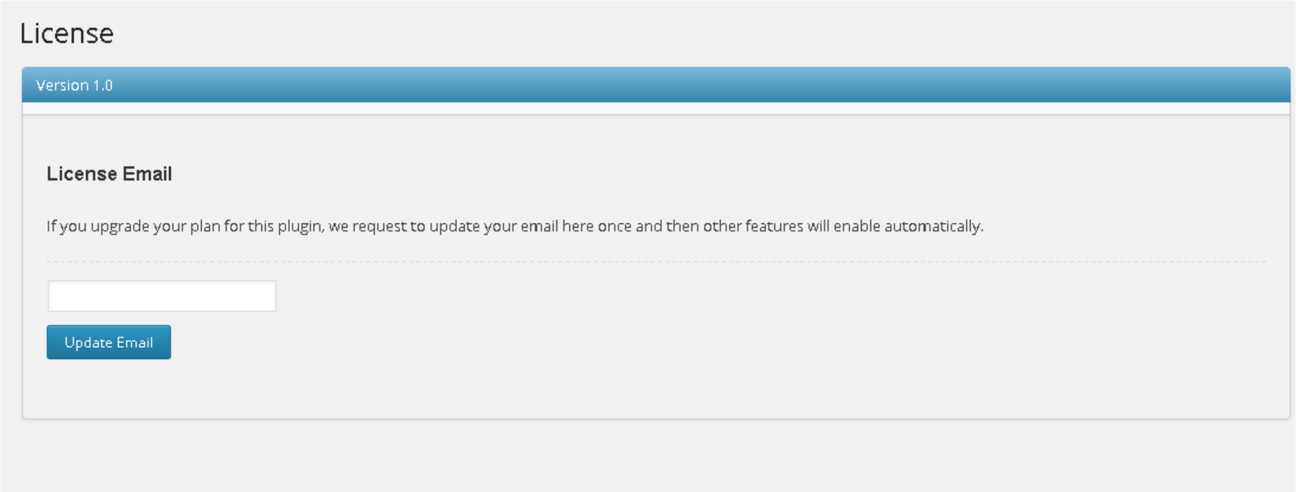
WPGateway Secure protects your website by blocking the hack attempts and by blocking IP addresses. Moreover, it reduces the security risk with its "EXTREME plan" features.

LICENSE KEY

If your website is hosted on WPGateway.com, **WPGateway Secure** - **Extreme plan** - which includes all possible features - is included in your hosting plan.

Otherwise, users have to buy a license and can add License key to activate plugin features.

WPGateway Secure enables the features - from basic, advanced or extreme - by getting details from your license key.


License

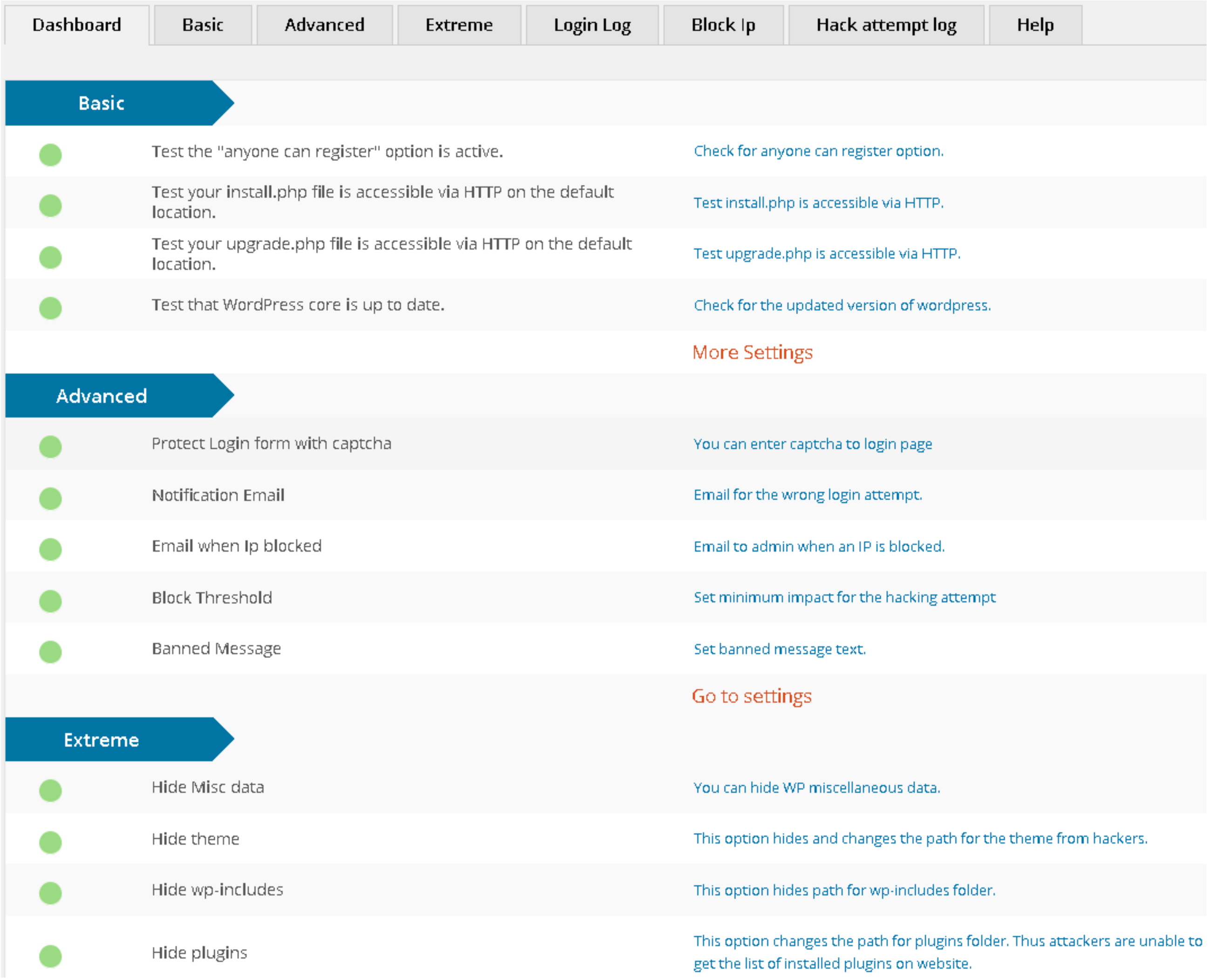
Version 1.0

License Email

If you upgrade your plan for this plugin, we request to update your email here once and then other features will enable automatically.

DASHBOARD

WPGateway Secure displays enabled features according to your license key. For instance, if you have the **EXTREME** plan, extreme points are displayed as green. You may enable or disable features as you wish.



Basic

●	Test the "anyone can register" option is active.	Check for anyone can register option.
●	Test your install.php file is accessible via HTTP on the default location.	Test install.php is accessible via HTTP.
●	Test your upgrade.php file is accessible via HTTP on the default location.	Test upgrade.php is accessible via HTTP.
●	Test that WordPress core is up to date.	Check for the updated version of wordpress.

More Settings

Advanced

●	Protect Login form with captcha	You can enter captcha to login page
●	Notification Email	Email for the wrong login attempt.
●	Email when Ip blocked	Email to admin when an IP is blocked.
●	Block Threshold	Set minimum impact for the hacking attempt
●	Banned Message	Set banned message text.

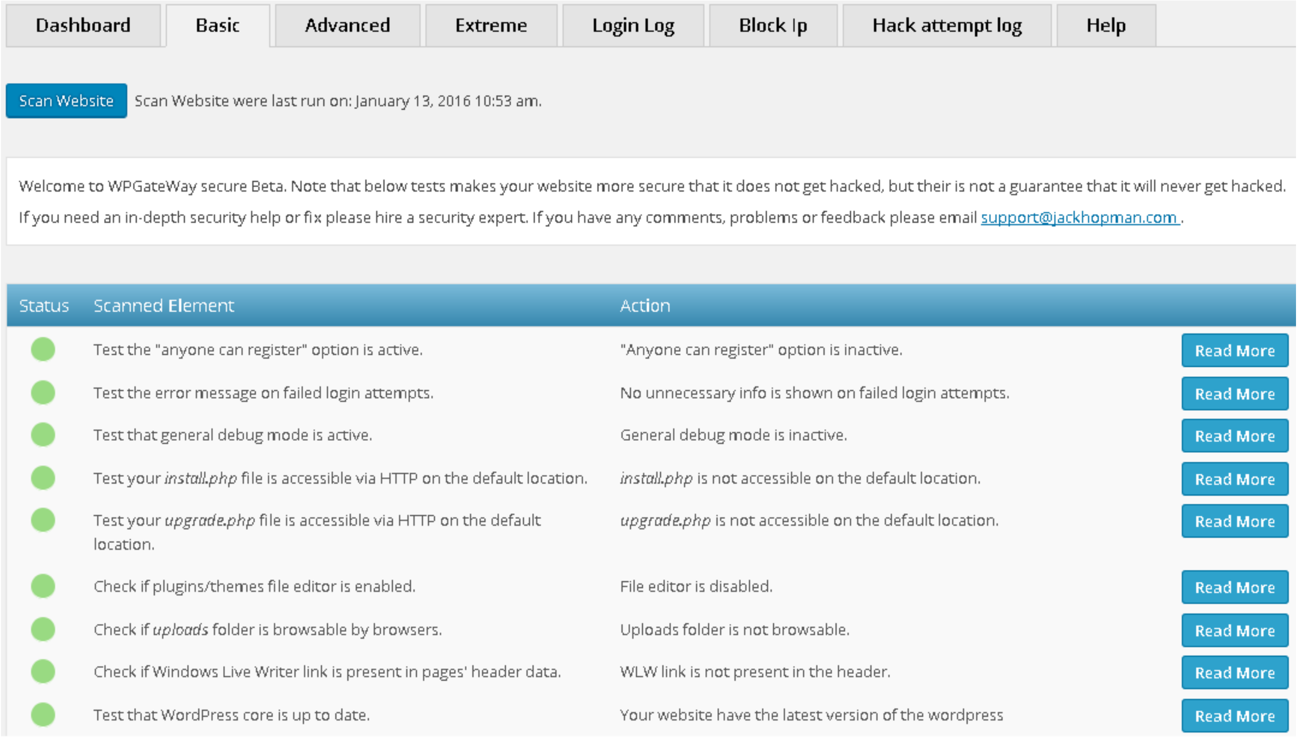
Go to settings

Extreme

●	Hide Misc data	You can hide WP miscellaneous data.
●	Hide theme	This option hides and changes the path for the theme from hackers.
●	Hide wp-includes	This option hides path for wp-includes folder.
●	Hide plugins	This option changes the path for plugins folder. Thus attackers are unable to get the list of installed plugins on website.

BASIC

A “Scan Website” button is above the BASIC tab. **WPGateway Secure** checks for the below listed key points of your website and shows the result as positive or negative in the scan results list. If you manually fix any of the following listed points, then you can scan your website again for the positive result.



Scan Website were last run on: January 13, 2016 10:53 am.

Welcome to WPGateWay secure Beta. Note that below tests makes your website more secure that it does not get hacked, but their is not a guarantee that it will never get hacked. If you need an in-depth security help or fix please hire a security expert. If you have any comments, problems or feedback please email support@jackhopman.com .

Status	Scanned Element	Action	
●	Test the "anyone can register" option is active.	"Anyone can register" option is inactive.	Read More
●	Test the error message on failed login attempts.	No unnecessary info is shown on failed login attempts.	Read More
●	Test that general debug mode is active.	General debug mode is inactive.	Read More
●	Test your *install.php* file is accessible via HTTP on the default location.	*install.php* is not accessible on the default location.	Read More
●	Test your *upgrade.php* file is accessible via HTTP on the default location.	*upgrade.php* is not accessible on the default location.	Read More
●	Check if plugins/themes file editor is enabled.	File editor is disabled.	Read More
●	Check if *uploads* folder is browsable by browsers.	Uploads folder is not browsable.	Read More
●	Check if Windows Live Writer link is present in pages' header data.	WLW link is not present in the header.	Read More
●	Test that WordPress core is up to date.	Your website have the latest version of the wordpress	Read More

1. Test the "anyone can register" option is active.

-- Under Setting tab , Click on general sub menu and then uncheck the checkbox of ANYONE CAN REGISTER

2. Test that WordPress core is up to date.

-- **WPGateway Secure** highly recommends that your WordPress sites be regularly updated. New security features prevent hackers from breaking into your website and inserting malicious code. Just go to Dashboard – Updates - or Appearance - Themes.

3. Test the plugins are up to date.

-- You need to keep your plugins updated always to protect from vulnerabilities. Always make a backup of the website before updating the plugin as it may affect your database.

4. Test that themes are up to date.

-- Its important to have your themes updated, to get new features and protect from the known vulnerabilities which may be corrected in a new version of the theme.

5. Test the server response headers contain detailed PHP version info.

-- Never disclosed php version info from the header as it will be easy for hacker to hack your website. You need to contact your hosting company to configure the HTTP server not to show PHP version info.

6.Test that "expose_php" PHP directive is turned off.

-- It is not good to disclose the exact PHP version - which helps hackers to access your website. You can write in php.ini file   expose_php = off

7. Test the user with username "admin" exists.

-- For brute-force attack they will most probably start with username "admin". So, add a new user with the role of administrator and delete the "admin" one and assign all post/pages he may have created to the new user

8. Test the error message on failed login attempts.

-- Whenever logins fail, WordPress tells you whether username or password is wrong - which helps the brute-force methods to hack the password as they can easily find the active username. We can prevent this by adding below code in functions.php of your current theme :

```
function wrong_login() {
        return \'Wrong username or password \'.
        }
    add_filter(\'login_errors\', \'wrong_login\')
```

9. Test for the prefix of the WordPress table "wp_")

-- It is not recommended to have a default prefix wp_ of the tables. On new installation, make sure that the prefix is unique. If you want to change the table prefix in a currently active website, it's a bit more complicated. You should only make the changes if you are comfortable doing these changes to your DB data via PhpMyAdmin. Always make a back up before changing the database settings.

10. Test the salts and keys have proper values.

-- WordPress Security Keys is a set of random variables that improve encryption of information stored in the user’s cookies. There are a total of four security keys: AUTH_KEY, SECURE_AUTH_KEY, LOGGED_IN_KEY, and NONCE_KEY. You can update these variable in wp-config from the link: https://api.WordPress.org/secret-key/1.1/

11. Test the strength of WordPress database password.

-- Database passwords need to be strong . You can change the db password by visiting to cpanel/plesk and find the option of changing password of the database. Once you changed the password , you need to update the wp-config.php file:-

```
define(\'DB_PASSWORD\', \'YOUR_NEW_DB_PASSWORD_GOES_HERE\');
```

12. Test that general debug mode is active.

-- Error reporting mode enabled on a production server will slow down the website and shows a weird message to user. Open wp-config.php file and update the code with define(\'WP_DEBUG\', true);

13. Test that database debug mode is enabled.

-- Error reporting mode enabled on a production server will slow down the website and shows a weird message to user. It helps the attacker to fetch the information about your system.

14. Test JavaScript debug mode is enabled.

-- Error reporting mode enabled on a production server will slow down the website and shows a weird message to user. It helps the attacker to fetch the information about your system.

15. Check if "display_errors" PHP directive is turned off.

-- It is not wise to display php error. You can open wp-config.php file and place a code of

```
ini_set(\'display_errors\', 0)
```

16. Test your "wp-config.php" file has the right permissions (chmod) set.

-- wp-config.php file contains sensitive information (database user name and password) in plain text and should not be accessible to anyone except you and WP. Try setting chmod to 0400 or 0440 and, if the site works properly, that's the best one to use

17. Test your "install.php" file is accessible via HTTP on the default location.

-- Once you install WP, this file becomes useless and there's no reason to keep it in the default location and accessible via HTTP. Move it to another location or chmod it so it's not accessible via HTTP.

18. Test your "upgrade.php" file is accessible via HTTP on the default location.

-- There have already been a couple of security issues regarding this file. Rename upgrade.php (you'll find it in the wp-admin folder) to something more unique like "upgrade-876.php"; move it to another location or chmod it so it's not accessible via HTTP

19. Test your "register_globals" PHP directive is turned off.

-- This is one of the biggest security issues you can have on your site. Update php.ini file to register_globals = off to solve it. '

20. Test the PHP safe mode is disabled.

-- This is another big security issue you can have on your site. Update php.ini file to safe_mode = off to solve it

21. Check if plugins/themes file editor is enabled.

-- Access to plugin and theme code is readily available in the WordPress dashboard. One thing you can do to protect the site from being destroyed is to disable both of these editors. You can do this in less than a minute. Open your wp-config.php file and add the following constant: define(\'DISALLOW_FILE_EDIT\',true)

22. Check if "uploads" folder is browsable by browsers.

-- Allowing anyone to view all files in the uploads folder, just by pointing the browser to it, will allow them to easily download all your uploaded files. It's a security and a copyright issue.

To fix the problem open .htaccess and add this directive into it: Options -Indexes

23. Check if Windows Live Writer link is present in pages' header data.

-- Disclosing the full WP version info in the default location (page header meta) is not wise. Place the following code in your theme's functions.php file in order to remove the header meta version info:

```
function remove_version() {
        return \'\';
}
```

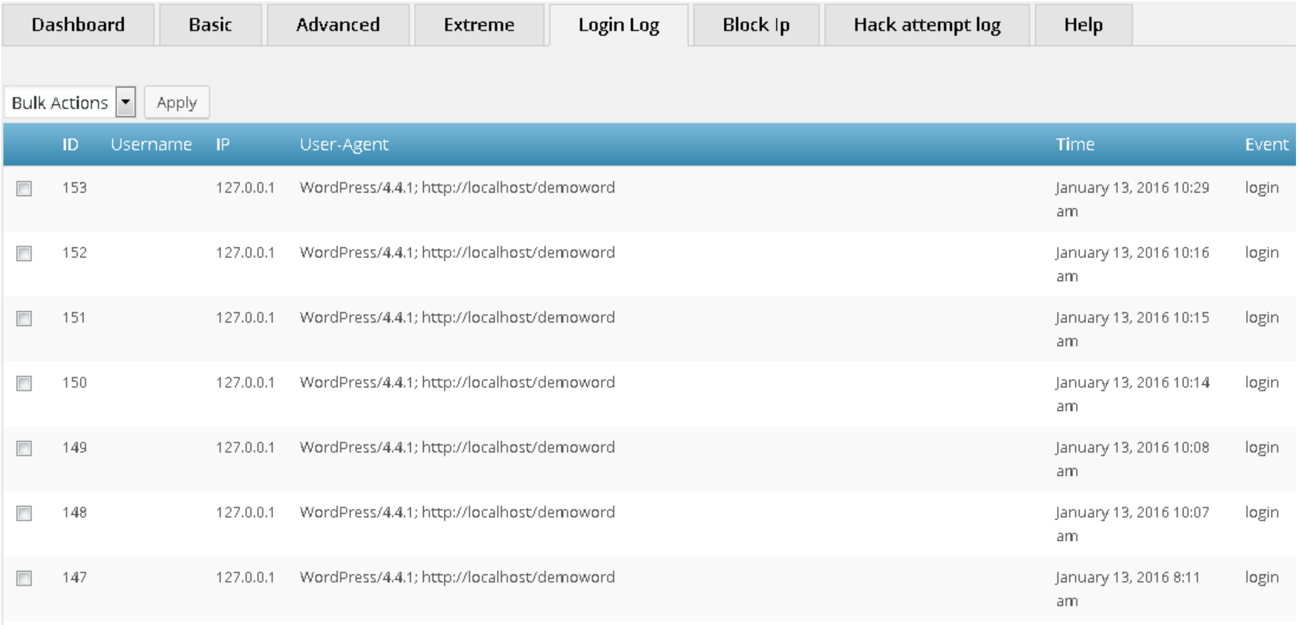
24. Test if MySQL server is connectable from outside with the WP user.

-- Allowing him to connect from any host will make attack easier for hackers. Fixing this issue involves changing the MySQL user or server config

25. Test your "wp-config.php" can be accessed via HTTP.

-- wp-config file should not be accessible via HTTP. You need to update your .htaccess file with the following code: <files wp-config.php>
order allow,deny
deny from all
</files>

LOGIN LOG:-



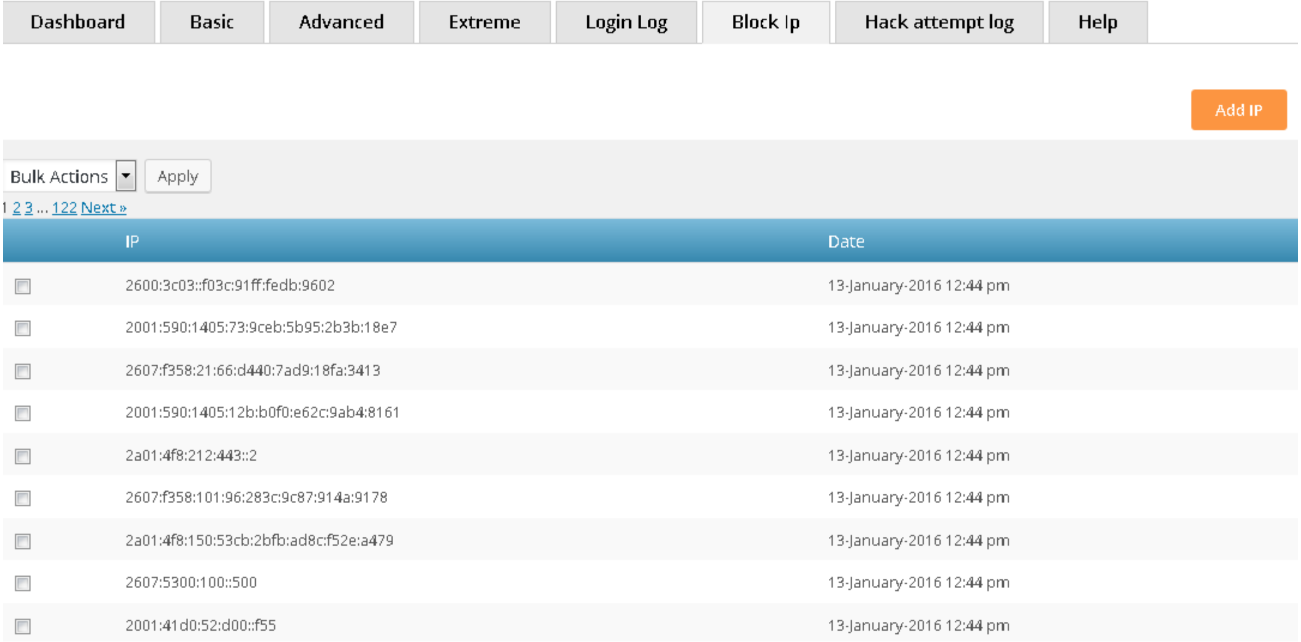
	ID	Username	IP	User-Agent	Time	Event
☐	153		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:29 am	login
☐	152		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:16 am	login
☐	151		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:15 am	login
☐	150		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:14 am	login
☐	149		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:08 am	login
☐	148		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 10:07 am	login
☐	147		127.0.0.1	WordPress/4.4.1; http://localhost/demoword	January 13, 2016 8:11 am	login

This section lists those users who have been logged in, in admin section.

BLOCK IP:-

Admin can add IP addresses that need to be blocked.
In addition to this, **WPGateway Secure** adds the latest IP addresses that are already Blacklisted, Spam Bots or IP with dangerous software.

This list also includes the IP addresses which are continuously trying to hack your website and they have been automatically banned by **WPGateway Secure** Plugin.



	IP	Date
□	2600:3c03::f03c:91ff:fedb:9602	13-January-2016 12:44 pm
□	2001:590:1405:73:9ceb:5b95:2b3b:18e7	13-January-2016 12:44 pm
□	2607:f358:21:66:d440:7ad9:18fa:3413	13-January-2016 12:44 pm
□	2001:590:1405:12b:b0f0:e62c:9ab4:8161	13-January-2016 12:44 pm
□	2a01:4f8:212:443::2	13-January-2016 12:44 pm
□	2607:f358:101:96:283c:9c87:914a:9178	13-January-2016 12:44 pm
□	2a01:4f8:150:53cb:2bfb:ad8c:f52e:a479	13-January-2016 12:44 pm
□	2607:5300:100::500	13-January-2016 12:44 pm
□	2001:41d0:52:d00::f55	13-January-2016 12:44 pm