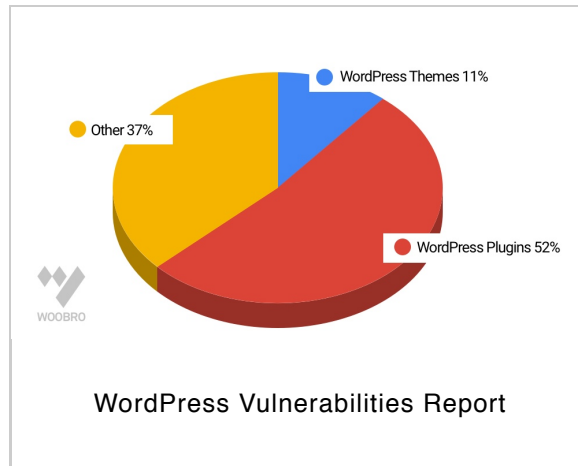


## WordPress SQL Injection: How to Prevent attacks in 2019?

**M**ost of the vulnerabilities including SQL Injection in WordPress were discovered in the plugins and themes.

WordPress plugins cause 52%, and WordPress themes produce 11% of WordPress vulnerabilities – reported by WpScan.



“If you’re able to avoid writing XSS and SQL injection vulnerabilities, you will have removed the risk of writing 65% of all vulnerabilities you might ever accidentally create.”  
– reported by  
**Wordfence**

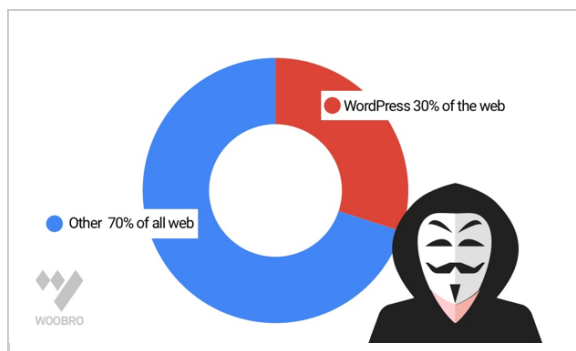
WordPress SQL Injection vulnerabilities are the second most common vulnerabilities found in WordPress. 39% of WordPress vulnerabilities are cross-site scripting (XSS)

issues.



“Previously, SQL Injection was the most basic and widely used hacking technique to manipulate the WordPress database. Nowadays, Cross Site Scripting (XSS) is popular and become the number one method to hack a WordPress site.”  
– reported by Cloudways

MySQL is at the top of the list because it powers more than 70% of the World Wide Web (www). WordPress that uses SQL alone has contributed to more than 29% of www and has become the most attractive target for attackers.

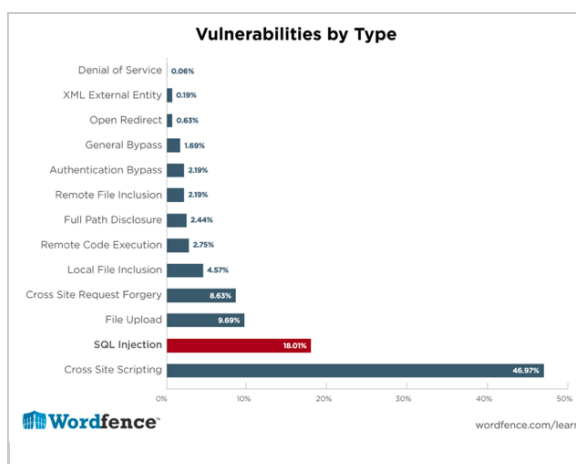


Ready to start a project?

[get in touch](#)

Considering that the number of total active websites is estimated at over 172 million according to a survey published by Netcraft, that means that around 75,000,000 websites are using WordPress right now.

As Wordfence says it is worth spending the time to learn more about WordPress SQL injection vulnerabilities and how to avoid them.



## SQL injection vulnerabilities

# E-commerce suffers 2x as many SQL injection attacks as other industries

The Imperva(Cyber Security Company) did the security summary report in 2013 and observing 70 websites in six months time period. Compared to 2012, the number of SQL injection attacks doubled.

## Key findings based on Imperva security summary report from examined 70 websites:

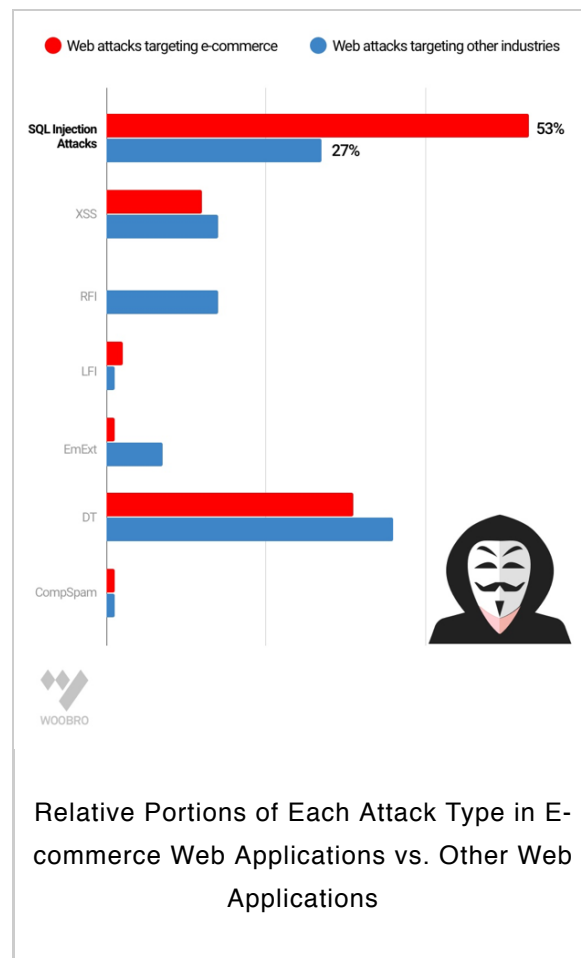
- While most web applications receive 4 or more web attack

campaigns per month,  
some sites are always  
under attack.

- Each website receives a **94,057** SQL injection attack requests in one day.
- E-commerce suffers 2x as many SQL injection attacks as other industries.
- One observed website was under attack **176** out of **180** days, or **98%** of the time.
- **94,057** equates to **1,567** SQL injection attacks per hour or 26 attack requests per minute, on average.

The chart below shows the types of web attacks targeting e-commerce websites compared to attacks targeting other industries. Compared to other industries, e-commerce

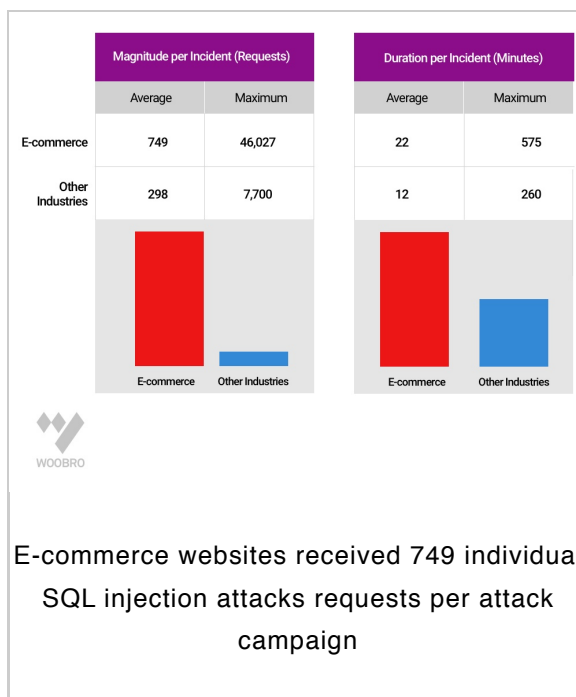
websites suffered twice as many SQL injection attacks.



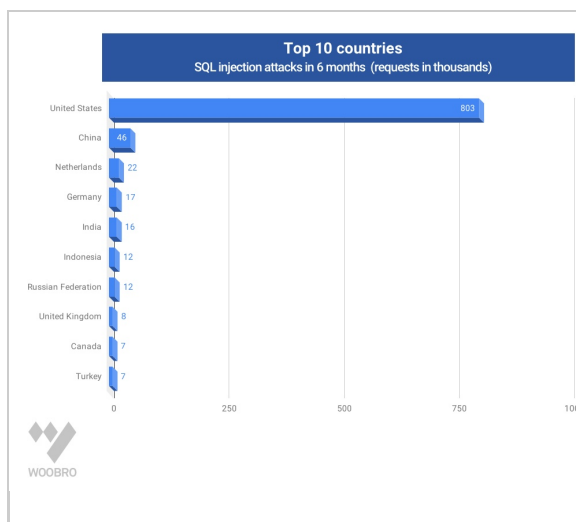
Imperva analysis, shown in Table below, revealed that SQL injection attacks on retail applications were more intense, both in terms of some attacks per incident and duration of an event. E-commerce websites received 749 individual attack requests per attack campaign.

Analysis of Magnitude and Duration of SQL Injection

## Attack Incidents:



Imperva analyzed the geographic distribution of the attack initiating hosts, as determined by their IP addresses. The chart below summarise the top 10 attacked countries in six month. (Requests in Thousands)





SQL Injection Attacks Top 10 Countries. Chart generated from Imperva report:

[https://www.imperva.com/docs/HII\\_Web\\_Application\\_Attack\\_Report\\_Ed4.p](https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed4.p)

## What is a WordPress SQL injection?

WordPress SQL Injection is the result of loopholes in the backend coding. An attacker can easily abuse the input fields by inserting malicious code that could execute SQL commands and can Create, Retrieve, Update, and even Delete the data in the database.



---

In the following video, created by the Wordfence team is a WordPress plugin that contains a SQL injection vulnerability. Then we demonstrate how to attack our test website and exploit the vulnerability.

WordPress SQL injection example:

Creating and Fixing a SQL Injection Vulnerability from Wordfence on Vimeo.

## How Hackers Breach the WordPress Database

A WordPress SQL injection can

happen anywhere that your site has a form element:

- Generic contact forms
- Login portals
- Blog comment forms
- Subscription pop-ups
- eCommerce checkout pages
- Search bars
- And so on

The top three plugins that hackers love breaking into are **TimThumb**, **Revslider**, and **Gravity Forms**.

Just one vulnerability in a form element can open a database up to outsiders. This is because the database captures each entry made on a WordPress site. And when hackers want to do serious harm to a website, all they have to do is enter malicious SQL commands

instead of valid form entries.  
How to clean the WordPress database after the hack, please read more [here](#).

## What type of attack is SQL injection?

There are two kinds of SQL injection attacks. A 'classic' SQL injection vulnerability is one where unfiltered user input lets an attacker send commands to the database, and the output is sent back to the attacker. A 'blind' SQL injection vulnerability is when the attacker can send commands to the database, but they don't actually see the database output.

### Classic SQL injection attack.

Classic SQL injections will

return data to the hacker's browser. Fundamentally, they use forms to query the website's database, just as you or WordPress might. This kind of SQL injection happens when a user-supplied field is not strongly typed or is not checked for type constraints. This could take place when a numeric field is to be used in an SQL statement, but the programmer makes no checks to validate that the user-supplied input is numeric.

For example:

```
statement := "SELECT *  
FROM userinfo WHERE id  
=" + a_variable + ";"
```

## What is the blind SQL injection attack?

The blind SQL injections don't return any data at all. Hackers can't see the database output,

they can only see the resulting web page.

That's why these are "blind" attempts. Instead, the hacker will use this SQL injection to execute various actions within the database (like to delete all data).

For example:

```
SELECT * FROM  
bookreviews WHERE ID =  
'Value(ID)';
```


To understand more about classic SQL injection vulnerability and how blind SQL injection work, please read an article by Wordfence.

## How to Prevent SQL Injection attacks in WordPress 2019

## Update Plugins and Theme

The most important for every WordPress user! Keep everything updated including WordPress core, theme, and plugins.

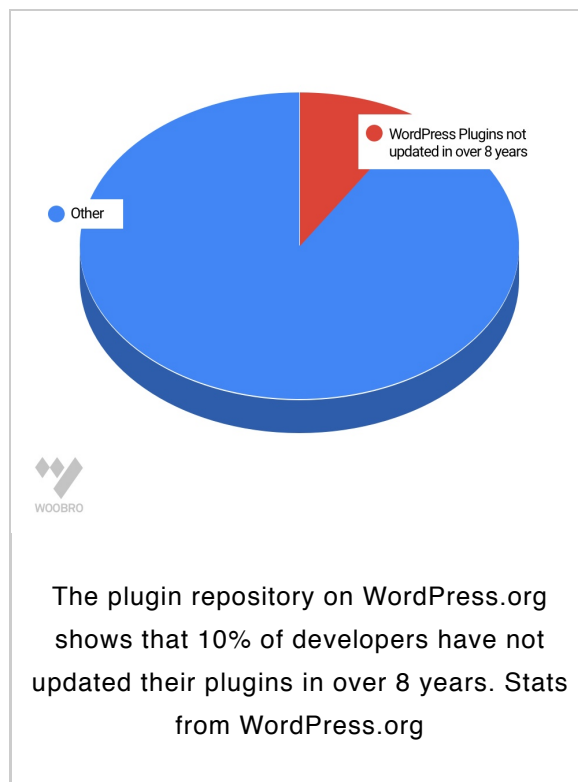
If a theme and plugin are not updated regularly, you insignificant risk to be hacked. Always use a WordPress theme and WordPress plugins that update frequently.



**Note:** Before performing an update, check the compatibility between the WordPress core, themes, and plugins to make sure your site is working as it should be. To test, you can make a copy of your live website, and then check the compatibilities in the WordPress staging environment.

There are currently a total of 56,400 + plugins available in the WordPress.org repository.

The plugin repository on WordPress.org shows that 10% of developers have not updated their plugins in over 8 years.

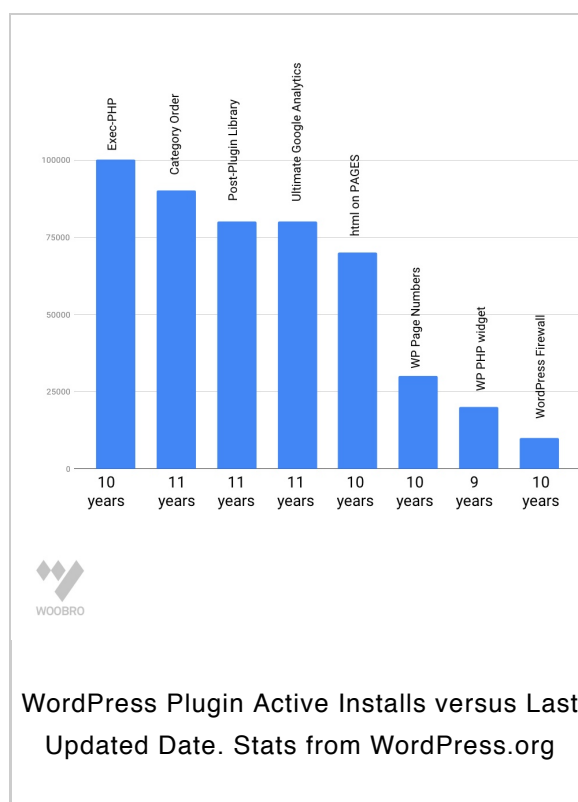


**Many Abandoned  
Plugins Have  
Thousands of Active  
Installs**

Inspired by Isabel Castillo work



“Abandoned WordPress Plugins” we took a closer look at abandoned plugins in the WordPress repository. We designed a chart that shows how many active installs versus last updated date.



Based on Isabel Castillo research there we made top 10 list of abandon plugins that have most active installs. You can find more [here](#).

Last  
Updated

Plugin

Author

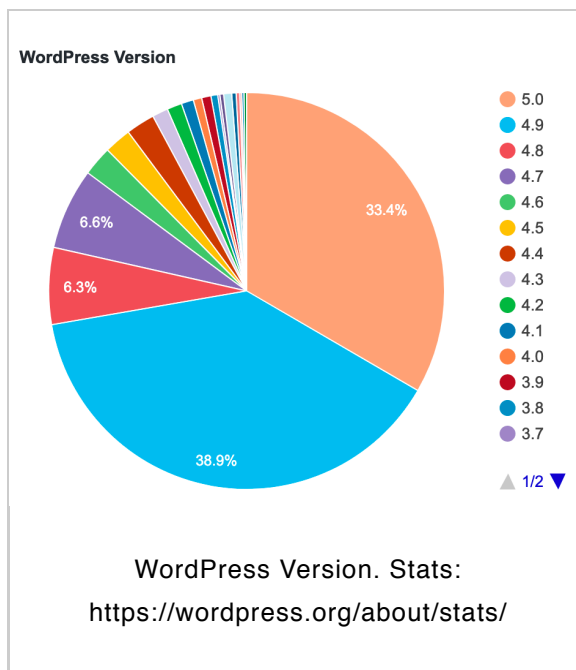
Active  
Installs

|            |                            |                       |        |
|------------|----------------------------|-----------------------|--------|
| 2009-06-23 | Exec-PHP                   | Sören Weber           | 100000 |
| 2008-05-30 | Category Order             | Wessley Roche         | 90000  |
| 2008-09-17 | Post-Plugin Library        | Rob Marsh, SJ         | 80000  |
| 2008-02-03 | Ultimate Google Analytics  | Wilfred van der Deijl | 80000  |
| 2009-10-16 | .html on PAGES             | IntroSites            | 70000  |
| 2009-07-05 | WP Page Numbers            | Jens Törnell          | 30000  |
| 2010-01-31 | Yoast Breadcrumbs          | Joost de Valk         | 30000  |
| 2009-03-06 | pageMash > Page Management | Joel Starnes          | 30000  |
| 2010-11-10 | WP PHP widget              | wpxue                 | 30000  |
| 2010-      | Facebook                   | Marcos                | 20000  |

|            |                          |                   |       |
|------------|--------------------------|-------------------|-------|
| 04-28      | Like Box                 | Esperon           |       |
| 2010-06-26 | Simply Show IDs          | Matt Martz        | 20000 |
| 2009-09-27 | Contact Form 7 Widget    | Stephanie Wells   | 20000 |
| 2009-03-09 | Featured Content Gallery | iePlexus          | 20000 |
| 2008-03-21 | KB Robots.txt            | Adam R. Brown     | 20000 |
| 2009-08-12 | WordPress Firewall       | SEO Egghead, Inc. | 10000 |

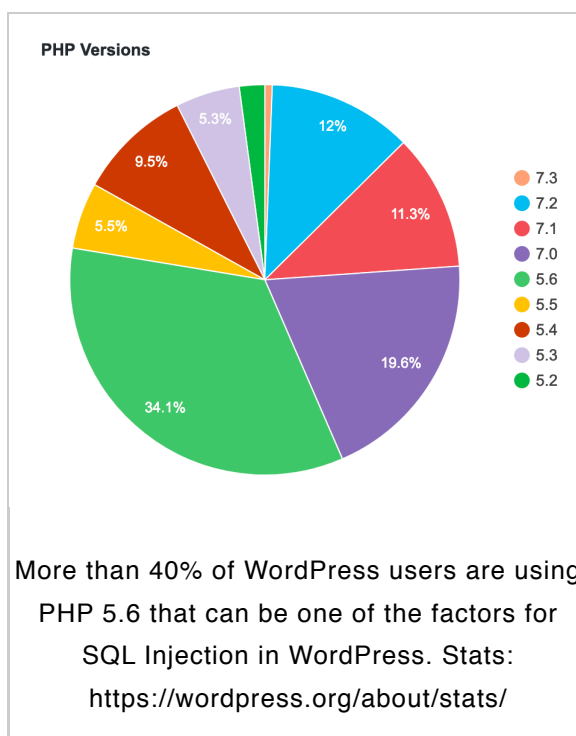
## Update Core

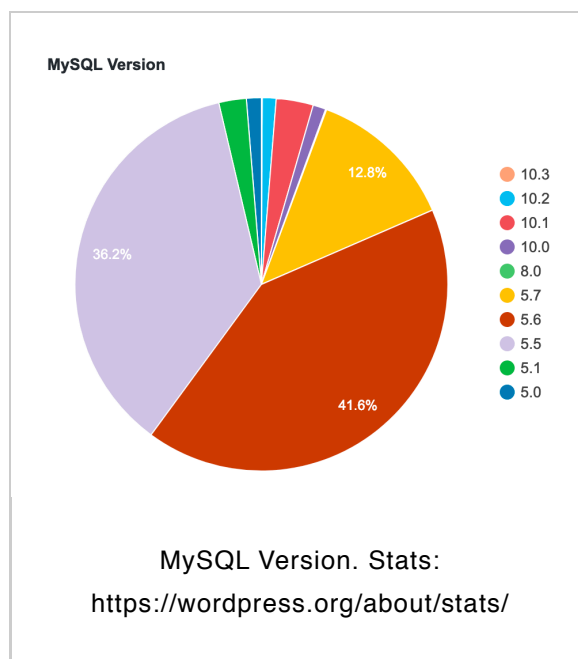
According to the official WordPress stats, only 42.3% of WordPress sites are using the latest version (4.9.x). All previous versions can be vulnerable and might result in getting hacked.



## Update PHP Version

More than 40% of WordPress users are using PHP 5.6 that can be one of the factors for SQL Injection in WordPress.





**Note:** If your WordPress hosting does not support the latest versions of PHP, it's time to switch the host immediately to a managed WordPress hosting that supports most recent versions of PHP like WOOBRO Hosting.

Scan for SQL Injection Vulnerabilities  
WordPress SQL injection checker

You can find some online tools to scan your WordPress site. I have shortlisted the top rated, all you need to do is just enter the WordPress site URL and start scanning for discovered vulnerabilities. WordPress security services

- **WordPress Security**

**Scan** – Checks for basic vulnerabilities on your WordPress site.

Advanced scans are available with a premium upgrade.

- **Sucuri SiteCheck** –

Your WordPress site can be checked for known malware, blacklisting status, errors and if your site is out-of-date.

- **WPScan** – A self-hosted vulnerability scanner that is free for personal use. You can also get a paid license for commercial use.

## WordPress admin password hack: Protecting your WordPress login details

The first and most secure way is to access your WordPress dashboard over an HTTPS connection.

You should also add two-factor authentication to your WordPress because even though malicious hackers can't steal your credentials when accessing the WordPress admin pages over SSL, it is still susceptible to brute force attacks. Two-factor authentication protects your WordPress from automated brute force attacks.

To find out more please click [here](#).

## Backups can help you

## to recover a hacked site

Backups may not be directly related to SQL Injection. But, it can help you to recover a hacked site. WordPress backups can be stored in two ways: Local Backup And Offsite Backup.

## Limiting the Database permissions

Limiting the database permissions on the database login used by the web application to only what is needed may help reduce the effectiveness of any SQL injection attacks that exploit any bugs in the web application.

For example, on Microsoft SQL Server, a database login could be restricted from selecting on some of the system tables which would limit exploits that



try to insert JavaScript into all the text columns in the database:

```
deny select on  
sys.sysobjects to  
webdatabaselogon;  
deny select on  
sys.objects to  
webdatabaselogon;  
deny select on  
sys.tables to  
webdatabaselogon;  
deny select on  
sys.views to  
webdatabaselogon;  
deny select on  
sys.packages to  
webdatabaselogon;
```

## Conclusion

If you are running an online business and want to protect your WordPress website from hackers, you need to take all the security solutions seriously.

Keep everything updated including WordPress core, theme, and plugins. Also, you need tools like WordPress SQL injection checker to monitor your website and receive notifications when you have vulnerability issues on your site.

#### Resources:

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.cloudways.com/blog/wordpress-sql-injection-tools-techniques>
- <https://www.wordfence.com/learn/how-to-prevent-sql-injection-attacks>
- <https://www.imperva.com>

## RELATED ARTICLES

INSIGHT

**WordPress  
Speed  
Optimisation  
Service**

INSIGHT

**Web  
Design  
Process  
for  
Clients**

INSIGHT

**10  
Essential  
Questions  
We Ask  
BEFORE  
We  
Designing  
a  
Client's  
Website**

WOOBRO

**WOOBRO  
Website  
Design  
Receives  
Three  
Offers  
From  
Dragons'  
Den  
Investors**

SERVICE

## WORDPRESS MAINTENANCE SERVICE

We will look after your website so you can spend time doing more important things... like running your business!

learn more >

| websites    | types       | services     | woobro   | clients    |
|-------------|-------------|--------------|----------|------------|
| wordpress   | api         | wordpress    | about us | invoices   |
| woocommerce | integration | maintenance  | work     | tasks      |
| website     | landing     | service      | contact  | management |
| speed       | pages       | websites     | articles | webmail    |
| ux & ui     | ecommerce   | hosting      |          | cloud      |
| design      | websites    | woocommerce  |          | terms and  |
| branding    | blogging    | theme        |          | conditions |
|             | websites    | development  |          |            |
|             | business    | wordpress    |          |            |
|             | websites    | speed        |          |            |
|             |             | optimisation |          |            |

Copyright © 2019 WOOBRO LTD, 86-90 Paul Street, London EC2A 4NE, Shoreditch.

Registered in England & Wales Company Number 10997949 / [privacy policy](#)

/ [terms and conditions](#)