Local Hosting vs. Cloud Hosting

Local Hosting vs. Cloud Hosting

Goals

By the end of this case you will:
- Understand what local hosting is
- Understand what cloud hosting is
- Understand the difference between local hosting and cloud hosting
- Be able to select between local hosting and cloud hosting in a given context

>

Introduction

Designed by Freepik

>

When developing a website, the code for that website is kept in files. Those files must be saved/stored somewhere. That storage space “hosts” the website files, and this is what we mean by website hosting. In this way, hosting is essential as websites are not accessible without it. We will see two kinds of hosting: local hosting and cloud hosting. We will review each in detail, discuss their respective pros and cons and invite you to select between them in a given context.

>

Business Context

As a website developer, you may be expected to set up a hosting environment or be asked to partner with a web host in the early stages of development. The better your understanding of these concepts, the more effectively you will be able to collaborate with hosting partners. Whether it

be for setup, settings adjustment, security concerns, or bug/incident response, you will be expected to work closely and efficiently with hosting partners to advance projects and address concerns.

What is Local Hosting?

What is Local Hosting?

In website development, when we say “local”, we mean “on your computer”. For example, when you save a document on your desktop, that document is said to have been saved locally. It is possible to save an HTML file on your computer and view it in your browser. In this case, your computer acts as a **local host** for the files. When files are hosted locally (on your computer), outsiders who are not on your computer will not be able to view those files.
>
The relative privacy of local hosting is a double edged sword. On the one hand, because files are local and not visible to outsiders, this is ideal if you are working alone and/or just getting started. On the other hand, it is not possible to collaborate with others in the context of local hosting unless you are sharing the physical computer with your fellow collaborators.
>
Sometimes local hosting can also mean files are stored on a private server that is only accessible to people within a local area network (LAN). It is also possible to connect a private server to the internet and use this private (local) server to deliver a website to the public, but this is rarely the best choice as we will see when we consider pros and cons.
>
What is Cloud Hosting?
You may already have some idea of what is meant by the “cloud”. When files are hosted (saved) on the cloud, it means the files have been saved on an outside server (not your computer) that is accessible using the internet. There are a few ways that you can move a file from your computer (local) to an outside server (cloud). We will look at some of these different ways in the next section. For now we only want to understand that cloud hosting refers to storing files on an outside server.
>
As I’m sure you’ve already guessed, cloud hosting is less private than local hosting. Though less private, it is necessary for collaboration in website development, and essential for users to access your website once it is developed. There are many ways to keep cloud hosting secure and we will address some of these security concerns later this week.
>
There are also fees associated with cloud hosting as you are renting space on the outside server to host your files. These fees are paid to the hosting provider (ex. Amazon, Bluehost, Dreamhost, HostGator). The cost depends on how much space you are renting and whether you are sharing the server with other people (shared hosting) or you have the server all to

yourself (dedicated hosting). Shared hosting is less expensive than dedicated hosting.
>
Pros and Cons
The table below outlines some of the pros and cons of local vs cloud hosting.
	Local Hosting	Cloud Hosting
———	———-	———-
Pros	Private	Public
		Availability of wider resources
	Good for testing/development or staging	Faster loading times
		Accessible to the public
	You are in control of the server/computer	Considered safer
Cons	Limited resources	Associated cost $
	Slower loading times	Depend on the web host to secure your hosting environment at the server level.
	Considered less safe	

Conclusion & Takeaways

Conclusion & Takeaways

Local hosting and cloud hosting each have their place in the field of website development. It's all about deciding where you want to save your files, and striking a balance between the pros and cons in any given context.
Consider the scenarios below and evaluate whether local hosting or cloud hosting is the most advisable option. After reading each scenario, **circle** the type of hosting you recommend.
>
Scenario 1
You've decided to build yourself a small website to serve as a portfolio of your work as a web developer. Eventually you will want to put it online, but for now you are still just playing around with the code, trying to get it to look polished and professional.

Scenario 2
Your customer wants to put up a one-page website as soon as possible so that they can begin running Google Ads that drive traffic to their page. The page will include their logo, mission statement, contact information, and opening hours. They may add to the website later, but for now, they just want a live page to work with Google Ads.

Scenario 3
You have been contracted to work on an e-commerce website for a large company. They have a local server room that hosts their website now as it is being developed. They would like to launch the website that they have now and make no changes to the live site once it is published. They would also like to keep a copy of the site on their local servers, so that they can continue to develop new features until they are ready for the public.
>

Scenario 4
Your friend has asked you to help them create a one-page HTML file with their resume's information. Your friend has not bought a domain name yet, they only want help with building the HTML file.

Attribution

https://www.freepik.com/free-photo/website-hosting-concept-with-screen_26412543.htm

Setting Up a Localhost

Setting Up a Localhost

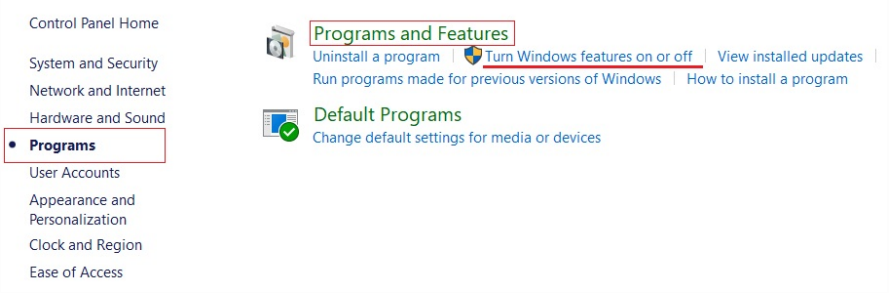
Goals

By the end of this lesson you will:
- Understand how to set up localhost
- Set up localhost on your computer
- Practice using your newly configured localhost
>
Introduction
Learning how to set up a localhost on your computer is a handy bit of knowledge that will allow you to play around with website development, without publishing unfinished work and without needing to pay for cloud hosting. The process is different depending on your operating system. We will consider how to set up a localhost server in Windows 10. If you are not running Windows 10 or if you encounter technical difficulties, an alternative activity will be provided.
>
Business Context
In a business context, your employer may already have a hosting set up as well as IT employees who assist with configurations and access. However, it is also possible that you will work for a small business, or that you will decide to work as a freelance web developer. In the later case, knowing how to use localhost will provide you with the independence you need to get started quickly.

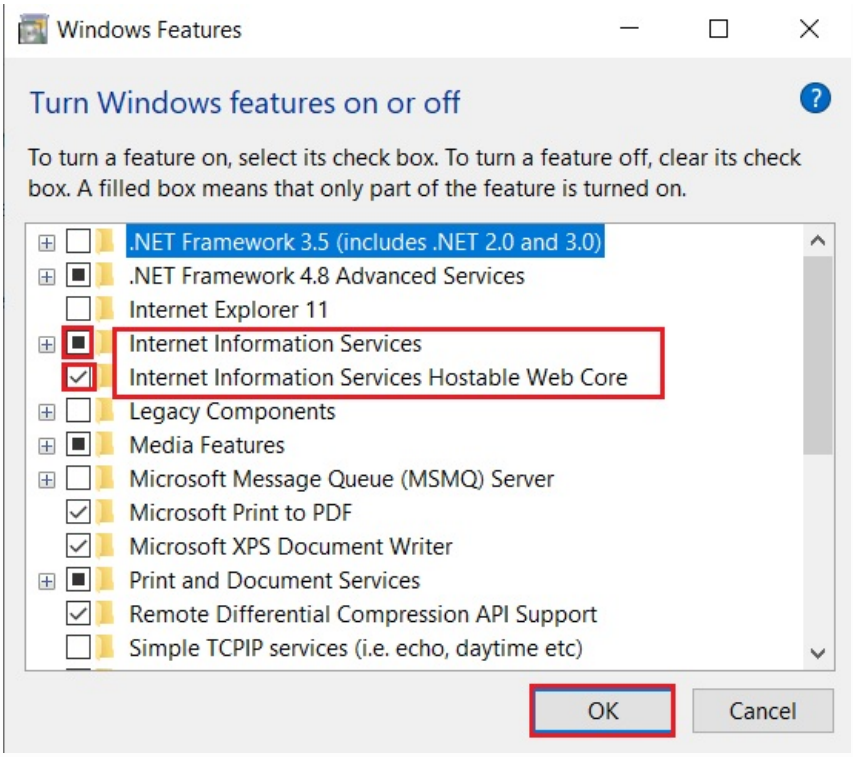
Localhost server in Windows 10

Localhost server in Windows 10

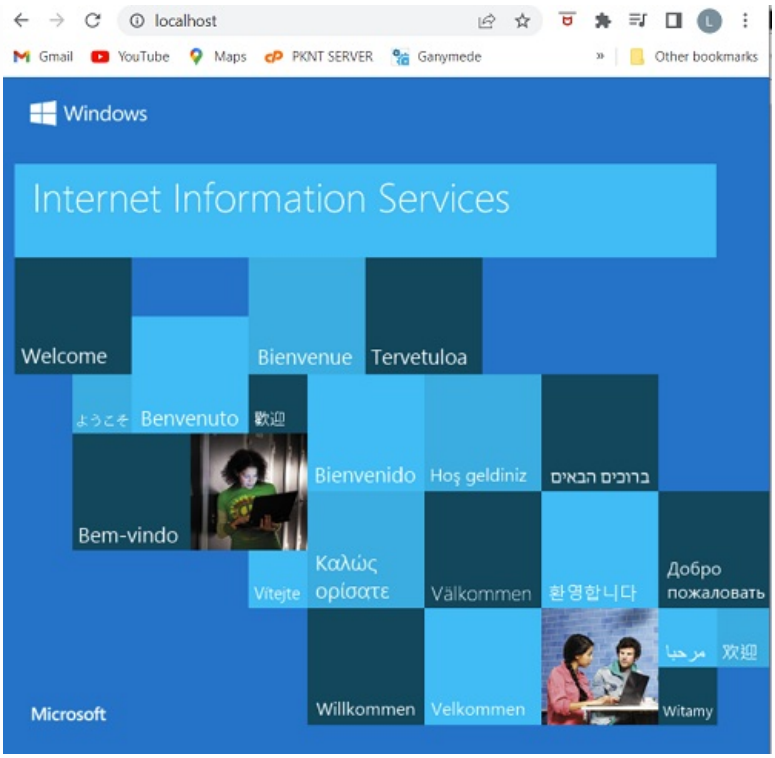
Watch the following video to learn how to set up localhost in Windows 10. It is recommended that you watch the video all the way through one time and then re-watch the video, following along by doing each step on your own computer, pausing as needed. Basic steps are listed below the video link to help you in case your computer looks different than the one in the video.
>
If you run into trouble (with permissions for example), you can use the alternate activity on the next page.
>
Video: How to set up a local host in Windows 10
>
1. Open your Control Panel
2. Open Programs and Features
3. Click on Turn Window features on or off



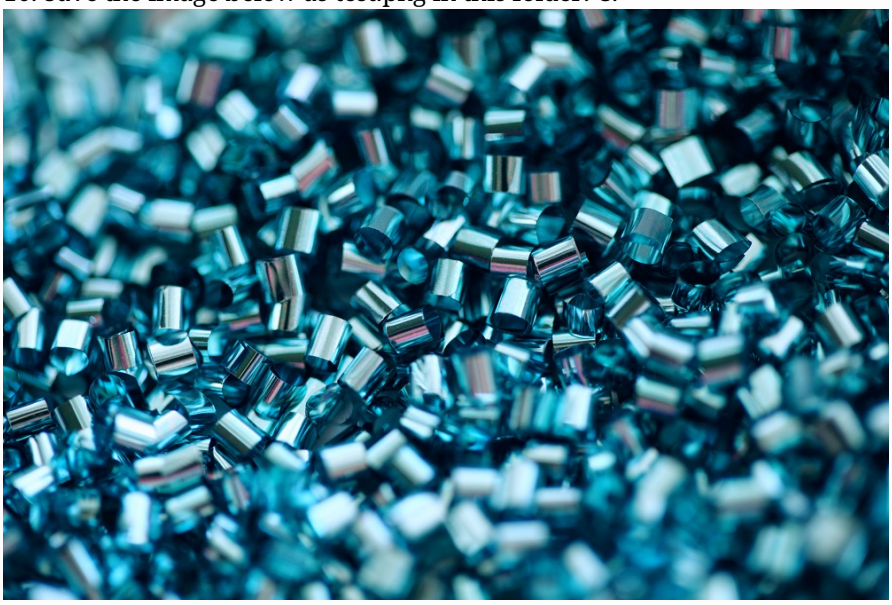
4. In the popup, locate Internet Information Services, check the box. If you also see Internet Information Services Hostable Web Core then check that box as well. Click OK.



5. Allow your computer to search for required files and apply changes. Do not cancel.
6. When your computer is finished making the changes, it may ask to restart your computer. This is normal. Save any changes you may need to in open files. Close everything including the Control Panel and restart your computer.
7. You are now ready to test your localhost. Open a new tab in your browser and type localhost and hit Enter.
>
You will see a window like this one:



8. Using file explorer go to C:and double click on iisstart.png
9. It will ask what program it should use to open .png files and suggest Photos. You can just click OK. It will open the png file in photos and will look like the localhost start page.
10. Save the image below as test.png in this folder: C:



11. Now return to your browser tab to view http://localhost/test.png

Alternate activity

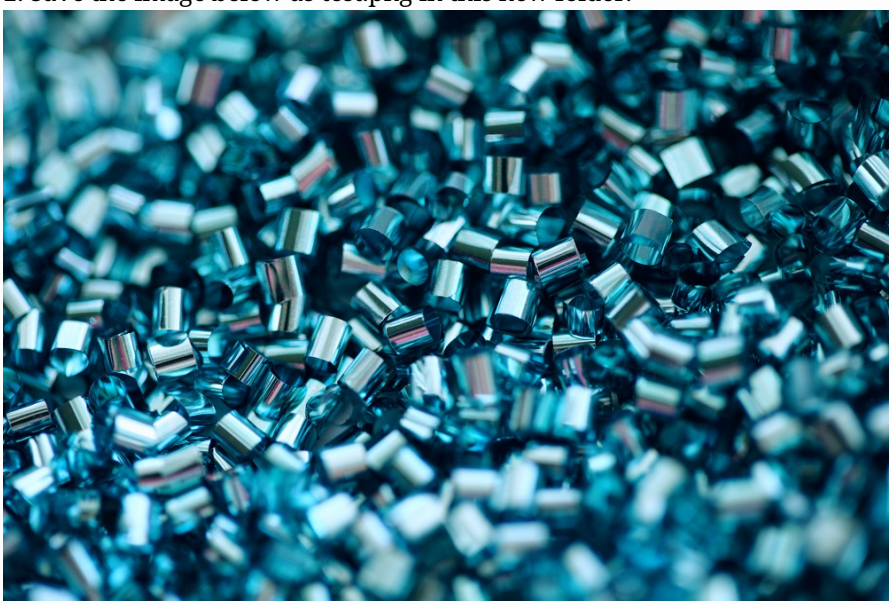
Alternate activity:

>

If you do not have Windows 10 or do not have the necessary permissions to set up localhost or if you did not have the necessary permissions to save an image in the wwwroot folder, you can try this activity instead.

>

1. Create a new folder on your computer called MyLocalWebsite.
2. Save the image below as test.png in this new folder.



3. Open TextPad or Notepad on your computer.
4. Copy the code below into TextPad or Notepad.

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="utf-8" />
   <title>My local web page</title>
</head>
<body>
   <h1 style="text-align:center;">Locally Hosted Web Page</h1>
   <img src="test.png" style="width:100%;" alt="This is a test
image"/>
</body>
</html>
```

5. Save the file as test.html in your MyLocalWebsite folder.
6. Now use file explorer to locate this file on your computer.
7. Double click on the file test.html to open it.
   The file will open in a tab on your browser. You can modify this local html file, save the changes, and refresh your browser tab to view the changes.
8. Since websites include many files, it's good practice to organize your images in a separate image folder. Create a new folder called img inside the MyLocalWebsite folder.
9. Save the following images as test2.jpg and test3.jpg in this new img folder.
   >

10. Update your code in your local test.html file to read these two images from the img folder instead of the original test.png image.

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="utf-8" />
   <title>My local web page</title>
</head>
<body>
   <h1 style="text-align:center;">Locally Hosted Web Page</h1>
   <img src="img/test2.jpg" style="width:45%;float:left;"
alt="This is a test image"/>
   <img src="img/test3.jpg" style="width:45%;float:right;"
alt="This is a test image"/>

</body>
</html>
```

Conclusion & Takeaways

Conclusion & Takeaways

Though it comes with some limitations, the flexibility of working locally in web development is sometimes very convenient, especially when you are just getting started with a project. Knowing that only you can see your files can remove pressure and free you to explore, take risks and get creative. Cloud hosting can always be set up later.
>
Attribution
- How to Setup localhost Server in Windows 10 Create Local Host Server IIS Server Windows 10 https://www.youtube.com/watch?v=gpSK0CbSu2g
>
- Free images resource https://unsplash.com/images/events/celebration
>
- https://unsplash.com/photos/ooxMySOfRRU Photo by Alexander Grey on Unsplash
>
- Open Access at the National Gallery of Art https://www.nga.gov/open-access-images.html
>
- “Mahana Atua” by Paul Gauguin, 1894 https://www.nga.gov/collection/art-object-page.4876.html
>
- “Le Sourire” by Paul Gauguin, 1899 https://www.nga.gov/collection/art-object-page.4877.html

Setting Up a Cloudhost

Setting Up a Cloudhost

Goals

By the end of this case you will:
- Know how to select a cloud hosting provider and a hosting package
- Understand how to use FTP to move files
- Familiarize yourself with cPanel
>
Introduction

Designed by Freepik
>
If the decision has been made to host the website using Cloud Hosting, the next step is to determine which cloud hosting provider will be contracted to host the website. Hosting providers offer a variety of options with their hosting packages. A decision must be made regarding which cloud hosting package is best suited for your project. Once the cloud hosting environment has been set up, you can use **FTP** to upload local copies of your website files (stored on your computer) to the cloud. It is also possible that your hosting package includes **cPanel** access, in which case you can directly access and update your website files in the cloud without the need for local copies of the files.
>
Business Context
If your employer or client already has a public website, then they already

have a Cloud Hosting environment. Sometimes a client does not know how to access their files but they do know who their Hosting provider is. In this case you can contact the hosting provider directly and they will provide you with either **FTP** or **cPanel** access. If your client does not have a website yet, you may need to recommend a hosting provider and package for the project as well as coordinate with the hosting provider on behalf of the client to set up the environment and gain access to it.

Selecting a Cloud Host & Package

Selecting a Cloud Host & Package

There are many web hosting providers to choose from. Some of the most popular include:
- Bluehost https://www.bluehost.com/
- HostGator https://www.hostgator.com/web-hosting/
- HOSTINGER https://www.hostinger.com/
>
Each of these providers offers the choice of shared hosting, dedicated hosting, and VPS hosting (Virtual Private Server). We will briefly overview the differences between these.
Shared Hosting - Best for small websites with low traffic
>
This is the most common type of cloud hosting and is the first choice for small businesses. With shared web hosting, many websites share resources on a single server. You will only have access to your files, but you will share bandwidth, processing power and memory with the other websites on that server. While this is the least expensive hosting option, there can be disadvantages, particularly if your website is very large and/or supports a great deal of traffic. Another concern with shared hosting relates to security. If a website on the shared server becomes infected with malware, for example, it can infect other websites on that server.
>
Package prices vary depending, among other things, on the amount of space included in the package. Discounted prices are offered at signup, but renewed at a different price. Other signup perks are also offered. Email should be included with a hosting package but isn't always.
>
No matter what package you select, it is always worthwhile to call the hosting provider to speak directly with a representative. They will be able to answer all of your questions about what is included for the first year only, and what is included when the package renews the following year.
>
One small note regarding SSL certificates: Though free SSL certificates are generally available for at least the first year of shared hosting, these are not the best SSL certificates. Most hosting providers and/or domain name registrars offer a variety of SSL certificates as a separate product depending on the level of data encryption your website requires. For simplicity, we will not worry about SSL certificates at this time.
>
Below, you will find information about three comparable hosting packages from different cloud hosting providers as of January 2023. Items in red,

though included with the package, are **free to everyone** regardless of their web hosting provider. Items in blue are **very nice to have**, but you'll want to ask the hosting provider if those benefits carry over to the following year, or if they only apply for the first year.

>

It is usually also possible to purchase add-ons if there is something you want that is not included in the package you are considering. Remember that hosting providers want your business and can sometimes be flexible when presented with a competing offer. Don't be afraid to ask lots of questions, and a little negotiation can only work in your favor.

Bluehost	HostGator	HOSTINGER
———	———-	———-
7.38 USD/month* *Renews at 27.08 USD/month*	*3.50 USD/month Renews at 12.99 USD/month*	*3.99 USD/month Renews at 8.99 USD/month*
40 GB SSD Storage	*Unmetered disk space*	200 GB SSD Storage
Free CDN	Unmetered bandwidth	*Unlimited Bandwidth*
Custom WP Themes	*Website & domain transfers*	*~100 000 Visits Monthly*
SSL certificate	SSL certificate	*Unlimited Free SSL*
Daily Website Backup - 1year	Unlimited Websites	100 Websites
Domain name - 1year	1 year domain registration	Free Domain ($9.99 value)
Domain Privacy	One-click WordPress installs	Nameservers
Malware Scanning	**Email**	**Email**
Resource protection	30 Days Money Back Guarantee	30 Days Money Back Guarantee
Domain manager		**DNS Management**
Google my business		Unlimited Databases
Yoast SEO		**Website builder**
		Cloudflare Protected
$150 Google Ads spend match credit	**$500 Google Ads spend match credit**	**Daily Backups ($25.08 value)**
	$100 Microsoft Advertising credit	*Managed WordPress*
		WordPress Acceleration
		WordPress Staging Tool
		24/7 Support
		99.90% Uptime Guarantee

>

As of January 2023

Note: Although all of the recommended packages meet the customer's shared hosting requirements, it is not advisable to choose the Bluehost package (Provider 1) due to its high cost and unreasonable renewal price.

Dedicated Hosting vs VPS Hosting

Dedicated Hosting vs VPS Hosting

Image by Freepik

>

As we saw in the previous section, shared hosting is an affordable solution for a smaller website that sees limited traffic.

>

Larger websites, however, will require additional resources. Among other things, they need more storage and more bandwidth to operate. For these websites, dedicated hosting & VPS hosting offer two alternatives to shared hosting.

>

Dedicated Hosting - Ideal for larger companies with more traffic

This kind of hosting is more expensive (between $100-$150 a month), but comes with many benefits. With dedicated hosting, your website is the only one on that server. With this kind of hosting, you are not sharing bandwidth or server resources or memory with other websites. This will help your website to run faster and handle more traffic than it could with shared hosting.

The risk of malware or virus infection from neighboring websites is also eliminated because your site is alone on the server (you have no neighbors). Since you're paying more, you can count on improved, around-the-clock technical support from the hosting provider.

>

VPS Hosting - Ideal for the in-between

This kind of hosting is a middle-ground between shared and dedicated hosting. Your website is on a shared server BUT a specific quantity of resources, bandwidth and memory are dedicated to your website. It is perfect for a website that has outgrown shared hosting but is not quite big enough to require dedicated hosting.

As with shared hosting, there are different packages available depending on the volume of server resources/bandwidth/memory that will be dedicated exclusively to your website, but you can expect to pay somewhere around $50 per month.
>

FTP : File Transfer Protocol

FTP : File Transfer Protocol

FTP is a means of moving files between your computer and the cloud hosting environment. You can upload files to the host server or download files from that host server. There are several programs that help you do this, but FileZilla (https://filezilla-project.org/) is FREE and widely used because it is available for Mac, Windows and Linux systems. There is also an affordable PRO version of the software that offers additional features, though generally the free software is sufficient.
>
The software must be downloaded to your computer and access to a website can be added using the login credentials provided to you by your web hosting provider.
>
One of the major advantages of using FTP is that you can upload and download not only files, but entire folders, including sub-folders with a simple drag and drop. Though it may take some time, the folder and sub-folder structure will be respected, which is great for moving a website from localhost to cloudhost, or for backing-up folders locally before making changes on the server files.
>
You can view some screenshots of the software here: https://filezilla-project.org/client_screenshots.php
>
Here is a short introductory video to FileZilla
https://www.youtube.com/watch?v=JilbuyOGA00
>
Getting to know cPanel
cPanel access is sometimes included with your cloud hosting package. There are hosting providers who will only make cPanel available at an additional charge.
>
cPanel is an easy-to-use website management platform offering a wide variety of features including a file manager, database access, virus scanner, PHP version manager and more. It is accessed through your web browser using login credentials provided to you by your web hosting provider. Always request cPanel access to your hosting environment as cPanel tools are tremendously helpful for web development.
>
You can view features and screenshots of the platform here
https://cpanel.net/products/cpanel-whm-features/

>
Here is a short introductory video to cPanel
https://www.youtube.com/watch?v=nwM5xd_AJOs

Conclusion & Takeaways

Conclusion & Takeaways

Selecting the best cloud hosting solution for your web project can seem a little daunting at first glance. There are so many features, packages and providers to choose from. Prices are often listed as discount prices for first-time clients and it is not always apparent what the renewal prices will be. Those low first-time prices also often depend on contracts that are billed annually even though prices are advertised as monthly.
>
To make the best choice, you need to think about what your project requires. If it is a small website, then a shared hosting solution is desirable. If it is a large website that expects a good deal of traffic, then dedicated hosting is more appropriate. If the website is medium sized, meaning it requires dedicated resources but is not large enough to justify the expense of dedicated hosting, then VPS hosting offers a reasonable middle-ground between shared and dedicated hosting.
>
Once you have a cloud hosted environment for your website, you will need to access it. FTP software like FileZilla and cPanel access will provide you with the means of managing your website.
>
Attribution

- https://www.freepik.com/free-vector/cloud-computing-polygonal-wireframe-technology-concept_12071198.htm
- https://www.freepik.com/free-vector/abstract-creative-website-hosting-illustration_21743698.htm
- Bluehost https://www.bluehost.com/
- HostGator https://www.hostgator.com/web-hosting/
- HOSTINGER https://www.hostinger.com/
- FileZilla screenshots https://filezilla-project.org/client_screenshots.php
- Introduction to FileZilla https://www.youtube.com/watch?v=JilbuyOGA00
- cPanel features https://cpanel.net/products/cpanel-whm-features/
- Introduction to cPanel https://www.youtube.com/watch?v=nwM5xd_AJOs

Common Website Attacks

Common Website Attacks

Goals

By the end of this case you will:
- Have a basic understanding of 4 types of common website attacks
- Understand where and how these common attacks occur
- Be able to identify possible outcomes for each of these common attacks.
>
Introduction

Image by Freepik
>
Web security is a critically important aspect of web development. Protecting your website's data, as well as the data of the website's users must always be a top priority. Malicious actors prey on a website's vulnerabilities for a variety of reasons. In this unit we will consider the following four types of common attacks:
1. Cross site scripting (XSS)
2. SQL injection
3. Directory traversal
4. DDoS

and what basic steps you can take to protect your website against them.
>
Business Context
You may think that large businesses make the best targets for attack, but

small businesses are desirable targets as well. One reason is that small businesses often have little to no budget for maintenance, leaving vulnerabilities unpatched for extended periods. This can make gaining access easier for attackers. Understanding how these attacks occur is the first step towards building a robust website with an eye toward web security.

Cross Site Scripting (XSS)

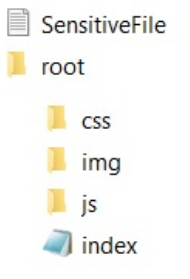
Cross Site Scripting (XSS)

Cross site scripting is a type of injection attack which often occurs at the level of the web interface. For example, if you have a contact form on your website, information received in that contact form is generally safe, but if the form submission contains malicious code, that code risks being injected through the contact form. In this way, an attacker may be able to access sensitive/private information or execute malicious code on the server. There are 3 main types of cross site scripting attacks: reflected, stored and dom-based.
>
Here is a short video to provide an overview of the three types of cross site scripting attacks.
https://www.youtube.com/watch?v=DxsmEXicXEE
>
SQL Injection
The vast majority of websites pair files containing code, with a database. The code in the files communicates with the database using MySQL statements. SQL injection is also a type of injection attack that injects malicious code directly into the website database. The result can reveal sensitive/private information and give the attacker control over the website. In a worst case scenario, the attacker might even be able to take control of the server hosting the website.
>
Here is a short video to provide an overview on SQL injection attacks.
https://www.youtube.com/watch?v=Yqu93GXx0vI

Directory Traversal

Directory Traversal

Directory traversal, also known as path traversal, is an HTTP attack wherein the attacker exploits vulnerabilities to gain access to directories and files outside of the website's root folder. If successful, the attacker can not only view sensitive files, they may also be able to execute commands on the server.
>
Consider the following file structure for a very simple website:



>
Everything in the root folder can be safely accessed through a web browser, however, outside of the root, suppose there is a sensitive file that the browser should not be able to access. This sensitive file might include server logs, for example, that expose sensitive data about the file structure, existing vulnerabilities or server settings. We want to ensure that malicious actors do not have access to sensitive information.
>
Let's assume that there are numerous images stored in the 'img' directory. The index page will determine which image to display based on the specific filename provided in the query string (parameters included within the URL).
>
So, for example, if the URL says: https://mywebsite.com/index.php?show=myimage.jpg, then the index file will load **/img/myimage.jpg**.
But if the attacker modifies the query string and the variables are not sanitized or permissions are not set securely then this command will reveal the contents of the sensitive file outside of the root directory
https://mywebsite.com/index.php?show=··/··/SensitiveFile.txt

Here is a short video illustrating how directory traversal (using ../ to navigate directories) can be exploited to access sensitive information.
https://www.youtube.com/watch?v=a0nXnY3_1gw
>
Distributed Denial of Service (DDoS)

This is a more complicated type of attack that requires the coordination of several computer systems to attack a given target. The target could be a particular website or server. The attack denies (blocks) service to regular/intended users of the target website or server. This can result in significant service interruptions impacting business and users alike.
>
For example, if a target banking website is bombarded with requests, this may create a digital traffic jam of sorts that prevents the website from being accessed by regular/intended users. Clients would no longer have access to their online banking. A large-scale denial of service attack can have important social impacts and constitutes one of the major digital threats of our time.
>
Here is a short video that illustrates DDoS attacks
https://www.youtube.com/watch?v=ilhGh9CEIwM

Conclusion & Takeaways

Conclusion & Takeaways

Cross site scripting, SQL injection, Directory Traversal and Distributed Denial of Service are four of the most common types of attacks that a website can encounter.
>
Understanding the basic idea behind each of these will help you construct code that better resists these and other types of attacks.

Image by rawpixel.com on Freepik
>

> ### Attribution
>
> - Image https://www.freepik.com/free-vector/cyber-security-concept_7970729.htm
> - Cross site scripting https://www.youtube.com/watch?v=DxsmEXicXEE
> - SQL Injection https://www.youtube.com/watch?v=Yqu93GXx0vI
> - Directory Traversal https://www.youtube.com/watch?v=a0nXnY3_1gw
> - DDoS https://www.youtube.com/watch?v=ilhGh9CEIwM
> - Image https://www.freepik.com/free-photo/eye-futuristic-robot_11309679.htm

Defending Against XSS

Defending Against XSS

Goals

By the end of this case you will:
- Understand how filtering user input resists cross site scripting (XSS)
- Use javascript to validate user input in a form
- Use javascript to sanitize user input variables
>
Introduction
Now that we have a solid understanding of some common website attacks, we must learn how to defend against them. Cybersecurity is a field unto itself, but as a website developer there are many things you can do to protect your employer/client and their data, as well as to protect users who visit your website. In this section, we will consider simple defenses against XSS attacks by learning how to filter user inputs on simple contact forms.
>

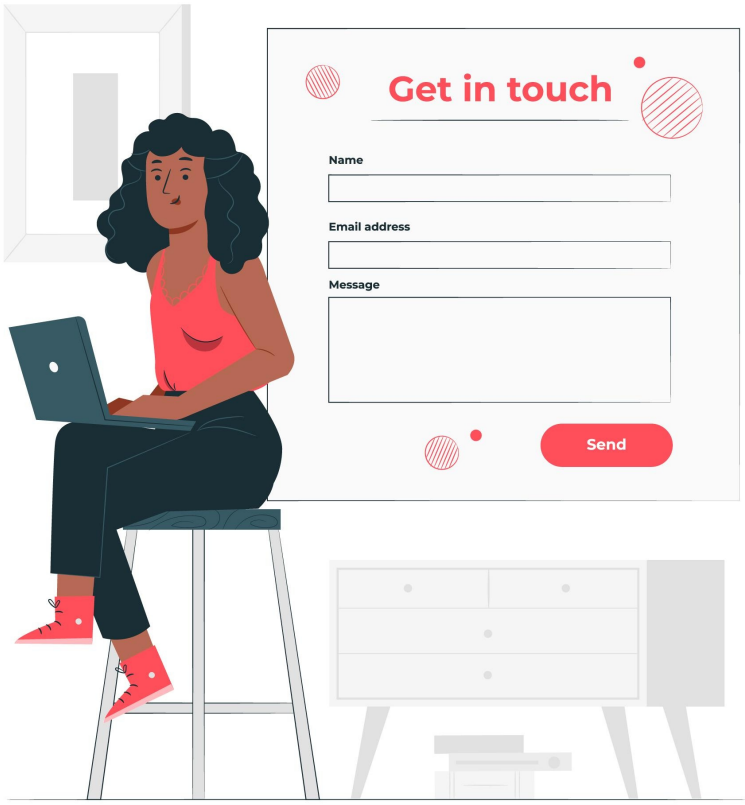


Image by storyset on Freepik

>
Business Context
While larger companies do employ cybersecurity experts to safeguard their websites, their servers, and their networks, smaller companies will depend on their web developers to make their websites as safe as possible. Web hosting providers also have a critically important role to play in securing the websites they host by securing their servers. As a website developer, you are not responsible for server level security. You are however responsible for ensuring that the website you build, and the code it uses, respect web security best practices.

Filtering User Inputs

Filtering User Inputs

You will recall that Cross Site Scripting attacks occur when malicious code is injected through a form on the website. The attacker needs to inject and execute their malicious code. You can prevent this by validating inputs and sanitizing variables. This is known as input encoding. The attacker will still be able to enter their malicious code, but your code will intercept it and clean it up before it can run, thereby thwarting the attack.
>
Consider the following HTML form.

This form will take input from the user (name and email address) in order to add the user to the list of Newsletter recipients. If an attacker tries to enter malicious code in the name or email fields, we will need to intercept the attack.
>
When the user clicks the submit button, a JavaScript function is called that will validate and sanitize the user inputs so that they can be safely submitted. If the user inputs are unsafe, the form will not submit and instead show an error message.
>
The HTML code for this form, as well as the JavaScript function are included below.
>
Save the code below as a file in your localhost environment, then view the file in your browser.
>

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="utf-8" />
   <title>My Basic Form</title>
</head>
<body>
   <h1 style="text-align:center;">Newsletter Sign-Up</h1>
```

```
   <form name="MyForm"  method="Post" action="thankyou.html">
     <div style="text-align:center;">
     <input type="text" name="fullname"  placeholder="Your
name">
     <input type="text" name="email"  placeholder="Your email">
     <input type="submit" name="submit"  value="Submit"
onClick="javascript:return validateInputs();">
    </div>
   </form>
<script>
function validateInputs()
  {
    //declaration of variables
    var SubmitForm;
    var FormErrors;

    //Initially set SubmitForm to true.
    SubmitForm = true;

    //Retrieve variables to be validated and sanitized
    //Assume they are dangerous for now
    var fullname    = new
String(document.MyForm.fullname.value);
    var email   = new String(document.MyForm.email.value);

    //Check that the user inputs are not blank
    //JavaScript logical operator for OR : ||
    if ( fullname.length<1 || email.length<1 )
    {
    FormErrors = "All fields are mandatory. Please complete the
form.";
    SubmitForm = false;
    } else {
//Set up a filter for the pattern of an email
//Learn more about referencing characters:
//https://developer.mozilla.org/en-
US/docs/Web/JavaScript/Guide/Regular_Expressions/Character_Class
es

var filter = /^([\w-]+(?:\.[\w-]+)*)@((?:[\w-]+\.)*\w[\w-]?)$/i;

    //Use test() method to check user email against the filter
    //test() method:
https://www.w3schools.com/jsref/jsref_regexp_test.asp
    if (!filter.test(email))
    {
        FormErrors = "Your form contains invalid field entries.
Please correct your form before submitting";
```

```
        SubmitForm = false;
     }
    }

    if (SubmitForm == false)
    {
        //The form cannot be submitted.
        alert(FormErrors);
        return false;
    } else {
        //SANITIZE user inputs by allowing only [a-z 0-9 _ - .
@]
        //strip forbidden characters
        fullname = fullname.replace(/[^a-z0-9\s\-]/gim,"");
        fullname = fullname.trim();
        email = email.replace(/[^a-z0-9_@.-]/gim,"");
        email = email.trim();

        //ready to submit
        document.MyForm.submit();
    }
}
</script>
</body>
</html>
```

Try submitting the form using your name and email address.
You should get a crash page on **thankyou.html** because you have not created this page yet.
>
Create and save an HTML file called thankyou.html then try the form again.
>
If you made it to your new thankyou.html page, then the form was successfully submitted.
>

Conclusion & Takeaways

Conclusion & Takeaways

Controlling user inputs on forms is an essential element of defense against XSS attacks. This can be done by limiting the length of inputs, matching inputs against expected patterns, and of course most importantly sanitizing variables before submitting them.
>
Never output unsanitized user inputs.
>
Attribution
- Image https://www.freepik.com/free-vector/get-touch-concept-illustration_8960459.htm
- test() method https://www.w3schools.com/jsref/jsref_regexp_test.asp
- referencing characters https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Regular_Expressions/Character_Classes

Defending Against Directory Traversal

Defending Against Directory Traversal

Goals

By the end of this case you will:
- Understand the importance of specifying your base directory
- Know the difference between full paths and relative paths
- Understand how to use relative paths to include files in your code
- Practice sanitizing a variable containing a file path
>
Introduction
Since directory traversal involves an attacker attempting to gain access to content outside of the website's root directory, the first line of defense occurs at the server level. Your web host will set permissions on the directories in your hosting environment which should prevent an attacker from gaining access to higher level directories.
>
That being said, you can still make your code more robust against directory traversal attacks.

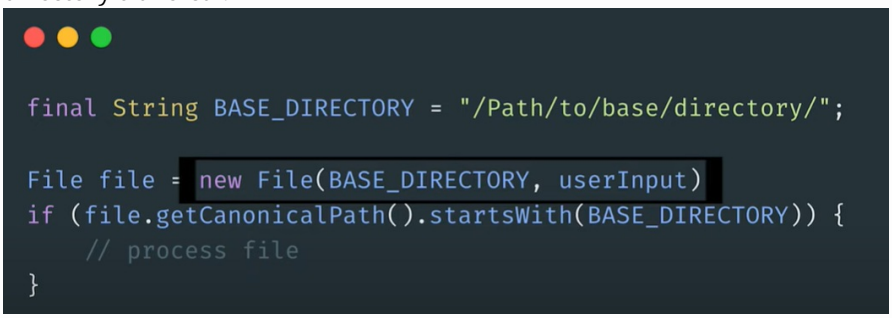
Image by rawpixel.com on Freepik
>
Business Context

Your employer/customer may know absolutely nothing about common cyber security attacks and how to guard against them. They will depend on you to integrate responsible and safe code and to advise them of any security precautions they should take. Web development is a field in which lifelong learning is rewarded. Never stop learning how to improve your code, because hackers will never stop trying to hack it.

Don’t Open the Door

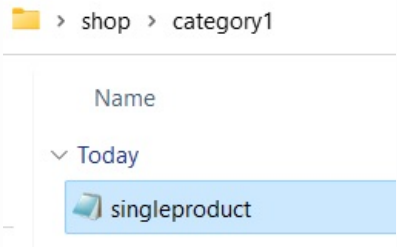
Don’t Open the Door

The most effective way to prevent directory traversal is to avoid passing any user supplied input to the file system in the first place. If the door is never open, an attacker will never be able to get through it. The risk arrives when a user has the opportunity to speak to the file system through a form or through a querystring as seen in unit 2.1.
>
BASE_DIRECTORY
Even if the door is closed, it is considered good practice to establish the base directory in your code. Website development platforms like WordPress will do this by default, but if you are not using a content management system, you can explicitly set the base directory as a variable to be used throughout your code.
>
The second most important thing you can do is to sanitize user input variables, as you did in the previous unit, to ensure that they do not contain directory traversing inputs. User inputs must always be sanitized.
>
Below is a screenshot that showcases an example of how to specify your base directory. It is assumed that the **userInput** has been sanitized.
>
Before processing the file, this code double checks that the file path begins with the base directory. This is another effective mitigation tactic against directory traversal.



Taken from: https://www.youtube.com/watch?v=Jg5lb_dmwuM
>
If the file path does not begin with the base_directory, the file absolutely must not be processed.
>
Using Relative Paths
Please take a moment to view this short video to refresh your memory about the difference between full (absolute) paths and relative paths: https://www.youtube.com/watch?v=EJ0xvY5wT5Q

>
Understanding how to use ../ as a means of navigating a file system will help you better understand directory traversal attacks and how to prevent them. Suppose your website URL is https://mysite.com.
>
You are working in a file whose full path is
https://mysite.com/shop/category1/singleproduct.php
And you would like to include a file whose full path is
https://mysite.com/js/functions.js
>
When you include this file, you could of course include it with the full path, but using a relative path is best. Every ../ moves you up a directory from where you currently are.
>
Suppose you are standing at singleproduct.php.



The first ../ will take you into the **category1** directory.
The next ../ will take you into the **shop** directory.
The next ../ will take you into the **base** directory for https://mysite.com .

Then you must go forward into the js directory before naming the file you want to include.
>
In this case, the relative path to include would be ··/··/··/js/functions.js

Conclusion & Takeaways

Conclusion & Takeaways

Good code is safe code. By taking basic precautions against common attacks, you can protect your website and its users from malicious actors. Forms can be weak points in terms of security because they allow users to enter and submit inputs. By restricting, validating and sanitizing user inputs your code can be made more robust. ALL user inputs should ALWAYS be sanitized before they are submitted.
>
Remember that cybersecurity is fluid. Attacks evolve as vulnerabilities emerge and web developers must implement new security practices and patches as they become available. A responsible web developer is proactive in learning about emerging threats so that their code can be maintained and made robust in the face of new attacks.
>
Attribution
- Image https://www.freepik.com/free-vector/characters-people-searching-through-files_3530103.htm
- Arbitrary File Read Video https://www.youtube.com/watch?v=Jg5lb_dmwuM
- Relative vs Absolute Path https://www.youtube.com/watch?v=ZQLpSOGOj8E

The OWASP® Foundation

The OWASP® Foundation

Goals

By the end of this case you will:
- Learn about the OWASP Foundation
- Join the OWASP community
- Familiarize yourself with the OWASP Top Ten security risks
- Understand how the OWASP Top Ten list is produced
>
Introduction
The Open Web Application Security Project® (OWASP) is the world's largest non-profit foundation concerned with software security. Their work seeks to improve software security through community-led open-source software projects. They have hundreds of chapters worldwide and provide valuable education and training conferences for professionals interested in developing their software security knowhow.

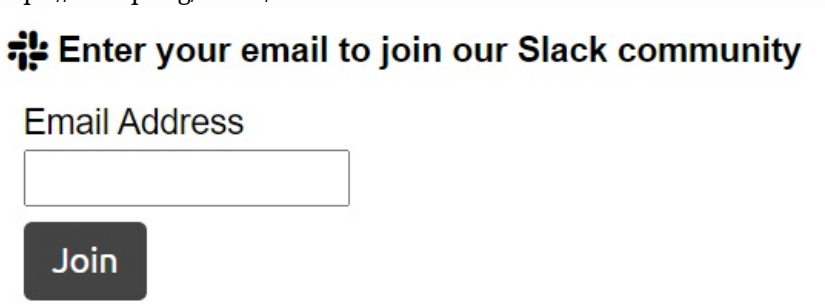
Image by rawpixel.com on Freepik
>
Business Context
Security is always a primary concern, and even if you are not inclined to attend software security conferences, OWASP is a valuable and credible source of security information. Familiarize yourself with their tools, resources, community and training opportunities.

About OWASP

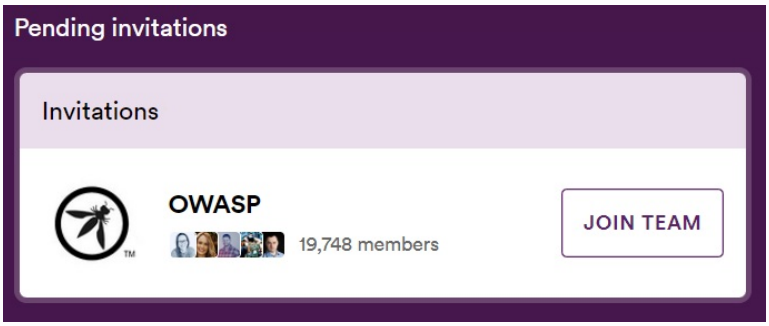
About OWASP

Here is a brief introductory video to OWASP
https://youtu.be/GJADjlBbv3Y
>
Activity: Join the OWASP community
To get a better feel for the OWASP community, we will join their Slack community.
If you do not already have a Slack account, visit https://slack.com/ to create one.

Now visit this page and join OWASP's Slack community.
https://owasp.org/about/

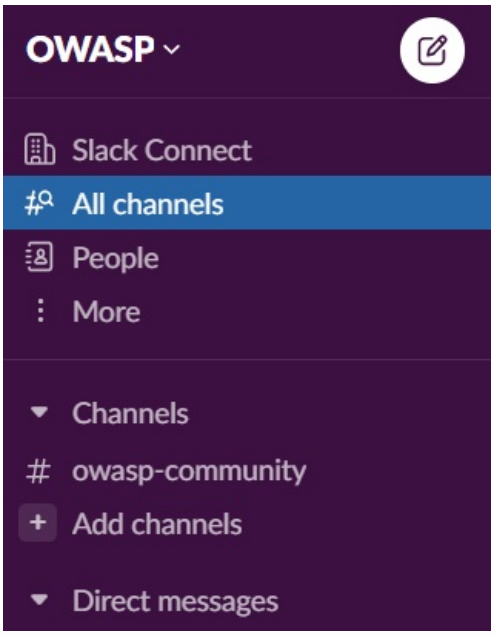


After you have entered your email to join, return to https://slack.com/ and you should see a pending invitation from OWASP. Click "JOIN TEAM".



pending invitation

Welcome to the OWASP community. You can browse different topics by clicking "All channels"



slack connect channels

Take a moment to look around and see if any of those channels are of particular interest to you. #Learning and #Developers are good places to start.

Major Security Risks

Major Security Risks

The OWASP Top Ten is a standard awareness document intended for developers. It highlights the top 10 security risks so that developers can apply focus to the most important/high risk areas.
>
Here is an introductory video about the OWASP Top Ten and how it can be used.
https://www.youtube.com/watch?v=hryt-rCLJUA
>
You can read more about the OWASP Top Ten on their website:
https://owasp.org/www-project-top-ten/
>
As you can see, insecure design and injection both feature on this list of top 10 concerns. Using the OWASP Top Ten to minimize security risk is an effective first step in securing the code you develop.

Conclusion & Takeaways

Conclusion & Takeaways

OWASP offers exciting and affordable opportunities to access software security knowledge, cultivate your professional expertise, network with other professionals and participate in an active and ethical like-minded community.
>
A security-first approach to web development is forward-thinking and increasingly the industry standard. The OWASP community is an excellent place to start taking this approach. Whether you consult their Slack channel or join a local chapter, it’s important to remember that you are not in this alone. You are part of a larger international community that seeks to make the web a safer place. Ask questions, make friends, and cultivate your security skills.
>
Attribution
- About the OWASP foundation https://youtu.be/GJADjlBbv3Y
- Slack https://slack.com
- To join OWASP Slack channel https://owasp.org/about/
- OWASP Top 10 (YouTube) https://www.youtube.com/watch?v=hryt-rCLJUA
- OWASP Top 10 (Website) https://owasp.org/www-project-top-ten

WordPress Security Part 1

WordPress Security

Goals

By the end of this case you will:
- Understand WordPress security risks
- Install the Wordfence Security plugin
- Familiarize yourself with WordFence settings and capabilities
- Perform a Wordfence security scan
>
Introduction
WordPress, as you know, is a website content management system that offers many advantages. It's also important to be mindful of the security risks that can emerge at various stages of development and how to mitigate them. The OWASP Top Ten Web Application Security Risks includes **Vulnerable and Outdated Components** which is of particular relevance to WordPress websites.

Image by kjpargeter on Freepik

>
Business Context
Approximately 63% of websites are built in WordPress making it very likely that you will work in WordPress as a developer. If you are building the website from the ground up, you will be able to include basic security measures at the outset. If, however, the website is already in place, it will be important to assess the security measures in place and to scan for vulnerabilities in order to take the steps necessary to secure the website's existing vulnerabilities.
>
WordPress Vulnerabilities
WordPress websites are built using themes and plugins that can present malicious actors with vulnerable points of entry. When new versions that include security patches are released you must update WordPress/theme/plugin versions to ensure that your website is not exposed to attacks that could have been prevented.
>
Installing too many plugins on a website exposes that website to an increased number of security risks. It is recommended that you limit the number of plugins your website requires and that you delete plugins and themes that you are not using. With fewer plugins, your website will be more secure, will load more quickly and will require less maintenance.
>
Take a quick look at this list of plugin vulnerabilities to understand the scope of the problem. https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins
>
Defending WordPress Websites
Let's make your personal WordPress website more secure by installing the Wordfence Security plugin.
>
Step 1: If you can remember from **Module 8**, we installed LocalWP to set up a local WordPress environment on our computers. Open the application **LocalWP** and go to your Admin settings.

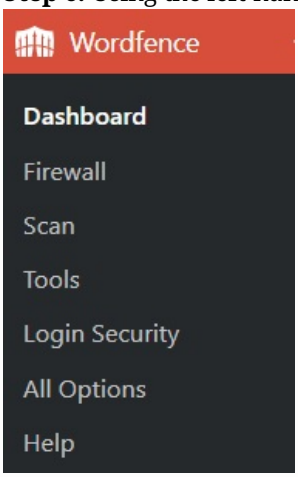
Tip: It is crucial to ensure that we exclusively use LocalWP for installing plugins, whether they are free or paid, rather than installing them directly on wordpress.com.

Step 2: Using the left-hand menu, navigate to **Plugins → Add New**
>
Step 3: Use the search bar in the upper left-hand corner to search for Wordfence
>
Step 4: Click **Install Now** button on the Wordfence Security plugin

Step 5: Once it is installed, click the **Activate** button.

>

Step 6: Using the left-hand menu, navigate to Wordfence Dashboard

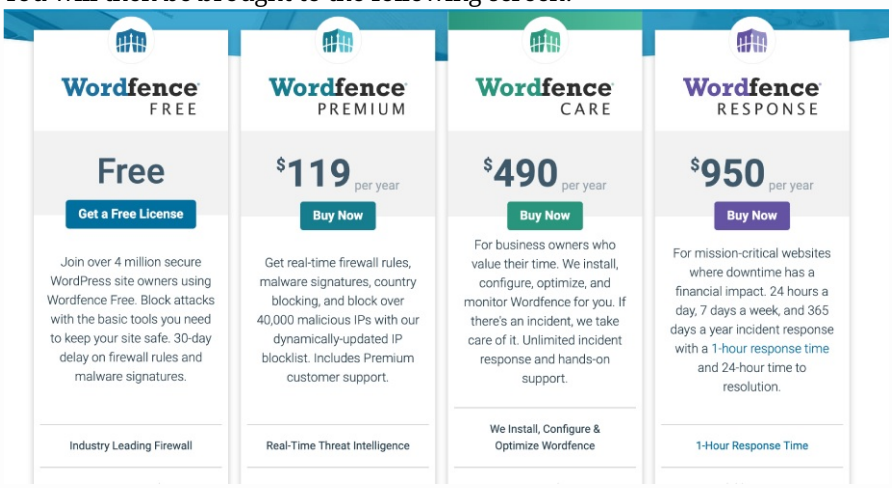


It may ask you for your email address. This is the email address that will receive security notifications and status updates. Ensure that you check this email regularly.

Here is the screenshot you will see:

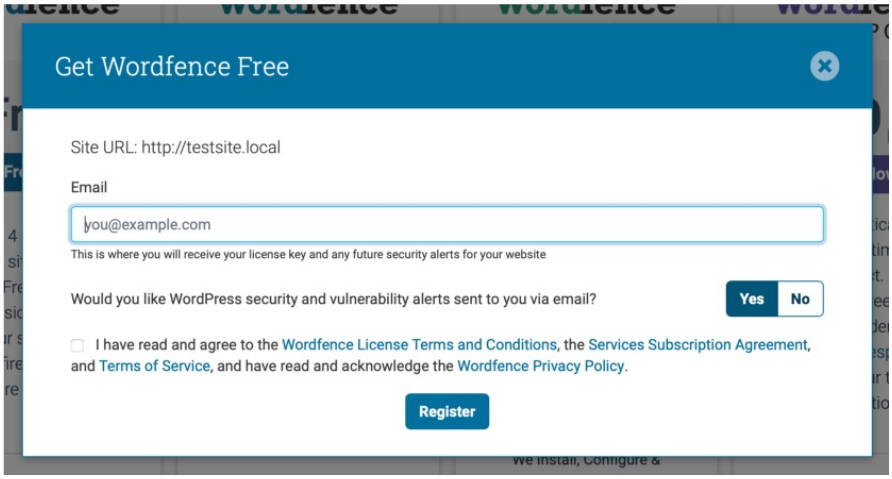
Click ‘Get your Wordfence license’

You will then be brought to the following screen:



Under ‘Free’ click ‘Get a Free License’

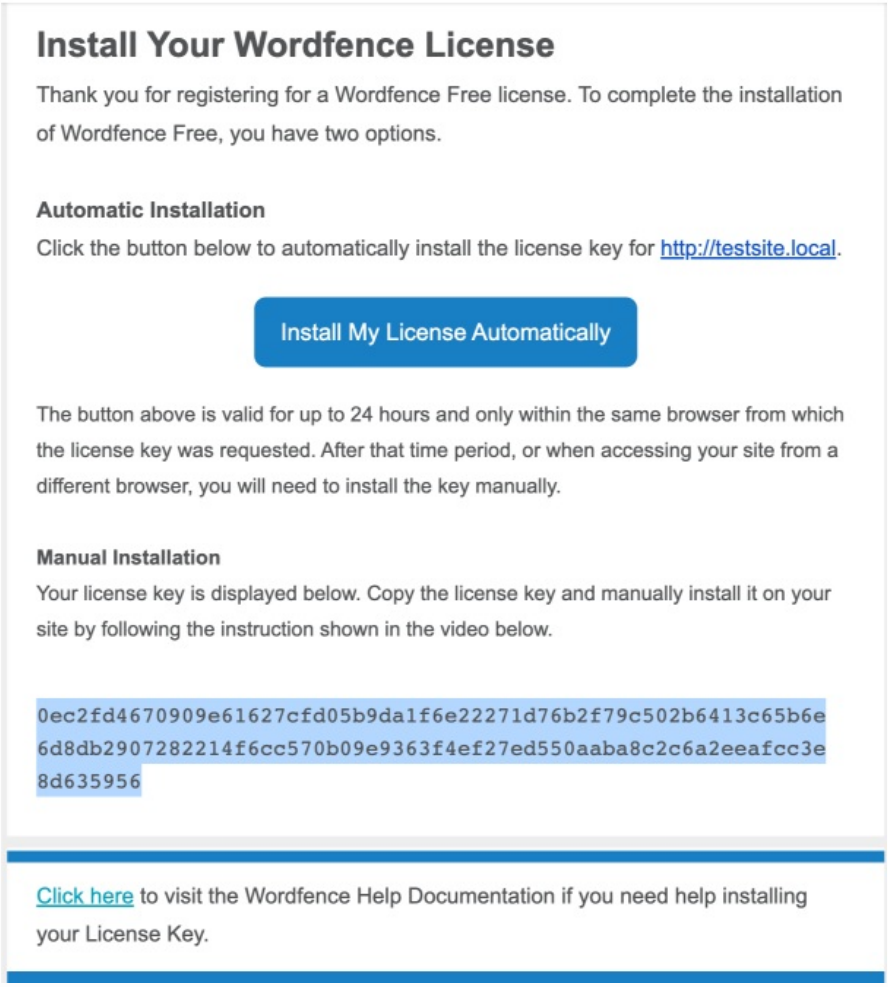
Then you will see the following screen, enter your email and press Yes for ‘Would you like to receive emails’ and check off the box for terms and conditions and click Register



>

Your license key is going to be emailed to you, and you will receive the

following email.



You then have to copy the long number below and go back to your Wordpress where you will be greeted with the same popup as before:

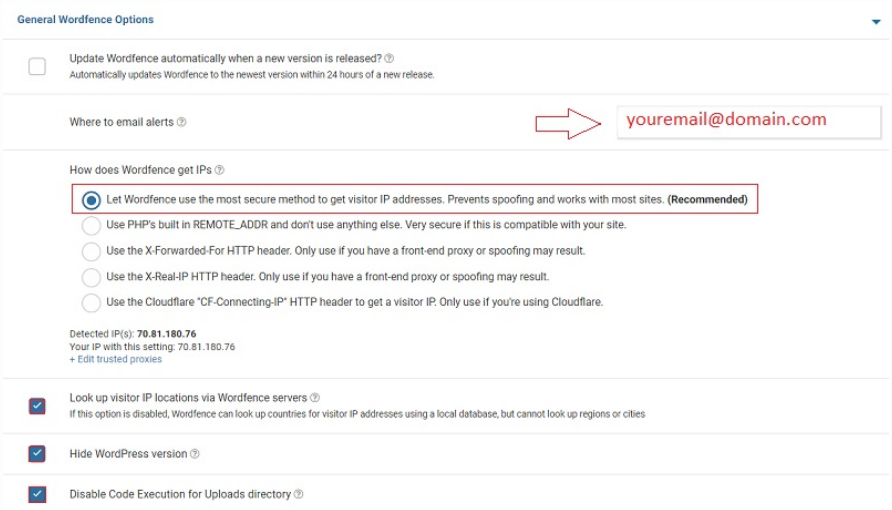
This time click ‘Install an existing license’ and once you click that, all you need to do is enter your email and the long license key that you copied, accept the terms and conditions and proceed. You will now have installed your free license. Click ‘Go to Dashboard’.

The Wordfence dashboard will give you an overview of your website security, and it is on this page that you will see (in the future) any security notifications or vulnerabilities that may have been identified in a recent

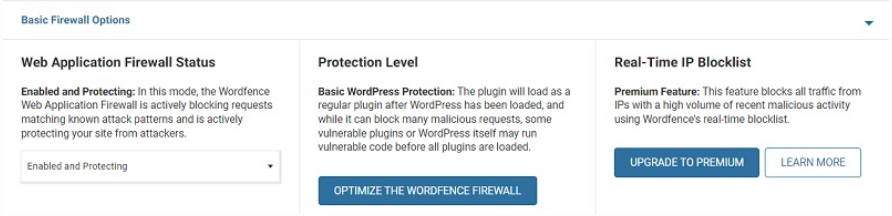
scan.

WordPress Security Part 2

Step 7: Navigate to **All Options** in the Wordfence sub-menu
>
Step 8: This is where we will configure your Wordfence plugin. There are premium options that can be accessed for a subscription fee, but these will not be discussed at this time.

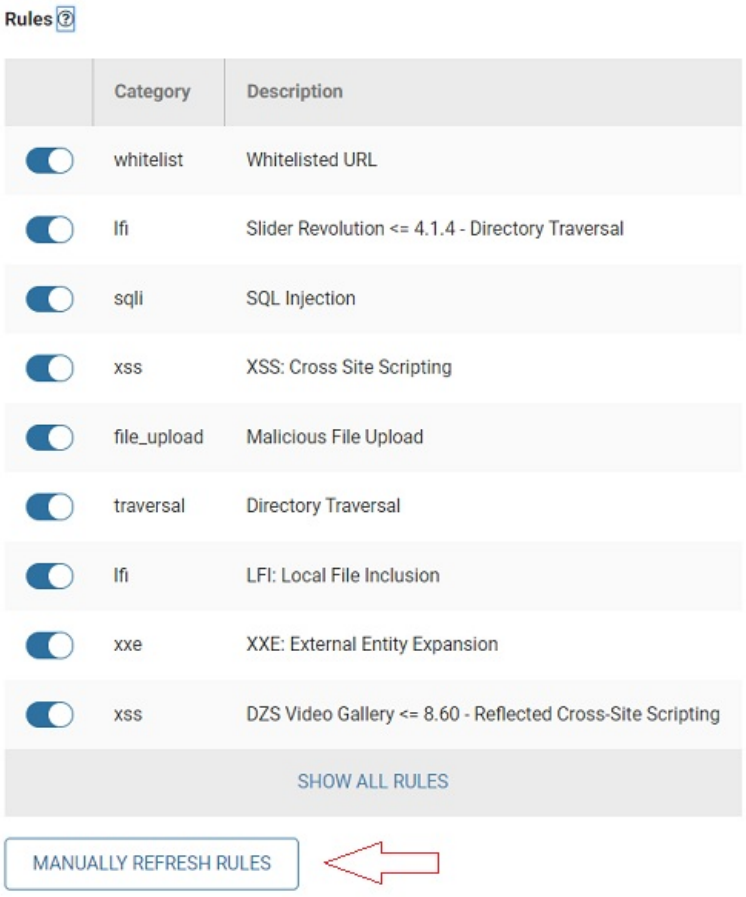


>
- If you haven't already, be sure to enter your email address to receive security alerts.
- Always select the **Recommended** settings if you are unsure.
- Hide the WordPress version from attackers. It's none of their business
- It is wise to disable code execution in the uploads directory.
- Scroll down to Email Alert Preferences and decide if there are alerts you would prefer not to receive.
- Below that you can also select how frequently you would like to receive Activity Reports.
- Scroll down to **Basic Firewall Options**. A firewall acts as a protective barrier against attackers. The firewall status may be set to learning mode and this is ok to start, but eventually it should be set to **Enabled and Protecting**.
- If you can, click **Optimize the Wordfence Firewall**.

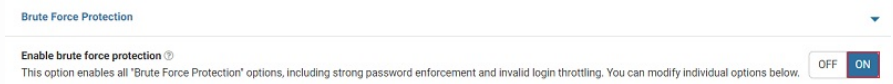


- Click on **Advanced Firewall Options** and then scroll down to **Rules**. These Wordfence rules guard against some common attacks. You may

notice that some of the attack categories are familiar to you ex. XSS and Traversal. All of these rules should be activated, though you do have the option to turn them off individually. If you are worried that your rules may be out of date, you also have the option to **Manually refresh rules**.



- Scroll down to **Brute Force Protection**.



This option should be on. Below that you can decide how strict your login rules are. Different websites will require different settings here. If many users need to login all of the time, you may not want to be too strict and lock valid users out. Security is important, but so is the user experience. For example, if you check the option **Immediately lock out invalid usernames**, valid users who forgot their account details may get blocked from the public website (not good).

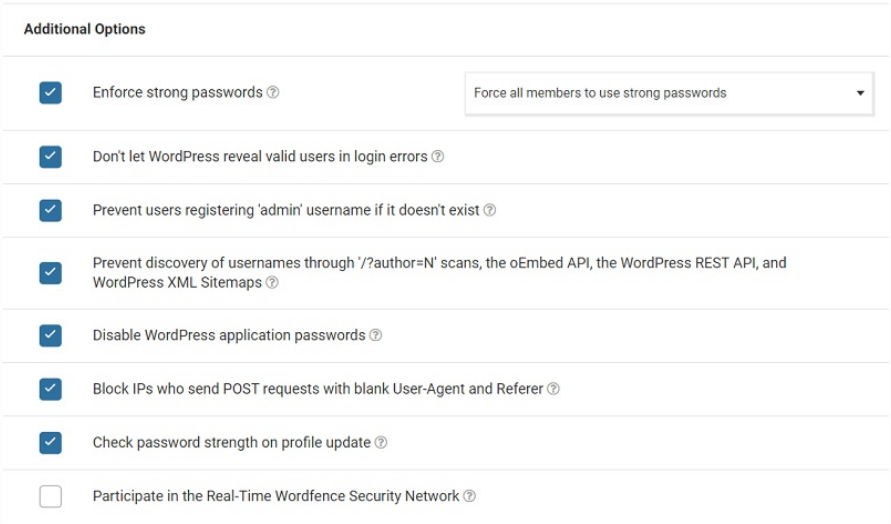
>

You should absolutely check the option: **Prevent the use of passwords leaked in data breaches**.

>

- Scroll down to **Additional Options**

You should **Enforce strong passwords** for all members. It is safe to select all or most of these additional options.



Step 9: Remember to save your changes.

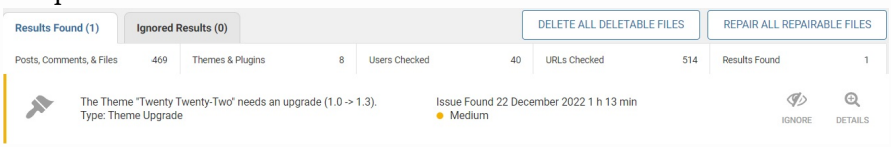
Scanning WordPress for Vulnerabilities

Scanning WordPress for Vulnerabilities

Now that we have configured Wordfence, we can also use it to scan our website files/themes/plugins for known vulnerabilities.
>
Using the left-hand menu, navigate to **Scan** in the Wordfence sub-menu.
>
From this page you can click the **Start New Scan** button to begin scanning your website.

This may take some time and it's important to give the scan time to run to completion. It is worth noting that websites do slow down while they are being scanned. Since we do not want to have a negative impact on user experience, security scans are best performed during low traffic periods.
>
Once the scan is complete, you can scroll down to see **Results Found**.
>

It is essential that regular security scans are performed on any website. New vulnerabilities will arise over time. Regular security scans allow you to identify and patch the vulnerabilities so that your website is not exposed to attack.
>
Note that you should always have a backup of your website ready to restore before attempting to update plugins or themes. Occasionally, updates will break the front end of the website and if this cannot be remedied promptly, you may need to restore your backup.
>
Sample Answer:



>

Git Reviews

Git Reviews

Git is a free version control system that is the most widely used version control system in the world and is considered the industry standard for developers. Version control refers to tracking and managing code changes. Version control allows teams to review code before it is live, and to restore previous versions if something goes wrong with the live version. In the context of performing WordPress version and plugin security updates, Git's version control allows you to undo and analyze any updates that would cause a display or compatibility problem.

Major Benefits of using Git
- Access to a complete change history of every file.
- Branching (new code) and merging (combine branches) capability.
- Ability to trace back changes, review and analyze them

Getting started with Git
To get started, follow the instructions on this page to install Git for Windows. https://git-scm.com/download/win

It is recommended that you accept the default (recommended) settings as you click "Next" through the installation. As we saw in the video, once you have installed Git, you can write your first commands to configure your username and email address.

```
$ git config --global user.name "Dana Devops"
$ git config --global user.email "danadevops@gmail.com"
```

Now you are ready to create your first Git repository. Watch this video to see how Git is set up. The start of the video shows the steps you just completed. The second half of the video will help you create your first repository, your first file and to do your first commit. Follow along in your Git terminal to get hands on Git experience. https://git-scm.com/video/get-going
>
Getting to know Git
As so many developer job openings list knowledge of Git as a required or preferred skill, taking the time to learn Git will strengthen your application.
>

Further reading to learn Git (documentation / instruction book / videos):
https://git-scm.com/doc
>
Once you have worked through the instruction book and are more familiar with Git commands, you may want to download this Git “cheat sheet” so that you don’t have to look up every command as you go:
https://www.atlassian.com/git/tutorials/atlassian-git-cheatsheet
>
Best Practices for using Git
- Commit often. Every time you “commit”, you are capturing a snapshot of the code base. This will be a version that you could return to if needed. It is better to commit too often rather than not often enough. A group of commits can always be combined to simplify the development history later on.
- When you commit you can and should leave a detailed log message explaining why you are making this commit and what is contained within it.
- Make sure to git pull (fetch) the global copy so you are working with the most recent version of the code.
- Use the staging area to collect/review a group of edits before writing them to a commit.

Conclusion & Takeaways

Conclusion & Takeaways

With continuously evolving cyber security threats, it is essential to monitor websites for vulnerabilities and resolve them as they occur. Prioritize WordPress version updates and Plugin version updates as outdated versions pose security risks. The Wordfence security plugin, and other plugins like it, can be configured to improve your website security and to identify vulnerabilities. Limiting the number of plugins that your site requires and ensuring that only secure versions of these plugins are used, will go a long way toward improving your site's performance and security.
>
Cybersecurity is a rapidly growing field. Security scanning is often a web developer's responsibility, so knowing how to do this is important. Learning about cPanel, file and folder permissions, or other security tools can make you more marketable. Sign up for security newsletters (wordfence has one) to learn how security breaches are investigated and uncovered. One employer has stated "If I'm hiring a web designer and they have an interest in security, that appeals to me."
>
Beware! Updates can (occasionally) break the front end of your website so proceed with caution. It is good practice to make updates in the development environment rather than in production when possible. It is also wise to have a website backup on hand so that a broken site can be restored promptly when there is a problem following a plugin update.
>
Attribution
- Image https://www.freepik.com/free-photo/3d-internet-secuirty-badge_38007814.htm
- Vulnerable and Outdated Components - OWASP Top Ten Web Application Security Risks https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
- Further reading re: WordPress Security https://developer.wordpress.org/apis/security/
- Further reading re: Wordpress Sanitization https://developer.wordpress.org/apis/security/sanitizing/
- WordPress plugin vulnerabilities https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins
- WordFence Security (Free version) https://www.wordfence.com/products/wordfence-free/
- Downloading Git for Window https://git-scm.com/download/win
- Video - Git basics episode 3 https://git-scm.com/video/get-going

- Git Documentation https://git-scm.com/doc
- Git cheat sheet https://www.atlassian.com/git/tutorials/atlassian-git-cheatsheet

Agile & Scrum

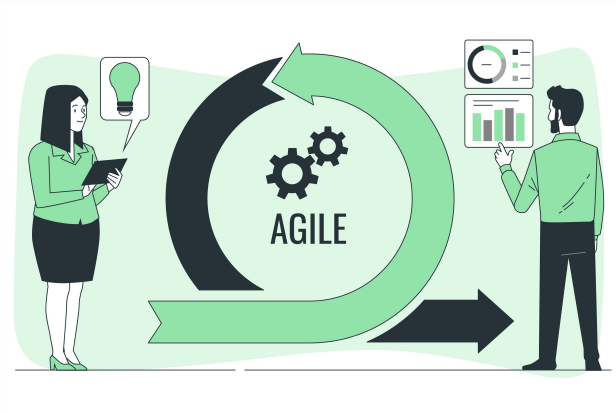
Goals

By the end of this lesson, you should:
- Have a basic understanding of Agile and Scrum principles and methodologies
- Be familiar with the importance and benefits of Agile and Scrum in the software development process
>
Introduction

When working as part of a software development team, efficient collaboration and project management can often be challenging. The Agile and Scrum methodologies have become vital tools for addressing these challenges, with their focus on enhancing efficiency, adaptability, and stakeholder satisfaction. This lesson will provide you with a basic overview of Agile and Scrum, as well as their key principles.

Overview of Agile

What is Agile?



Agile is a paradigm in project management based on the Agile Manifesto, written in 2001 by a group of seventeen software professionals who met to discuss the philosophy behind lightweight software development. The Manifesto outlines **4 key values** and **12 principles**. These values and principles form the basis of Agile and guide the practices and techniques in Agile methodologies. We'll explore the key values and principles more shortly.

Agile, in a nutshell, is a response to the limitations of the traditional Waterfall model for project management and represents a monumental shift in the approach to software development. The Waterfall model was linear and required detailed planning and documentation, which often led to longer development cycles and difficulty in accommodating changes. Agile, with its iterative and incremental approach, presents a great solution to these issues.

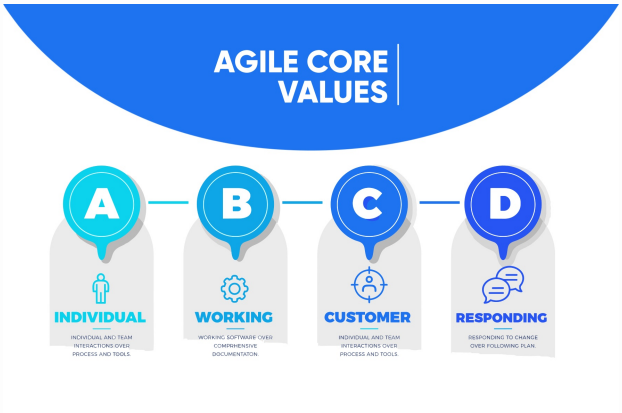
While the principles and values of Agile are constant, within the Agile paradigm there are several methodologies or frameworks that teams can use to implement Agile. In this lesson we will focus on **Scrum**, which is one of the most popular implementations of Agile in software development.

Agile Values and Principles

As mentioned earlier, the Agile Manifesto (the seminal work that established Agile as a philosophy and methodology for product development), sets out **4 key values** and **12 guiding principles**. Let's now

explore each of these values and principles to better understand what Agile is.

4 Key Values:



1. **Individuals and Interactions over Processes and Tools**: Agile places a higher value on individuals and their interactions. While processes and tools are important, they should serve the people doing the work, not the other way around.
2. **Working Software over Comprehensive Documentation**: In traditional methodologies, large amounts of time are spent creating detailed documentation. Agile, however, places emphasis on delivering working software. That's not to say documentation isn't important in Agile; it's about creating documentation that truly delivers value.
3. **Customer Collaboration over Contract Negotiation**: Rather than negotiating terms and sticking strictly to them, Agile encourages continuous customer or stakeholder involvement. The idea is to work with the customer throughout the development process to understand their needs and adapt the product accordingly.
4. **Responding to Change over Following a Plan**: In Agile, change is not only expected but also welcomed, even late in development. Agile teams are ready to respond to change in order to provide the customer with the best possible product. While having a plan is important, the ability to adapt to changes is viewed as more crucial.

12 Guiding Principles:

1. *Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.*
2. *Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.*

3. *Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.*
4. *Business people and developers must work together daily throughout the project.*
5. *Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.*
6. *The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.*
7. *Working software is the primary measure of progress.*
8. *Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.*
9. *Continuous attention to technical excellence and good design enhances agility.*
10. *Simplicity–the art of maximizing the amount of work not done–is essential.*
11. *The best architectures, requirements, and designs emerge from self-organizing teams.*
12. *At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.*

Overview of Scrum

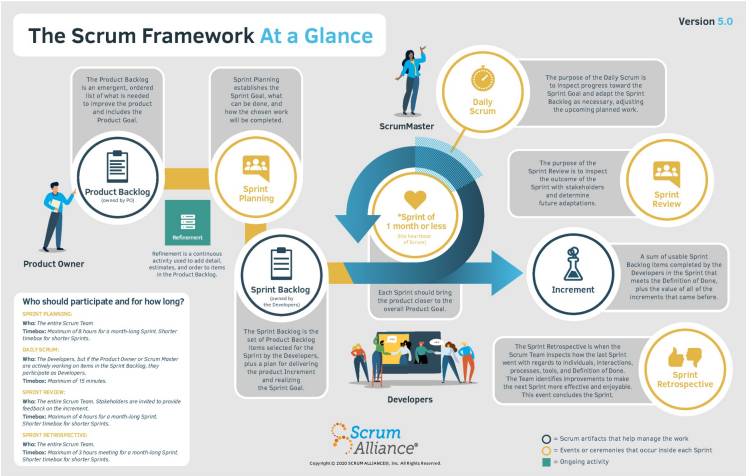
What is Scrum?

Scrum, named after a formation in rugby where team members act together to get the ball, is a lightweight yet powerful framework for complex product development. It doesn't provide detailed instructions for every scenario but offers a set of rules, roles, events, and artifacts for managing work. Scrum embraces the Agile principles of flexibility, speed, customer collaboration, and continuous improvement.

Scrum Principles

Scrum operates on six key principles:

1. **Empirical Process Control**: Scrum relies on evidence-based decision-making where progress is based on observed results rather than predictions.
2. **Self-organization**: Teams are given the autonomy to manage and organize their work, leveraging the expertise of its members.
3. **Collaboration**: All stakeholders, including team members and customers, work closely together throughout the development process.
4. **Value-based prioritization**: Features and tasks are prioritized based on their value to the customer or project outcome.
5. **Time-boxing**: Work is structured into fixed-length intervals (sprints) with specific goals, ensuring timely delivery and feedback.
6. **Iterative development**: The product is developed and improved in small increments, allowing for regular feedback and adjustments.



Components of Scrum

Scrum Artifacts

Scrum Artifacts are tools that provide information and give insights into the product and the project. These include the **Product Backlog**, a prioritized list of desired product features or changes; the **Sprint Backlog**, a subset of the Product Backlog that the team commits to deliver during a Sprint; and the **Increment**, the sum of all Product Backlog items completed during a Sprint and the value of the increments of all previous Sprints. These artifacts help teams plan and track their work, assess their progress, and adapt their plans as needed.

Scrum Roles

There are three main roles in Scrum: the Product Owner, the Scrum Master, and the Development Team.

The **Product Owner** is the key stakeholder who has a vision of what they wish to build and conveys that vision to the team. The **Scrum Master** facilitates the Scrum process, removes impediments, and helps the team perform at their highest level. The **Development Team** is the group of professionals who do the work of delivering a potentially releasable product Increment at the end of each Sprint.

Scrum Events

Scrum Ceremonies, also known as *events*, provide the framework for the team to get work done in a structured manner, facilitate communication, and reduce unnecessary meetings.

These include **Sprint Planning** (where the team determines the product backlog items they will work on during the sprint and discusses the plan for delivering the product increment), **Daily Scrum** (a quick meeting for the team to sync up and plan their day's work), **Sprint Review** (where the team, stakeholders, and Product Owner review what was accomplished during the sprint and update the backlog), and **Sprint Retrospective** (where the team reflects on their performance during the sprint and discusses ways to improve for the next sprint).

User Stories

User Stories are a powerful tool in Agile and Scrum, serving as a simple description of a product feature from the end-user's perspective.

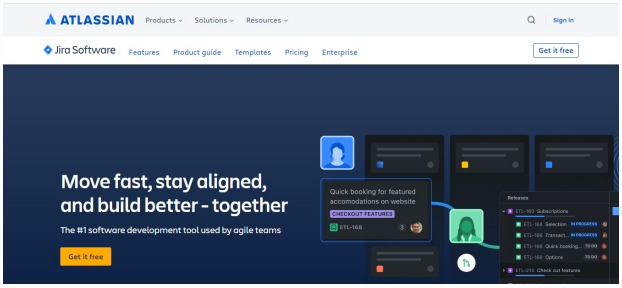
Effective User Stories should conform to the INVEST criteria: **I**ndependent (can be developed in any sequence), **N**egotiable (details can be worked out over time), **V**aluable (provides value to the customer), **E**stimable (enough information is provided to estimate size), **S**mall (can be completed within one sprint), and **T**estable (clear acceptance criteria are defined).

A User Story might be something like: "As a user, I want a search function on the homepage so that I can easily find information on the website." The corresponding acceptance criteria might include: "Given I am on the homepage, when I enter 'FAQ' into the search bar and hit enter, then the FAQ page should appear in the search results."

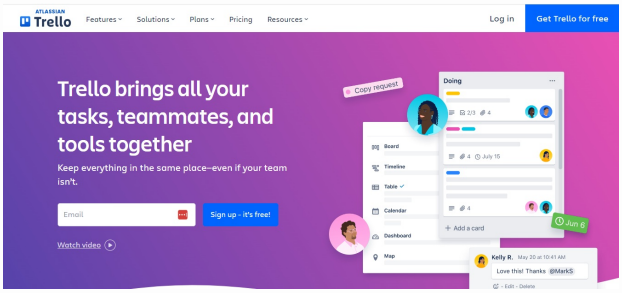
Common Software Tools

Tools can play a significant role in implementing Agile and Scrum effectively. Jira, Trello, and Asana are some popular ones. **Jira**, developed by Atlassian, is an issue tracking product that allows bugs tracking and agile project management. It can manage the entire life cycle of a task, from requirement to deployment. **Trello**, with its Kanban-style boards, lists, and cards, is great for managing and visualizing project tasks. **Asana** allows for task assignments, commenting, and tracking, making it a useful tool for managing work, especially in a remote setting. These tools can help teams collaborate, track progress, manage changes, and stay aligned with their goals.

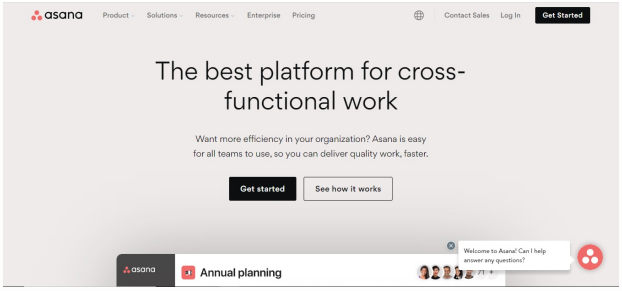
JIRA



TRELLO



ASANA


asana
Product
Solutions
Resources
Enterprise
Pricing
Contact Sales
Log In
Get Started
The best platform for cross-functional work
Want more efficiency in your organization? Asana is easy for all teams to use, so you can deliver quality work, faster.
Get started
See how it works
asana
Annual planning
Welcome to Asana! Can I help answer any questions?

Certifications

Becoming certified can enhance your understanding of Agile and Scrum and boost your credibility in the field. There are several certification programs available:

Certified ScrumMaster (CSM): Offered by the Scrum Alliance, the CSM certification validates your understanding of Scrum principles and your skill in applying Scrum in projects.

Professional Scrum Master (PSM): Offered by Scrum.org, the PSM certification comes in three levels (I, II, and III), each with an increasing depth of knowledge and expertise in Scrum.

PMI Agile Certified Practitioner (PMI-ACP): Offered by the Project Management Institute (PMI), the PMI-ACP certification recognizes knowledge of Agile principles and skill with various Agile methodologies.

Conclusion & Takeaways

Conclusion & Takeaways

In this lesson, we covered the roots of Agile and Scrum, their principles, artifacts, roles, and events, some real-world applications, and common tools used by Agile teams. Agile and Scrum are more than just methodologies - they represent a mindset; as we touched on, they are a way of approaching work that values individuals and interactions, customer collaboration, and responsiveness to change. As you continue your journey in software development, it's crucial to keep learning, exploring and adapting...

This is the [Agile] Way.

Attribution

- Agile Manifesto https://agilemanifesto.org/
- The Scrum Framework at a glance https://www.scrumalliance.org/about-scrum#!section2
- Agile agility nimble quick fast volant concept Free Photo. (2021, August 11). Freepik. https://www.freepik.com/free-photo/agile-agility-nimble-quick-fast-volant-concept_17057425.htm
- Agile Alliance. (2023a, April 15). Agile Manifesto for Software Development | Agile Alliance. Agile Alliance |. https://www.agilealliance.org/agile101/the-agile-manifesto/
- Agile Alliance. (2023b, July 29). Agile Essentials | Agile Alliance. Agile Alliance |. https://www.agilealliance.org/agile-essentials/
- Agile method concept illustration Free Vector. (2022, June 29). Freepik. https://www.freepik.com/free-vector/agile-method-concept-illustration_28902469.htm
- Agile principles. (2023, January 6). https://www.productplan.com/glossary/agile-principles/
- Arun, R. (2023). What is Agile: Understanding Agile Methodology and Principles. Simplilearn.com. https://www.simplilearn.com/tutorials/agile-scrum-tutorial/what-is-agile
- Atlassian. (n.d.). What is Agile? | Atlassian. https://www.atlassian.com/agile
- Cprime Inc. (2023, April 17). What is Agile? - What is Scrum? - Agile FAQ's | Cprime. Cprime. https://www.cprime.com/resources/what-is-agile-what-is-scrum/
- Dark mode concept illustration Free Vector. (2020, December 11). Freepik. https://www.freepik.com/free-vector/dark-mode-concept-illustration_11608452.htm
- Drapkin, A. (2023). The key principles of Scrum in Project Management. Tech.co. https://tech.co/project-management-software/key-principles-scrum
- Gradient blue agile core values infographic Free Vector. (2020, June 20). Freepik. https://www.freepik.com/free-vector/gradient-blue-agile-core-values-infographic_8848307.htm
- McCormack, C. (2023). Introduction to agile. monday.com Blog. https://monday.com/blog/project-management/introduction-to-agile/
- Ops, D. (2023, April 15). What does INVEST Stand For? | Agile Alliance. Agile Alliance |. https://www.agilealliance.org/glossary/invest/
- Scrum infographic Free Vector. (2020, June 17). Freepik. https://www.freepik.com/free-vector/scrum-infographic_8806106.htm

Client / Stakeholder Management

Client / Stakeholder Management

Goals

By the end of this case you will:
- Understand why client/stakeholder management is one of the most important things a professional web developer does
- Familiarize yourself with the concept of scope creep
- Recognize that perception is reality
>
Introduction
If your work puts you in direct contact with your client, it will be necessary to manage that client's expectations. A well-managed client is a happy client, and you too will reap the benefits of having happy clients. Regular and targeted communication with your client can help build trust which in turn facilitates the client/stakeholder management task.

Helping Your Client Feel Heard

Helping Your Client Feel Heard

The start of your relationship with a given client often consists of a meeting or a phone call where the client will talk to you about what they are looking for. Whether they are starting a new project or building on an existing one, this stage of the relationship sets the tone for what follows. This is your opportunity to show the customer that you are actively listening to their needs and responding in kind.
>
Remember that your client is not a developer. They may say things that are not technically correct, but this is not the time to correct them. In the first interaction, you are listening to their story to understand their long-term vision. It's ok to take notes, but do not interrupt them. Make eye contact. Nod and smile encouragingly. Save your questions for the end. Detailed specifications will be produced only after you have a solid understanding of what will make this client's heart sing.
>
Managing Expectations and Building Trust
Managing client expectations starts with setting clear goals. Suppose your client has requested a functionality add-on to their e-commerce website. You estimate that you will need 2 weeks to deliver the add-on. Telling your customer that you will be able to launch the new functionality in two weeks, does not leave you any wiggle room for unexpected hurdles that can and do arise. If the customer expects a 2 week delivery timeline, and you run into trouble and miss the deadline, the customer will not be happy and they will not trust your ability to estimate deliverables.
>
In this case, it would have been better to tell the customer that you will be ready to begin testing the new functionality in 2 weeks, and anticipate launching in 3 weeks time. This way, you have wiggle room for incidentals, you can deliver in line with the customer's expectations, and the customer can trust in your ability to estimate deliverables.
>
Similarly, you want to be transparent about your fee structure. Most clients would rather know what to expect upfront. Zero clients want to be surprised with unexpected invoices.
>
The same idea applies to your availability. If you are not available for work on the weekends, that's allowed, but you have to be clear about that with your customer. Customers need to know when they can call you to collaborate on the project. If they expect you are working, and then can't reach you, they will perceive you to be slacking off.

Perception is Reality

Perception is Reality

When you call or email your customer to give them an update on their project, they perceive you as working hard. When you fail to call or email your customer to give them an update, they perceive you as not working at all, even if you are working harder than you ever have in your entire life. This is what we mean by perception is reality. You have to manage your client's perception of you and of the work you are doing for them.
>
If you have included many "extras" on the project, but you never told your client about these "extras", your client is unable to perceive and therefore unable to appreciate the extra effort that you made. Communicating is not bragging. Tell your customer explicitly what you have done for them using simple (non-technical) language they can understand. Only then can they perceive how hard you are working for them, and this too will build trust in the relationship.
>
Scope Creep
Scope creep occurs when clients request work that is not included within the scope of the initial project. This might occur, for example, if you are integrating a new homepage layout and the client asks you to fix a few typos on their About-Us page "while you're in there". If the request is very small, you might use your discretion to decide whether or not to fulfill the request, but small "extras" can add up, and before you know it, you may have crept well beyond the initial project's scope.
>
This is problematic because you are being asked to do more work without additional financial compensation. Furthermore, the customer's expectations regarding launch timelines will not change even though they are causing delays with additional requests. That means that if you miss deadlines, their trust in your capacity is negatively impacted.
>
It is best to develop and sign detailed specifications regarding the project scope up front and to make clear that while you are overjoyed to receive any additional requests, the specifications for those requests will be drawn up as part of a separate mandate with a revised timeline if applicable. This way the customer's expectations are adjusted and scope creep is limited.
>
Further reading : https://www.projectmanager.com/blog/5-ways-to-avoid-scope-creep

Conclusion

Conclusion

Effective Client / Stakeholder management is an important part of forming and maintaining successful customer relationships. Making sure your customer feels heard is where trust begins. Limiting scope creep using clearly written contractual specifications helps to manage client expectations and end of cycle satisfaction. Remember that perception is reality and that regular communications foster trust and forge rapport. Satisfied customers are more easily retained for future business, and they are more likely to provide referrals for new business.

Cross-Browser and Device Testing

Cross-Browser and Device Testing

Goals

By the end of this case you will:
- Know what cross-browser and device testing refers to
- Understand why no project is complete without this step
- Learn to use “inspect” in Chrome to test different screen sizes.
>
Introduction
When a website is nearly ready to go live, the final step is cross-browser testing and device testing. In this step, you must try to use the website (as a target user might) on different browsers and different devices. Typically browsers tested include Chrome and Safari, but depending on your customer, you may also need to test on Microsoft Edge and FireFox. Testing for different devices means desktop screens, laptops, tablets and different cell phones. Don’t worry if you don’t have all those devices, we will use a Chrome feature to test different screen sizes. Your goal is for the website to display and function seamlessly regardless of screen size, and no matter which browser is used.

Defining the scope of your testing

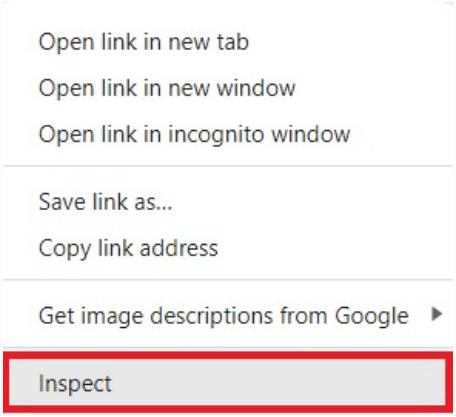
Defining the scope of your testing

It is important to include which browsers and devices your website will support in the contracted project specifications. Without this detail, your customer may insist the code be made compatible with versions of Explorer, for example, which are no longer supported.
>
Responsive Design Includes Cell Phones
Even if your website is intended to be used primarily on desktops, the design must nevertheless be responsive for optimal display across all screen sizes, including cell phones. As of 2021, 85% of Americans owned a smartphone, up from just 35% in 2011. Knowing this, it is not surprising that the field of Web Development has adopted a mobile-first mindset. Google search results also prioritize responsive websites in their search results, meaning your website will be penalized in search ranking if it is not mobile-friendly.

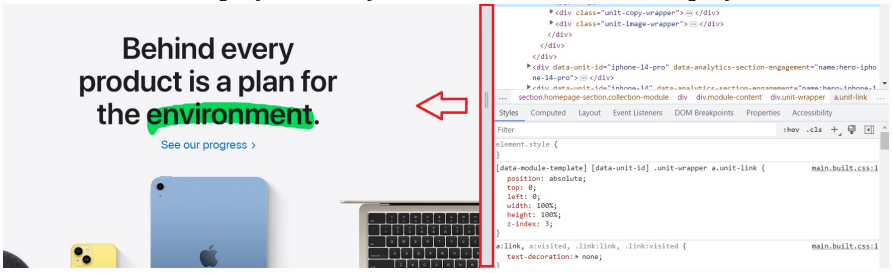
Using “INSPECT” in Chrome

Using “INSPECT” in Chrome

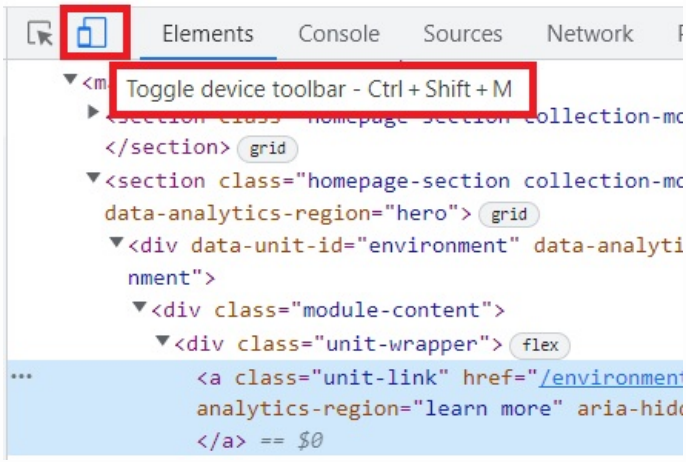
One way to test website display on different screen sizes is to use the “Inspect” feature in Chrome. Open https://www.apple.com/ in a new tab. Right click on an element of the page and select INSPECT from the menu.



As you can see, this opens a split screen with the website’s HTML on the right hand side. At the (vertical) center of the screen there is a bar that you can drag left or right to make the website view wider or more narrow. Your website should display correctly, no matter what size is displayed.



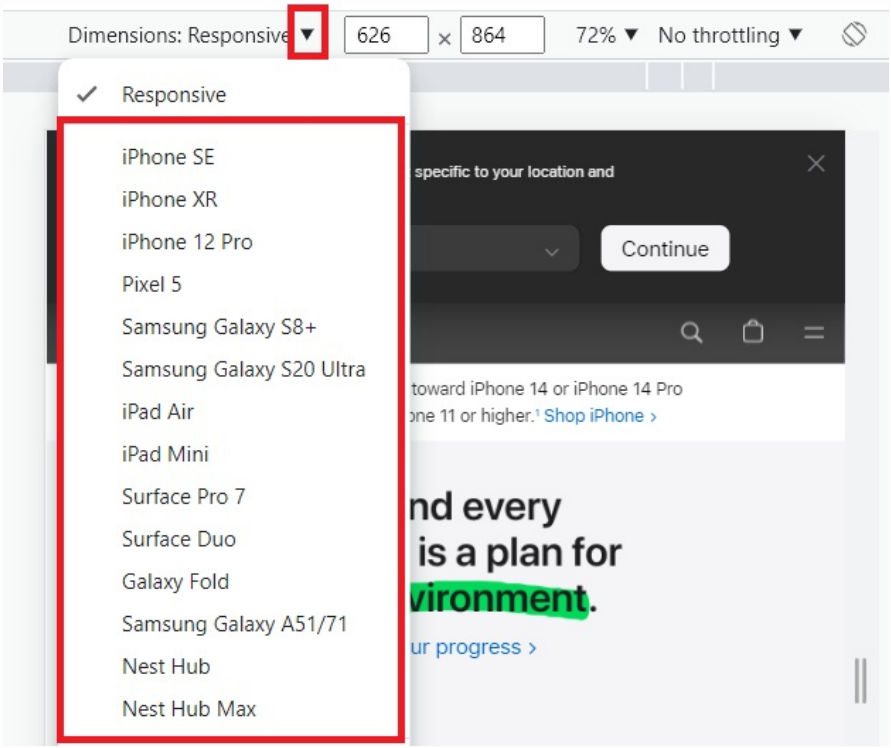
You can also use INSPECT to test different devices. On the right hand side of the screen you can toggle the device toolbar.



This will slightly modify the display on the left hand side.

>

Click on the arrow next to Dimensions: Responsive to select the device for testing.



Modify the website CSS as needed to ensure seamless display across devices.

Conclusion

Conclusion

Cross-browser and device testing is the final stage of producing a product you can be proud of. When this stage is omitted or rushed you can trust that your client will find display and functionality problems post-launch. That outcome dramatically reduces customer satisfaction and should be avoided at all costs. Instead, test your site on different browsers and devices until you are sure there are no bugs. Leave your client overjoyed with their flawless new website so that they remain your client for future business and sing your praises to everyone with ears.
>
Attribution
- https://www.pewresearch.org/internet/fact-sheet/mobile/
- https://www.apple.com/

Contact Forms in WordPress

Contact Forms in WordPress

Goals

By the end of this case you will:
- Install the Contact Form 7 plugin for WordPress
- Create a simple contact form for your website
- Protect your website by integrating Google reCaptcha V3 on your form
>
Introduction
Creating contact forms in WordPress is relatively straight-forward. There are a variety of (free and paid) form builder plugins available and your choice of plugin will depend on what it is you need your form to do.
>
Select a plugin that receives regular updates and that is highly rated. Plugins that have not received any updates in two years are considered abandoned. It is not recommended that you use abandoned plugins.

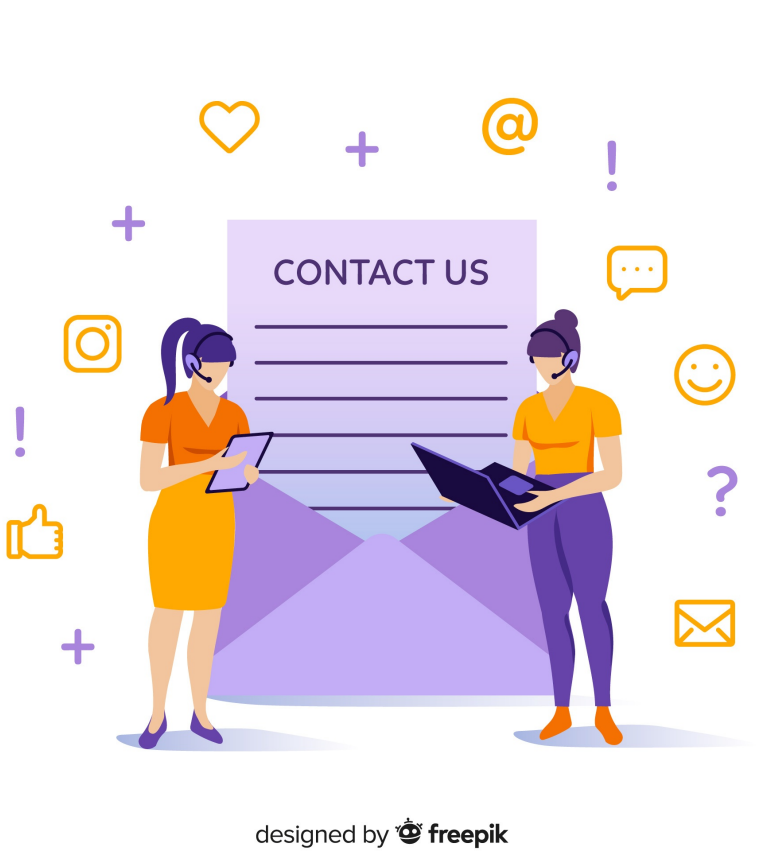


Image by Freepik

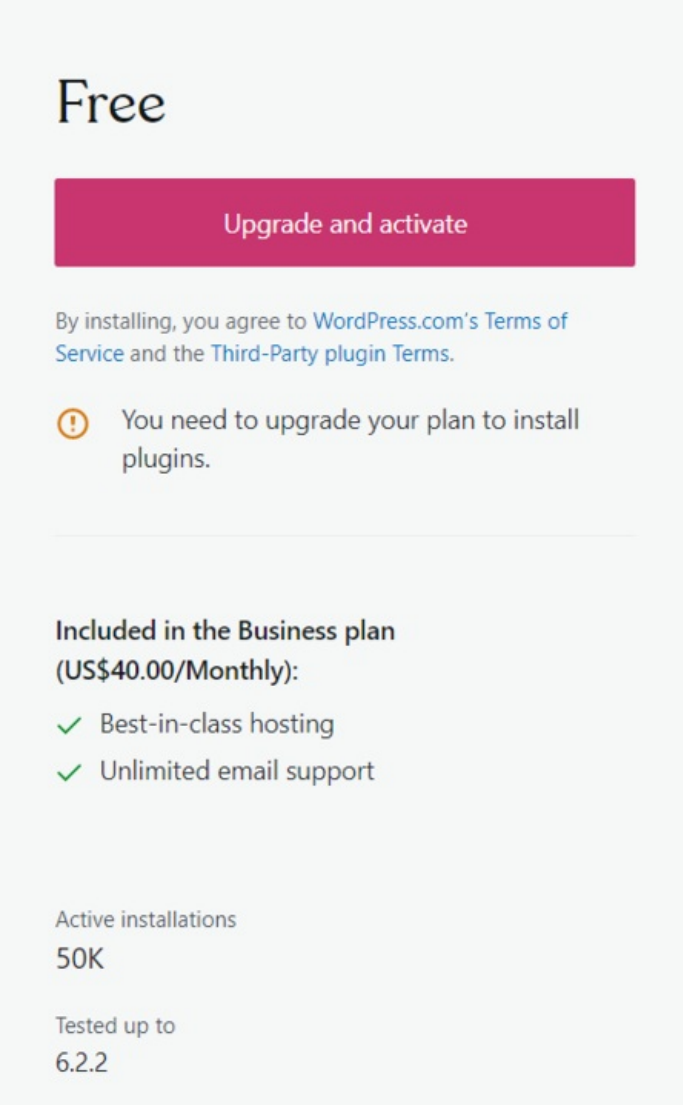
>
Business Context
As a developer, you may be called on to create new forms and/or modify existing forms in WordPress. If your employer/customer is already using a certain plugin for their forms, and assuming that plugin is secure, you should work with the plugin that is already in place. Only introduce a new form solution if the existing solution is no longer secure or is no longer compatible with the rest of the website.

Contact Form 7 - Installation & Configuration

Before we proceed with the plugin installation steps, let's **review a few troubleshooting** steps:
1. Use LocalWP

If you can remember from **Module 8**, we installed **LocalWP** to set up a local WordPress environment on our computers. It is **crucial to ensure that we exclusively use LocalWP for installing plugins**, whether they are free or paid, rather than installing them directly on wordpress.com.

If you are installing plugins directly on www.wordpress.com, you might come across a prompt like this to upgrade:

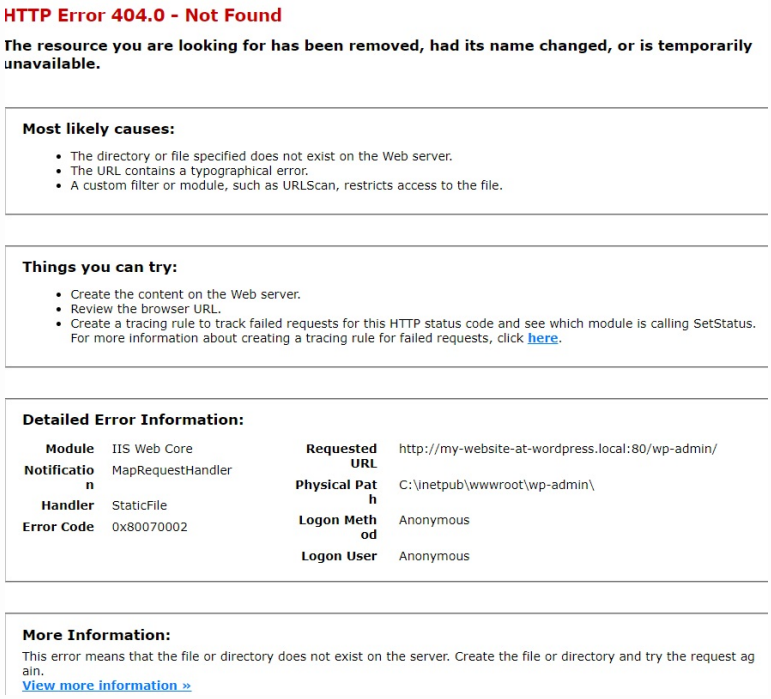


wordpress.com upgrade

If you **don't have LocalWP installed**, you can download it from https://localwp.com/. If you need help with the installation process, please refer to this video.

2. Revert IIS setting from Module 16 Lesson 1.2

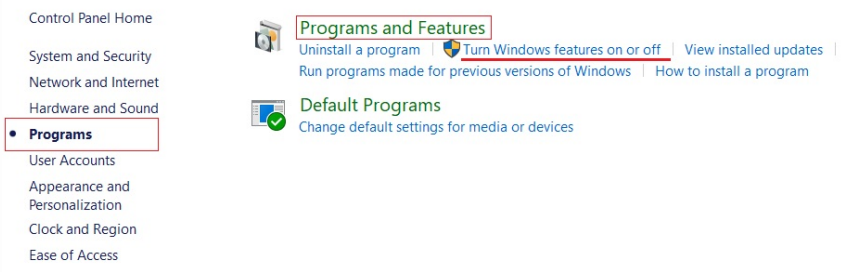
Another problem that you might encounter when attempting to **view your site using LocalWP** is the following error:



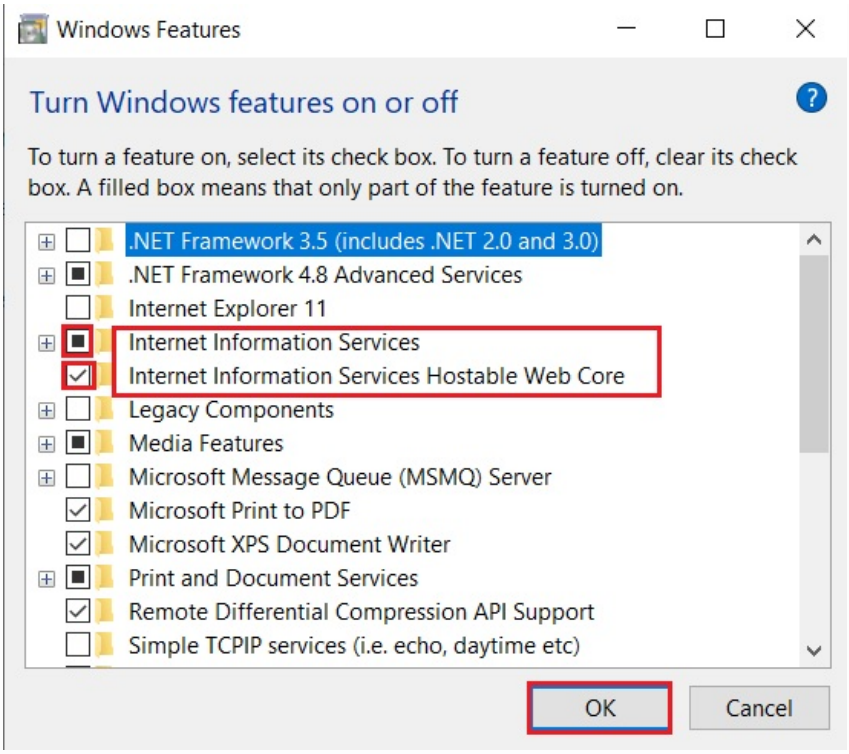
wordpress.com upgrade

To **resolve this error**, you need to **revert** back the **IIS changes** you made, on **Module 16, Lesson 1.2**.

1. Open your Control Panel
2. Open Programs and Features
3. Click on Turn Window features on or off



4. In the popup, locate Internet Information Services, **uncheck the box**. If you also see Internet Information Services Hostable Web Core then **uncheck** that box as well. Click OK.



5. When your computer is finished making the changes, it may ask to restart your computer. This is normal. Save any changes you may need to in open files. Close everything including the Control Panel and restart your computer.

Contact Form 7 - Installation & Configuration

Now, let's create a simple contact form for your personal website using the plugin Contact Form 7.

>

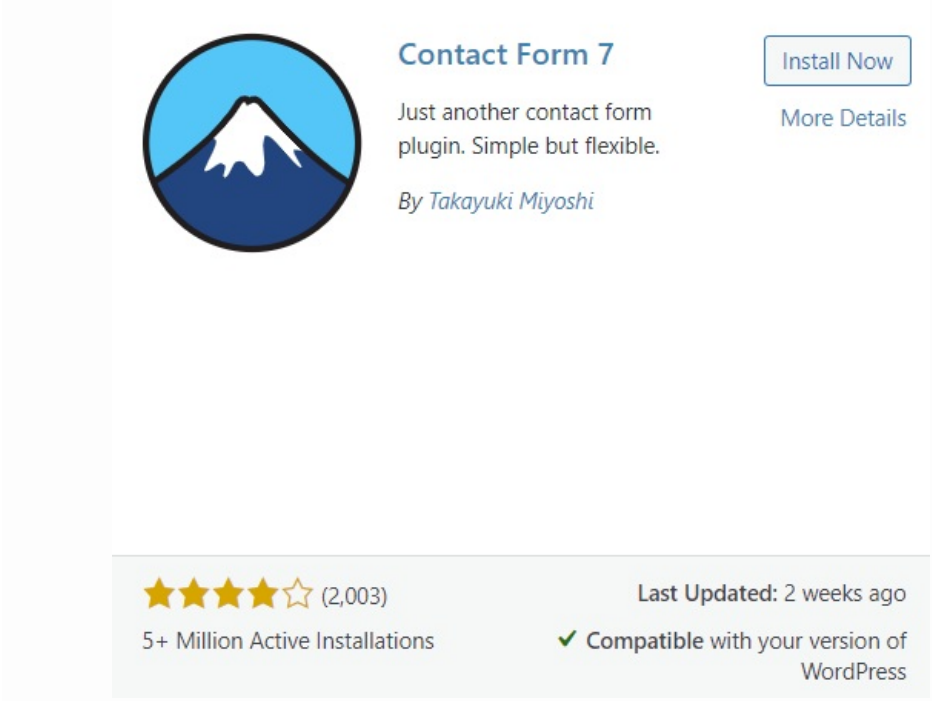
Step 1: Using the left-hand menu, navigate to **Plugins → Add New**

>

Step 2: Use the search bar in the upper left-hand corner to search for **Contact Form 7**

>

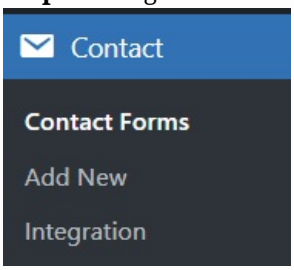
Step 3: Click **Install Now** button on the Contact Form 7 plugin



Step 4: Once it is installed, click the **Activate** button.

>

Step 5: Using the left-hand menu, navigate to **Contact → Contact Forms**



Step 6: Notice that a default contact form is already in place. Click **Edit** on the default form.

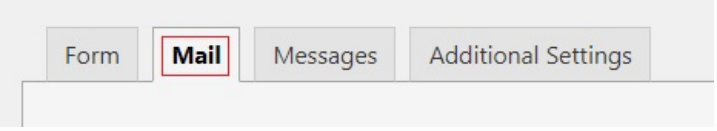
Step 7: Begin by re-naming the form to something else along the lines of **Contact YourFullName**

>

Step 8: The default form includes the fields name, email, subject, message Let's also add a phone number field. Your code should look something like this:

```
<label> Your name
    [text* your-name autocomplete:name] </label>

<label> Your email
    [email* your-email autocomplete:email] </label>

<label> Your phone number
    [tel usrphone placeholder "123-456-7890"] </label>

<label> Subject
    [text* your-subject] </label>

<label> Your message (optional)
    [textarea your-message] </label>

[submit "Submit"]
```

Step 9: Remember to **Save** your changes.
>
Step 10: So far, by editing code in the **Form** tab, we have only added the phone number field to the front end form. We still must add the phone number to the notification email. This is done in the **Mail** tab. Navigate to the **Mail** tab now.



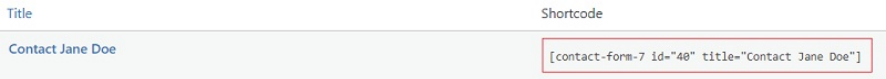
Step 11: In this tab you can modify the **To**, **From** and **Subject** of the notification email that will be sent when someone uses the contact form.
>
(Note that it is good practice to send From the domain name of the website. For example, the website https://mysite.com could send email from contact@mysite.com.)
>
Add the phone number field to the body of the email that will be sent. Your code should look something like this:

```
From: [your-name] <[your-email]>
Subject: [your-subject]

Phone: [usrphone]

Message Body:
[your-message]

--
This email was sent from a contact form on [_site_title]
([_site_url])
```

By default this is a text email, but Contact Form 7 does offer the option (free) of sending an email in HTML format so that you can style the appearance of this email as desired.

Step 12: Remember to save your form.

Step 13: Now that we have a contact form, we can integrate it on our contact page. Return to **Contact → Contact Forms**. Your contact form has a shortcode that you must copy.



Step 14: Now that you have copied the shortcode for your contact form, use the left-hand menu to navigate to **Pages**. If you do not have a contact page yet, you will need to create one now.
>
Paste the shortcode into the body of the page. Publish the changes.
>
Step 15: View your contact page, including your new contact form, on the front end of your website. You can submit a test to receive the notification email.
>
Please note that your form has not been styled and may look less than excellent depending on your active theme. If you have some time now, modify your theme's css file to style the form.

Protecting Your Contact Form

Protecting Your Contact Form

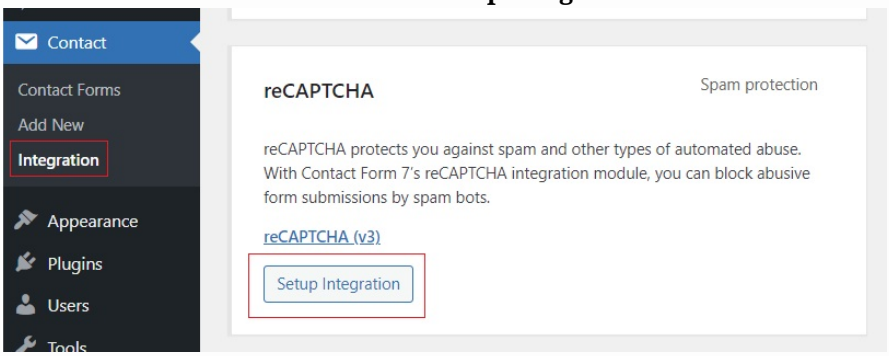
We have a contact form that works, but is vulnerable to spam. Bots will flood your inbox with junk unless you activate some form of spam filter. We will integrate Google reCAPTCHA V3 to limit bot spam that comes through the form.

>

Navigate to Contact → Integration

>

Scroll down to reCAPTCHA and click **Setup Integration**.



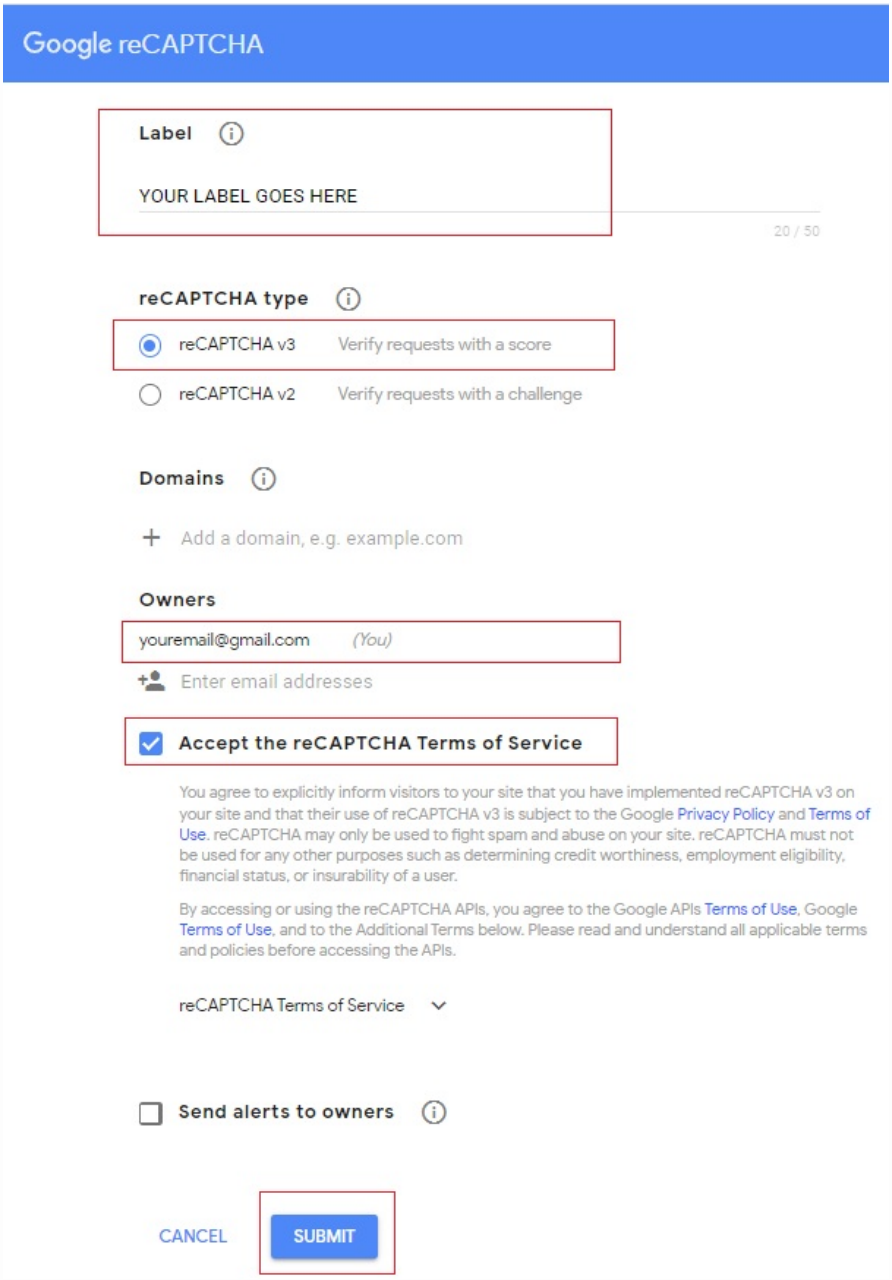
We must create a Site Key and a Secret Key.

>

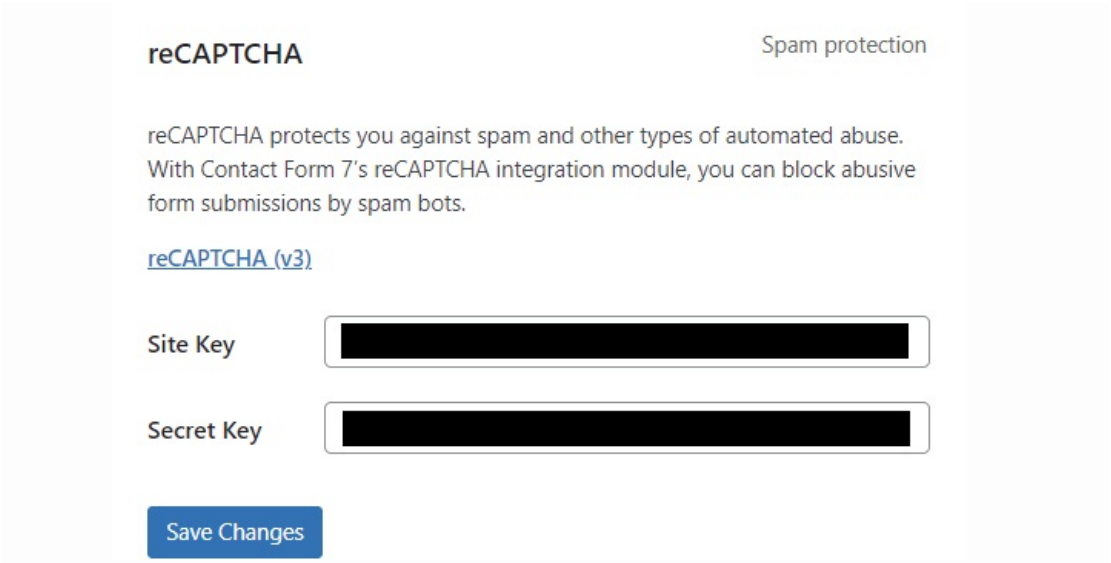
In a new browser tab, login to your google account the visit: https://www.google.com/recaptcha/admin/create

>

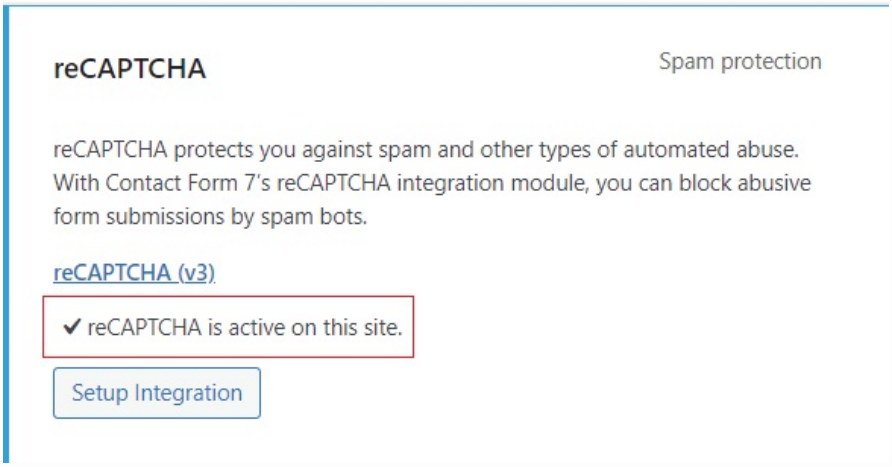
Complete the form as follows:



Once you click SUBMIT, you will be taken to a screen that includes your site key and your secret key. These must be copied and pasted into their respective fields in the Contact Form integration screen from your previous browser tab.



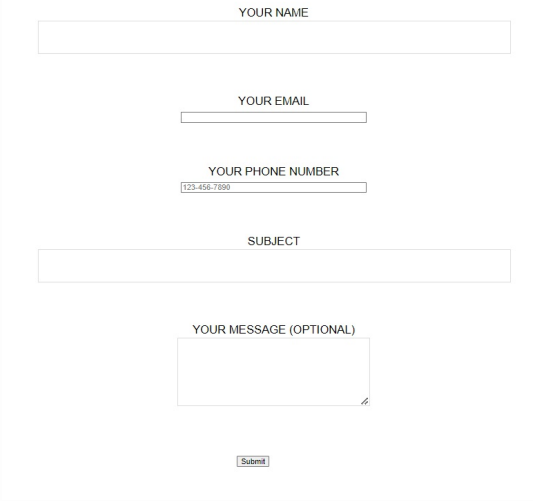
Remember to **Save Changes**. Your form now has some protection from Spam.



Turning Design into Code

Turning Design into Code

The contact form we just created is very plain. Depending on your active theme, it may look like the image on the left. We will want to make the front end of this form much more attractive to users.
>
Sometimes you will be presented with designs that you will “bring to life” on the website. Suppose you were given the task to create the following form on the right. Notice that it contains all the same fields as your new contact form. That means we can use our new contact form as a starting point for design integration, so that the end result looks like the form on the right.

Plain	Designed
	

> To do this, you will need not only a mock-up (as above), but also specifications regarding fonts, spacing, margins, padding, components and interaction, functionality requirements and responsive design requirements. Even if it is not specified, all of your code should be responsive for optimal display across screen sizes.
>
> The designer can provide you with all of the relevant specifications. As a developer, your job is not to critique the design work, but rather to implement it. Designers are artistic individuals who are emotionally invested in their work. It is essential that you maintain an open back-and-forth dialogue with designers on your team. Ask as many questions as you must to get the job done and, if you must provide design feedback, keep your feedback as complimentary as possible.
>
> Think about how you can use CSS to modify the layout of your form so that it is visually appealing for users.

Conclusion & Takeaways

Conclusion & Takeaways

Adding a contact form to a WordPress website is a straightforward task that will make your website more interactive and will help you gather leads. No matter what form builder plugin you decide to use, that plugin must receive regular security updates as security patches are released in new plugin versions. It is also important to protect contact forms against spam. All form builders will offer some kind of anti-spam integration. Forms must be secure, functional and attractive to users, in that order.
>
Learn more about creating forms with Contact Form 7: https://contactform7.com/docs/
>
Attribution
- Image https://www.freepik.com/free-vector/contact-concept-landing-page_5102922.htm
- Contact Form 7 Documentation https://contactform7.com/docs/
- Google reCAPTCHA keys https://www.google.com/recaptcha/admin/create

Project: Security

Sanitized Variables & Relative Paths

Goals

By the end of this project you will:
- Restrict user inputs
- Validate user inputs
- Sanitize user inputs
- Include a file using a relative path
>
Introduction
This project aims to bring together your knowledge on the use of localhost and basic web security tactics.
>
Business Context
There are many ways to add forms to websites that vary according to context and platform. Nevertheless, your ability to build a basic form in HTML and improve its security using JavaScript will serve you well no matter which context you ultimately develop in.

Instructions

Instructions

1. Begin with the Newsletter sign up form developed locally in **Day 2, Lesson 1 Defending against XSS**.
2. Add a **phone number field** to your Newsletter Signup form.
3. Use `maxlength` attribute to further restrict user inputs.
4. **Create** a **JavaScript function** to **retrieve the phone number input** from the user.
5. **Check** that the **phone number input is not blank**.
6. **Check** that the **phone number** contains only **numbers and dashes**.
7. If there are any issues with the phone number field, prepare an **error message for the user**.
8. If there are **no problems** with the phone number input, **sanitize it before submitting the form**.

Submission steps:

Before you click on “Mark as Completed”:

You need to do one of the following: either upload all of your files to Codio or deploy a GitHub Page for this project.

Also, if you mark this project as complete but any of the boxes are blank, your TA will be unable to grade your project.

Codio upload:

- Make sure all of your project code has been uploaded to Codio.
  - If you did not write your code in Codio, you will need to import all of the required files into your workspace file tree.
  - You can do this by going to File => Upload Files, and either manually importing each file, or dragging and dropping your project folder.
  - Please refer to this video if you are unsure of what to do.

GitHub Pages:

- If you would rather upload your project to GitHub, please make sure to have the project deployed as a GitHub page so we can thoroughly test it.
  - If you are unsure of how to do this, please follow these instructions.
  - It is important to understand you will need to make a separate repository for every project. You **cannot** deploy multiple pages from the same repository, even with different branches.

Also, no matter whether you uploaded your files from your computer or not, **make sure to thoroughly test your code**! This only takes a few minutes, but will prevent the amount of resubmissions because you missed something.