Web Fundamentals - Debug Project

Piotr Kobylis

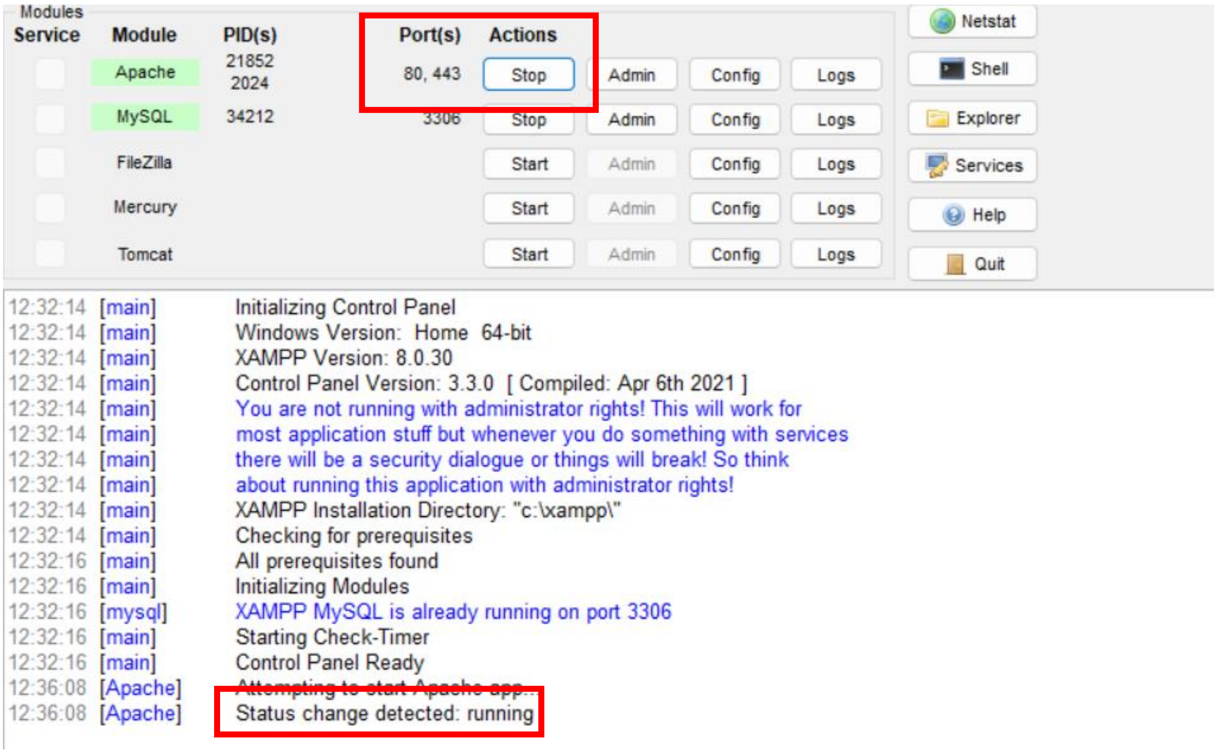
Red Team Specialist

1 Configure the XAMPP server so the website will work.

I have downloaded XAMPP from below link installed and launched Apache server from XAMPP Control Panel.

Default folder where XAMPP is installed is C:\xampp

https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/8.0.30/xampp-windows-x64-8.0.30-0-VS16-installer.exe

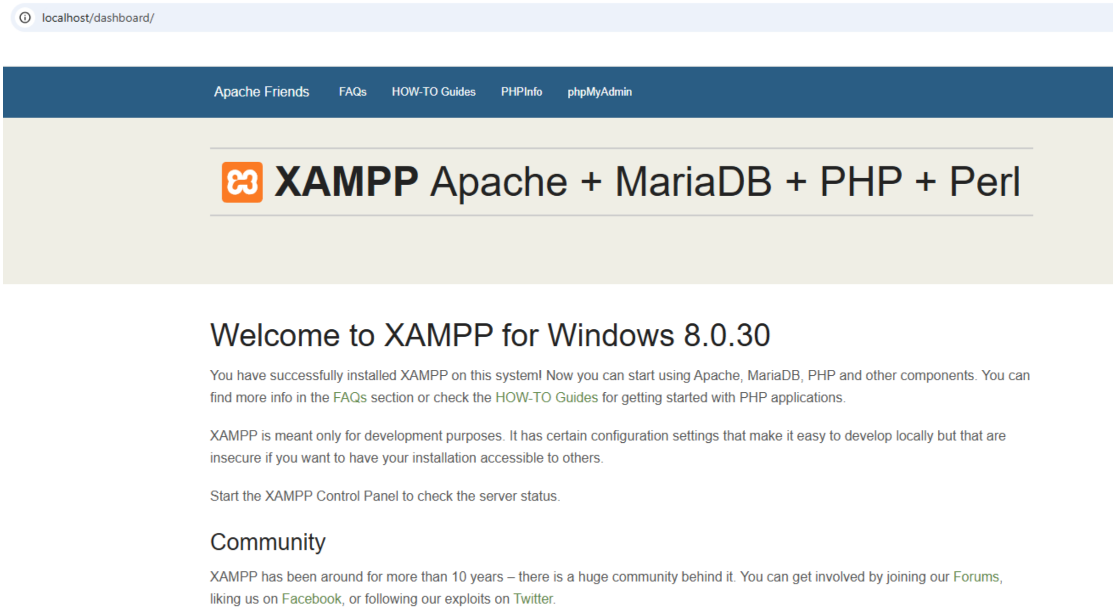


Modules

Service	Module	PID(s)	Port(s)	Actions			
□	Apache	21852 2024	80, 443	Stop	Admin	Config	Logs
□	MySQL	34212	3306	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

```
12:32:14  [main]      Initializing Control Panel
12:32:14  [main]      Windows Version:  Home  64-bit
12:32:14  [main]      XAMPP Version: 8.0.30
12:32:14  [main]      Control Panel Version: 3.3.0  [ Compiled: Apr 6th 2021 ]
12:32:14  [main]      You are not running with administrator rights! This will work for
12:32:14  [main]      most application stuff but whenever you do something with services
12:32:14  [main]      there will be a security dialogue or things will break! So think
12:32:14  [main]      about running this application with administrator rights!
12:32:14  [main]      XAMPP Installation Directory: "c:\xampp\"
12:32:14  [main]      Checking for prerequisites
12:32:16  [main]      All prerequisites found
12:32:16  [main]      Initializing Modules
12:32:16  [mysql]     XAMPP MySQL is already running on port 3306
12:32:16  [main]      Starting Check-Timer
12:32:16  [main]      Control Panel Ready
12:36:08  [Apache]    Attempting to start Apache app...
12:36:08  [Apache]    Status change detected: running
```

I have also checked it on a URL: localhost



Welcome to XAMPP for Windows 8.0.30

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

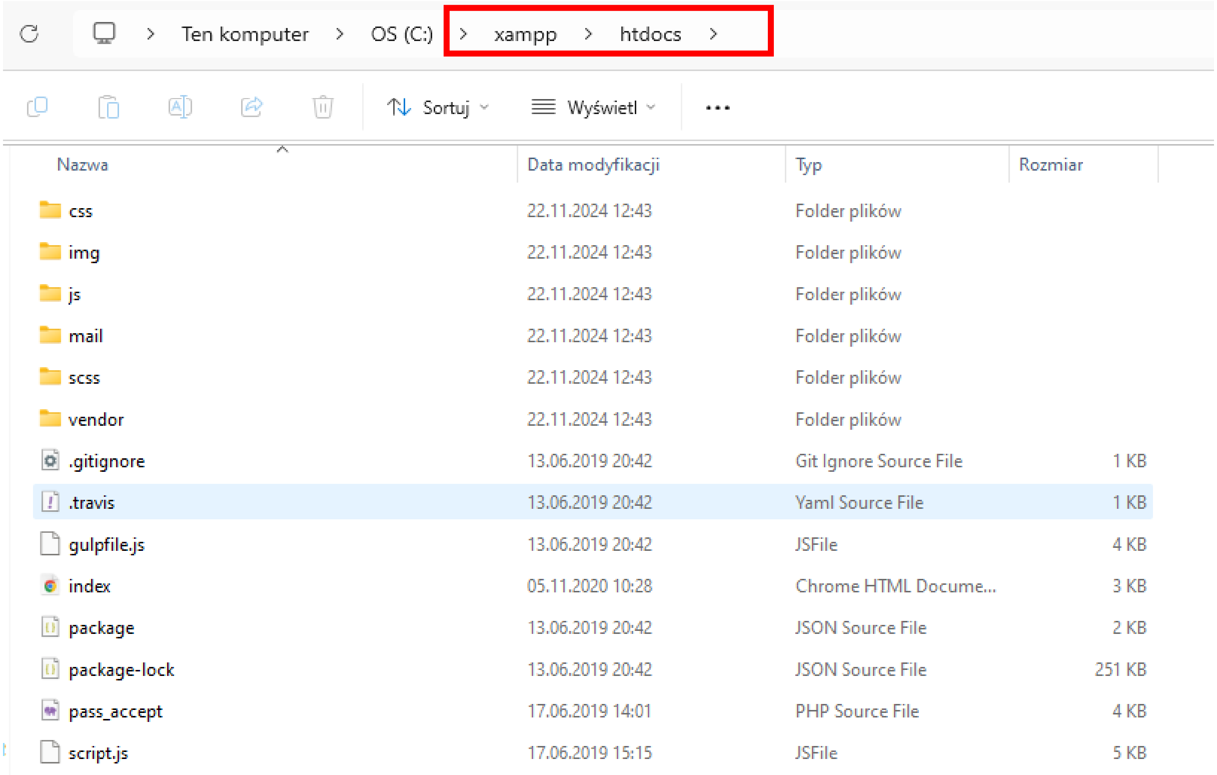
XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others.

Start the XAMPP Control Panel to check the server status.

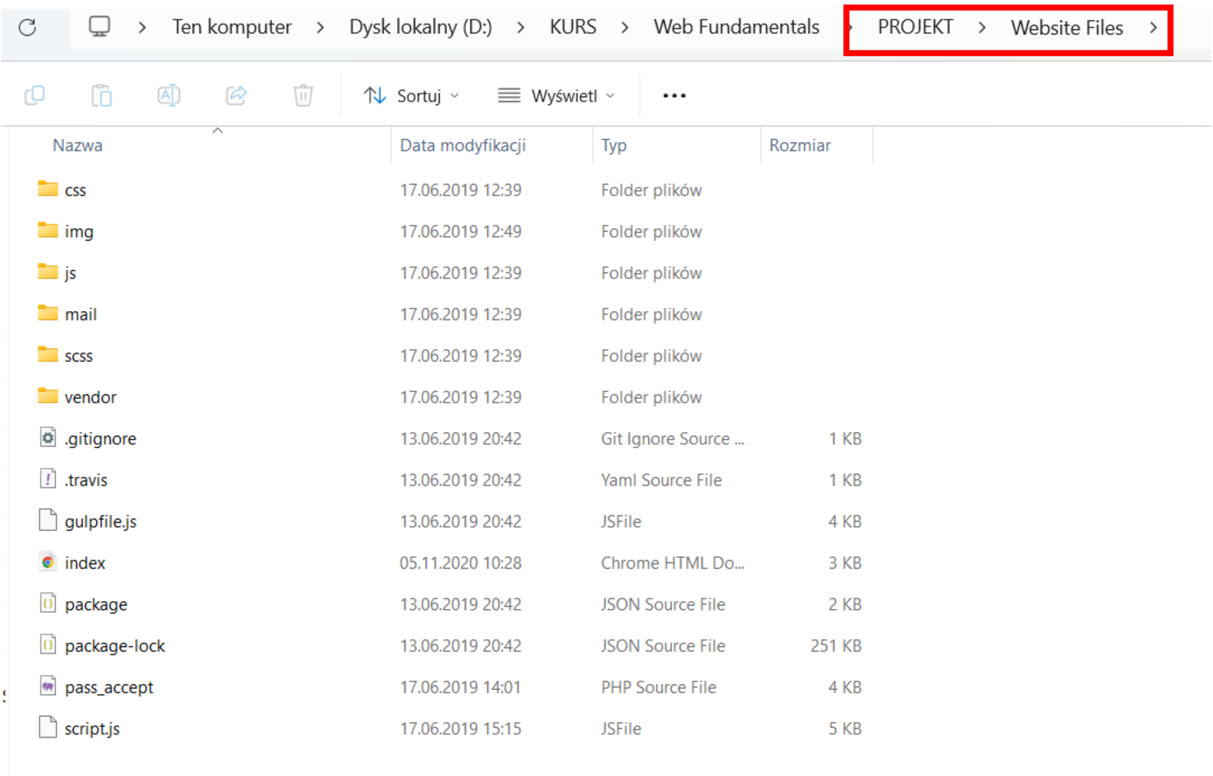
Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, liking us on Facebook, or following our exploits on Twitter.

Next I have changed files default files from C:\xampp\htdocs to Project file called Website Files that I have downloaded from Hackampus

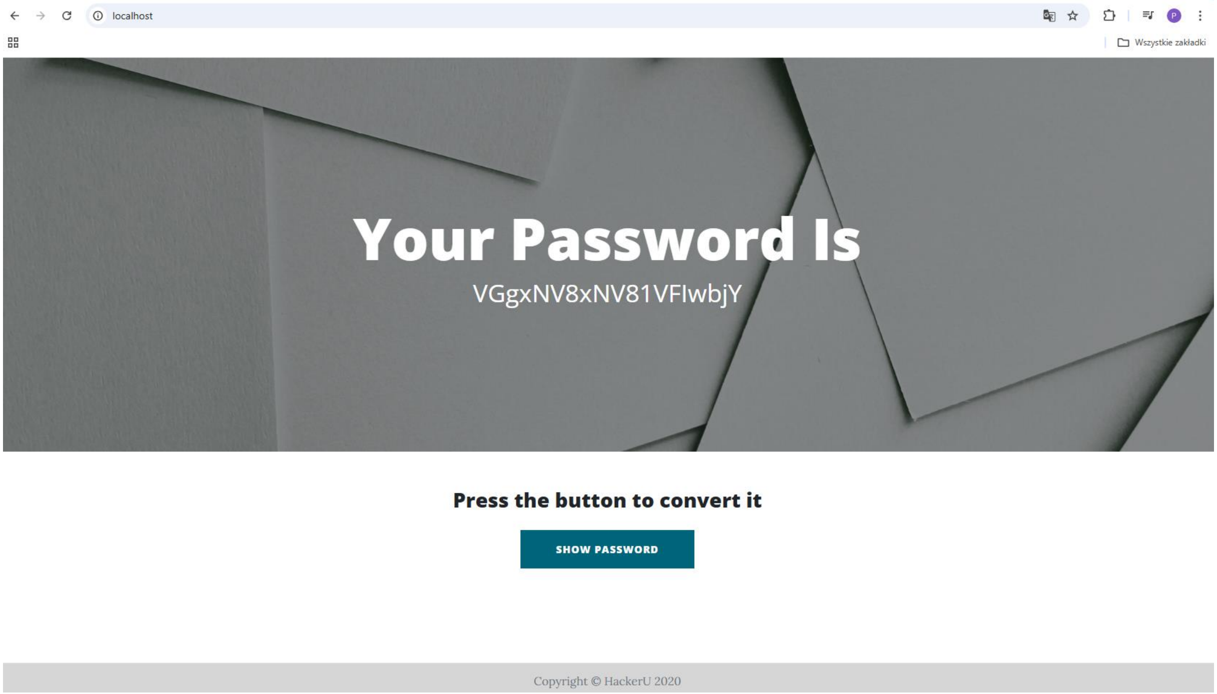


Nazwa	Data modyfikacji	Typ	Rozmiar
css	22.11.2024 12:43	Folder plików	
img	22.11.2024 12:43	Folder plików	
js	22.11.2024 12:43	Folder plików	
mail	22.11.2024 12:43	Folder plików	
scss	22.11.2024 12:43	Folder plików	
vendor	22.11.2024 12:43	Folder plików	
.gitignore	13.06.2019 20:42	Git Ignore Source File	1 KB
.travis	13.06.2019 20:42	Yaml Source File	1 KB
gulpfile.js	13.06.2019 20:42	JSFile	4 KB
index	05.11.2020 10:28	Chrome HTML Docume...	3 KB
package	13.06.2019 20:42	JSON Source File	2 KB
package-lock	13.06.2019 20:42	JSON Source File	251 KB
pass_accept	17.06.2019 14:01	PHP Source File	4 KB
script.js	17.06.2019 15:15	JSFile	5 KB


Ten komputer > Dysk lokalny (D:) > KURS > Web Fundamentals > PROJEKT > Website Files >
Sortuj
Wyświetl
...

Nazwa	Data modyfikacji	Typ	Rozmiar
css	17.06.2019 12:39	Folder plików	
img	17.06.2019 12:49	Folder plików	
js	17.06.2019 12:39	Folder plików	
mail	17.06.2019 12:39	Folder plików	
scss	17.06.2019 12:39	Folder plików	
vendor	17.06.2019 12:39	Folder plików	
.gitignore	13.06.2019 20:42	Git Ignore Source ...	1 KB
.travis	13.06.2019 20:42	Yaml Source File	1 KB
gulpfile.js	13.06.2019 20:42	JSFile	4 KB
index	05.11.2020 10:28	Chrome HTML Do...	3 KB
package	13.06.2019 20:42	JSON Source File	2 KB
package-lock	13.06.2019 20:42	JSON Source File	251 KB
pass_accept	17.06.2019 14:01	PHP Source File	4 KB
script.js	17.06.2019 15:15	JSFile	5 KB

Now website looks like this:



Your Password Is

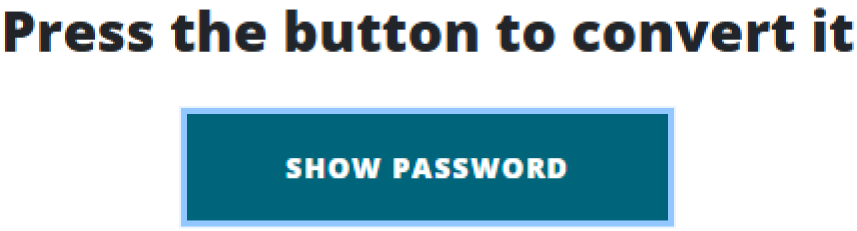
VGgxNV8xNV81VFIwbjY

Press the button to convert it

SHOW PASSWORD

Copyright © HackerU 2020

This button doesn't work



Press the button to convert it

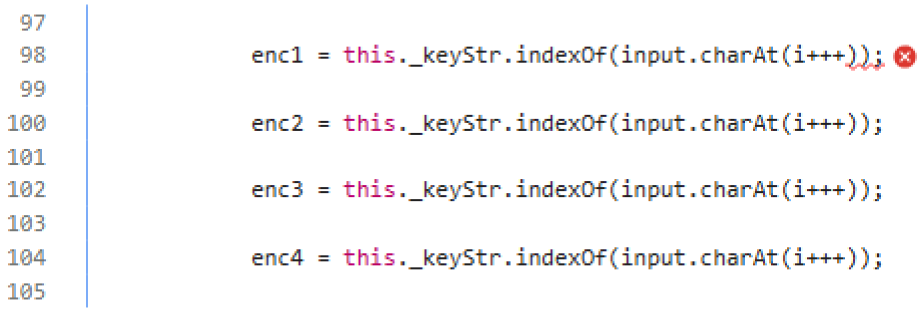
SHOW PASSWORD

2 Fix the website's JS code. Use the debugger to inspect the errors.

Lets start debugger and check script.js to look for a bugs

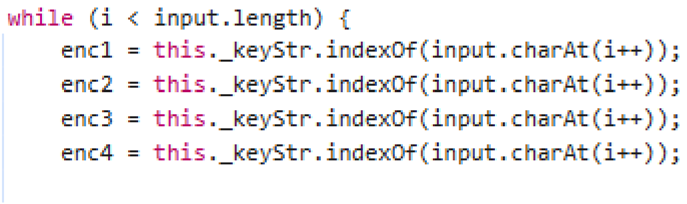
Debugger shows that in the line 98 in script.js is a bug. chatgpt advised to reduce "+" operator.

So instead of this:



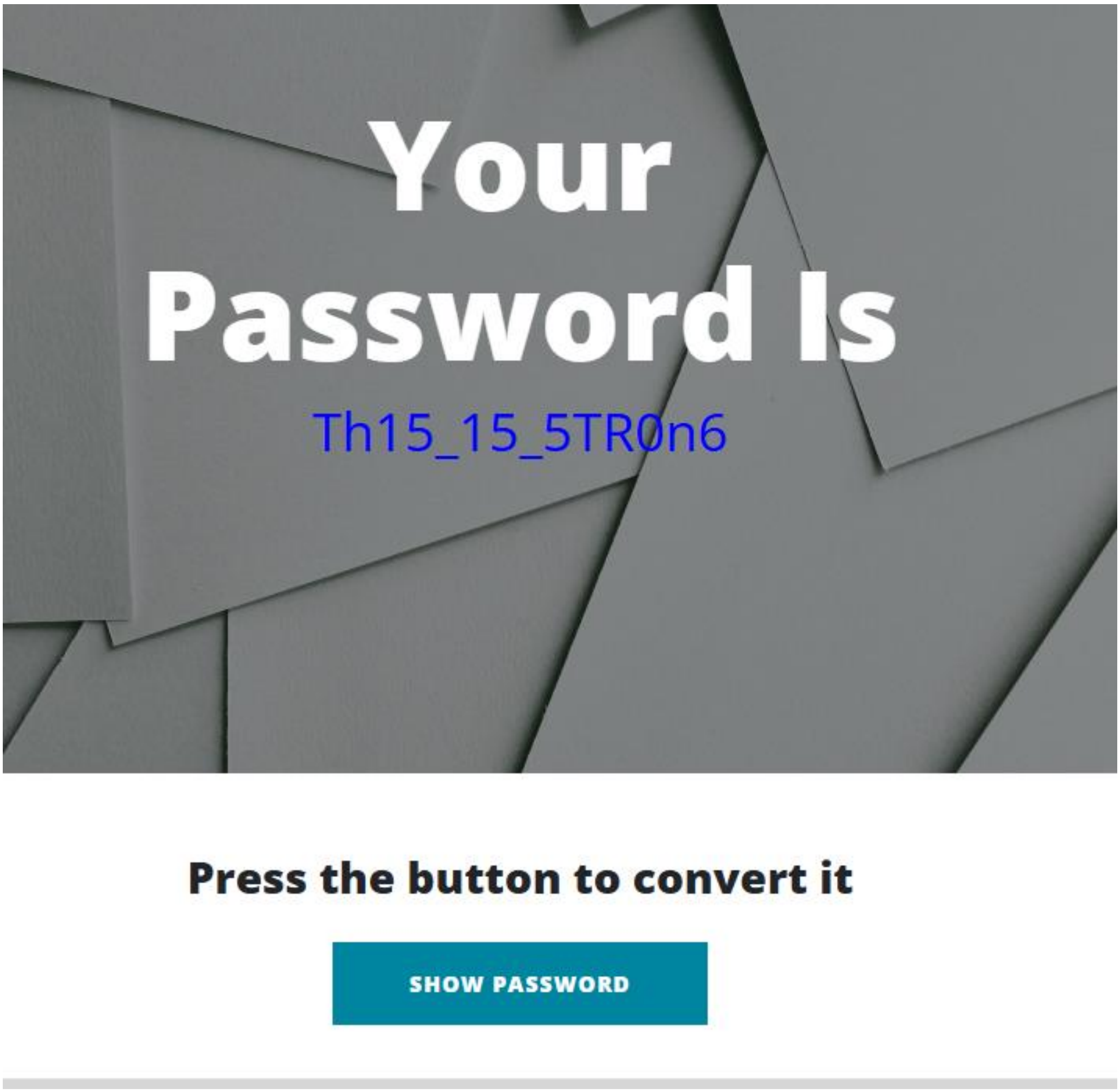
```
 97
 98             enc1 = this._keyStr.indexOf(input.charAt(i+++));
 99
100             enc2 = this._keyStr.indexOf(input.charAt(i+++));
101
102             enc3 = this._keyStr.indexOf(input.charAt(i+++));
103
104             enc4 = this._keyStr.indexOf(input.charAt(i+++));
105
```

We get



```
while (i < input.length) {
    enc1 = this._keyStr.indexOf(input.charAt(i++));
    enc2 = this._keyStr.indexOf(input.charAt(i++));
    enc3 = this._keyStr.indexOf(input.charAt(i++));
    enc4 = this._keyStr.indexOf(input.charAt(i++));
```

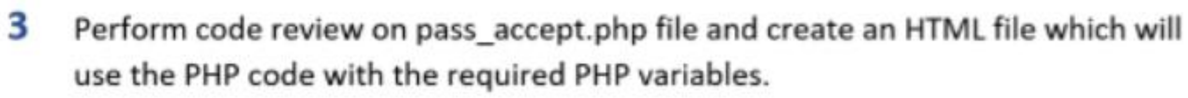
Now it works like this:



Your Password Is

Th15_15_5TR0n6

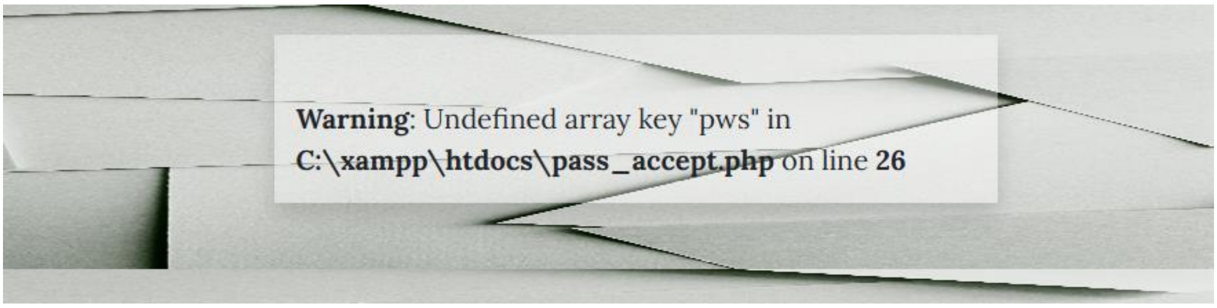
Press the button to convert it



3 Perform code review on pass_accept.php file and create an HTML file which will use the PHP code with the required PHP variables.

I have used ChatGPT to review that code and generate correct one. Saved new code as an index.php and run this file on a server localhost/index.php.

Now website looks like this



Warning: Undefined array key "pws" in **C:\xampp\htdocs\pass_accept.php** on line **26**

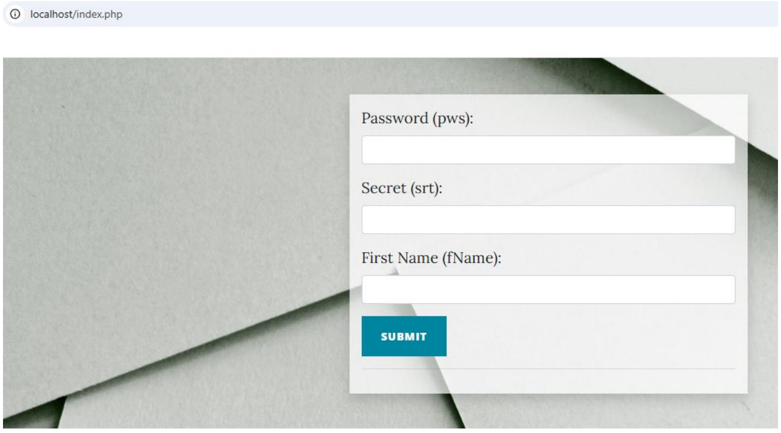
New code looks like this:

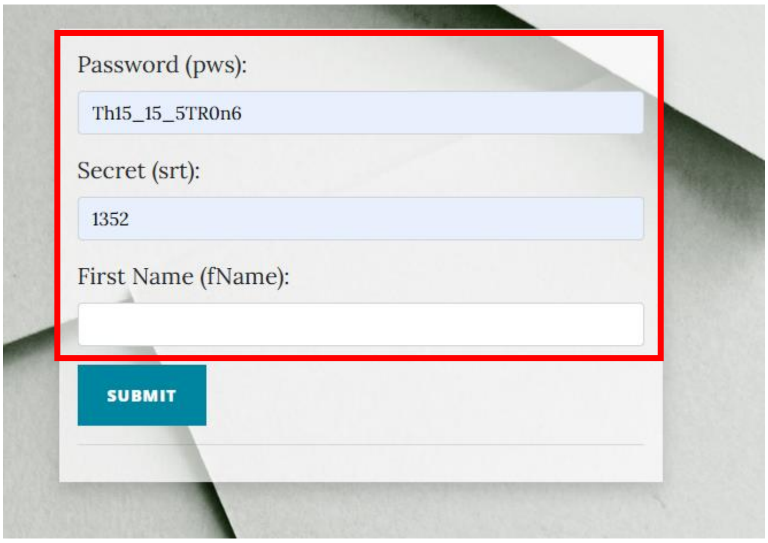
```
<!DOCTYPE html>

<html lang="en">


<head>

  <meta charset="utf-8">

  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <meta name="description" content="">

  <meta name="author" content="">

  <title>HackerU</title>

  <!-- Bootstrap core CSS -->

  <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">

  <!-- Custom fonts for this template -->

  <link href="vendor/fontawesome-free/css/all.min.css" rel="stylesheet" type="text/css">

  <link href='https://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic' rel='stylesheet' type='text/css'>

  <link href='https://fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600italic,700italic,800italic,400,300,600,700,800' rel='stylesheet' type='text/css'>

  <!-- Custom styles for this template -->

  <link href="css/clean-blog.min.css" rel="stylesheet">
```

```
</head>


<body style="background-image: url('img/background.jfif'); background-size: cover;
background-attachment: fixed;">


  <!-- Page Header -->
  <div class="container py-5">
    <div class="col-12 col-md-8 col-lg-6 mx-auto">
      <div style="background-color: rgba(255, 255, 255, 0.7);" class="p-3 shadow">
        <!-- Form to input "pws", "srt", and "fName" -->
        <form method="POST" action="">
          <div class="form-group">
            <label for="pws">Password (pws):</label>
            <input type="text" class="form-control" id="pws" name="pws" required>
          </div>
          <div class="form-group">
            <label for="srt">Secret (srt):</label>
            <input type="text" class="form-control" id="srt" name="srt" required>
          </div>
          <div class="form-group">
            <label for="fName">First Name (fName):</label>
            <input type="text" class="form-control" id="fName" name="fName">
          </div>
          <button type="submit" class="btn btn-primary">Submit</button>
        </form>


        <hr>


        <?php
        // Sprawdzamy, czy dane zostały wysłane i poprawne
        if (
          isset($_POST["pws"], $_POST["srt"]) &&
          $_POST["pws"] === base64_decode("VGgxNV8xNV81VFIwbjY") &&
          $_POST["srt"] === "1352" &&
          empty($_POST["fName"])  // Pole "fName" musi być puste
        ) {
          // Generujemy kod JavaScript do wyświetlenia alertu
          echo '<script>
              alert("AMAZING YOU DID IT !!!");
             </script>';
        }
        ?>
      </div>
    </div>
  </div>

</body>

</html>
```

4 Examine and use the code within HTML so it will work.

And works like this. I have provided credentials that I have received in a previous task.





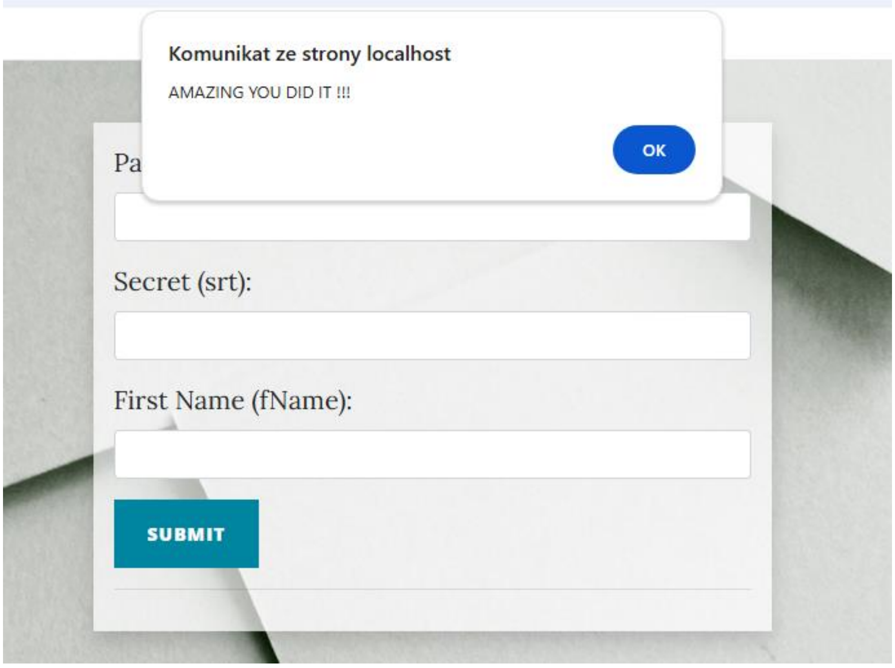
Password (pws):

Th15_15_5TR0n6

Secret (srt):

1352

First Name (fName):



Komunikat ze strony localhost

AMAZING YOU DID IT !!!