**G.P.Y.A**

**A PROJECT REPORT**

***Submitted by***

**Harshit Mathur (19BCY10009)**

**Abhinav Gupta (19BCY10110)**

**Harsh Kumar (19BCY10159)**

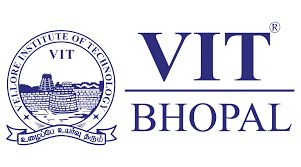
*In partial fulfillment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE ENGINEERING SPECIALIZED IN CYBER**

**SECURITY & DIGITAL FORENSICS**



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY KOTRI KALAN, SEHORE**

**MADHYA PRADESH - 466114**

NOVEMBER 2020

**VIT BHOPAL UNIVERSITY, KOTRI KALAN, SEHORE MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“G.P.Y.A”** is the bonafide work of “**Harshit Mathur (19BCY10009), Abhinav Gupta (19BCY10110) & Harsh Kumar (19BCY10159)”** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported here does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

**PROGRAM CHAIR**

Dr. Shishir Kumar Shandilya

Senior Associate Professor

School of Computer Science Engineering, VIT BHOPAL UNIVERSITY

**PROJECT GUIDE**

Dr. Praveen Lalwani

Assistant Professor

School of Computer Science Engineering, VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on **29 NOVEMBER, 2020**

**ACKNOWLEDGEMENT**

First and foremost we would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

We wish to express our heartfelt gratitude to **Dr. Shishir Kumar Shandilya**, ***Division Head of the Department, Cyber Security and Digital Forensics,*** for much of his valuable support encouraged in carrying out this work.

We would like to thank our internal guide **Dr. Praveen Lalwani**, for continually guiding and actively participating in our project, giving valuable suggestions to complete the project work.

We would like to thank all the technical and teaching staff of the School of computer science and engineering, who extended directly or indirectly all support.

Last, but not least, We are deeply indebted to our parents who have been the greatest support while we worked day and night for the project to make it a success.

**ABSTRACT**

The Covid-19 pandemic has brought with it a horrendous amount of difficulties for the people in the health and medical sector, but the threat has not been limited to these sectors alone, but has gone on to affect the world of technology as well. The number of cyber attacks has been on the rise since the lockdown regulations were implemented all over the world. One of the most popular cyber attacks among the culprits has been the phishing attack. With the number of people shopping online and using other online tools going up exponentially by the day, the number of phishing attacks has also been on the rise. With a high number of people still not well versed in certain areas of technology, attackers have been enjoying a high rate of success in such attacks.

A great way of preventing falling prey to such attacks is to verify the URL being visited to avoid being directed to malicious websites or clicking on malicious links. We have planned our project in a way so as to provide a tool for users to check whether a URL of a website they are visiting is legitimate or a phished one. Our goal is to check for the authenticity of the URL and display the result in as simple a way as possible in order to help even the most basic of users understand what we mean to say. We also aim to increase awareness about such phishing attacks by providing users a deep insight about what phishing is, its types and the techniques used by attackers in such attacks. Finally we would inform the users about certain preventive measures that the users can follow in order to prevent falling prey to such attacks.

**TABLES OF CONTENT**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1** | **(i) ABSTRACT**  **(ii) LIST OF FIGURES**  **(iii) LIST OF TABLES**  **(iv) LIST OF ABBREVIATIONS** | **4**  **6**  **7**  **7** |
| **2** | **INTRODUCTION**  1.1 Introduction  1.2 Motivation for Work  1.3 Technical Aspects  1.3.1 Software Requirements  1.4 Problem Statement  1.5 Objective of the Work  1.6 Summary | **8**  **9**  **9**  **10**  **11**  **1111** |
| **3** | **LITERATURE SURVEY** | **12** |
| **4** | **PROJECT PROCEDURE**  3.1 Planning and Requirements  3.2 Analysis and Design  3.3 Implementation  3.4 Testing  3.5 Evaluation | **13**  **1313**  **1314** |
| **5** | **WORK DONE**  4.1 Web page using HTML  4.2 CSS for Design  4.3 PHP for database and connection  4.4 Database entries using XAMPP | **15**  **1821**  **23** |
| **6** | **OBSERVATION** | **27** |
| **7** | **CONCLUSION** | **28** |
| **8** | **RECOMMENDATION FOR FUTURE WORK** | **29** |
| **9** | **REFERENCES** | **30** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **FIGURE NAME** | **PAGE NO.** |
| **1** | **Phishing Attack Statistics** | **13** |
| **2** | **HTML Sample code Page 1** | **16** |
| **3** | **HTML Sample code Page 2** | **17** |
| **4** | **HTML Sample code Page 3** | **17** |
| **5** | **HTML Sample code Page 4** | **18** |
| **6** | **HTML Sample code Page 5** | **18** |
| **7** | **CSS Sample Code** | **19** |
| **8** | **CSS Sample Code** | **19** |
| **9** | **Website Image Homepage** | **20** |
| **10** | **Website Image About** | **20** |
| **11** | **Website Image Types** | **21** |
| **12** | **Website Image Techniques** | **21** |
| **13** | **Website Image Safety** | **22** |
| **14** | **PHP Sample Code 1** | **22** |
| **15** | **PHP Sample Code 2** | **23** |
| **16** | **PHP Sample Code 3** | **23** |
| **17** | **Database Image 1** | **24** |
| **18** | **Database Image 2** | **25** |
| **19** | **Database Image 3** | **26** |
| **20** | **Database Image 4** | **27** |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE**  **NO.** | **TITLE** | **PAGE NO.** |
| **1** | **LIST OF ABBREVIATIONS** | **9** |
| **2** | **SOFTWARE REQUIREMENTS** | **12** |

**LIST OF ABBREVIATIONS**

The following is a list of terms, acronyms and abbreviations used during our project.

|  |  |
| --- | --- |
| **ABBREVIATIONS** | **DEFINITIONS** |
| **API** | Application Programming Interface |
| **ETH** | Ethereum |
| **IDE** | Integrated Development Environment |
| **JSON** | JavaScript Object Notation |
| **EC** | Election Commission |
| **OS** | Operating System |
| **SRS** | Software Requirement Specifications |
| **SDLC** | Software Development Life Cycle |
| **ERC - 20** | Ethereum Tokens |
| **HTML** | Hypertext Markup Language |
| **CSS** | Cascading Style Sheets |
| **PHP** | Personal Home Page / Hypertext Preprocessor |
| **DBS** | Database Set |

Table 1. List of Abbreviations, used in the Report.

**1. INTRODUCTION**

**1.1 Introduction**

Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a fake Website by sending them faked e-mails (or instant messages), and stealthily get the victim's personal information such as user name, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank accounts). The frequently used attack method is to send e-mails to potential victims, which seemed to be sent by banks, online organizations, or ISPs. In these e-mails, they will make up some causes, e.g. the password of your credit card had been mis-entered for many times, or they are providing upgrading services, to allure you visit their Web site to conform or modify your account number and password through the hyperlink provided in the e-mail. If you input the account number and password, the attackers then successfully collect the information at the server side, and is able to perform their next step actions with that information (e.g., withdraw money out from your account).Phishing itself is not a new concept, but it's increasingly used by phishers to steal user information and perform business crime in recent years. Within one to two years, the number of phishing attacks increased dramatically.

The common characteristics of the hyperlinks in phishing e-mails. Our analysis identifies that the phishing hyperlinks share one or more characteristics as listed below:

1) The visual link and the actual link are not the same;

2) The attackers often use dotted decimal IP address instead of DNS name;

3) Special tricks are used to encode the hyperlinks maliciously;

4) The attackers often use fake DNS names that are similar (but not identical) with the target website.

**1.2 Motivation for the Work**

Duping people of their confidential data by making them either enter that data on a fake website or by stealing the data when they click on malicious links is the jest of phishing attacks. Being people who understand the concept and can help others in the prevention of falling prey to such attacks, we found it really motivating to help people by providing a tool for them and help them in this fight against phishing. The fact that this can help an awfully large number of internet users to keep themselves safe was a huge driving force for this project.

**1.3 Technical Aspect**

Evaluating the technical study is the trickiest aspect of a feasibility study. This is because at this point, not too many detailed plans of the system, making it hard to get to issues like performance, costs (on account of the kind of technology to be deployed), and the various number of issues must become in our mind while doing a detailed investigation Understand the different technologies involved in the proposed system before commencing the project we have to be very clear about what are the technologies that are to be required for the development of the new system. In general, this study needs to exhibit that the proposed system which is needed to be developed is technically feasible.

This requires:

• An outline of the requirements.

• A possible system design.

• Possible choices of software to be used or developed the smart contract.

• Estimates on the number of users, data, etc.

**1.3.1 Software Requirements**

This area of the report describes the various tools and techniques that were required in the making of this project.

Our website allows the user to enter the URL of the website they are visiting and checks the same with the contents of our database and tells if the URL is legitimate or malicious based on the results.

For the proper working of the system we can list our assumptions and dependencies as follows:

|  |  |  |
| --- | --- | --- |
| **Software** | **Type** | **Version** |
| Sublime Text | IDE | 1.0.0.1 |
| XAMPP | Cross-Platform | 7.4.11 |
| Google Chrome | Web Browser | 86.0.4240.111 |
| Visual Studio Code | IDE | 1.46 |
| Windows OS | Operating System | Windows 10 |

Table 2. Software Requirements

**1.4 Problem Statement**

The number of phishing attacks during these uncertain times of the covid-19 pandemic has been on the rise and the solutions existing on the web can be a bit too overwhelming for users not so much in the technological background. A website which can check the authenticity of a URL and display the results in as simple a way as possible is the need of the hour.

**1.5 Objective of the Work**

The objectives for developing the project are as follows:

● To help users and provide them with a simple way to check for the authenticity of a URL.

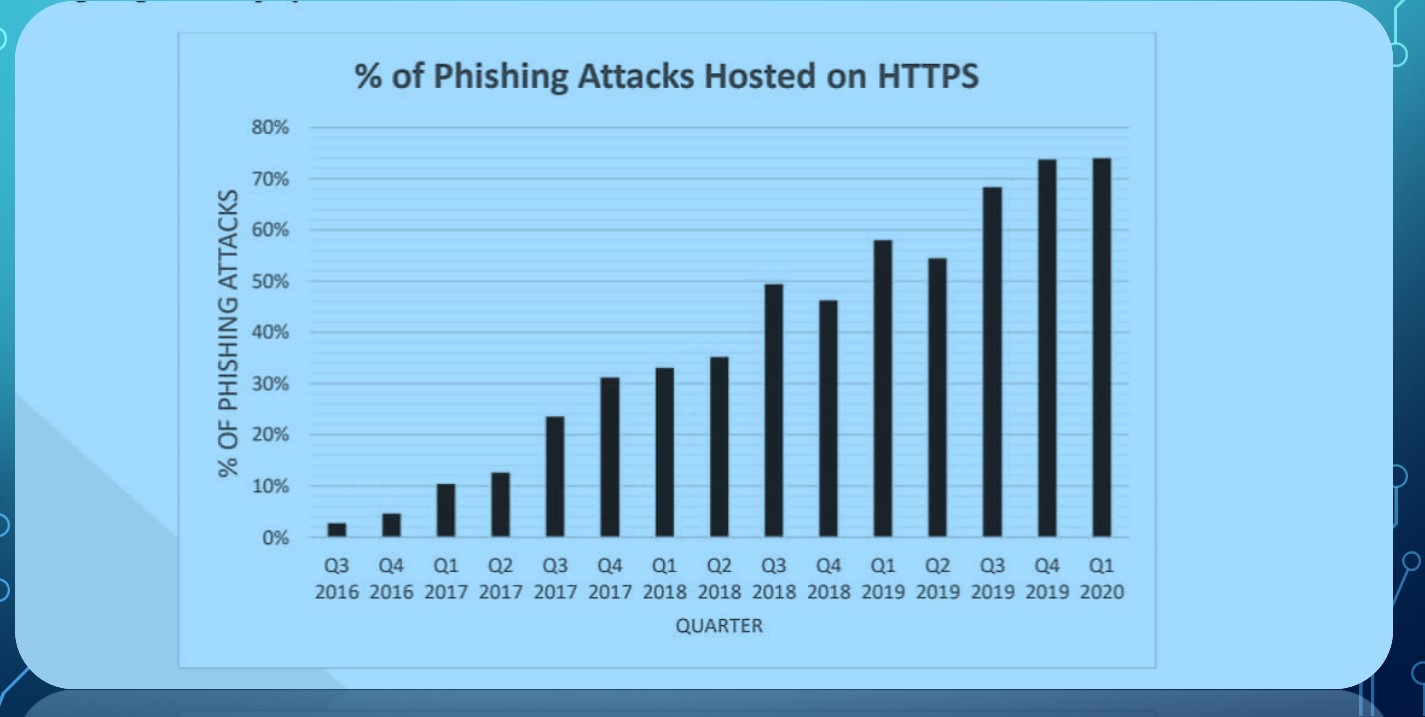
● To provide users with an in-depth insight into the concept of phishing as well as providing them with certain precautionary measures for them to be alert in the future.

**1.6 Summary**

We have developed a website for the users to check the authenticity of a URL and display the results in as simple a manner as possible for even the most naive of users to understand.

**2. LITERATURE SURVEY**

The number of phishing attacks has been on the rise during these uncertain times of the covid-19 pandemic. As shown in the image here, the rise has been huge as compared to the previous years and is expected to keep growing with time.



As mentioned in the image the number of attacks has been growing through the use of malicious links and websites which are used to dupe users on the internet.

Checking the authenticity of a URL is one of the best ways to prevent such attacks and help other users to prevent themselves from falling prey as well.

**3. PROJECT PROCEDURE**

**3.1 Planning & Requirements:** As with most any development project, the first step is to go through an initial planning stage to map out the specification documents, establish software or hardware requirements, and generally prepare for the upcoming stages of the cycle. Thus, we began with planning out our project on a piece of paper, we did mindmapping, group discussions, and several other techniques to find out what could be implemented to make it best.

**3.2 Analysis & Design:** Once planning is complete, an analysis is performed to nail down the appropriate business logic, database models, and the like that will be required at this stage in the project. The design stage also occurs here, establishing any technical requirements (languages, data layers, services, etc.) that will be utilized in order to meet the needs of the analysis stage.

We proposed that our project will help people in detecting malicious links, we are doing this by using basic rules like:-

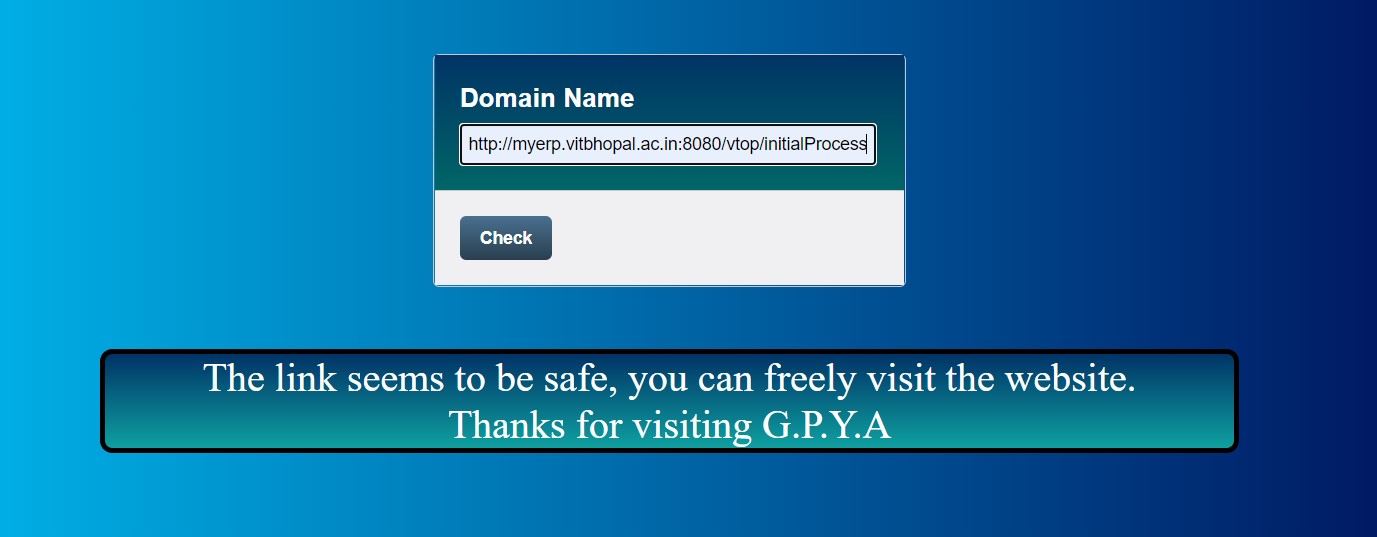
•It's been aforesaid that succeeding a part of "@" symbol in URL is ignored by the browser. It has been said that the next part of "@" symbol in URL is often the real address. Rule: If URL is containing @ symbol → phishing, otherwise→ legitimate.

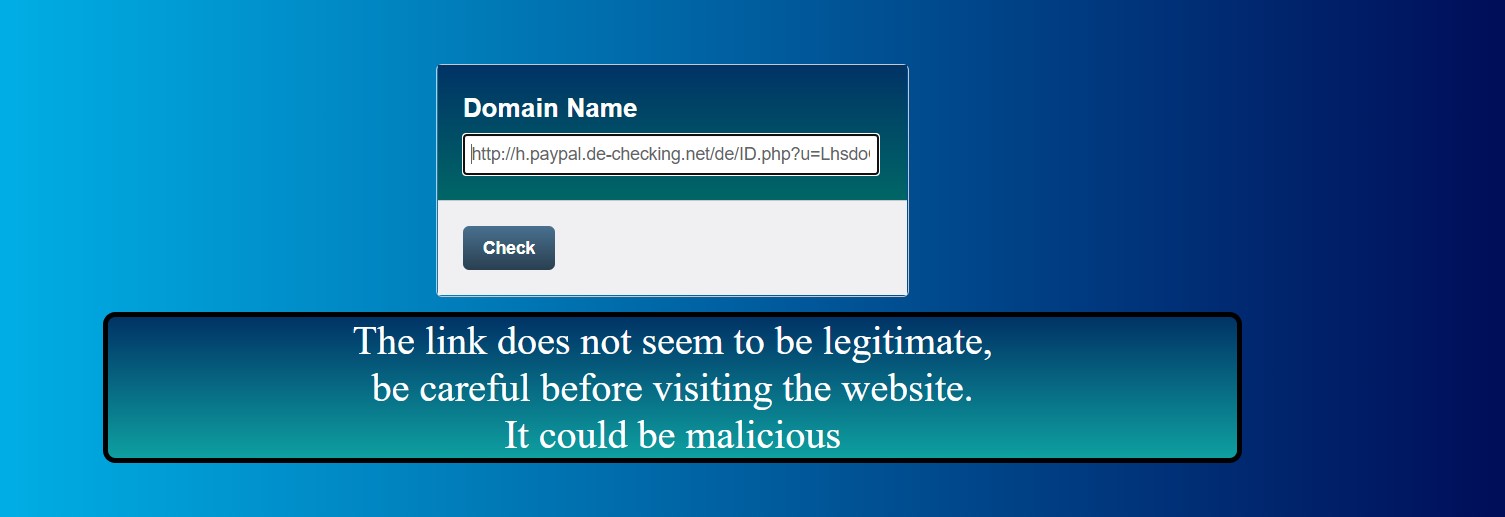
•The user may be directed to another web site using “//”in URL. If URL starts with “HTTP” then “//” symbol must be in the 6th position. If URL starts with “HTTPS” then “//” symbol must be in the 7th position. Rule: The position of last occurrence of "//" in URL > 7 → phishing, otherwise→ legitimate.

•The phishing link may have domain name and subdomain name different but in a way that it look familiar e.g.- amozon.com (for amazon.com) and flpkrt.com (for flipkaart.com).

**3.3 Implementation:** With the planning and analysis out of the way, the actual implementation and coding process can now begin. All planning, specification, and design docs up to this point are coded and implemented into this initial iteration of the project. We have used solidity to code the smart contracts that are the most important part of our project.

**3.4 Testing:** Once this current build iteration has been coded and implemented, the next step is to go through a series of testing procedures to identify and locate any potential bugs or issues that have cropped up. After completing the whole implementation work, we tested the code and checked it for a legitimate URL as well a fake URL as shown in the figures here.



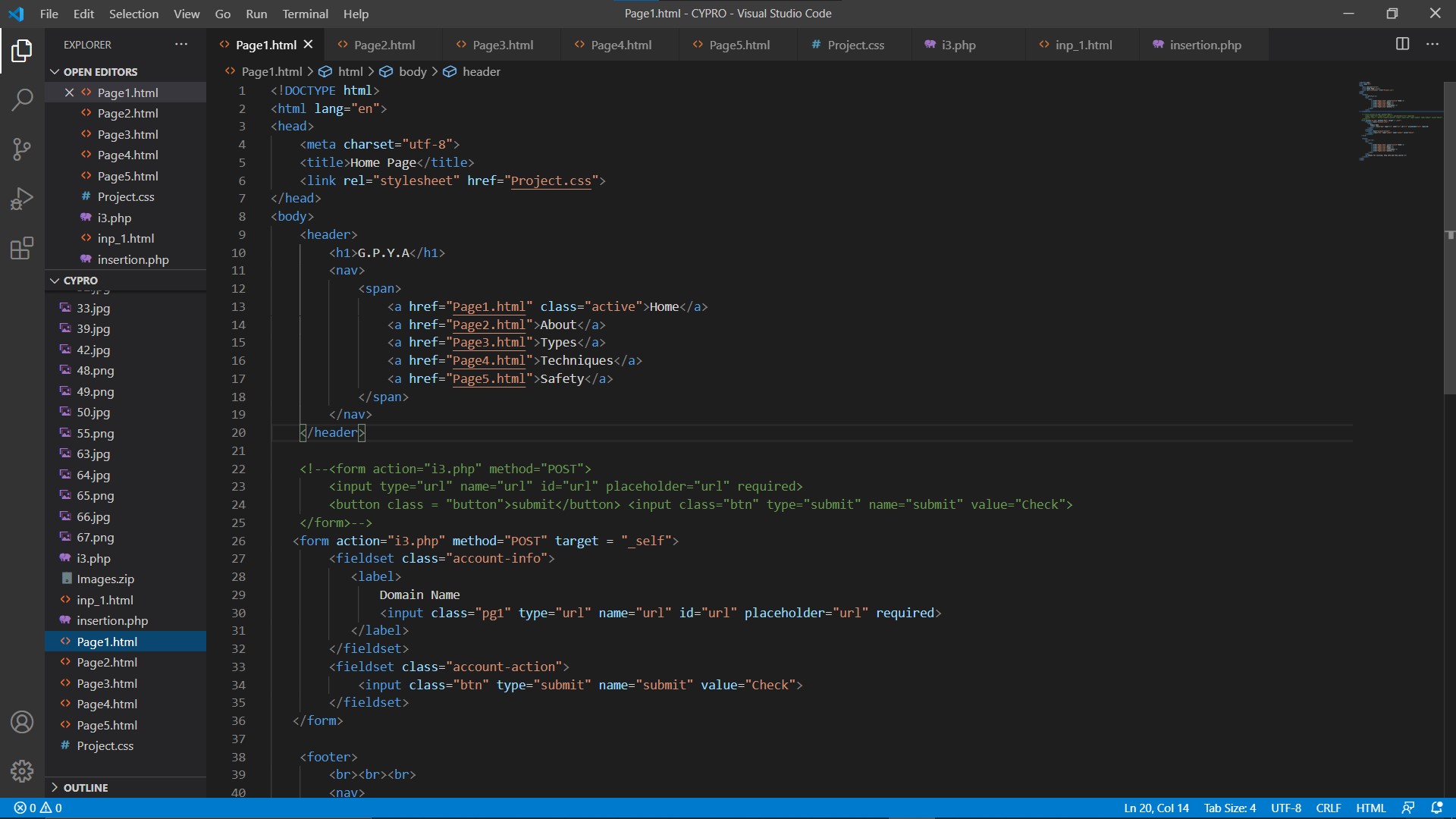


**3.5 Evaluation:** Once all prior stages have been completed, it is time for a thorough evaluation of development up to this stage. This allows the entire team, as well as clients or other outside parties, to examine where the project is at, where it needs to be, what can or should change, and so on. We have done the evaluation before the final presentation of the project.

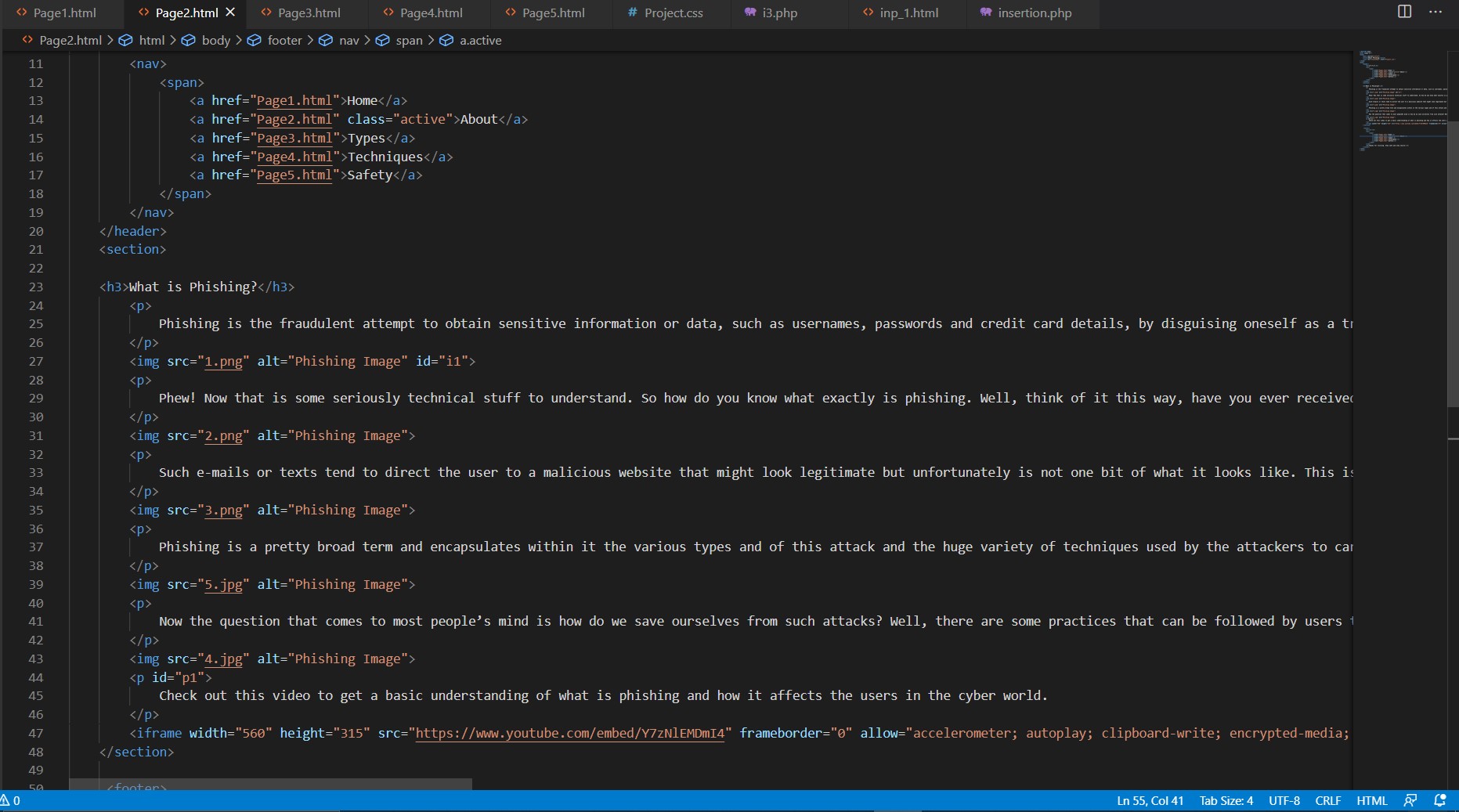
**4. WORK DONE**

**4.1 Web Pages Using HTML**

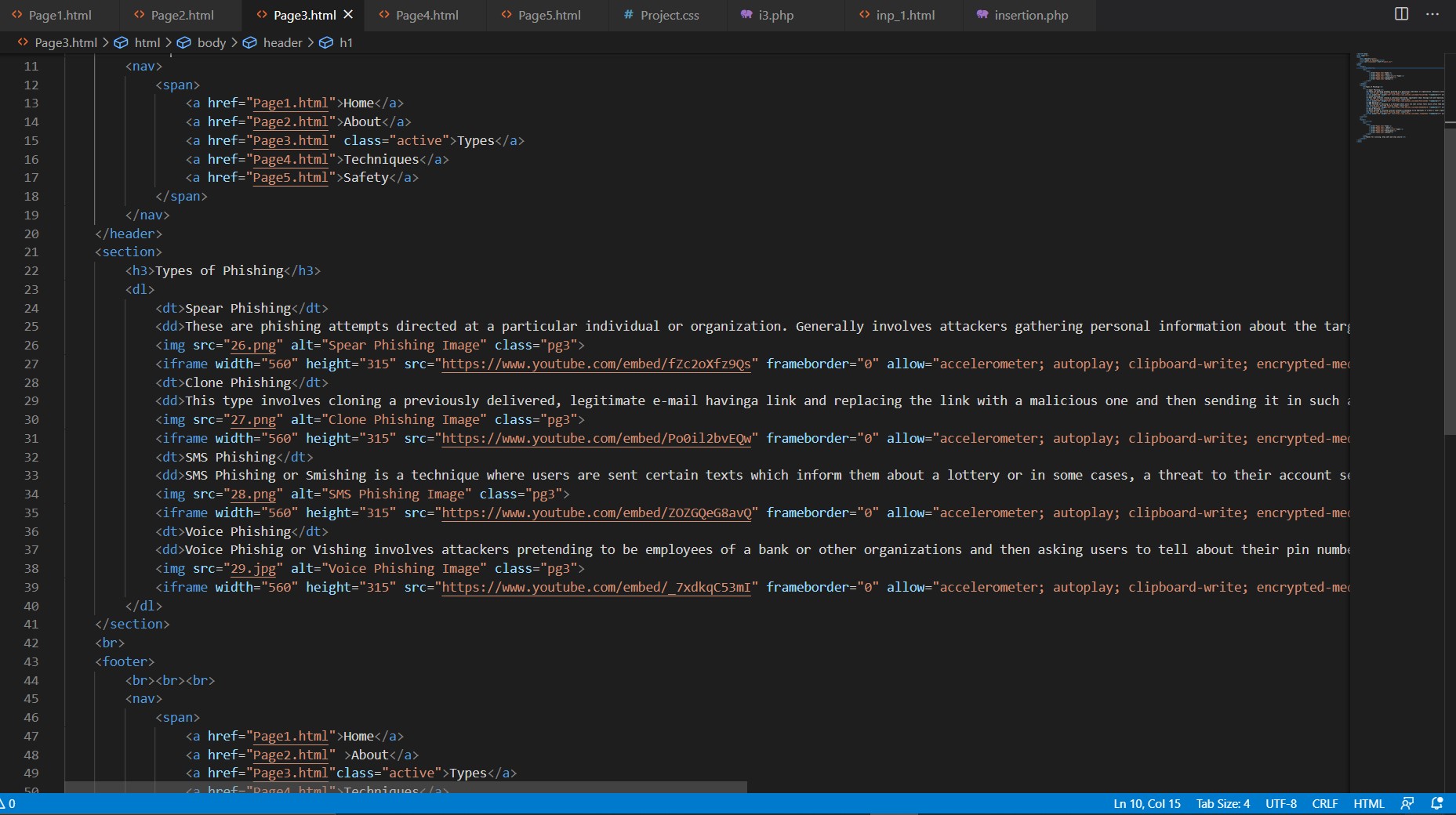
Our first task was to develop the structure of our web page using html. This would include pages about phishing 's types and techniques as well as safety precautions for the users to read from along with the main page for checking the authenticity of the URL entered by the users.



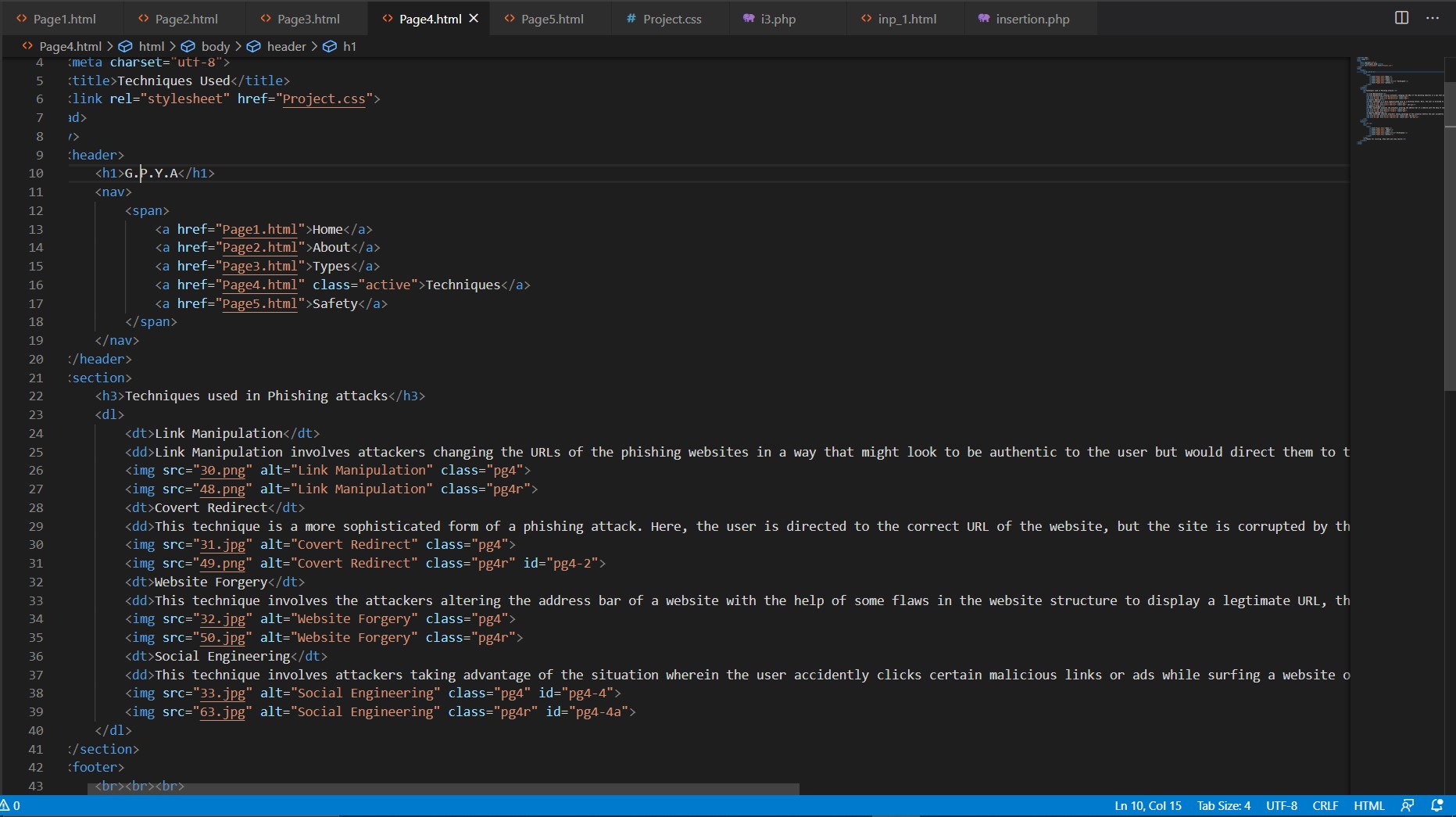
Html Page1 sample code



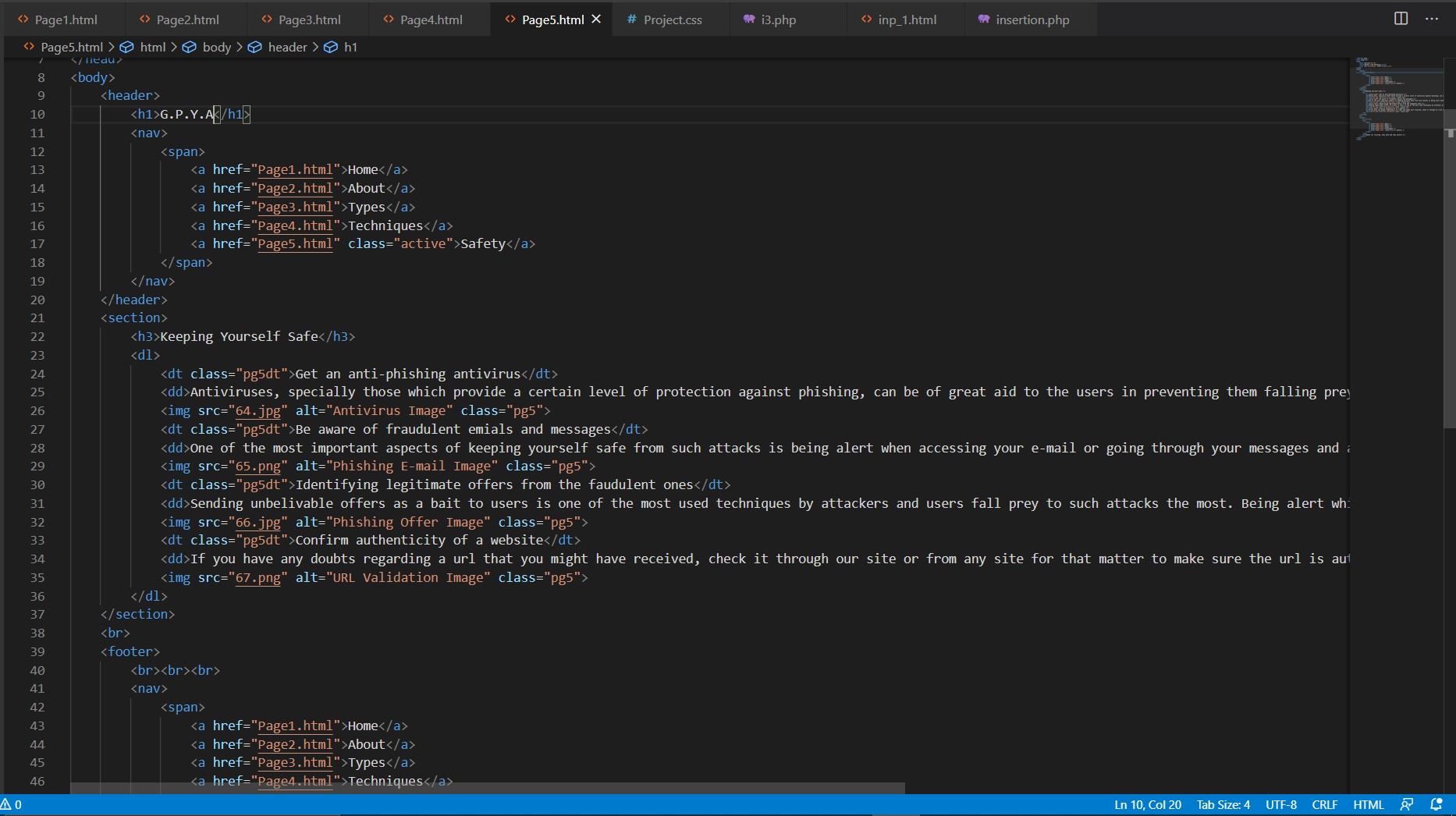
HTML Page 2 Sample-code



HTML Page3 Sample-code



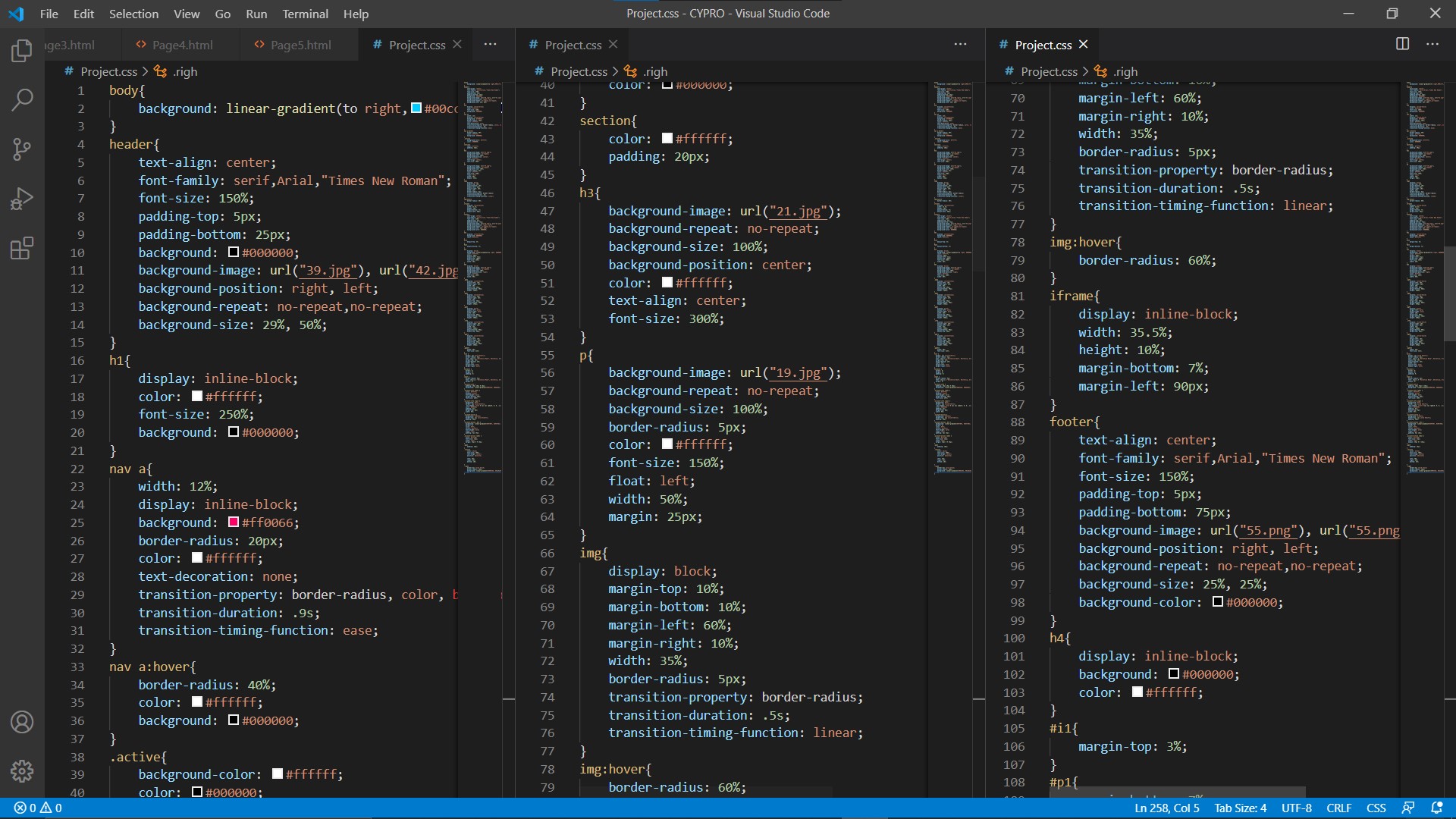
HTML Page4 Sample-code



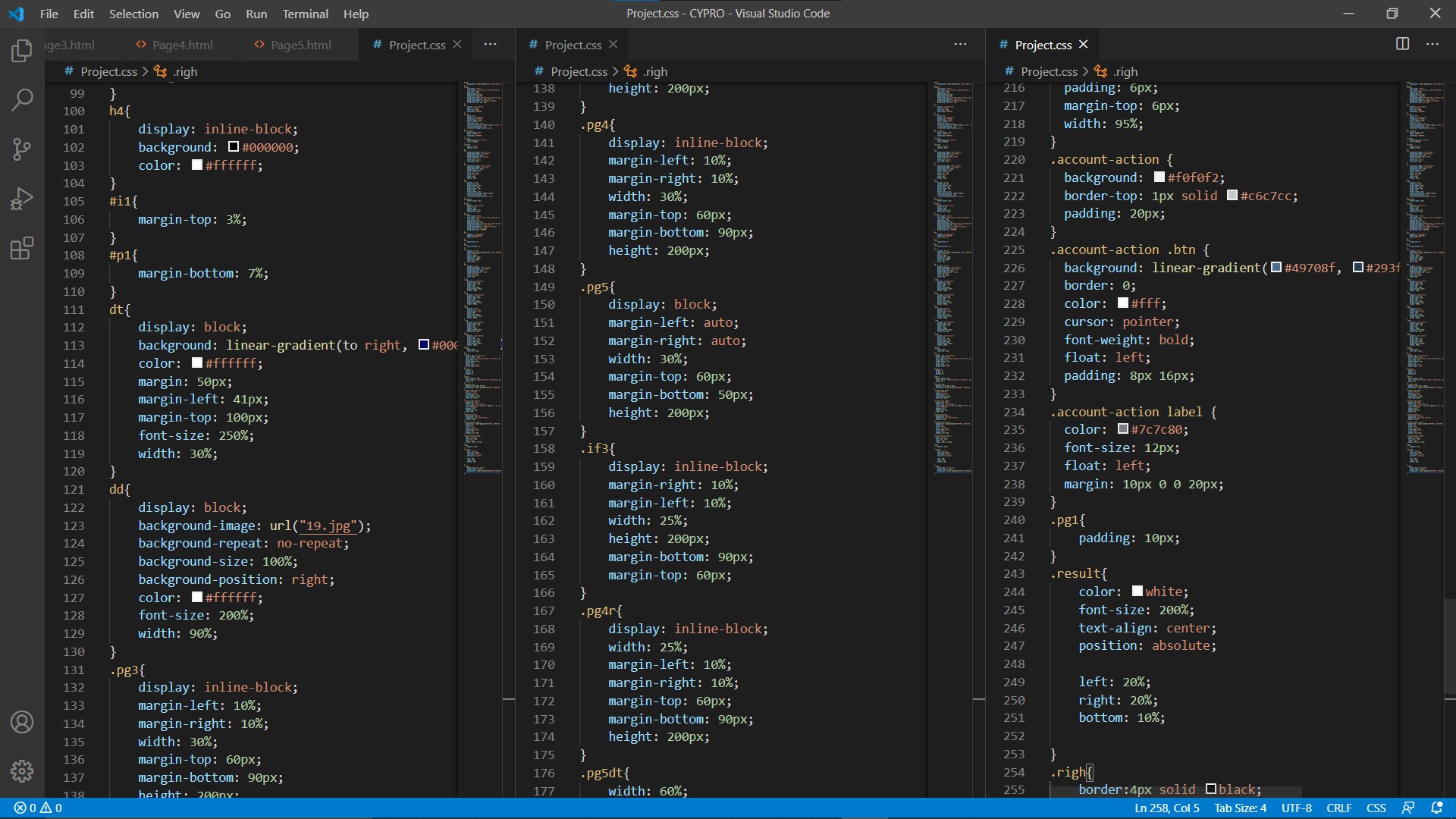
HTML page5 Sample-code

**4.2 - CSS for Designing**

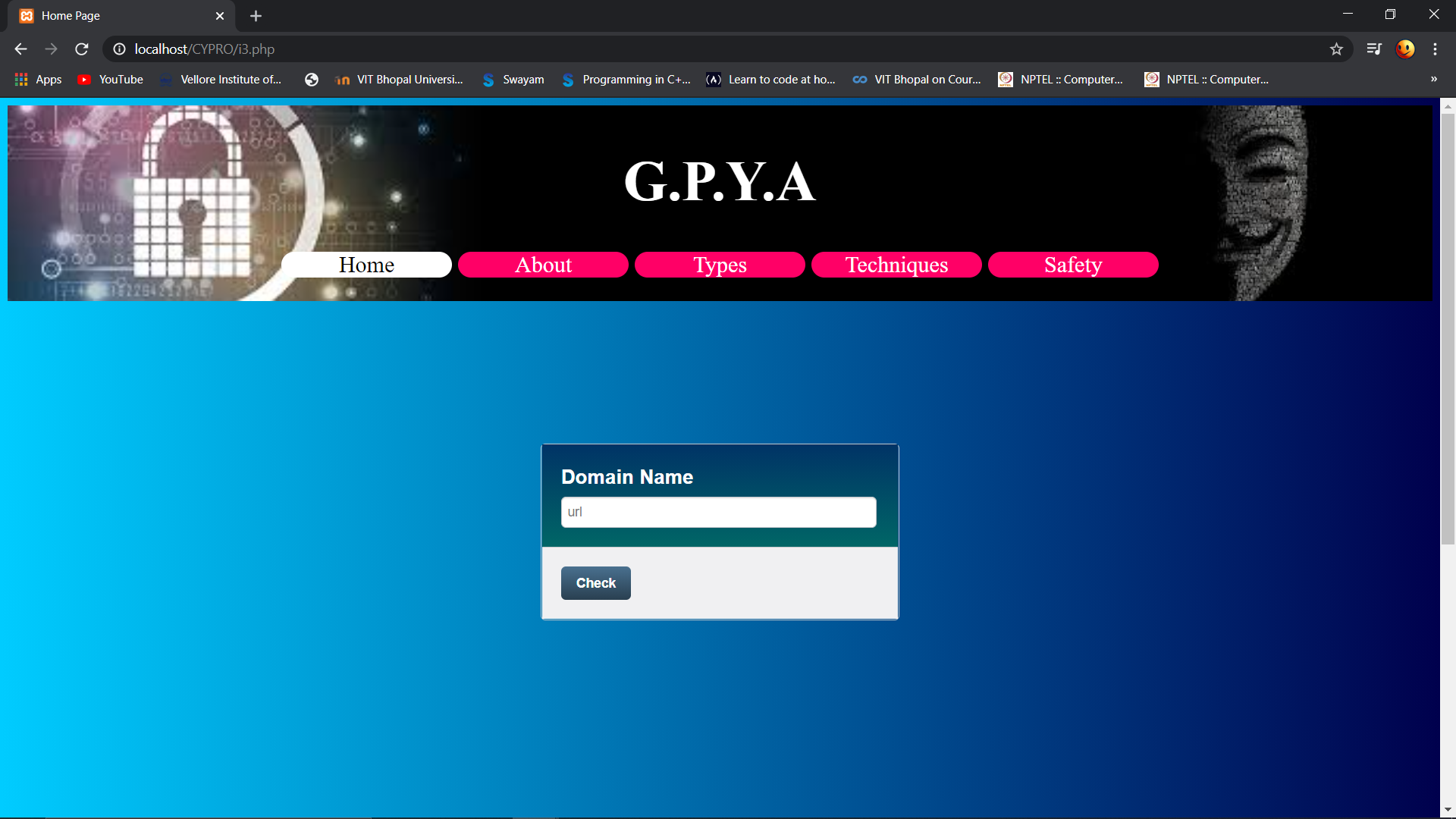
Our next task was to design our website and give it the proper aesthetics using the CSS software and including the proper transitioning and interactivity for the user to feel good while using our website.



CSS Page1 Sample-code



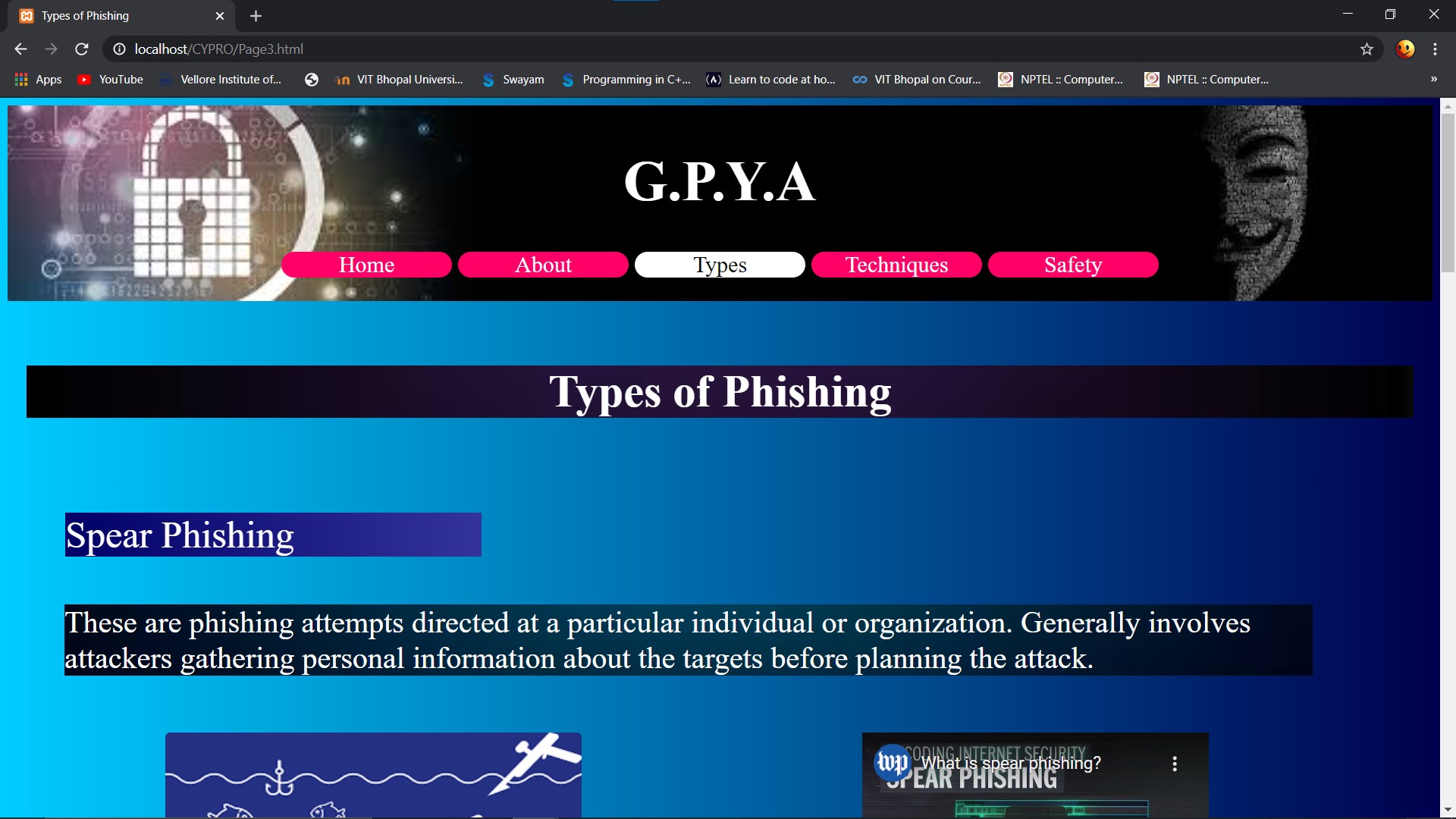
CSS Page2 Sample-code



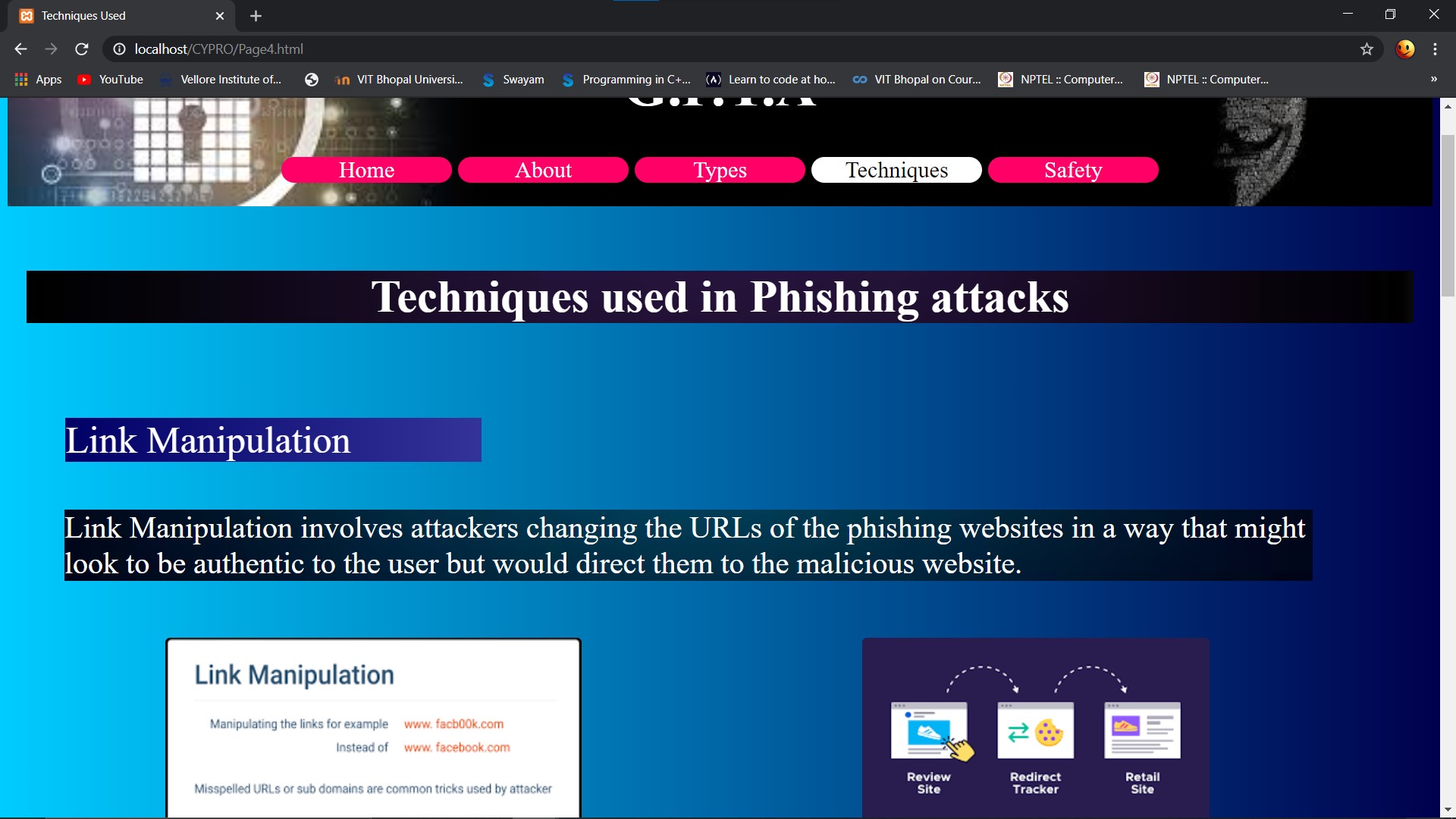
WEB Page Home tab



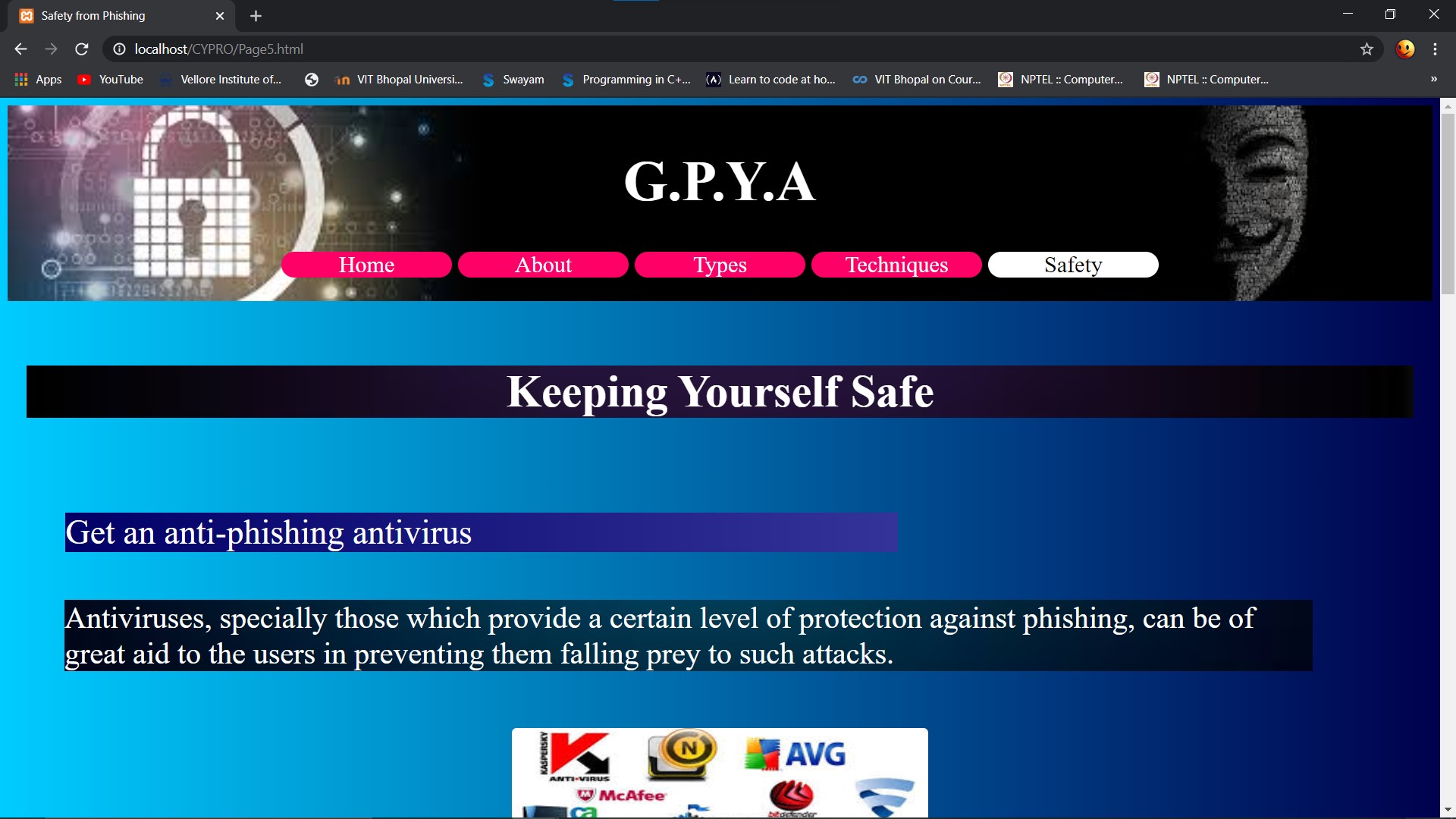
WEB Page2 About



WEB Page3 Types



WEB Page4 Techniques

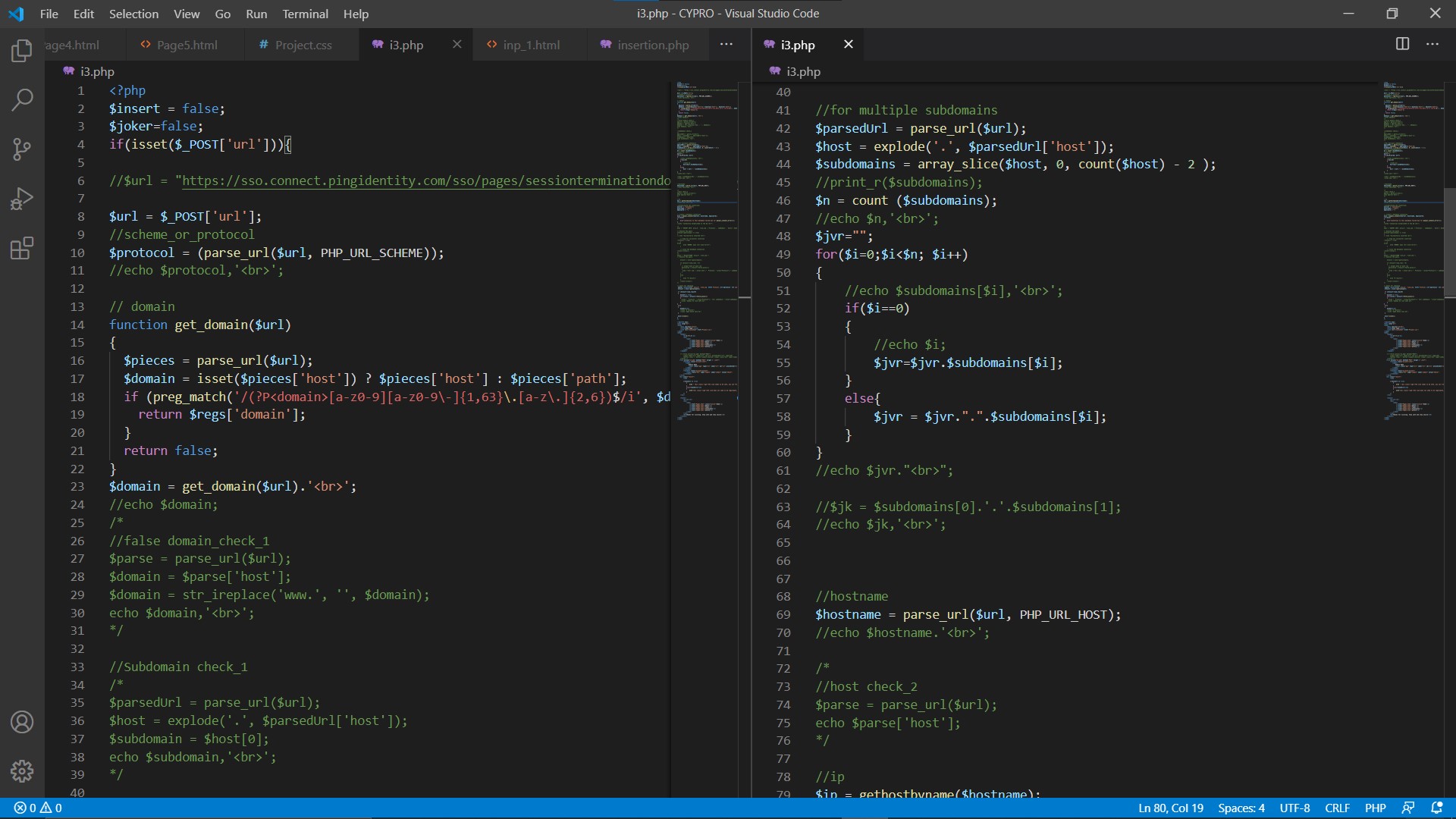


WEB Page5 Safety

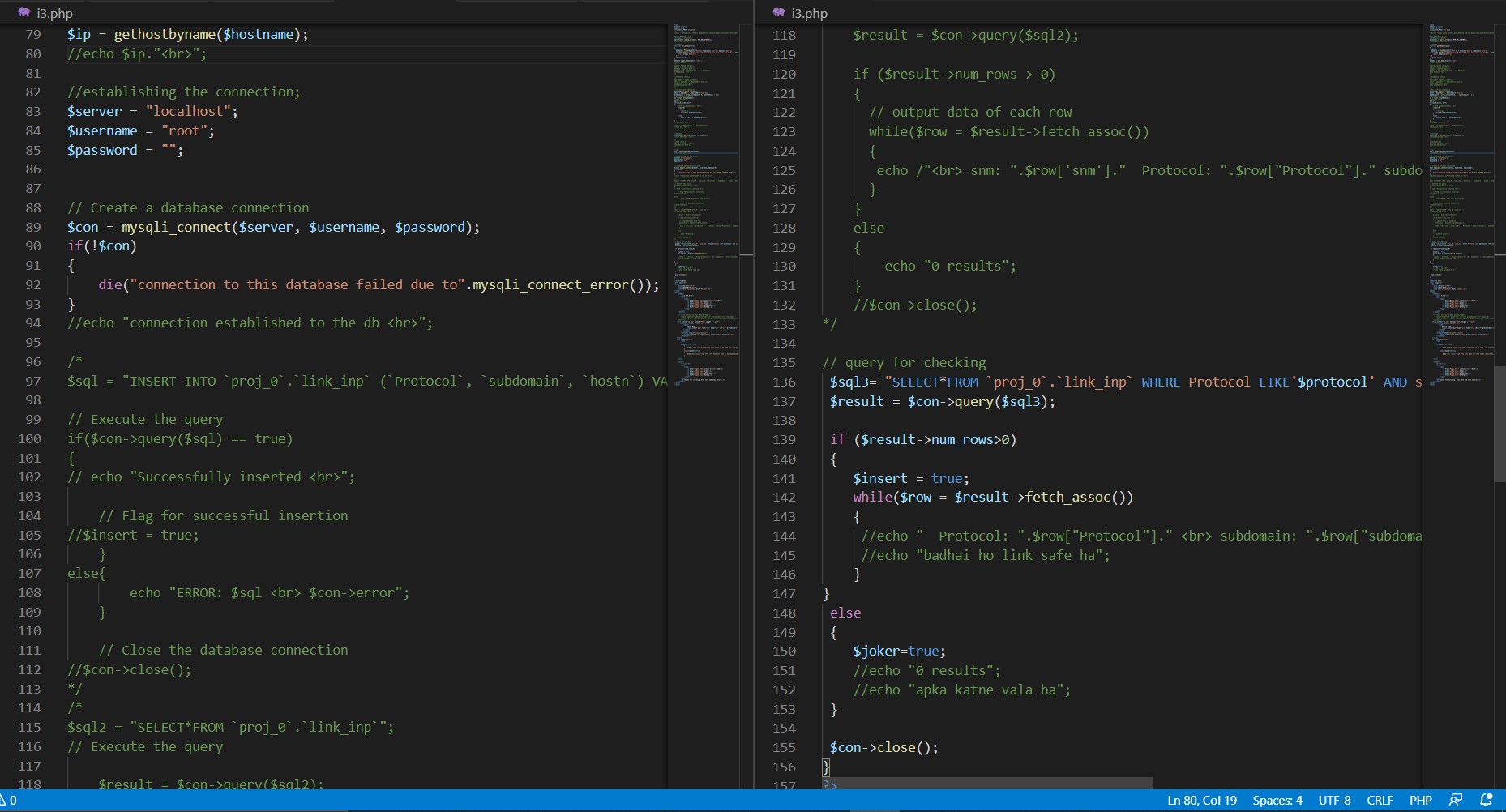
**4.3 - PHP for Database and connecting the different aspects of the project**

Our final task was to create a database of the legitimate URLs for our website to check from. We then connected the database with our website to finally implement

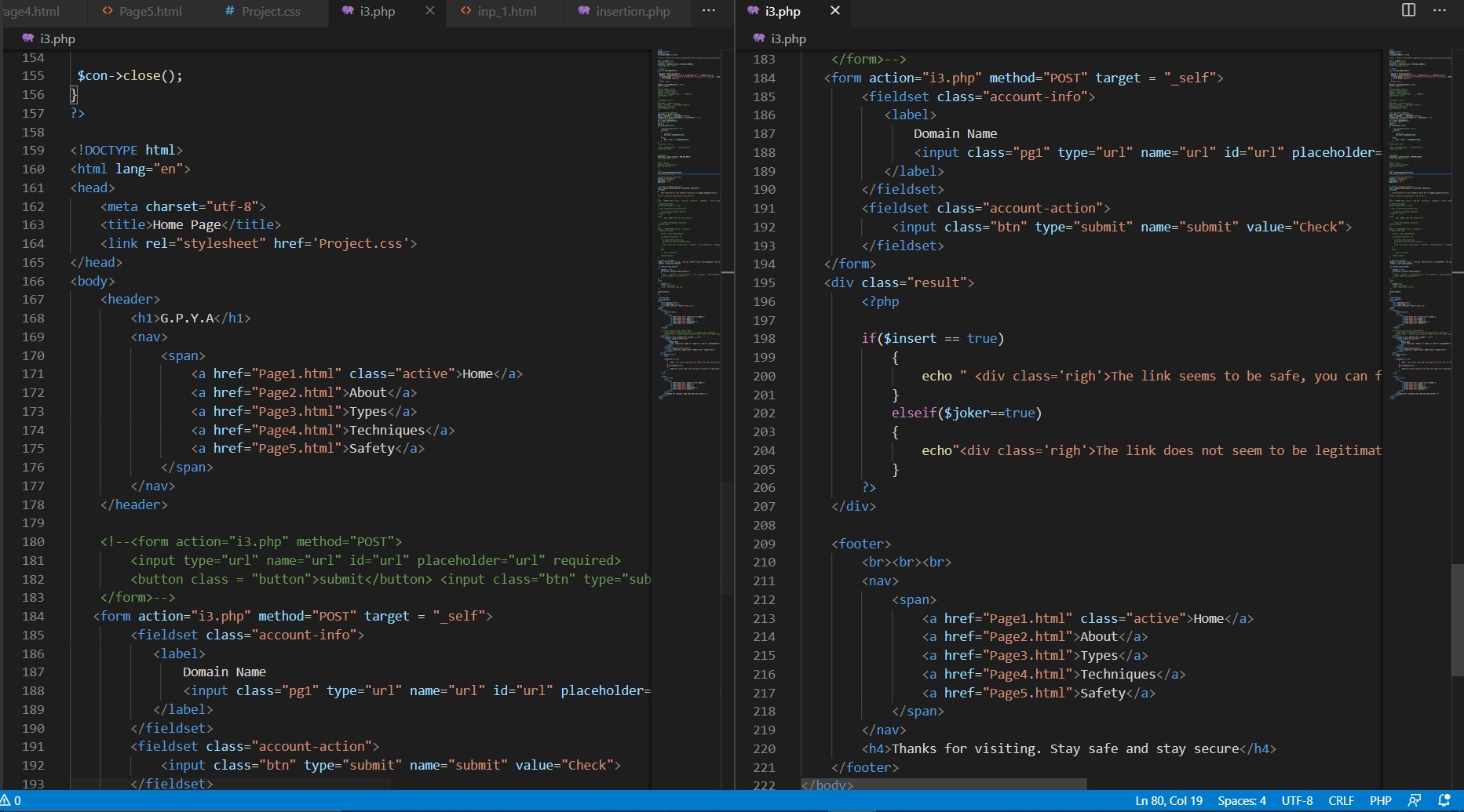
the idea of our project and used PHP for the same.



PHP Page1 Sample-code



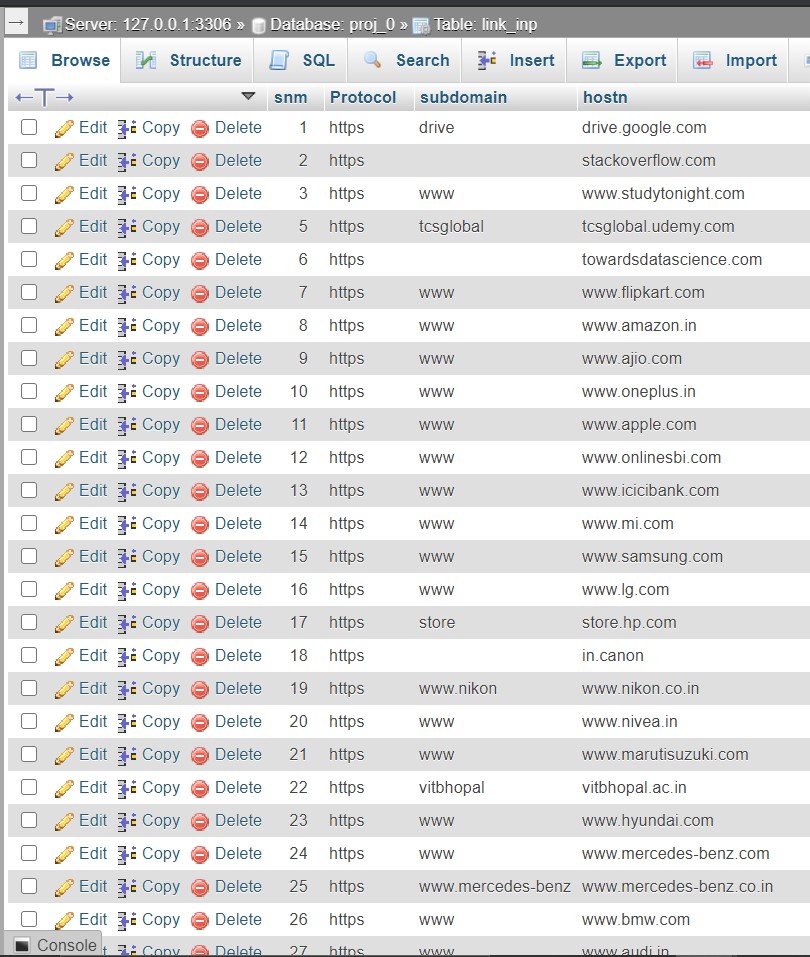
PHP Page 2 Sample-code



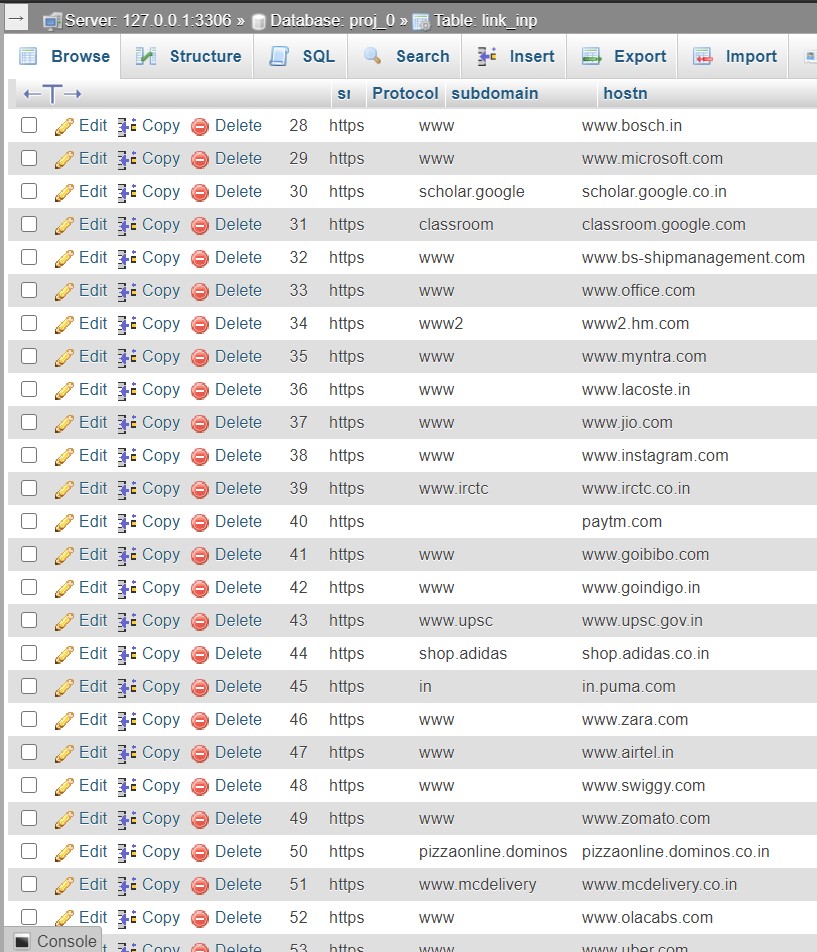
PHP Page3 Sample-code

**4.4 - Database entries using XAMPP**

We finally created a database using XAMPP to make a list of legitimate websites.We went to these particular websites and procured the completely legitimate and verified links for our websites. Then we had a complete breakdown of the particular links into some particular field that helped us to follow some observed patterns and then with the help of this , we ensured the legitimacy of the links. Although we plan to expand our database on a huge level so that it would contain more and more popularly visited websites.This Database acts as a base of our project as it contains the list of legitimate links.The links entered to the website are checked for their presence in our website, Only after its presence is confirmed.



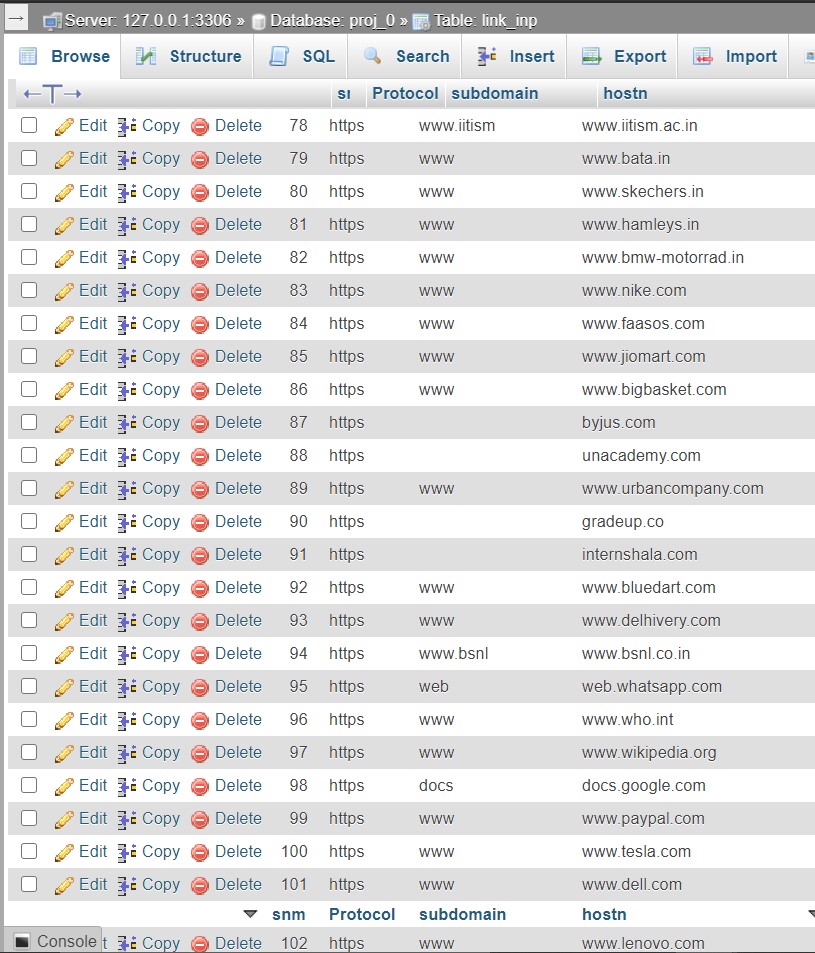
Data Set 1



Data Set 2



Data Set 3



Data Set 4

**5. OBSERVATION**

The requirements for a project are distinguished after the association mentions objective facts about the project. Perceptions are regularly theoretical and along these lines somebody with mastery about the proposed undertaking should assist with mentioning objective facts. A decent observer can distinguish the necessities of the undertaking by addressing key inquiries regarding the venture. In the event that the perceptions mull over the task itself and the result of the undertaking, the perceptions should address the entirety of the issues of the venture.

In the end of the project, it can be observed that we have successfully implemented the prototype of the project, which is actually a website which helps the users to check the authenticity of a URL and displays the results in as simple a way as possible. The project was based on the concepts of HTML, CSS and the PHP languages and using a database connected with a website in order to check the authenticity of a URL and prevent themselves from falling prey to phishing attacks.

As soon as the user gets to our website , first he is provided with ample information about the threats that he is put into if he clicks on unidentified links. Not only he is made aware of the threats but he is also given with sufficient information about how to combat this situations and prevent them to occur on a regular basis.The homepage of our website provides a text box which asks the user to enter the suspected link so that our website could check of its legitimacy.As soon as the user enters the link and clicks on the check button right below , He is notified of the legitimacy of the link in a very simple language and the user gets aware about it without even being indulged to the complexities.This helps him have a peace of mind and that is what we aim at. Harmful websites could be identified right befor clicking on it cutting off the possibilities of any kinds of damage it can cause.

**6. CONCLUSION**

So finally we would like to conclude our project. We found it as quite an opportunity to gain some really useful skills which is sure to help ourselves in future.Our main motive is to make internet a safer place to be in for people ranfging from naive users to professionals.We tried with our little efforts that we make it safer for people and help them combat from getting themselves into such kind of situations.

There are plenty of examples where people have been ripped off their total life savings just because they were not aware of the complexities that come with particular field. Certainly they are not the only ones responsibles and the price they paid was quite huge. This was a little effort from our side that we ensure no other person fall prey to such kind of practices.It is also very important for people to feel safe while they spend their time online and that the job of cyber warriors like us to provide them with peace of mind.

I really hope that you would like the efforts that we had put in and I would like to thank our mentor for the same for appreciating and motaivating us throughout.

THANKS!

**7. RECOMMENDATION FOR FUTURE WORK**

So today privacy has become one of the prime concern for both the governmental or private institutions and one of the prime methods used to compromise on data is none other than phishing, and our motive was to protect people to fall prey to such kind of malpractices. We tried to reflect the same using this opportunity to make this situation more and more better

Certainly we have future plans for the particular website.We plan to expand our database so that it could dtecet morte and more of legitimate links and will also try to take some help of machine learning in the process..As to make it more and more reachable as well as usable for the general people, we will try to put as a extension to browsers so the link could be checked as soon as the user enters it and then it will check for the link legitimacy.This will definataly help in providing people with more and more security online as well as they will be aware about the threats they possess.

Also we need will try to make an app which will try to monitor the links that a user gets via sms so that it can be identified as soon as it comes to the reach of the user and the link can be a checked for its legitimacy .This will automatically ensure that people will be well aware of the links they receive via sms

**8. REFERENCES**

1. <https://www.namecheck.com/phishing-check/> For examples of phishing links.
2. <https://towardsdatascience.com/phishing-domain-detection-with-ml-5be9c99293e5> .
3. <https://nevonprojects.com/detecting-phishing-websites-using-machine-learning/> .
4. <https://www.kaggle.com/akashkr/phishing-website-dataset> .
5. <https://www.w3schools.com/php/> For PHP.
6. <https://www.w3schools.com/html/> For HTML.
7. <https://www.w3schools.com/css/> For CSS.
8. <https://chamanthmvs.github.io/Phishing-Website-Detection/> .
9. <https://www.ijert.org/a-review-paper-on-detection-of-phishing-websites-using-machine-learning> .
10. <https://www.researchgate.net/publication/324999540_Detection_of_phishing_attacks> research papers.