



EVALUATION OF INTERNSHIP REPORT

B.Tech: III Year

Department of Computer Science & Information Technology

Name of the Student :- Nilesh Panchal

Branch & section :-CSIT-2

Roll No:-0827CI201121

Year:- 2022-23

Department of Computer Science & Information Technology

AITR, Indore

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

Certificate

Certified that training work entitled Cyber Security is a bonafied work carried out after sixth semester by Nilesh Panchal in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from Mr. Yash Arya Acropolis Institute of Technology and Research during the academic year 2022-23.

Name and Sign of Training Coordinator

Name & Sign of Internship Coordinator

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

ACKNOWLEDGEMENT

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training coordinator, Mr. Yash Aarya , CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

Nilesh Panchal

0827CI201121

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

INDEX

S.no	CONTENTS	Page no
1.	Introduction to technology Undertaken.....	1
2.	Objectives	2
3.	Project undertaken 4	
4.	Screenshots of Project and Certificates.....	4
5.	Github Links (Project/certificate/video/copy of report.... ..)	10
7.	Conclusion.....	10
8.	References/ Bibilography.....	10

INTRODUCTION

~Phishing

Social engineering attack is a common security threat used to reveal private and confidential information by simply tricking the users without being detected. The main purpose of this attack is to gain sensitive information such as username, password and account numbers. According to, phishing or web spoofing technique is one example of social engineering attack. Phishing attack may appear in many types of communication forms such as messaging, SMS, VOIP and fraudster emails. Users commonly have many user accounts on various websites including social network, email and also accounts for banking. Therefore, the innocent web users are the most vulnerable targets towards this attack since the fact that most people are unaware of their valuable information, which helps to make this attack successful.

Typically phishing attack exploits the social engineering to lure the victim through sending a spoofed link by redirecting the victim to a fake web page. The spoofed link is placed on the popular web pages or sent via email to the victim. The fake webpage is created similar to the legitimate webpage. Thus, rather than directing the victim request to the real web server, it will be directed to the attacker server. The current solutions of antivirus, firewall and designated software do not fully prevent the web spoofing attack. The implementation of Secure Socket Layer (SSL) and digital certificate (CA) also does not protect the web user against such attack. In web spoofing attack, the attacker diverts the request to fake web server. In fact, a certain type of SSL and CA can be forged while everything appears to be legitimate. According to, secure browsing connection does virtually nothing to protect the users especially from the attackers that have knowledge on how the “secure” connections actually work. This paper develops an anti-web spoofing solution based on inspecting the URLs of fake web pages. This solution developed series of steps to check characteristics of websites Uniform Resources Locators (URLs).

OBJECTIVE

PYTHON:

In technical terms, Python is an object-oriented, high-level programming language with integrated dynamic semantics primarily for web and app development. It is extremely attractive in the field of Rapid Application Development because it offers dynamic typing and dynamic binding options.

Python is relatively simple, so it's easy to learn since it requires a unique syntax that focuses on readability. Developers can read and translate Python code much easier than other languages. In turn, this reduces the cost of program maintenance and development because it allows teams to work collaboratively without significant language and experience barriers.

Additionally, Python supports the use of modules and packages, which means that programs can be designed in a modular style and code can be reused across a variety of projects. Once you've developed a module or package you need, it can be scaled for use in other projects, and it's easy to import or export these modules.

One of the most promising benefits of Python is that both the standard library and the interpreter are available free of charge, in both binary and source form. There is no exclusivity either, as Python and all the necessary tools are available on all major platforms. Therefore, it is an enticing option for developers who don't want to worry about paying high development costs.

That makes Python accessible to almost anyone. If you have the time to learn, you can create some amazing things with the language.

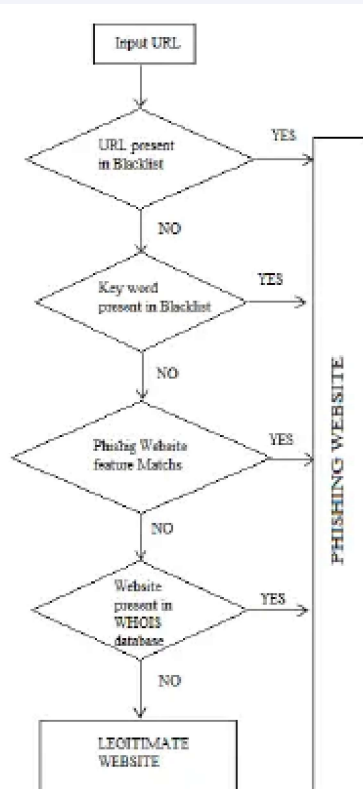
Python is a general-purpose programming language, which is another way to say that it can be used for nearly everything. Most importantly, it is an interpreted language, which means that the written code is not actually translated to a computer-readable format at

runtime. Whereas, most programming languages do this conversion before the program is even run. This type of language is also referred to as a "scripting language" because it was initially meant to be used for trivial projects.

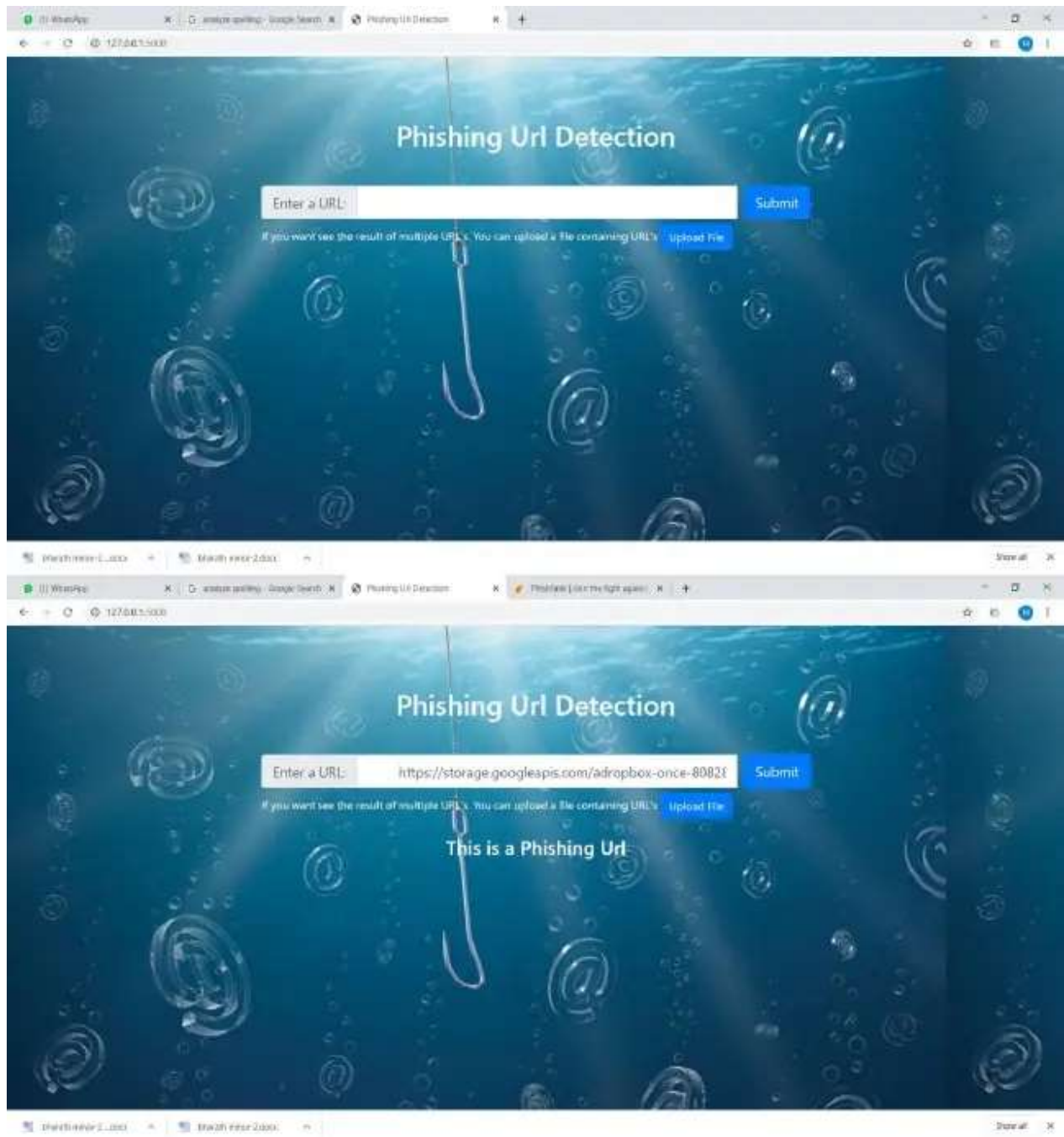
WHOIS

The life of phishing site is very short, therefore; this DNS information may not be available after some time. If the DNS record is not available anywhere then the website is

phishing. If the domain name of the suspicious webpage is not match with the WHOIS database record, then webpage considers as phishing.

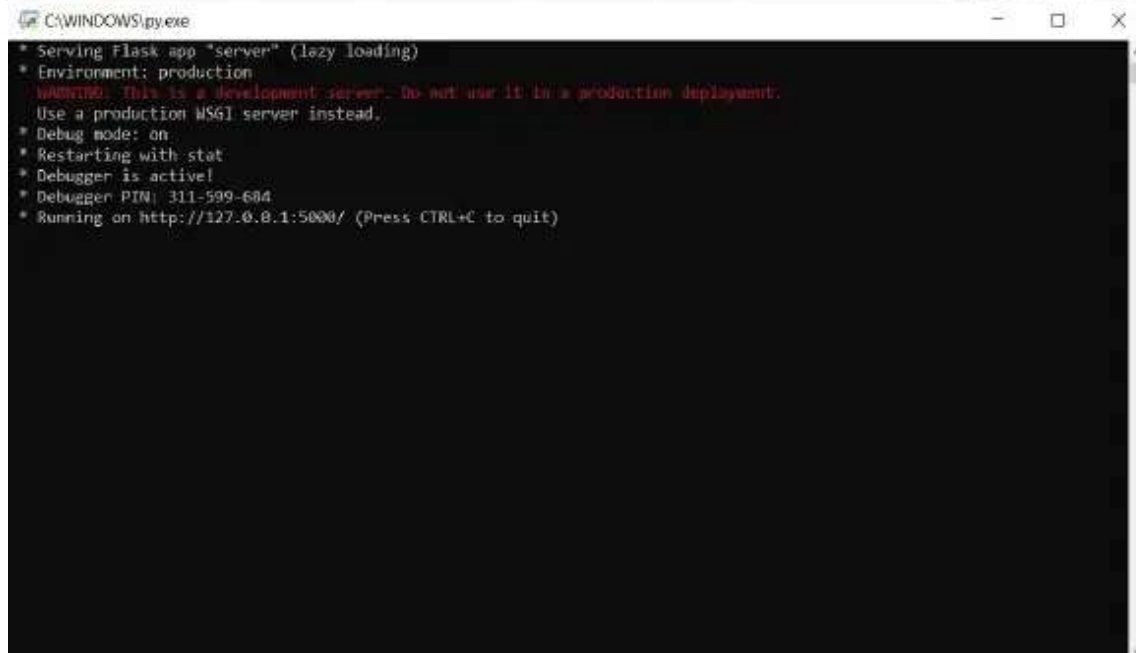


Screenshots:

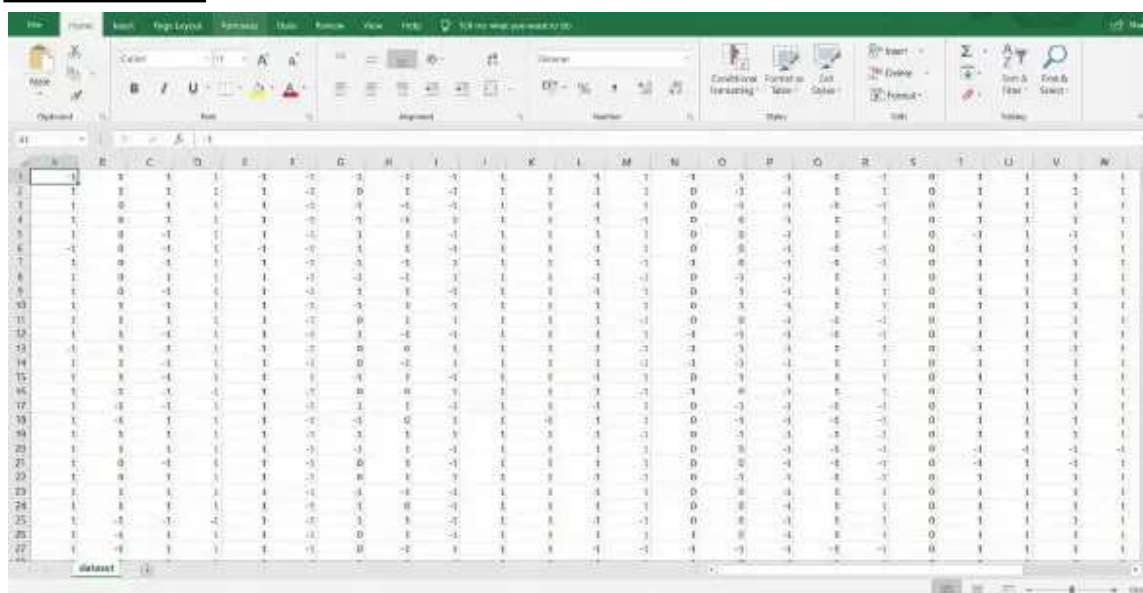


OUTPUT_ILLEGITIMATE URL

SERVER RUNNING




DATASETS:



CERTIFICATE

FORTINET®
Training Institute

This acknowledges that
Nilesh Panchal
successfully completed the course
Information Security Awareness



Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: July 27, 2022

FORTINET®
NSE Certification
Program

This certifies that
Nilesh Panchal
has achieved
NSE 1 Network Security Associate



Date of achievement: July 27, 2022

Valid until: July 27, 2024

Certification Validation number: XAamBGM8b5



Ken Xie
CEO of Fortinet



Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php



Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

GITHUB LINK:

[Nileshpanchal1494 \(github.com\)](https://github.com/Nileshpanchal1494)

CONCLUSION

Phishing is a technique to gather sensitive information about the target using malicious links and emails. It is one of the most dangerous cyber-attacks that occurs in organizations, personal devices, etc. It is often difficult to distinguish between genuine emails and phishing emails. There are several methods that can be used to avoid this attack. Periodical updating of anti-phishing tools and platforms can prove to be very powerful. This study provides an in-sight to phishing, the mechanism of the attack, various forms it can occur in and the possible solutions to overcome them.

REFERENCE

- www.security.net
- www.google.com
- www.youtube.com