**PES UNIVERSITY**



A Project Report on

*“Tracking user details from an insecure website using HTTP”*

Submitted by:

* **Name (SRN) Nikshitha SV(PES2UG19EC087)**
* **Name (SRN) Mansoora S(PES2UG19EC070)**
* **Name (SRN) Nikhita Sridhar (PES2UG19EC086)**

Under the guidance of:

**Dr. PRAMOD M S**

**Associate Professor,**

**Department of Electronics and Communication Engineering**

**PES UNIVERSITY**

Electronic City, Bangalore-560100

2021 - 2022

**ABSTRACT**

Cyber attacks have increased rapidly at present. It is indeed very necessary for users to make a choice between secure and insecure website. Logging into an insecure website might lead to loss of personal data. It is also getting harder to successfully detect a cyber crime on network level due to increasing volume and encryption of network traffic and growing ubiquity of high-speed networks. Therefore, it is very essential for the user to know about the security details of the website they are logging into. This project is demonstrated to show the attack or hacking of our personal data from a malicious website using HTTP and how it is very secure to use HTTPS websites. The software used to carry out the above demonstration is Wireshark.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO** | **TITLE** | **PAGE NO.** |
| **1.** | **INTRODUCTION**   * 1. BACKGROUND   2. MOTIVATION   3. OBJECTIVE | 3  3  3-4  4 |
| **2.** | **LITERATURE SURVEY** | 5 |
| **3.** | **METHODOLOGY** | 6 |
| **4.** | **IMPLEMENTATION** | 7-9 |
| **5.** | **RESULT** | 10 |
| **6.** | **CONCLUSION** | 11 |
| **7.** | **REFERENCES** | 12 |

**CHAPTER 1**

**INTRODUCTION**

Internet users must check whether a website with different interfaces is safe enough to enter their personal information. While web browsing, users use many new websites or seemingly safe and familiar ones. Mistyped URLs or search engine links can direct users to potentially malicious websites. Modern web browsers provide security indicators to prevent this, but the technical details of these indicators are understood only by a few users. Therefore, the user’s knowledge about logging into a website which may be secure or insecure is very essential.

* 1. **Background**

Modern web browsers use security indicators, however users often fail to utilize them, and may unknowingly share their personal information on insecure websites.

Today, many of the web browsers use HTTP [Hypertext transfer protocol] as a common website protocol. HTTP acts as the foundation for any data exchange on the web, and it is a client- server protocol. Client and server communicate by exchanging individual messages with each other. The messages sent by the client are called requests and messages sent by the server are called responses. Between the client and the server there are numerous entities known as proxies which perform different operations and act as gateways or caches. HTTP is a great language for computers but it is not encrypted. So, it is very easy for hackers to hack into a website and fetch all the details of the user. Therefore, an extension of HTTP called HTTPS [Hypertext transfer protocol secure] is used. HTTPS is encrypted using secure socket layers. HTTPS helps us to prevent websites from having their information broadcasted in a way that is easily understood by anyone snooping on that particular network. When information is sent over HTTP, its broken into packets of data that can be easily sniffed using a free software making the communication insecure. With HTTPS, traffic is encrypted in such a way that even if the packets are sniffed, no valuable information is returned.

Checking whether a website is secure or insecure can be done using several software. In this project we are using Wireshark as our software. Wireshark is a software which is widely used as a network protocol analyzer. It is a go to network packet capture tool. It captures network packets and displays them at a granular level. Once the packets are broken down, they can be used for real time analysis. Wireshark performs packet capture, filtering and visualization. So, this software is used to show how the details of the user can be hacked on an insecure website.

* 1. **Motivation**

Security in the online world becomes more important every day. At present due to forwarding technology the number of attacks on the web has increased rapidly and the number of insecure usernames and passwords that are being used give attackers more chance of success. This could cause personal or financial losses due to leakage of data. Users often fail to make an attempt to understand whether the website in which they are logging into is secure or not. This significantly adds to the number of cyber-crimes happening around the world. These crimes have led to more dangerous events like life threats, financial loss or reputational damage- for instance, Travelex [foreign exchange company] is facing demands for payment to decrypt all the important work files after it was hit by Sodinokibi (Sophisticated ransomware attacks ) which disabled its IT systems on New Year’s Eve.

All these causes huge stress on users mentally. Therefore, users must know about the security of the website before they are logging into a website and avoid logging into random, malicious websites.

* 1. **Objective**

The main objective of this project is to create awareness among users about tracking of user details from an insecure website under HTTP using Wireshark.

**CHAPTER 2**

**LITERATURE SURVEY**

A packet sniffer collects all the data frames from data-linking layers moving via the network adapter of a system. They are used to catch all the incoming and outgoing traffic for further analysis. According to Dr. Dayanand, Mr. Parikshith, Mrs. Veena, Dr. Brahmananda and Mrs. Sahana, the data provided by these packet sniffers like Wireshark and TCP dump , is very large and finding the required details can be hard and suggest using a packet sniffer for secret credentials. They stated that upon reviewing some of the problems from a diverse range of internet backgrounds, they found that http protocol is excessively used in Nepal’s internet space for transferring web credentials (Shodan, 2019) and that majority of end users do not know basic concepts about ssl and encryption. Using a traditional tool like Wireshark, we were able to extract the user details very easily from a basic site that uses HTTP. With advance software that can sniff secret credentials like the one mentioned by Dr. Dayanand and et al, extracting user details will be made even easier if the data is not well protected.

Kelley, Timothy, and Bennett performed a new Two-Alternative Forced Choice experiment to assess the effects of security indicators on participants' decision-making when detecting potentially unsafe websites. Participants were encouraged to browse a succession of secure and insecure websites and determine whether or not it was safe to connect as quickly and precisely as possible using Amazon's Mechanical Turk. To correctly discern between secure and insecure websites, hierarchical linear regression models were used to determine the impact of the presence of security indicators, security domain knowledge, and familiarity with the given websites. The way websites were searched before a decision was assessed via a study of participants' mouse movements. Security domain expertise and website familiarity both influenced the likelihood of logging in. Spoofed websites with security signs resulted in less searches on the website, according to mouse tracking data, as seen by Kelley, Timothy, and Bennett. This implies that it is very necessary to be aware as well as responsible with your choices to avoid loss of personal information.

According to Mohammed, Degadzor, Effrim, and Appiah, Brute force attacks are widely being used by hackers these days using various algorithms to find the perfect combination of username and password. When an incorrect password is entered, FTP servers respond with a specific response code ‘530’. Wireshark filter can be used to track those packets which have the specific FTP code. Using this we get to know the information about the number of login attempts made by the specific IP address, which helps in analysing brute force attack. According to Mohammed and et al, end point security can be used to prevent these attacks. It also becomes imperative for people to understand the security risks before entering sensitive data on public sites.

**CHAPTER 3**

**METHODOLOGY**

Tracking of user details from an insecure website can be done using Wireshark which is an opensource packet analyzer, its main objective is analyzing traffic and communications and resolving network problems.

Insecure websites can be identified by the protocols ‘HTTP’ and ‘HTTPS’. Websites having the URL starting with the header ‘HTTP’ are insecure and websites having the URL starting with the header ‘HTTPS’ are secured. The ‘s’ in ‘HTTPS’ stands for ‘secured’.

Wireshark uses different range of filters to facilitate the definition of search criteria. Tracking user details can be done using the Wireshark filter ‘HTTP’. Adding this in the Wireshark filter window filters out only the HTTP packets. Further, to get the exact packets with the login details, modifying the filter to ‘http.request.method==”POST” ’, gives only the packets with that contain login details as the HTTP protocol uses POST method.

HTTP ‘POST’ method is used to send data from the client to the server. This method requests the server to accept the data enclosed in the post message. POST method is generally used while submitting login details or while uploading files and images to the web server.

**CHAPTER 4**

**IMPLEMENTATION**

1. Open Wireshark

2. Start Packet Capture

3. Enter the URL of insecure website

Fig 2.1 Steps of packet sniffing

5. stop Packet capture

4. Enter the Login details

1. Enter the ‘http.request.method==”POST”’ filter

2. Right click on the packet listed containing login details

3. Click on follow

4. Then click on “TCP Stream”

5. A description window opens that contains the login details username and password

Fig 2.2 Steps for Analysis

Figure 2.1 explains the steps used to retrieve the username and password from an insecure website and is as follows:

For capturing the packets of the traffic, open Wireshark packet sniffing window. Start Wireshark packet capture, then enter the URL of the insecure website in the web browser. After the login page opens enter the username and password and click on login, then stop packet capture in Wireshark.

Figure 2.2 shows the analysis and checking of the user details entered and is as follows:

Enter the ‘HTTP. request.method==”POST”’ filter in the filter describing window in Wireshark. Right click on the packet listed that contains the login details, then click on “follow” 🡪 “TCP Stream”. A description window opens with the user details showing username and password (As entered in the login page previously).

**CHAPTER 5**

**RESULTS**

When the analysis is run, the username and password entered in an insecure website such as <http://testphp.vulnweb.com/login.php> which uses the HTTP protocol, is retrieved very easily as shown in Figure 3 below.

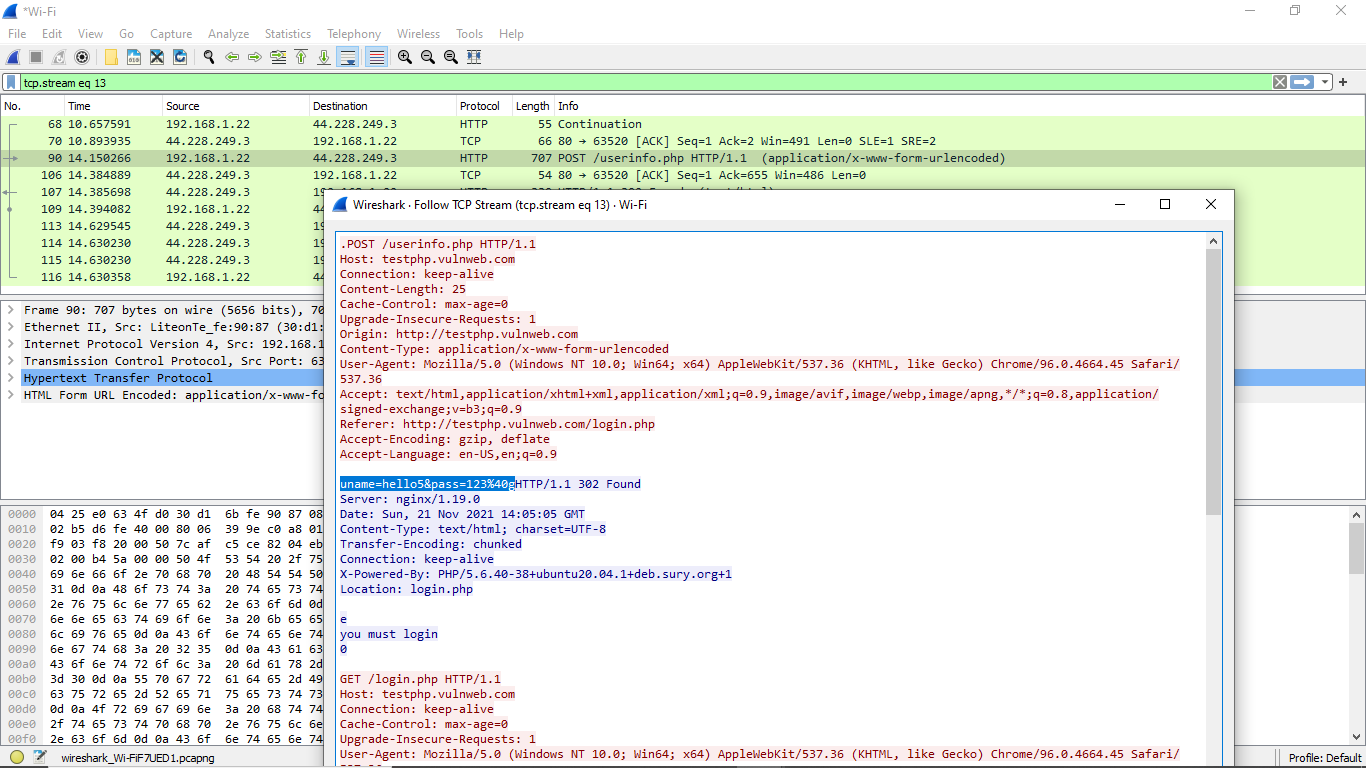
****

Figure 3 Window showing username and password

Along with the username and password, a 3rd person may even retrieve other details of the user such as the encoding specifications and location. Hence it is very important to make sure only secure and trusted websites are used when entering personal information.

Since the HTTPS protocol is secure and prevents misuse by encrypting the data, it is preferred over HTTP when entering personal information.

**CONCLUSION**

Today, the world is gravitating towards a technology dependent lifestyle. This results in the creation and authentication of more websites for private and public use. Without understanding the security features of a website, a user may become a victim of cyber-crime. By entering personal details and/or login credentials into an insecure website, a 3rd person can easily retrieve the data as demonstrated in the project. Many software like Wireshark is used to analyze data and communication from hosts to clients. However, when used for malicious reasons, can result in loss or illegal extraction of data. Thus, ensure that any classified information is sent from one host to another only as encoded data. This project acts as a demonstration to show how susceptible your information can be to such malpractice and to give a clearer understanding of the protocols HTTP and HTTPS. Hence it becomes essential for a user to always use trusted websites or at least check for the HTTPS protocol before uploading personal information.

**REFERENCES**

[1] Nayak, Mr. Parikshith, S. H. Brahmananda, and Mrs. Sahana DS. "An Approach to Sniff Sensitive Information by Packet Sniffing."

[2] Kelley, Timothy, and Bennett I. Bertenthal. "Real-world decision making: Logging into secure vs. insecure websites." *Proceedings of the USEC’16* (2016).

[3] Mohammed, M. A., Degadzor, A. F., Effrim, B. F., & Appiah, K. A. (2017). Brute force attack detection and prevention on a network using wireshark analysis. *International Journal Of Engineering Sciences & Research Technology*.

[4] http://testphp.vulnweb.com/login.php

[5]  <https://www.instructables.com/How-to-Find-Passwords-Using-Wireshark/>