ITG E ITI VIBO VALENTIA

Informatica

PRIVACY E SICUREZZA

Progetto e sviluppo di un sito web e un database per creare un Password Generator

Candidato:

Antonio Manduca

Anno Scolastico 2020/2021

Indice

1 SICUREZZA DEI DATI

Quando si vuole mandare un messaggio ad una persona, ovviamente, non si vuole che chiunque possa avervi accesso e quindi leggerlo, ma si pretende una certa riservatezza; si immagini quando si spedisce un pacco, se sul furgone del corriere ci fosse scritto “PACCO IMPORTANTE” di sicuro i malintenzionati non starebbero lontani. Per mantenere al sicuro e quindi nascondere ad occhi a noi sconosciuti i messaggi che vogliamo condividere, questi vanno nascosti.

1 . 1 STEGANOGRAFIA

La Steganografia consente, non solo di nascondere il messaggio, ma l’intera comunicazione tra due persone. Esistono diversi metodi per farlo: uno tra tanti era quello di rasare la testa di uno schiavo, scriverci un messaggio e aspettare che ricrescessero i capelli per poi mandarlo appunto al diretto interessato che rasava di nuovo per leggere il messaggio; un altro metodo è quello di mescolare succo di limone e acqua poi chiamato inchiostro simpatico e poi scrivere su un foglio, inizialmente si vede qualcosina ma poi scompare, per farla ricomparire deve essere scaldato il foglio; un altro metodo ancora era quello di scrivere con aceto su un uovo, essendo il guscio dell’uovo poroso, l’aceto ci passava attraverso e per leggere il messaggio bastava sgusciarlo. Con l’avvento del digitale ovviamente i metodi si sono evoluti, uno molto famoso è LSB, Least Significant Bit, consiste nel cambiare il bit meno significativo di uno o più colori dell’immagine, questa non sarà molto diversa dall’originale.

1 . 2 CRITTOGRAFIA

Per rendere sicuri i messaggi esiste la crittografia. Essa può essere simmetrica o asimmetrica. Quando si cifra con la crittografia simmetrica si stabilisce un cifrario e si fa sapere al destinatario, però chiunque è in grado di leggere come decifrare il messaggio perciò non è al sicuro. Con la crittografia asimmetrica invece sono state inventate la chiave pubblica e la chiave privata. Da qui si ricavano tre possibilità: garantire Riservatezza corrisponde a cifrare con la chiave pubblica del destinatario; per garantire Autenticazione e non ripudio si cifra con la chiave privata del mittente; per garantire Riservatezza, Autenticazione e non ripudio si cifra prima con la chiave privata del mittente e quello che si ottiene con la chiave pubblica del destinatario, così si può anche garantire che il messaggio non è stato compromesso. Ovviamente anche nel passato bisognava mantenere al sicuro i messaggi e vennero inventati vari oggetti e macchine automatiche per cifrare.

1 . 3 MACCHINE CIFRANTI

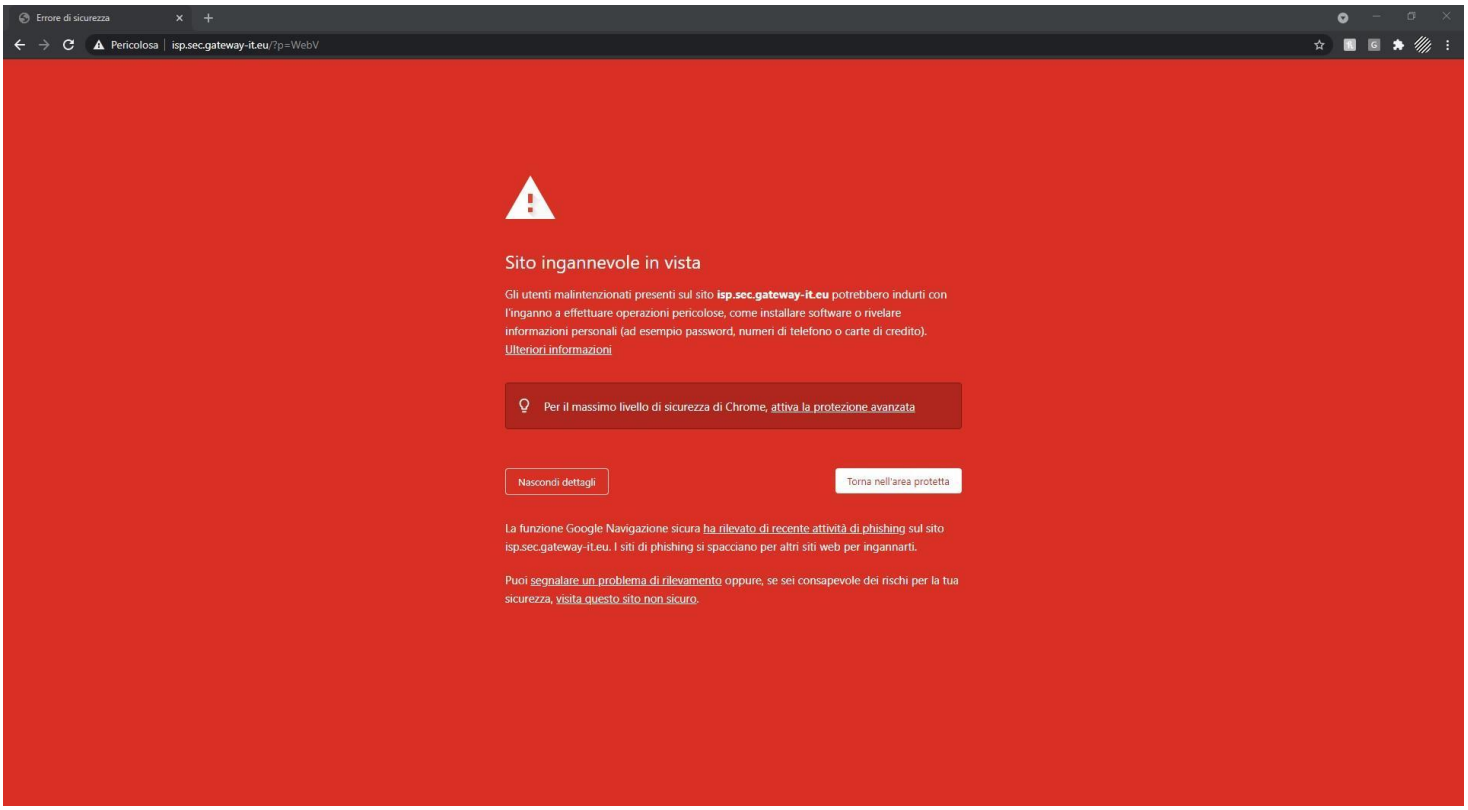
Nel XV secolo nasceva il Disco Cifrante di Alberti, costituito da due cerchi di cui uno libero di ruotare sui quali sono state incollate sagome di carta; per cifrare con questo veniva stabilita una chiave, cioè la lettera del primo cerchio corrispondeva a quella del secondo (esempio Fx), si scriveva il messaggio senza spazi, accenti e doppie, si inserivano a caso nel messaggio i numeri (1, 2, 3, 4) e si cifrava fino al primo numero, avuta la lettera corrispondente al primo numero la si faceva ruotare fino alla prima lettera della chiave e si andava avanti così anche per gli altri numeri. Per decriptare si posizionava il disco in base alla chiave e nel messaggio cifrato si sostituivano le lettere minuscole alle corrispondenti maiuscole. Un secolo dopo invece è stato pubblicato il Cifrario di Vigenère il quale era una rivisitazione del Cifrario di Cesare; però tutti questi lavori di cifratura e decifratura erano lunghi e stancanti per questo vennero inventate alcune macchine

cifranti automatiche. La più importante è Enigma, inventata nel 1918 e usata dai Tedeschi, poi quella di Lorenz e per i Giapponesi la Purple.

1 . 4 PROBLEMI AL GIORNO D'OGGI

Oggi esistono migliaia di piattaforme online sulle quali viene chiesto di registrarsi, perciò noi utenti che appunto vogliamo usare una determinata funzione di quella piattaforma ci registriamo, come per esempio sui Social Network, ma anche su siti vari di qualsiasi genere, come i siti per l'Home Banking, quindi per gestire le proprie carte e conti, che sono tra l'altro molto delicate come informazioni, o ancora i siti di Ecommerce sui quali ci sono i nostri dati più sensibili tra cui gli indirizzi per le spedizioni. Quindi, l'utente medio tende a fare la registrazione su quel sito web, caricando in un database i propri dati. La maggior parte degli utenti però, tende a dimenticare la password che ha inserito e lo ricorda per la prossima volta, così decide di inserirne una già usata da altre parti, o magari dappertutto. Questa potrebbe sembrare una cosa buona, perché si è soliti pensare: "su qualsiasi sito ci si trova le credenziali sono quelle", ma in realtà non lo è. Purtroppo nel mondo si sono diffusi i "malintenzionati", ovvero ci sono persone che hanno cattive intenzioni , vogliono rubare le credenziali e i dati personali degli utenti in svariati metodi. Questi metodi che potrebbero essere creati proprio da loro, vengono ideati in modo tale che un utente standard non riesca ad accorgersi di ciò che sta succedendo, potrebbe sembrargli una normale procedura di accesso. Uno dei metodi più famosi si chiama Phishing, questo è un tipo di truffa tramite la quale un malintenzionato cerca di ingannare la prescelta vittima facendo in modo che inserisca i suoi dati che potrebbero essere finanziari, di accesso o altro, fingendosi magari la Banca di fiducia o l'assicurazione o ancora il Gestore di Telefonia e può avvenire tramite mail, sms, internet o altri mezzi di comunicazione. Un esempio consiste nel mandare messaggi di tipo segnaletico come : "La tua PostePay è stata bloccata, effettua l'accesso su isp.sec.gateway-it.eu/?p=WebV per sbloccarla", da questo messaggio si può chiaramente capire che c'è qualcosa che non va, infatti

guardando il sito si capisce che non è il sito delle Poste e se si va su Chrome con la protezione abilitata esce questo errore:



Da ciò si può determinare che è un tentativo di furto dei dati di accesso al sito ufficiale delle Poste per accedere ai nostri conti, le nostre carte e tutti i dati presenti nel Database e, quindi, legati a noi. Dopo aver scoperto il nome utente e la password i malintenzionati provano ad andare su altri siti che potrebbero fortemente contenere nostri dati e ce li inseriscono, e nel caso in cui quella vittima aveva inserito le stesse credenziali durante la registrazione, riescono ad entrare e rubare qualsiasi informazione.

2 . SITI WEB

Un sito web, o sito internet, può tranquillamente essere paragonato ad un libro, il quale possiede contenuti di ogni genere e ci si possono trovare immagini, video e audio. Un sito è quindi una raccolta di file i quali vengono interpretati da un browser, sono collegati tra di loro mediante i link e si trovano caricati su i server. I siti vengono creati tramite un linguaggio chiamato HTML, per dare un po' di stile si usa il CSS e a questo punto si ha un sito statico. Per renderlo dinamico e

cioè avere la possibilità di fare il login o sorteggiare i prodotti di un catalogo, si usano altri linguaggi che sono: PHP, Javascript e altri a seconda di quello che si vuole implementare.

2.1 SERVER

I server sono dei computer i quali sono in grado di fornire qualsiasi tipo di servizio e/o risorsa ad altri computer in una rete, conosciuti anche come clients che ne fanno richiesta. Questi hanno un indirizzo ip associato per essere raggiunti, ma, essendo molto difficile da ricordare, si è pensato di raggiungerli usando i domini. Esistono svariate categorie di server: i File server consentono di accedere a file situati su un dispositivo in modo da facilitarne la condivisione; Web server usato per ospitare i siti Web; Mail server per la gestione della posta elettronica; Game server usato per le sessioni di gioco online multiplayer. La parte hardware del server può essere detta Standalone quando il server è assemblato dentro un comune case come i PC, oppure server Rack o Blade che sono rispettivamente i primi posizionabili in armadi rack e i secondi sono disposti in verticale e a gruppi. Questi Server si trovano nei data center che possono essere interni all'azienda o esterni.

2.2 DOMINIO

Un dominio è un nome con un'estensione che corrisponde a delle risorse contenute su un server. Il dominio è un nome leggibile, accattivante e facile da memorizzare (Esempio: Amazon, Google, Youtube). Se un utente prova a collegarsi a un sito web, inserisce il suo dominio nella barra degli indirizzi del browser. Il browser contatta un servizio di indirizzamento chiamato DNS, Domain Name Server, che si occupa di analizzare una tabella con le corrispondenze tra dominio e indirizzo IP, ossia l'indirizzo utilizzato dai computer. Trovato

l'IP corrispondente al dominio richiesto, il client dell'utente viene messo in contatto con il server corretto; in questo modo comincia lo scambio di dati che permette la navigazione internet. Le estensioni dei domini, che sono in continuo aumento, dovevano determinare, inizialmente, il settore del sito o la nazionalità: .it per Italia, .us per United States, .com per commercial, .org per organization.

2.3 HTML

HTML è ormai arrivato alla versione 5, è un linguaggio di Markup ed è strutturale e statico che serve appunto a definire il layout di una pagina web tramite dei tag di formattazione. La sua sintassi è definita dal W3C, World Wide Web Consortium. Questo è stato sviluppato negli anni novanta da Tim Berners-Lee al CERN di Ginevra, assieme al protocollo HTTP dedicato al trasferimento di documenti in tale formato.

2.4 CSS

Il CSS è il linguaggio usato per formattare i documenti HTML, le cui regole sono sempre definite dal W3C. Il CSS può essere interno, in linea o esterno, in linea quando è scritto dentro ogni tag HTML, interni quando si trovano nel file HTML ed esterni quando si trovano su un file a parte con estensione .css. Il vantaggio di avere un foglio di stile esterno è quello di ridurre le dimensioni dei file HTML e di poter modificare l'aspetto di un sito intero cambiando solamente un unico file.

2.5 JavaScript

JavaScript or JS is used to run client-side scripts on web pages for making them interactive. For example, it can be used: to add effects to web pages, display pop-up messages or to add moving pictures. JavaScript is the scripting language of the World Wide Web and is built into all major web browsers including Safari and Chrome. Almost every website incorporates some element of JavaScript to enhance the user experience.

2.6 PHP

PHP, Hypertext Pre-Processor, was not originally intended to be a programming language, it was the acronym for Personal Home Page. It was created as a set of tools for maintaining a personal home page. It is an interpreted scripting language, currently used to develop server-side web applications, but can also be used to write command line scripts or stand-alone applications with a graphical interface. PHP is able to interface with some DBMS including MySQL.

2.7 PRIVACY E SICUREZZA SUI SITI

Non tutti i siti Web sono attendibili e possono quindi presentare virus e bug o comunque componenti a scopo malevole. Su alcuni browser vi è la segnalazione dei siti che vengono ritenuti non sicuri. Un altro modo per capire se un sito è sicuro è quello di controllare la presenza del protocollo HTTPS che garantisce la crittografia della connessione. Farlo è molto semplice, basta controllare che all'inizio dell'URL sia presente la dicitura https://, tramite questo si capisce che quel sito

dispone del certificato SSL, Secure Sockets Layer. Se ci si fa caso, quando si entra in un sito esce una notifica push che dice di accettare termini e condizioni d'uso, molte volte si tende a dare il consenso senza nemmeno prestare attenzione a ciò che c'è scritto, quindi, molte aziende, grazie anche all'Intelligenza Artificiale che riesce ad elaborare milioni di dati in pochissimo tempo, vengono a conoscenza di ciò che visitiamo, cerchiamo, se inseriamo dati, quindi è come se lasciassimo la porta di casa aperta e può entrare chiunque a sbirciare. Fortunatamente il 4 Maggio 2016 è stato emanato il GDPR(General Data Protection Regulation) però è stato attivato il 25 Maggio 2018, questo stabilisce delle norme da rispettare per garantire la protezione dei dati personali. Un buon metodo per aumentare il livello di sicurezza e mantenere la privacy online è sicuramente quello di utilizzare una VPN.

2.7.1 VPN

VPN è l'acronimo di Virtual Private Network, rete privata virtuale e rappresenta una tecnica che, grazie al tunneling (si pensi ad un tunnel visto dall'alto, non si saprà mai cosa sia accaduto all'interno), permette sia di rendere invisibili le proprie attività in Rete a occhi non autorizzati (ad esempio i criminali informatici) sia di mascherare l'indirizzo IP da cui si accede a Internet. Questo viene ottenuto creando, tra i computer coinvolti, una vera e propria rete privata, accessibile soltanto a utenti autorizzati. Tale rete è virtuale, cioè creata sfruttando il mezzo di comunicazione Internet. Quando ci si connette ad Internet i dati vengono scambiati sulla rete, se ci si trova connessi ad un hotspot wifi pubblico, chiunque altro sia connesso può accedere a questi dati. Per questo tramite una connessione privata virtuale questi dati vengono prima crittografati e poi inviati così può accedervi solo il diretto interessato. La VPN consente anche di bloccare la tracciabilità degli annunci che compaiono sempre.

3 DATABASE

The Database is the way of storing data in digital format. Nowadays Databases are used by every company and schools to keep records of their customer accounts or their students. Data is presented in records and fields into one or more tables. Fields could contain different types of data: text, date and time, numbers or graphics. A Database can be called a flat-file database where there is only one table or relational database where data from different files are interlinked. Obviously, these data can be easily viewed, managed, modified, updated, checked and organized through the DBMS. The language used to write data and query to sort it, is SQL, Structured Query Language.

3 . 1 SQL

SQL is a special-purpose programming language used by almost all relational databases to query, manipulate and define data, as well as provide access control. Developed for the first time in the 70s in IBM with the important contribution of Oracle.

3 . 2 SICUREZZA SUI DATABASE

Le minacce ai Database si possono dividere in tre categorie: perdita di integrità se vengono apportate modifiche non autorizzate al Database, perdita di disponibilità se non sono disponibili i dati agli utenti, perdita di riservatezza, se non esiste la protezione dei dati stessi. Queste minacce possono essere causate da attacchi: a livello fisico, a livello logico (di intercettazione, di deduzione, di intrusione, di disturbo), disastri naturali o accidentali, errori o bug software/hardware o errori umani. Alcune problematiche si possono risolvere con la copia dei dati

su un supporto diverso anche se dovessero esserci aggiornamenti mancanti. Perciò bisogna implementare delle regole ovvero si deve poter tenere traccia di tutti i cambiamenti che avvengono in un Database per poter ricostruire il tutto. Anche sugli utenti si possono implementare le regole che riguardano il livello di amministrazione del Database, cioè cosa può o non può fare chi ci si collega.

4. IL SITO PROPROTECT

Il sito PROProtect è la mia idea per iniziare a diminuire questa serie di problemi relativi la sicurezza online. In questo sito ci sono svariate funzionalità, prima di tutte quella di poter generare una Password casuale tramite il generatore integrato, poi vi è la possibilità di immagazzinare le proprie Password per essere sicuri di non dimenticarne nemmeno una.

4.1 STRUTTURA DEL SITO “PROPROTECT”

Il sito PROProtect è stato realizzato mediante l’uso di cinque linguaggi diversi che sono: HTML per il layout delle pagine, CSS per lo stile di ogni singolo elemento, PHP per elaborare dati lato server, JavaScript per eseguire gli script e modificare il comportamento delle pagine Web ed SQL per eseguire le azioni necessarie sul Database.

4 . 2 FUNZIONE DI HASH

Ovviamente le Password che verranno inserite nel Database dovranno essere criptate. Per farlo è stata utilizzata la funzione *password_hash()* di PHP. Questa, grazie ad un potente algoritmo, prende la stringa fornita e la trasforma. La funzione citata è a senso unico, con questo si intende che dalla password originaria si può generare il valore di hash, però poi da questo non si può tornare all'origine. Il valore generato ha una lunghezza fissa, quindi non importa quanti caratteri si immetteranno perché sarà lungo uguale. Questo valore che verrà generato dalla funzione può anche essere chiamato "fingerprint", impronta digitale, per indicare l'unicità di ogni valore come un'impronta digitale appunto. Si pensi che utilizzando solo lettere minuscole da "a" a "f" e i numeri da "0" a "9", avendo un valore di hash della lunghezza di 64 caratteri, esistono infinite possibilità di valori ottenibili.

4 . 3 LE PAGINE

Il sito è composto da svariate pagine: la pagina di login, di registrazione, dei servizi offerti, del generatore di Password e del Gestore delle Password. La pagina di login è composta da un semplice form che richiede di inserire lo username scelto in fase di registrazione e ovviamente la Password che verrà confrontata con quella inserita nel Database per per poter permettere l'accesso. Anche nella pagina di registrazione verrà visualizzato un form che richiede: username, password, conferma della password, nome ed email, alla quale email sarà inviata la richiesta di attivazione account senza la quale non sarà attivato il profilo dell'utente. Nella pagina relativa ai servizi, verranno mostrati i servizi messi a disposizione di ogni utente che visita la nostra piattaforma e ci si registra. Cliccando sulla sezione riguardante il Generatore di Password, verrà aperta una nuova scheda contenente il generatore nel quale si potrà scegliere la lunghezza preferita della password stessa, stabilire l'uso di lettere maiuscole, di

lettere minuscole, di numeri e di simboli. Dalla pagina dei servizi, cliccando invece sulla sezione riguardante il Gestore delle Password, si andrà in un'altra pagina nella quale viene descritto questo Gestore e per usarlo bisognerà obbligatoriamente essere loggati.