WEB SECURITY SOLUTIONS

Software Requirement Specification

Overview of Project :-

The concept of security applies to all information. Security relates to the protection of valuable assets against loss, disclosure, or damage. Valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure. Hence, by this project, we aim to create a secure system which could be used in websites or which could be used to gain information about various threats and vulnerabilities or information regarding domain or network infrastructure.

Scope of Project :

The fact that integrating security solutions, may it be an additional layer of security using secure shell like HTTPS or the use of OTP / captchas are a difficult task to code along with extra technical mainframe infrastructure that one has to establish has prevented organisations from investing into this field. By providing API's for the above mentioned services, we will be creating a platform for all those entrepreneurs and organisations which lack the technicalities needed for creating a security system.

Features :-

- Easy to understand user Interface to enhance communication gap between user and system.
- Different classes of users, like Computer Scientists, end users and administrators.
- Network information groping utility integrated into the system to offer a one place destination for entire information.
- Various domain scans available to retrieve data about dns.
- Secret Message Sender using steganography.
- Email Sending using Gmail's SMTP Servers.
- Facility to implement Flooding (Denial of Service Attack).
- Various encryption methods available.
    - Chel's Encryption
    - ABM Encryption.
    - Bey's Encryption
    - MD5 (Message Direct Algorithm) Encryption

Intended Users :-

There are four types of users that will be using this system.
1. Computer Scientists :-
They will have access to all the features of our system. Their main aim while using these utilities will be research, experimentation or other scientific purposes.

2. Administrator :-
They will have complete access to all the utilities and feature. Their main aim will be to manage and maintain the system.

3. End Users :-
They will have limited access. Features like arp scan and nmap will not be available to them. Their main aim when using these utilities will be to solve their problem or out of curiosity.

4. Computer programmers :-
They will have complete access of all the features. Their main aim while using these utilities will be to integrate these functionalities in their projects/ websites.
They will have access to all the source codes in form of a library..

Functional Requirements:

Simple Attacks :-
This module describes few of the most prevalent security attacks occurring over a network. Attacks mentioned here includes Denial of service, distributed Denial of service, flooding etc.

Denial of Service :-
These are attacks where the perpetrator aims to make machine or system resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet / Network.
A DOS attack is accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Distributed Denial of Service :-
A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

Ping Flood :-
It is a kind of denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Requests (ping) packets. This is most effective by using flood option of ping utility which sends ICMP packets as fast as possible without waiting for replies.

Domain & Network Infrastructure Information using Web Utilities:-
This module performs search operations to collect information regarding domain and network infrastructure using basic utility commands.
Utility Commands include arp scan, nslookup, robots.txt scan and nmap scan.

Arp Scan is a tool used for system discovery and fingerprinting. It constructs and sends ARP requests to the specified IP addresses, and displays any response that are received.

Nmap is a utility for network discovery and security auditing. It can also be used for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It uses raw packets in a way so as to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use and other similar features.

Nslookup us a tool use dfor querying the Domain Name Server (DNS) to obtain domain name of IP address mapping or for any other specific DNS record.

Website owners use the /robots.txt file to give instructions about their site to web robots.
It is a part of **" The Robots Exclusion protocol ".** The benefits that this provides to us are that since it is a publically available file, anyone can see what sections of our server we don't want crawlers to crawl in.

Steagnography:-
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal.

OTP:-
OTP Verification plugin verifies Email Address/Mobile Number of users by sending verification code(OTP) during registration. It removes the possibility of a user registering with fake Email Address/Mobile Number. This plugin checks the existence of the Email Address/Mobile Number and the ability of a user to access that Email Address/Mobile Number.
How does this work?
1. On submitting the registration form an Email/SMS with OTP is sent to the email address/mobile number provided by the user.
2. Once the OTP is entered, it is verified and the user gets registered.

Recaptcha :
reCAPTCHA is a CAPTCHA-like system designed to establish that a computer user is human (normally in order to protect websites from bots) and, at the same time, assist in the

digitization of books. The reCAPTCHA service supplies subscribing websites with images of words that are hard to read for optical character recognition (OCR) software.
The reCAPTCHA tests are displayed from the central site of the reCAPTCHA project, which supplies the words to be deciphered. This is done through a JavaScript API with the server making a callback to reCAPTCHA after the request has been submitted. The reCAPTCHA project provides libraries for various programming languages and applications to make this process easier. reCAPTCHA is a free service (that is, the CAPTCHA images are provided to websites free of charge, in return for assistance with the decipherment), but the reCAPTCHA software itself is not open source

Encryption :

Encryption is the process of encoding messages or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor..
An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

We have used following encryption algorithms.

Chel's Encryption :

It encrypt the file by changing the ascii value of every character that occurs in file by doing some operations on ascii value. We can decrypt the file by just reversing the operations on that character and using public key we can make the file only accessible to its owner and if any other user tries to open that file he will see the encrypted file not the original one.

MD5 (Message Digest Algorithm):-

The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Like most hash functions, MD5 is neither encrypted nor encoding. It can be reversed by brute-force attack and suffers from extensive vulnerabilities. The security of the MD5 has been severely compromised, with its weaknesses having been exploited in the field, most infamously by the Flame malware in 2012. The CMU Software Engineering Institute considers MD5 essentially "cryptographically broken and unsuitable for further use".

ABM's Encryption:-

It encrypts file by using a polymorphic code. **polymorphic code** is **code** that uses a **polymorphic** engine to mutate while keeping the original algorithm intact. the code changes itself each time it runs, but the function of the code (its semantics) will not change at all. For example, 1+3 and 6-2 both achieve the same result while using different code.
The main body of the code (also called its payload) is encrypted and will appear meaningless. For the code to function as before, a decryption function is added to the code. When the code is *executed* this function reads the payload and decrypts it before executing it in turn. Encryption alone is not polymorphism. To gain polymorphic behavior, the encryptor/decryptor pair are mutated with each copy of the code. This allows different versions of some code which all function the same.

Non functional Requirements :

1. Performance requirement :-
The system can provide ease both at admin level or local level
and focus on program logic so that the task is done in systematic, efficient and in quantifiable approach.

2. Availability :-
The system should be available at all times, meaning the user can access it using a web browser, only restricted by the down time of the server on which the system runs. A customer friendly system which is in access of people around the world should work 24 hours. In case of a of a hardware failure or database corruption, a replacement page will be shown. Also in case of a hardware failure or database corruption, backups of the database should be retrieved from the server and saved by the Organizer. Then the service will be restarted. It means 24 x 7 availability.

3. Security Requirement :-
The system use SSL (secured socket layer) in all transactions that include any confidential customer information. The system must automatically log out all customers after a period of inactivity. The system should not leave any cookies on the customer's computer containing the user's password. The system's back-end servers shall only be accessible to authenticated management.

4. Maintainability:
A commercial database is used for maintaining the database and the application server takes care of the site. In case of a failure, a re-initialization of the project will be done. Also the software design is being done with modularity in mind so that maintainability can be done efficiently.

5. Portability:
The system is developed for secured purpose, so it is can't be portable.

6.Reliability :-
The reliability of the overall project depends on the reliability of the separate components. The main pillar of reliability of the system is the backup of the database which is continuously maintained and updated to reflect the most recent changes. Also the system will be functioning inside a container. Thus the overall stability of the system depends on the stability of container and its underlying operating system.