CAPSTONE PROJECT REPORT

(Project Term August-December 2019)

(WEBSITE SECURITY)

Submitted by

A Y C Sai Kumar	**Registration Number:**	**11603455**
B Ajith Lakshma Reddy	**Registration Number:**	**11602721**
B Srinivasulu Reddy	**Registration Number:**	**11602071**

Under the Guidance of

Ms. Richa Jain

Project Group Number: CSERGC0110

Couse Code: CSE439

Discipline of CSE/IT

School of Computer Science & Engineering

Lovely Professional University, Phagwara

INDIA'S LARGEST UNIVERSITY*

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering (SCSE)

Program : P132::B.Tech. (Computer Science & Engineering)

COURSE CODE : CSE439 REGULAR/BACKLOG : Regular GROUP NUMBER : CSERGC0110

Supervisor Name : Richa Jain UID : 17688 Designation : Assistant Professor

Qualification : ________________________ Research Experience : ________________________

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Appana Youdhister Chitti Sai Kumar	11603455	2016	K1610	9872219922
2	Bapathu Ajith Lakshma Reddy	11602721	2016	K1609	9115512393
3	Bakkireddy Srinivasulu Reddy	11602071	2016	K1607	7993435403

SPECIALIZATION AREA : Networking and Security Supervisor Signature: ___________________

PROPOSED TOPIC : Website Security

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	6.85
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.69
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.38
5	Social Applicability: Project work intends to solve a practical problem.	6.85
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.85

PAC Committee Members		
PAC Member (HOD/Chairperson) Name: Dr. Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member (Allied) Name: Vishu	UID: 18807	Recommended (Y/N): Yes
PAC Member 3 Name: Ravishanker	UID: 12412	Recommended (Y/N): Yes

Final Topic Approved by PAC: Website Security

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal Approval Date: 29 Apr 2019

11/14/2019 3:13:34 PM

DECLARATION

We hereby declare that the project work entitled **"Website Security"** is an authentic record of our own work carried out as requirements of Capstone Project for the award of B. Tech degree in Computer Science Engineering from Lovely Professional University, Phagwara, under the guidance of Ms. Richa Jain, during August to December 2019. All the information furnished in this capstone project report is based on our own intensive work and is genuine.

Project Group Number:

Name of Student 1: A Y C Sai Kumar
Registration Number: 11603455

Name of Student 2: B Ajith Lakshma Reddy
Registration Number: 11602721

Name of Student 3: B Srinivasulu Reddy
Registration Number: 11602071

Signature:
Date:

Signature:
Date:

Signature:
Date:

CERTIFICATE

This is to certify that the declaration statement made by this group of students is correct to the best of my knowledge and belief. They have completed this Capstone Project under my guidance and supervision. The present work is the result of their original investigation, effort and study. No part of the work has ever been submitted for any other degree at any University. The Capstone Project is fit for the submission and partial fulfilment of the conditions for the award of B. Tech degree in Computer Science Engineering from Lovely Professional University, Phagwara.

Signature and Name of the Mentor

Designation

School of Computer Science and Engineering,
Lovely Professional University,
Phagwara, Punjab.

Date:

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to my teacher Ms. **Richa Jain** who gave us the golden opportunity to do this wonderful project on the topic **“Website Security”** which also helped us in doing a lot of Research and we came to know about so many new things we are really thankful to them.

Secondly it would also like to thank our Group Members who helped us a lot in finalizing this project within the limited time frame.

TABLE OF CONTENTS

1. INTRODUCTION

Website security is critical component to protect and secure websites and servers. Websites are scanned for any possible vulnerabilities and malware through website security software. This software can scan for backdoor hacks, redirect hacks, Trojans, and many other threats. A website security software notifies the user if the website has any issue and provides solutions to address them.

Enterprise Networks are always at high risk of vulnerability and ensuring website security is vital. If the Network gets compromised, the server and the website get compromised as well – this would let the malware infiltrate through the enterprise network and introduce malware activities

1.1 Features of a good Website Security Plan

- Malware scan
- Malware removal
- Manual malware and hack removal
- File change monitoring
- Blacklist/spam monitoring
- Blacklist removal
- Security monitoring
- Advanced DDoS mitigation
- Web Application Firewall (WAF)
- Content Delivery Network (CDN)
- Site Seal

1.2 Details of Web Security

There are a lot of factors that go into web security and web protection. Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.

There are a variety of security standards that must be followed at all times, and these standards are implemented and highlighted by the OWASP. Most experienced web developers will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services.

2. Scope of Study

While in its early days, the Web was mostly static, it has organically grown into a full-fledged technology stack. This evolution has not followed a security blueprint, resulting in many classes of vulnerabilities specific to the Web. Even though the server-side code of the past has long since vanished, the Internet Archive gives us a unique view on the historical development of the Web’s client side and its (in)security. Uncovering the insights which fuelled this development bears the potential to not only gain a historical perspective on client-side Web security, but also to outline better practices going forward.

To that end, we examined the code and header information of the most important Web sites for each year between 1997 and 2016, amounting to 659,710 different analysed Web documents. From the archived data, we first identify key trends in the technology deployed on the client, such as the increasing complexity of client-side Web code and the constant rise of multi-origin application scenarios. Based on these findings, we then assess the advent of corresponding vulnerability classes, investigate their prevalence over time, and analyse the security mechanisms developed and deployed to mitigate them.

Correlating these results allows us to draw a set of overarching conclusions: Along with the dawn of JavaScript-driven applications in the early years of the millennium, the likelihood of client-side injection vulnerabilities has risen. Furthermore, there is a noticeable gap in adoption speed between easy-to-deploy security headers and more involved measures such as CSP. But there is also no evidence that the usage of the easy-to-deploy techniques reflects on other security areas. On the contrary, our data shows for instance that sites that use HTTP-only cookies are actually more likely to have a Cross-Site Scripting problem. Finally, we observe that the rising security awareness and introduction of dedicated security technologies had no immediate impact on the overall security of the client-side Web.

3. EXISTING TOOLS

3.1 Existing Systems:

- Nogotofail

  A network traffic security testing tool from Google, Nogotofail is a lightweight application that is able to detect TLS/SSL vulnerabilities and misconfigurations

- SonarQube

  Another opportune open source security testing tool is SonarQube. In addition to exposing vulnerabilities, it is used to measure the source code quality of a web application. Despite being written in Java, SonarQube is able to carry out analysis of over 20 programming languages.

- Iron Wasp

  An open-source, powerful scanning tool, Iron Wasp is able to uncover over 25 types of web application vulnerabilities. Additionally, it can also detect false positives and false negatives

- Zed Attack Proxy (ZAP)

  Developed by OWASP (Open Web Application Security Project), ZAP or Zed Attack Proxy is a multi-platform, open source web application security testing tool. ZAP is used for finding a number of security vulnerabilities in a web app during the development as well as testing phase.

- Grabber

  The portable Grabber is designed to scan small web applications, including forums and personal websites. The lightweight security testing tool has no GUI interface and is written in Python.

3.2 Proposed System:

As we have known many security tools available as mentioned above here, we want to provide security to a website without using the above-mentioned security tools.

3.3 DFD for present system

DFD LEVEL - 0

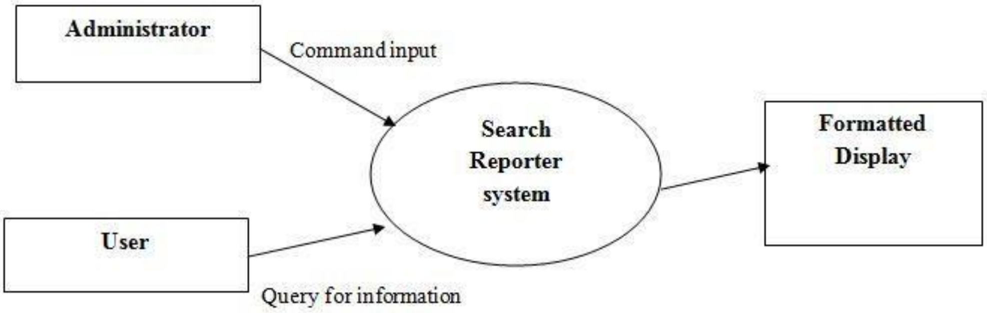


Figure 3.3.1 DFD LEVEL 0

DFD LEVEL - 1

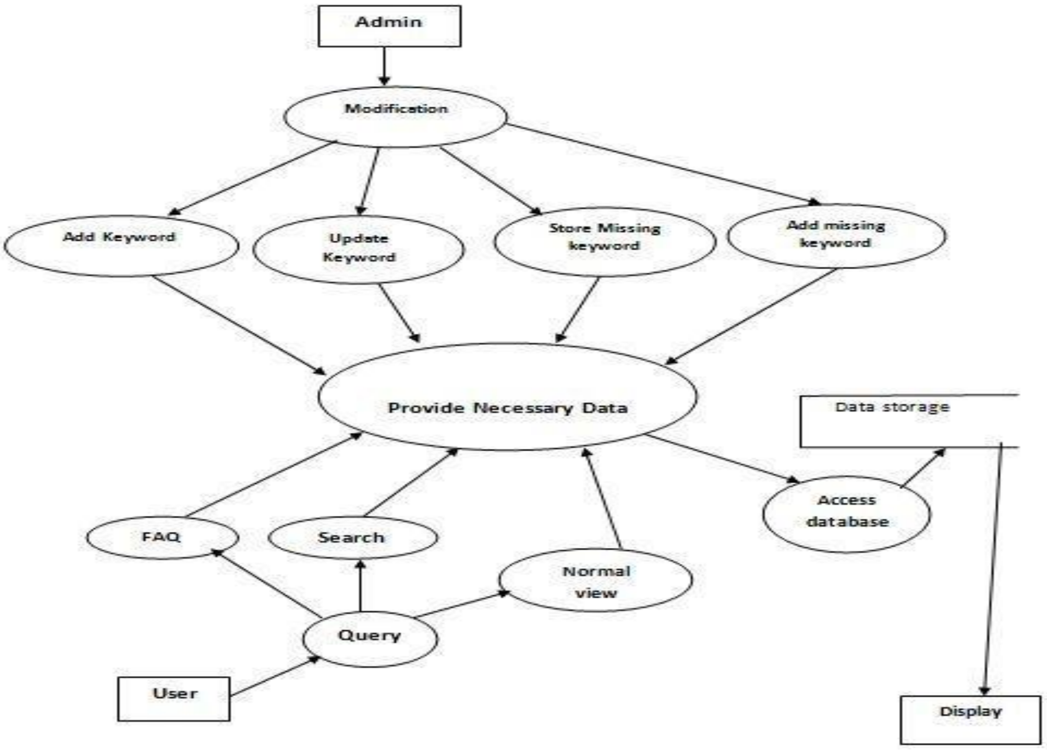


Figure 3.3.2 DFD LEVEL 1

DFD LEVEL – 2

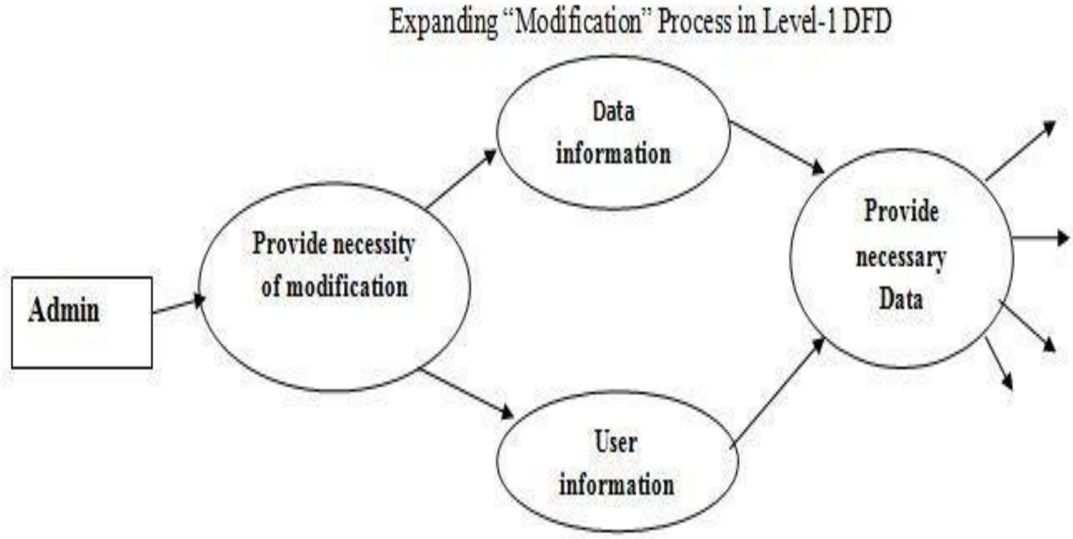

Expanding "Modification" Process in Level-1 DFD
Admin
Provide necessity of modification
Data information
User information
Provide necessary Data

Figure 3.3.3 DFD LEVEL 2

4. PROBLEM ANALYSIS

Everybody wants to know what it's going to cost.

- Agree to a budget up front.

Why You Need to Keep Your Website Secure

- Every website is potentially vulnerable to these attacks.
- You need to keep yours safe. An unsecured site can be compromised. Your customer’s data might be stolen. This can lead to lost revenue, costly website coding repairs, and many other problems.
- You can protect your website from hackers. We’ll start off with a few basic descriptions of the types of attacks that you might encounter. This is followed by the eleven tips to secure your website

The system shall allow the administrator to add the following information:

- Email Address
- Password
- Security Question
- Email OTP
- Plugins

The system shall allow the administrator to modify following information:

- Email Address
- Password
- Security Question
- Email OTP
- Plugins
- Failed Login Limit

4.1 UML Diagrams

Use case is used to identify and partition system functionality. It separates the system into actors and use cases.

Two **actors** using administrative interfaces are **Website Administrator** and **Help Desk**. Help Desk uses a subset of functions available to the Website Administrator. All top level **use cases** shown are abstract as each represents some group or "package" of administrative functionality

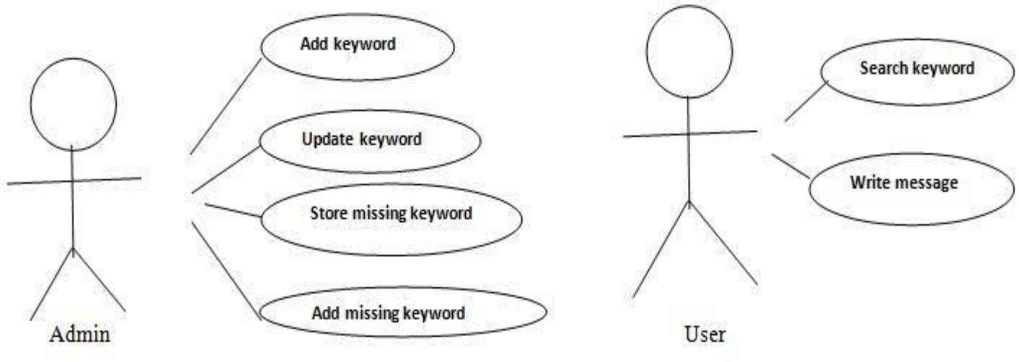


Figure 4.1.1 UML DIAGRAM

4.2 Project Plan

Week1: Here we determined the requirements of the project and website. We discussed the project i.e. what will be the functionalities and how it will perform its task in a corrective manner.

Week2: Divides the module to be completed in the further weeks and designed the UML diagram for the module.

Week3: We took Domain and Hosting service from GoDaddy Site and designed the website to which security has to be provided.

Week4: Provided the login details to the Admin to makes changes to the website.

Week5: Added required plugins to the website to make more secured.

Week6: We added 2factor authentication to the Admin login portal and also security question plugin.

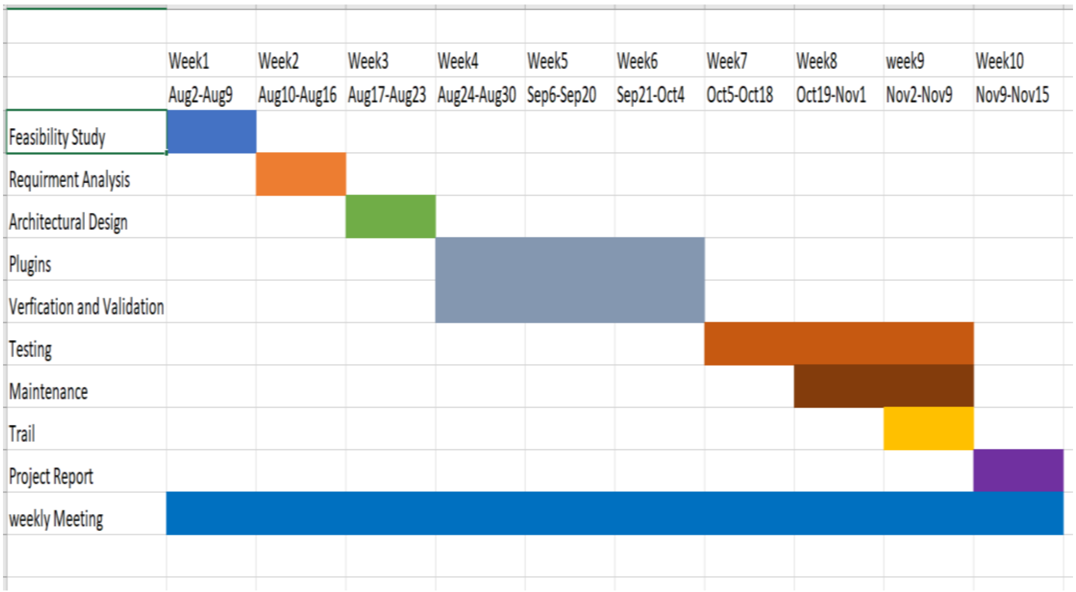
Week7: We added another plugin where it will monitor the no. of visitors to the website.

Week8: In this week we performed testing using Failed login attempts plugin to block the ip address of suspicious login attempts.

Week9: In this week we changed the status of the site from HTTP to HTTPS which is more secured.

Week10: In this week We developed the report of our project and made changes to the website according to the requirement.

4.3 Gantt Chart



	Week1 Aug2-Aug9	Week2 Aug10-Aug16	Week3 Aug17-Aug23	Week4 Aug24-Aug30	Week5 Sep6-Sep20	Week6 Sep21-Oct4	Week7 Oct5-Oct18	Week8 Oct19-Nov1	week9 Nov2-Nov9	Week10 Nov9-Nov15
Feasibility Study	■									
Requirment Analysis		■								
Architectural Design			■							
Plugins				■	■	■				
Verfication and Validation				■	■	■				
Testing							■	■	■	
Maintenance								■	■	
Trail									■	
Project Report										■
weekly Meeting	■	■	■	■	■	■	■	■	■	■

Figure 4.3 Gantt Chart

Gantt Chart Table

4.4 Feasibility Study

A feasibility study is a test of system proposal according to its workability, impact on the organization, ability to meet user needs and effective use of resources. The objective of feasibility study is not to solve the problem, but to acquire a sense of its scope. During the study, the problem definition is crystallized and aspects of the problem to be included in the system are determined, consequently costs and benefits are estimated with greater detail at this stage. The result of the feasibility study is a system formal proposal. This is simply a form of documenting or detailing the nature and scope of proposed solutions. The proposal summarizes what is known and what is going to be done. Three key considerations involved in the feasibility analysis:

- Economic feasibility
- Technical feasibility

4.4.1 Economical Feasibility:

- No hardware and software were purchased to make the project
- Additional Cost: For hosting the website bought “Domain and Host” in GoDaddy website
- Testing the website was even feasible because we just require laptop and internet connection.
- The website needs maintenance, which does not require lot of charges

4.4.2 Technical Feasibility:

- The technology used was WordPress application, which is an open source, and well developed for study and are able to build different website products using this technology. Therefore, the application was technically feasible.

5. SOFTWARE REQUIREMENT ANALYSIS

Software:

Operating System: Windows

Language: PHP

Network: LAN, Mobile Network

Hardware:

Processor: 2GHz dual core

RAM: 2GB RAM

Hard Disk: 25 GB hard-drive

6. DESIGN

Pick a theme / design for your website

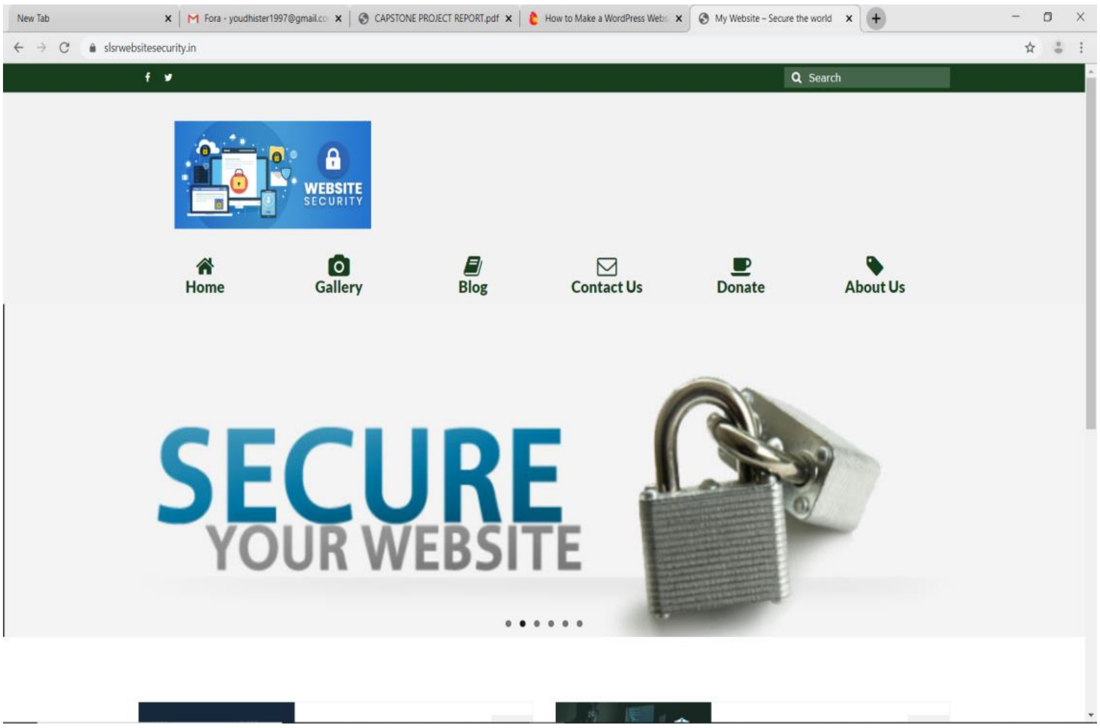
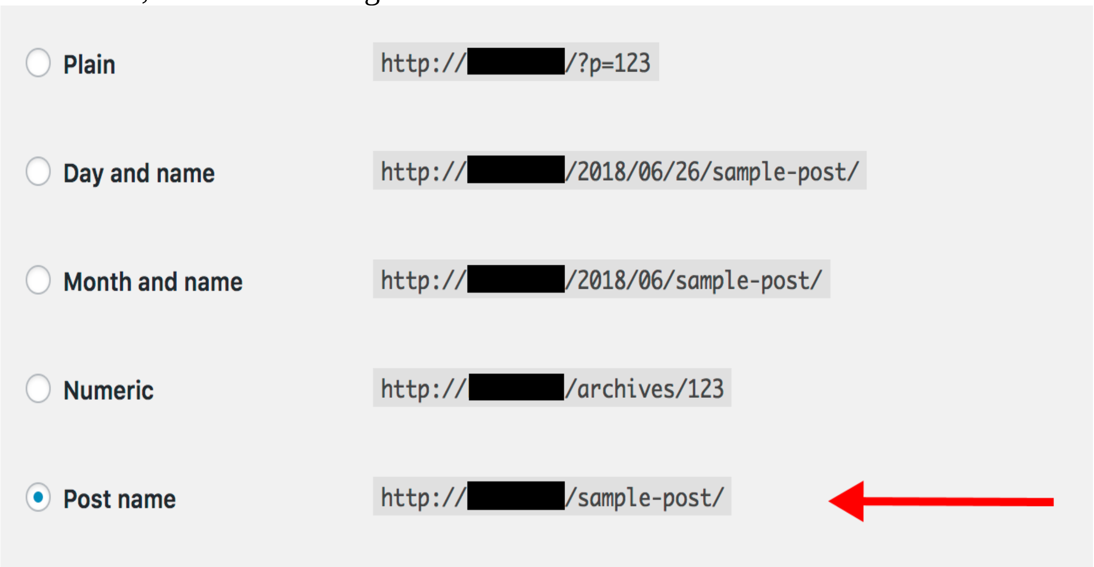

New Tab
Fora - youdhister1997@gmail.co
CAPSTONE PROJECT REPORT.pdf
How to Make a WordPress Web
My Website – Secure the world
slsrwebsitesecurity.in
Search
WEBSITE SECURITY
Home
Gallery
Blog
Contact Us
Donate
About Us
SECURE
YOUR WEBSITE

Figure 6.1 DESIGN

a) Set permalinks

To set your permalinks, go to **Settings** → **Permalinks** from the main sidebar in your WP dashboard.

Once there, select this setting:



○ Plain http://[redacted]/?p=123

○ Day and name http://[redacted]/2018/06/26/sample-post/

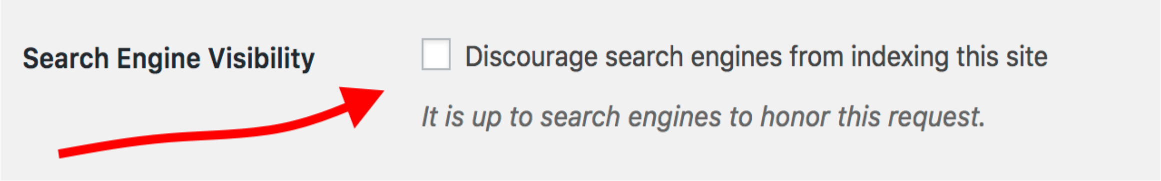
○ Month and name http://[redacted]/2018/06/sample-post/

○ Numeric http://[redacted]/archives/123

● Post name http://[redacted]/sample-post/

Figure 6.2 DESIGN

b) Making your site public



Search Engine Visibility □ Discourage search engines from indexing this site

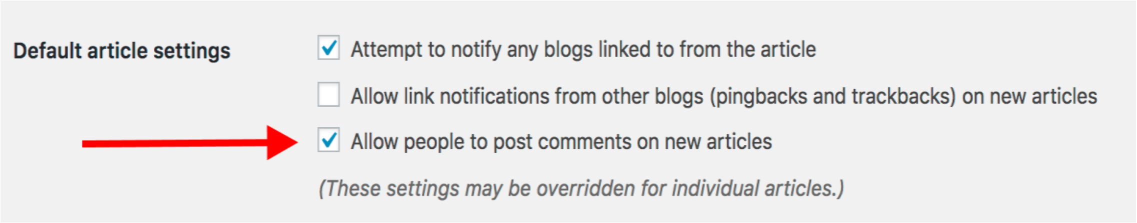
It is up to search engines to honor this request.

Figure 6.3 DESIGN

c) Set your website title and tagline

Go to **Settings** → **General** and set the **Site Title** and **Tagline** fields to what you want.

d) Allow or disable comments



Default article settings

☑ Attempt to notify any blogs linked to from the article

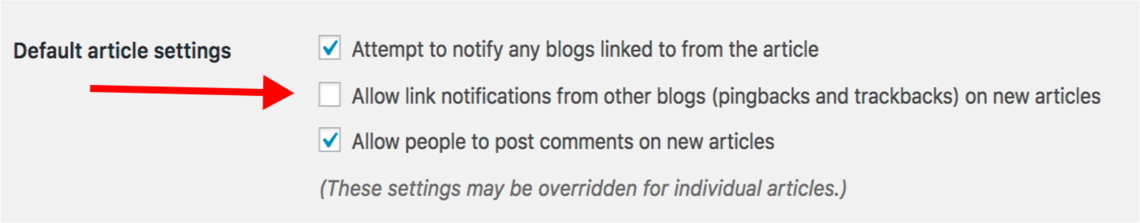
□ Allow link notifications from other blogs (pingbacks and trackbacks) on new articles

☑ Allow people to post comments on new articles

(These settings may be overridden for individual articles.)

Figure 6.4 DESIGN

e) Disable pingbacks and trackbacks



Default article settings

☑ Attempt to notify any blogs linked to from the article

□ Allow link notifications from other blogs (pingbacks and trackbacks) on new articles

☑ Allow people to post comments on new articles

(These settings may be overridden for individual articles.)

Figure 6.5 DESIGN

f) Set your time zone

Setting your time zone correctly will make publishing new pages and posts more predictable.

7. IMPLEMENTATION

Step 1: Choose WordPress as your website platform

- it's open source
- it's free
- it's the ultimate DIY solution for website building
- it's extra versatile – can run any type of website
- it's fast, optimized, and secure
- it's SEO-ready – makes promotion easier

Step 2: Pick a name for your website, buy a domain & hosting

In short, a good domain name should be:

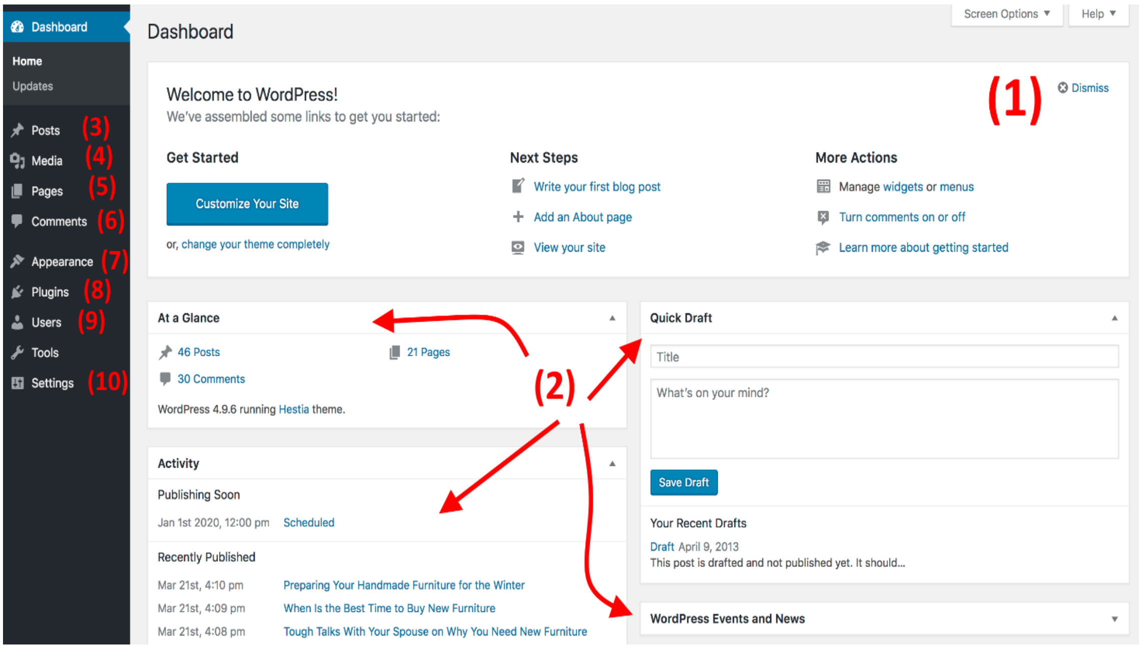
- brandable – unique sounding, like nothing else that's out there in the market
- easy to memorize
- short – those are also easier to memorize
- easy to type and hard to mix up – you don't want people to be wondering how to spell your site's name
- including niche-related keywords – for instance, if you do anything with pizza, it would be cool to have "pizza" somewhere in the name of the site; it works the same in non-pizza industries as well.

Step 3: Buying your domain name and hosting

- GoDaddy is a reputable web host that's optimized for WordPress and will make sure that your website operates with no hiccups
- it's one of the few companies recommended on the official WordPress.org website
- it's cheap (from $2.95/month)
- it's easy to use and beginner-friendly
- you get a **domain name for free**

Step 4: Telling Bluehost to install WordPress for you

Step 5: Get familiar with the WordPress UI



Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

or, change your theme completely

Write your first blog post

Add an About page

View your site

Manage widgets or menus

Turn comments on or off

Learn more about getting started

WordPress 4.9.6 running Hestia theme.

What's on your mind?

Your Recent Drafts

Draft April 9, 2013

This post is drafted and not published yet. It should…

Publishing Soon

Jan 1st 2020, 12:00 pm Scheduled

Recently Published

Mar 21st, 4:10 pm Preparing Your Handmade Furniture for the Winter

Mar 21st, 4:09 pm When Is the Best Time to Buy New Furniture

Mar 21st, 4:08 pm Tough Talks With Your Spouse on Why You Need New Furniture

Figure 7.1 IMPLEMENTATION

(1) Welcome message – Some of the most important areas of the admin panel listed as quick shortcuts links – these are usually your shortcuts to how to make a website.

(2) The current status of your site and what's going on with it.

(3) Posts – go here to create blog posts.

(4) Media – upload/manage images and other media files here.

(5) Pages – go here to create sub-pages.

(6) Comments – this is where you can moderate comments.

(7) Appearance – change your site's design here and/or customize how certain things are displayed on the current design.

(8) Plugins – install new plugins here.

(9) Users – manage user accounts that can access the admin panel of the website.

(10) Settings – the main settings

Step 6: Get plugins to extend your website's abilities

- **Web Application Security Implementation**

This chapter discusses the implementation of web application security, picking up the following nine vulnerabilities, and shows threats each vulnerability may pose, what types of websites might be most vulnerable, possible fundamental solutions and mitigation measures.

  - SQL Injection
  - OS Command Injection
  - HTTP Header Injection
  - Mail Header Injection
  - Lack of Authentication and Authorization

- **SQL Injection**

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their OWASP Top 10 2017 document as the number one threat to web application security.

Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.

SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.

SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.

You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.

In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

Possible Threats

This vulnerability could allow malicious attackers to:

View sensitive data stored in the database
e.g. Disclosure of personal information

Falsify and/or delete data stored in the database
e.g. Falsification of web pages, password change, system shutdown

Bypass login authentication
All the operations permitted under the privileges of a login account become unauthorizedly possible.

Execute OS commands using stored procedures
e.g. System hijacking, making the target PC a bot (launching point) to attack others

Mitigation Measures

“Limit information to display in error message on the web”

“Grant minimum privileges to databaseaccounts.”

- **OS Command Injection**

Command injection is basically injection of operating system commands to be executed through a web-app. The purpose of the command injection attack is to inject and execute commands specified by the attacker in the vulnerable application. In situation like this, the application, which executes unwanted system commands, is like a pseudo system shell, and the attacker may use it as any authorized system user. However, commands are executed with the same privileges and environment as the web application has. Command injection attacks are possible due to lack of correct input data validation, which can be manipulated by the attacker (forms, cookies, HTTP headers etc.).

There is a variant of the Code Injection attack. In code injection, the attacker adds his own code to the existing code. Injected code is executed with the same privileges and environment as the application has.
An OS command injection attack occurs when an attacker attempts to execute system level commands through a vulnerable application. Applications are considered vulnerable to the OS command injection attack if they utilize user input in a system level command.

Possible Threats

This vulnerability could allow attackers to:

- **View, falsify and delete files stored in the server**

・e.g. Disclosure of sensitive information, falsification of configuration files

- **Maliciously manipulate the system**

・e.g. Unintended OS shutdown, adding/deleting user accounts

- **Download and execute malicious programs**

・e.g. Virus, worm and bot infection, backdoor implementation

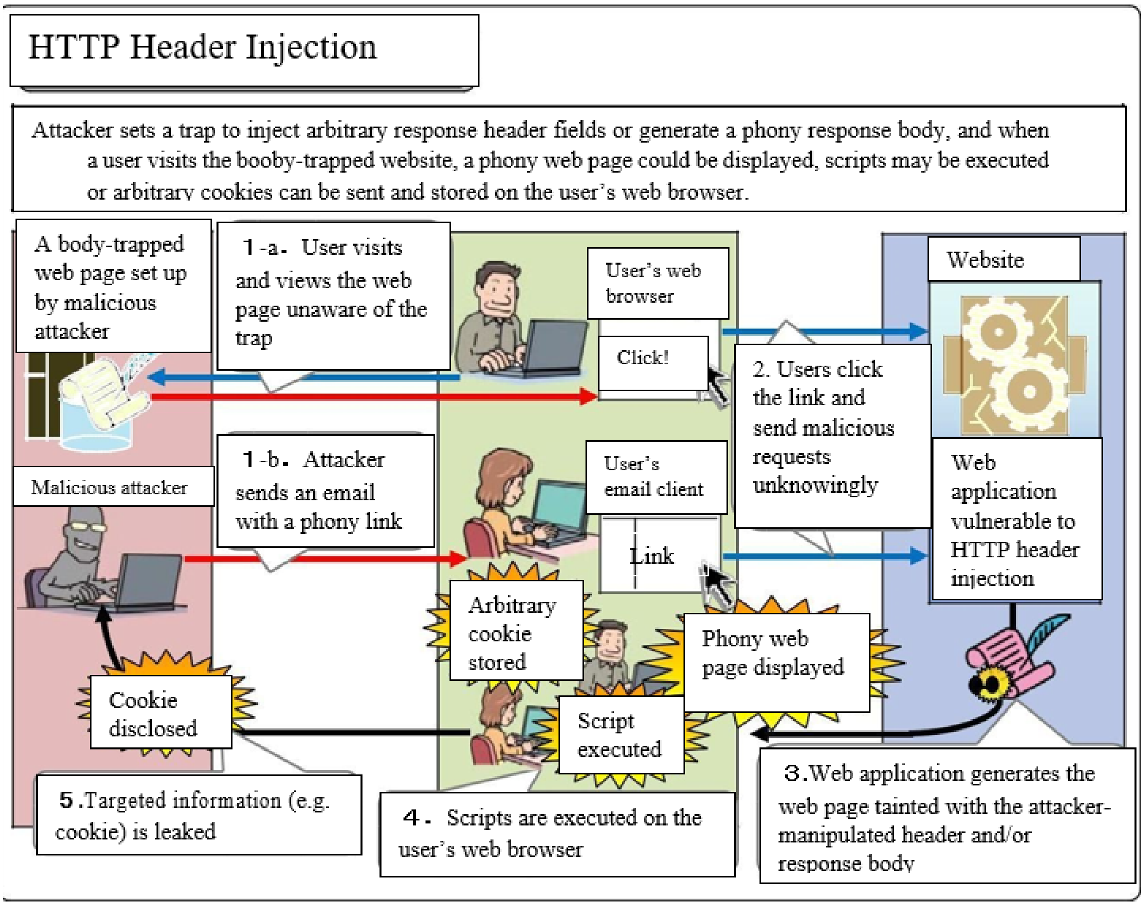
Make the system a launching point to attack others

・e.g. Denial of Service attack, reconnaissance and spamming

Websites That Need Special Attention Regardless of what kind of website it is or who operates it, special attention is needed if a website runs any web applications using the functions that are capable of calling external programs.

- **HTTP Header Injection**

Some web applications dynamically set the value of the HTTP response header fields based on the value passed by the external parameters. For example, HTTP redirection is implemented by setting a redirected-to URL specified in the parameter to the Location header field, or a web application may set the names entered in a bulletin board to the Set-Cookie header filed. If the process of building an HTTP response header in such web applications has vulnerabilities, an attacker could add header fields, manipulate the response body and have the web application generate multiple responses. This issue is called “HTTP Header Injection vulnerability” and the attack method exploiting this vulnerability is called “HTTP Header Injection attack”. In particular, the attack that leads the web application to produce multiple responses is called “HTTP Response Splitting attack”.


HTTP Header Injection
Attacker sets a trap to inject arbitrary response header fields or generate a phony response body, and when a user visits the booby-trapped website, a phony web page could be displayed, scripts may be executed or arbitrary cookies can be sent and stored on the user’s web browser.
A body-trapped web page set up by malicious attacker
１-a. User visits and views the web page unaware of the trap
User’s web browser
Click!
Website
2. Users click the link and send malicious requests unknowingly
Malicious attacker
１-b. Attacker sends an email with a phony link
User’s email client
Link
Web application vulnerable to HTTP header injection
Arbitrary cookie stored
Phony web page displayed
Cookie disclosed
Script executed
５.Targeted information (e.g. cookie) is leaked
４. Scripts are executed on the user’s web browser
３.Web application generates the web page tainted with the attacker-manipulated header and/or response body

Possible Threats

This vulnerability could allow malicious attackers to:

Present the same threats posed by the cross-site scripting vulnerability

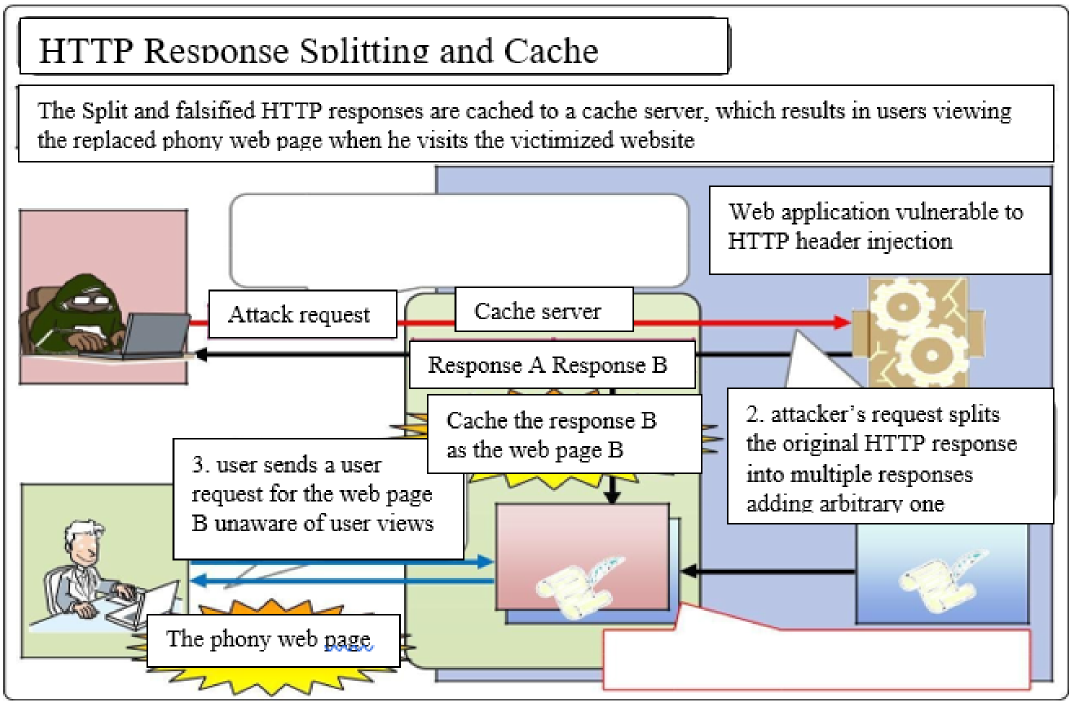
If an arbitrary response body is injected, the user's browser may result in displaying the false information or be forced to execute arbitrary scripts. Those are the same threats discussed earlier in "1.5 Cross-Site Scripting

Create arbitrary cookies

When an HTTP Set-Cookie header is inserted, an arbitrary cookie is created and stored in the user's browser.

Poison web cache

HTTP response splitting forces a web server to generate multiple HTTP responses and could inflict cache poisoning 27, which results in web page falsification, by having a proxy server cache an arbitrary HTTP response and replacing the original cached web page with it. The users visiting the victimized website are to view the replaced phony web page. Compared to the cross-site scripting attack, in which only a targeted individual would fall victim just once right after the attack, the threat cache poisoning poses would affect a larger number of users and last long time.

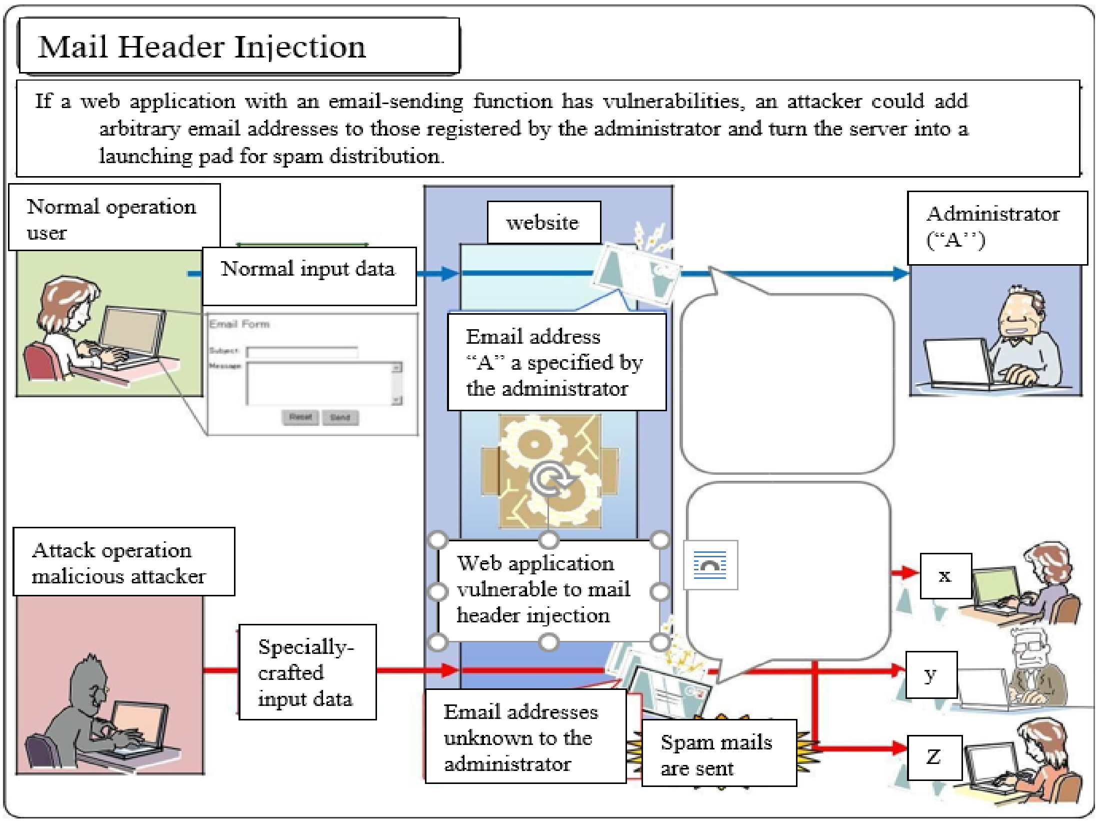

HTTP Response Splitting and Cache
The Split and falsified HTTP responses are cached to a cache server, which results in users viewing the replaced phony web page when he visits the victimized website
Web application vulnerable to HTTP header injection
Attack request
Cache server
Response A Response B
Cache the response B as the web page B
2. attacker's request splits the original HTTP response into multiple responses adding arbitrary one
3. user sends a user request for the web page B unaware of user views
The phony web page

Websites That Need Special Attention

Regardless of what kind of website it is or who operates it, the websites that dynamically set the value of the HTTP response header fields, such as the Location header field and the Set-Cookie header field, based on the values passed by the external parameters should be cautious about this vulnerability. The websites Reports related to HTTP header injection vulnerability account only a few percent of all website-related cases but it keeps coming up since we started receiving the reports. The following are some of the software products with this issue reported to IPA. The vulnerabilities in these products are now fixed.

- **Mail Header Injection**

Some web applications provide a function that sends emails to the particular email addresses about, for example, the merchandise the users have purchased or survey replies. In general, these email addresses are prespecified and only the web administrator can change. Depending on how it is implemented, however, an attacker may be able to set and change them to arbitrary email addresses. This vulnerability is called “Mail Header Injection” and the attacking method exploiting this vulnerability is called “Mail Header Injection attack”.


Mail Header Injection
If a web application with an email-sending function has vulnerabilities, an attacker could add arbitrary email addresses to those registered by the administrator and turn the server into a launching pad for spam distribution.
Normal operation user
Normal input data
Email Form
Subject
Message
Reset
Send
website
Administrator (“A””)
Email address “A” a specified by the administrator
Attack operation malicious attacker
Specially-crafted input data
Web application vulnerable to mail header injection
Email addresses unknown to the administrator
Spam mails are sent
x
y
Z

Possible Threats

This vulnerability could allow malicious attackers to:

Third party mail relay

Used as a launching pad for spam distribution.

Websites That Need Special Attention

The websites that have a function to send the user input data to the administrator via email should be warned of third-party mail relay. For example, a function like the “Contact” or “Survey” form could be susceptible.

Reported Vulnerabilities

Reports related to the vulnerabilities that enable Third Party Mail Relay attacks account only a few percent of all website-related vulnerabilities but it keeps coming up intermittently since we started receiving the reports. The following are some of the software products with this issue reported to IPA. The vulnerabilities in these products are now fixed.

For example, to prevent the line break, you can insert a space or horizontal tab after the line feed character to have the program process the lines as one continuous line, delete the characters after the line feed character or stop generating a web page if the line break is detected.

“Do not specify the email addresses in HTML “

This may sound absurd but it did happen nevertheless and we feel we should warn you not to specify the recipient email addresses directly in the hidden parameter.

Implementation like specifying recipient email addresses directly in a parameter that is to be passed to the web application may be exploited by the third-party mail relay attack by changing the parameter value.

Mitigation Measure

“Remove all line feed characters that appear in the external “

Remove all line feed characters that appear in the input text passed by the external parameters 30. You may even want to remove all control characters instead of just line feed characters. Note that if a web application performs the removal process on those that may contain line feeds, such as the mail contents, systematically removing every single line feed from all input data may hinder the web application’s proper operation and thus caution is advised.
By implementing these measures, security against Mail Header Injection is expected to improve. For more information on Mail Header Injection, you could refer to the following documents as well.

- ## Lack of Authentication and Authorization

There are some inadequately designed websites in operation due to lack of the operator’s security awareness. In this chapter, we will show you the vulnerabilities reported to us that stem form the lack of important functions such as “authentication” and “authorization”.

Lack of Authentication

Fundamental Solutions

“When a web site needs access control, implement an authentication mechanism that requires users to enter some kind of secret information such as password. “

Normally, when the website handles sensitive information or allows only the owner/provider of each information to change or edit the information, it needs an authentication mechanism.

However, there was a reported case about a vulnerable website where a user could login to the website and access the personal information by just providing his or her email address.

Email address is open information available to others and using such information to limit access to personal information means having almost no authentication mechanism at all 31 .

Design a web application to require something that people think it should be kept secret, such as Password.

Approaches to Improve Website Security

Secure Web Server

To safely operate a website, the administrator should not only secure web applications but also securely guard the web server. Use the following chapters as reference, and see if your web server’s settings and operation are secure.

“Check OS and software vulnerability information constantly and take necessary actions accordingly. “

Even though you implement an authentication mechanism to control access to the server, it can be breached if the attackers exploit the vulnerabilities in OS or applications. Vulnerabilities have been found on a daily basis. Check vulnerability information provided by OS and software vendors constantly and update software or practice necessary workarounds.

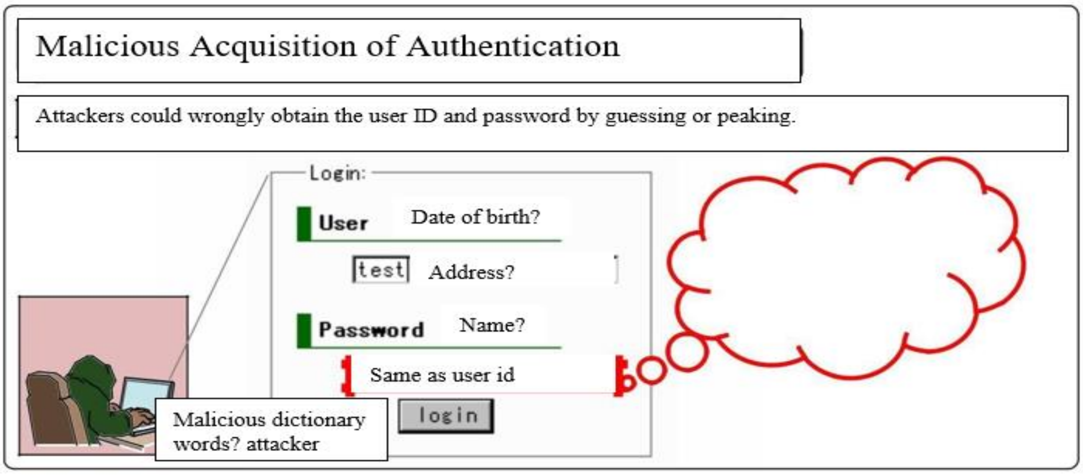
“Implement an authentication mechanism other than using passwords for remote server access. “

It is a common practice to allow remote access to the web server for management efficiency, but if

authentication is done by just password; its security may be breached by brute force attacks. To ensure higher security, we recommend the use of a cryptographic authentication method, such as public key authentication.

Secure Password

Most common way of implementing user authentication is to use a user ID /password pair. If password management and processing by the website are inappropriate, the risk of a malicious attacker stealing user authentication information becomes higher.


Malicious Acquisition of Authentication
Attackers could wrongly obtain the user ID and password by guessing or peaking.
Login:
User
Date of birth?
test
Address?
Password
Name?
Same as user id
login
Malicious dictionary words? attacker

One way to wrongly obtain the user ID or password is guessing it. This is often tried for the websites with a simple password scheme full of easy-to-guess passwords. How you display a web page may give out even more hints for attackers to work on. If the website has an authentication mechanism, be careful about the following points.

“Set hard-to-guess default passwords. “

When issuing a default password, use secure random numbers to eliminate regularity and, if possible, make it long and use alphabets, numbers and symbols. If password generation has regularity, an attacker could register more than once and try to work out the generation mechanism. Some users may never change their default password, thus making the default password difficult to guess is essential.

“Require users to enter the current password to change password. “

Make sure to require the user to enter the current password to change password

“Do not give away unnecessary hints in authentication error message. “

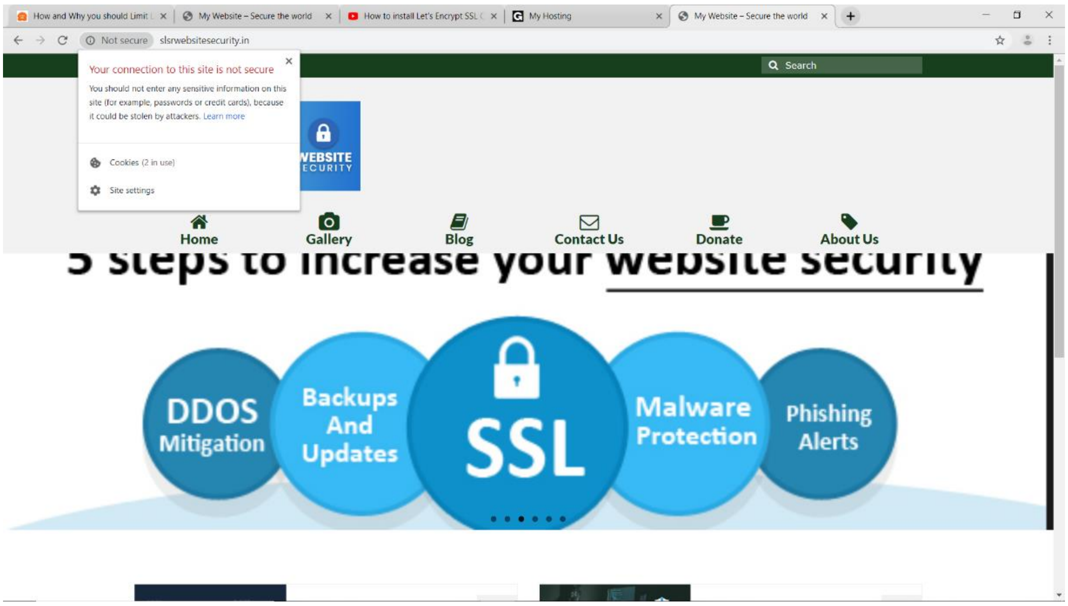
When a user makes a mistake in providing authentication information, returning “Password doesn’t match” on the error page would imply that “the user ID is correct”. This could help an attacker finds out the user IDs and thus not recommended. Make the error message like “Invalid user ID or password” and try not to give away clues possibly used to guess authentication information unnecessarily.

“Mask password being entered in the passwordbox. “

Mask the password entered by the user with asterisk (*).

- ## Changing HTTP to HTTPS

Before adding SSL Certificate



Not secure slsrwebsitesecurity.in

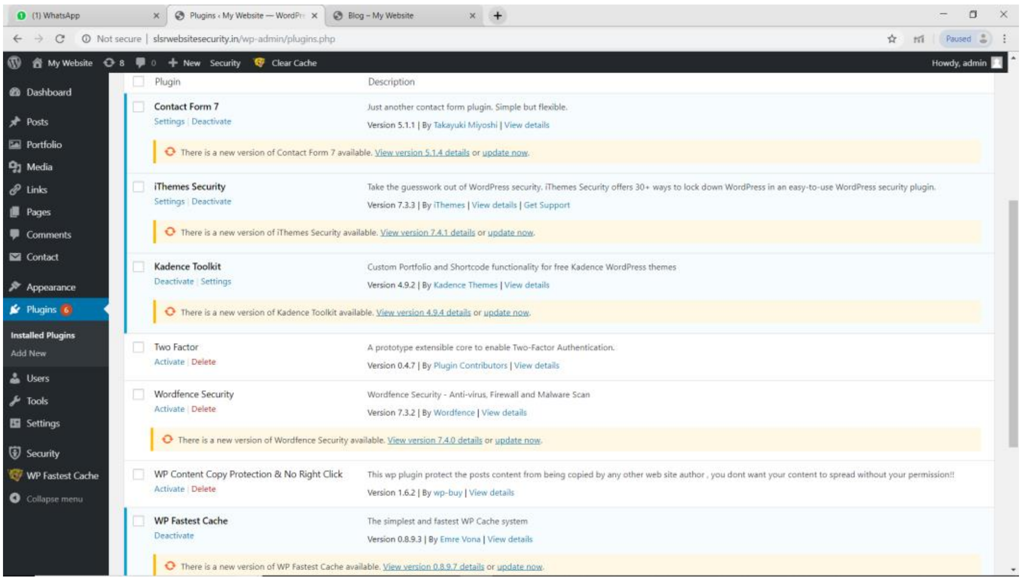
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies (2 in use)

Site settings

How and Why you should Limit
My Website – Secure the world
How to install Let's Encrypt SSL
My Hosting
My Website – Secure the world
Search
WEBSITE SECURITY
Home
Gallery
Blog
Contact Us
Donate
About Us
5 steps to increase your website security
DDOS Mitigation
Backups And Updates
SSL
Malware Protection
Phishing Alerts



□ Plugin	Description
□ Contact Form 7 Settings | Deactivate	Just another contact form plugin. Simple but flexible. Version 5.1.1 | By Takayuki Miyoshi | View details
	There is a new version of Contact Form 7 available. View version 5.1.4 details or update now.
□ iThemes Security Settings | Deactivate	Take the guesswork out of WordPress security. iThemes Security offers 30+ ways to lock down WordPress in an easy-to-use WordPress security plugin. Version 7.3.3 | By iThemes | View details | Get Support
	There is a new version of iThemes Security available. View version 7.4.1 details or update now.
□ Kadence Toolkit Deactivate | Settings	Custom Portfolio and Shortcode functionality for free Kadence WordPress themes Version 4.9.2 | By Kadence Themes | View details
	There is a new version of Kadence Toolkit available. View version 4.9.4 details or update now.
□ Two Factor Activate | Delete	A prototype extensible core to enable Two-Factor Authentication. Version 0.4.7 | By Plugin Contributors | View details
□ Wordfence Security Activate | Delete	Wordfence Security - Anti-virus, Firewall and Malware Scan Version 7.3.2 | By Wordfence | View details
	There is a new version of Wordfence Security available. View version 7.4.0 details or update now.
□ WP Content Copy Protection & No Right Click Activate | Delete	This wp plugin protect the posts content from being copied by any other web site author , you dont want your content to spread without your permission!! Version 1.6.2 | By wp-buy | View details
□ WP Fastest Cache Deactivate	The simplest and fastest WP Cache system Version 0.8.9.3 | By Emre Vona | View details
	There is a new version of WP Fastest Cache available. View version 0.8.9.7 details or update now.

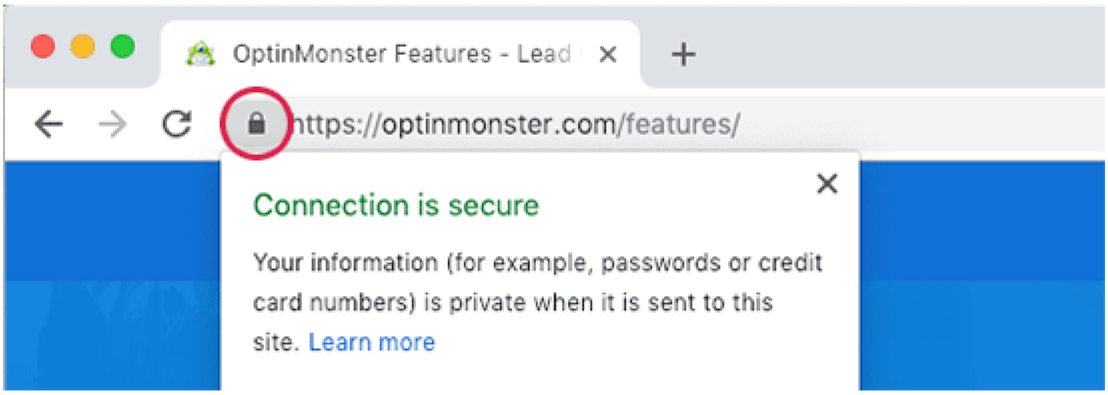
What is SSL?

SSL stands for Secure Sockets Layer. It is an internet protocol for securing data transfer between a user’s browser and the website they are visiting.

Every internet user transfers information when they visit websites. This information can often be sensitive like payment details, credit card information, or login credentials.

Using the normal HTTP protocol means this information can be hijacked by hackers. This is where SSL or HTTPS comes in.

Websites need an SSL certificate issued by one of the recognized certificates issuing authority. This certificate is verified and highlighted in the user’s browser address bar with a padlock sign and HTTPS instead of HTTP.



OptinMonster Features - Lead
https://optinmonster.com/features/

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Do We Need an SSL Certificate for My WordPress Website?

SSL / HTTPS is recommended for all websites on the internet. However, it is absolutely required for all websites that collect user information like login details, payment information, credit cards, and more.

If you are running an e-commerce store, a membership website, or require users to login, then you need to get an SSL certificate right away.

Most online payment services require your website to use SSL/HTTPs before you can receive payments.

Apart from security, SSL certificate also creates a positive impression of your brand among your users. Google also recommends using SSL, and research shows that SSL-enabled websites rank slightly higher in search results.

Last but not least, if your website is not using an SSL certificate, then Google Chrome will show your users that your website is not secure.

How to Setup Cloudflare Flexible SSL for WordPress

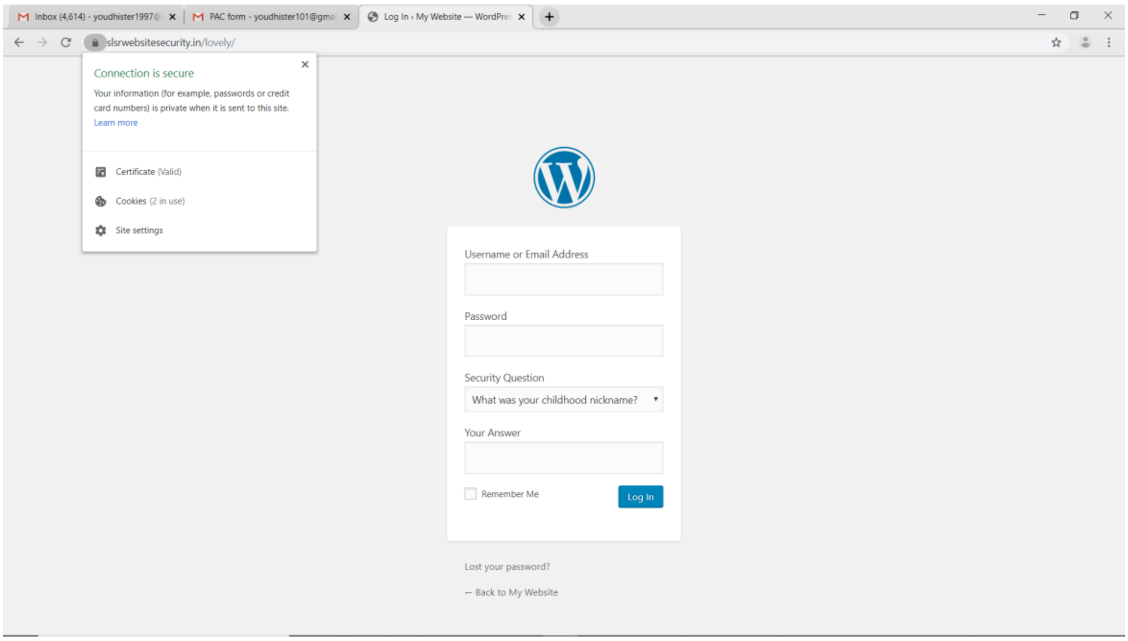
As we all know Google has announced that it will be counting HTTPS as a ranking factor now. That means if you use HTTPS it will increase the chances of Google ranking you higher in its searches results.

Previously switching to HTTPS was expensive and technical having to buy SSL certificates and install them yourself. Thankfully Cloudflare have released a free version that does exactly the same job and is easier to set up.

Setting up your free Cloudflare Flexible SSL

1. Sign up to Cloudflare
2. Select the free plan
3. Follow the step for adding your domain name
4. When you have registered and set up your domain name, click on your domain
5. At the top there will be a row of icons click on Crypto
6. The first option will be SSL, select flexible SSL

After adding SSL Certificate


Inbox (4,614) - youdhister1997@
PAC form - youdhister101@gma
Log In ‹ My Website — WordPre
slsrwebsitesecurity.in/lovely/

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)
Cookies (2 in use)
Site settings

Username or Email Address

Password

Security Question

What was your childhood nickname?

Your Answer

□ Remember Me

Log In
Lost your password?
← Back to My Website

Here the site secured and the users will have trust on it.

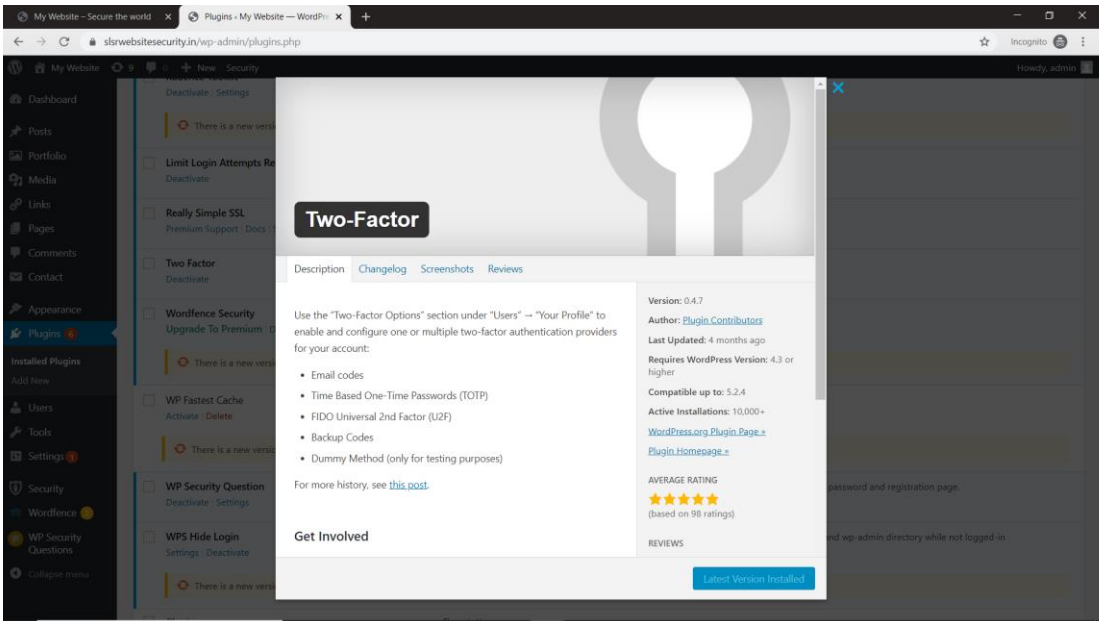
8. PLUGINS

A plugin is a piece of software containing a group of functions that can be added to a WordPress website. They can extend functionality or add new features to your WordPress websites.

WordPress plugins are written in the PHP programming language and integrate seamlessly with WordPress. In the WordPress community, there is a saying that goes around: “there’s a plugin for that”. They make it easier for users to add features to their website without knowing a single line of code.

Two Factor

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access



Use the “Two-Factor Options” section under “Users” → “Your Profile” to enable and configure one or multiple two-factor authentication providers for your account:

- Email codes
- Time Based One-Time Passwords (TOTP)
- FIDO Universal 2nd Factor (U2F)
- Backup Codes
- Dummy Method (only for testing purposes)

For more history, see this post.

Version: 0.4.7

Author: Plugin Contributors

Last Updated: 4 months ago

Requires WordPress Version: 4.3 or higher

Compatible up to: 5.2.4

Active Installations: 10,000+

WordPress.org Plugin Page »

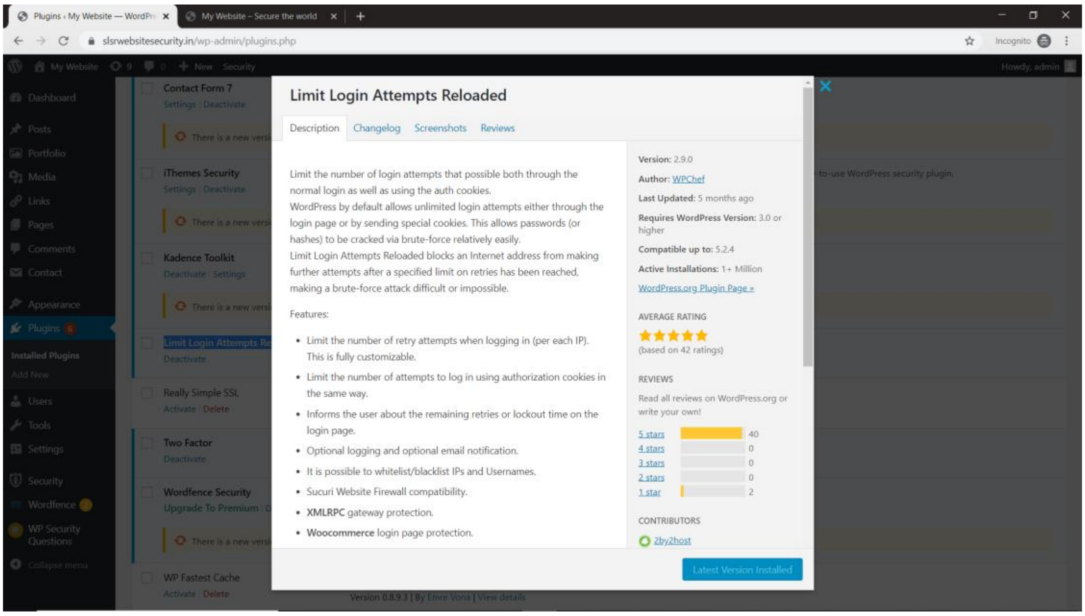
Plugin Homepage »

★★★★★ (based on 98 ratings)

Figure *8.1 PLUGINS*

Limit Login Attempts Reloaded

Limit the number of retry attempts when logging in (per each IP). This is fully customizable. Limit the number of attempts to log in using authorization cookies in the same way. Informs the user about the remaining retries or lockout time on the login page.



Plugins ‹ My Website — WordPress
My Website – Secure the world
slsrwebsitesecurity.in/wp-admin/plugins.php
Incognito
Description
Changelog
Screenshots
Reviews
Latest Version Installed

Limit Login Attempts Reloaded

Limit the number of login attempts that possible both through the normal login as well as using the auth cookies.
WordPress by default allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be cracked via brute-force relatively easily.
Limit Login Attempts Reloaded blocks an Internet address from making further attempts after a specified limit on retries has been reached, making a brute-force attack difficult or impossible.

Features:

- Limit the number of retry attempts when logging in (per each IP). This is fully customizable.
- Limit the number of attempts to log in using authorization cookies in the same way.
- Informs the user about the remaining retries or lockout time on the login page.
- Optional logging and optional email notification.
- It is possible to whitelist/blacklist IPs and Usernames.
- Sucuri Website Firewall compatibility.
- **XMLRPC** gateway protection.
- **Woocommerce** login page protection.

Version: 2.9.0
Author: WPChef
Last Updated: 5 months ago
Requires WordPress Version: 3.0 or higher
Compatible up to: 5.2.4
Active Installations: 1+ Million
WordPress.org Plugin Page »

AVERAGE RATING
★★★★★
(based on 42 ratings)

REVIEWS
Read all reviews on WordPress.org or write your own!

5 stars	40
4 stars	0
3 stars	0
2 stars	0
1 star	2

CONTRIBUTORS
2by2host

Figure 8.2 PLUGINS

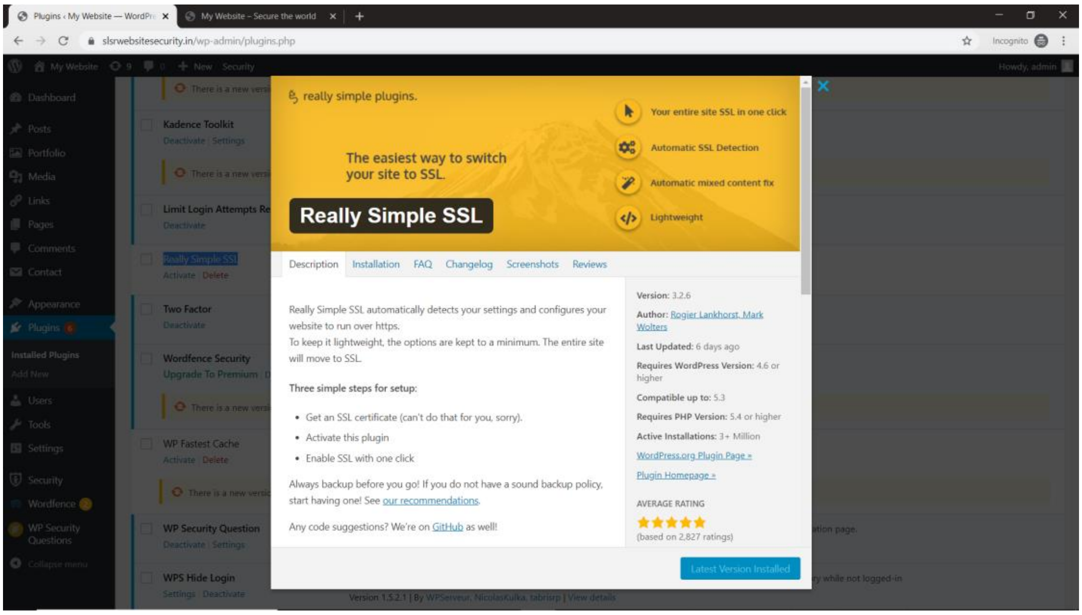
Really Simple SSL

Really Simple SSL automatically detects your settings and configures your website to run over https. To keep it lightweight, the options are kept to a minimum. The entire site will move to SSL.

Get an SSL certificate (can’t do that for you, sorry).

Activate this plugin

Enable SSL with one click



Plugins ‹ My Website — WordPress
My Website – Secure the world
slsrwebsitesecurity.in/wp-admin/plugins.php
Incognito
really simple plugins.
The easiest way to switch your site to SSL.
Really Simple SSL
Your entire site SSL in one click
Automatic SSL Detection
Automatic mixed content fix
Lightweight
Description
Installation
FAQ
Changelog
Screenshots
Reviews
Latest Version Installed

Really Simple SSL automatically detects your settings and configures your website to run over https.
To keep it lightweight, the options are kept to a minimum. The entire site will move to SSL.

Three simple steps for setup:

- Get an SSL certificate (can't do that for you, sorry).
- Activate this plugin
- Enable SSL with one click

Always backup before you go! If you do not have a sound backup policy, start having one! See our recommendations.

Any code suggestions? We're on GitHub as well!

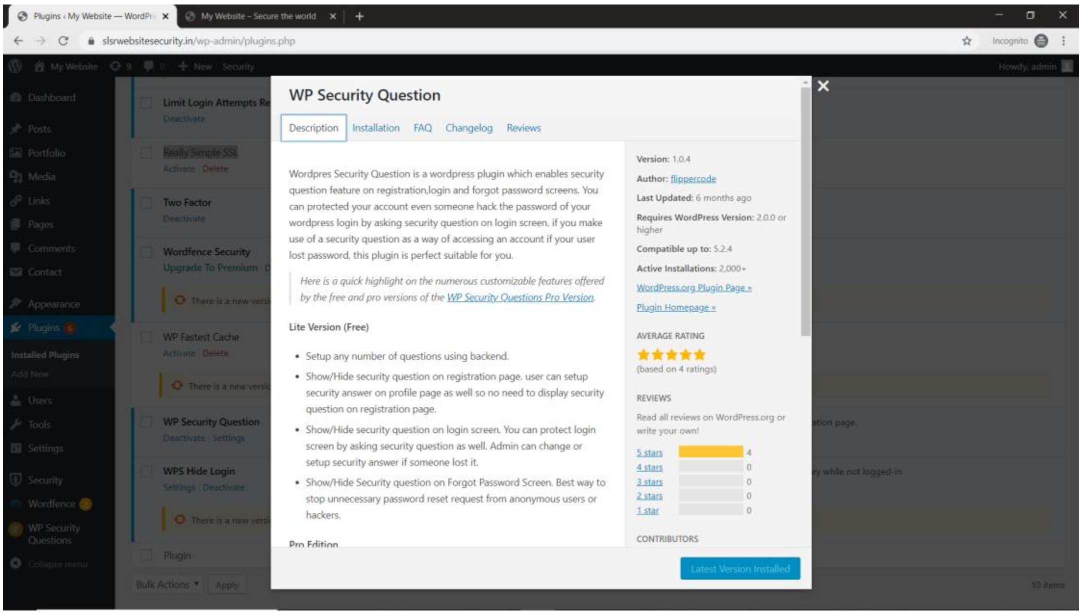
Version: 3.2.6
Author: Rogier Lankhorst, Mark Wolters
Last Updated: 6 days ago
Requires WordPress Version: 4.6 or higher
Compatible up to: 5.3
Requires PHP Version: 5.4 or higher
Active Installations: 3+ Million
WordPress.org Plugin Page »
Plugin Homepage »

AVERAGE RATING
★★★★★
(based on 2,827 ratings)

Figure 8.3 PLUGINS

WP Security Question

WordPress Security Question is a WordPress plugin which enables security question feature on registration, login and forgot password screens. You can protect your account even someone hack the password of your WordPress login by asking security question on login screen. if you make use of a security question as a way of accessing an account if your user lost password, this plugin is perfect suitable for you



WP Security Question

Description | Installation | FAQ | Changelog | Reviews

Wordpres Security Question is a wordpress plugin which enables security question feature on registration,login and forgot password screens. You can protected your account even someone hack the password of your wordpress login by asking security question on login screen. if you make use of a security question as a way of accessing an account if your user lost password, this plugin is perfect suitable for you.

> *Here is a quick highlight on the numerous customizable features offered by the free and pro versions of the WP Security Questions Pro Version.*

Lite Version (Free)

- Setup any number of questions using backend.
- Show/Hide security question on registration page. user can setup security answer on profile page as well so no need to display security question on registration page.
- Show/Hide security question on login screen. You can protect login screen by asking security question as well. Admin can change or setup security answer if someone lost it.
- Show/Hide Security question on Forgot Password Screen. Best way to stop unnecessary password reset request from anonymous users or hackers.

Pro Edition

Version: 1.0.4

Author: flippercode

Last Updated: 6 months ago

Requires WordPress Version: 2.0.0 or higher

Compatible up to: 5.2.4

Active Installations: 2,000+

WordPress.org Plugin Page »

Plugin Homepage »

AVERAGE RATING

★★★★★
(based on 4 ratings)

REVIEWS

Read all reviews on WordPress.org or write your own!

5 stars	4
4 stars	0
3 stars	0
2 stars	0
1 star	0

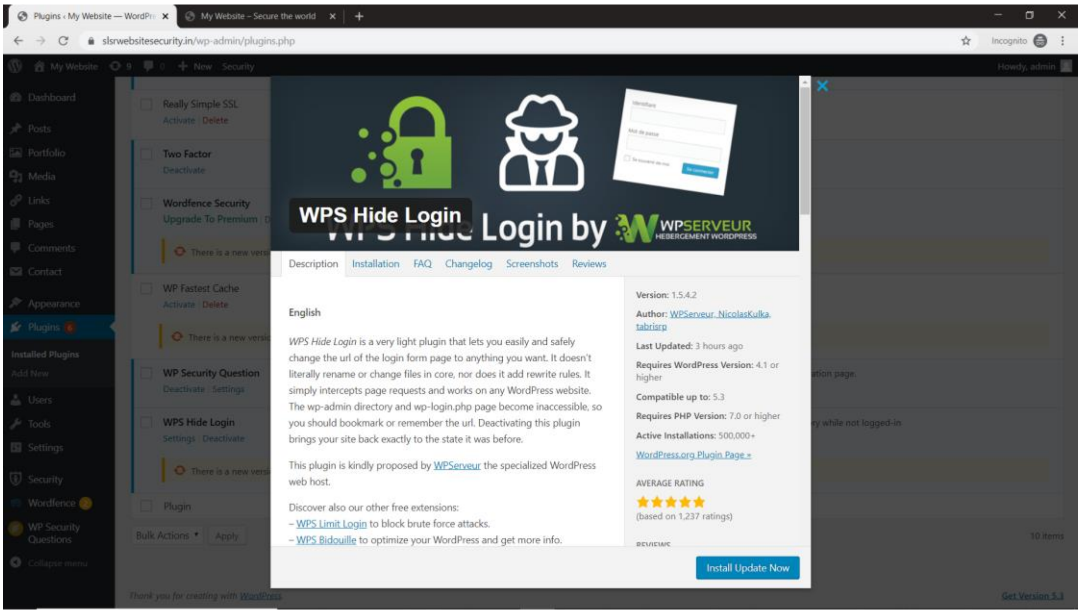
CONTRIBUTORS

Latest Version Installed

Figure 8.4 PLUGINS

WPS Hide Login

WPS Hide Login is a very light plugin that lets you easily and safely change the url of the login form page to anything you want. It doesn’t literally rename or change files in core, nor does it add rewrite rules. It simply intercepts page requests and works on any WordPress website. The wp-admin directory and wp-login.php page become inaccessible, so you should bookmark or remember the url. Deactivating this plugin brings your site back exactly to the state it was before.



English

WPS Hide Login is a very light plugin that lets you easily and safely change the url of the login form page to anything you want. It doesn't literally rename or change files in core, nor does it add rewrite rules. It simply intercepts page requests and works on any WordPress website. The wp-admin directory and wp-login.php page become inaccessible, so you should bookmark or remember the url. Deactivating this plugin brings your site back exactly to the state it was before.

This plugin is kindly proposed by WPServeur the specialized WordPress web host.

Discover also our other free extensions:
– WPS Limit Login to block brute force attacks.
– WPS Bidouille to optimize your WordPress and get more info.

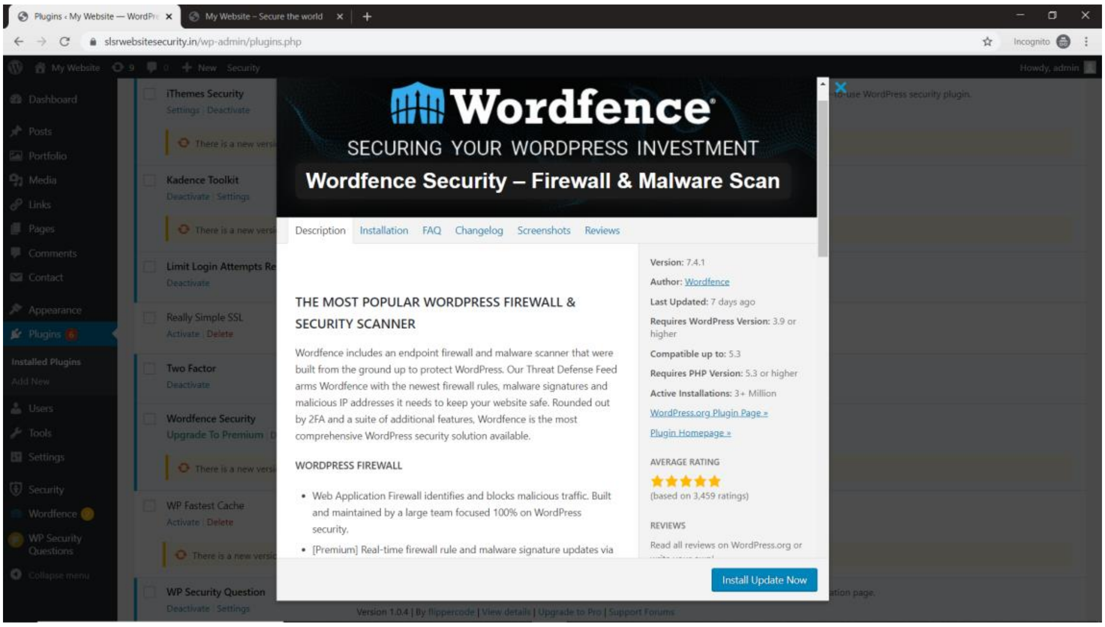
Version: 1.5.4.2
Author: WPServeur, NicolasKulka, tabrisrp
Last Updated: 3 hours ago
Requires WordPress Version: 4.1 or higher
Compatible up to: 5.3
Requires PHP Version: 7.0 or higher
Active Installations: 500,000+
WordPress.org Plugin Page »

AVERAGE RATING
★★★★★
(based on 1,237 ratings)

Figure 8.5 PLUGINS

Wordfence Security

Wordfence includes an endpoint firewall and malware scanner that were built from the ground up to protect WordPress. Our Threat Defense Feed arms Wordfence with the newest firewall rules, malware signatures and malicious IP addresses it needs to keep your website safe. Rounded out by 2FA and a suite of additional features, Wordfence is the most comprehensive WordPress security solution available.



THE MOST POPULAR WORDPRESS FIREWALL & SECURITY SCANNER

Wordfence includes an endpoint firewall and malware scanner that were built from the ground up to protect WordPress. Our Threat Defense Feed arms Wordfence with the newest firewall rules, malware signatures and malicious IP addresses it needs to keep your website safe. Rounded out by 2FA and a suite of additional features, Wordfence is the most comprehensive WordPress security solution available.

WORDPRESS FIREWALL

- Web Application Firewall identifies and blocks malicious traffic. Built and maintained by a large team focused 100% on WordPress security.
- [Premium] Real-time firewall rule and malware signature updates via

Version: 7.4.1
Author: Wordfence
Last Updated: 7 days ago
Requires WordPress Version: 3.9 or higher
Compatible up to: 5.3
Requires PHP Version: 5.3 or higher
Active Installations: 3+ Million
WordPress.org Plugin Page »
Plugin Homepage »

AVERAGE RATING
★★★★★
(based on 3,459 ratings)

REVIEWS
Read all reviews on WordPress.org or

Figure 8.6 PLUGINS

9. TESTING

Testing is the process of executing the program to find if there are any errors. It is the final verification and validation activity. In testing phase, we have tried to affirm the quality of the product. We have also tried to eliminate errors in the previous stages. **Why testing is done**

- Testing is the process of running a system with the intention of finding errors.
- Testing enhances the integrity of a system by detecting deviations in design and errors in the system.
- Testing aims at detecting error-prone areas. This helps in the prevention of errors in a system.
- Testing also add value to the product by confirming to the user requirements.

Causes of Errors

The most common causes of errors in a software system are:

- **Communication gap between the developer and the business decision maker**: A communication gap between the developer and the business decision maker is normally due to subtle differences between them. The differences can be classified into five broad areas: Thought process, Background and Experience, Interest, Priorities, Language.
- **Time provided to a developer to complete the project:** A common source of errors in projects comes from time constraints in delivering a product. To keep to the schedule, features can be cut. To keep the features, the schedule can be slipped. Failing to adjust the feature set or schedule when problems are discovered can lead to rushed work and flawed systems.
- **Over Commitment by the developer:** High enthusiasm can lead to over commitment by the developer. In these situations, developers are usually unable to adhere to deadlines or quality due to lack of resources or required skills on the team.
- **Insufficient testing and quality control**: Insufficient testing is also a major source of breakdown of e-commerce systems during operations, as testing must be done during all phases of development.
- **Inadequate requirements gathering**: A short time to market results in developers starting work on the Web site development without truly understanding the business and

technical requirements. Also, developers may create client-side scripts using language that may not work on some client browsers.

Keeping pace with the fast-changing Technology: New technologies are constantly introduced. There may not be adequate time to develop expertise in the new technologies. This is a problem for two reasons. First, the technology may not be properly implemented. Second, the technology may not integrate well with the existing environment.

Testing Principles

- To discover as yet undiscovered errors.
- All tests should be traceable to customer's requirement.
- Tests should be planned long before the testing actually begins.
- Testing should begin "in the small" & progress towards "testing in the large".
- Exhaustive Testing is not possible.
- To be most effective training should be conducted by an Independent Third-Party **Testing Objectives**
- Testing is a process of executing a program with the intent of finding errors.
- A good test case is one that has a high probability of finding an as yet undiscovered error.
- A successful test is one that uncovers an as yet undiscovered error.

Kinds of Testing

- **Black Box Testing-** Not based on any knowledge of internal designs or code. Tests are based on requirements and functionality.
- **White Box Testing-** Based on the knowledge of the internal logic of an application's code. Tests are based on coverage of code statements, branches, paths and statements. • **Unit Testing-** The most 'micro' scale of testing; to test particular functions and code modules. Typically done by the programmer and not by the testers, as it requires detailed knowledge of the internal program design and code. Not always easily done unless the application has a well-designed architecture with tight code; may require developing test driver modules or test harnesses.
- **Integration Testing-** Testing of combined parts of an application to determine if they function together correctly. The 'parts' can be code modules, individual applications, client and server applications on a network, etc. This type of testing is especially relevant to client/ server and distributed systems.

- **Functional Testing-** Black-box type testing geared to functional requirements of an application; testers should do this type of testing. This doesn't mean that the programmers shouldn't check that their code works before releasing it.
- **Regression Testing-** Re-testing after fixes or modifications of the software or its environment. It is difficult to determine how much re testing is needed, especially near the end of the development cycle. Automated testing tools can be especially useful for this type of testing.
- **Acceptance Testing-** Final testing based on the specifications of the end user or customer or based on use by end-users/ customers over some limited period of time.
- **User Acceptance Testing-** Determining if software is satisfactory to an end user customer

STRATEGIC APPROACH TO SOFTWARE TESTING

The software engineering process can be viewed as a spiral. Initially system engineering defines the role of software and leads to software requirement analysis where the information domain, functions, behaviour, performance, constraints and validation criteria for software are established. Moving inward along the spiral, we come to design and finally to coding. To develop computer software, we spiral in along streamlines that decrease the level of abstraction on each turn. A strategy for software testing may also be viewed in the context of the spiral. Unit testing begins at the vertex of the spiral and concentrates on each unit of the software as implemented in source code. Testing progress by moving outward along the spiral to integration testing, where the focus is on the design and the construction of the software architecture. Talking another turn on outward on the spiral we encounter validation testing where requirements established as part of software requirements analysis are validated against the software that has been constructed. Finally, we arrive at system testing, where the software and other system elements are tested as a whole.

Unit Testing

Unit testing focuses verification effort on the smallest unit of software design, the module. The unit testing, we have is white box oriented and some modules the steps are conducted in parallel.

White Box

Testing This type of testing ensures that

- All independent paths have been exercised at least once.
- All logical decisions have been exercised on their true and false sides.
- All loops are executed at their boundaries and within their operational bounds.
- All internal data structures have been exercised to assure their validity.

To follow the concept of white box testing we have tested each form .we have created independently to verify that Data flow is correct, All conditions are exercised to check their validity, All loops are executed on their boundaries.

BASIC PATH TESTING

Established technique of flow graph with cyclomatic complexity was used to derive test cases for all the functions. The main steps in deriving test cases were: Use the design of the code and draw correspondent flow graph.

CONDITIONAL TESTING

In this part of the testing each of the conditions were tested to both true and false aspects. And all the resulting paths were tested. So that each path that may be generate on particular condition is traced to uncover any possible errors.

DATA FLOW TESTING

This type of testing selects the path of the program according to the location of definition and use of variables. This kind of testing was used only when some local variable was declared. The definition-use chain method was used in this type of testing. These were particularly useful in nested statements.

LOOP TESTING

In this type of testing all the loops are tested to all the limits possible. The following exercise was adopted for all loops:

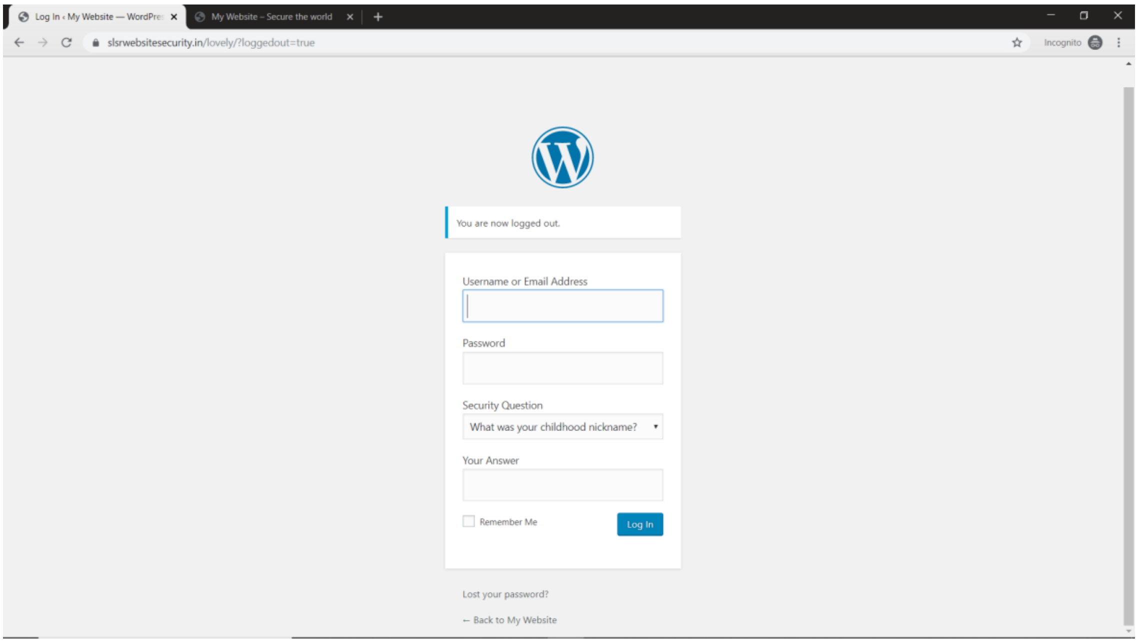
- All the loops were tested at their limits, just above them and just below them.
- All the loops were skipped at least once.
- For nested loops test the inner most loop first and then work outwards.
- For concatenated loops the values of dependent loops were set with the help of connected loop.
- Unstructured loops were resolved into nested loops or concatenated loops and tested as above.

Each unit has been separately tested by the development team itself and all the input have been validated

10. SCREENSHOT

Login Details

Provide Login details like username and password. Enter the correct login details.


Log In ‹ My Website — WordPre
My Website – Secure the world
slsrwebsitesecurity.in/lovely/?loggedout=true
Incognito

You are now logged out.

Username or Email Address

Password

Security Question

What was your childhood nickname?

Your Answer

□ Remember Me

Log In

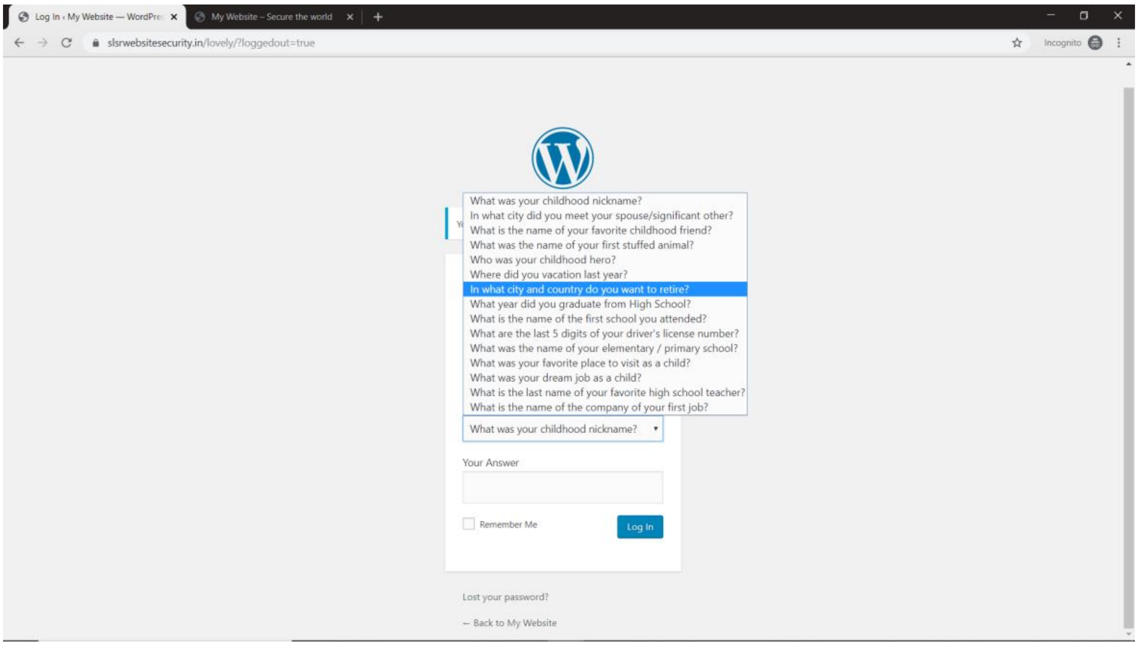
Lost your password?

← Back to My Website

Figure 10.1 SCREENSHOT

Security Question

Here they are list of security questions available select the correct question and provide exact answer to the question.


Log In ‹ My Website — WordPre
My Website – Secure the world
slsrwebsitesecurity.in/lovely/?loggedout=true
Incognito

- What was your childhood nickname?
- In what city did you meet your spouse/significant other?
- What is the name of your favorite childhood friend?
- What was the name of your first stuffed animal?
- Who was your childhood hero?
- Where did you vacation last year?
- In what city and country do you want to retire?
- What year did you graduate from High School?
- What is the name of the first school you attended?
- What are the last 5 digits of your driver's license number?
- What was the name of your elementary / primary school?
- What was your favorite place to visit as a child?
- What was your dream job as a child?
- What is the last name of your favorite high school teacher?
- What is the name of the company of your first job?

What was your childhood nickname?

Your Answer

□ Remember Me

Log In

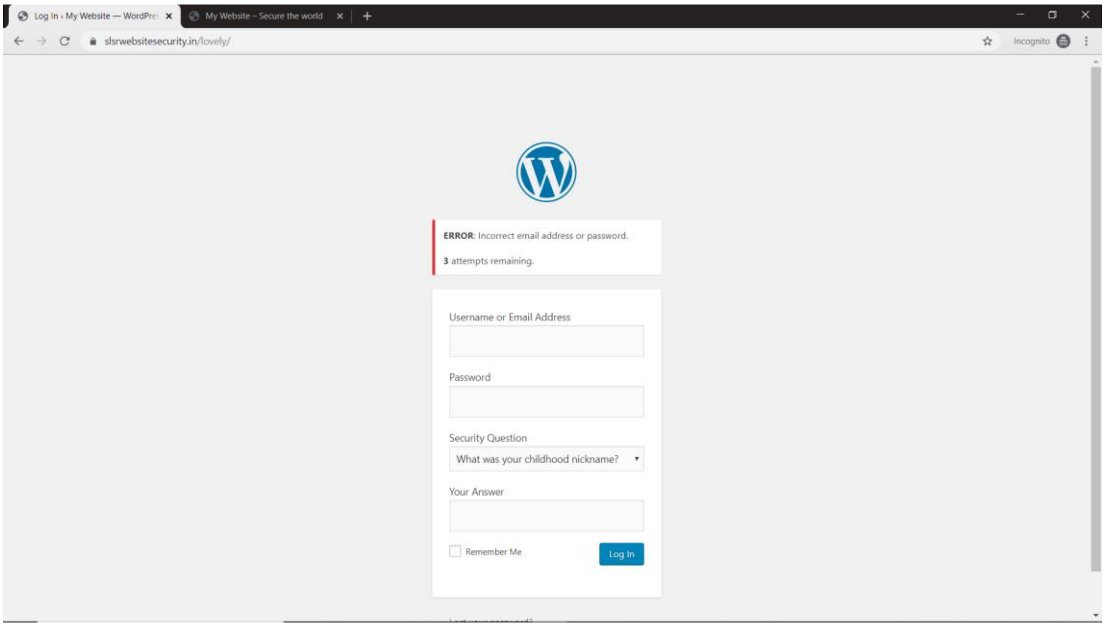
Lost your password?

← Back to My Website

Figure 10.2 SCREENSHOT

Failed login attempts

If you provide wrong login credentials it will give an error and if this continues for more than 4 types the respective ip address will be blocked and have to wait for specific time to continue again,



Log In ‹ My Website — WordPre
My Website – Secure the world
slsrwebsitesecurity.in/lovely/
Incognito

ERROR: Incorrect email address or password.

3 attempts remaining.

Username or Email Address

Password

Security Question: What was your childhood nickname?

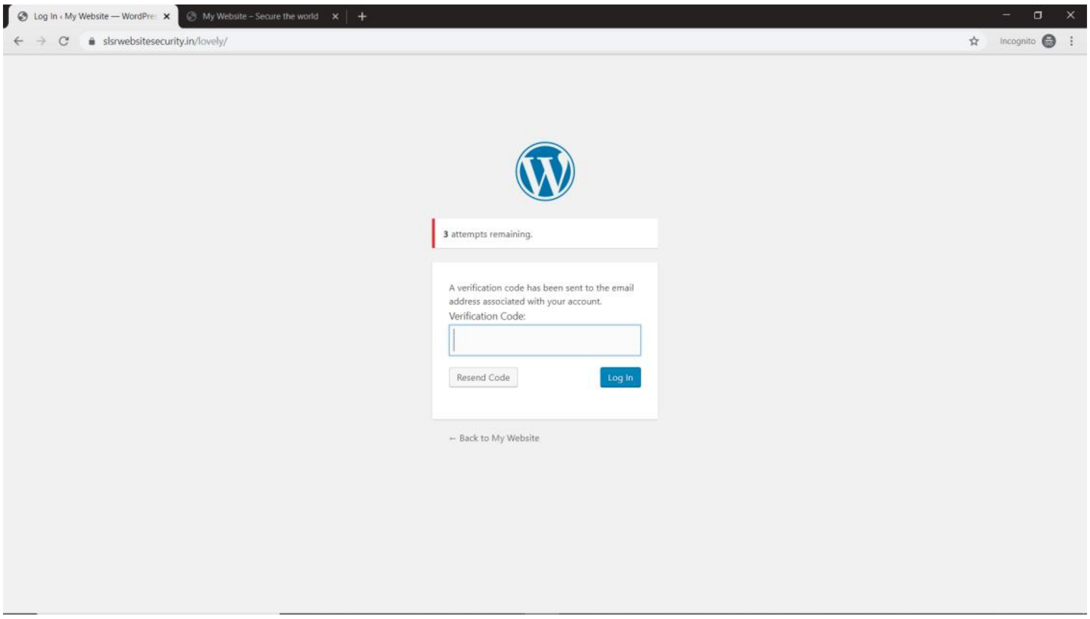
Your Answer

□ Remember Me

Figure 10.3 SCREENSHOT

OTP VERIFICATION

OTP verification is the main security feature and it will be sent for registered mail address.



Log In ‹ My Website — WordPre
My Website – Secure the world
slsrwebsitesecurity.in/lovely/
Incognito

3 attempts remaining.

A verification code has been sent to the email address associated with your account.

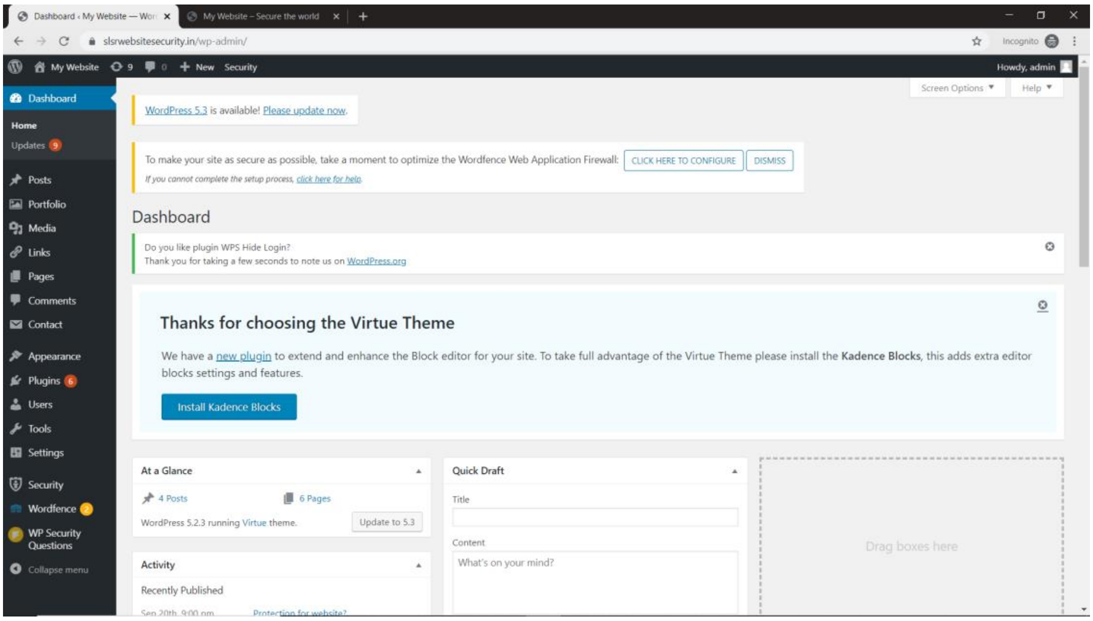
Verification Code:

Resend Code
Log In
← Back to My Website

Figure 10.4 SCREENSHOT

Dashboard

In the dashboard we can the all the available options to add or remove the plugin.



WordPress 5.3 is available! Please update now.

To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall:

If you cannot complete the setup process, click here for help.

Dashboard

Do you like plugin WPS Hide Login?
Thank you for taking a few seconds to note us on WordPress.org

Thanks for choosing the Virtue Theme

We have a new plugin to extend and enhance the Block editor for your site. To take full advantage of the Virtue Theme please install the **Kadence Blocks**, this adds extra editor blocks settings and features.

At a Glance

4 Posts 6 Pages

WordPress 5.2.3 running Virtue theme.

Activity

Recently Published

Sep 20th, 9:00 pm Protection for website?

Quick Draft

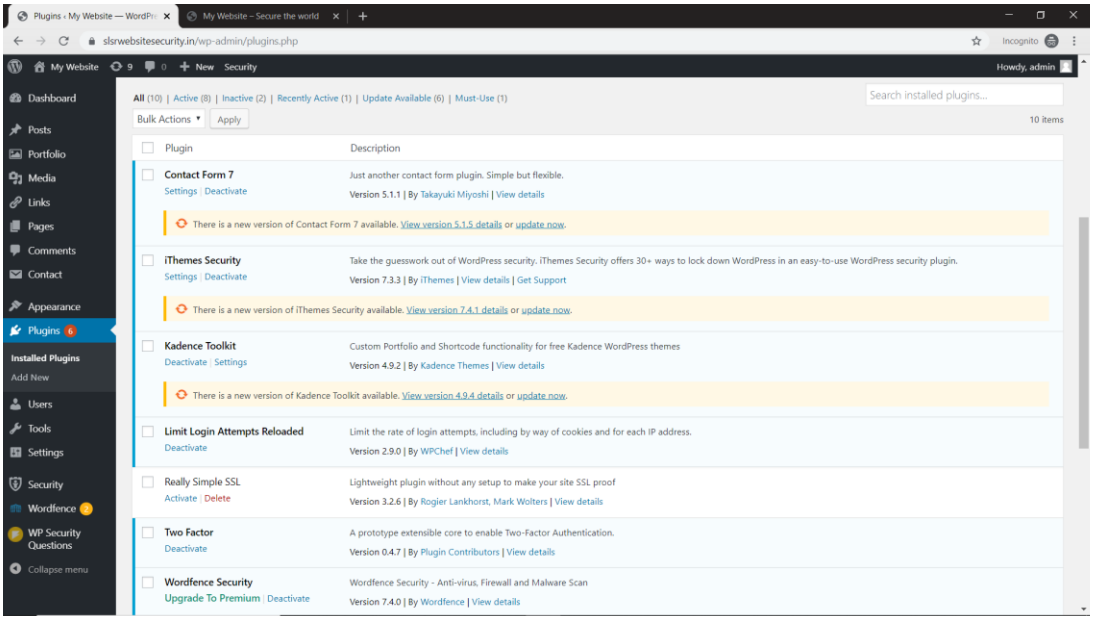
Title:

Content: What's on your mind?

Figure 10.5 SCREENSHOT

Plugins

In the plugins section you will be able to add or remove the plugins and can update the plugin to the latest version available.



All (10) | Active (8) | Inactive (2) | Recently Active (1) | Update Available (6) | Must-Use (1)

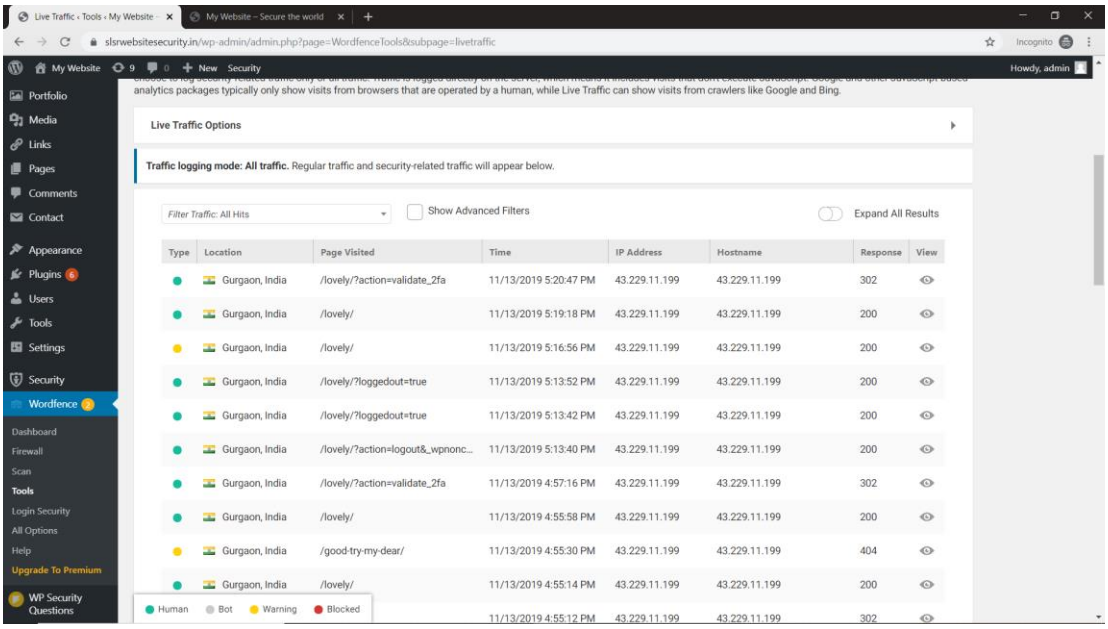
10 items

Plugin	Description
□ Contact Form 7 Settings | Deactivate	Just another contact form plugin. Simple but flexible. Version 5.1.1 | By Takayuki Miyoshi | View details
	There is a new version of Contact Form 7 available. View version 5.1.5 details or update now.
□ iThemes Security Settings | Deactivate	Take the guesswork out of WordPress security. iThemes Security offers 30+ ways to lock down WordPress in an easy-to-use WordPress security plugin. Version 7.3.3 | By iThemes | View details | Get Support
	There is a new version of iThemes Security available. View version 7.4.1 details or update now.
□ Kadence Toolkit Deactivate | Settings	Custom Portfolio and Shortcode functionality for free Kadence WordPress themes Version 4.9.2 | By Kadence Themes | View details
	There is a new version of Kadence Toolkit available. View version 4.9.4 details or update now.
□ Limit Login Attempts Reloaded Deactivate	Limit the rate of login attempts, including by way of cookies and for each IP address. Version 2.9.0 | By WPChef | View details
□ Really Simple SSL Activate | Delete	Lightweight plugin without any setup to make your site SSL proof Version 3.2.6 | By Rogier Lankhorst, Mark Wolters | View details
□ Two Factor Deactivate	A prototype extensible core to enable Two-Factor Authentication. Version 0.4.7 | By Plugin Contributors | View details
□ Wordfence Security Upgrade To Premium | Deactivate	Wordfence Security - Anti-virus, Firewall and Malware Scan Version 7.4.0 | By Wordfence | View details

Figure 10.6 SCREENSHOT

Visitors

Using word fence plugin you will be able to see the visitors to your site and can block them according to their action



analytics packages typically only show visits from browsers that are operated by a human, while Live Traffic can show visits from crawlers like Google and Bing.

Live Traffic Options

Traffic logging mode: All traffic. Regular traffic and security-related traffic will appear below.

Filter Traffic: All Hits

□ Show Advanced Filters

Expand All Results

Type	Location	Page Visited	Time	IP Address	Hostname	Response	View
🟢	Gurgaon, India	/lovely/?action=validate_2fa	11/13/2019 5:20:47 PM	43.229.11.199	43.229.11.199	302	👁
🟢	Gurgaon, India	/lovely/	11/13/2019 5:19:18 PM	43.229.11.199	43.229.11.199	200	👁
🟡	Gurgaon, India	/lovely/	11/13/2019 5:16:56 PM	43.229.11.199	43.229.11.199	200	👁
🟢	Gurgaon, India	/lovely/?loggedout=true	11/13/2019 5:13:52 PM	43.229.11.199	43.229.11.199	200	👁
🟢	Gurgaon, India	/lovely/?loggedout=true	11/13/2019 5:13:42 PM	43.229.11.199	43.229.11.199	200	👁
🟢	Gurgaon, India	/lovely/?action=logout&_wpnonc...	11/13/2019 5:13:40 PM	43.229.11.199	43.229.11.199	200	👁
🟢	Gurgaon, India	/lovely/?action=validate_2fa	11/13/2019 4:57:16 PM	43.229.11.199	43.229.11.199	302	👁
🟢	Gurgaon, India	/lovely/	11/13/2019 4:55:58 PM	43.229.11.199	43.229.11.199	200	👁
🟡	Gurgaon, India	/good-try-my-dear/	11/13/2019 4:55:30 PM	43.229.11.199	43.229.11.199	404	👁
🟢	Gurgaon, India	/lovely/	11/13/2019 4:55:14 PM	43.229.11.199	43.229.11.199	200	👁
			11/13/2019 4:55:12 PM	43.229.11.199	43.229.11.199	302	👁

🟢 Human ⚪ Bot 🟡 Warning 🔴 Blocked

Figure 10.7 SCREENSHOT

Website

This the final website where users can access the website and can get the information provided.

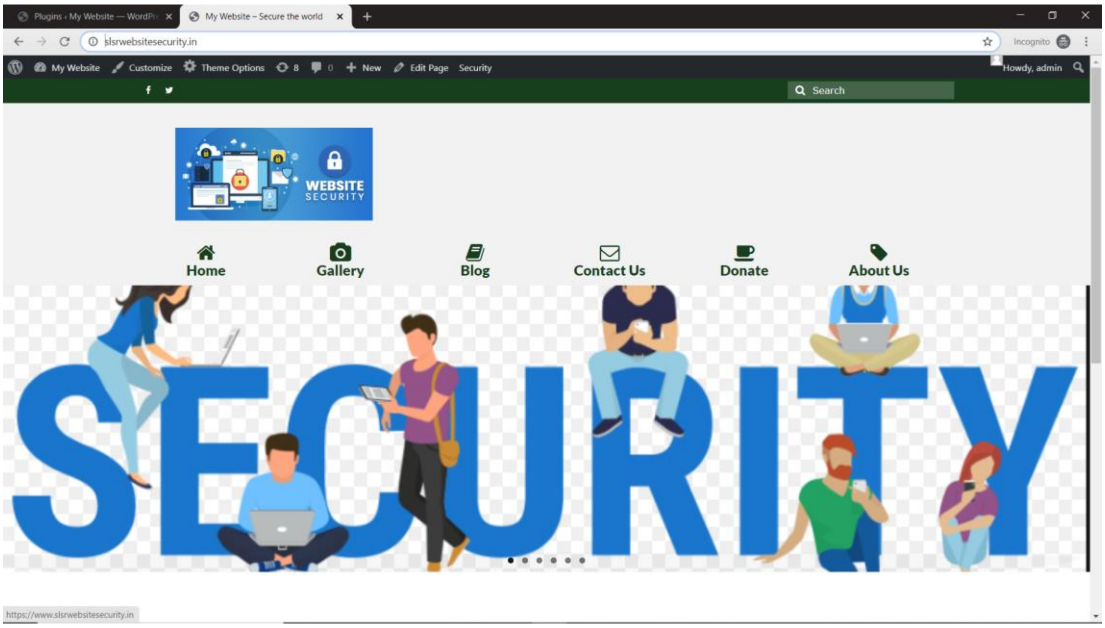


Figure 10.8 SCREENSHOT

11. USER INPUT MANUAL

1) Slsrwebitesecurity.in (user portal)
2) Slsrwebsitesecurity.in/lovely (Admin portal)
3) Provide login Details
4) Select correct security Question and Give Answer.
5) Enter OTP sent to the mail.
6) From Admin Portal look for Suspicious entries.
7) Add required Plugins.

12. ADVANTAGES

- Protects the user's computer from viruses.
- Easily navigable to which **websites** are contained with malware.
- Easy to renew after the subscription is expired.
- Real inspection of malware codes prevents worms from infecting computer.
- Can be shared through communication channels.
- Big assurance to users about their data security on the Internet.
- Big security bridge to prevent third party access.
- Influence users trust and confidence scale and turn them as potential users.
- Ensuring users safety could enhance brand or reputation of the platform as secure and safe platform on the Internet.
- Boost the return of investment without losing potential users.
- The last but not least, Staying Safe and Secure on the Internet for your valuable business and customers.

13. CONCLUSION

This report discussed website security principles and fundamental information that can help us to prevent web exploits in our system. Websites are considered the most exposed and least protected, thereafter vulnerable because the standards somehow are not focused on security but more in the serve need functionality.

Security threats are more common than before because the internet has become today's economy most valuable tool for everyone. So, there is indeed need to protect our resources, data and user privacy information. As technology move forward and brings new strategies, tools, models and methods to increase security levels, hackers will be part of this never end game.

Regarding the penetration test we can conclude that website security tools are a fundamental component in the security process but the known security vulnerabilities by their nature can be consider complex and created by real intellectual minds with the “code” word written in their forehead, this is why we need the best minds armed with great tools to eliminated these weaknesses in a cost-effective way.

The research performed to the IT business is still under a test process, but based on the actual results some conclusions can be taken into consideration. The action to test the code manually and modify the security holes has given significant results for the website integrity. Such modification has changed the condition of the after-test results and the pieces of code that needed to be modified related to the found vulnerability had accomplished to be hack resilient.

Finally, prevention is a one key component to ensure security. We can understand security as a long process that results in the assets integrity, not an accident

14. BIBILOGRAPHY

1) https://www.w3schools.com/php/

2) https://www.commonplaces.com/blog/common-website-security-vulnerabilities/

3) https://en.wikipedia.org/wiki/PHP

4) https://www.hotscripts.com/category/scripts/php/

5) https://wordpress.org/

6) https://www.slideshare.net/vikasraj225/complete-web-vulnerability-scanner-project-report/