



# Secure Programming for Web: Individual Project (**GoLoad**)

Project Report

*for*  
Irina Tal

*by*  
Rohan Bhangale (x18147119)

## [Secure Programming for Web: Individual Project \(GoLoad\)](#)

### [Executive Summary](#)

#### [Background](#)

[Aim](#)

[Technology](#)

[Hardware Architecture](#)

[Soft Architecture](#)

[PHP](#)

[MySQLi Database](#)

[Javascript](#)

[CSS](#)

#### [System Requirement](#)

[Business Requirement](#)

[Functional Requirement](#)

[Security Requirement](#)

[User Requirement](#)

#### [Architecture Design](#)

[Use Case Diagram](#)

[Abuse Diagram](#)

[Sequence Diagram](#)

[Class Diagram](#)

#### [Functional Implementation](#)

[Web Implementation](#)

[Database Implementation](#)

#### [Security Implementation](#)

[HTTPS CA Certificate:](#)

[HSTS Security](#)

[CAptcha](#)

[Blocking Remote Directory Browsing](#)

[Content Security Policy](#)

[CSRF Token](#)

[Input Validation](#)

#### [Testing & Risk Assessment](#)

[Static Code Analysis](#)

[Dynamic Code Analysis](#)

[Peer Code Review by Nathaniel \(x18159419\)](#)

#### [Conclusion](#)

#### [Bibliography](#)

# Executive Summary

*GOLOAD* is a delivery portal which relies solely on peer to peer delivery service. That means one person usually known as *PORTER* will carry the cargo from *SOURCE* to *DESTINATION* for the *CUSTOMER*.

There are 3 major roles

- Admin
- Porter
- Customer

Data being transferred and stored by these entities is secured using security implements as per OWASP standards. User-friendly GUI which allows Customers to post delivery requirements(source, destination, weight and date) while the porter has access to the list of delivery requirements posted by the user, Porter is then to pick any of the given delivery requirements, once Porter has selected one of the delivery requirement request, contact of the customer is then revealed to the porter for further dealings.

## Background

The motivation behind Goload is the luggage limitation which travellers face while using public means of transport and at the times when cargo is to be couriered. Goload allow this process of transferring cargo in flexible and smooth way. Application is implemented with Role-Based Access Control where Customer can only post delivery request while the Porter can only view and select from a given list of delivery requirement. Thus Goload a centralized peer to peer platform.

## Aim

The online portal offers a free delivery listing marketplace. Helps Customers find porters and assist porters finding delivery jobs. Portal possess the following functionality that constitutes:

- Registration (Customer;Porter)
- Login (Customer;Porter)
- Home Page (Customer;Porter)
- Post Delivery (Customer)
- Pick Delivery (Porter)

## Technology

Goload is a web application which uses Xampp Server for Apache and MySQL for back-end. HTML,CSS,PHP and JS are used for front end.[1]

## Hardware Architecture

Web Server is hosted on Windows 10 Operating System (x64) which runs i7 Processor, 8 Gig-RAM and 2Gig Graphics. Solid State Drive for faster IOPS to serve the request - response by the server.

## Soft Architecture

Software Architecture is based on the working methodology of the web server(XAMPP) used. It incorporates HyperText Markup Language [2],Cascading StyleSheet ,PHP,MySQL and JScript, which are used to perform different operations required to carry out workings for the delivery portal

### PHP

PHP is used on the server-side to handle processing such as exchange of data, interacting with forms,submitting data acquired(using GET or POST method) from forms to server[3]. While authenticating user and adding database is also done using PHP. Furthermore it is used for Input Data Validation and Sanitization[4].

### MySQLi Database

Enhanced version of MySQL. MySQL is an open source RDBMS used to store and retrieve data[5], it allows multiple users to interact with database also implementing security aspect such as RBAC and granting privileges to the users and deploys encrypted connections, thus underlying a secured connection between the webpages and backend[6]

### Javascript

Javascript is a scripting language used to perform on client side, for creating dynamic web pages and adding functionalities such as CSRF Token, Captcha. [7]

### CSS

User Interface is based on the framework known as CSS which used to style the visual representation of the web application and renders html design elements as required by the development giving the UX needed [8].

# System Requirement

## Business Requirement

Goload Portal requires Customers to post loads and Porters to pick loads in flexible fashion, while the Porter should only have access to the database with load listings and can have only the users mobile number in order to contact them for taking the job.

## Functional Requirement

Functional Requirement will depict and identify role of the web application and workings.

When the User first initiates the application, a landing page comes over the GUI with options to pursue role as a Customer or Porter further into Login and Registration respectively, thereby clicking on the Login/Sign Up button. The Credentials submitted will be cross checked with the ones on the database, if validated user access is granted.

- **Registration:** Customer/Porter can sign up with the application by submitting information such as
  - Name(First,Last)
  - Email
  - Password
  - Mobile
  - Profile Picture
- **Login:** Once the user has registered as Porter/ Customer, with the valid credentials they can sign in
- **Post Delivery:** Customer can post delivery jobs stating source, destination, weight and date for Porters
- **Pick Delivery:** Porters can pick a delivery job from a list of delivery jobs posted by the customers
- **Settings:** Customer/Porter can update profile details such as email,mobile.
- **Logout:** Terminates sessions and logs Customer/Porter out of the system.

## Security Requirement

Abiding by the main principles of security such as,

- Data Confidentiality
- Data Integrity
- Data Availability
- Encryption of sensitive data
- Maintain logs

- Authority Certificates

## User Requirement

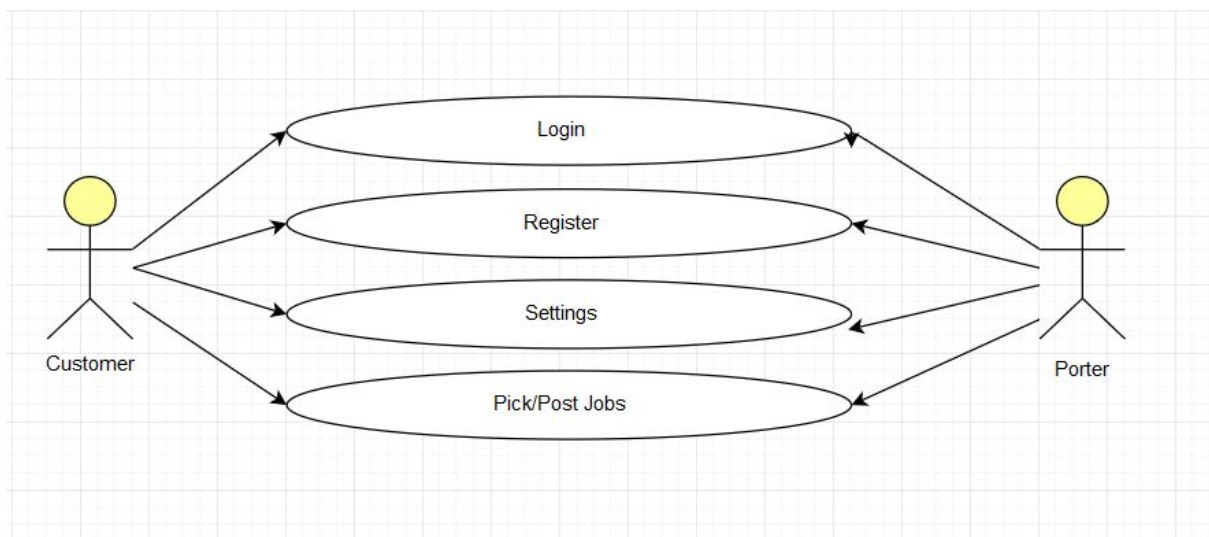
User must possess any device capable of having a browser and network connectivity

## Architecture Design

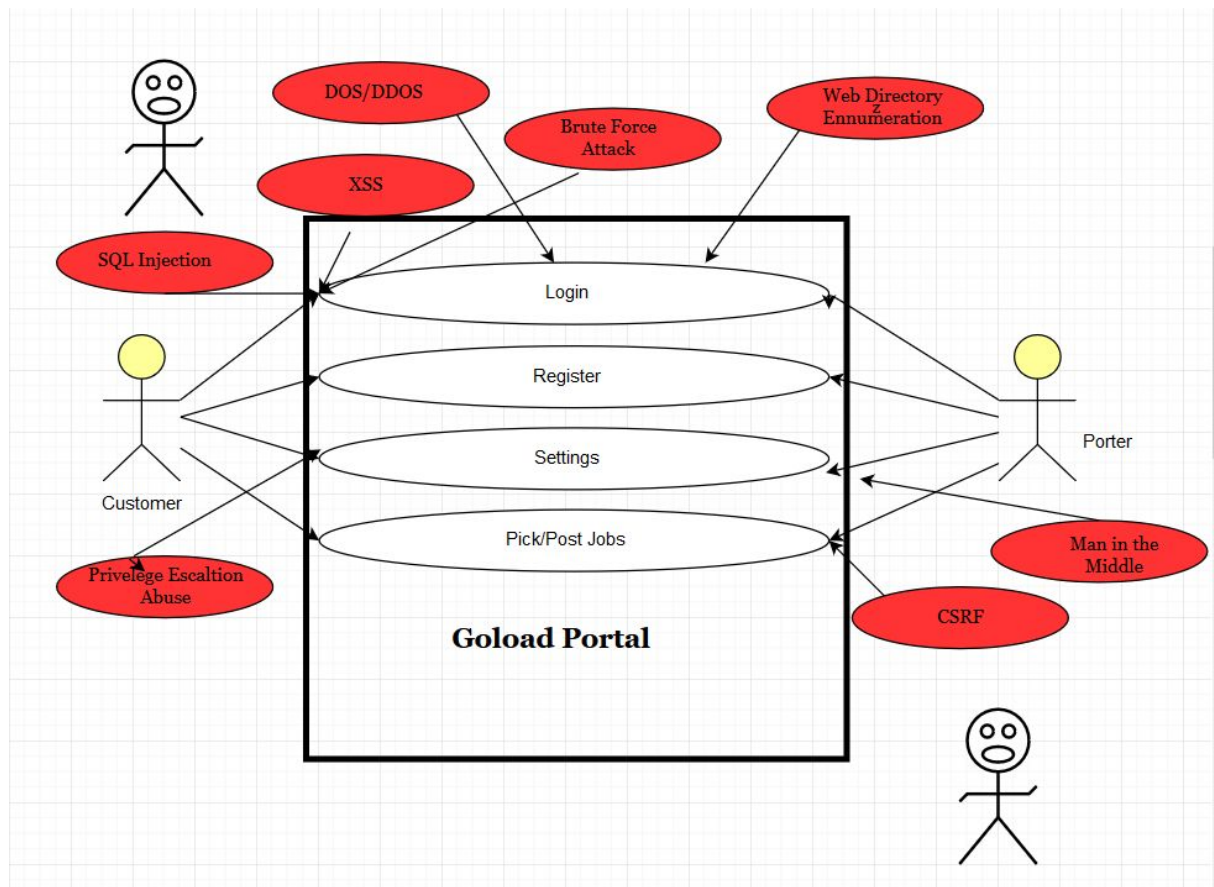
The Web Application has an Apache Web Server and MySQL Database residing on the loopback address 127.0.0.1 as the architecture with underlying Hardware.

## Use Case Diagram

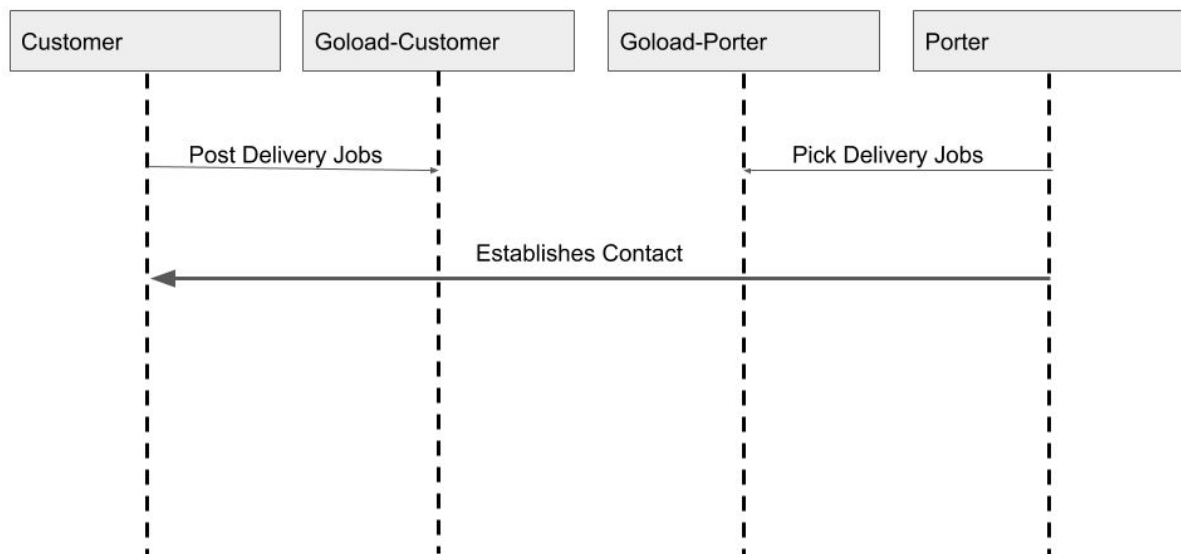
Functional Illustration of the web application



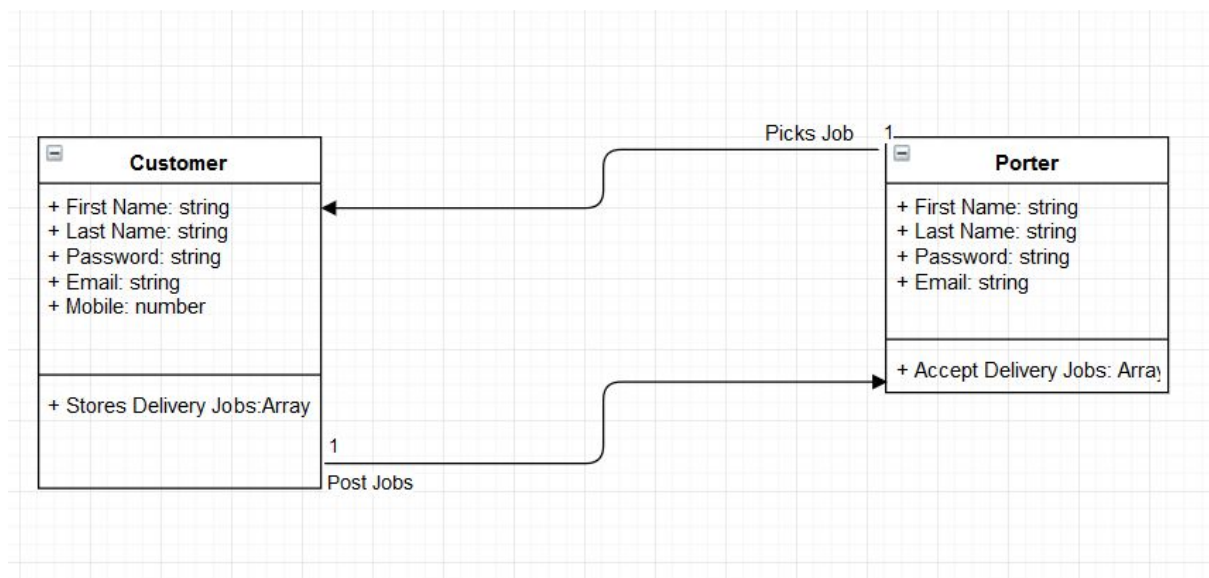
## Abuse Diagram



## Sequence Diagram



## Class Diagram





# Functional Implementation

## Web Implementation

**Index.php** Landing Page where the user is presented with option to login as customer or porter and a registration form for customer

The screenshot displays a web browser window with the URL `goload.lonehawk/ccer/index.php`. The page is titled "Goload Customer" and features a sidebar with a "Bookmarks" section containing various links like "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", "Aircrack-ng", "Kali Forums", "NetHunter", "Kali Training", "Panda", "web.whatsapp", and "Getting Started". The main content area is divided into two sections: "Login" and "Customer Registration".

**Login Section:**

- A dropdown menu labeled "Customer" is selected.
- Input fields for "Email" and "Password".
- A red "Login" button.
- A link for "Forgot Password?" in red text.

**Customer Registration Section:**

- Input fields for "First name" and "Last name".
- Input fields for "Your email id", "Your password", and "Your Mobile Number".
- A "Browse..." button and a text "No file selected.".
- A red "Sign up as Porter" link.
- A CAPTCHA image showing the number "76381" with the instruction "Type the above number:".
- A red "Sign Up" button.

The browser's address bar shows the URL `goload.lonehawk/ccer/index.php`. The Windows taskbar at the bottom indicates the system time as 23:34 on 23-04-2019.



```

12 </div>
13 </div>
14
15 <div id="login">
16 <p id="lid">Login
17 <hr size="2px" color="red" width="400px"><br><br><br><br> </p>
18 <form id="in" action="login1.php" method="post">
19 <table>
20
21 <td colspan="2">
22 <select id="dropdown" name="selected_option">
23 <option value="user">Customer</option>
24 <option value="professional">Porter</option>
25 </select>
26 </td>
27 <tr>
28 <td colspan="2"><input type="email" name="email" id="MailID" placeholder="Email ID" required="true"/></td>
29 </tr>
30 <tr>
31 <td colspan="2"><input type="password" name="password" id="pswd2" placeholder="Password" required="true"/></td>
32 </tr>
33 <tr>
34 <td><a href="" id="fp1" style="color:red">Forgot Password?</a></td>
35 </tr>
36 </table>
37 <br>
38 <!-- csrf-->
39 <input type="hidden" name="_token" class="form-control" value="{?php echo $_session['_token'];?}" />
40
41 <input type="submit" name="login" value="Log In" id="signupButton"/>
42 </form><br><br><br><br>
43 </div>
44
45 <div id="signup">
46 <p id="sid">Porter Registration
47 <hr size="2px" color="red" width="400px"> <br></p>
48
49 <form id="form2">
50 <table id="signup1">
51 <tr>
52 <td colspan="2"><input type="hidden" name="selected_option" value="professional">
53 </td>
54 <td></td>
55 <td><input type="text" name="Firstname" id="Firstname" placeholder="First Name" required="true"/></td>
56 <td><input type="text" name="Lastname" id="Lastname" placeholder="Last Name" required="true"/></td>
57 </tr>
58 <tr>
59 <td></td>
60 <td></td>
61 <td colspan="2"><input type="email" name="email" id="MailID" placeholder="Email" required="true"/></td>
62 </tr>
63 <tr>
64 <td></td>
65 <td colspan="2"><input type="password" name="password" id="pswd2" placeholder="Password" required="true"/></td>
66 </tr>
67 </table>
68 </form>
69 </div>

```


**Customerhomepage.php** here the customer is to fill in the source, destination and weight for the load to be delivered along with the date

Report for reference - rohanbi | X Reports - rohanbhangale08@ | Customer Home

goload.lonehawk/ccer/customerhomepage.php

Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Kali Training | Panda | web.whatsapp | Getting Started | NCI | VirusTotal | Google Calendar

Home | Post Delivery | Settings | Past Orders | Sign out

 Tony Thomas

Source

Destination

Weight in Kg(s)

dd / mm / yyyy

**Delivery Req >**

```

1 <html>
2 <head>
3 <title>
4 </title> Customer Home
5 </head>
6 <link rel="stylesheet" href="userhome.css.css" type="text/css">
7 </head>
8 <body>
9 <?php
10 <include 'menu.php';
11 >
12 <form id="deliveryreq" action="chomepage.php"method="post">
13 <table>
14 <tr>
15 <td colspan="2"><input type="text" name="source" id="source" class="chomepage" placeholder="Source" required="true"/>
16 </td>
17 </tr>
18 <tr>
19 <td colspan="2"><input type="text" name="destination" id="destination" class="chomepage" placeholder="Destination" required="true"/>
20 </td>
21 </tr>
22 <tr>
23 <td colspan="2"><input type="text" name="weight" id="weight" class="chomepage" placeholder="Weight In Kg(s)" required="true"/>
24 </td>
25 </tr>
26 <tr>
27 <td colspan="2"><input type="date" name="date" min="2019-04-24" max="2020-04-24" id="date" class="chomepage" placeholder="Date" required="true"/>
28 </td>
29 </tr>
30 </table>
31 <br>
32 <button type="submit" name="deliveryreq" id="chomepage" >Delivery Req</button>
33 </form>
34 </body>
35 </html>

```

**Porterhomepage.php** Here the porter is to select from the list of delivery jobs, on selecting a job, contact number of the customer will be given out for further dealings.

goload.lonehawk/ccer/porterhomepage.php

Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Panda web.whatsapp Getting Started NCI VirusTotal Google Calendar dpa

Home Pick Delivery Settings Sign out

sarell lopes

Source	Destination	Weight	Date	
0	0	40	2019-04-24	
mumba	pune	40	2019-04-24	
dubai	bangkok	20	2019-04-25	
dubai	bangkok	20	2019-04-25	
dubai	bangkok	20	2019-04-25	

Mobile: 7878787866

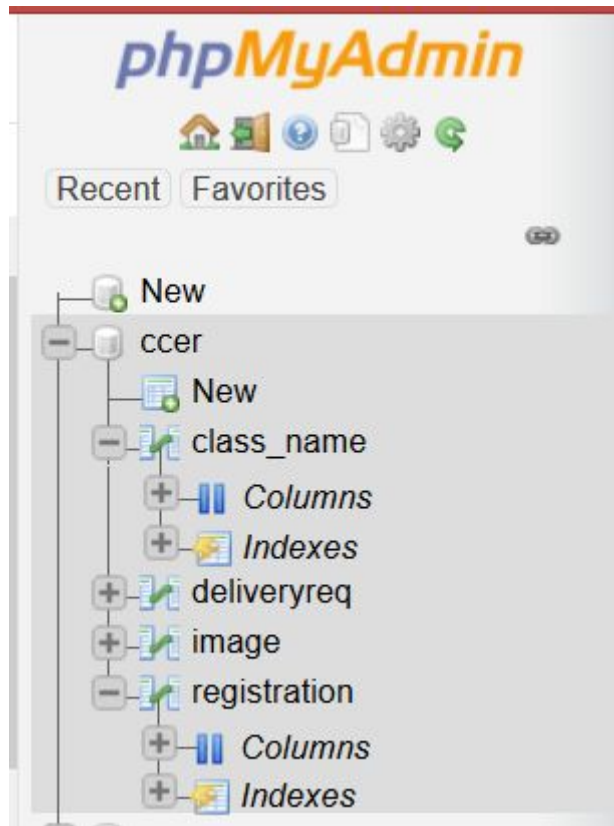
Figure 2

```

1  <?php
2  require "dbconn.php";
3  ini_set('display_errors',1);
4
5  if($_GET['id']){
6
7      $user_id = trim($_GET['id']);
8      if(is_numeric($user_id)){
9
10         $selstmt = mysqli_query($conn,"SELECT mobile from registration where id= $user_id");
11         $res = mysqli_fetch_assoc($selstmt);
12         $mobile = $res['mobile'];
13         echo json_encode(array('msg'=> 'success','mobile' => $mobile));
14
15
16
17
18
19     }else{
20         echo json_encode(array('msg' => 'failure 1'));
21     }
22
23
24 }else{
25     echo json_encode(array('msg' => 'failure 2'));
26 }
27
28 ?>

```

## Database Implementation



## Security Implementation

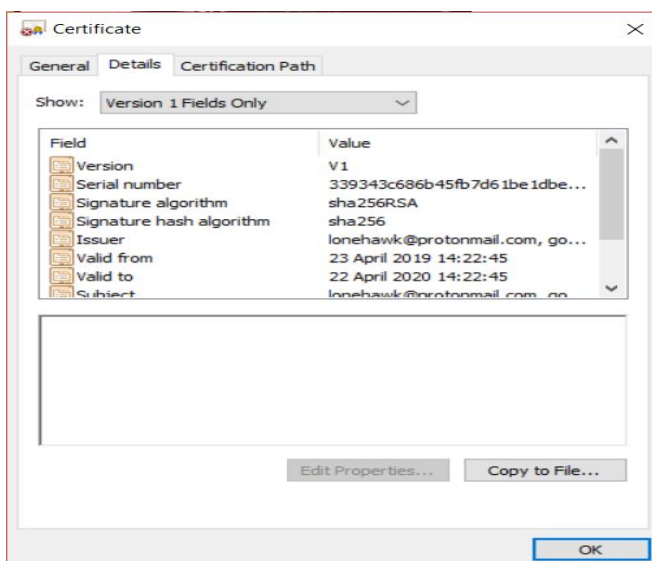
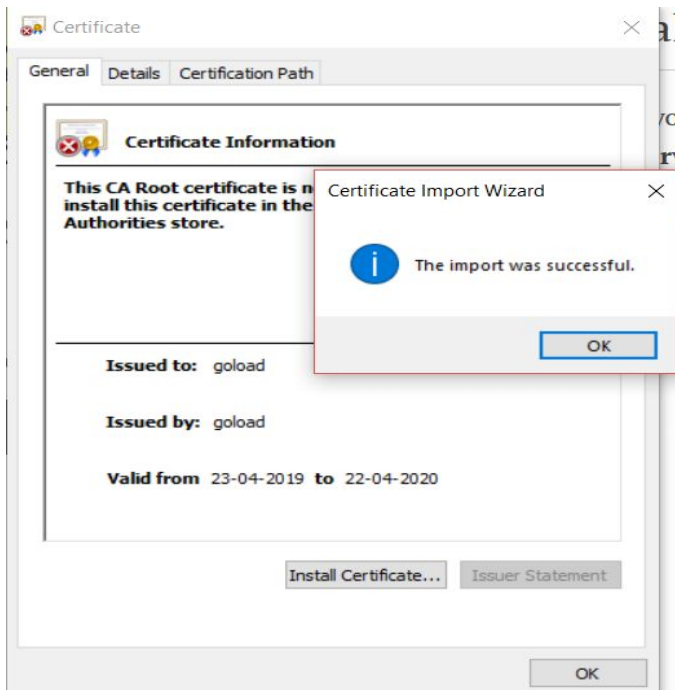
### HTTPS CA Certificate:

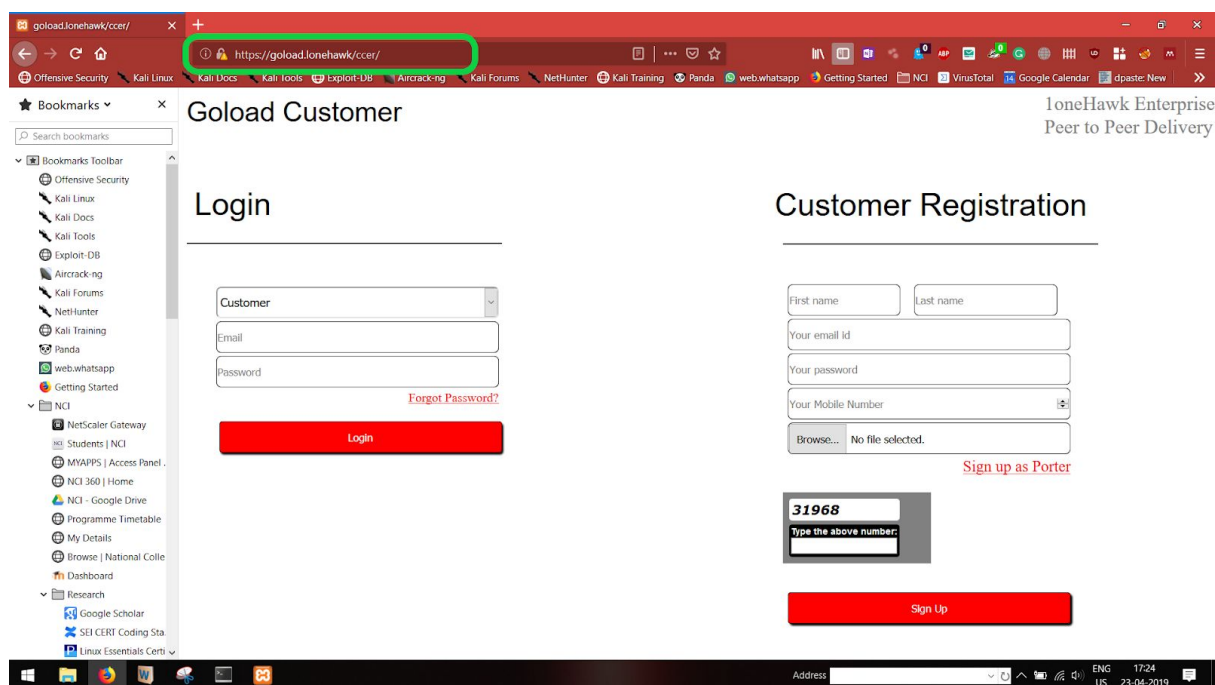
HTTPS CA certificate is a certificate issued by the Certificate Authority to help web applications operate more securely. The Certificate is a digital file that contains the ownership public key of a website. These digital certificate CAs issue millions of Digital Certificates each year, and these certificates are used to protect information, encrypt billions of transactions, and enable secure communication[11].



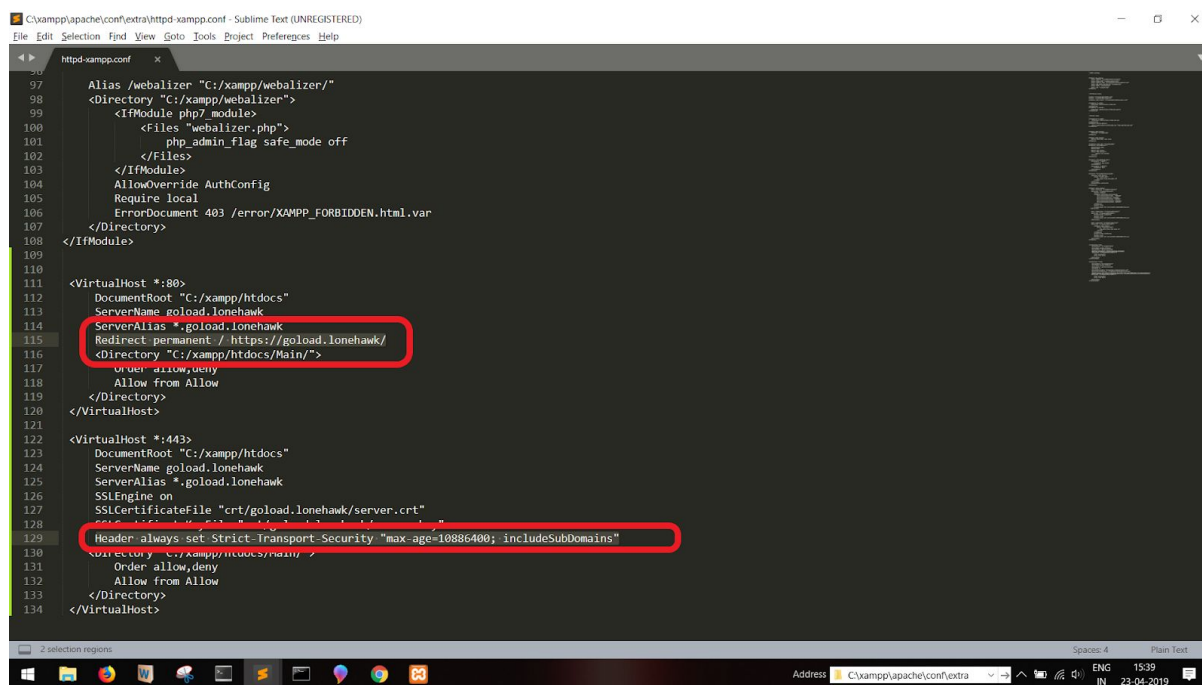
```
C:\WINDOWS\system32\cmd.exe
Generating a RSA private key
.....+++++
...+++++
Writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LoneHawk Enterprise
Organizational Unit Name (eg, section) []:Dublin Hub
Common Name (e.g. server FQDN or YOUR name) []:goload
Email Address []:lonehawk@protonmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:goload
An optional company name []:goload.lonehawk
Enter pass phrase for privkey.pem:
Writing RSA key
Signature ok
subject=O = LoneHawk Enterprise, OU = Dublin Hub, CN = goload, emailAddress = lonehawk@protonmail.com
Getting Private Key
Could not find C:\xampp\apache\.\rnd
1 file(s) moved.
1 file(s) moved.
```





## HSTS Security



HSTS: known as the Https Strict Transport Security. The HSTS requests all clients to communicate with HTTPS only and stop all communication on HTTP. Having HTTPS alone is not enough because the server might have HTTP enabled but if the client the server is communicating with is doing so in HTTP then the data being sent is still at risk. HSTS can help to mitigate attacks like SSL stripping and cookie[10].



## Captcha

Captcha determines whether an online request or submission is made by human or robot by generating a testing which only humans can pass and will be impossible for a computer program to solve - involves scrambled and istorted words or pictures, letters inside pictures.[13]

```
97 <!-- START CAPTCHA -->
98 <br>
99 <div class="capbox">
100
101 <div id="CaptchaDiv"></div>
102
103 <div class="capbox-inner">
104 Type the above number:<br>
105
106 <input type="hidden" id="txtCaptcha">
107 <input type="text" name="CaptchaInput" id="CaptchaInput" size="15"><br>
108
109 </div>
110 </div>
111 <br><br>
112 <!-- END CAPTCHA -->
113
```

C:\xampp\htdocs\ccer\index.php (ccer) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

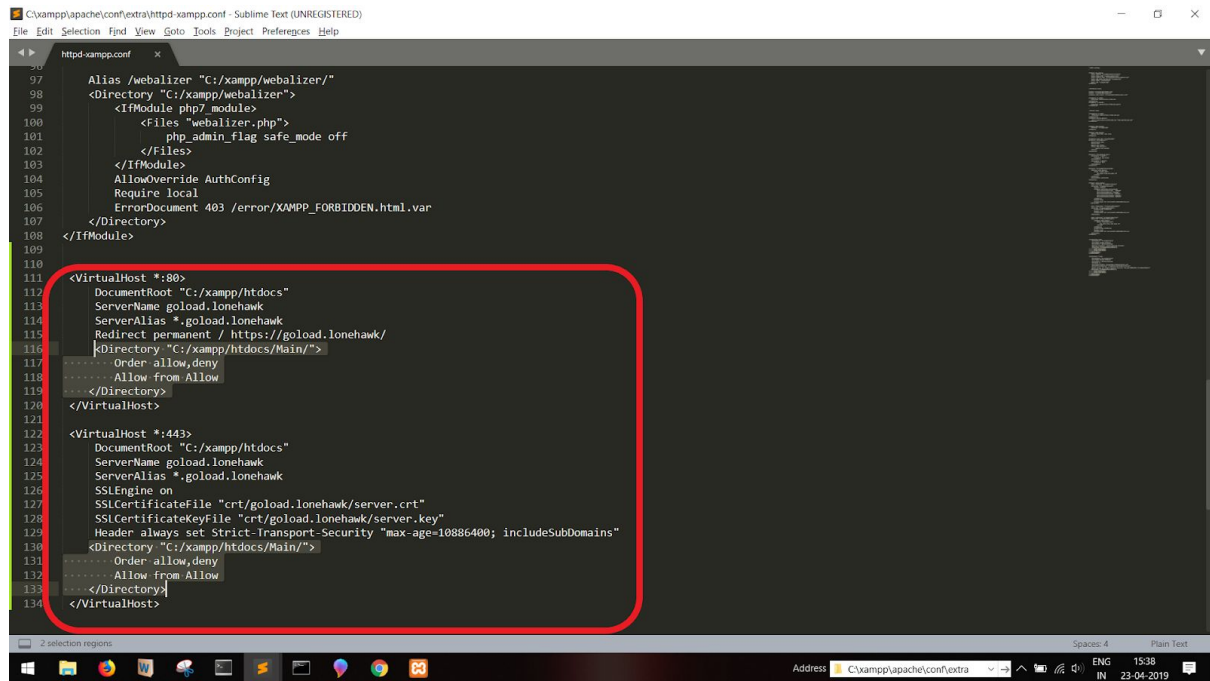
**FOLDERS**

- ccer
  - css
  - database\_file
  - images
  - profile\_picture
    - ajax-loader.gif
    - back\_icon.png
    - back\_icon1.png
  - change.php
  - chomepage.php
  - csrf.php
  - customerhomepage.php
  - dbconn.php
  - get\_userdata.php
  - index.php
  - /\* Login.css
  - <> Login.html
  - login1.php
  - logout.php
  - menu.php
  - pastorder.php
  - porterhomepage.php
  - Professional\_account.php
  - professional\_account\_register.php
  - register1.php
  - update.php
  - update1.php
  - upload\_file.php
  - /\* userhome.css.css
  - userhome.php

```
119
120 // Captcha Script
121
122 function checkform(theform){
123     var why = "";
124
125     if(theform.CaptchaInput.value == ""){
126         why += "- Please Enter CAPTCHA Code.\n";
127     }
128     if(theform.CaptchaInput.value != ""){
129         if(ValidCaptcha(theform.CaptchaInput.value) == false){
130             why += "- The CAPTCHA Code Does Not Match.\n";
131         }
132     }
133     if(why != ""){
134         alert(why);
135         return false;
136     }
137 }
138
139 var a = Math.ceil(Math.random() * 9)+ '';
140 var b = Math.ceil(Math.random() * 9)+ '';
141 var c = Math.ceil(Math.random() * 9)+ '';
142 var d = Math.ceil(Math.random() * 9)+ '';
143 var e = Math.ceil(Math.random() * 9)+ '';
144
145 var code = a + b + c + d + e;
146 document.getElementById("txtCaptcha").value = code;
147 document.getElementById("CaptchaDiv").innerHTML = code;
148
149 // Validate input against the generated number
150 function ValidCaptcha(){
151     var str1 = removeSpaces(document.getElementById('txtCaptcha').value);
152     var str2 = removeSpaces(document.getElementById('CaptchaInput').value);
153     if (str1 == str2){
154         return true;
155     }else{
156         return false;
157     }
158 }
159
160 // Remove the spaces from the entered and generated code
161 function removeSpaces(string){
162     return string.split(' ').join('');
163 }
164 </script>
165
166 </div>
167
168
169 </body>
170 </html>
```

## Blocking Remote Directory Browsing

Attacker is able to find secret directories by crawling and brute-forcing possible directory names and try to gain access to them[9].



```
107 </Directory>
108 </IfModule>
109
110 <VirtualHost *:80>
111     DocumentRoot "C:/xampp/htdocs"
112     ServerName goload.lonehawk
113     ServerAlias *.goload.lonehawk
114     Redirect permanent / https://goload.lonehawk/
115     <Directory "C:/xampp/htdocs/Main/">
116         Order allow,deny
117         Allow from All
118     </Directory>
119 </VirtualHost>
120
121
122 <VirtualHost *:443>
123     DocumentRoot "C:/xampp/htdocs"
124     ServerName goload.lonehawk
125     ServerAlias *.goload.lonehawk
126     SSLEngine on
127     SSLCertificateFile "crt/goload.lonehawk/server.crt"
128     SSLCertificateKeyFile "crt/goload.lonehawk/server.key"
129     Header always set Strict-Transport-Security "max-age=1886400; includeSubDomains"
130     <Directory "C:/xampp/htdocs/Main/">
131         Order allow,deny
132         Allow from All
133     </Directory>
134 </VirtualHost>
```

## Content Security Policy

CSP is an extra layer of security which detects various types of attacks which includes XSS and sql injection attacks and provides defence to these attacks protecting from data theft. It is completely backward compatible[12].



```
1 <?php
2 header("Content-Security-Policy-Report-Only: policy : default-src 'self'");
3 header('X-FRAME-OPTIONS: SAMEORIGIN');
4
5 include "csrf.php"; ?>
6
7
8 <html>
9 <head>
10
11
12 <link rel="stylesheet" href="Login.css" type="text/css">
13 </head>
14 <body><p id="title"><span style="font-family:">GoLoad Customer</span></p>
```

```
169 LoadModule setenvif_module modules/mod_setenvif.so
170 #LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
171 #LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
172 #LoadModule socache_dbm_module modules/mod_socache_dbm.so
173 #LoadModule socache_memcache_module modules/mod_socache_memcache.so
174 #LoadModule socache_redis_module modules/mod_socache_redis.so
175 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
176 #LoadModule spelling_module modules/mod_spelling.so
177 LoadModule ssl_module modules/mod_ssl.so
178 LoadModule status_module modules/mod_status.so
179 #LoadModule substitute_module modules/mod_substitute.so
180 #LoadModule unique_id_module modules/mod_unique_id.so
181 #LoadModule userdir_module modules/mod_userdir.so
182 #LoadModule usertrack_module modules/mod_usertrack.so
183 LoadModule version_module modules/mod_version.so
184 #LoadModule vhost_alias_module modules/mod_vhost_alias.so
185 #LoadModule watchdog_module modules/mod_watchdog.so
186 #LoadModule xml2enc_module modules/mod_xml2enc.so
187
188 Header set X-Content-Type-Options "nosniff"
189 Header set X-XSS-Protection "1; mode=block"
190 Header set X-Frame-Options "DENY"
191
```

# Goload Customer

## Login

Customer

Email

Password

Forgot Password?

Login

## Customer Registration

First name

Last name

Your email id

Your password

Your Mobile Number

Register

Status	Method	Domain	File	Cause	Type	Transferred	Size	Time
200	GET	localhost	/cc...	document	html	4.70 KB	4.30 KB	11 ms
304	GET	localhost	Lo...	stylesheet	css	cached	3.11 KB	
200	GET	localhost	favi...	img	x-icon	cached	197.83 KB	

Headers

Content-Security-Policy-Report-Only: policy: default-src 'self'

Content-Type: text/html; charset=UTF-8

Date: Tue, 23 Apr 2019 04:11:57 GMT

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4

X-Content-Type-Options: nosniff

X-FRAME-OPTIONS: DENY

X-Powered-By: PHP/7.3.4

X-XSS-Protection: 1; mode=block

```

C:\Users\lonehawk\Downloads\Compressed\nikto-2.1.5>nikto.bat -h http://localhost/ccer/ -p 443
- Nikto v2.1.5


-----
+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:    2019-04-23 04:47:28 (GMT1)
-----

+ Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4
+ Retrieved x-powered-by header: PHP/7.3.4
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ No CGI Directories found (use '-C all' to force check all possible dirs)

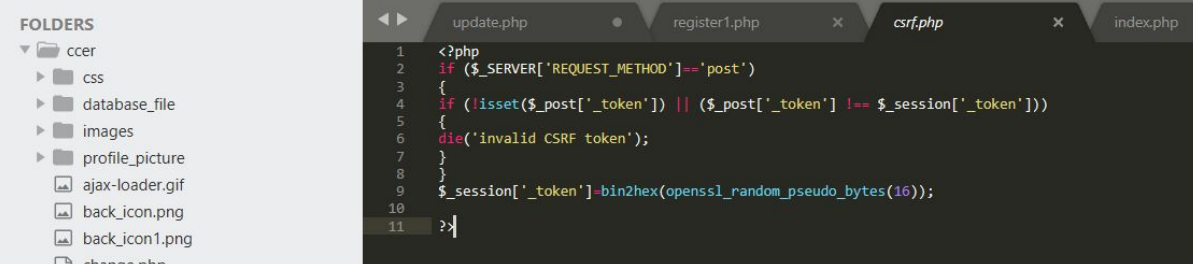
```

## CSRF Token

CSRF also known as XSRF, is a type of vulnerability in Web Applications, in which User is forced by the attacker to issue request using browser in which the user is logged in currently.

 C:\xampp\htdocs\ccer\csrf.php (ccer) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help



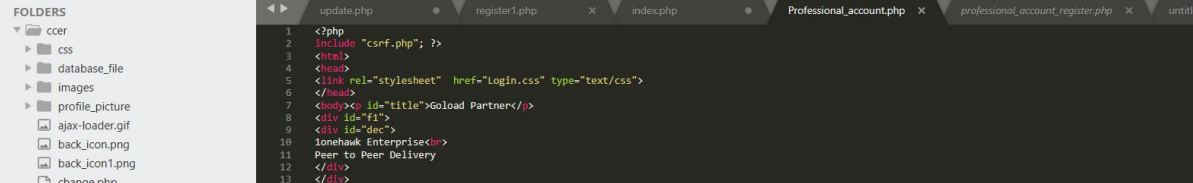
```

1 <?php
2 if ($_SERVER['REQUEST_METHOD']=='post')
3 {
4     if (!isset($_post['_token']) || ($_post['_token'] != $_session['_token']))
5     {
6         die('invalid CSRF token');
7     }
8 }
9 $_session['_token'] = bin2hex(openssl_random_pseudo_bytes(16));
10
11 >|

```

 C:\xampp\htdocs\ccer\Professional\_account.php (ccer) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help



```

1 <?php
2 include "csrf.php"; ?>
3 <html>
4 <head>
5 <link rel="stylesheet" href="Login.css" type="text/css">
6 </head>
7 <body><div id="title">GoLoad Partner</div>
8 <div id="fl">
9 <div id="dec">
10 lonehawk Enterprise<br>
11 Peer to Peer Delivery
12 </div>
13 </div>
14

```

## Input Validation

Input Validation is done to ensure that any malicious script isn't passed in through the data fields.

```

156 <script>
157
158 $('#username').keypress(function (e) {
159     var regex = new RegExp("[a-zA-Z0-9]+$");
160     var str = String.fromCharCode(e.charCode ? e.which : e.charCode);
161     if (regex.test(str)) {
162         $('#msg').html("");
163         $('#submit').prop("disabled", false);
164         return true;
165     }
166     else
167     {
168         e.preventDefault();
169         $('#submit').prop("disabled", true);
170         $('#msg').html("");
171         $('#msg').html("<center>Use alphabets & numbers only!</center>");
172         return false;
173     }
174 });
175
176 $('#password').keyup(function (e) {
177     var regex = new RegExp("(?=[a-z])(?=[A-Z])(?=[0-9])(?=[!@#$%^&*])(?=.{10,})");
178     //var str = String.fromCharCode(e.charCode ? e.which : e.charCode);
179     var str = this.value;
180     //console.log(regex.test(str));
181     if (regex.test(str)) {
182         $('#msg').html("");
183         $('#submit').prop("disabled", false);
184         return true;
185     }
186     else
187     {
188         //e.preventDefault();
189         $('#submit').prop("disabled", true);
190         $('#msg').html("");
191         $('#msg').html("<center>Use atleast 10 characters,<br>1 lowercase | 1 uppercase | 1 special | 1 numeric</center>");
192         //return false;
193     }
194 });
195
196
197 $('#email').keypress(function (e) {
198     var regex = new RegExp("[a-zA-Z0-9.!#$%&'*/-?^_`{|}~]+@[a-zA-Z0-9](?:[a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?(?:\.[a-zA-Z0-9](?:[a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?)*$");
199     //var str = String.fromCharCode(e.charCode ? e.which : e.charCode);
200     var str = this.value;
201     //console.log(str);
202     //console.log(regex.test(str));
203     if (regex.test(str)) {
204         $('#submit').prop("disabled", false);
205         $('#msg').html("");
206         return true;
207     }
208     else
209     {
210         //e.preventDefault();
211         $('#submit').prop("disabled", true);

```

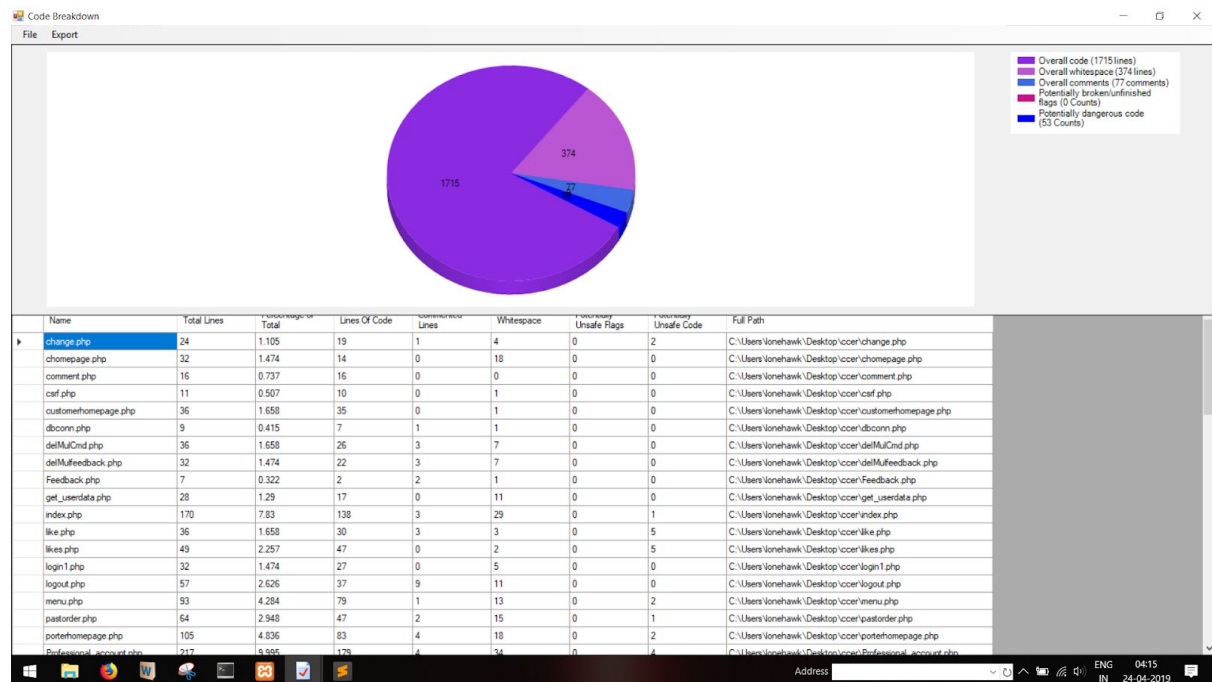
# Testing & Risk Assessment

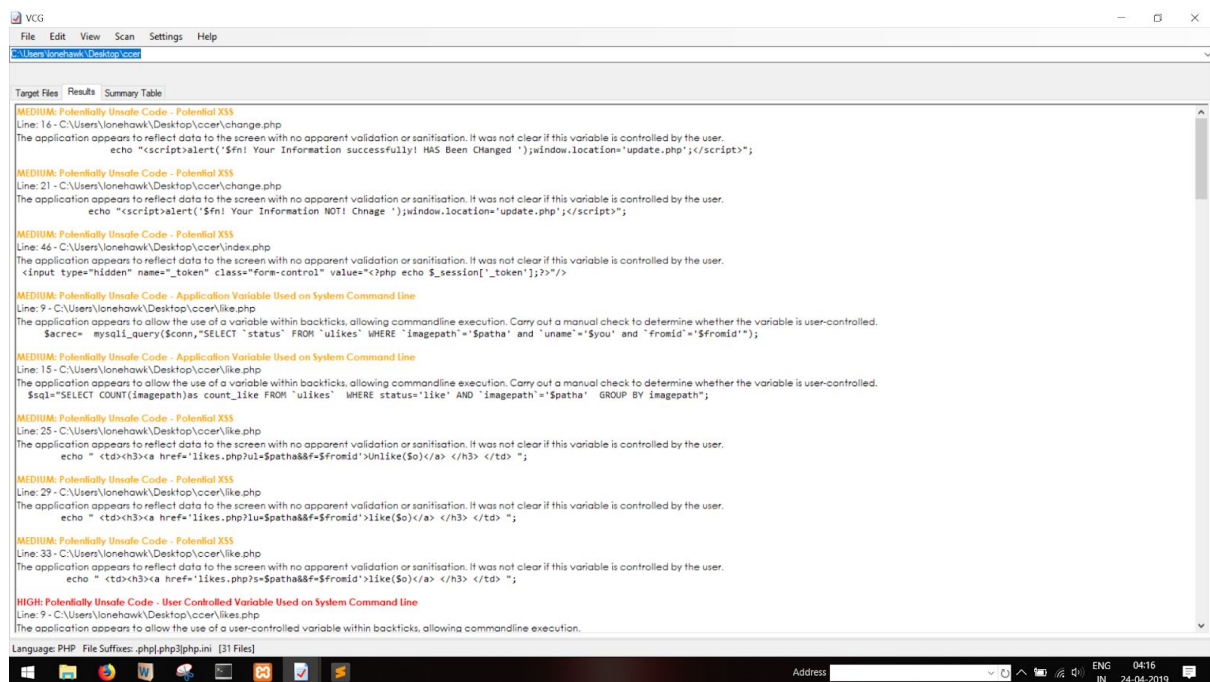
Parameter	Risk Rating	Vulnerability Description
Blind SQL Injection	High	Injection which asks database boolean questions and determines the answer
Apache server-info enabled	Medium	Displays information about Apache Configuration
Apache server-status enabled	Medium	Allows to identify server running condition
Development configuration file	Medium	Exposes sensitive information
Directory listing	Medium	Possibility of browsing directory without Authentication and



		Authorization
Error message on page	Medium	Exposes sensitive information of the inner system

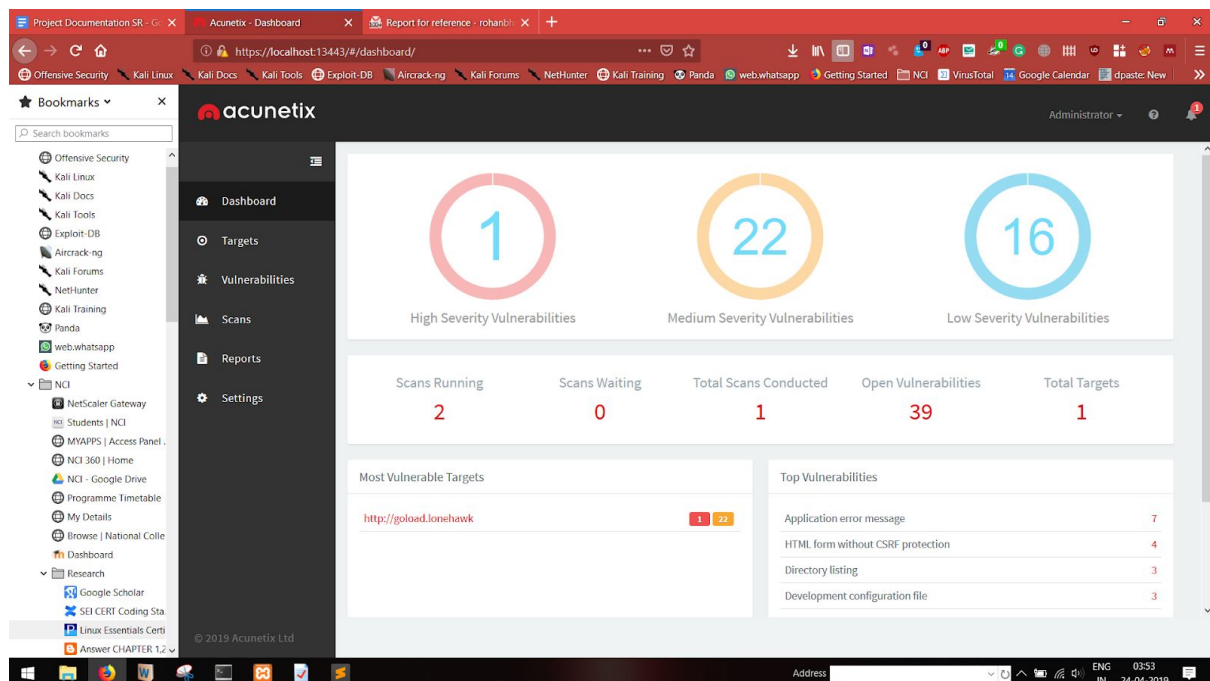
## Static Code Analysis





Here, it shows that the Application is vulnerable to XSS but it can be a false-positive as the code has implemented Data Input Validation and Sanitization

## Dynamic Code Analysis



Vulnerability scan test was conducted to detect security flaws and loopholes, it was found that input data from forms were directly passed on to PHP execution without Input Data Validation and Sanitization, as the web application is vulnerable to Blind SQL and XSS from Acunetix Scan.



## Peer Code Review by *Nathaniel* (x18159419)

File	Issue Description	Remediation Measure	Current Status
Index.php	Missing Validation	Input Data Validation	Fixed
dbconn.php	connection credentials are present in code	Storing in Configuration file stored separately	Not Fixed
professional_account_register.php	XSS	Sanitizing	Fixed

## Conclusion

Goload is a simple web application with security implementation such as XSS,CSRF and implements HSTS. Further development can be made by implementing the project on cloud for easy access and mobility.

## Bibliography

1. XAMPP Installers and Downloads for Apache Friends. 2019. XAMPP Installers and Downloads for Apache Friends. [ONLINE] Available at: <https://www.apachefriends.org/index.html>. [Accessed 23 April 2019].
2. HTML Tutorial. 2019. HTML Tutorial. [ONLINE] Available at: <https://www.w3schools.com/html/>. [Accessed 23 April 2019].
3. www.guru99.com. 2019. No page title. [ONLINE] Available at: <https://www.guru99.com/php-regular-expressions.html>. [Accessed 23 April 2019].
4. Input Validation and Data Sanitization - SEI CERT Oracle Coding Standard for Java - Confluence. 2019. Input Validation and Data Sanitization - SEI CERT Oracle Coding Standard for Java - Confluence. [ONLINE] Available at: <https://wiki.sei.cmu.edu/confluence/display/java/Input+Validation+and+Data+Sanitization>. [Accessed 23 April 2019].
5. Website Tutorials - Find Out How to Use the Most Popular Web Apps. 2019. What is MySQL Tutorial. [ONLINE] Available at: <https://www.siteground.com/tutorials/php-mysql/mysql/>. [Accessed 23 April 2019].
6. MySQL :: Security in MySQL :: 6 Security Plugins. 2019. MySQL :: Security in MySQL :: 6 Security Plugins. [ONLINE] Available at:

<https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/security-plugins.html>.

[Accessed 23 April 2019].

7. MDN Web Docs. 2019. JavaScript | MDN. [ONLINE] Available at: <https://developer.mozilla.org/en-US/docs/Web/JavaScript>. [Accessed 23 April 2019].
8. 2019. Learn CSS Today The Easy Way ». [ONLINE] Available at: <https://html.com/css/>. [Accessed 23 April 2019].
9. How to Disable Directory Listing on Your Web Server | Netsparker. 2019. How to Disable Directory Listing on Your Web Server | Netsparker. [ONLINE] Available at: <https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/>. [Accessed 24 April 2019].
10. How to Disable Directory Listing on Your Web Server | Netsparker. 2019. How to Disable Directory Listing on Your Web Server | Netsparker. [ONLINE] Available at: <https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/>. [Accessed 24 April 2019].
11. What is a Certificate Authority?. 2019. What is a Certificate Authority?. [ONLINE] Available at: <https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/>. [Accessed 24 April 2019].
12. MDN Web Docs. 2019. Content Security Policy (CSP) - HTTP | MDN. [ONLINE] Available at: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>. [Accessed 24 April 2019].
13. whatismyipaddress.com. 2019. No page title. [ONLINE] Available at: <https://whatismyipaddress.com/captcha>. [Accessed 24 April 2019].