Assignment 2

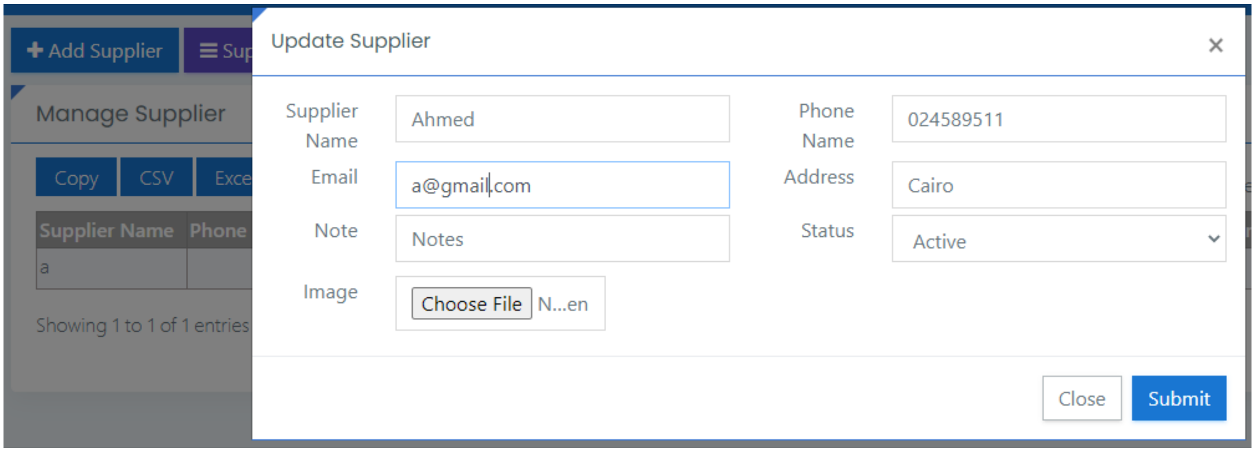
Ahmed Khaled Saad Ali Mekheimer

ID: 1809799

We will discuss possible fields that could be vulnerable to SQL Injection.

1. Adding a Supplier (email & Phone No. fields)

First we need to have a Supplier info like the one below from “Manage Supplier” page.



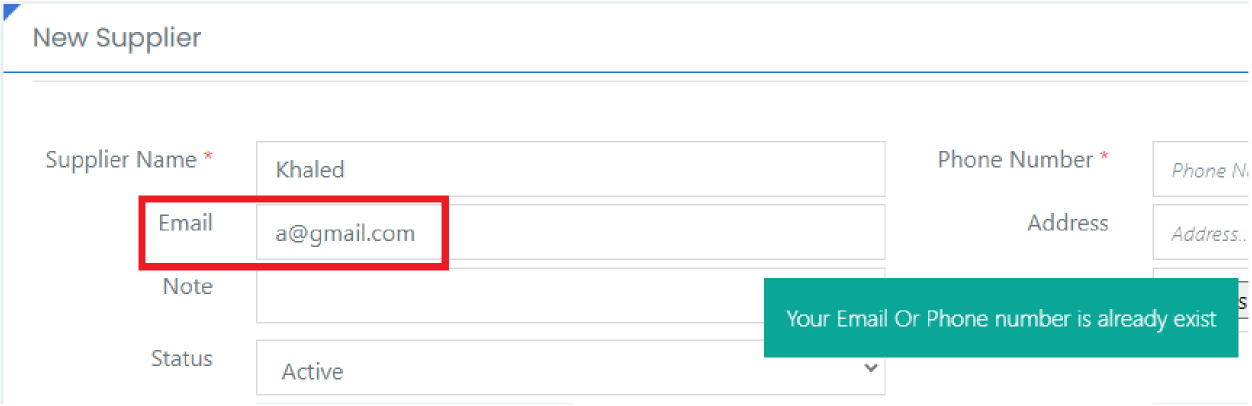
Supplier Name | Phone
a

Showing 1 to 1 of 1 entries

Update Supplier

Supplier Name: Ahmed
Phone Name: 024589511
Email: a@gmail.com
Address: Cairo
Note: Notes
Status: Active
Image: N...en

Then we will go “Add a Supplier” if we put an already existed email or Phone No. we will get the below warning.

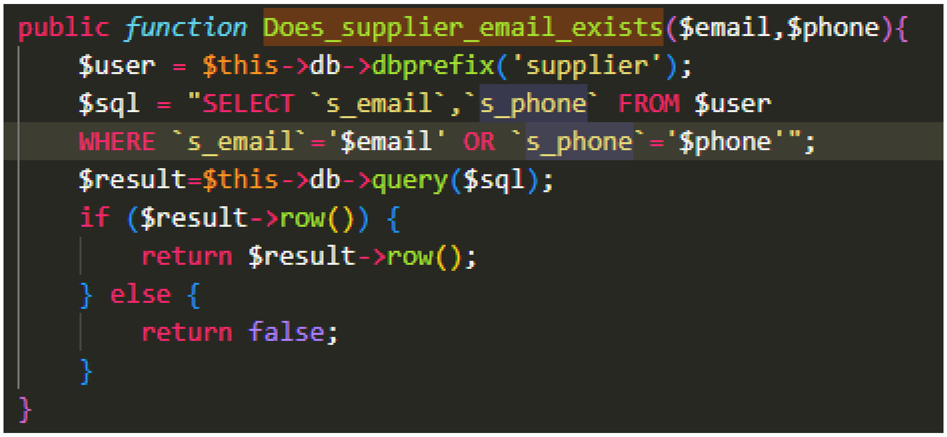


New Supplier

Supplier Name *: Khaled
Phone Number *: Phone N
Email: a@gmail.com
Address: Address..
Note:
Status: Active

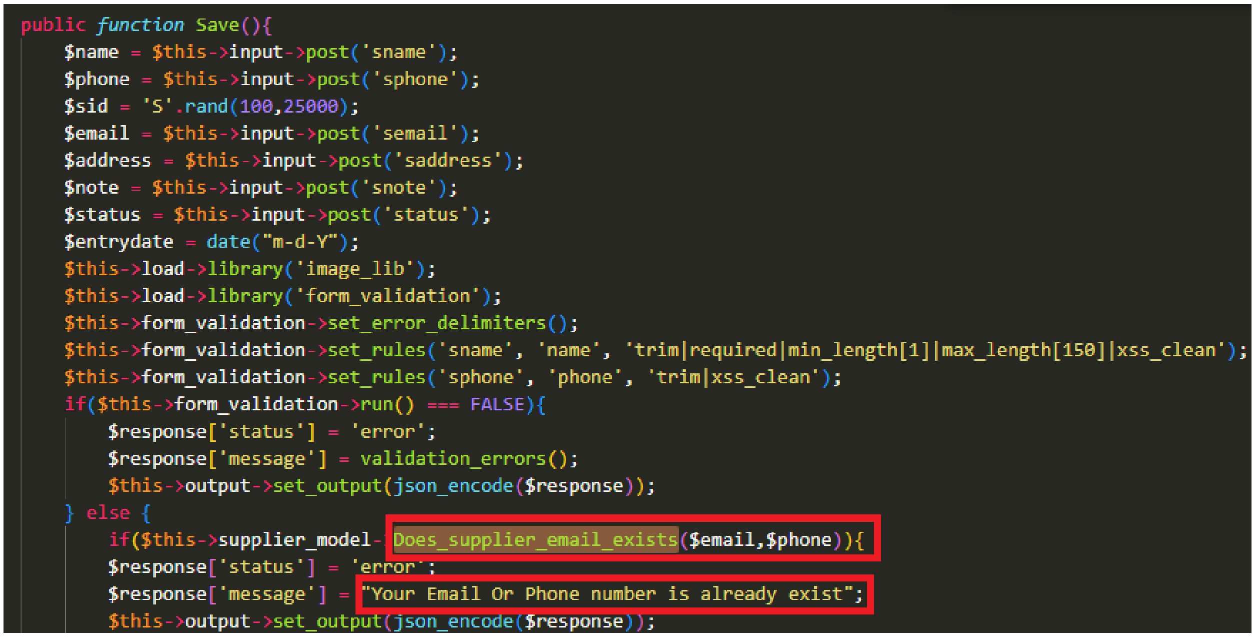
Your Email Or Phone number is already exist

This warning is due to this function in Supplier_model.php that checks if supplier email exists.



```
public function Does_supplier_email_exists($email,$phone){
    $user = $this->db->dbprefix('supplier');
    $sql = "SELECT `s_email`,`s_phone` FROM $user
    WHERE `s_email`='$email' OR `s_phone`='$phone'";
    $result=$this->db->query($sql);
    if ($result->row()) {
        return $result->row();
    } else {
        return false;
    }
}
```

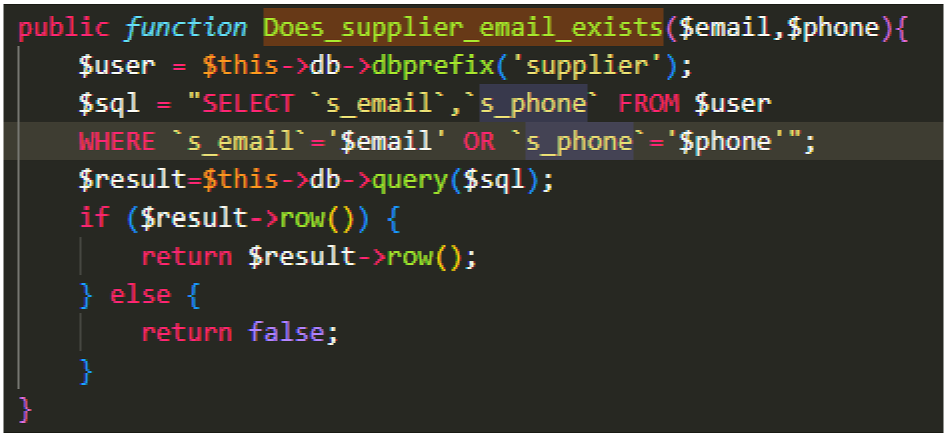
Then in Supplier.php the below function: Save( ) , calls “Does_supplier_email_exists” function, if true (yes email already exists) then the message “Your Email Or Phone number is already exist” is displayed.



```
public function Save(){
    $name = $this->input->post('sname');
    $phone = $this->input->post('sphone');
    $sid = 'S'.rand(100,25000);
    $email = $this->input->post('semail');
    $address = $this->input->post('saddress');
    $note = $this->input->post('snote');
    $status = $this->input->post('status');
    $entrydate = date("m-d-Y");
    $this->load->library('image_lib');
    $this->load->library('form_validation');
    $this->form_validation->set_error_delimiters();
    $this->form_validation->set_rules('sname', 'name', 'trim|required|min_length[1]|max_length[150]|xss_clean');
    $this->form_validation->set_rules('sphone', 'phone', 'trim|xss_clean');
    if($this->form_validation->run() === FALSE){
        $response['status'] = 'error';
        $response['message'] = validation_errors();
        $this->output->set_output(json_encode($response));
    } else {
        if($this->supplier_model-Does_supplier_email_exists($email,$phone)){
        $response['status'] = 'error';
        $response['message'] = "Your Email Or Phone number is already exist";
        $this->output->set_output(json_encode($response));
```

In conclusion, to SQL Inject the below code, we can put in email field:

1’ OR 1=1 --



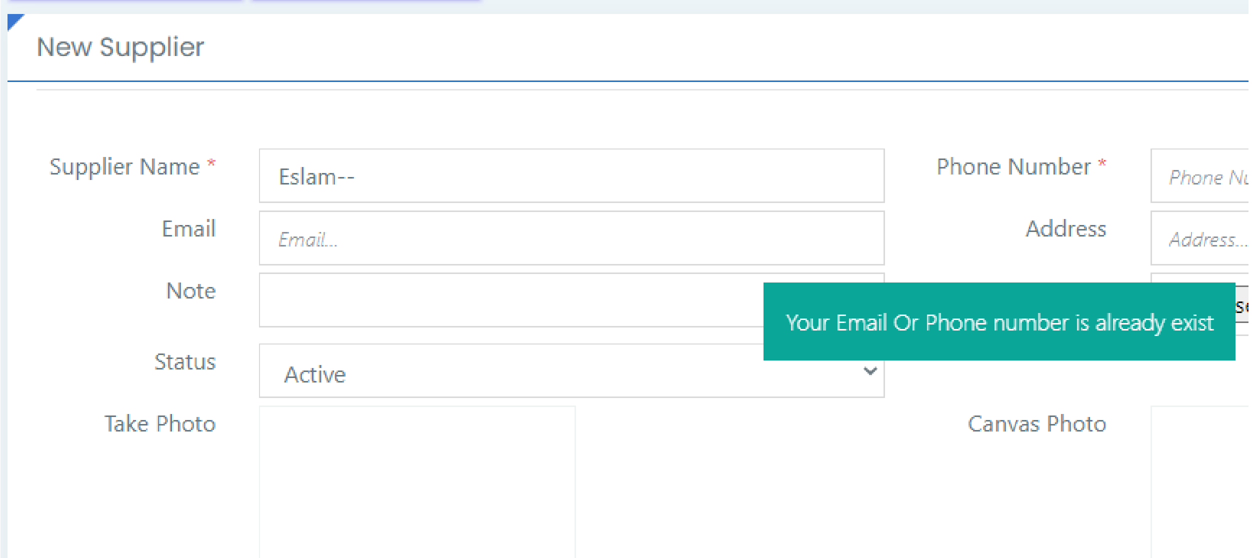
```
public function Does_supplier_email_exists($email,$phone){
    $user = $this->db->dbprefix('supplier');
    $sql = "SELECT `s_email`,`s_phone` FROM $user
    WHERE `s_email`='$email' OR `s_phone`='$phone'";
    $result=$this->db->query($sql);
    if ($result->row()) {
        return $result->row();
    } else {
        return false;
    }
}
```

So, it should evaluate to TRUE and message “Your Email Or Phone number is already exist” pops up.

But unfortunately, we can’t SQL Inject neither email field nor Phone No. field because there are constaraints on inputs of such fields.

Email field will only accept an email format and Phone No. field will accept only numbers.

However, I have noticed in “Add Supplier” page that when inserting in “Name” field an alphabetic character then-- (SQL’s comment) as typed below:



New Supplier

Supplier Name * Eslam--

Email Email...

Note

Status Active

Take Photo

Phone Number * Phone Nu

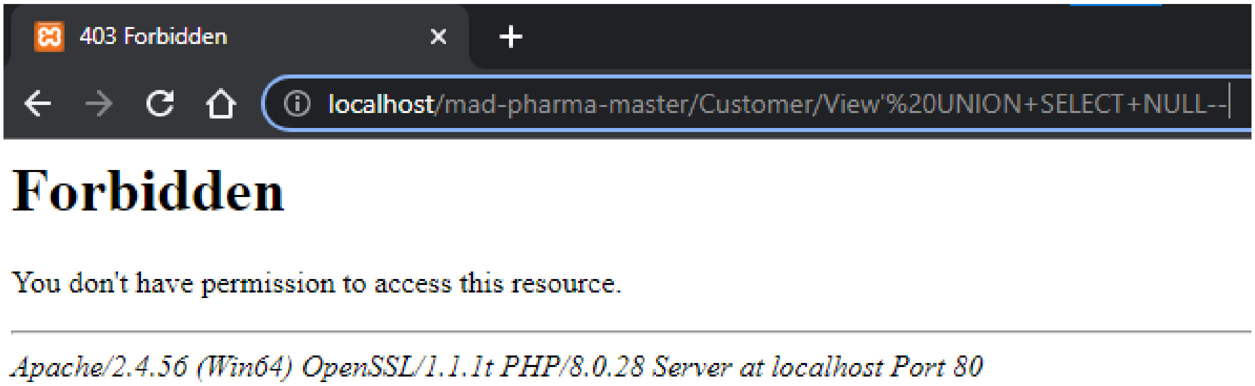
Address Address...

Canvas Photo

Your Email Or Phone number is already exist

It gives message “Your Email Or Phone number is already exist” although I have no Emails with named “Eslam”, which means by just putting -- after some characters, somehow commenting the rest of the query evaluates “Does_supplier_email_exists” function to TRUE causing the message to pop up.

2. At any page we can’t SQL Inject URL as it gives the below error.



localhost/mad-pharma-master/Customer/View'%20UNION+SELECT+NULL--

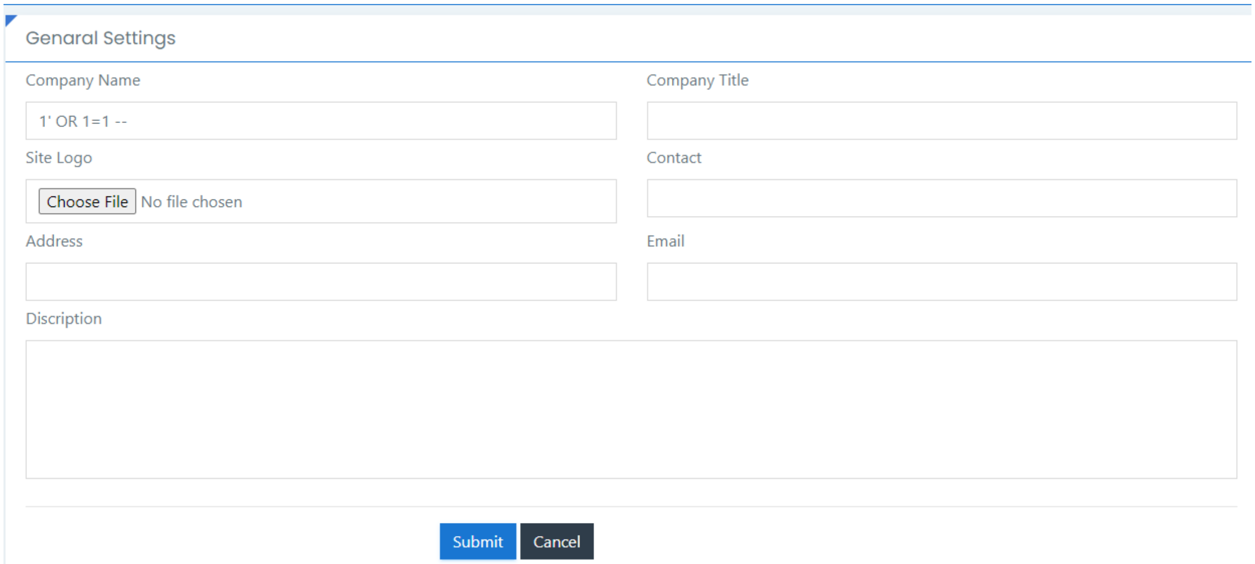
Forbidden

You don't have permission to access this resource.

Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28 Server at localhost Port 80

3. In Settings page, multiple fields could be vulnerable to SQL Injection but they aren’t affected neither by Simple SQL Injection nor Time Delay nor Blind SQL injection as shown below, what happens instead is the text itself gets typed in the database table.

Simple SQL injection



Genaral Settings

Company Name: 1' OR 1=1 --

Company Title:

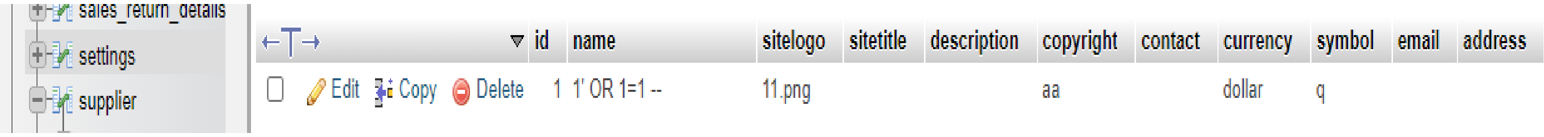
Site Logo: Choose File No file chosen

Contact:

Address:

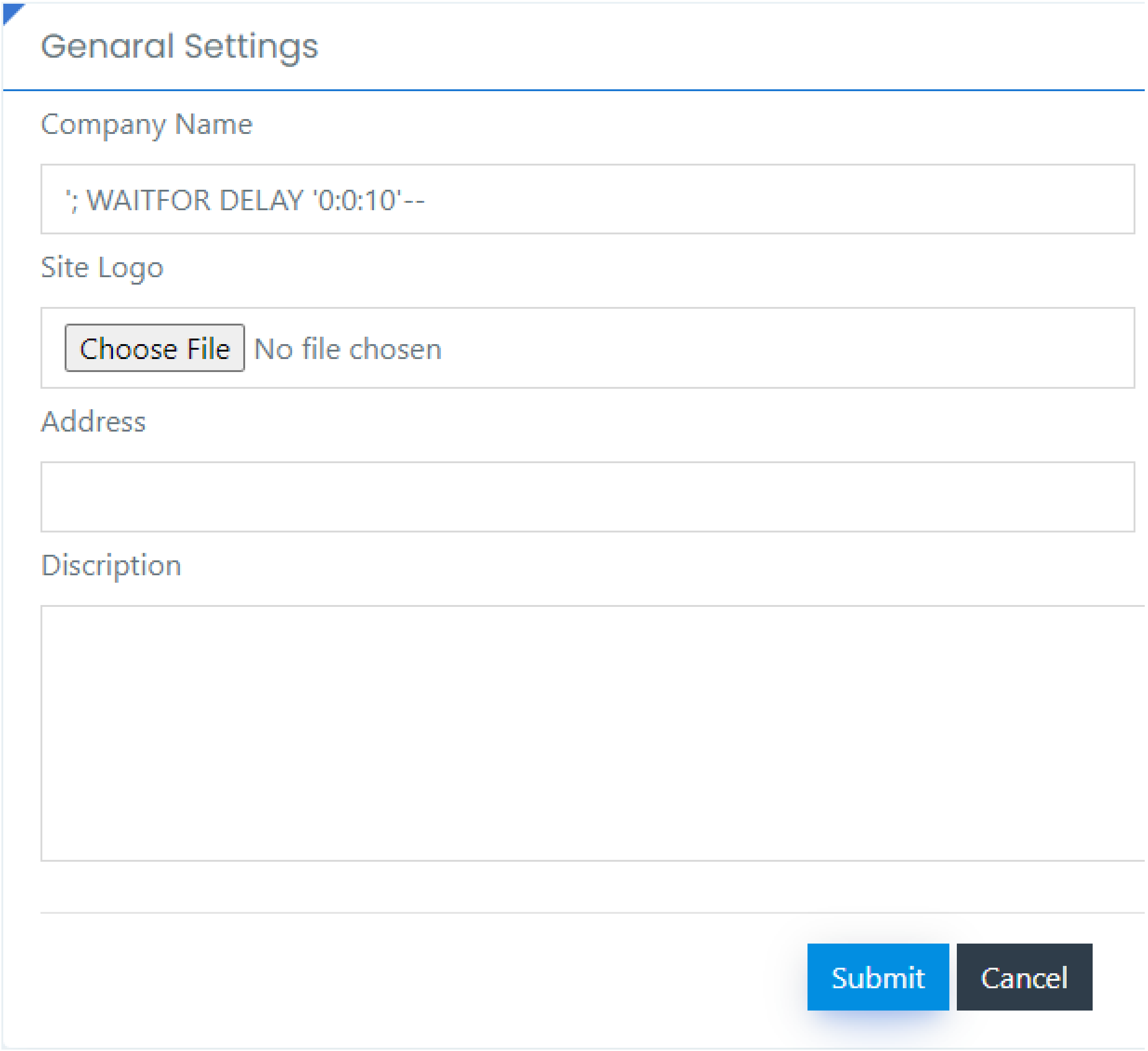
Email:

Discription:



id	name	sitelogo	sitetitle	description	copyright	contact	currency	symbol	email	address
1	1' OR 1=1 --	11.png			aa		dollar	q		

Time Delay SQL injection



Genaral Settings

Company Name

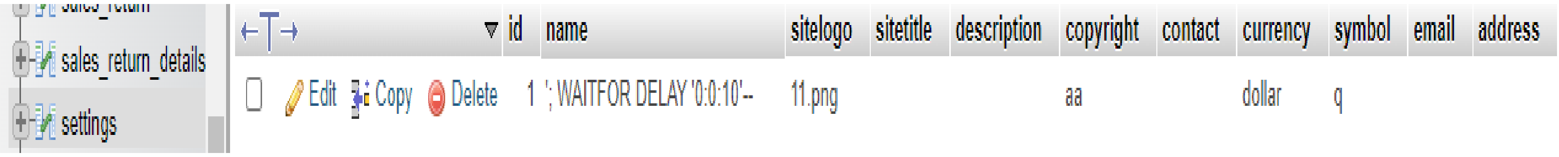
'; WAITFOR DELAY '0:0:10'--

Site Logo

No file chosen

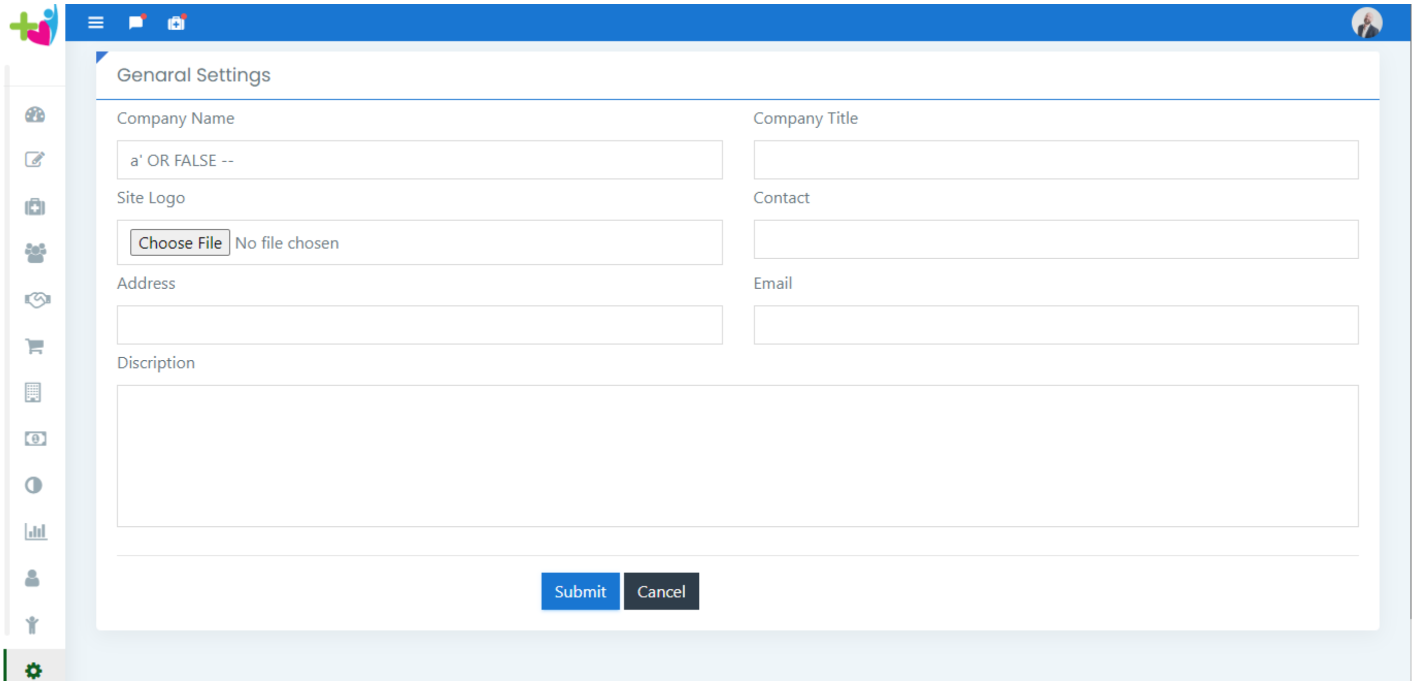
Address

Discription



id	name	sitelogo	sitetitle	description	copyright	contact	currency	symbol	email	address
1	'; WAITFOR DELAY '0:0:10'--	11.png			aa		dollar	q		

Conditional Based (No change to page happened)



Genaral Settings

Company Name: a' OR FALSE --

Company Title:

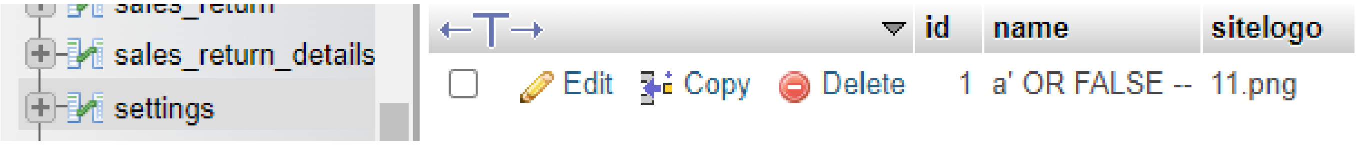
Site Logo: Choose File No file chosen

Contact:

Address:

Email:

Discription:



id	name	sitelogo
1	a' OR FALSE --	11.png