

FCS Project - Security Vulnerabilities

Group 28

Mihir Chaturvedi - 2019061

1. Misconfigured CORS Policy

The website's CORS policy allows requests from all origins, thereby allowing any mock website to POST or GET to their URL's and get privileged information.

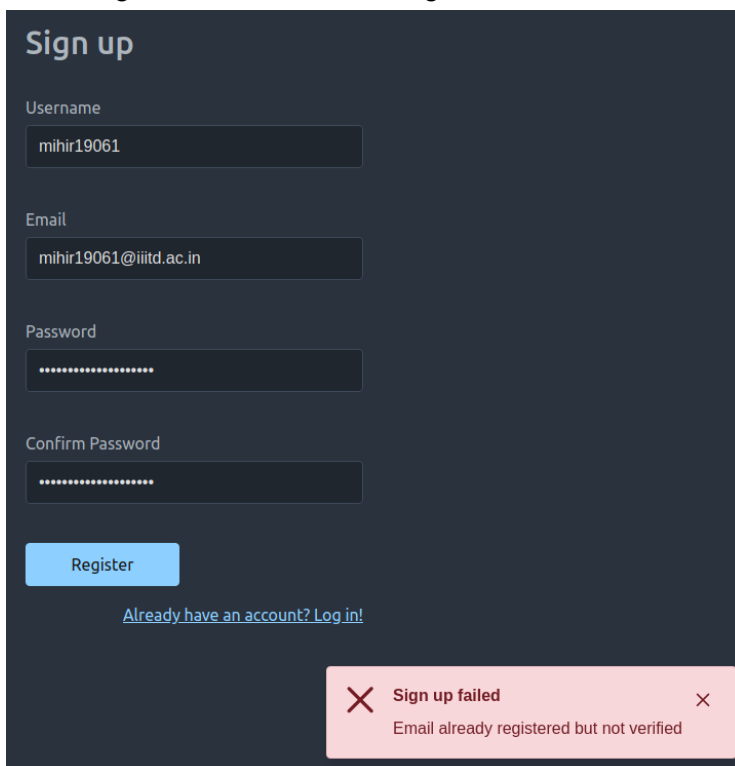
```
▼ Response Headers    View source
access-control-allow-credentials: true
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: cid,Accept,Authorization,Cache-Control,Keep-Alive,Origin,User-Agent,X-Requested-With
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
access-control-expose-headers: cid,authorization
Connection: keep-alive
```

2. No CSRF Protection

Without CSRF protection, this website is susceptible to double form submissions and CSRF attacks. Through social engineering, the victim can submit a form on the attacker's website, which can then be used to request information from the real website.

3. Stuck in login-register loop

I can't register because according to the website, this email already exists.



The screenshot shows a 'Sign up' form with the following fields: Username (filled with 'mihir19061'), Email (filled with 'mihir19061@iiitd.ac.in'), Password (masked with dots), and Confirm Password (masked with dots). A blue 'Register' button is at the bottom left. Below the button is a link: 'Already have an account? Log in!'. At the bottom right, there is a red error message box that says: 'Sign up failed' and 'Email already registered but not verified'.

I can't request to change the password because according to them, this email does not exist.

Forgot Password

Kindly enter the email where you want to receive the verification code

mihir19061@iiitd.ac.in



Send Code



Unsuccessful email send request



Email doesn't exist