waste my time. Check the program policy & check their stance on this. Most websites implement strong password policies and 2FA.

## Updating account information

- **Is there any CSRF protection when updating your profile information?** (*There should be, so expect it. Remember, we're expecting this site to be secure and we want to challenge ourselves on bypassing their protection*). If yes, how is this validated? What happens if I send a blank CSRF token, or a token with the same length?

```
------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="_method"

PATCH
------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="_token"

oElYfJJaEu0NAdRlqD8FHC0gRrRvYZ2Ff7pDQ9ax
------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="profile_image"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="profile_name"

Patrice S.
------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="profile_description"

Junior developer at Barker
------WebKitFormBoundaryTnCDHp0fXMPGoZBQ
Content-Disposition: form-data; name="country"
```

- **Any second confirmation for changing your email/password?** If **no**, then you can chain this with XSS for account takeover. Typically by itself it isn't an issue, but if the program wants to see impact from XSS then this is something to consider.

- **How do they handle basic < > " ' characters and where are they reflected?** What about unicode? %09 %07 %0d%0a - These characters should be tested