

Web Application Security Testing -> Root Me (HTML - disabled buttons, JavaScript - Authentication, JavaScript - Source, XSS - Stored 1)

- Web Application Security Testing -> Root Me (HTML - disabled buttons, JavaScript - Authentication, JavaScript - Source, XSS - Stored 1)
 - Root Me (HTML - disabled buttons)
 - Root Me (JavaScript - Authentication)
 - Root Me (JavaScript - Source)
 - Root Me (XSS - Stored 1)

Root Me (HTML - disabled buttons)

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', and 'Kali Linux'. 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 list of '310 visitors now' and 'Newest members'. The main content area displays the challenge title 'HTML - disabled buttons' with '5 Points' and 'HTML protection?'. It also shows the author 'Final' and the date '16 July 2017'. The 'Statement' section reads: 'This form is disabled and can not be used. It's up to you to find a way to use it.' Below this is a 'Start the challenge' button. The 'Vulnerability sheet(s)' section lists 'HTML - Button disabled [EN]'. The 'Validation' section has a label 'Enter password' and a corresponding input field.

Solution:

1. Start the challenge

The screenshot shows a 'Website temporarily closed.' message. Below the message is a red-bordered box containing an input field and a button labeled 'Member access'. Red arrows point to both the input field and the button. The text '1) Input and button disabled' is written below the box.

2. Press the [F12] button (to open the developer toolbar).

3. Go to the "Inspector" tab.
4. Expand all branches of the form.
5. The `<input>` and `<button>` tags have the `disabled=""` attribute.
6. Double click on it (to edit) and delete them.

The screenshot shows a web browser at the URL `challenge01.root-me.org/web-client/ch25/`. The page displays the "Root Me" logo and a message "Website temporarily closed." Below this is a form with an input field and a "Member access" button. The browser's developer tools are open to the "Inspector" tab, showing the HTML structure. The form is expanded, revealing the `<input disabled="" type="text" name="auth-login" value="">` and `<input disabled="" type="submit" value="Member access" name="authbutton">` tags. Red arrows point from the instructions to the relevant elements: the "Inspector" tab, the form branches, and the disabled attributes.

1) Press the [F12] button
(to open the developer toolbar).

2) Go to the "Inspector" tab.

3) Expand all branches of the form.

4) The `input` and `button` tags have the `disabled=""` attribute. Double click on it (to edit) and delete them.

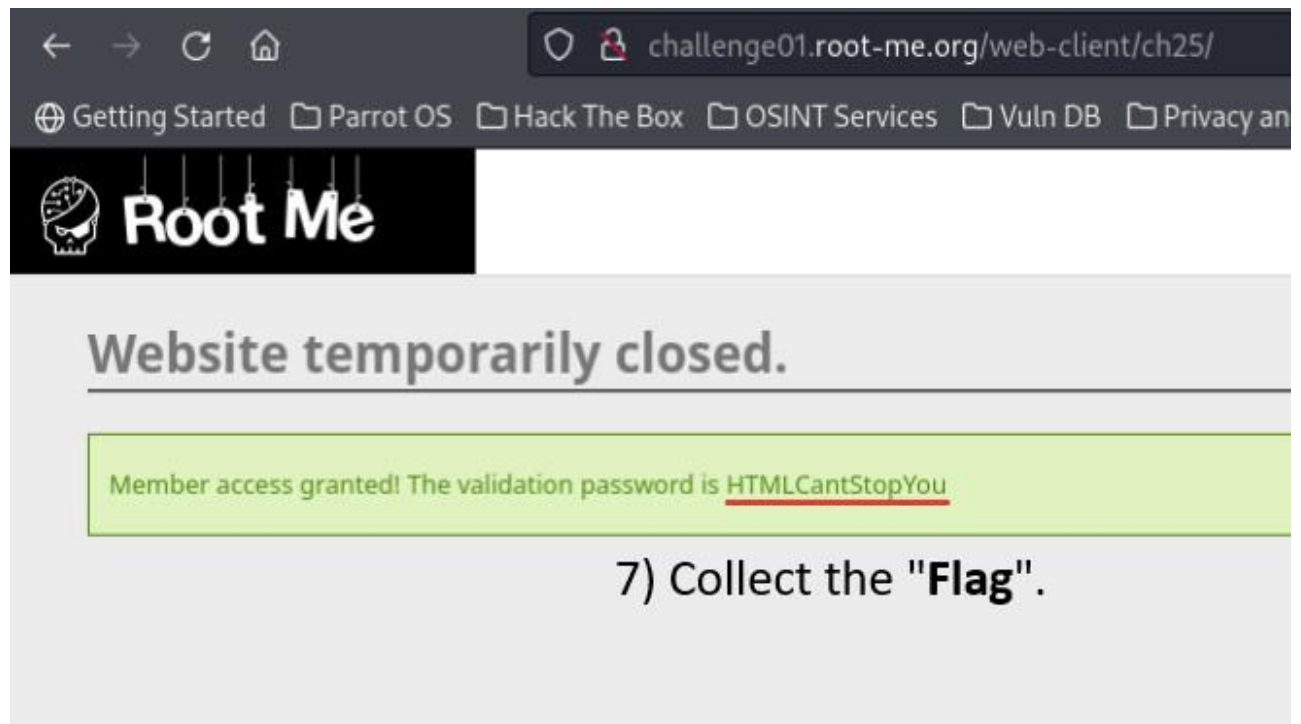
7. Enter any message (e.g.: *hello world*).
8. Click the [Member Access] button.

The screenshot shows the same web browser page. The input field now contains the text "hello world". The "Member access" button is highlighted with a red arrow. Red arrows also point from the instructions to the input field and the button.

5) Enter any message (e.g.: *hello world*)

6) Click the [Member Access] button.

9. Collect the "Flag".



Root Me (Javascript - Authentication)

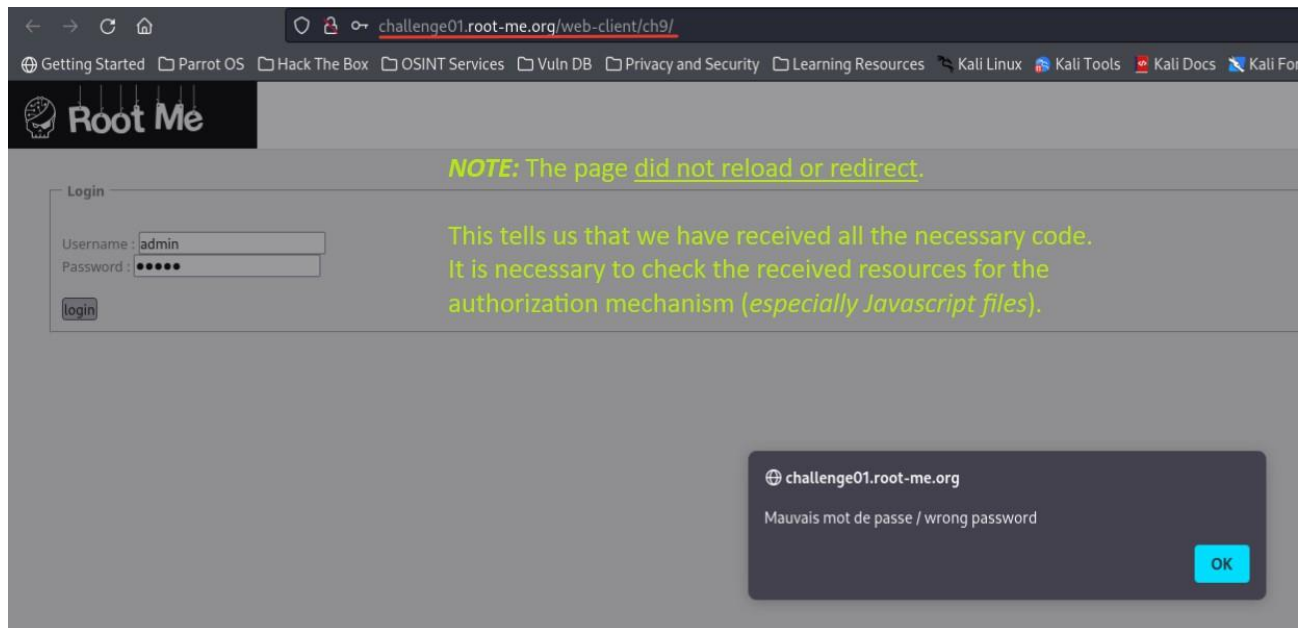
The screenshot shows the Root Me website interface. The top navigation bar includes links to Getting Started, Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, Learning Resources, and Kali Linux. The main header features the Root Me logo and a search bar. The left sidebar contains links to Capture The Flag, Challenges, Community, and Information, along with a visitor count of 410 and a list of newest members. The main content area displays the challenge title 'Javascript - Authentication' with 5 points, the author 'g0uZ' (8 October 2006), and a level indicator. A 'Start the challenge' button is prominently displayed. Below this, the challenge statement is shown, followed by a list of vulnerabilities: 'JavaScript - Authentication [EN]' and 'Javascript - Code source [EN]'. The validation section includes a password input field and a 'login' button.

Solution:

1. Start the challenge.
2. Enter *Username*: `admin` and *Password*: `admin`.
3. Press the `[login]` button.

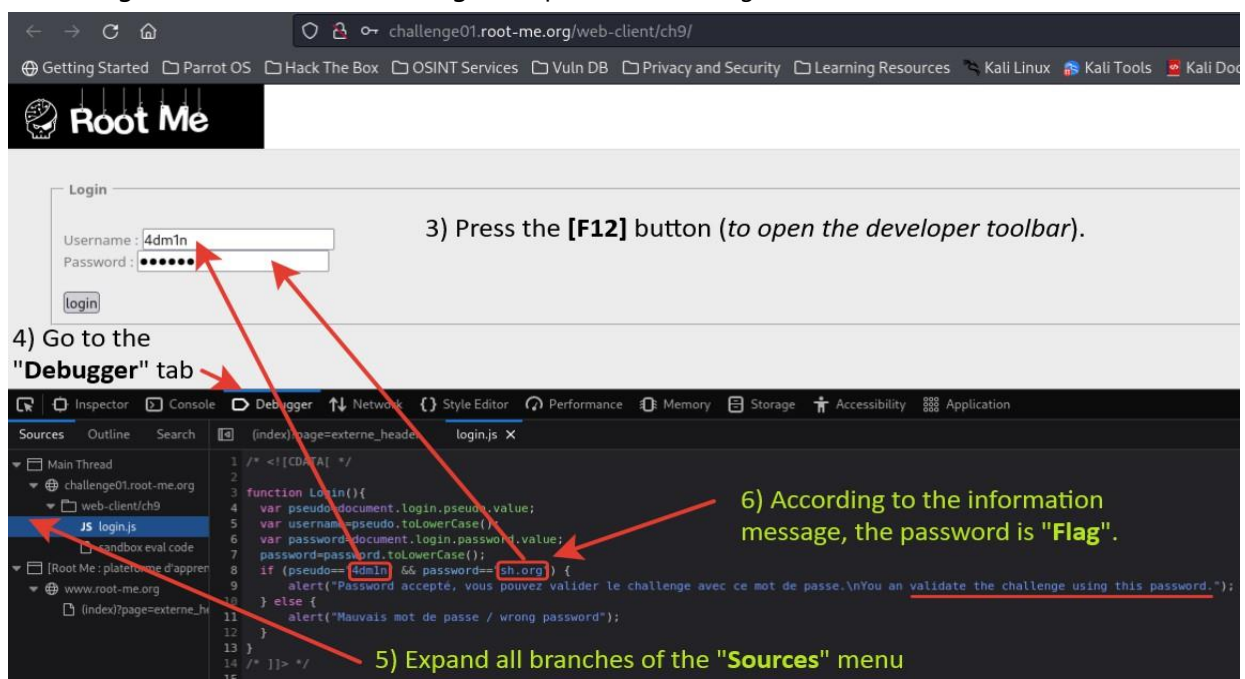
This screenshot shows the login form on the Root Me website. The form is titled 'Login' and contains two input fields: 'Username' and 'Password'. The 'Username' field is pre-filled with 'admin', and the 'Password' field is filled with dots. A 'login' button is located below the input fields. Red arrows point to the 'Username' and 'Password' fields, and another red arrow points to the 'login' button. To the right of the form, text instructions are provided: '1) Enter Username: "admin" and Password: "admin"' and '2) Press the [login] button'.

4. The message "Mauvais mot de passe / wrong password." appears.

**NOTE:**

The page did not reload or redirect. This tells us that we have received all the necessary code. It is necessary to check the received resources for the authorization mechanism (*especially Javascript files*).

5. Press the [F12] button (to open the developer toolbar).
6. Go to the "Debugger" tab.
7. Expand all branches of the "Sources" menu.
8. Here we found the `login.js` file.
9. According to the information message, the password is "Flag".



Root Me (Javascript - Source)

The screenshot shows the Root Me website interface. The top navigation bar includes links for Getting Started, Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, Learning Resources, and Kali Linux. The main header features the Root Me logo and a search bar. The left sidebar contains navigation links for Capture The Flag, Challenges, Community, and Information, along with a visitor count of 402 and a list of newest members. The main content area displays the 'Javascript - Source' challenge with a 5-point rating, a 'Start the challenge' button, and a list of related resources. The bottom section shows a validation input field for the password.

Root Me

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources Kali Linux

HOME / CHALLENGES / WEB - CLIENT

Javascript - Source

5 Points

You know javascript ?

Author: g0uZ, 7 October 2006

Level ?

Statement

[Start the challenge](#)

Vulnerability sheet(s)

Javascript - Code source [EN]

1 related ressource(s)

- rfc1945 (RFC)

Validation

Enter password

402 visitors now

Newest members :

- mudomudo Sneakes Blah
- Nicels84086 sal4djm6
- Anonymous Ace

Offers

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

Sponsored by

- Oteria Cyber School
- Elysium Security
- École 2600
- GEOIDE
- Almond
- Synacktiv
- You ;-)

Solution:

1. Start the challenge.
2. Press the **[F12]** button (to open the developer toolbar).
3. Go to the "Debugger" tab.
4. Expand all branches of the "Sources" menu.
5. Here we found the (**index**) file.
6. According to the information message, the password is "Flag".



Root Me (XSS - Stored 1)

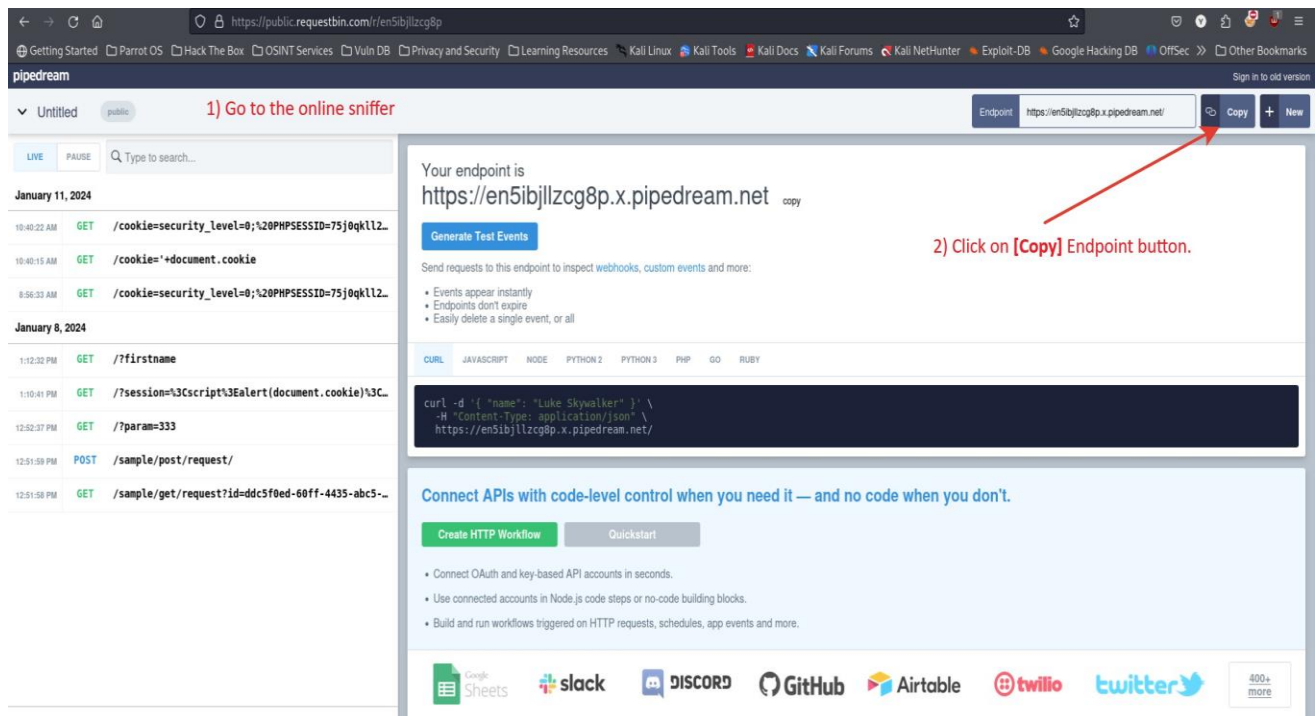
The screenshot shows the Root Me website interface. The top navigation bar includes links to Getting Started, Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, Learning Resources, Kali Linux, and a search bar. The main content area displays the challenge details for 'XSS - Stored 1', which is worth 30 points and is described as 'So easy to exploit'. The author is g0uZ, and the challenge was created on 3 March 2012. The statement of the challenge is: 'Steal the administrator session cookie and use it to validate this chall.' A 'Start the challenge' button is visible. Below the statement, there is a section for 'Vulnerability sheet(s)' listing 'XSS - Stored [EN]'. A section for '7 related ressource(s)' lists several related challenges and exploits, including 'XSS enregistrée (Web)', 'Blackhat US 2011 : XSS street fight (Exploitation - Web)', 'XSS et phishing (Exploitation - Web)', 'SSTIC 2009 : XSS de la brise à l'ouragan (Exploitation - Web)', and 'BlackHat US 2009 favorite XSS Filters-IDS and how to attack them (Exploitation - Web)'. The left sidebar shows the user's profile, navigation links, and a list of offers.

Solution:

1. Start the challenge.

The screenshot shows the challenge interface for 'challenge01.root-me.org/web-client/ch18/'. The interface features a 'Forum v0.001' section with a form for posting a message. The form includes a 'Title:' field, a 'Message:' text area, and a 'send' button. Below the form, there is a section for 'Posted messages:' which currently displays a 'Welcome' message: 'N'hésitez pas à me laisser un message / Feel free to leave a message'.

- Go to the online sniffer (e.g.: <https://public.requestbin.com/r/>).
- Click on **[Copy]** Endpoint button.



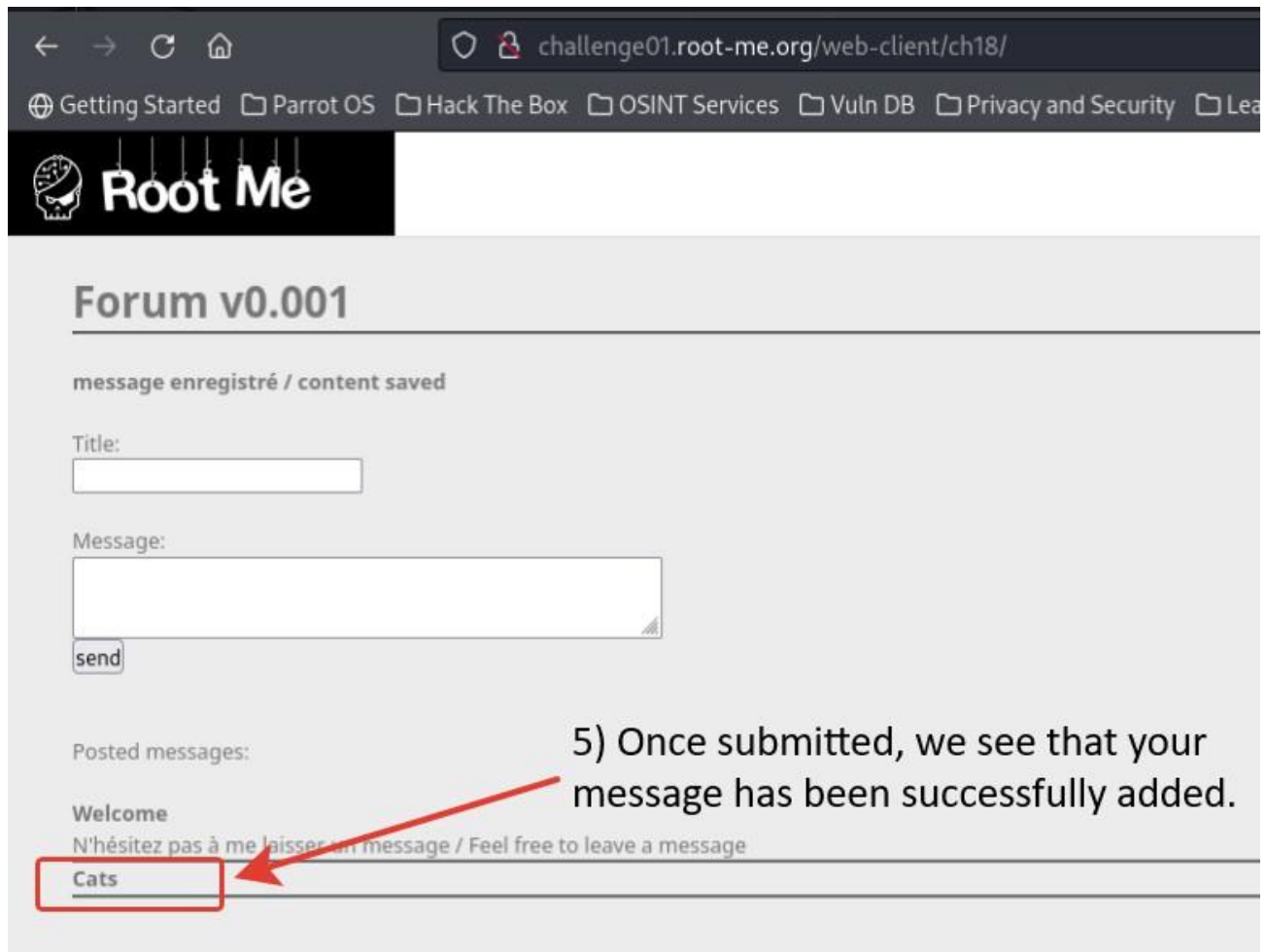
- Prepare the following JavaScript code (to intercept cookies)

```
<script>document.write('');</script>
```

- Enter any title (*e.g.: **Cats**) and paste the code prepared in **Step 4** into the text input area.



6. Click the [send] button.



7. Go to the online sniffer page and wait for the `ADMIN_COOKIE` to be intercepted.

8. The value of `ADMIN_COOKIE` is "Flag".

