

# Root Me (HTTP - Verb tampering)

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 visitor count of 286 and a list of newest members. The main content area displays the challenge details for 'HTTP - Verb tampering', which is worth 15 points and is categorized under 'HTTP authentication'. The author is listed as 'g0uZ' from February 2011. The challenge statement is 'Bypass the security establishment.' with a 'Start the challenge' button. Below this, there is a 'Vulnerability sheet(s)' section with a link to 'HTTP - Methods [EN]' and a '3 related ressource(s)' section listing RFC 2617, RFC 2069, and a link to 'HTTP basic authentication and digest authentication (Exploitation - Web)'. The page also includes a 'Validation' section.

Root Me

HOME / CHALLENGES / WEB - SERVER

## HTTP - Verb tampering

15 Points 🌤️

HTTP authentication

Author: g0uZ, 3 February 2011

Level ?

Statement: Bypass the security establishment.

[Start the challenge](#)

Vulnerability sheet(s): [HTTP - Methods \[EN\]](#)

3 related ressource(s):

- 🇬🇧 [rfc2617 \(RFC\)](#)
- 🇬🇧 [rfc2069 \(RFC\)](#)
- 🇬🇧 [HTTP basic authentication and digest authentication \(Exploitation - Web\)](#)

Validation

## Solution

1. Run the challenge.

The screenshot shows a web browser window with the URL 'challenge01.root-me.org/web-serveur/ch8/'. The page displays a login form for 'challenge01.root-me.org'. The form includes a message 'This site is asking you to sign in.' and two input fields: 'Username' and 'Password'. Below the input fields are two buttons: 'Cancel' and 'Sign in'.

challenge01.root-me.org

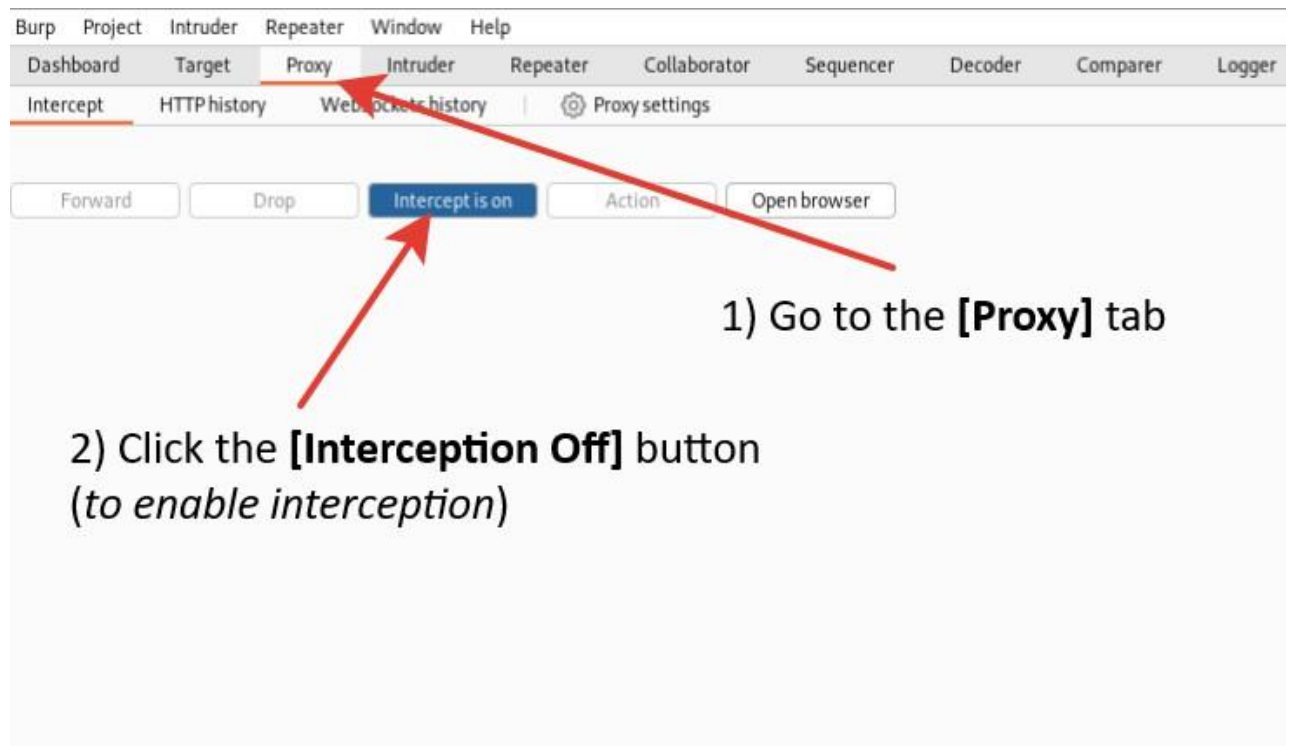
This site is asking you to sign in.

Username

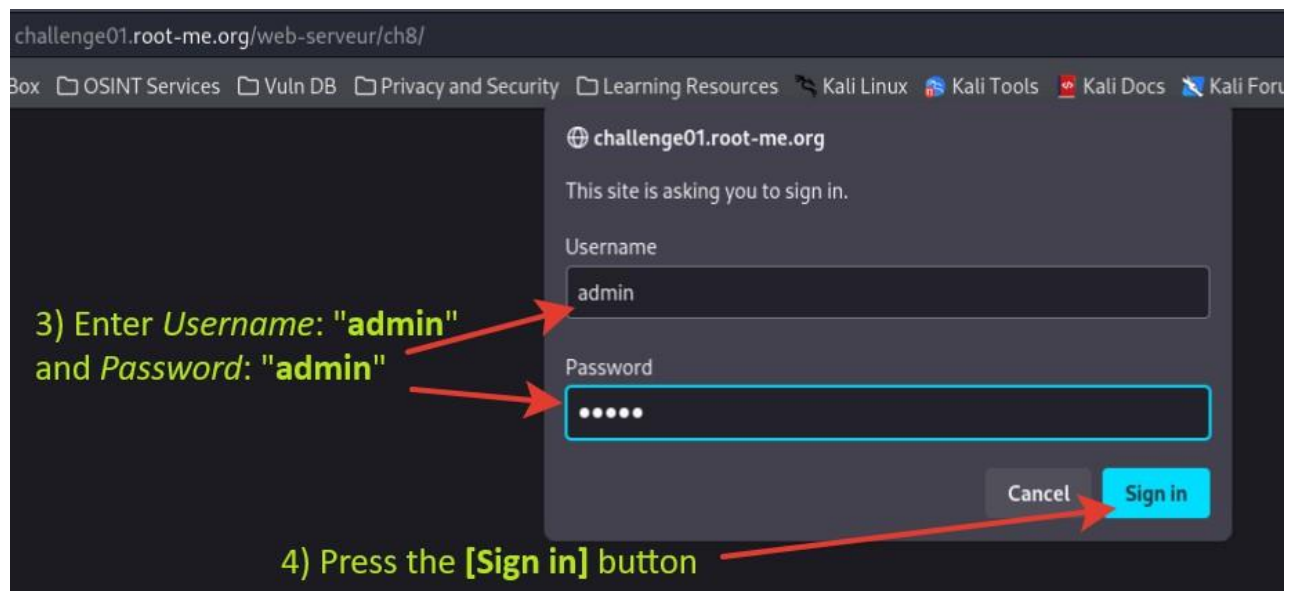
Password

[Cancel](#) [Sign in](#)

2. Launch "Burp Suite".
3. Go to the [Proxy] tab.
4. Click the [Interception Off] button (to enable interception).



5. Enter Username: **admin** and Password: **admin**.
6. Press the [Sign in] button.



7. After intercepting the request, the Burp Suite window will appear.

The *GET method* is used to retrieve data from the server. This is a **read-only** method. But inside the intercepted request we can find the line **Authorization: Basic YWRtaW46YWRtaW4=** - these are specific changes to the resource. To apply the change, we need to use another method that can change the resource. These methods:

- **POST** - creates a new resource,
- **PUT** - updates an existing resource, but its body must contain the complete structure of the modified resource,
- **PATCH** - updates an existing resource and contains in its body only specific changes for the resource.

In this case, we **must replace** the **GET** method with **PATCH** to apply the authorization state change.

- Click the **[Forward]** button (to submit the modified request).
- Click the **[Interception is on]** button (to disable interception).

5) Replace the "GET" method with "PATCH"

6) Click the **[Forward]** button (to submit the modified request)

7) Click the **[Interception is on]** button (to disable interception)

**NOTE:** These are specific changes to the resource that need to be applied.

- Return to the browser.
- Collect the "Flag"

Mot de passe / password : **a23e\$dme96d3saez\$\$prap**

- Collect the "Flag"