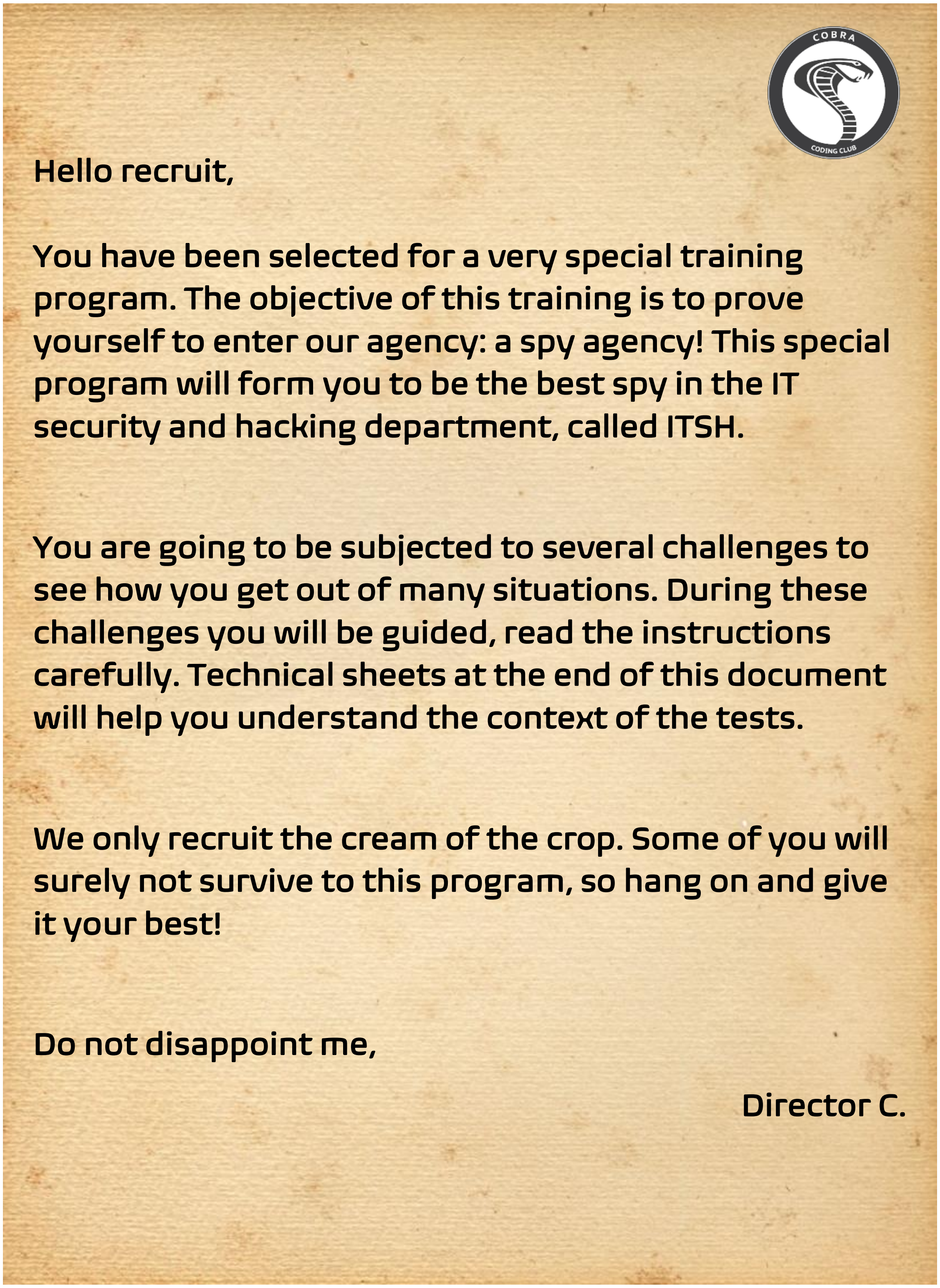
DIVERSITY by EPITECH

COBRA

CODING CLUB

Secret Agent Training Formation

Become an agent of the IT Security and Hacking department (ITSH)



Hello recruit,

You have been selected for a very special training program. The objective of this training is to prove yourself to enter our agency: a spy agency! This special program will form you to be the best spy in the IT security and hacking department, called ITSH.

You are going to be subjected to several challenges to see how you get out of many situations. During these challenges you will be guided, read the instructions carefully. Technical sheets at the end of this document will help you understand the context of the tests.

We only recruit the cream of the crop. Some of you will surely not survive to this program, so hang on and give it your best!

Do not disappoint me,

Director C.

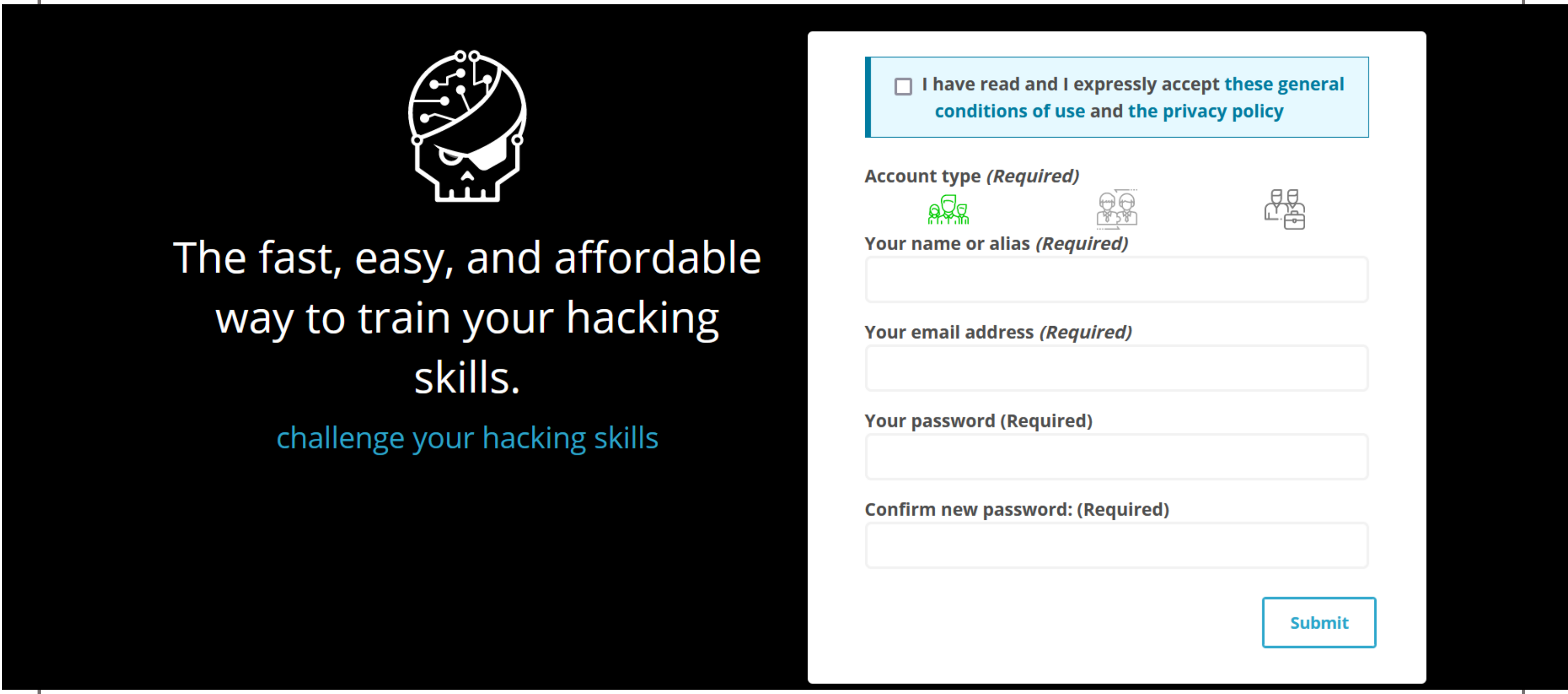
Contents

1. Platform presentation

Our training program will be handled on a website platform call root-me.org.

Root-me is an online platform that permits to anyone to tests and improve their knowledge in IT security and hacking through exercises and challenges!

➔ Go to the website and create an account.



The fast, easy, and affordable way to train your hacking skills.

challenge your hacking skills

□ I have read and I expressly accept these general conditions of use and the privacy policy

Account type *(Required)*

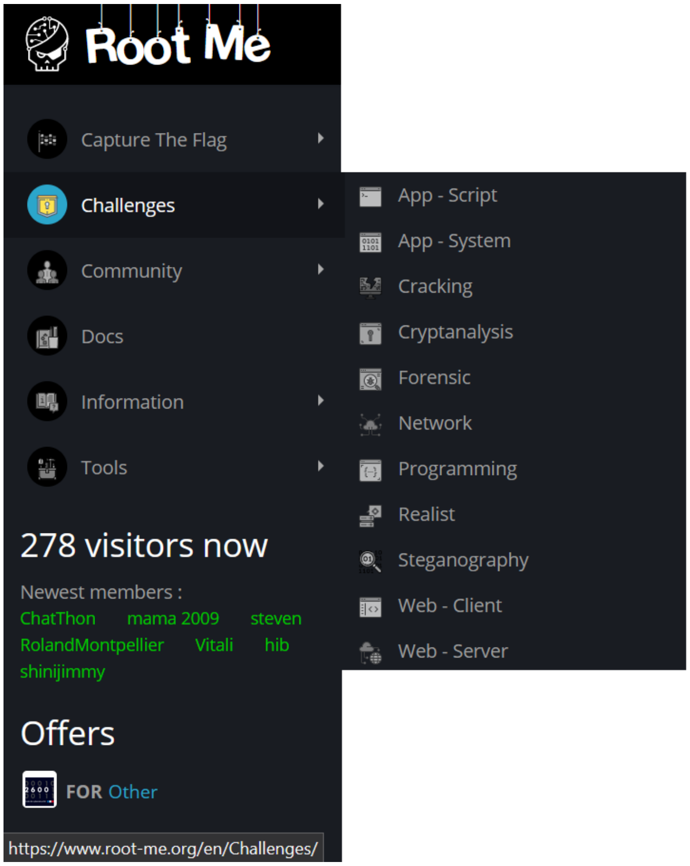
Your name or alias *(Required)*

Your email address *(Required)*

Your password (Required)

Confirm new password: (Required)

Now that you created your account, you officially started the formation program. Come on, recruit!



Take a look on the left side of the website. The panel board permits you to navigate through the website.

There are many rubrics:

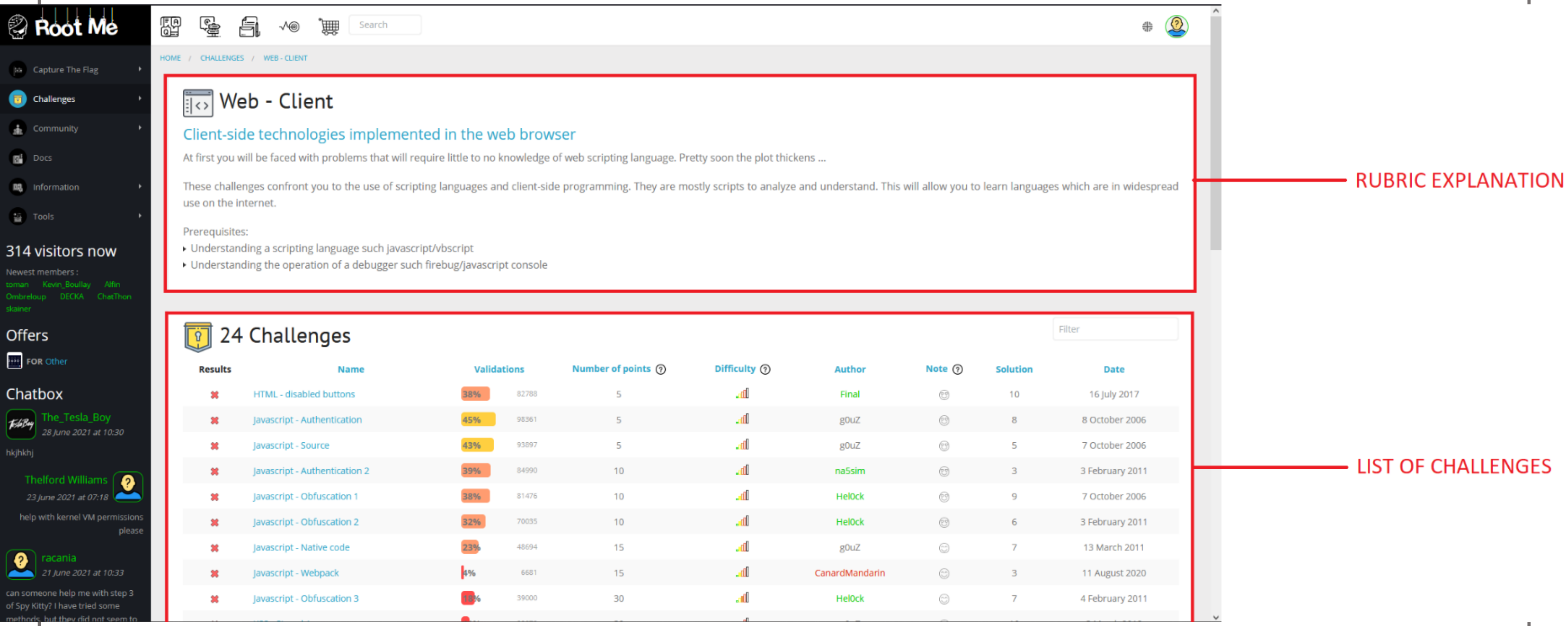
- **Capture flag**: Scheduled hacking contest.
- **Challenges**: here are all the challenges, order by type of knowledge.
- **Community**: communication sector to get in touch with hackers from around the world.
- **Information**: Legal section with rules and general information.
- **Tools**: precious rubrics offering you many documentations. Have a look on it later!

This formation program will focus on your web hacking skills. You will be evaluated on both of server and client sides.

The best of you will have the opportunity to be formed by your supervisors on Stenography: so, start your engines, and may the best spy win.

2. Challenges

You will be guided for the first challenges and then, we will see who the bests spies are in here!



314 visitors now

Newest members :
toman Kevin_Boullay Alfin Ombreloup DECKA ChatThon skainer

Offers

FOR Other

Chatbox

The_Tesla_Boy
28 June 2021 at 10:30
hkjhkhj

Thelford Williams
23 June 2021 at 07:18
help with kernel VM permissions please

racania
21 June 2021 at 10:33
can someone help me with step 3 of Spy Kitty? I have tried some methods, but they did not seem to

Web - Client

Client-side technologies implemented in the web browser

At first you will be faced with problems that will require little to no knowledge of web scripting language. Pretty soon the plot thickens ...

These challenges confront you to the use of scripting languages and client-side programming. They are mostly scripts to analyze and understand. This will allow you to learn languages which are in widespread use on the internet.

Prerequisites:
- Understanding a scripting language such javascript/vbscript
- Understanding the operation of a debugger such firebug/javascript console

24 Challenges

Results	Name	Validations	Number of points ?	Difficulty ?	Author	Note ?	Solution	Date
✖	HTML - disabled buttons	38% 82788	5	📶	Final	☺	10	16 July 2017
✖	Javascript - Authentication	45% 98361	5	📶	g0uZ	☺	8	8 October 2006
✖	Javascript - Source	43% 93897	5	📶	g0uZ	☺	5	7 October 2006
✖	Javascript - Authentication 2	39% 84990	10	📶	na5sim	☺	3	3 February 2011
✖	Javascript - Obfuscation 1	38% 81476	10	📶	Hel0ck	☺	9	7 October 2006
✖	Javascript - Obfuscation 2	32% 70035	10	📶	Hel0ck	☺	6	3 February 2011
✖	Javascript - Native code	23% 48694	15	📶	g0uZ	☺	7	13 March 2011
✖	Javascript - Webpack	4% 6681	15	📶	CanardMandarin	☺	3	11 August 2020
✖	Javascript - Obfuscation 3	18% 39000	30	📶	Hel0ck	☺	7	4 February 2011

RUBRIC EXPLANATION

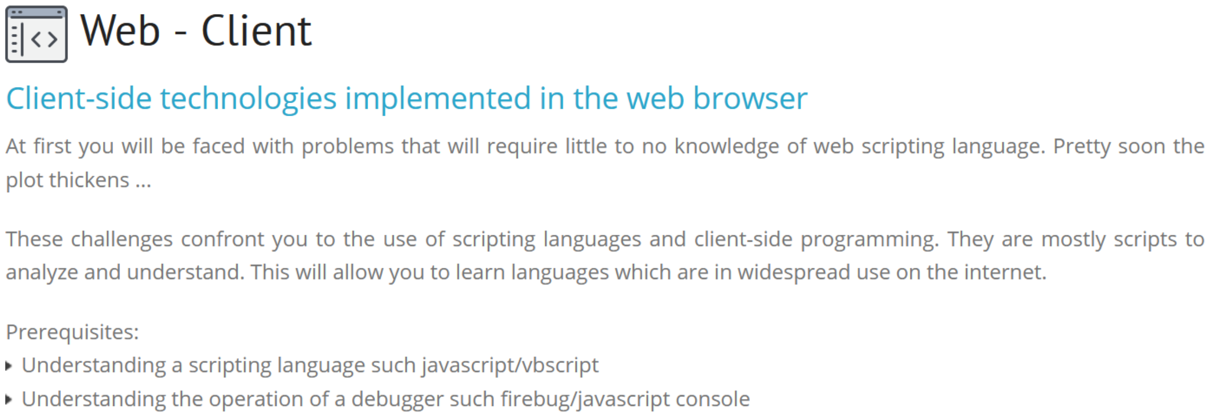
LIST OF CHALLENGES

Each challenges rubric looks the same, you can find the **rubric explanation** on the top, describing challenge contexts and goals and knowledge related.

Then, you can check the **list of challenges** existing on this rubric with their details: percentage of validation, points that you can gain resolving those challenges, difficulty, etc.…

If you are really blocked and need some help: you have the results of each challenge on the bottom of the page. Do not try to cheat, we are watching you!

A. Client



Web - Client

Client-side technologies implemented in the web browser

At first you will be faced with problems that will require little to no knowledge of web scripting language. Pretty soon the plot thickens ...

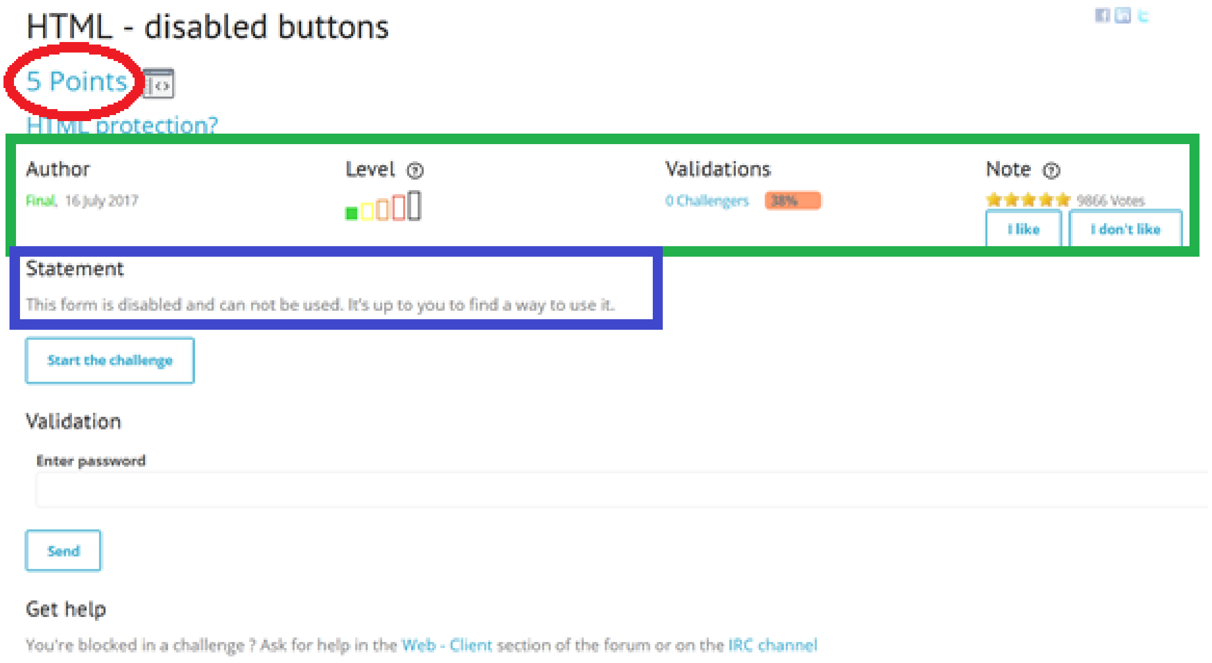
These challenges confront you to the use of scripting languages and client-side programming. They are mostly scripts to analyze and understand. This will allow you to learn languages which are in widespread use on the internet.

Prerequisites:

- Understanding a scripting language such javascript/vbscript
- Understanding the operation of a debugger such firebug/javascript console

➔ Start on with: HTML - Disabled Button

Come on recruit, this first challenge will be guided. Do not get use to it, we will not hold your hand for the next challenges!



HTML - disabled buttons

5 Points

HTML protection?

Author
Final, 16 July 2017

Level

Validations
0 Challengers 38%

Note
★★★★★ 9866 Votes

Statement
This form is disabled and can not be used. It's up to you to find a way to use it.

Validation

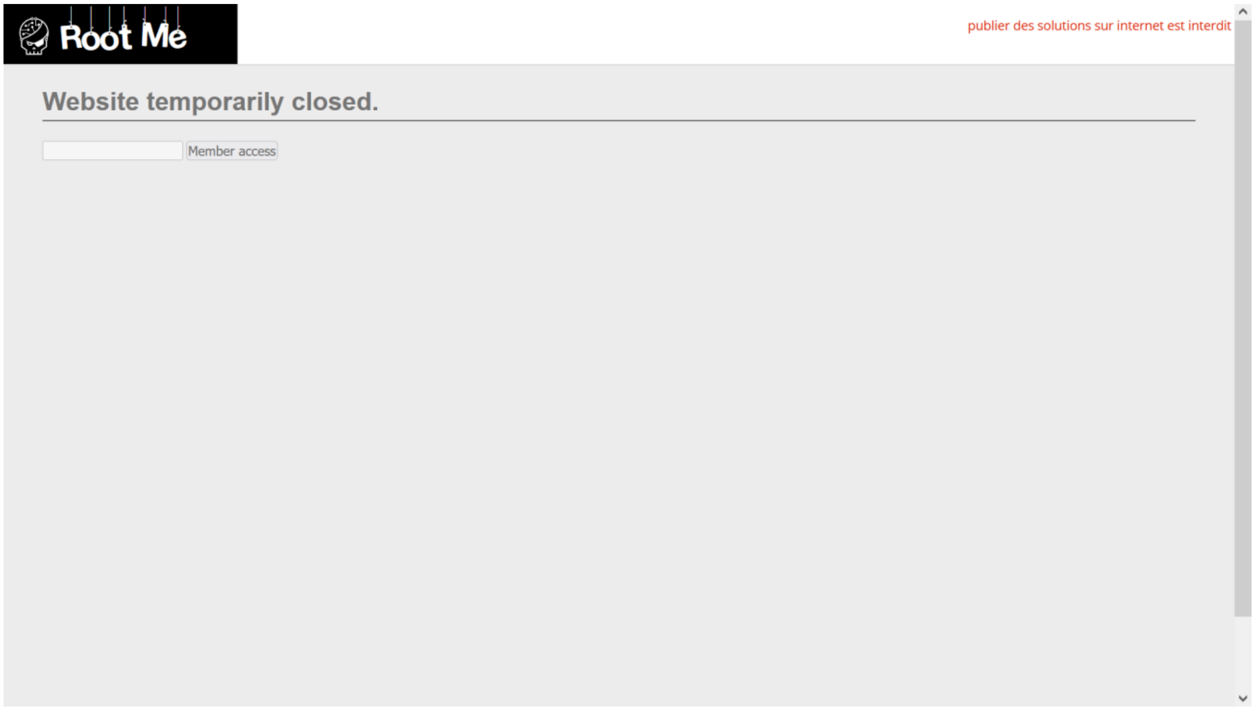
Enter password

Get help
You're blocked in a challenge ? Ask for help in the Web - Client section of the forum or on the IRC channel

Clicking on the challenge's link you will end up on this interface.

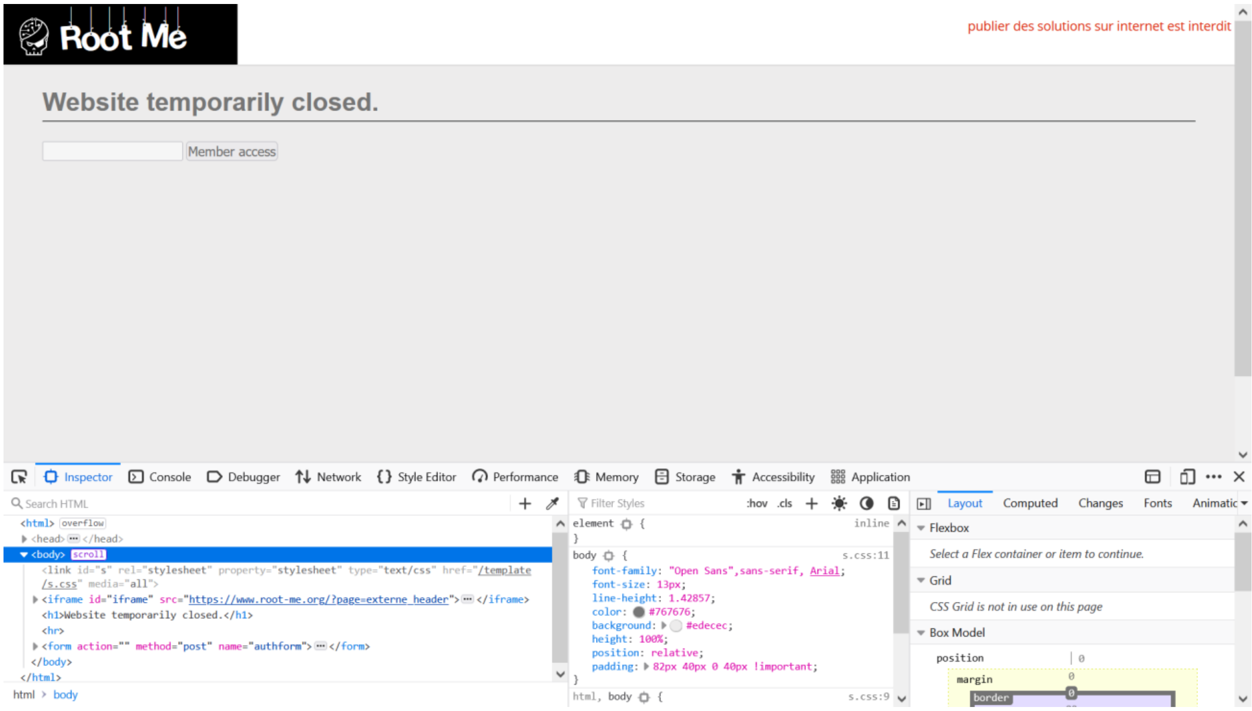
You can see underneath the title, the **value of this exercise**. Here, validating this challenge will give you 5 points. Then you can see some **details about this challenge** and the **challenge explanation**. Finally, you can see a button to '*Start the challenge*' and a text zone to enter you answer.

For this challenge, you kick-off in this website:



Website temporarily closed.

As you can see, the **Member access** button is disabled. **You must make it enabled**. To do so, on the website, click on your keyboard key F12.



Website temporarily closed.

```
<html> overflow
  <head> ··· </head>
  <body> scroll
    <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="/template
    /s.css" media="all">
    <iframe id="iframe" src="https://www.root-me.org/?page=externe_header"> ··· </iframe>
    <h1>Website temporarily closed.</h1>
    <hr>
    <form action="" method="post" name="authform"> ··· </form>
  </body>
</html>
```

```
element {                                              inline
}
body {                                                 s.css:11
    font-family: "Open Sans",sans-serif, Arial;
    font-size: 13px;
    line-height: 1.42857;
    color: #767676;
    background: #edecec;
    height: 100%;
    position: relative;
    padding: 82px 40px 0 40px !important;
}
html, body {                                           s.css:9
```

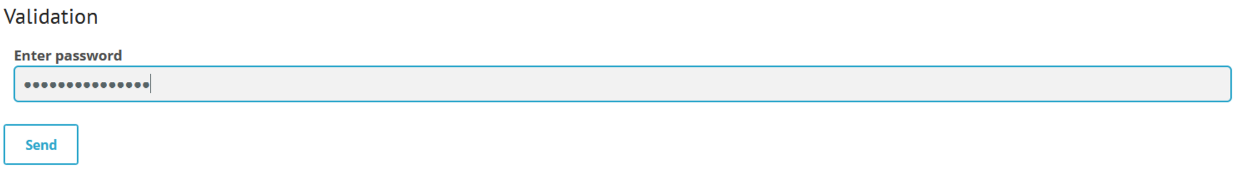
Select a Flex container or item to continue.

CSS Grid is not in use on this page

Welcome on the inspector, the source code manager, debugger and console of the website. On the bottom left you can see the source HTML code of this page.

Somewhere within it, is the code creating the Button you have enable. Look for it and remove the disabled option!

When you are done, you will see the password. Go back on the main page of the exercise and enter the password.



Continue with the others Web Client challenges:

- Go on with: JavaScript - Authentication
  - Advice: Look deeper in the **F12** inspector. This time, have a look on the *Network* part!
- Come on! JavaScript - Source
  - Continue inspecting the network section…
- Try harder with JavaScript - Authentication n°2
  - This one is easier, recruit! Look for the JavaScript file in charge of the login pop-up and look for the answer in it.
- Recruit, go, go! JavaScript - Obfuscation n°1
  - For this challenge, look first for the encrypted password. Then, learn how to use an ASCII Table to decrypt it.
- Almost done. Try this one: JavaScript - Obfuscation n°2
  - This one is a little bit tricky. Find the encrypted value of the variable *pass*. Then try to decrypt it using the same way than before. Then, have a look on this website.
- Last one: JavaScript - Native code

B. Server

Web - Server

Discover the mechanisms, protocols and technologies used on the Internet and learn to abuse them!

These challenges are designed to train users on HTML, HTTP and other server side mechanisms. The following series of challenges will cultivate a better understanding of techniques such as : Basic workings of multiple authentication mechanisms, handling form data, inner workings of web applications, etc. ...

Prerequisites:

- Understand HTML.
- Understand the HTTP protocol.
- Ability to manipulate a web browser.

➔ Kick-off with HTML - Source code

➔ Go on with Weak password

➔ Go, go, go! HTTP - Directory indexing

➔ Keep on it: HTTP - Headers

➔ Finally: HTTP - POST

C. Stenography and Decryption

If you end up this far, you are probably on the best spy of this formation. Go on with a new skill: stenography.

Stenography is also known as the art of hiding information within an image. Hiding information is a precious skill for a great spy.

- ➔ Start on with: Gunnm
  - Advice: this one do not require technical skills. Open your eyes!
- ➔ A little bit harder with: Squared
  - The password is on the image but not visible, play with an image editor!
- ➔ Go on: Twitter Secret Messages
  - There is no better friend than Google…

3. Tricks and tools

A. Cookies: Agent, do not eat the cookies!

No recruit, this is not lunch time. Stay focus!

What are those strange cookies that a website has surely already propose to you?

Most of the time, when a web server proposes a cookie, users ignore this term and click on ‘*Accept all cookies*’. A **cookie** is, in fact, **a file stored on the user Hard Disk**. It allows a web server to recognize the user from one page to the other. Cookies are mainly used by commercial websites in order to keep user preferences, settings, etc.

Cookies and security

The major problem with cookies is the information they contain. Indeed, when a user connects to a customizable site, the latter will ask him some questions in order to draw up their profile, then store this data in a cookie. Depending on the site, the manner in which the information is stored may be harmful to the user.

Cookies functioning

Cookies are part of the HTTP protocol specifications, the protocol that allows you to surf web pages. The HTTP protocol allows the exchange of messages between the client and the server through HTTP requests and responses.

HTTP requests and responses contain headers that allow specific information to be sent bilaterally. One of these headers is dedicated to writing files to the hard drive: **cookies**.

The HTTP header that is reserved for the use of cookies is called Set-Cookie. It is a line of simple text in the following form:

```
Set-Cookie : NAME=VALUE; domain=VALUE; expires=DATE
```

B. HTML/CSS: A spy might talk many languages.

First of all, HTML and CSS are not identical. They work in teams! Together, they form the bones and skin of any website.

HTML stands for Hypertext Markup Language. See HTML as the skeleton of a document. HTML is what gives structure to the site. This is done through tags, elements and attributes. Whether you want titles, lists, images or links, HTML does it all.

CSS stands for Cascading Style Sheet. If HTML is the skeleton of your page, CSS is the skin. Without CSS, your websites would be really boring and dare we say, naked.

C. Header HTTP

HyperText Transfer Protocol (HTTP) is the most widely used protocol on the Internet since 1990. The purpose of the HTTP protocol is to allow a file transfer (mainly in HTML format) localized through a string called URL between a browser (the client) and a Web server.

A HTTP request is a set of lines sent to the server by the browser. It includes:

- **A query line**: this is a line specifying the type of document requested.
- The **header** fields of the request: this is a set of optional lines to give additional information about the request and/or the client (Browser, operating system, ...)
- The **body** of the request: core of the request

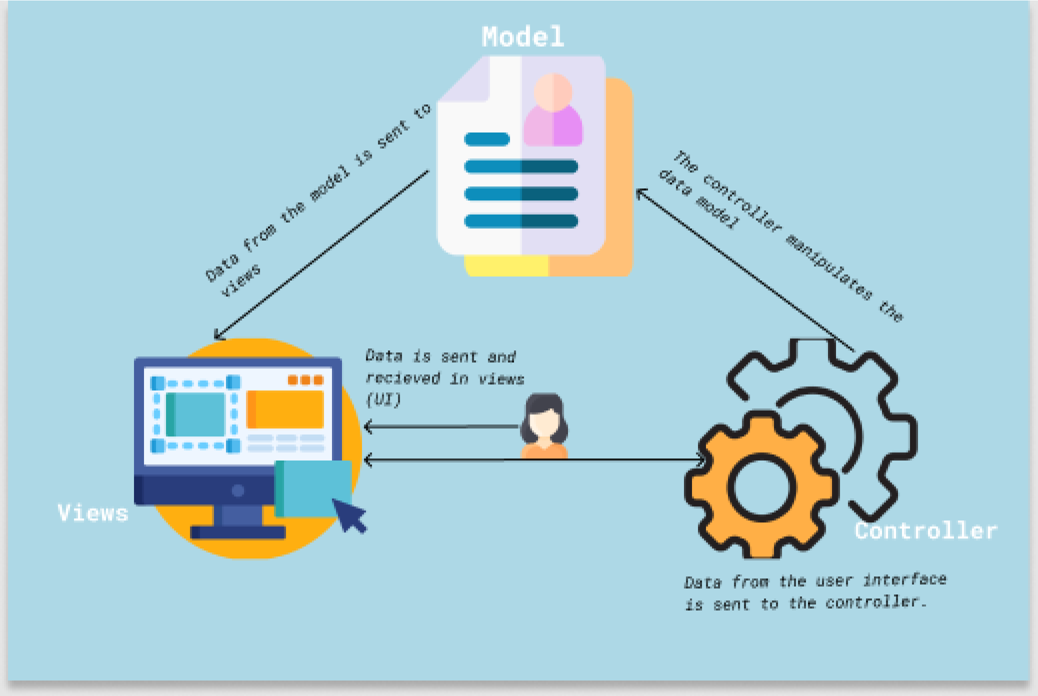
You may find a lot of really interesting information about the request in the header! Keep it in mind.

D. JavaScript: This is not Russian, but definitely helpful.

JavaScript is a scripting language mainly used in interactive web pages and as such is an essential part of web applications.

JavaScript code can be integrated directly into the web pages, to be executed on the client workstation. It is then the web browser that supports the execution of these programs called scripts.

Generally**, JavaScript is used to control the data entered in HTML forms**, or Generally, JavaScript is used to control the data entered in HTML forms, or to interact with the HTML document. **It is also used to perform dynamic applications, transitions, animations or manipulate reactive data, for ergonomic or cosmetic purposes.**


Model
Data from the model is sent to views
The controller manipulates the data model
Data is sent and recieved in views (UI)
Views
Controller
Data from the user interface is sent to the controller.

You can see in the example above, a JavaScript MVC model. M for Model, this is what the server will display. V for Views, this is what you see. C as Controller, this is what transform the model.

For instance, you click on a website on a button (the View) which is sent to the controller. The controller will do the modification it has to do on the model so the server can send back the new model to the views. And you will then see the modification after clicking on this button.

This is JavaScript's power, among many script languages.

E. Images: Agent, look for any clue!

F. Cryptography: Keep secrets and hide it!