

Домашнее задание:

1. Исследуйте комментарии в коде страницы <http://IP/mutillidae/index.php?page=home.php> на наличие в них полезной информации. Какие сведения можно обнаружить?
2. Найдите в ВМ pdf-файл(ы) и укажите, при помощи какого средства, когда и кем был создан(ы) данный(е) объект(ы).
3. Решите задание <https://www.root-me.org/en/Challenges/Web-Server/HTML>. Надо подобрать пароль — укажите его в ответе.

Домашнее задание (повышенная сложность):

1. * Решите задание <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source>. Надо подобрать пароль — укажите его в ответе.
2. * В ВМ установлен сайт на drupal. Может ли злоумышленник подобрать для него рабочий эксплоит? Ответ обоснуйте.

1.

```
<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai web testing framework.
It is ok to put the password in HTML comments because no user will ever see
this comment. I remember that security instructor saying we should use the
framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
rather than HTML comments, but we all know those
security instructors are just making all this up. --> <!-- End Content -->
try{
  //if(!window.localStorage.length){
    window.localStorage.setItem("SelfDestructSequence1","Destruct sequence 1, code 1-1A");
    window.localStorage.setItem("SelfDestructSequence2","Destruct sequence 2, code 1-1A-2B");
    window.localStorage.setItem("SelfDestructSequence3","Destruct sequence 3, code 1B-2B-3");
    window.localStorage.setItem("MessageOfTheDay","Go Cats!");
    window.localStorage.setItem("SecureMessage","Shh. Do not tell anyone.");
    window.localStorage.setItem("FYI","A couple of keys are not showing in this list. Why?");
  }
  //if(!window.sessionStorage.length){
    window.sessionStorage.setItem("AuthorizationLevel", "0");
    window.sessionStorage.setItem("ChuckNorrisJoke1","When Alexander Bell invented the telephone he had 3 missed calls from ");
    window.sessionStorage.setItem("ChuckNorrisJoke2","Death once had a near-Chuck Norris experience");
    window.sessionStorage.setItem("ChuckNorrisJoke3","He counted to infinity; twice");
    window.sessionStorage.setItem("ChuckNorrisJoke4","Chuck Norris can slam a revolving door");
    window.sessionStorage.setItem("ChuckNorrisJoke5","Chuck Norris can cut through a hot knife with butter");
    window.sessionStorage.setItem("SecureKey", "You cannot see me on the HTML5 Storage page. I wonder why?");
  }
```

Из html комментариев можно достать логин и/или пароль samurai

В // и /* комментариях ничего интересного нет.

Есть интересные строки SecureKey, SecureMessage.

2. Качаем pdf файлы (на момент скриншота уже скачал, поэтому такая директория).

Нашелся только один файл в /mutillidae/documentation

```
(kali@kali)-[~/192.168.56.11/mutillidae/documentation]
$ wget --accept pdf --mirror --page-requisites --adjust-extension --convert-links --backup-converted --no-parent http://192.168.56.11/
```

```

$ exiftool mutillidae-installation-on-xampp-win7.pdf
ExifTool Version Number      : 12.16
File Name                    : mutillidae-installation-on-xampp-win7.pdf
Directory                    :
File Size                    : 1569 KiB
File Modification Date/Time   : 2018:10:19 18:53:20-04:00
File Access Date/Time        : 2021:04:06 05:33:13-04:00
File Inode Change Date/Time   : 2021:04:06 05:33:13-04:00
File Permissions              : rw-r--r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.5
Linearized                   : No
Page Count                   : 12
Language                     : en-US
Tagged PDF                   : Yes
Author                       : Jeremy
Creator                      : Microsoft® Word 2010
Create Date                  : 2011:11:10 18:39:03-05:00
Modify Date                  : 2011:11:10 18:39:03-05:00
Producer                     : Microsoft® Word 2010

```

Jeremy автор файла.
 Файл был создан в MS Word 2010 и экспортирован в pdf.
 Дата создания 10.11.2011.

3. Сделал это задание еще после первого урока.

| | | | | | | |
|---|-------------------------------------|-----|--------|----|--|----------|
| ✓ | HTML - Code source | 49% | 104252 | 5 | | g0uZ |
| ✗ | HTTP - Contournement de filtrage IP | 1% | 620 | 10 | | Cyrhades |
| ✓ | HTTP - Open redirect | 10% | 40087 | 10 | | Swissky |
| ✗ | HTTP - User-agent | 25% | 51876 | 10 | | g0uZ |
| ✓ | Mot de passe faible | 33% | 70516 | 10 | | g0uZ |
| ✗ | PHP - Injection de commande | 10% | 38136 | 10 | | sambecks |
| ✗ | Fichier de sauvegarde | 1% | 35674 | 15 | | g0uZ |
| ✓ | HTTP - Directory indexing | 24% | 49462 | 15 | | g0uZ |

Инспектор

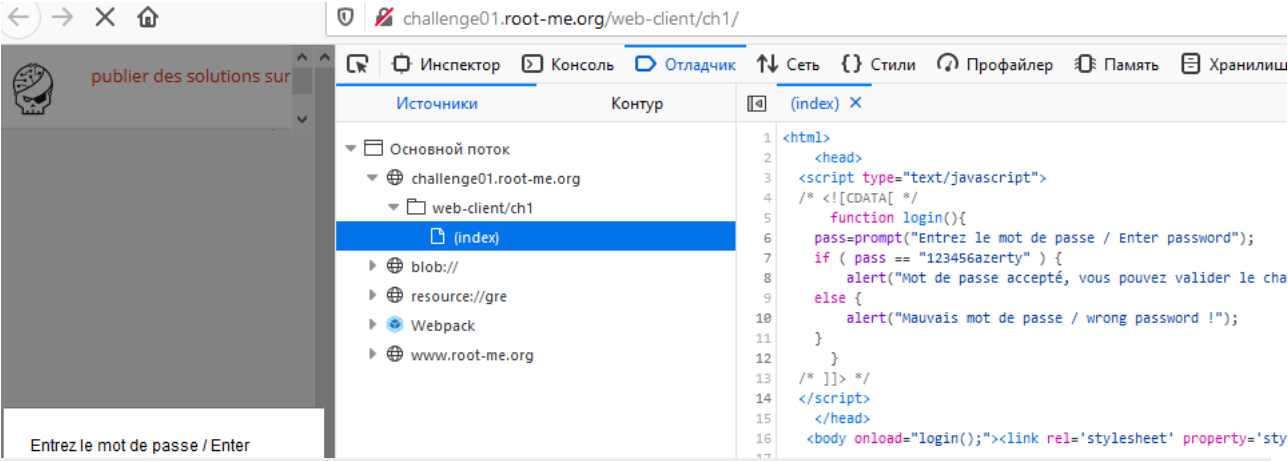
Поиск в HTML

```

<html>
<head>
<body>
  <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="https://www.root-me.org/?page=1" />
  <!-- Bienvenue sur ce portail, welcome on this portal, J'esp
  you will enjoy your time among us, and above that all y
  -->
  <h1>Login v0.00001</h1>
  <form>
    <input type="text" value="v" />
    <input type="password" value="Password" />
    <input type="button" value="login" />
  </form>
  <!-- Je crois que c'est vraiment trop simple là !
  It's really too easy !
  password : nZ^&@q5&sJjHev0
  -->
</body>
</html>

```

1*. Открываем дебаггер и видим строчку `pass == "тут искомый пароль"`



challenge01.root-me.org/web-client/ch1/

publier des solutions sur

Источники

- Основной поток
 - challenge01.root-me.org
 - web-client/ch1
 - (index)
 - blob://
 - resource://gre
 - Webpack
 - www.root-me.org

```

1 <html>
2 <head>
3 <script type="text/javascript">
4 /*  */
5 function login(){
6   pass=prompt("Entrez le mot de passe / Enter password");
7   if ( pass == "123456azerty" ) {
8     alert("Mot de passe accepté, vous pouvez valider le cha
9   else {
10    alert("Mauvais mot de passe / wrong password !");
11  }
12 }
13 /* ]]] */
14 &lt;/script&gt;
15 &lt;/head&gt;
16 &lt;body onload="login();"&gt;&lt;link rel='stylesheet' property='sty
17
</pre>
<p>Entrez le mot de passe / Enter</p>
<h2>24 Challenges</h2>
<p>Filter</p>
<table border="1">
<thead>
<tr>
<th>Results</th>
<th>Name</th>
<th>Validations</th>
<th>Number of points</th>
<th>Difficulty</th>
<th>Author</th>
<th>Note</th>
<th>Solution</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>✖</td>
<td>HTML - disabled buttons</td>
<td>38% 79801</td>
<td>5</td>
<td>📊</td>
<td>Final</td>
<td>👤</td>
<td>10</td>
<td>16 July 2017</td>
</tr>
<tr>
<td>✖</td>
<td>Javascript - Authentication</td>
<td>45% 95596</td>
<td>5</td>
<td>📊</td>
<td>g0uZ</td>
<td>👤</td>
<td>8</td>
<td>8 October 2006</td>
</tr>
<tr>
<td>✔</td>
<td>Javascript - Source</td>
<td>43% 91300</td>
<td>5</td>
<td>📊</td>
<td>g0uZ</td>
<td>👤</td>
<td>5</td>
<td>7 October 2006</td>
</tr>
</tbody>
</table>
</div>
<div data-bbox="90 521 896 572" data-label="Text">
<p>2*. Можно просканировать <a href="http://192.168.56.11/drupal">http://192.168.56.11/drupal</a> сканером nikto и обнаружить каталоги характерные для drupal 7. Папок includes и scripts нет в 8 версии. Скриншот не влез, на след странице.</p>
</div>
```

```
(kali@kali)-[~/192.168.56.11/mutillidae]
$ nikto -host http://192.168.56.11/drupal/
- Nikto v2.1.6
```

```
+ Target IP: 192.168.56.11
+ Target Hostname: 192.168.56.11
+ Target Port: 80
+ Start Time: 2021-04-06 08:51:55 (GMT-4)
```

```
+ Server: Apache/2.4.18 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /drupal/scripts/: Directory indexing found.
+ OSVDB-3268: /drupal/includes/: Directory indexing found.
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /drupal/misc/: Directory indexing found.
+ Entry '/misc/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /drupal/modules/: Directory indexing found.
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /drupal/profiles/: Directory indexing found.
+ Entry '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/scripts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /drupal/themes/: Directory indexing found.
+ Entry '/themes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
```