

Урок 3. Разведка

Задание 1:

Исследуйте комментарии в коде страницы

<http://192.168.56.11/mutillidae/index.php?page=home.php> на наличие в них полезной информации. Какие сведения можно обнаружить?

Решение:

Из полезной информации обнаружить только этот комментарий:

```
</table>
```

```
<!-- 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 -->
</blockquote>
</td>
</tr>
</table>
```

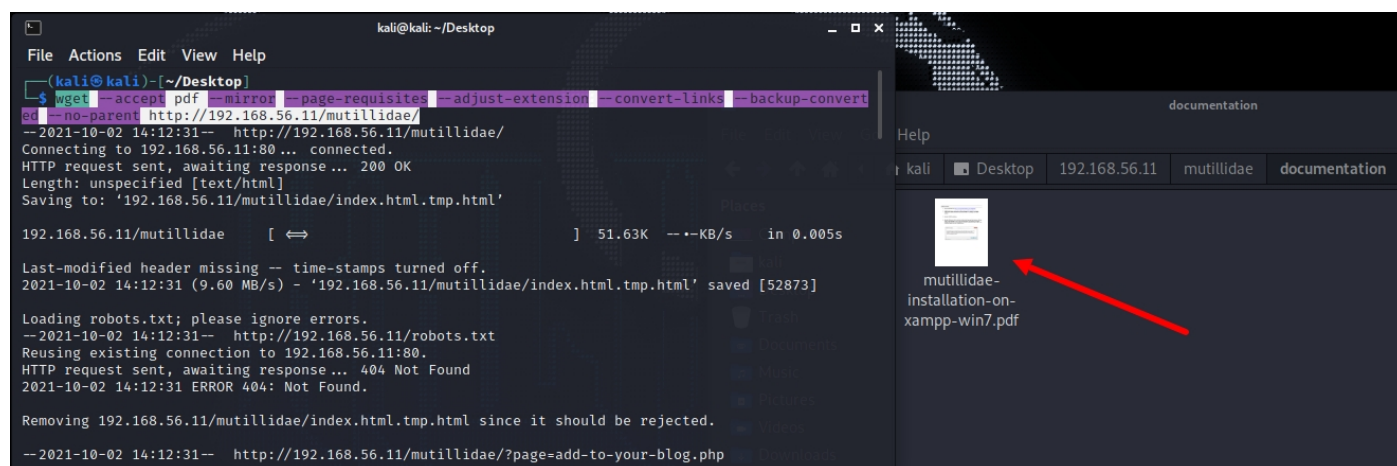
Задание 2:

Найдите в ВМ pdf-файл(ы) и укажите, при помощи какого средства, когда и кем был создан(ы) данный(е) объект(ы).

Решение:

Получить pdf файлы можно при помощи команды:

```
wget --access pdf --mirror --page-requisites --adjust-extension --convert-links --backup-converted --no-parent http://192.168.56.11/mutillidae/
```



Далее, чтобы узнать метаданные полученного pdf, можно воспользоваться утилитой *exiftool*:

```
kali@kali: ~/Desktop/192.168.56.11/mutillidae/documentation
File Actions Edit View Help

(kali@kali)~[~/Desktop/192.168.56.11/mutillidae/documentation]
$ exiftool mutillidae-installation-on-xampp-win7.pdf
ExifTool Version Number      : 12.30
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       : 2021:10:02 14:12:39+04:00
File Inode Change Date/Time  : 2021:10:02 14:12:31+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

(kali@kali)~[~/Desktop/192.168.56.11/mutillidae/documentation]
```

Задание 3:

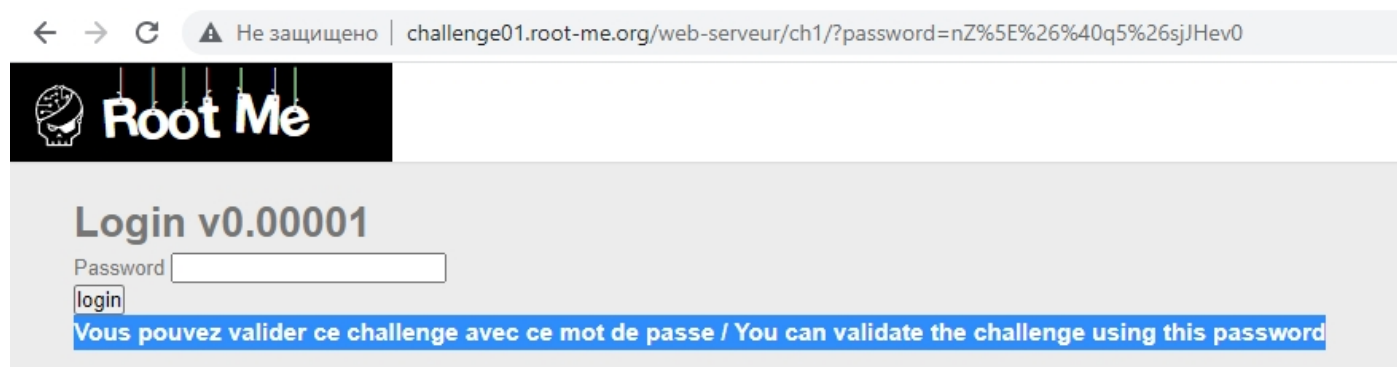
Решите задание <https://www.root-me.org/en/Challenges/Web-Server/HTML>. Надо подобрать пароль — укажите его в ответе.

Решение:

Проанализировав исходный код страницы я нашёл комментарий со следующим содержимым:

```
Je crois que c'est vraiment trop simple là !
It's really too easy !
password : nZ^&@q5&sjJHev0
```

А дальше решение не заставило себя долго ждать



Пароль: nZ^&@q5&sjJHev0

Задание 4:

* Решите задание <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source>.
Надо подобрать пароль — укажите его в ответе.

Решение:

Проанализировав код страницы в панели разработчика я нашёл интересный участок js кода:

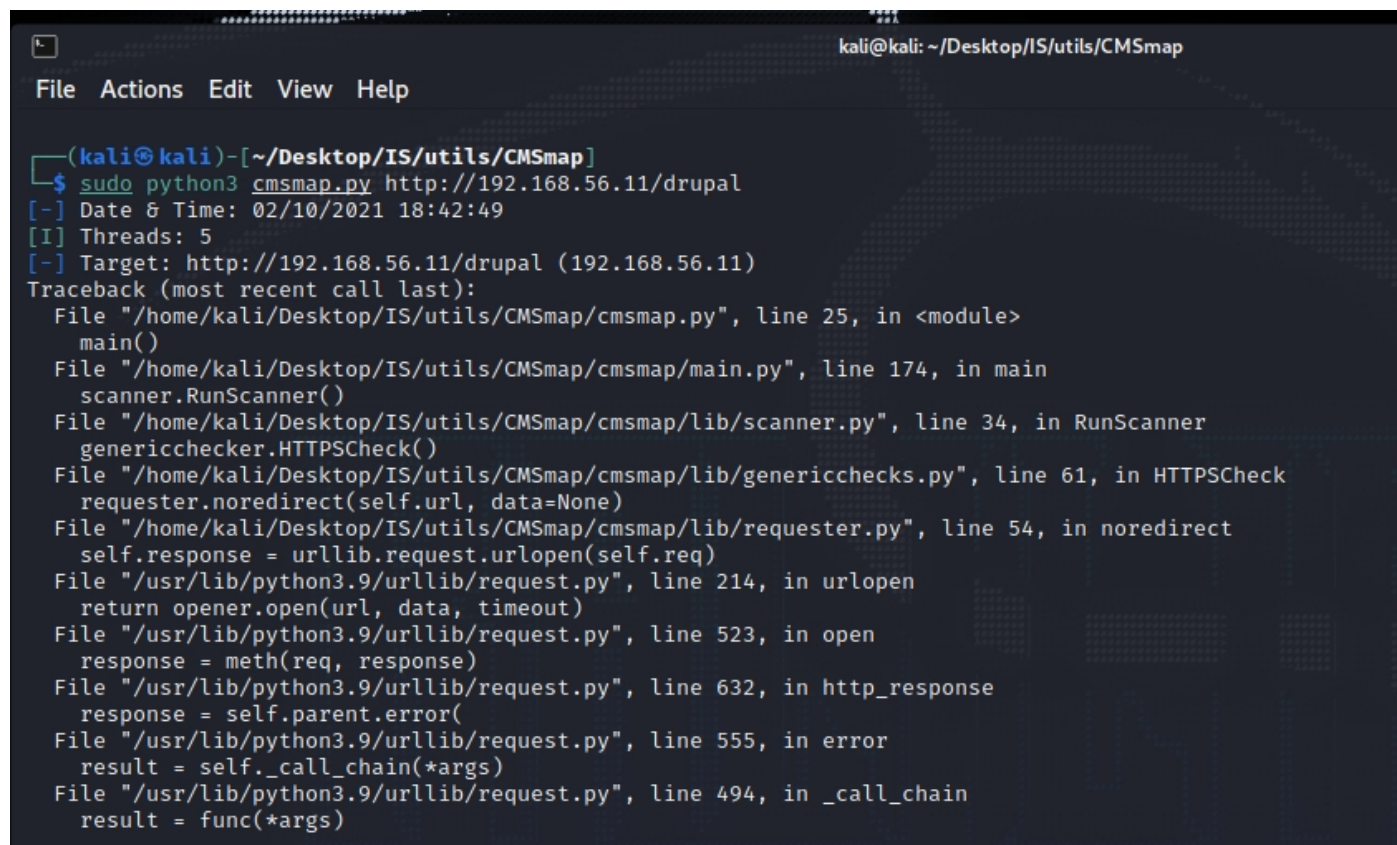
```
<html>
<head>
  <script type="text/javascript">
    ...
    /*  */
    function login(){
      pass=prompt("Entrez le mot de passe / Enter password");
      if ( pass == "123456azerty" ) {
        alert("Mot de passe accepté, vous pouvez valider le challenge avec ce mot de passe.\nYou can validate the challenge
using this password."); }
      else {
        alert("Mauvais mot de passe / wrong password !");
      }
    }
  /* ]]&gt; */
  == $0
&lt;/script&gt;
&lt;/head&gt;
&lt;body onload="login();"&gt;
  &lt;link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/template/s.css" media="all"&gt;
  &lt;iframe id="iframe" src="https://www.root-me.org/?page=externe_header"&gt;...&lt;/iframe&gt;
&lt;/body&gt;
&lt;/html&gt;</pre></div><div data-bbox="45 634 715 652" data-label="Text"><p>После перезагрузки страницы, введя данный пароль я получил алерт:</p></div><div data-bbox="223 679 750 758" data-label="Text"><p>Подтвердите действие на странице challenge01.root-me.org<br/>Mot de passe accepté, vous pouvez valider le challenge avec ce mot de<br/>passe.<br/>You can validate the challenge using this password.</p></div><div data-bbox="693 779 724 793" data-label="Text"><p>OK</p></div>
```

Задание 5:

* В ВМ установлен сайт на drupal. Может ли злоумышленник подобрать для него рабочий эксплоит? Ответ обоснуйте.

Решение:

Может, при условии, если уточнит версию CMS. Уточнить её можно несколькими способами: утилитой CMSmap



```
kali@kali: ~/Desktop/IS/utis/CMSmap
File Actions Edit View Help

(kali@kali)~[~/Desktop/IS/utis/CMSmap]
$ sudo python3 cmsmap.py http://192.168.56.11/drupal
[-] Date & Time: 02/10/2021 18:42:49
[I] Threads: 5
[-] Target: http://192.168.56.11/drupal (192.168.56.11)
Traceback (most recent call last):
  File "/home/kali/Desktop/IS/utis/CMSmap/cmsmap.py", line 25, in <module>
    main()
  File "/home/kali/Desktop/IS/utis/CMSmap/cmsmap/main.py", line 174, in main
    scanner.RunScanner()
  File "/home/kali/Desktop/IS/utis/CMSmap/cmsmap/lib/scanner.py", line 34, in RunScanner
    genericchecker.HTTPSCheck()
  File "/home/kali/Desktop/IS/utis/CMSmap/cmsmap/lib/genericchecks.py", line 61, in HTTPSCheck
    requester.noredirect(self.url, data=None)
  File "/home/kali/Desktop/IS/utis/CMSmap/cmsmap/lib/requester.py", line 54, in noredirect
    self.response = urllib.request.urlopen(self.req)
  File "/usr/lib/python3.9/urllib/request.py", line 214, in urlopen
    return opener.open(url, data, timeout)
  File "/usr/lib/python3.9/urllib/request.py", line 523, in open
    response = meth(req, response)
  File "/usr/lib/python3.9/urllib/request.py", line 632, in http_response
    response = self.parent.error(
  File "/usr/lib/python3.9/urllib/request.py", line 555, in error
    result = self._call_chain(*args)
  File "/usr/lib/python3.9/urllib/request.py", line 494, in _call_chain
    result = func(*args)
```

(Не захотела она у меня работать... Пробовал версию python менять — не помогло. Попробовал другой сайт проанализировать — всё ок.)

Либо можно найти в файле robots.txt строку с интересной директорией (файлом) — CHANGELOG.txt, в котором имеются записи с нужной нам информацией.

Узнав версию друпала, для поиска эксплоита можно воспользоваться утилитой *exploitdb* и её командой *searchsploit*, которая выведен нам список потенциальных эксплоитов:

```
kali@kali: ~/Desktop/IS/utis/CMSmap
File Actions Edit View Help

(kali@kali)-[~/Desktop/IS/utis/CMSmap]
$ searchsploit drupal 7.5
```

Exploit Title	Path
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)	php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)	php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)	php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)	php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)	php/webapps/35150.php
Drupal < 7.34 - Denial of Service	php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)	php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution	php/webapps/46459.py

```
Shellcodes: No Results

(kali@kali)-[~/Desktop/IS/utis/CMSmap]
$
```