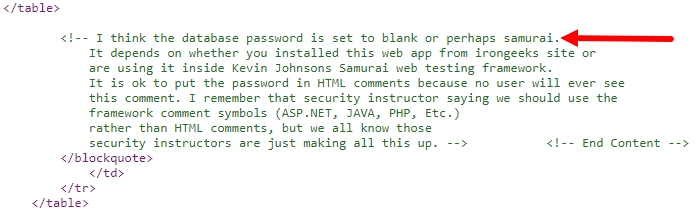
### **Урок 3. Разведка**

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:

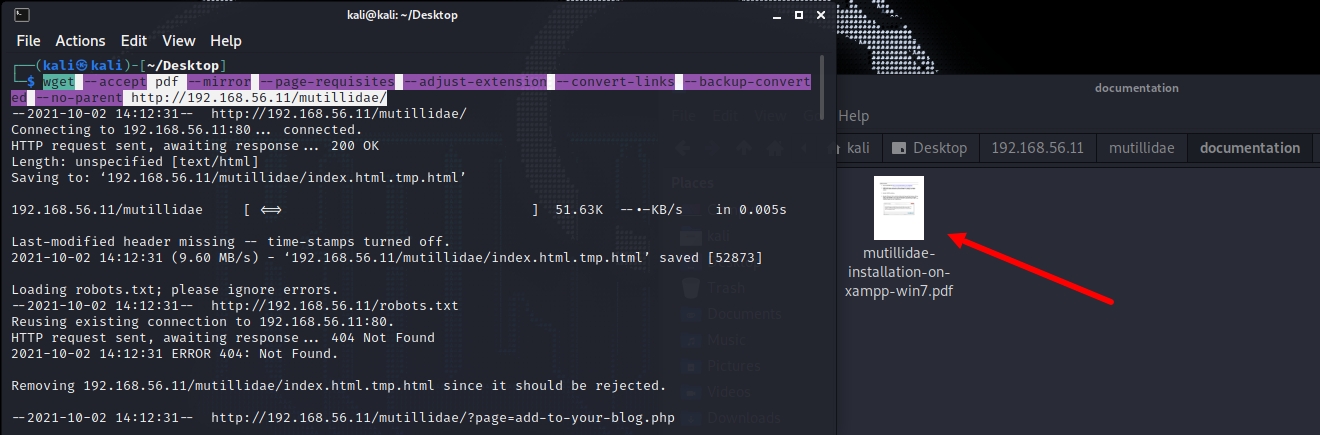
 Из полезной информации обнаружить только этот комментарий:

Задание 2:  
 Найдите в ВМ pdf-файл(ы) и укажите, при помощи какого средства, когда и кем был создан(ы) данный(е) объект(ы).

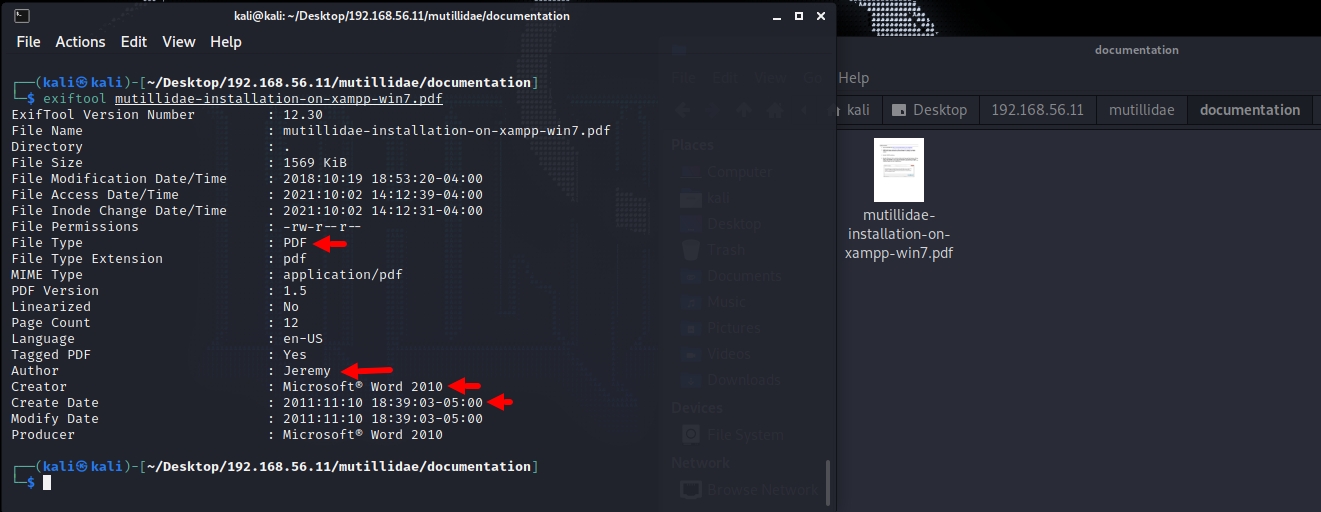
Решение:

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/*

**

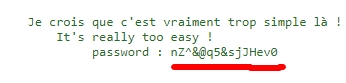
Далее, чтобы узнать метаданные полученого pdf, можно воспользоваться утилитой *exiftool*:



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:



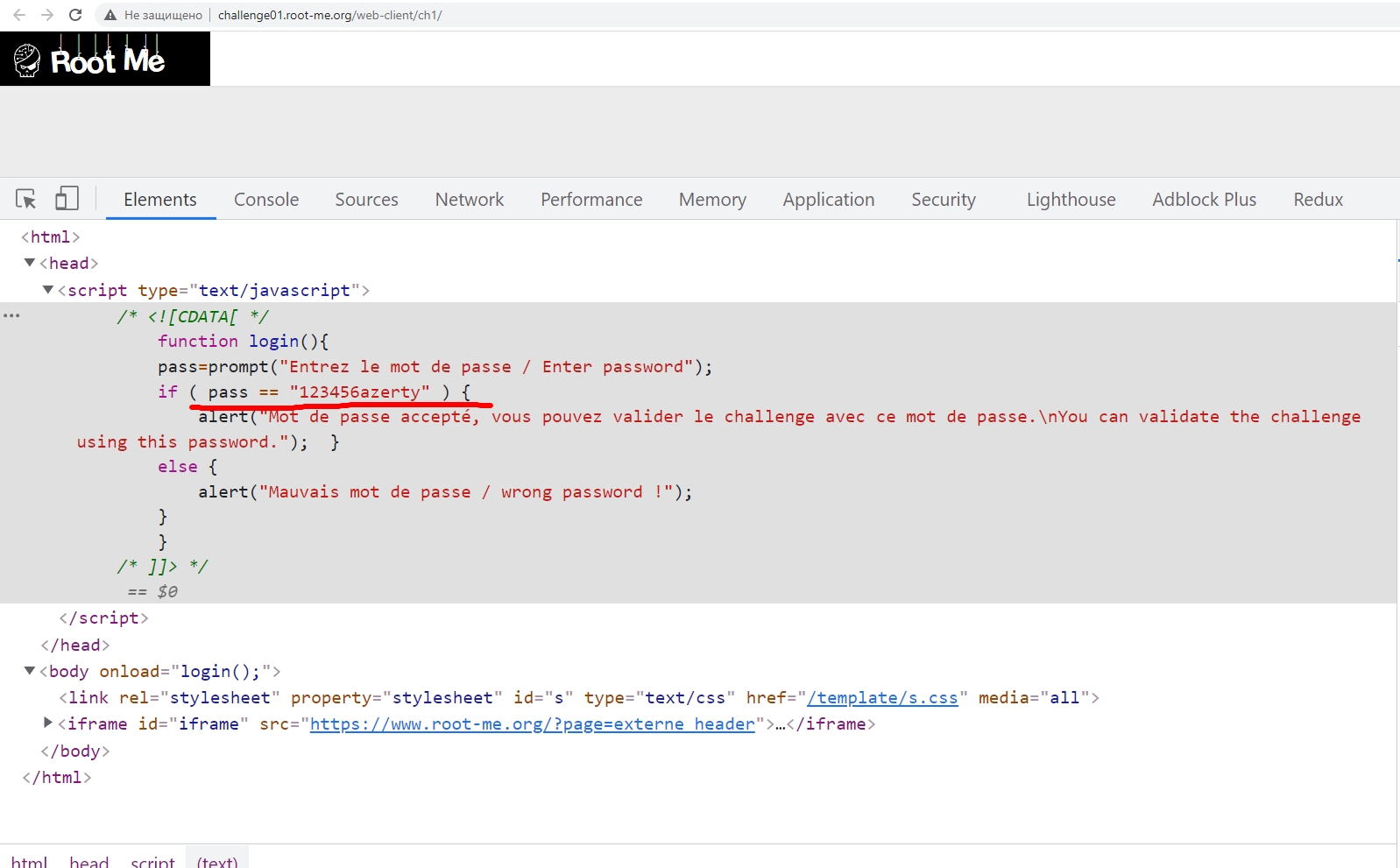
А дальше решение не заставило себя долго ждать

Пароль: nZ^&@q5&sjJHev0

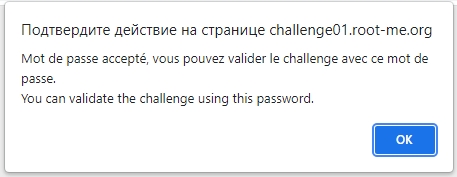
Задание 4:  
 \* Решите задание *https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source*. Надо подобрать пароль — укажите его в ответе.

Решение:

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



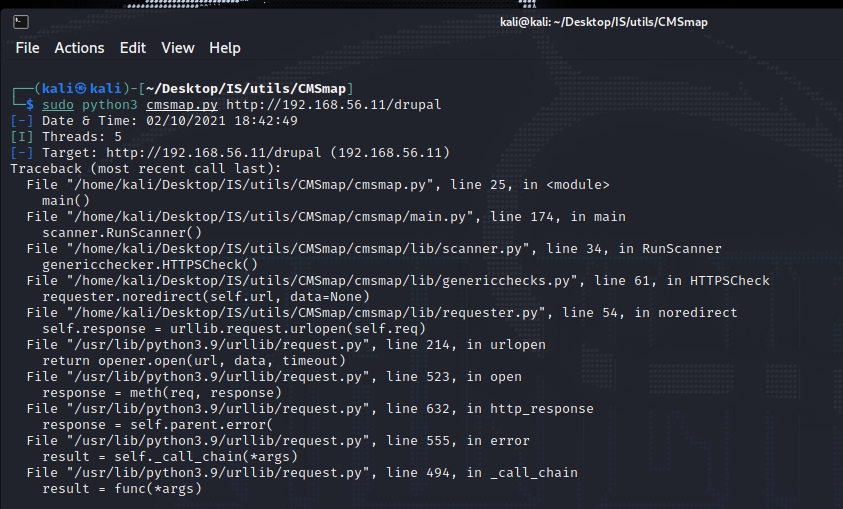
После перезагрузки страницы, введя данный пароль я получил алерт:



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

(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*:*

