19.07.2023

Курс:

Практическая работа к уроку № Lesson_4

--

Задание_1:

Найдите в ВМ **Metasploitable 3** (Linux) адрес страницы **Login Page** проекта **Continuum** (предварительно отключите межсетевой экран командой iptables -F, затем перезапустите continuum командой service continuum restart), который запущен на одном из кастомных портов. В ответе укажите адрес страницы.

- Поиск в ВМ **Metasploitable 3**

```
vagrant@ubuntu:~$ sudo find / -type f -iname continuum
/opt/apache_continuum/apache-continuum-1.4.2/bin/continuum
```

- `/opt/apache_continuum/apache-continuum-1.4.2/bin/continuum`
- `service apache2 start`
- `service (apache2-)continuum restart ???`

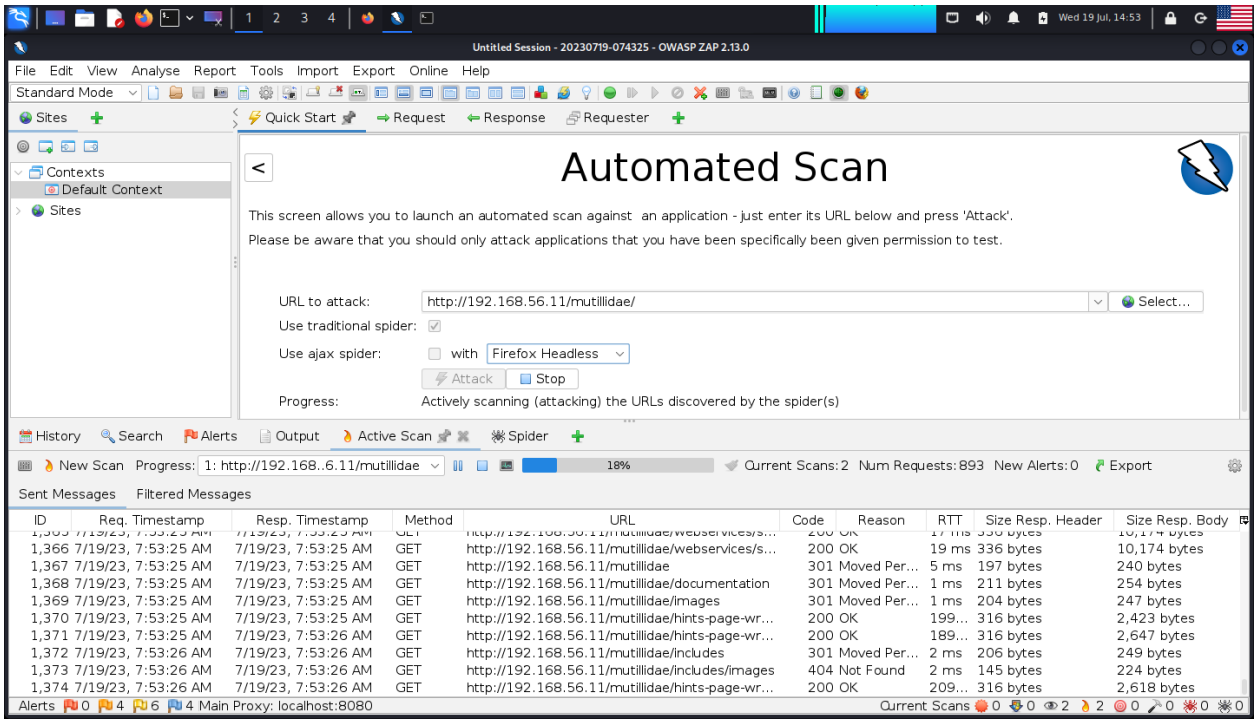
Поиск сервисов по открытым портам

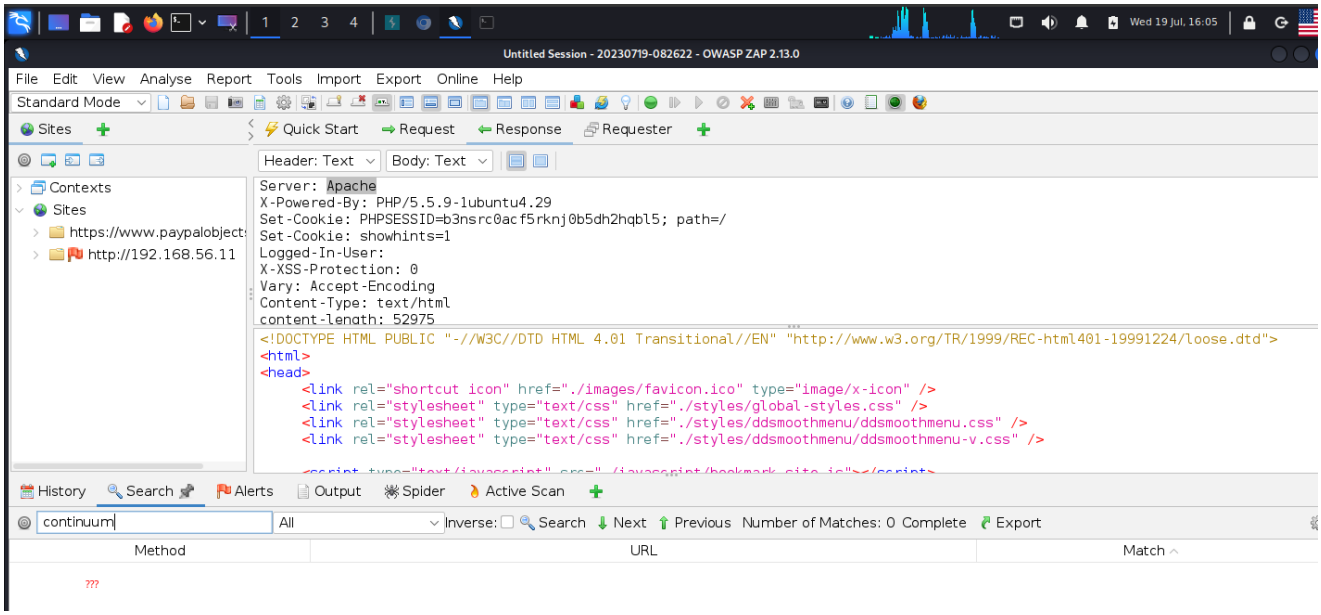
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 04:54 EDT
Nmap scan report for 192.168.56.11
Host is up (0.0015s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8181/tcp open   intermapper
Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

- Отключаем межсетевой экран командой `iptables -F`

```
┌──(kali㉿kali)-[~]
└─$ wget -S --spider http://192.168.56.11/zabbix
Spider mode enabled. Check if remote file exists.
--2023-07-19 07:39:38--  http://192.168.56.11/zabbix
Connecting to 192.168.56.11:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 404 Not Found
  Date: Wed, 19 Jul 2023 11:36:04 GMT
  Server: Apache
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1
Remote file does not exist -- broken link!!!
```

- ZAP





Задание_2:

Какой сервис запущен на порту 6697 в ВМ **Metasploitable 3** (Linux)?

Сервис ircs-u
A trojan that opens a back door on the compromised computer by connecting to the IRC server irc.anonops.li on port _6697

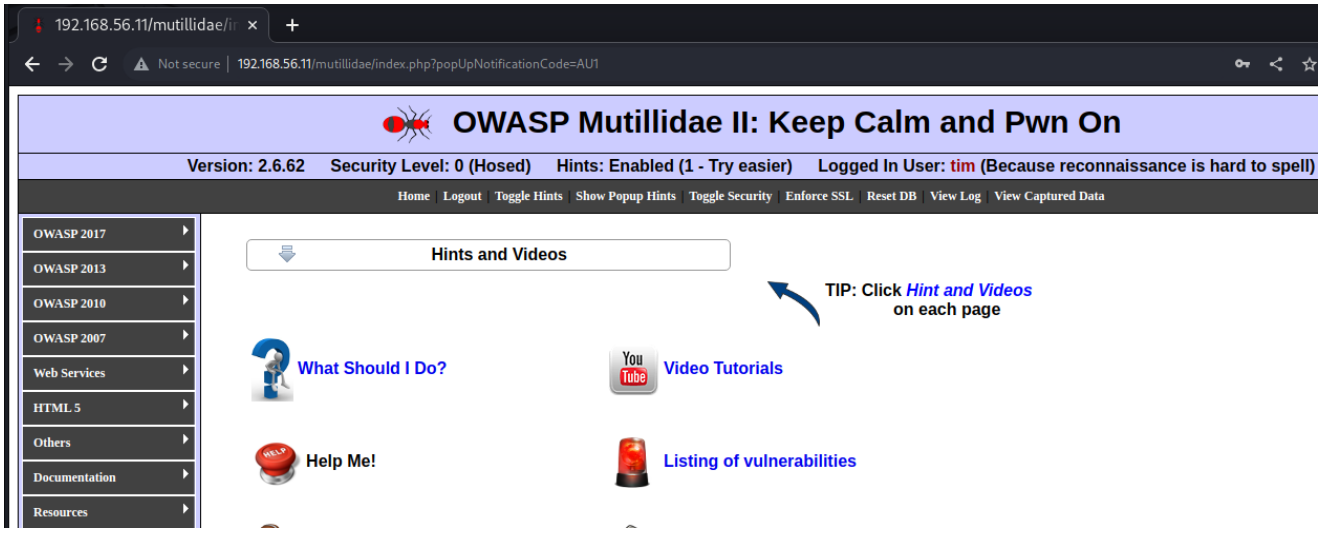
- nmap -p-

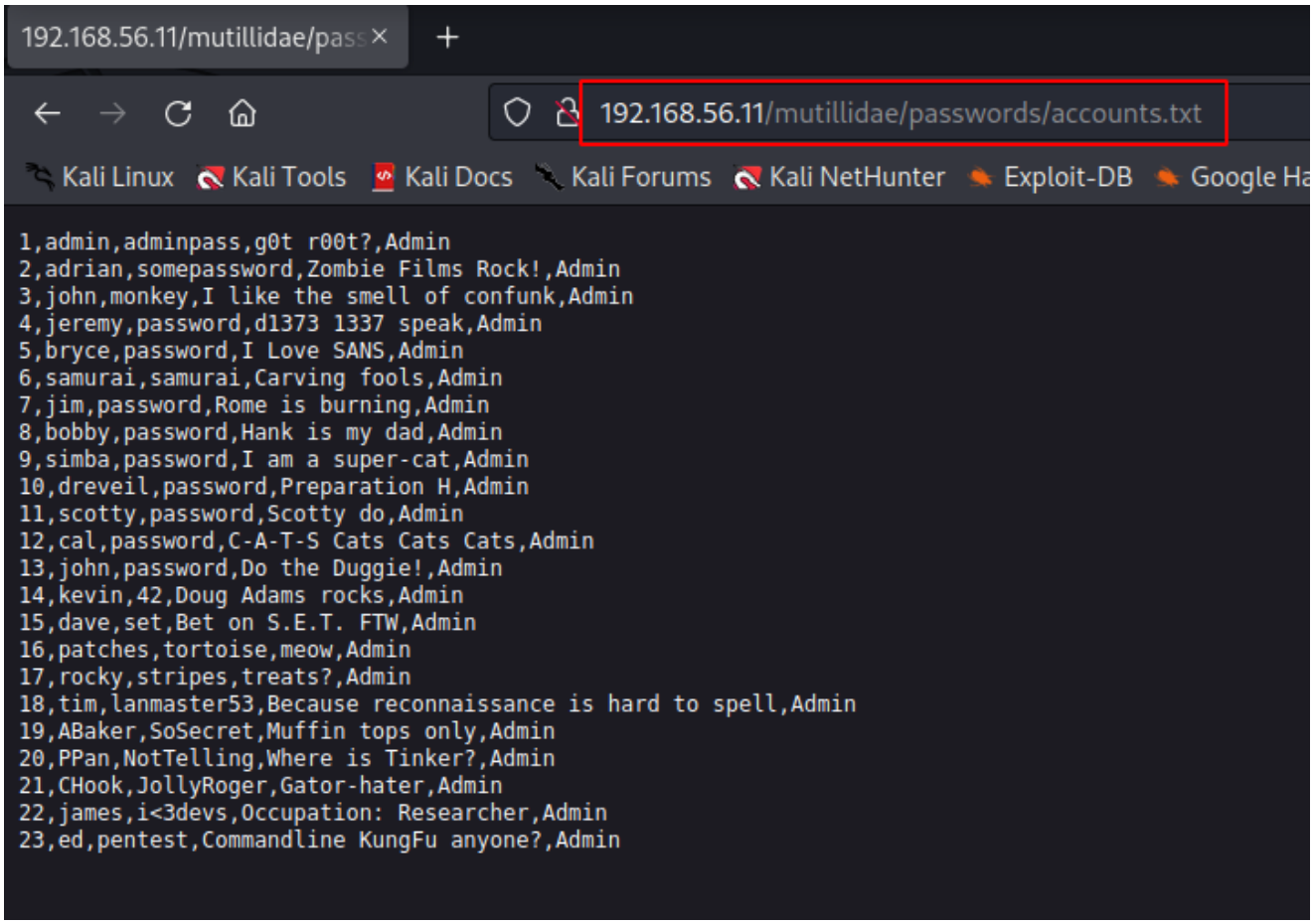
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.56.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 08:34 EDT
Nmap scan report for 192.168.56.11
Host is up (0.0027s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
6666/tcp  open  irc
6667/tcp  open  irc
6697/tcp  open  ircs-u
8067/tcp  open  infi-async
8181/tcp  open  intermapper
35741/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 5.35 seconds
```

Задание_3:

Какой пароль пользователя **tim** из проекта **mutillidae**? В каком файле он содержится?

user: tim
password: lanmaster53





Задание_4:

(*) В каком файле можно найти информацию о том, какой любимый фильм у юзера с именем **selene** (не является УЗ в bwapp)?

Zombie Films ???

```
locate film

find . -type f -exec file -N -i -- {} + | sed -n 's!: video/[^:]*$!!p

locate *.mkv *.webm *.flv *.vob *.ogg *.ogv *.drc *gifv *.mng *.avi *.mov
*.qt *.wmv *.yuv *.rm *.rmvb *.asf *.amv *.mp4 *.m4v *.mp *.m?v *.svi
*.3gp *.flv *.f4v

cat /var/log/apache2/access.log | grep -i "selene"   ???
```

Задание_5:

(*) Составьте правило (или набор правил) для mod_rewrite, при помощи которого можно заблокировать доступ утилиты **curl** на веб сервер ВМ.

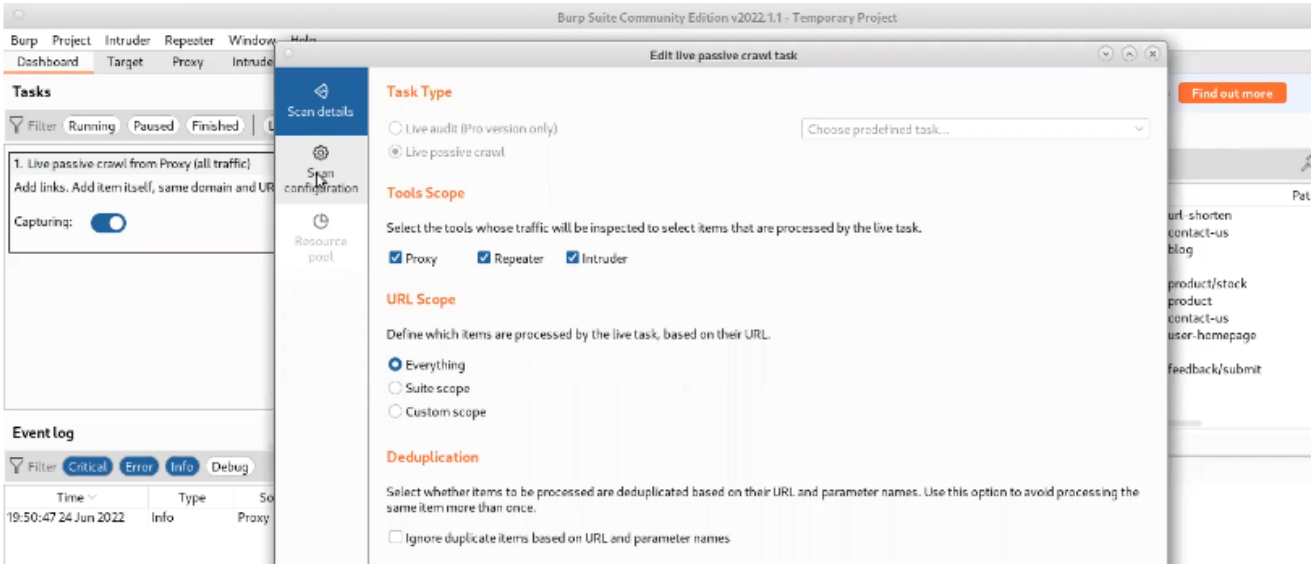
Блокировать подозрительные пользовательские запросы и агенты

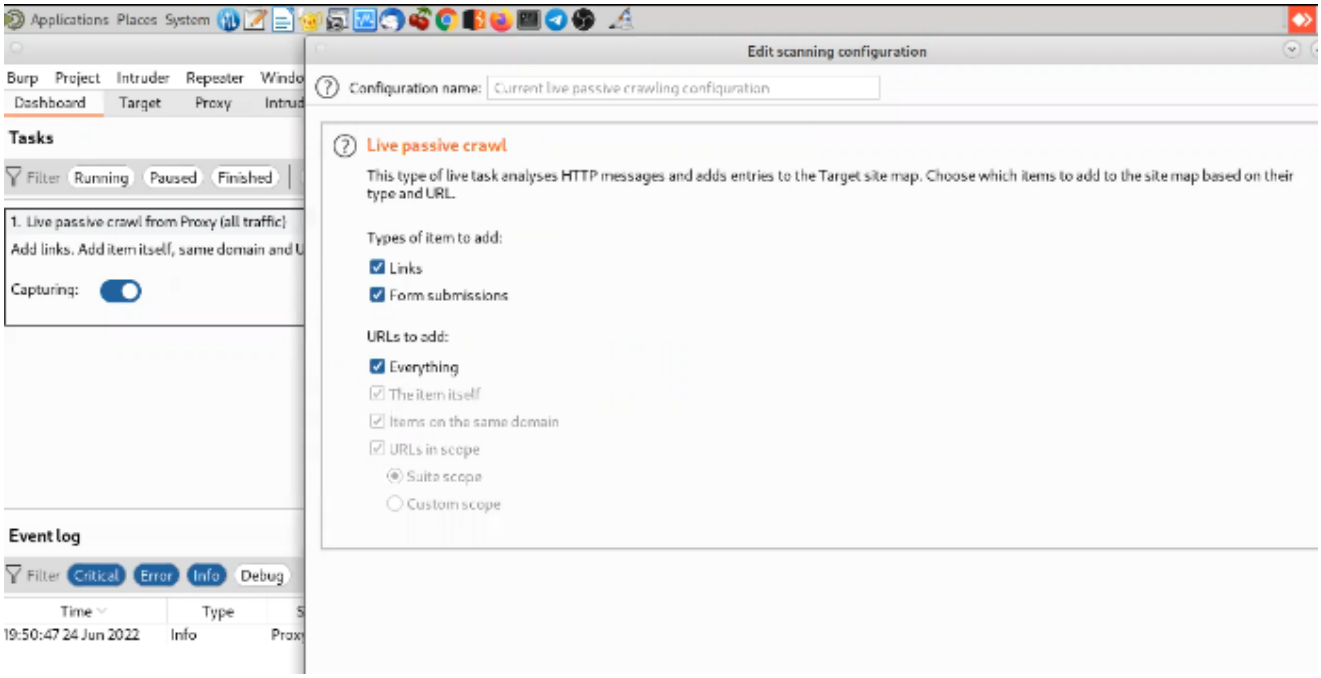
```
RewriteCond %{HTTP_USER_AGENT} (libwww-
perl|wget|python|nikto|curl|scan|java|winhttp|clshttp|loader) [NC,OR]
```

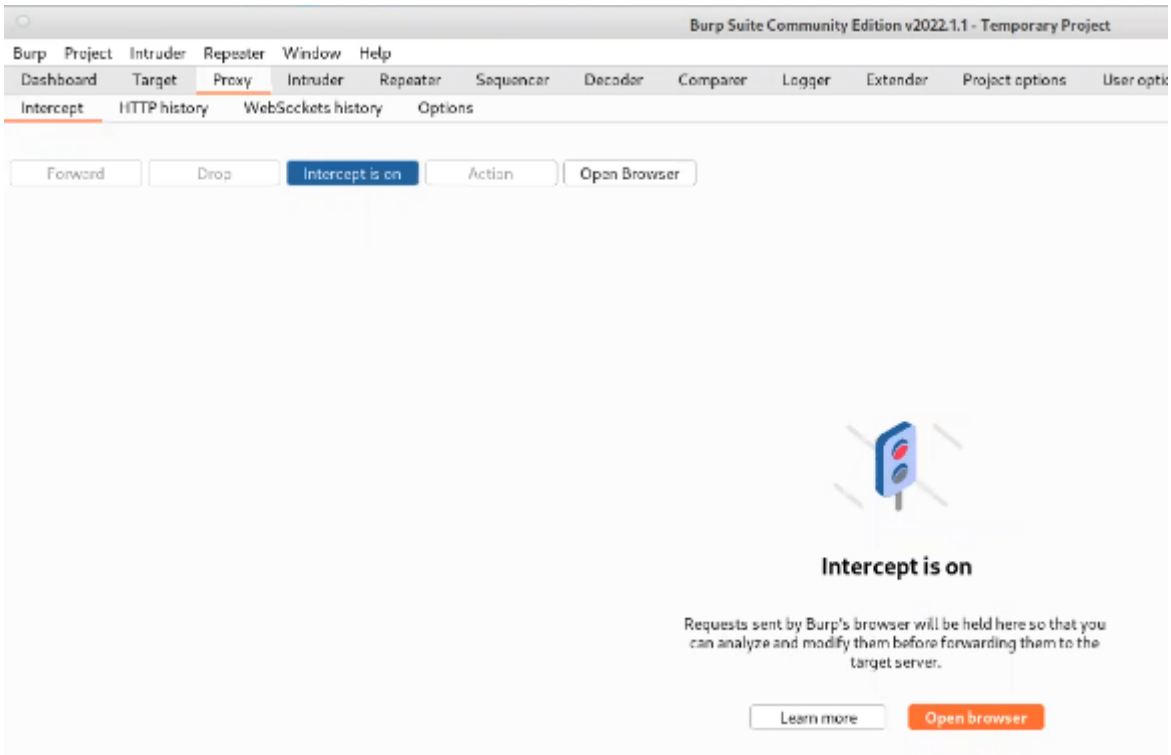
Заметки

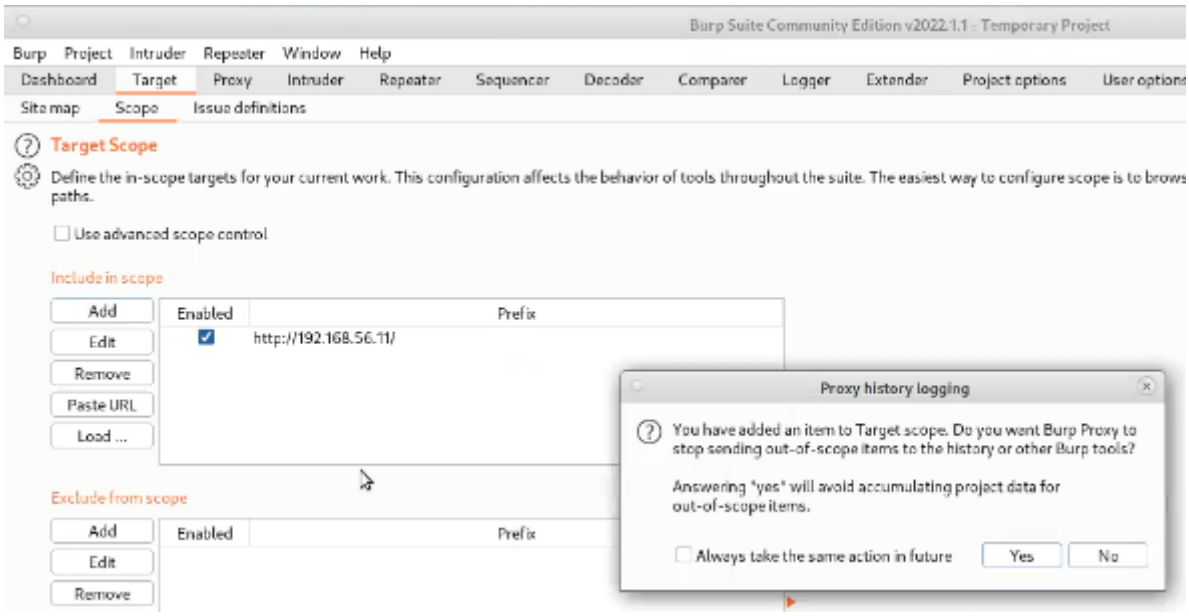
- **Файл .htaccess** — конфигурационный файл веб-сервера Apache, позволяющий переопределять глобальные настройки сайта для конкретного каталога.
- **User-agent** — поле http-запроса, в котором клиентское приложение обычно пересылает веб-серверу информацию о себе в виде текстовой строки, например версию браузера, спайдера, версию и тип прокси, имя бота поисковой системы.

из Урока:

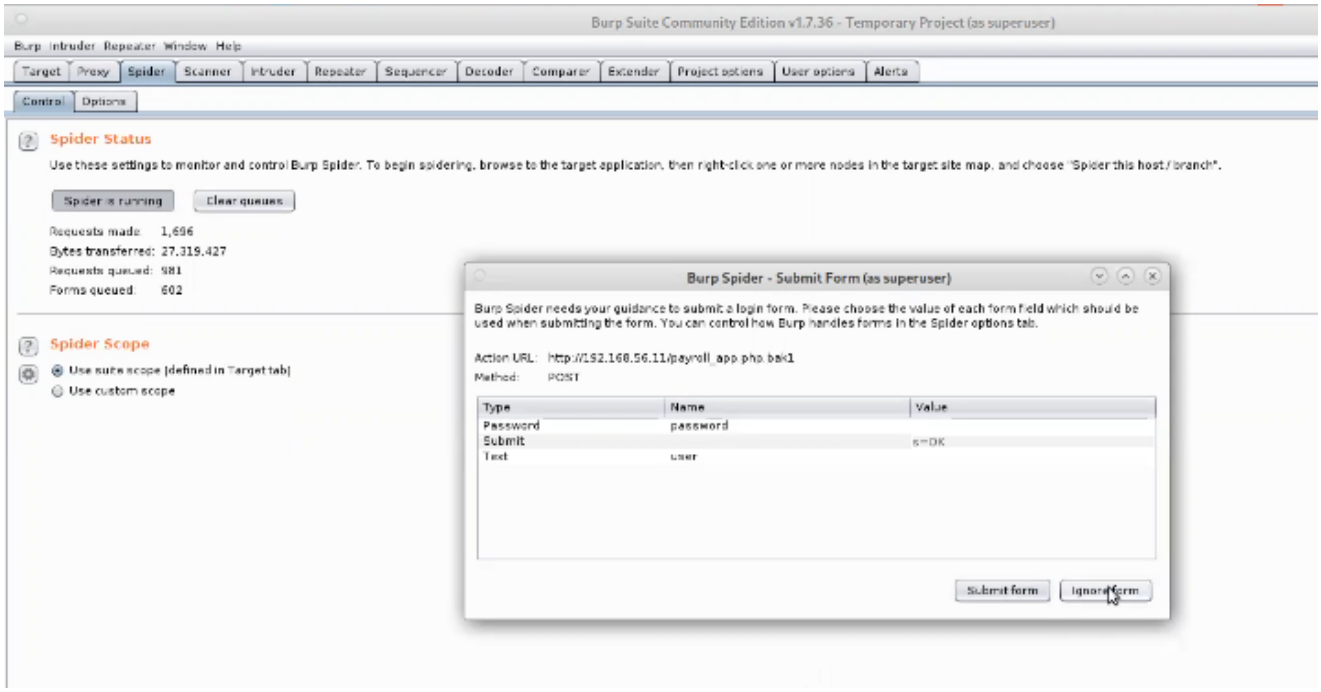

Burp Suite Community Edition v2022.1.1 - Temporary Project
Edit live passive crawl task
Scan details
Scan configuration
Resource pool
Task Type
Live audit (Pro version only)
Live passive crawl
Choose predefined task...
Tools Scope
Select the tools whose traffic will be inspected to select items that are processed by the live task.
Proxy
Repeater
Intruder
URL Scope
Define which items are processed by the live task, based on their URL.
Everything
Suite scope
Custom scope
Deduplication
Select whether items to be processed are deduplicated based on their URL and parameter names. Use this option to avoid processing the same item more than once.
Ignore duplicate items based on URL and parameter names
Tasks
Filter
Running
Paused
Finished
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URL
Capturing:
Event log
Filter
Critical
Error
Info
Debug
Time
Type
19:50:47 24 Jun 2022
Info
Proxy
Find out more


Applications Places System
Edit scanning configuration
Configuration name:
Current live passive crawling configuration
Live passive crawl
This type of live task analyses HTTP messages and adds entries to the Target site map. Choose which items to add to the site map based on their type and URL.
Types of item to add:
Links
Form submissions
URLs to add:
Everything
The item itself
Items on the same domain
URLs in scope
Suite scope
Custom scope
Tasks
Filter
Running
Paused
Finished
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and U
Capturing:
Event log
Filter
Critical
Error
Info
Debug
Time
Type
19:50:47 24 Jun 2022
Info


Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is on
Action
Open Browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser



- Burp Suite v1.7.36



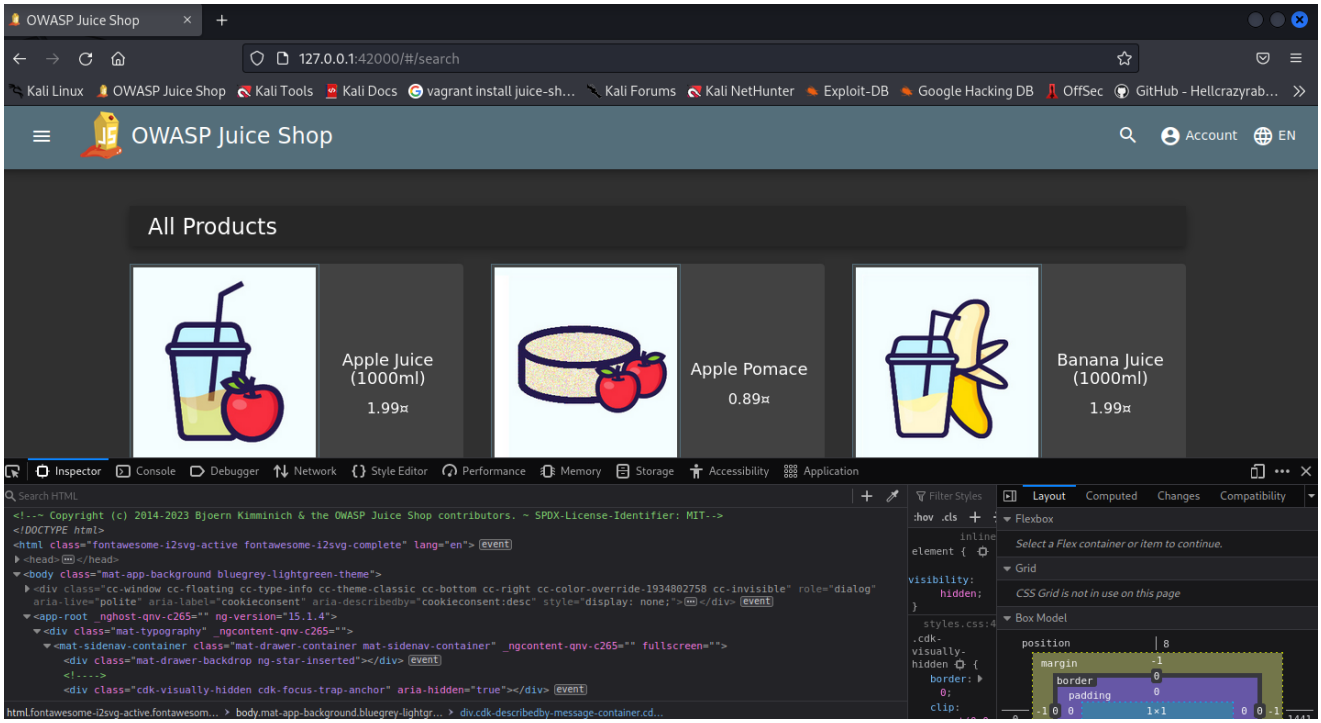

```
wget https://portswigger.net/burp/releases/professional-community-1-7-36
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo sh burpsuite_community_linux_v1_7_36.sh
Unpacking JRE ...
Starting Installer ...

┌──(kali㉿kali)-[~]
└─$ sudo juice-shop -h
[*] Please wait for the Juice-shop service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:42000
```

```
● juice-shop.service - juice-shop web application
     Loaded: loaded (/lib/systemd/system/juice-shop.service; disabled;
preset: disabled)
     Active: active (running) since Wed 2023-07-19 06:30:01 EDT; 5s ago
   Main PID: 11559 (npm start)
      Tasks: 23 (limit: 2262)
     Memory: 182.5M
        CPU: 4.907s
     CGroup: /system.slice/juice-shop.service
             ├─11559 "npm start"
             ├─11589 sh -c "node build/app"
             └─11590 node build/app

Jul 19 06:30:01 kali systemd[1]: Started juice-shop.service - juice-shop
web application.
Jul 19 06:30:02 kali npm[11559]: > juice-shop@14.5.1 start
Jul 19 06:30:02 kali npm[11559]: > node build/app
Jul 19 06:30:03 kali npm[11590]: info: All dependencies in ./package.json
are satisfied (OK)

[*] Opening Web UI (http://127.0.0.1:42000) in: 5... 4... 3... 2... 1...
```




```
--OWASP Juice Shop (Kali)
sudo apt install juice-shop
juice-shop -h
juice-shop-stop -h
+npm install
+npm start
+nodejs install
Alternative:
```

```
1. Install a 64bit [Node.js](http://nodejs.org/) on your Windows, MacOS or Linux machine.
2. Download `juice-shop-<version>_<node-version>_<os>_x64.zip` (or `.tgz`) attached to the [latest release on GitHub](https://github.com/juice-shop/juice-shop/releases/latest).
3. Unpack the archive and run `npm start` in unpacked folder to launch the application
4. Browse to [http://localhost:3000](http://localhost:3000)
--Uninstall
sudo apt purge --autoremove juice-shop
sudo apt purge --autoremove nodejs npm
which node
which npm
sudo rm -rf /usr/bin/node /usr/bin/npm
--

ls -a
ls -al

┌──(kali㉿kali)-[~]
└─$ cat /var/log/apache2/access.log
tail -f /var/log/apache2/access.log

nikto -h http://192.168.56.11/xvwa

dirb --help

ls (192.168.56.11...dirsearch.py)
python3 dirsearch.py

namp -p- 192.168.56.11

nc 192.168.56.11 21

┌──(kali㉿kali)-[~]
└─$ python3 dirsearch/dirsearch.py -u 'http://192.168.56.11/mutillidae' -e php,txt,html -w /usr/share/dirb/wordlists/big.txt -x 503,403 --random-agent

wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 400,404,403 http://192.168.56.11/multillidae/FUZZ

--
```

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -m conntrack --ctstate ESTABLISHES,RELATED -j ACCEPT
iptables -m conntrack --ctstate INVALID -j LOG --log-level 7 --log-prefix
'[FW INPUT]:'
iptables -m conntrack --ctstate INVALID -j DROP
iptables -P INPUT DROP
```

Выполнил: AndreiM