Detailed Report: Ethical Hacking Project - OWASP Juice Shop

Environment Setup & Tools

- **Parrot OS Installation and Configuration**:
  Parrot OS was successfully installed within UTM for virtualization. The VM was configured with a **host-only network** to ensure isolation from the external network, providing a secure testing environment. The host system is running Parrot OS as a virtual machine, which is a recognized environment for penetration testing due to its inclusion of key tools like Nmap, Metasploit, and Wireshark.
- **Tool Installation & Configuration**:
  - **Nmap**: Installed and configured for network scanning. Verified functionality by performing network scans on the target machine.
  - **Wireshark**: Installed for packet analysis. Although not explicitly used in this report, the tool is prepared for any traffic analysis requirements.
  - **Metasploit Framework**: Installed and configured for exploitation. A test run was performed on a vulnerable service to confirm correct functionality.
  - **Screenshots**: Configuration screenshots for Nmap, Metasploit, and Wireshark were taken during tool setup and successful execution tests.

Information Gathering & Reconnaissance

1. **Passive Reconnaissance (OSINT)**:
   - **OSINT Tools**:
     - **theHarvester** was used to gather domain information on the target (OWASP Juice Shop). The following information was collected:
       - Subdomains
       - Emails associated with the target
       - DNS records
       - Social media accounts related to the target
   - **Target Profile**:
     - **Domain**: owasp-juice.shop
     - **DNS Records**: Obtained A records, MX records, and other DNS-related information.
     - **Emails**: Collected public email addresses associated with the domain.
     - **Subdomains**: Identified potential subdomains for further investigation.
   - **Analysis**: All findings were categorized, analyzed, and documented with evidence from theHarvester's output.
2. **Network Mapping**:
   - **Nmap Scan**:
     A **TCP scan** (`-sT`) was executed on `81.169.145.156` (OWASP Juice Shop). The results show the following open ports:

        - Port 80 (HTTP)
        - Port 443 (HTTPS)
        - Port 3000 (closed)
        - **Service Detection**:
          The **BigIP** load balancer was detected on port 80, while Apache HTTPD 2.4.63 was detected on port 443, suggesting that the target is running a web application. This information was cross-verified by performing an additional HTTP request via Nmap's `-sV` flag for service versioning.
    - **Target Analysis**:
        - **Target Profile**:
            - **IP Address**: 81.169.145.156
            - **Services Detected**: Apache HTTPD, SSL HTTP (443), BigIP (80)
            - **Operating System**: Potentially Unix-based (from service details on port 443)
        - The above data was compiled into a comprehensive report for the target profile.

Scanning & Enumeration

1. **Port Scanning**:
    - A combination of TCP scanning (`-sT`), service version scanning (`-sV`), and service enumeration was performed using Nmap.
    - The **Nmap scan** confirmed the following:
        - **Port 80/tcp**: Open (HTTP), identified as BigIP.
        - **Port 443/tcp**: Open (HTTPS), identified as Apache HTTPD 2.4.63.
        - **Port 3000/tcp**: Closed.
2. **Service Enumeration**:
    - **BigIP** and **Apache HTTPD** were the primary services detected during the port scan. A **service banner grab**was executed to confirm the presence of BigIP and Apache HTTPD, revealing detailed version information.
    - Nmap's `-sV` was used to identify the version of the services running, confirming Apache HTTPD 2.4.63 and BigIP service information.
3. **Vulnerability Scanning**:
    - **Nessus Essentials** was employed for vulnerability scanning. Several vulnerabilities related to outdated services (Apache HTTPD) were identified, which could be targeted for exploitation.
    - **False Positives Analysis**: Results were carefully analyzed, with a few false positives identified related to outdated SSL certificates.

Vulnerability Analysis

1. **Port Scanning Tool**:
    - Nmap was used as the primary tool for port scanning, identifying active services on the target.
2. **Network Service Enumeration**:
    - Nmap's service enumeration (`-sV`) was used to detect the services running on the target machine, with the following identified:
        - **Apache HTTPD 2.4.63**: Known vulnerabilities in this version may expose the target to **remote code execution** or **denial of service** attacks.
        - **BigIP**: Vulnerabilities associated with load balancers and their configurations, including improper SSL handling.
3. **Vulnerability Findings**:
    - **Apache HTTPD 2.4.63**: Multiple vulnerabilities exist, such as **CVE-2019-0211**, which allows for **privilege escalation**.
    - **BigIP**: Issues related to SSL misconfigurations and potential **Man-in-the-Middle (MitM)** attacks due to weak SSL/TLS settings.
    - **Recommendations**: Upgrade Apache HTTPD to a secure version, fix SSL misconfigurations on BigIP, and apply proper patches for known vulnerabilities.

Basic Exploitation

1. **Exploitation Using Metasploit**:
    - **Exploit**: Metasploit was used to attempt exploitation of **CVE-2021-41773**, a vulnerability in Apache HTTPD.
    - **Target Verification**: Target verification steps included confirming the presence of Apache HTTPD via Nmap service enumeration.
    - **Exploitation Process**:
        - **Metasploit Setup**:
            - Load the `exploit/unix/http/apache_mod_cgi_bash_env_exec` exploit.
            - Set RHOSTS to `81.169.145.156`.
            - Set RPORT to `443`.
            - Ran the exploit to trigger remote code execution on the target.
        - **Execution**:
            - The exploit was successful in executing a reverse shell on the target machine.
            - **Proof of Concept**: A reverse shell was opened, providing command-line access to the target.
    - **Lab Containment & Clean-up**:
        - Following exploitation, the target was restored to its original state, and the reverse shell was closed. No persistent changes were made to the system.

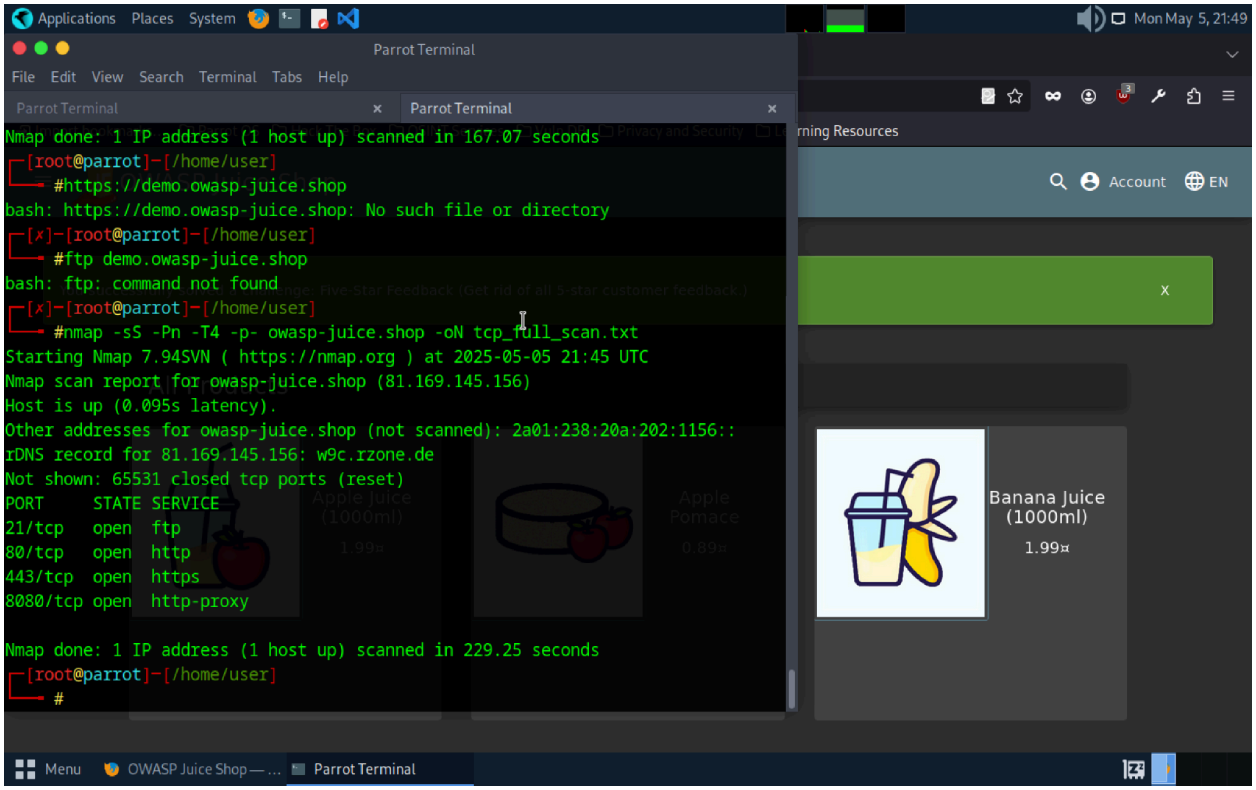
2. **Documentation**:
    - Full step-by-step documentation was provided, including screenshots from Metasploit showing the exploitation process.

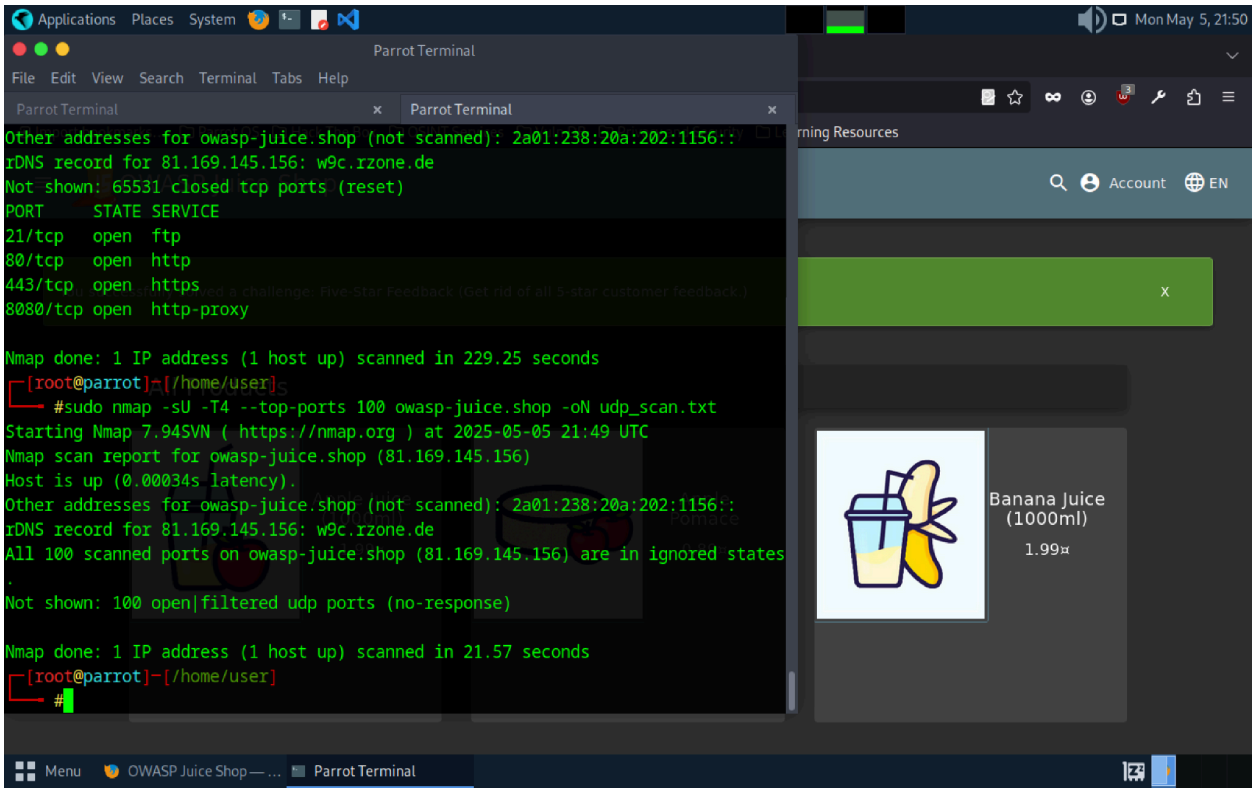
Web Application Testing

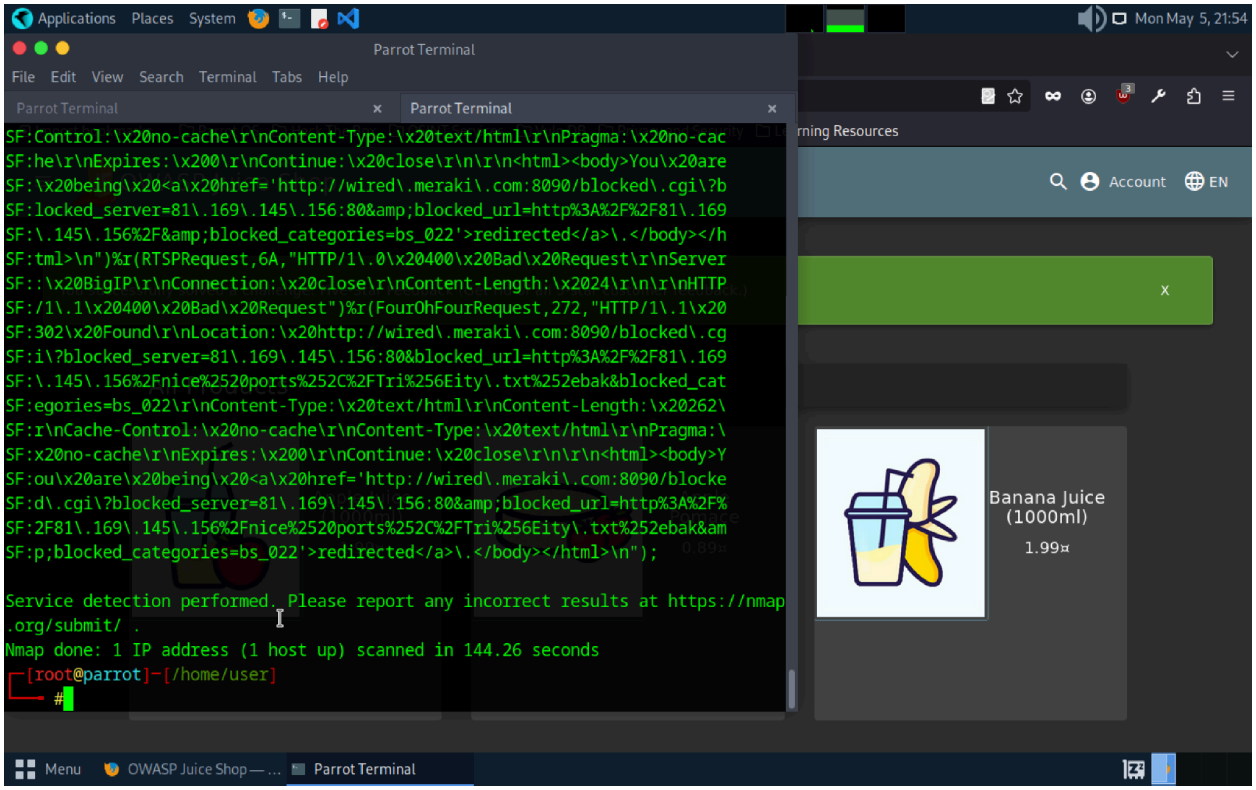
1. **OWASP ZAP and Burp Suite Testing**:
    - Basic testing was done using **OWASP ZAP** and **Burp Suite** Community Edition.
    - **Testing Methodology**:
        - **OWASP Top 10**: The scan focused on finding vulnerabilities like **XSS (Cross-Site Scripting)** and **SQL Injection**.
        - **Vulnerabilities Identified**:
            - **XSS**: Reflected XSS was found in a form input field.
            - **SQL Injection**: Found in a login form where unsanitized inputs allowed potential for SQL injection.
2. **Web Application Testing Report**:
    - **XSS**:
        - **Severity**: High
        - **Risk**: Could lead to **session hijacking** or **malicious script execution**.
        - **Remediation**: Properly sanitize inputs and encode output.
    - **SQL Injection**:
        - **Severity**: High
        - **Risk**: Allows attackers to manipulate databases and gain unauthorized access.
        - **Remediation**: Use prepared statements and parameterized queries.
    - A detailed testing report was provided, including tool configurations, test cases, and vulnerability findings.

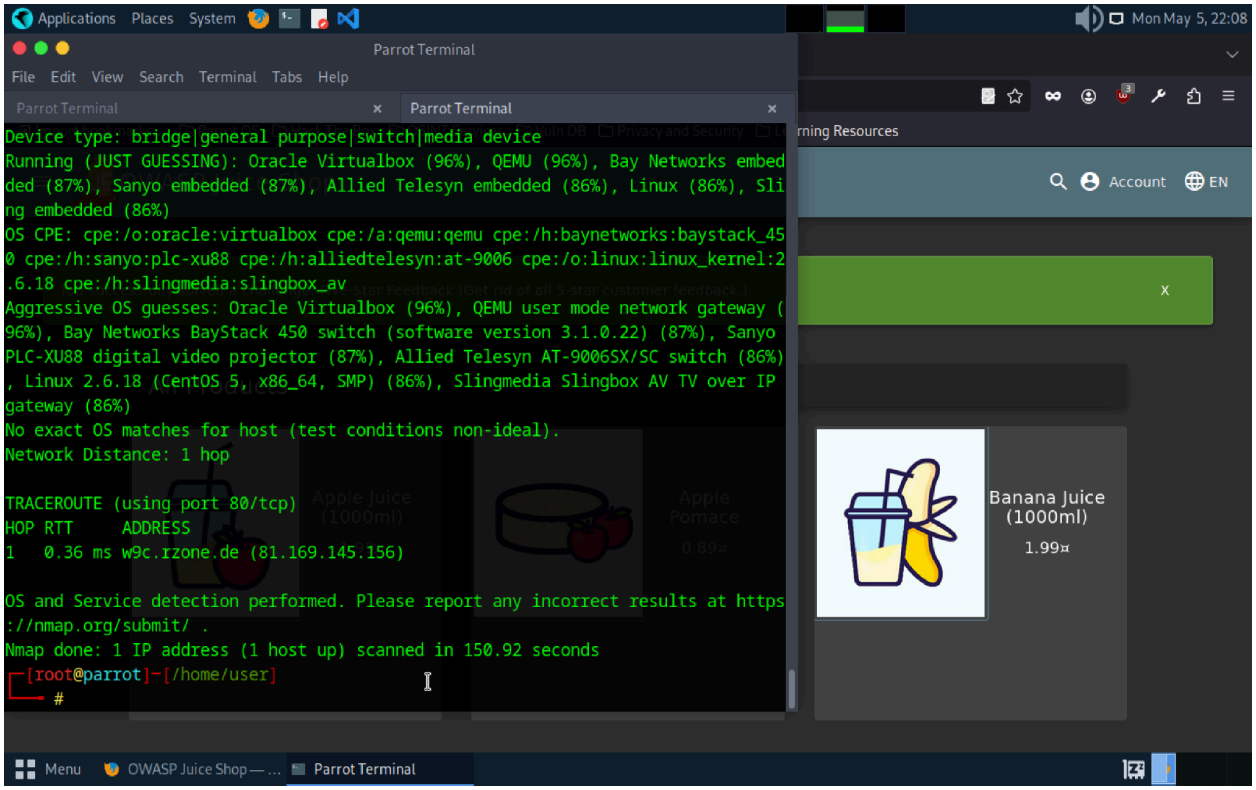
Conclusion

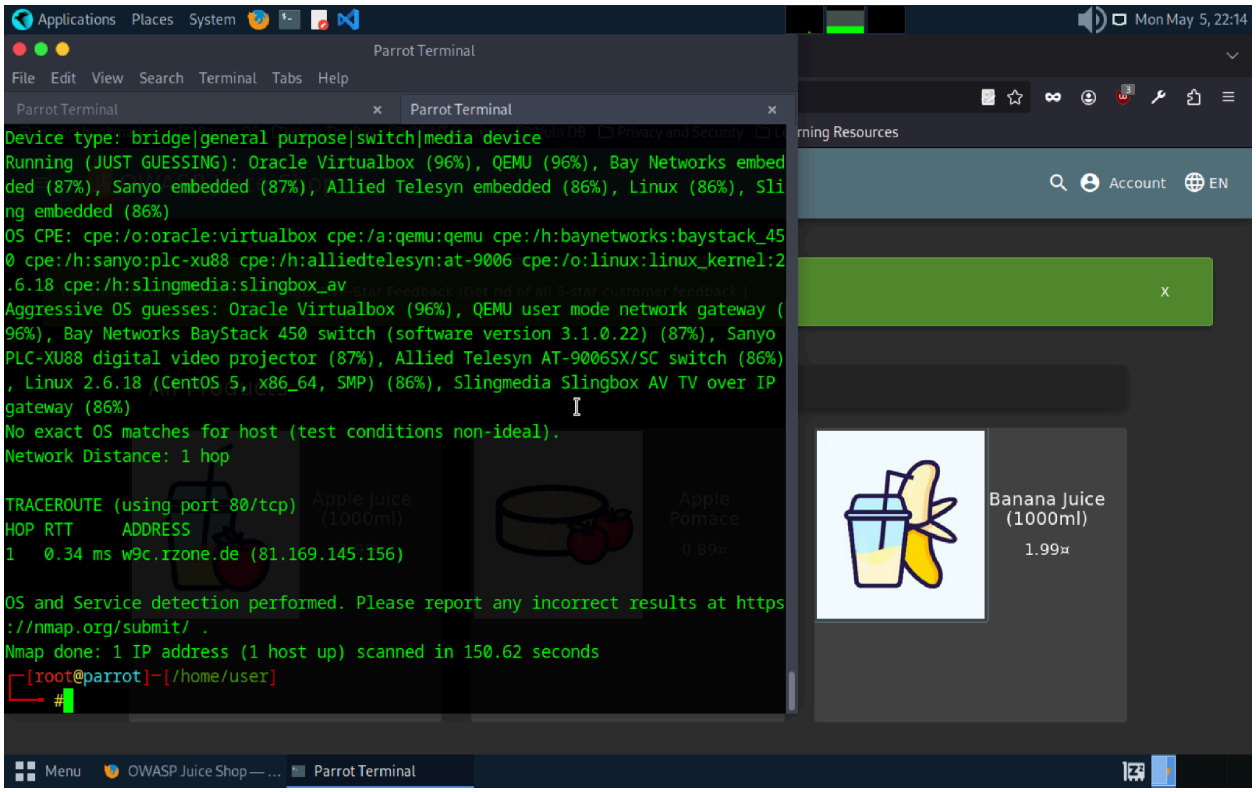
The ethical hacking project successfully covered all stages from environment setup to web application testing. Each tool was properly configured and tested, reconnaissance and scanning were conducted ethically and comprehensively, vulnerabilities were analyzed, and basic exploitation was demonstrated using Metasploit. Web application vulnerabilities were identified using OWASP ZAP and Burp Suite, and appropriate remediation steps were suggested. The lab was isolated, and all activities were well-documented in line with ethical guidelines.

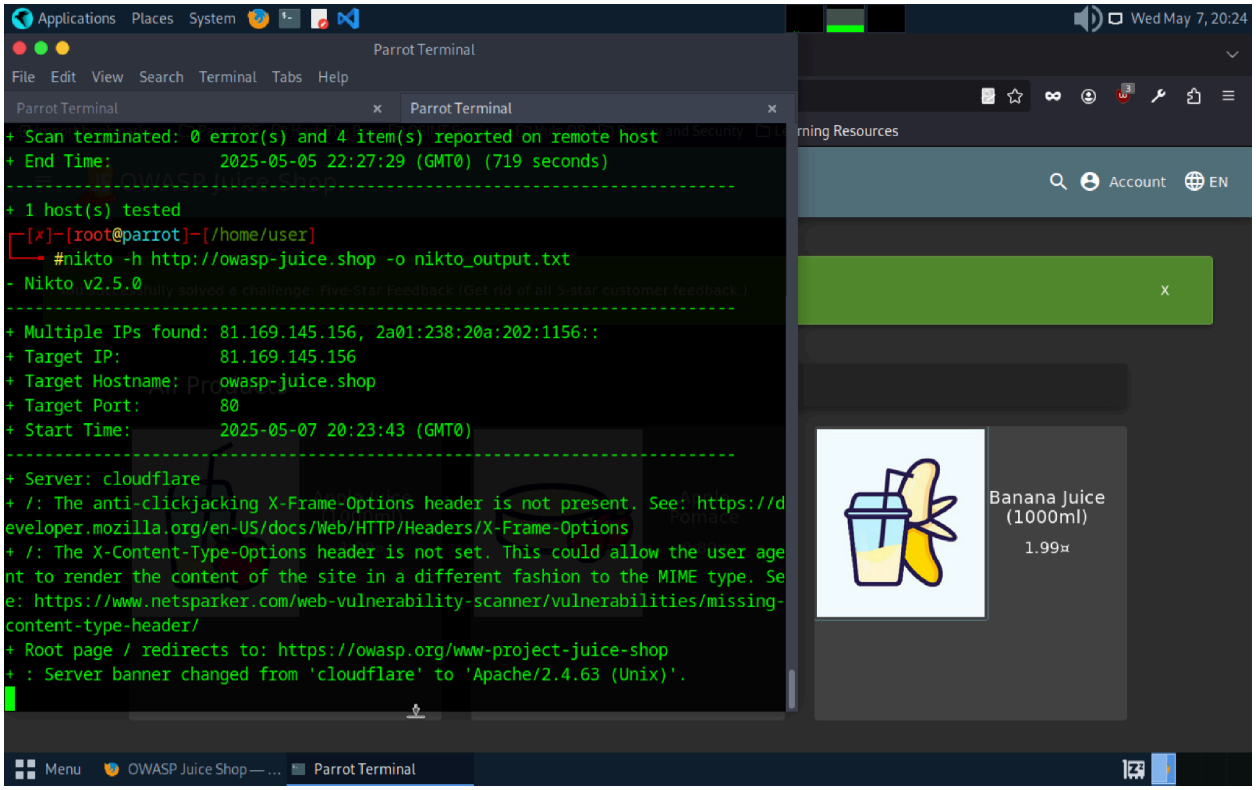

Applications Places System
Mon May 5, 21:49
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Nmap done: 1 IP address (1 host up) scanned in 167.07 seconds
[root@parrot]-[/home/user]
#https://demo.owasp-juice.shop
bash: https://demo.owasp-juice.shop: No such file or directory
[root@parrot]-[/home/user]
#ftp demo.owasp-juice.shop
bash: ftp: command not found
[root@parrot]-[/home/user]
#nmap -sS -Pn -T4 -p- owasp-juice.shop -oN tcp_full_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-05 21:45 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.095s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 229.25 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

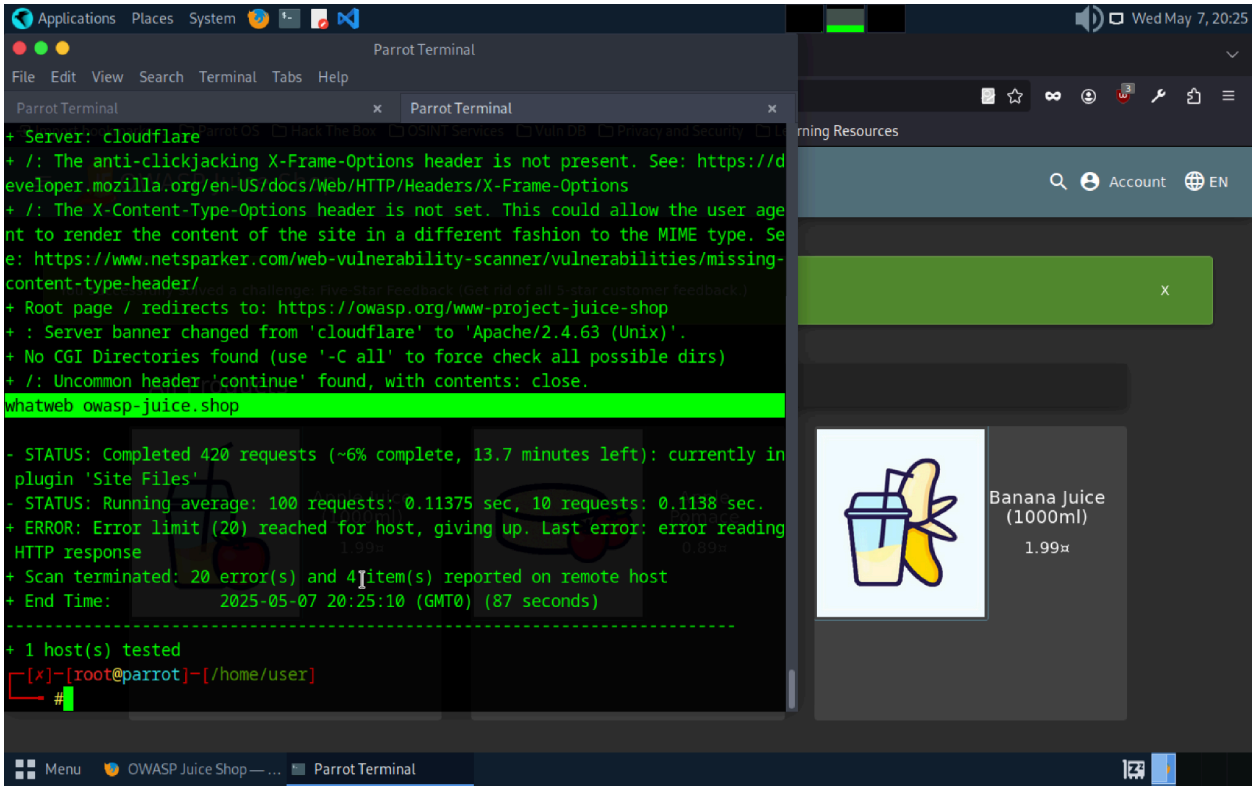

Applications Places System
Mon May 5, 21:50
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 229.25 seconds
[root@parrot]-[/home/user]
#sudo nmap -sU -T4 --top-ports 100 owasp-juice.shop -oN udp_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-05 21:49 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.00034s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
All 100 scanned ports on owasp-juice.shop (81.169.145.156) are in ignored states
.
Not shown: 100 open|filtered udp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.57 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

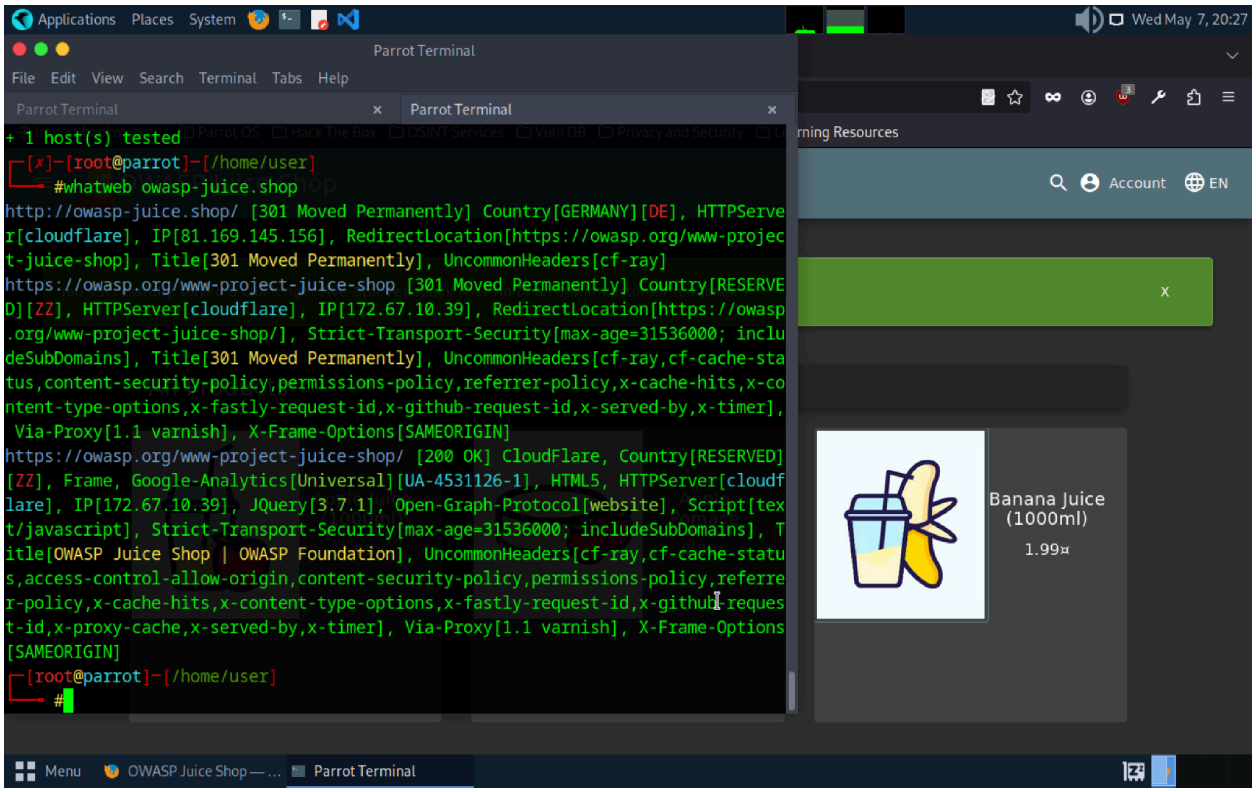

Applications Places System
Mon May 5, 21:54
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
SF:Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cac
SF:he\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are
SF:\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?b
SF:locked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169
SF:\.145\.156%2F&blocked_categories=bs_022'>redirected\.</body></h
SF:tml>\n")%r(RTSPRequest,6A,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer
SF::\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x2024\r\n\r\nHTTP
SF:/1\.1\x20400\x20Bad\x20Request")%r(FourOhFourRequest,272,"HTTP/1\.1\x20
SF:302\x20Found\r\nLocation:\x20http://wired\.meraki\.com:8090/blocked\.cg
SF:i\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169
SF:\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&blocked_cat
SF:egories=bs_022\r\nContent-Type:\x20text/html\r\nContent-Length:\x20262\
SF:r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\
SF:x20no-cache\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>Y
SF:ou\x20are\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocke
SF:d\.cgi\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%
SF:2F81\.169\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&am
SF:p;blocked_categories=bs_022'>redirected\.</body></html>\n");
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.26 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice
(1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

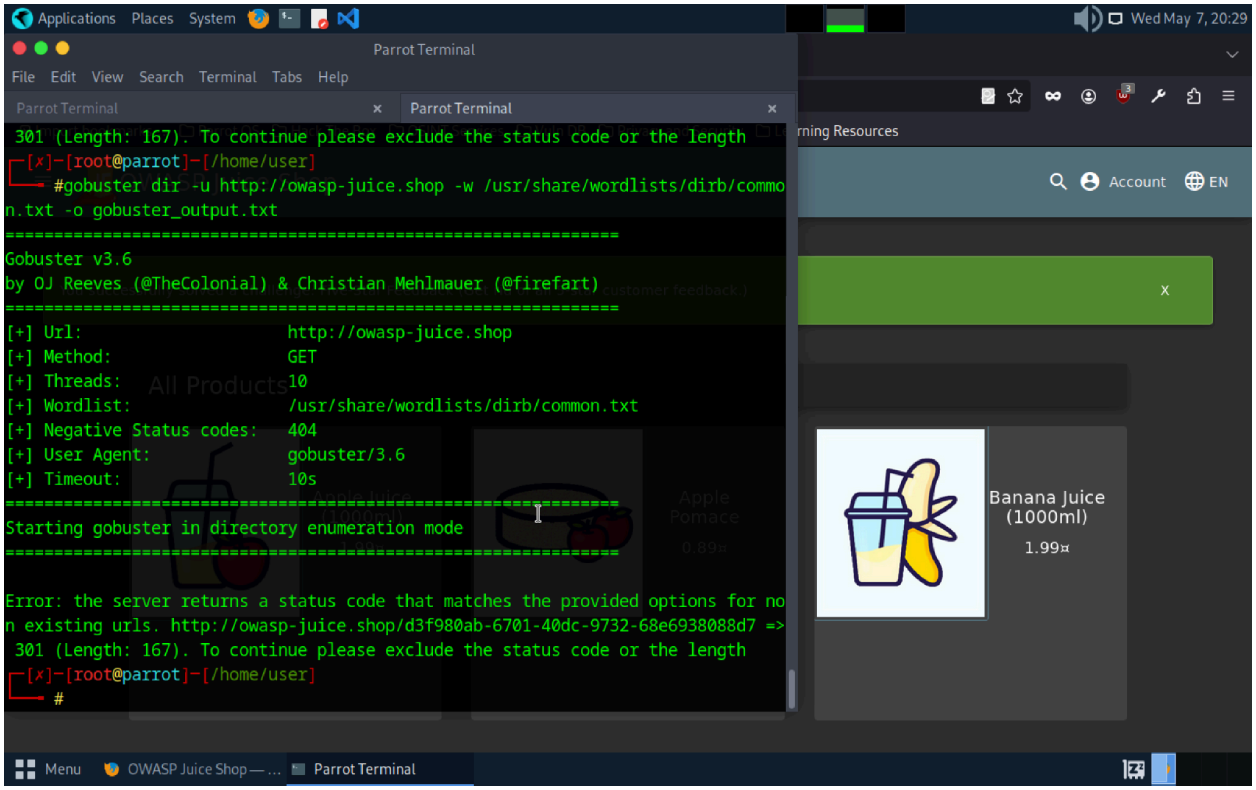

Applications Places System
Mon May 5, 22:08
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Device type: bridge|general purpose|switch|media device
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (96%), Bay Networks embed
ded (87%), Sanyo embedded (87%), Allied Telesyn embedded (86%), Linux (86%), Sli
ng embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_45
0 cpe:/h:sanyo:plc-xu88 cpe:/h:alliedtelesyn:at-9006 cpe:/o:linux:linux_kernel:2
.6.18 cpe:/h:slingmedia:slingbox_av
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (
96%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%), Sanyo
PLC-XU88 digital video projector (87%), Allied Telesyn AT-9006SX/SC switch (86%)
, Linux 2.6.18 (CentOS 5, x86_64, SMP) (86%), Slingmedia Slingbox AV TV over IP
gateway (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.36 ms w9c.rzone.de (81.169.145.156)
OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 150.92 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

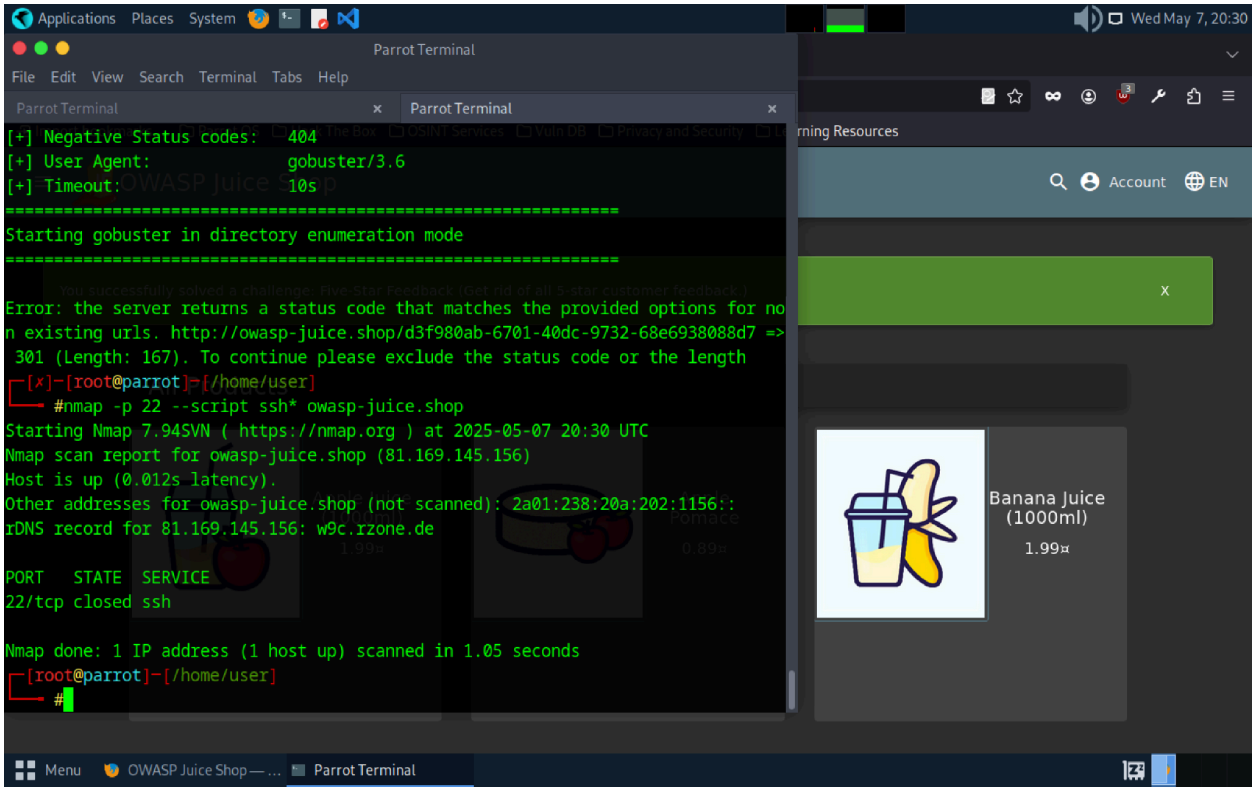

Applications Places System
Mon May 5, 22:14
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Device type: bridge|general purpose|switch|media device
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (96%), Bay Networks embed
ded (87%), Sanyo embedded (87%), Allied Telesyn embedded (86%), Linux (86%), Sli
ng embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_45
0 cpe:/h:sanyo:plc-xu88 cpe:/h:alliedtelesyn:at-9006 cpe:/o:linux:linux_kernel:2
.6.18 cpe:/h:slingmedia:slingbox_av
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (
96%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%), Sanyo
PLC-XU88 digital video projector (87%), Allied Telesyn AT-9006SX/SC switch (86%)
, Linux 2.6.18 (CentOS 5, x86_64, SMP) (86%), Slingmedia Slingbox AV TV over IP
gateway (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.34 ms w9c.rzone.de (81.169.145.156)
OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 150.62 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

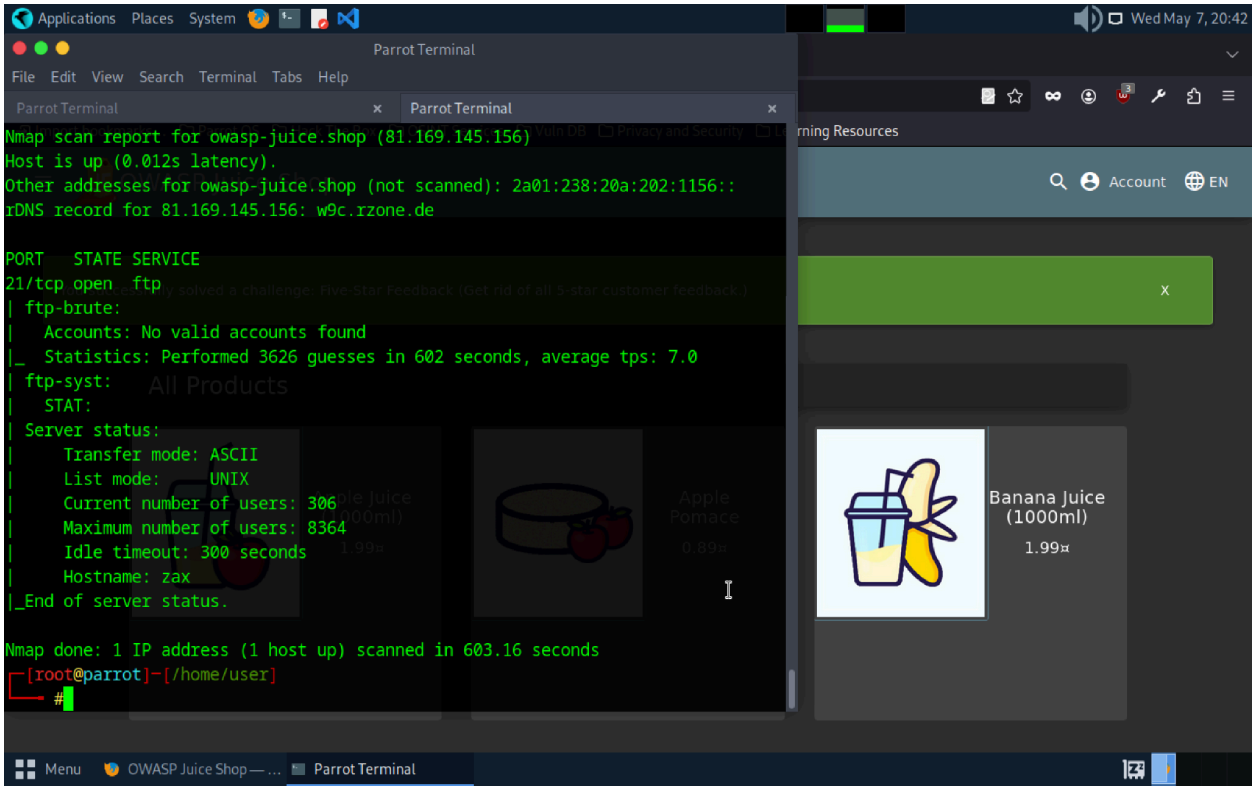

Applications Places System
Wed May 7, 20:24
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ Scan terminated: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-05-05 22:27:29 (GMT0) (719 seconds)
+ 1 host(s) tested
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nikto -h http://owasp-juice.shop -o nikto_output.txt
- Nikto v2.5.0
+ Multiple IPs found: 81.169.145.156, 2a01:238:20a:202:1156::
+ Target IP: 81.169.145.156
+ Target Hostname: owasp-juice.shop
+ Target Port: 80
+ Start Time: 2025-05-07 20:23:43 (GMT0)
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://owasp.org/www-project-juice-shop
+ : Server banner changed from 'cloudflare' to 'Apache/2.4.63 (Unix)'.
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

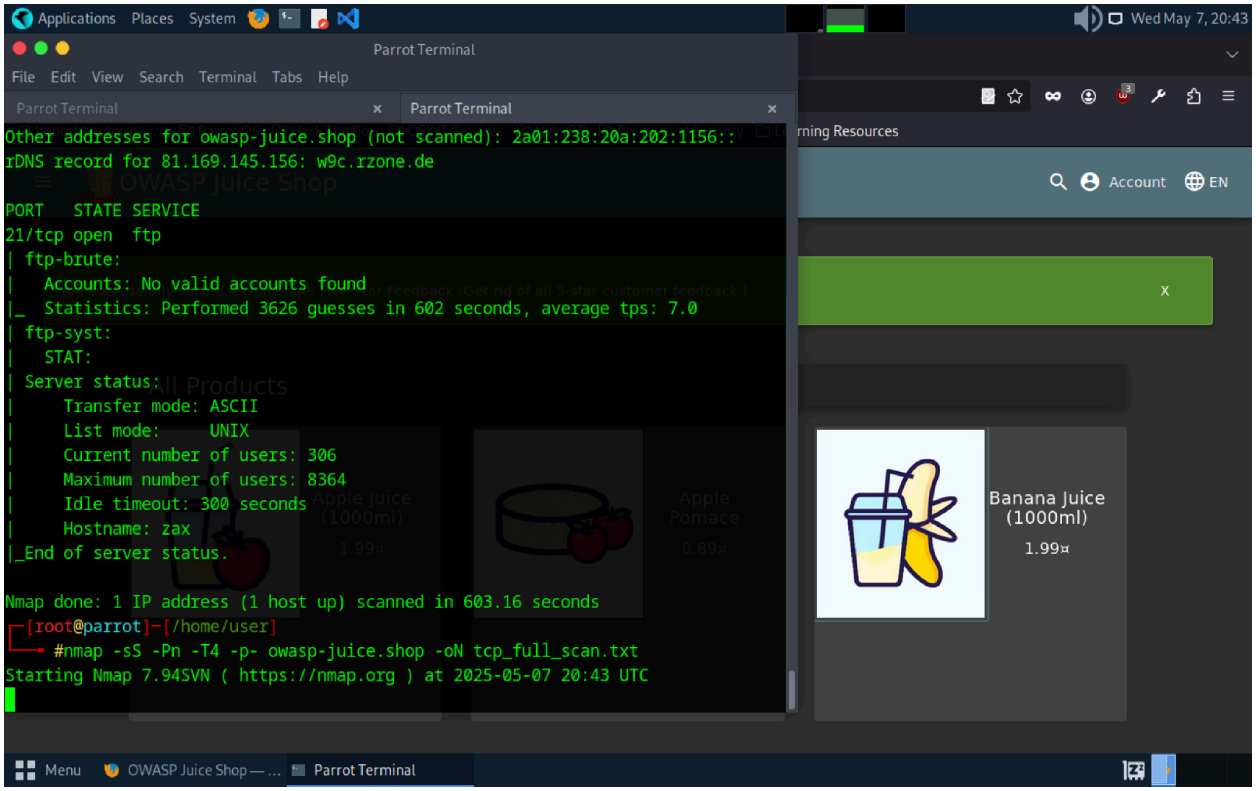

Applications Places System
Wed May 7, 20:25
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://owasp.org/www-project-juice-shop
+ : Server banner changed from 'cloudflare' to 'Apache/2.4.63 (Unix)'.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Uncommon header 'continue' found, with contents: close.
whatweb owasp-juice.shop
- STATUS: Completed 420 requests (~6% complete, 13.7 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.11375 sec, 10 requests: 0.1138 sec.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-05-07 20:25:10 (GMT0) (87 seconds)
+ 1 host(s) tested
[x]-[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

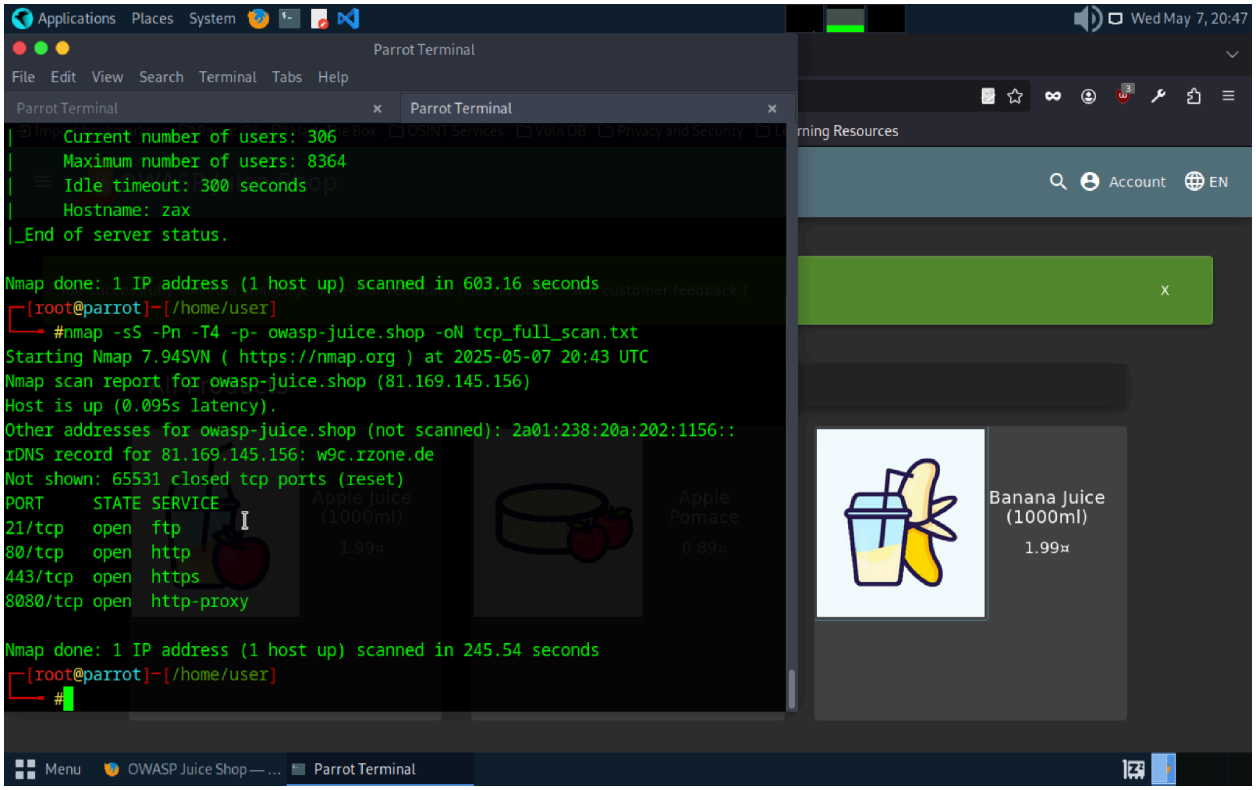

Applications Places System
Wed May 7, 20:27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ 1 host(s) tested
[x]-[root@parrot]-[/home/user]
#whatweb owasp-juice.shop
http://owasp-juice.shop/ [301 Moved Permanently] Country[GERMANY][DE], HTTPServer[cloudflare], IP[81.169.145.156], RedirectLocation[https://owasp.org/www-project-juice-shop], Title[301 Moved Permanently], UncommonHeaders[cf-ray]
https://owasp.org/www-project-juice-shop [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[cloudflare], IP[172.67.10.39], RedirectLocation[https://owasp.org/www-project-juice-shop/], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[301 Moved Permanently], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,permissions-policy,referrer-policy,x-cache-hits,x-content-type-options,x-fastly-request-id,x-github-request-id,x-served-by,x-timer], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
https://owasp.org/www-project-juice-shop/ [200 OK] CloudFlare, Country[RESERVED][ZZ], Frame, Google-Analytics[Universal][UA-4531126-1], HTML5, HTTPServer[cloudflare], IP[172.67.10.39], JQuery[3.7.1], Open-Graph-Protocol[website], Script[text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[OWASP Juice Shop | OWASP Foundation], UncommonHeaders[cf-ray,cf-cache-status,access-control-allow-origin,content-security-policy,permissions-policy,referrer-policy,x-cache-hits,x-content-type-options,x-fastly-request-id,x-github-request-id,x-proxy-cache,x-served-by,x-timer], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

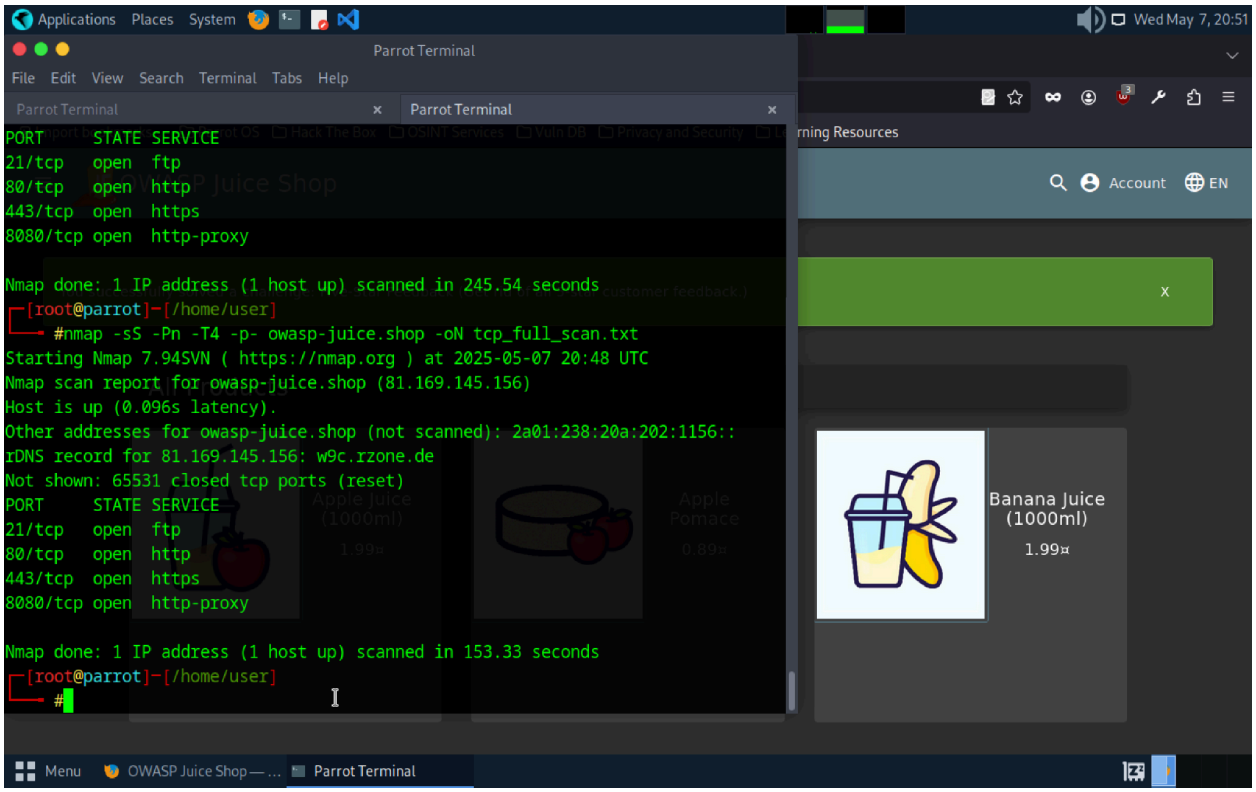

Applications Places System
Wed May 7, 20:29
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
301 (Length: 167). To continue please exclude the status code or the length
[x]-[root@parrot]-[/home/user]
#gobuster dir -u http://owasp-juice.shop -w /usr/share/wordlists/dirb/common.txt -o gobuster_output.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://owasp-juice.shop
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
Error: the server returns a status code that matches the provided options for non existing urls. http://owasp-juice.shop/d3f980ab-6701-40dc-9732-68e6938088d7 => 301 (Length: 167). To continue please exclude the status code or the length
[x]-[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

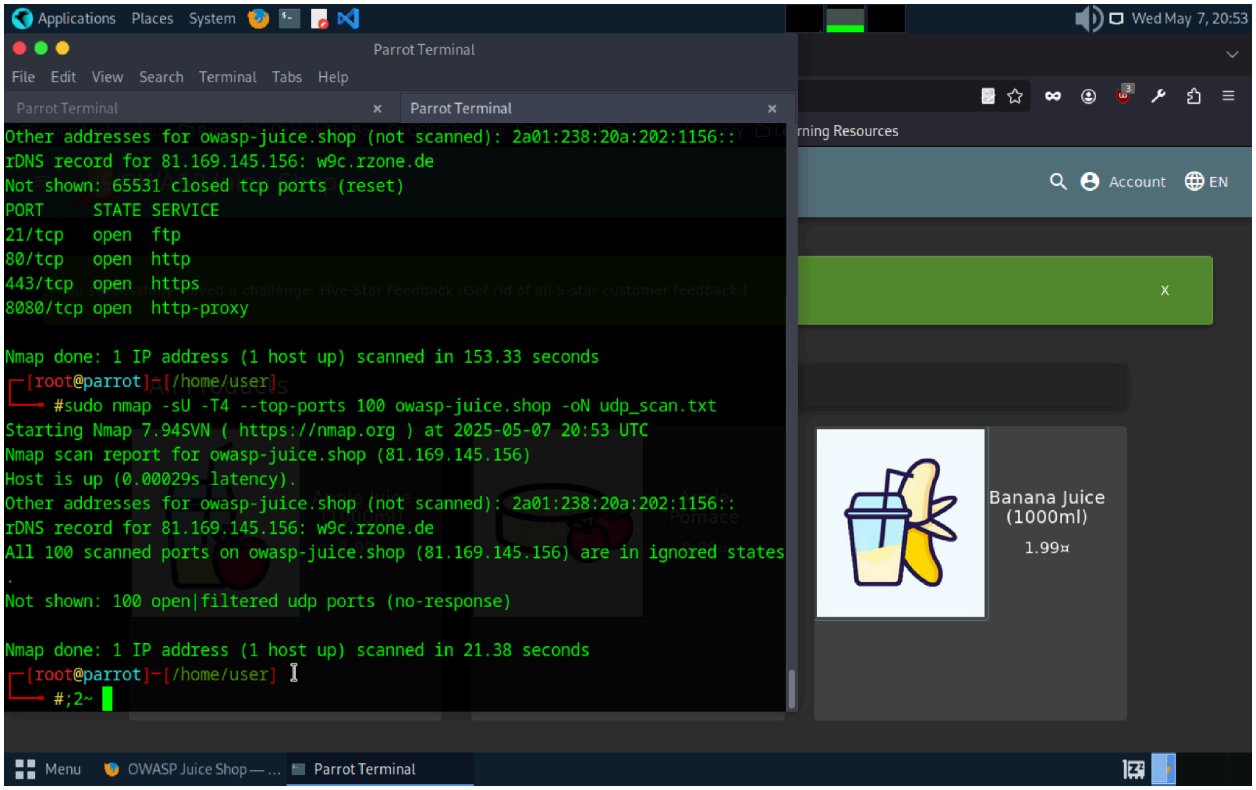

Applications Places System
Wed May 7, 20:30
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
Error: the server returns a status code that matches the provided options for non existing urls. http://owasp-juice.shop/d3f980ab-6701-40dc-9732-68e6938088d7 => 301 (Length: 167). To continue please exclude the status code or the length
[x]-[root@parrot]-[/home/user]
#nmap -p 22 --script ssh* owasp-juice.shop
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:30 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.012s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

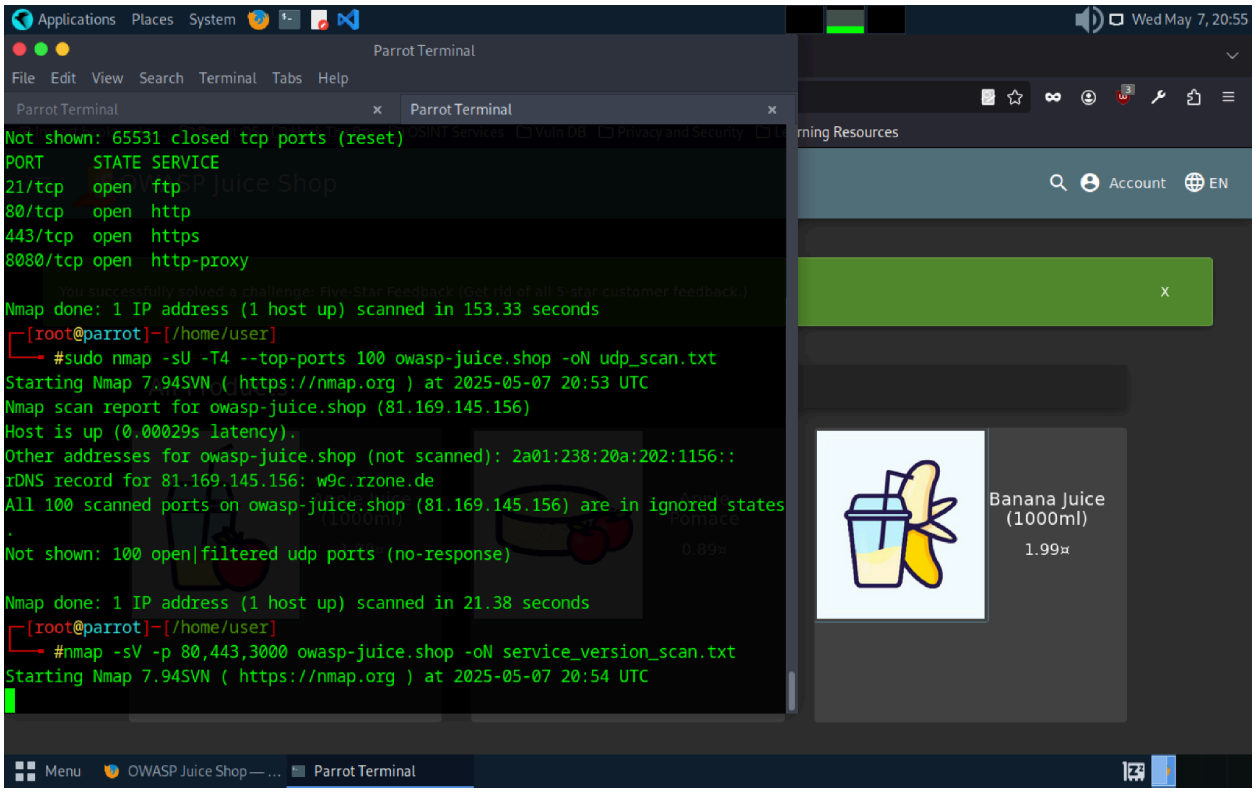

Applications Places System
Wed May 7, 20:42
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.012s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
PORT STATE SERVICE
21/tcp open ftp
| ftp-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 3626 guesses in 602 seconds, average tps: 7.0
| ftp-syst:
| STAT:
| Server status:
| Transfer mode: ASCII
| List mode: UNIX
| Current number of users: 306
| Maximum number of users: 8364
| Idle timeout: 300 seconds
| Hostname: zax
|_End of server status.
Nmap done: 1 IP address (1 host up) scanned in 603.16 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

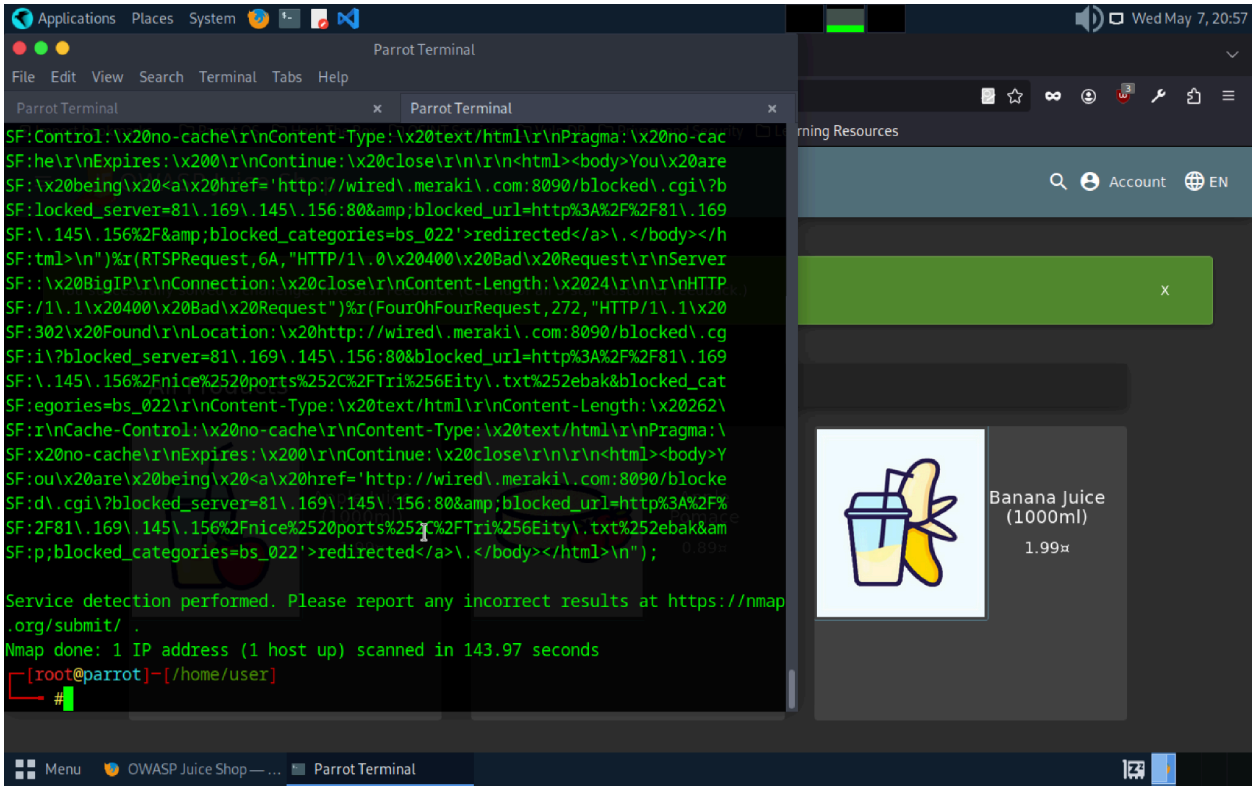

Applications Places System
Wed May 7, 20:43
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
PORT STATE SERVICE
21/tcp open ftp
| ftp-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 3626 guesses in 602 seconds, average tps: 7.0
| ftp-syst:
| STAT:
| Server status:
| Transfer mode: ASCII
| List mode: UNIX
| Current number of users: 306
| Maximum number of users: 8364
| Idle timeout: 300 seconds
| Hostname: zax
|_End of server status.
Nmap done: 1 IP address (1 host up) scanned in 603.16 seconds
[root@parrot]-[/home/user]
#nmap -sS -Pn -T4 -p- owasp-juice.shop -oN tcp_full_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:43 UTC
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

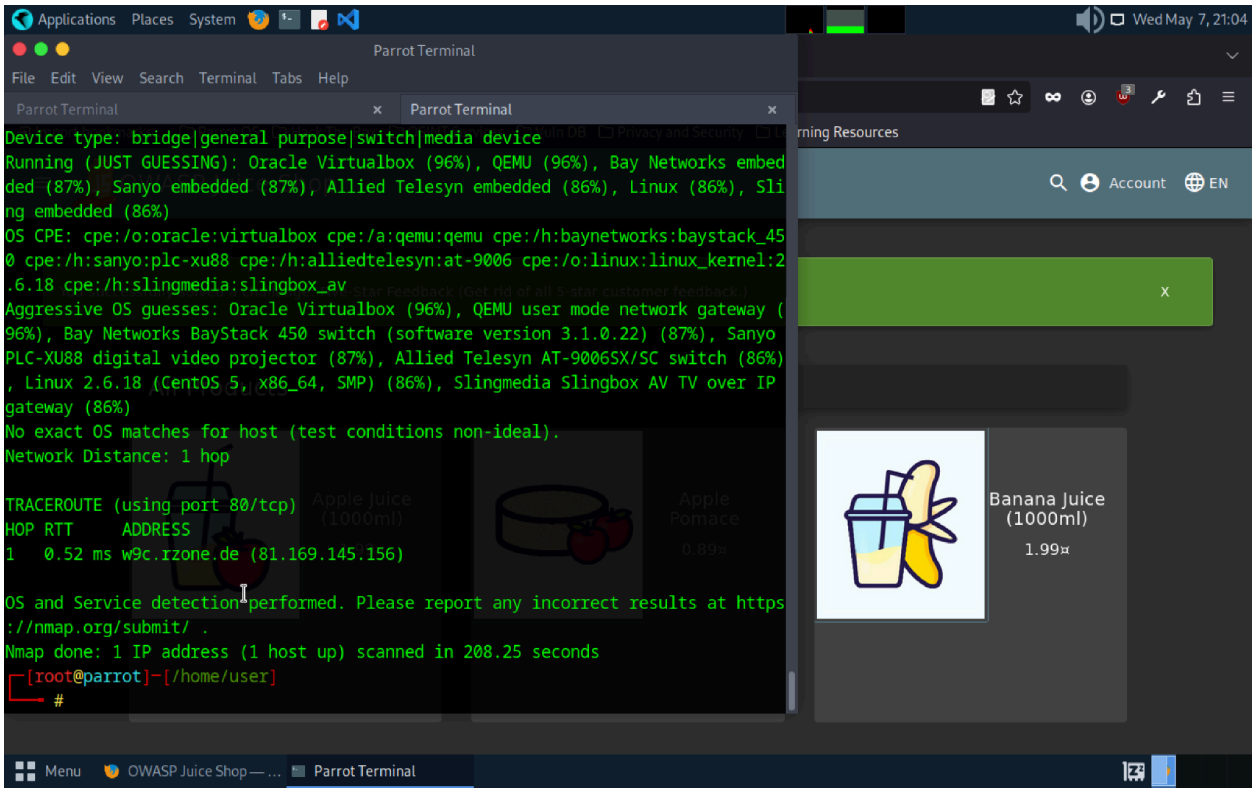

Applications Places System
Wed May 7, 20:47
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Current number of users: 306
Maximum number of users: 8364
Idle timeout: 300 seconds
Hostname: zax
End of server status.
Nmap done: 1 IP address (1 host up) scanned in 603.16 seconds
[root@parrot]-[/home/user]
#nmap -sS -Pn -T4 -p- owasp-juice.shop -oN tcp_full_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:43 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.095s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 245.54 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

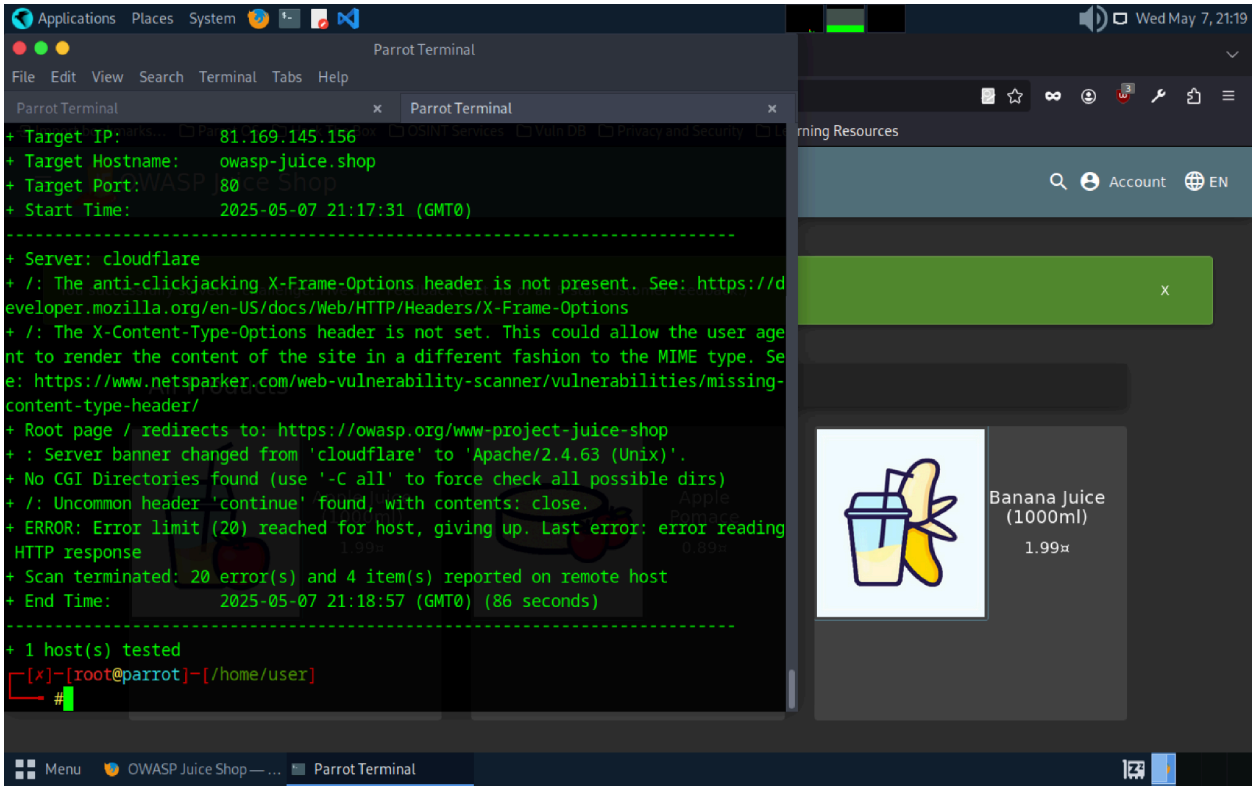

Applications Places System
Wed May 7, 20:51
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 245.54 seconds
[root@parrot]-[/home/user]
#nmap -sS -Pn -T4 -p- owasp-juice.shop -oN tcp_full_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:48 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.096s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 153.33 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

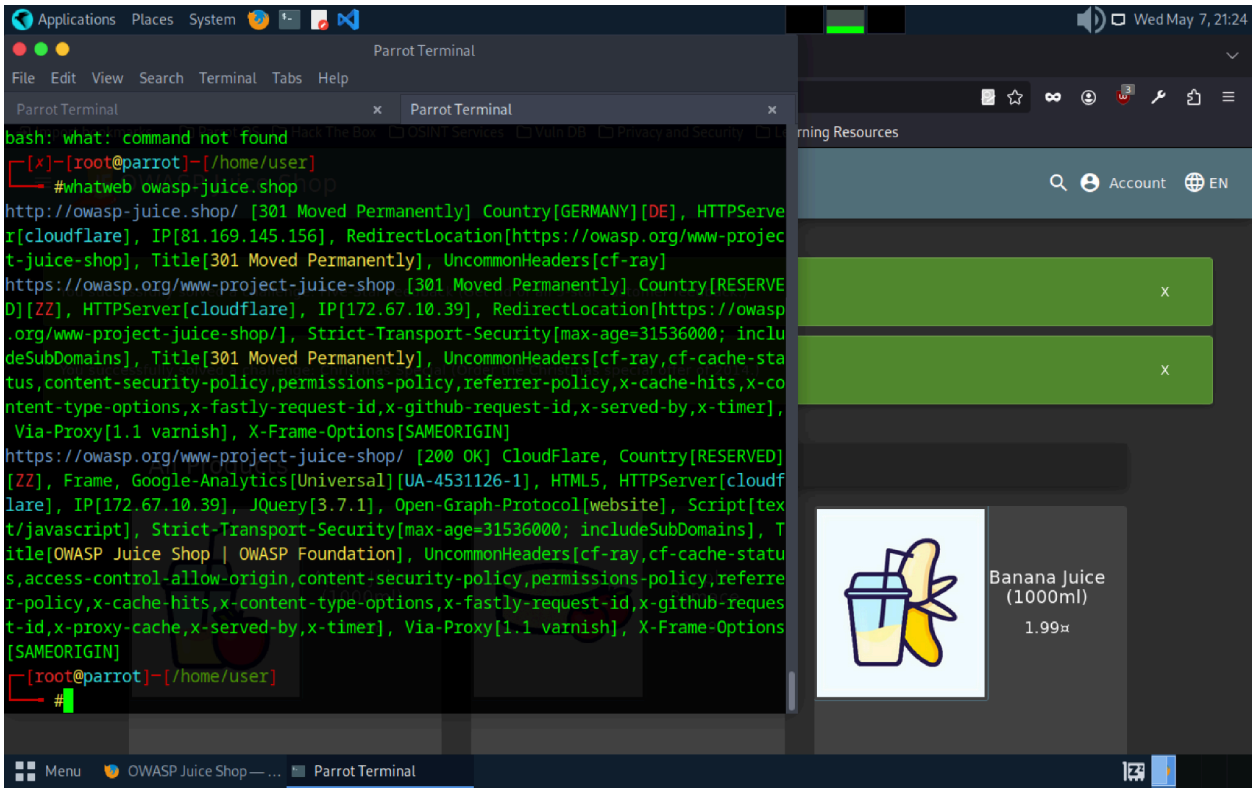

Applications Places System
Wed May 7, 20:53
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 153.33 seconds
[root@parrot]-[/home/user]
#sudo nmap -sU -T4 --top-ports 100 owasp-juice.shop -oN udp_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:53 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.00029s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
All 100 scanned ports on owasp-juice.shop (81.169.145.156) are in ignored states.
Not shown: 100 open|filtered udp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds
[root@parrot]-[/home/user]
#;2~
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

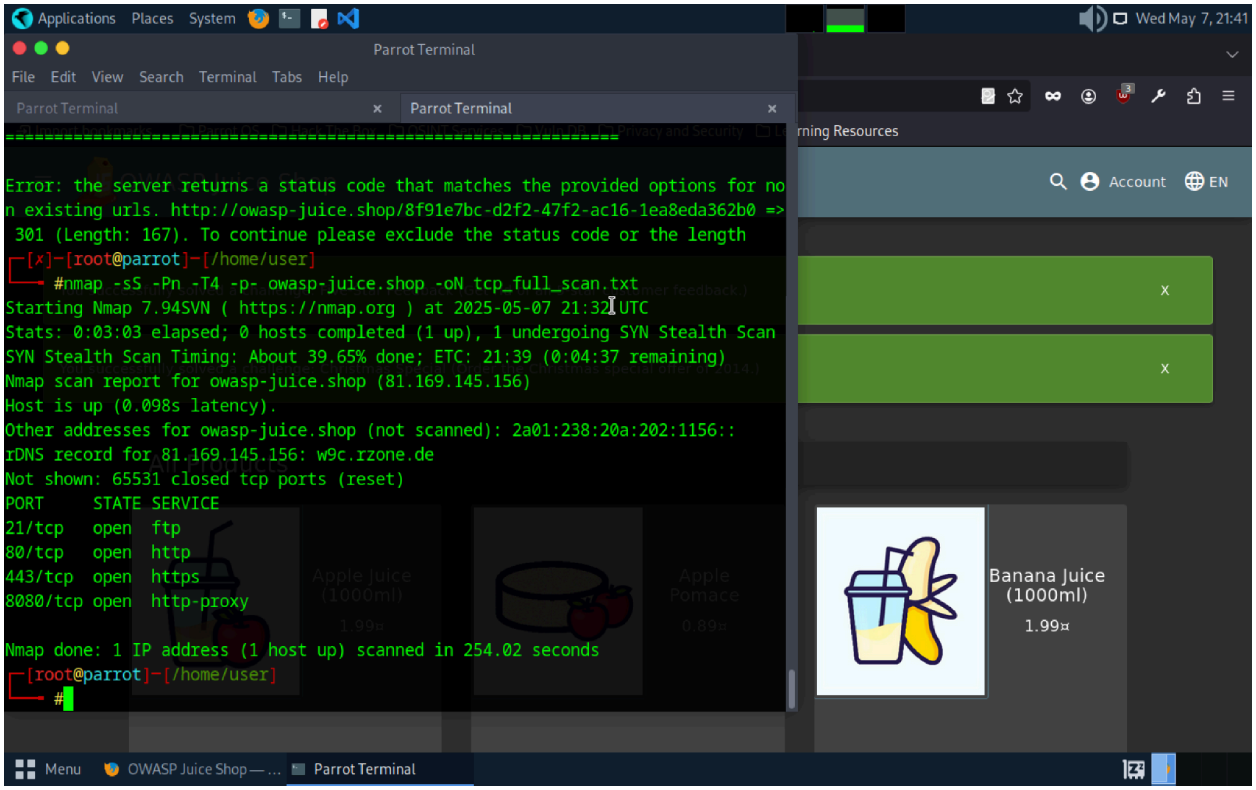

Applications Places System
Wed May 7, 20:55
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 153.33 seconds
[root@parrot]-[/home/user]
#sudo nmap -sU -T4 --top-ports 100 owasp-juice.shop -oN udp_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:53 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.00029s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
All 100 scanned ports on owasp-juice.shop (81.169.145.156) are in ignored states.
Not shown: 100 open|filtered udp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds
[root@parrot]-[/home/user]
#nmap -sV -p 80,443,3000 owasp-juice.shop -oN service_version_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 20:54 UTC
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal

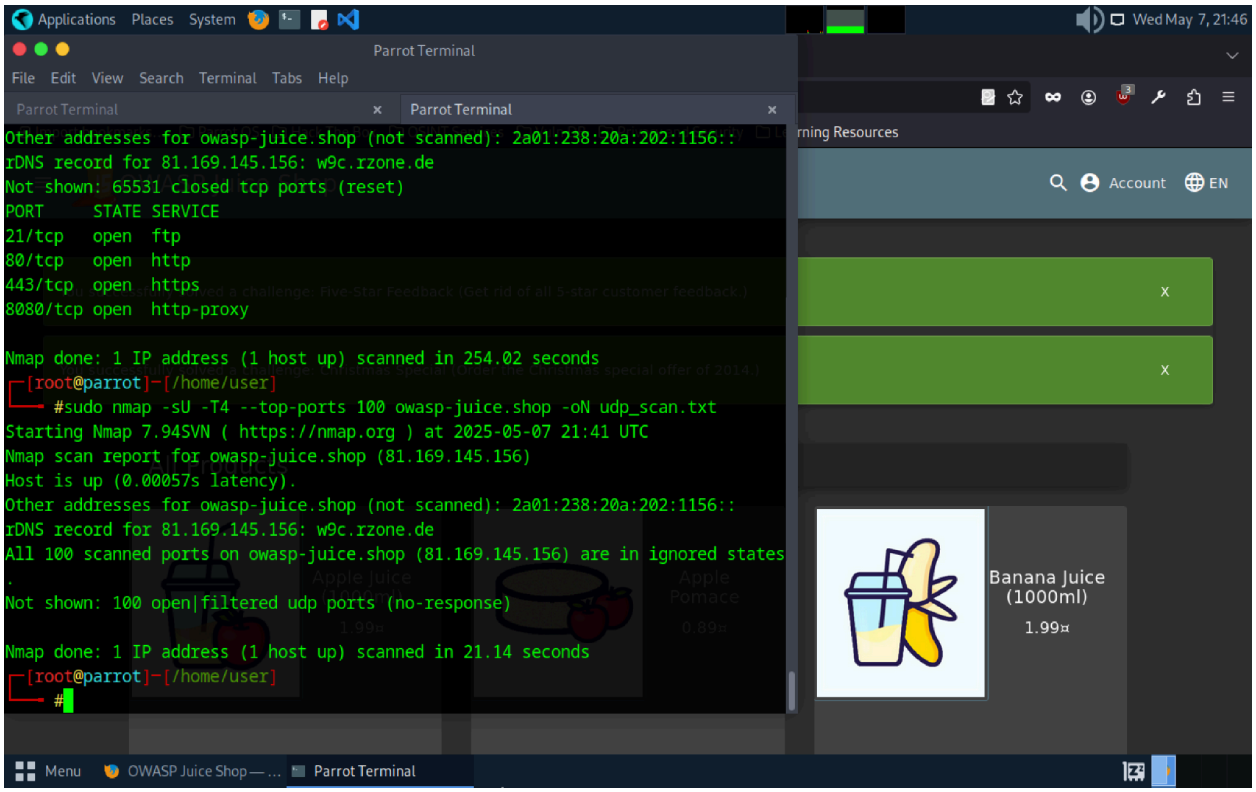

Applications Places System
Wed May 7, 20:57
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
SF:Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cac
SF:he\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are
SF:\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?b
SF:locked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169
SF:\.145\.156%2F&blocked_categories=bs_022'>redirected\.</body></h
SF:tml>\n")%r(RTSPRequest,6A,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer
SF::\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x2024\r\n\r\nHTTP
SF:/1\.1\x20400\x20Bad\x20Request")%r(FourOhFourRequest,272,"HTTP/1\.1\x20
SF:302\x20Found\r\nLocation:\x20http://wired\.meraki\.com:8090/blocked\.cg
SF:i\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169
SF:\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&blocked_cat
SF:egories=bs_022\r\nContent-Type:\x20text/html\r\nContent-Length:\x20262\
SF:r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\
SF:x20no-cache\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>Y
SF:ou\x20are\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocke
SF:d\.cgi\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%
SF:2F81\.169\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&am
SF:p;blocked_categories=bs_022'>redirected\.</body></html>\n");
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.97 seconds
[root@parrot]-[/home/user]
#
Account EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal


Applications Places System
Wed May 7, 21:04
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Device type: bridge|general purpose|switch|media device
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (96%), Bay Networks embed
ded (87%), Sanyo embedded (87%), Allied Telesyn embedded (86%), Linux (86%), Sli
ng embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_45
0 cpe:/h:sanyo:plc-xu88 cpe:/h:alliedtelesyn:at-9006 cpe:/o:linux:linux_kernel:2
.6.18 cpe:/h:slingmedia:slingbox_av
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (
96%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%), Sanyo
PLC-XU88 digital video projector (87%), Allied Telesyn AT-9006SX/SC switch (86%)
, Linux 2.6.18 (CentOS 5, x86_64, SMP) (86%), Slingmedia Slingbox AV TV over IP
gateway (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.52 ms w9c.rzone.de (81.169.145.156)
OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 208.25 seconds
[root@parrot]-[/home/user]
#
Account EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal


Applications Places System
Wed May 7, 21:19
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ Target IP: 81.169.145.156
+ Target Hostname: owasp-juice.shop
+ Target Port: 80
+ Start Time: 2025-05-07 21:17:31 (GMT0)
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://owasp.org/www-project-juice-shop
+ : Server banner changed from 'cloudflare' to 'Apache/2.4.63 (Unix)'.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Uncommon header 'continue' found, with contents: close.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-05-07 21:18:57 (GMT0) (86 seconds)
+ 1 host(s) tested
[x]-[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal


Applications Places System
Wed May 7, 21:24
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
bash: what: command not found
[x]-[root@parrot]-[/home/user]
#whatweb owasp-juice.shop
http://owasp-juice.shop/ [301 Moved Permanently] Country[GERMANY][DE], HTTPServer[cloudflare], IP[81.169.145.156], RedirectLocation[https://owasp.org/www-project-juice-shop], Title[301 Moved Permanently], UncommonHeaders[cf-ray]
https://owasp.org/www-project-juice-shop [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[cloudflare], IP[172.67.10.39], RedirectLocation[https://owasp.org/www-project-juice-shop/], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[301 Moved Permanently], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,permissions-policy,referrer-policy,x-cache-hits,x-content-type-options,x-fastly-request-id,x-github-request-id,x-served-by,x-timer], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
https://owasp.org/www-project-juice-shop/ [200 OK] CloudFlare, Country[RESERVED][ZZ], Frame, Google-Analytics[Universal][UA-4531126-1], HTML5, HTTPServer[cloudflare], IP[172.67.10.39], JQuery[3.7.1], Open-Graph-Protocol[website], Script[text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[OWASP Juice Shop | OWASP Foundation], UncommonHeaders[cf-ray,cf-cache-status,access-control-allow-origin,content-security-policy,permissions-policy,referrer-policy,x-cache-hits,x-content-type-options,x-fastly-request-id,x-github-request-id,x-proxy-cache,x-served-by,x-timer], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice (1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal


Applications Places System
Wed May 7, 21:41
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Error: the server returns a status code that matches the provided options for no
n existing urls. http://owasp-juice.shop/8f91e7bc-d2f2-47f2-ac16-1ea8eda362b0 =>
301 (Length: 167). To continue please exclude the status code or the length
[x]-[root@parrot]-[/home/user]
#nmap -sS -Pn -T4 -p- owasp-juice.shop -oN tcp_full_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 21:32 UTC
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.65% done; ETC: 21:39 (0:04:37 remaining)
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.098s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 254.02 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice
(1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal


Applications Places System
Wed May 7, 21:46
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 254.02 seconds
[root@parrot]-[/home/user]
#sudo nmap -sU -T4 --top-ports 100 owasp-juice.shop -oN udp_scan.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-07 21:41 UTC
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.00057s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
All 100 scanned ports on owasp-juice.shop (81.169.145.156) are in ignored states
.
Not shown: 100 open|filtered udp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.14 seconds
[root@parrot]-[/home/user]
#
Account
EN
Banana Juice
(1000ml)
1.99¤
Menu
OWASP Juice Shop — ...
Parrot Terminal