🔍 Vulnerability Scan Report

1️⃣Scan Details

- **Date and Time of Scan:**
  Tue Jun 17 17:33:30 2025

- **Target Scanned:**
  `demo.owasp-juice.shop` (81.169.145.156)
  rDNS: w9c.rzone.de

Nmap Command Used:

bash
CopyEdit

```
nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
```

-

2️⃣Open Ports and Services

Port	State	Service	Version
21/tcp	open	ftp	`ftpd.bin round-robin file server 3.4.0r16`
25/tcp	filtered	smtp	*filtered* (no version info)
80/tcp	open	http-proxy	`F5 BIG-IP load balancer http proxy`

3️⃣Vulnerabilities Found

CVE	Vulnerability	Description	References
CVE-2011-3192	**Apache byterange filter DoS**	Apache web server vulnerable to DoS via numerous overlapping byte ranges requests.	CVE-2011-3192, BID-49303, Full Disclosure

CVE-2005-3299	**phpMyAdmin grab_globals.lib.php Traversal LFI**	Possible Local File Inclusion vulnerability in phpMyAdmin via `subform` parameter. State is *UNKNOWN* (test inconclusive).	CVE-2005-3299

4️⃣ Critical Assets

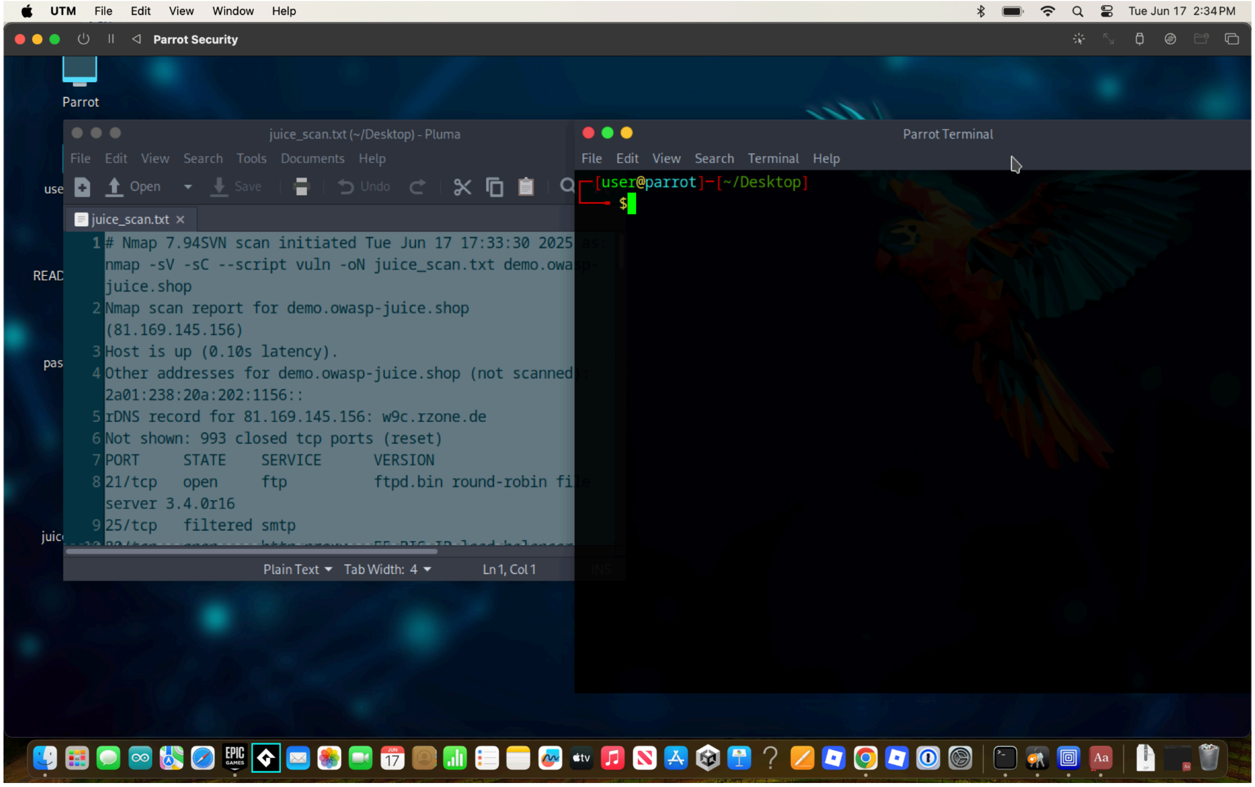
- **FTP Service (Port 21):**
  Might allow file transfer operations; if misconfigured, could expose sensitive files or credentials.

- **HTTP Proxy (Port 80):**
  The web server is running on a load balancer; vulnerabilities here could lead to denial of service or exploitation of web application flaws (e.g., the Juice Shop’s known vulnerabilities).

- **phpMyAdmin Interface:**
  If accessible, could allow database manipulation or unauthorized data disclosure through Local File Inclusion (LFI).

5️⃣ Threat Hunting Commentary

The scan reveals several notable points of concern. The open FTP service could be an entry point for brute-force attacks or file exfiltration if not properly secured. The web server shows signs of an old Apache vulnerability (CVE-2011-3192) that can be exploited for denial of service, which although old, still represents risk if unpatched. Additionally, the possible phpMyAdmin Local File Inclusion highlights misconfiguration risk that could allow attackers to read sensitive server files. Combined, these issues suggest that the target has legacy or insecure components that require patching and proper access controls to prevent exploitation. Further manual testing and patch verification are recommended.



UTM File Edit View Window Help
Tue Jun 17 2:34 PM
Parrot Security
Parrot
juice_scan.txt (~/Desktop) - Pluma
File Edit View Search Tools Documents Help
Open
Save
Undo
juice_scan.txt
Plain Text
Tab Width: 4
Ln 1, Col 1
Parrot Terminal
File Edit View Search Terminal Help

```
# Nmap 7.94SVN scan initiated Tue Jun 17 17:33:30 2025 as: nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
Nmap scan report for demo.owasp-juice.shop (81.169.145.156)
Host is up (0.10s latency).
Other addresses for demo.owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 993 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          ftpd.bin round-robin file server 3.4.0r16
25/tcp    filtered smtp
```

```
┌─[user@parrot]─[~/Desktop]
└──╼ $
```