Vulnerability Assessment Report

Target: `demo.owasp-juice.shop` (IP: `81.169.145.156`)
Scan Date & Time: Tuesday, June 17, 2025, 16:16:05 UTC
Scanner: Parrot OS + Nmap
Command Used:

bash
Copy code

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

📡 Open Ports & Services

Port	State	Service	Version / Notes
21	Open	FTP	`ftpd.bin round-robin file server 3.4.0r16`
25	Filtered	SMTP	Unknown (filtered)
80	Open	HTTP Proxy	`F5 BIG-IP load balancer http proxy`

⚠️ Vulnerabilities Found

1. phpMyAdmin Local File Inclusion (LFI)

- **Script**: `http-phpmyadmin-dir-traversal`
- **CVE ID**: `CVE-2005-3299`
- **Description**: A vulnerability in `grab_globals.lib.php` allows local file inclusion via the `subform` parameter. Can lead to access of sensitive files like `/etc/passwd`.
- **Severity**: High (possible path traversal exploit).
- **Status**: Test inconclusive but potentially exploitable.

- **Disclosure Date**: October 2005

🔐 Critical Assets Identified

- **Login Page**: Detected in HTML response
- **Admin Panel**: Potential entry point inferred from structure; no direct admin endpoint listed, but likely due to Juice Shop's known CTF structure.
- **Public Metadata**: Extensive front-end JS, jQuery, cookie consent libraries — likely exploitable via XSS if inputs are not sanitized.

🌐 HTTP Content Sample

html
Copy code

```html
<title>OWASP Juice Shop</title>
<meta name="description" content="Probably the most modern and sophisticated insecure web application">
<link rel="icon" href="assets/public/favicon_js.ico">
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
```

🔎 Threat Hunting Commentary

The application is a known intentionally vulnerable platform, but this does not diminish the need to simulate real-world assessments. Notably:

- **FTP Service** is outdated and potentially misconfigured, often exploited for credential reuse or file uploads.

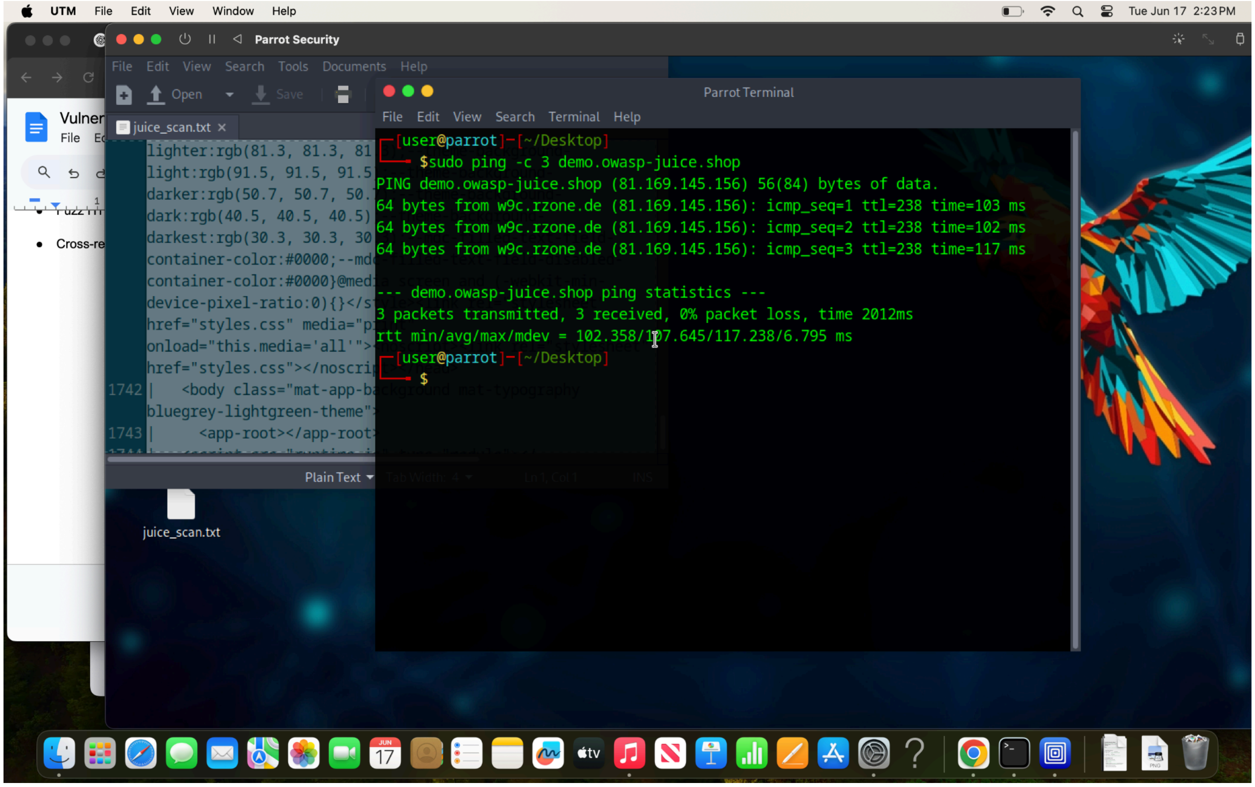
- **phpMyAdmin LFI** could lead to further privilege escalation if combined with writable directories or exposed logs.
- **Filtered SMTP (Port 25)** could be a sign of spam protection or firewall — still worth probing in a full assessment.
- No CSRF, DOM-XSS, or Majordomo2 directory traversal found, though this doesn’t rule out deeper issues.

📊 Analysis Summary

This scan exposed a critical LFI vulnerability (CVE-2005-3299) in phpMyAdmin, alongside potentially weak FTP and proxy HTTP configurations. The use of known libraries and an exposed proxy hints at attack vectors like XSS or cache poisoning. Given the target is a purposely insecure app, these findings are expected, but in a real-world scenario, the LFI combined with open FTP and weak proxy setup would raise major red flags.

Next Steps:

- Enumerate deeper into `phpMyAdmin` for file inclusion exploitability.
- Brute-force FTP credentials if authorized.
- Fuzz HTTP endpoints for hidden panels and XSS/CSRF injection.
- Cross-reference services against known exploit databases.



```
lighter:rgb(81.3, 81.3, 81
light:rgb(91.5, 91.5, 91.5
darker:rgb(50.7, 50.7, 50.
dark:rgb(40.5, 40.5, 40.5)
darkest:rgb(30.3, 30.3, 30
container-color:#0000;--md
container-color:#0000}@med
device-pixel-ratio:0){}</s
href="styles.css" media="p
onload="this.media='all'">
href="styles.css"></noscri
|   <body class="mat-app-b
bluegrey-lightgreen-theme">
|     <app-root></app-root
```

```
┌─[user@parrot]─[~/Desktop]
└──╼ $sudo ping -c 3 demo.owasp-juice.shop
PING demo.owasp-juice.shop (81.169.145.156) 56(84) bytes of data.
64 bytes from w9c.rzone.de (81.169.145.156): icmp_seq=1 ttl=238 time=103 ms
64 bytes from w9c.rzone.de (81.169.145.156): icmp_seq=2 ttl=238 time=102 ms
64 bytes from w9c.rzone.de (81.169.145.156): icmp_seq=3 ttl=238 time=117 ms

--- demo.owasp-juice.shop ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 102.358/107.645/117.238/6.795 ms
┌─[user@parrot]─[~/Desktop]
└──╼ $
```