Risk Management Report

1️⃣ Overview

On **Tuesday, June 17, 2025, at 17:33:30**, a vulnerability assessment was conducted against **demo.owasp-juice.shop** (IP address **81.169.145.156**, rDNS: **w9c.rzone.de**). The scan used an Nmap command with version detection, default scripts, and the `vuln` script to identify potential security weaknesses. This proactive measure aims to uncover vulnerabilities that could compromise the confidentiality, integrity, and availability of the Juice Shop environment.

2️⃣ Open Ports and Identified Services

The assessment detected three key network ports in various states:

- **Port 21/tcp (FTP)**: Open, running `ftpd.bin` round-robin file server version 3.4.0r16.
- **Port 25/tcp (SMTP)**: Filtered, with no version information provided.
- **Port 80/tcp (HTTP Proxy)**: Open, with an **F5 BIG-IP load balancer** acting as an HTTP proxy.

These services represent critical exposure points that, if improperly secured, could be leveraged by attackers to compromise the system.

3️⃣ Detailed Risk Analysis

A) FTP Service (Port 21)

The open FTP service poses an immediate security risk, especially considering that FTP transmits data, including credentials, in clear text. An improperly configured FTP server could allow unauthorized file transfers, leading to data exfiltration or unauthorized access to sensitive directories. Attackers could also perform brute-force attacks against weak user credentials. Given the nature of `ftpd.bin` as a round-robin file server, misconfiguration could result in unexpected file sharing among multiple hosts, exacerbating data leakage risks. It is recommended to replace FTP with secure alternatives like SFTP or FTPS and to restrict access using strong authentication and network-level controls.

B) HTTP Proxy (Port 80) — Apache Byterange Filter DoS (CVE-2011-3192)

The web server behind the F5 BIG-IP load balancer is susceptible to the well-known **Apache byterange filter Denial of Service vulnerability** (CVE-2011-3192). This issue allows an attacker to send multiple overlapping HTTP byte range headers to exhaust server resources, resulting in a service crash or severe degradation. Although this CVE is over a decade old, it remains exploitable if the server has not been patched or properly configured to limit byte range requests. The impact is a potential **Denial of Service (DoS)**, making the Juice Shop application unavailable to legitimate users, affecting user trust, and possibly violating availability commitments. Mitigation should include immediate patching of the Apache server, configuring the server to disable or limit byte range requests, and deploying a Web Application Firewall (WAF) to detect and block exploit attempts.

C) phpMyAdmin Interface — Local File Inclusion (CVE-2005-3299)

The scan indicates a possible **Local File Inclusion (LFI)** vulnerability in phpMyAdmin (CVE-2005-3299). Although the scan result is inconclusive, this known issue suggests that an attacker could exploit insecure input validation to read arbitrary files on the server through the `subform` parameter in `grab_globals.lib.php`. This can lead to unauthorized disclosure of configuration files, credentials, or other sensitive data, and may be used as a stepping stone to escalate privileges or compromise the entire database. Even if the LFI is only theoretical in this case, its presence highlights poor configuration or outdated phpMyAdmin versions. It is strongly recommended to restrict access to phpMyAdmin to trusted IPs, ensure the latest stable version is deployed, enforce strong authentication, and consider disabling phpMyAdmin entirely if it is not actively used for administrative purposes.

4️⃣ SMTP Service (Port 25)

Although the SMTP port is filtered and no version information was revealed, its presence implies that an email server may be accessible if not properly secured. Misconfigured or unsecured SMTP services can be abused for spam relay, phishing campaigns, or as an entry point for further attacks. It is advisable to confirm whether this service is necessary. If active, it should be hardened with proper authentication, spam controls, and access restrictions. If unused, the port should be closed to reduce the attack surface.

5️⃣ Overall Risk and Recommendations

The vulnerability assessment underscores critical gaps in patch management and secure configuration practices. The risks range from **service disruption** (Apache DoS) to **potential**

data breaches (LFI and open FTP). These vulnerabilities, while individually manageable, collectively increase the likelihood of compromise if not addressed promptly.

Recommended actions include:

- **Patch Management:** Apply all relevant security updates for Apache, phpMyAdmin, and related software immediately.

- **Service Hardening:** Replace insecure services like FTP with secure protocols; configure strict access controls for phpMyAdmin and limit it to internal use.

- **Network Controls:** Close unused ports, monitor all open ports for suspicious activity, and enforce firewall rules to block unauthorized connections.

- **Continuous Monitoring:** Implement regular vulnerability scans and intrusion detection to identify misconfigurations or new threats.

- **Incident Preparedness:** Develop and test an incident response plan to respond swiftly if these vulnerabilities are exploited.