🔎 Risk Analysis and Management

1. Local File Inclusion Vulnerability in phpMyAdmin (RSK-001)

A legacy vulnerability, **CVE-2005-3299**, was detected via a vulnerable phpMyAdmin component (`grab_globals.lib.php`). This Local File Inclusion (LFI) flaw may allow remote attackers to include local system files, potentially exposing sensitive data such as `/etc/passwd`. Given the critical nature of this asset and its widespread exploitation history, the risk is assessed as **High Likelihood** and **High Impact**, resulting in a **Critical Severity**. Immediate remediation includes removing or upgrading the phpMyAdmin instance and ensuring sensitive directories are protected or inaccessible through the web server.

2. Publicly Accessible FTP Service on Port 21 (RSK-002)

The FTP service running `ftpd.bin 3.4.0r16` is exposed on the public interface. FTP transmits credentials and data in plaintext, making it susceptible to interception and brute force attacks. The presence of such a service in a modern web architecture is a red flag. This risk is evaluated as **Medium Likelihood** due to attack feasibility and **High Impact** because of potential credential exposure, categorizing it as **High Severity**. Recommended actions include disabling the service if not essential or migrating to secure alternatives like SFTP or FTPS with robust authentication mechanisms.

3. Exposure of HTTP Proxy (F5 BIG-IP) on Port 80 (RSK-003)

Port 80 is open and serving via an F5 BIG-IP load balancer HTTP proxy. While the scan did not identify direct vulnerabilities, such infrastructure components are commonly targeted for misconfigurations and privilege escalation. Because no immediate flaw was detected, the **Likelihood is Low** but the **Impact could be Medium**, yielding a **Medium Severity** rating. Best practices involve reviewing configuration settings, applying updates, and limiting public access where feasible.

4. Presence of Admin Interfaces and Web Controls (RSK-004)

Evidence of admin pages or configuration interfaces (e.g., phpMyAdmin, cookie management scripts, and tracking JS) was found in the HTML response and behavior of the application. These are considered **Critical Assets** due to their control over application logic and data. Their exposure raises concerns of unauthorized access or information leakage. With a **Medium Likelihood** and **Medium Impact**, the **Severity is Medium**. Security controls should include access restrictions, authentication, and security logging on sensitive paths.

5. Filtered but Accessible SMTP Port (RSK-005)

Port 25 (SMTP) appears to be filtered but still reachable. While no vulnerability was confirmed, exposed SMTP services can be exploited for spam relaying, phishing attacks, or enumeration if misconfigured. The **Likelihood is Low**, but the **Impact is Medium**, leading to a **Low Severity**. Verification of server configuration and disabling unused mail services is strongly advised.

✅ Recommendations Summary

Risk ID	Recommendation
RSK-001	Remove or upgrade phpMyAdmin, restrict directory access.
RSK-002	Disable FTP, use secure file transfer protocols.
RSK-003	Audit proxy configurations, restrict exposure.
RSK-004	Lock down admin interfaces with authentication and ACLs.
RSK-005	Confirm or disable SMTP service, secure if necessary.

🧠 Conclusion

While OWASP Juice Shop is an intentionally insecure application, this risk assessment reflects realistic conditions often observed in poorly maintained production environments. The vulnerabilities and misconfigurations discovered pose serious risks if left unaddressed in a live context. By following the recommended mitigations, system administrators can significantly reduce the attack surface and strengthen the overall security posture of the environment.