🗒️ Risk Registry Report

🔴 R-001 – phpMyAdmin Local File Inclusion (CVE-2005-3299)

A critical vulnerability was identified in the phpMyAdmin component of the web application. This Local File Inclusion (LFI) vulnerability, tracked as CVE-2005-3299, allows attackers to access sensitive files on the server (such as `/etc/passwd`) by manipulating the `subform` parameter in the `grab_globals.lib.php` script. The likelihood of exploitation is high, and the impact is severe, as it could lead to privilege escalation or full system compromise. Immediate mitigation is recommended by disabling or removing the vulnerable phpMyAdmin instance, applying necessary patches, and restricting file access using proper permissions. The Web Application Administrator is responsible for addressing this issue.

🟠 R-002 – Login Page Brute-force Vulnerability

The login page is susceptible to brute-force attacks or credential stuffing, where attackers repeatedly attempt password combinations or reuse leaked credentials. Given its exposure and critical function, this risk has a medium likelihood but a high impact if exploited. It could result in unauthorized access to user or admin accounts. Mitigation steps include enforcing rate-limiting, implementing CAPTCHA mechanisms, and locking accounts after multiple failed login attempts. The Web Application Developer is tasked with implementing these security controls.

🟠 R-003 – Inferred Admin Panel Access

An administrative panel is suspected based on the application's structure, even though no explicit endpoint was discovered. This hidden or weakly protected access point could be targeted for privilege escalation, especially in known vulnerable platforms like Juice Shop. The risk has a medium likelihood and a high impact due to its potential to grant deep access to the application. Security Analysts should take action by identifying hidden endpoints, verifying authentication mechanisms, and applying Role-Based Access Controls (RBAC).

🟠 R-004 – Outdated FTP Service

An FTP service was found running on the target system, and it appears to be outdated. FTP is an insecure protocol often exploited for unauthorized access or file manipulation, especially when it lacks encryption or allows anonymous login. The likelihood of exploitation is high, with a moderate impact if attackers are able to upload or download sensitive files. It is recommended

that the FTP service be replaced with a secure alternative such as SFTP, and that strong authentication be enforced. Anonymous login should be disabled. The Network Administrator should oversee this remediation.

🟡 R-005 – Public Metadata & Outdated JavaScript

The web application includes outdated JavaScript libraries (e.g., jQuery 2.2.4) and publicly accessible scripts. This introduces the potential for Cross-Site Scripting (XSS) vulnerabilities, particularly if inputs are not properly sanitized. The risk has a medium likelihood and medium impact, as it may allow attackers to inject malicious scripts affecting user sessions. Front-End Developers should update all external libraries, implement strict Content Security Policies (CSP), and sanitize user inputs to minimize this exposure.

🟠 R-006 – HTTP Proxy Misconfiguration

The application appears to utilize an open or misconfigured HTTP proxy, which presents opportunities for Man-in-the-Middle (MITM) attacks or cache poisoning. Attackers could potentially intercept or modify communications, leading to session hijacking or data leakage. With a medium likelihood and high impact, this risk should be promptly addressed. Infrastructure Leads must audit the proxy configuration, apply Access Control Lists (ACLs), and validate HTTP headers to secure this vector.

🟢 R-007 – Filtered SMTP Port (Port 25)

Port 25, commonly used for SMTP email traffic, appears to be filtered but may still indicate a running mail service. Misconfigured mail servers can be exploited to send spam or relay phishing emails, though the likelihood of such exploitation is low. The impact is moderate if abused. As a precaution, the Email Server Administrator should verify whether the SMTP service is necessary, monitor outbound mail activity, and apply strict firewall rules to limit access.