Configuration and Deployment Management Testing

1. Introduction

Configuration and deployment management testing focuses on identifying flaws related to the server's configuration, the application's platform, and the files and directories it serves. A misconfigured server or application can expose sensitive information, create unintended functionality, or allow unauthorized access. This section of the test ensures that the web server, application server, and the application itself are securely configured and do not reveal any unnecessary information that could aid an attacker.

2. CVSS Score Summary

Test Case	Vulnerability	CVSS v3.1 Score	CVSS Vector	Severity
OTG-CONFIG-001	Information Disclosure (Open Ports/Services)	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Medium
OTG-CONFIG-002	Information Disclosure (PHP/Apache Info)	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Medium
OTG-CONFIG-003	File Extensions Handling	0.0	N/A	Informational
OTG-CONFIG-004	Old, Backup, and Unreferenced Files	0.0	N/A	Informational

OTG-CONFIG-005	Enumerate Admin Interfaces	0.0	N/A	Informational
OTG-CONFIG-006	Insecure HTTP Methods Enabled	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	Medium
OTG-CONFIG-007	Missing HSTS Header	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Medium
OTG-CONFIG-008	RIA Cross-Domain Policy	0.0	N/A	Informational

3. Summary of Findings

The most significant findings in this category are related to information disclosure. The application and server are overly verbose, revealing details about the network infrastructure, running services, and the full PHP and Apache configuration. This information could be leveraged by an attacker to mount more targeted attacks. Additionally, several potentially insecure HTTP methods are enabled, and the application is missing the HTTP Strict Transport Security (HSTS) header, leaving it more susceptible to man-in-the-middle attacks.

A key challenge during this test was the absence of the `ffuf` and `gobuster` tools, which prevented the successful execution of the file extension and backup file checks (OTG-CONFIG-003 and OTG-CONFIG-004). While the other tests were completed successfully, the inability to perform these checks leaves a potential gap in the assessment of the application's configuration security.

4. General Recommendation/Remediation

- **Restrict Access to Services:** The open ports for `msrpc`, `microsoft-ds`, and `vmware-auth` should be firewalled from public access unless absolutely necessary. If they are required, they should be restricted to trusted IP addresses.
- **Disable Unnecessary HTTP Methods:** The web server should be configured to only allow necessary HTTP methods, such as `GET` and `POST`. The `PUT`, `DELETE`, `PATCH`, `TRACK`, and `DEBUG` methods should be disabled.
- **Implement HSTS:** The `Strict-Transport-Security` header should be implemented to enforce the use of HTTPS, which helps to prevent man-in-the-middle attacks.
- **Reduce Server Verbosity:** The web server should be configured to not reveal detailed version information in its banners and error pages. The `phpinfo()` page should be removed from the

production environment.

- **Install and Use File Discovery Tools:** To ensure a complete assessment, security testing tools such as `ffuf` and `gobuster` should be installed and used to identify potentially sensitive files and directories.