PTES Report

1) Executive Summary (PTES)

A penetration test was conducted against the Drupal web application to identify security weaknesses that could be exploited by an attacker. During testing, the application was found to be running **Drupal version 7.31**, which is affected by a known critical vulnerability (**CVE-2014-3704 – Drupageddon**). This flaw allows unauthenticated remote attackers to execute arbitrary commands on the server. Successful exploitation resulted in access to the Drupal application directory and sensitive configuration files. The vulnerability poses a critical risk as it enables full compromise of the web application and potential exposure of backend systems. Immediate remediation is required to reduce the attack surface and prevent unauthorized access.

2) Findings

The Drupal application discloses its version via publicly accessible files, enabling attackers to identify vulnerable instances. Exploitation of the Drupageddon vulnerability allowed unauthenticated remote code execution with web-server privileges. The attacker was able to access **/var/www/drupal** and retrieve sensitive configuration files such as **settings.php**, exposing database credentials. This confirms complete application compromise and a high likelihood of further exploitation, including data theft and privilege escalation.

3) Recommendations

- Upgrade Drupal to the latest supported version immediately
- Apply all vendor security patches
- Remove public access to version disclosure files
- Restrict file permissions on sensitive directories
- Deploy a Web Application Firewall (WAF)
- Perform a rescan after patching to verify remediation effectiveness

4) Non-Technical Management Summary

The security assessment identified a critical weakness in the Drupal web application caused by outdated software. This flaw allows attackers to gain unauthorized access without needing login credentials. During testing, the vulnerability was successfully exploited, demonstrating the risk of data exposure and system compromise. If left unpatched, attackers could misuse this access to steal information or disrupt services. Updating the application, applying security patches, and validating fixes through a follow-up scan will significantly reduce risk. Prompt action is strongly recommended to protect business data and maintain system integrity.