01
Vulnerability Scanning Lab

Critical Web Vulnerabilities

Findings:

1. ***rlogin Passwordless Login***

   Host: 192.168.225.129

   CVSS Score / Severity: Critical (Score: 10)

   The rlogin service allows remote users to log in as root without requiring a password, leading to full compromise of the target system. This vulnerability allows attackers to gain complete control over the host.

   Remediation:

   Disable the rlogin service immediately and replace it with secure alternatives such as SSH. Ensure that password authentication and key-based authentication are properly configured to prevent unauthorized access.

2. **TWiki XSS and Command Execution Vulnerabilities**

   Host: 192.168.225.129

   Port: 80/tcp

   CVSS Score / Severity: 10.0 (Critical)

   CVE IDs: CVE-2008-5304, CVE-2008-5305

   TWiki versions prior to 4.2.4 have XSS and eval-injection flaws allowing script injection and command execution via %URLPARAM{} and %SEARCH{}.

   Remediation:

   Upgrade TWiki to v4.2.4 or later; if upgrade is not immediately possible, disable or restrict access to TWiki and apply web application filtering rules (WAF).

3. **Possible Backdoor: Ingreslock**

   Host: 192.168.225.129:1524/tcp

   Severity / CVSS: Critical (10)

Service responds as root (uid=0), indicating an installed backdoor that allows arbitrary command execution and full compromise.

Remediation:

Isolate the host, perform a full incident response & forensic cleanup or rebuild from known-good images; change all credentials and block the service.

4. **rexec service running (unencrypted remote exec)**

   Host: 192.168.225.129:512/tcp

   Severity / CVSS: Critical (10) — CVE-1999-0618 referenced

   rexec sends credentials in cleartext and permits remote command execution.

   Remediation:

   Disable/remove rexec and any inetd entry; require SSH with strong authentication and firewall off access to the port.

5. **Operating System End-of-Life (Ubuntu 8.04)**

   Host: 192.168.225.129 (OS detection)

   Severity / CVSS: Critical (10)

   Host runs an EOL OS that receives no security updates (high risk of unpatched vulnerabilities).

   Remediation:

   Upgrade OS to a supported, patched release or rebuild host with current supported distribution; apply hardened baseline.

6. **Distributed Ruby (dRuby/DRb) — Multiple RCE vectors**

   Host: 192.168.225.129:8787/tcp

   Severity / CVSS: Critical (10)

   DRb server allows submission of commands/objects; observed syscall responses indicate possible remote code execution.

   Remediation:

   Disable/stop DRb if unused; if required, restrict access via ACLs/firewall, run service with least privilege and $SAFE >= 2 plus input tainting.

7. **MySQL / MariaDB Default Credentials (root with empty password)**

   Host: 192.168.225.129:3306/tcp

   Severity / CVSS: Critical (9.8)

   Able to authenticate as root with empty password — full DB compromise risk. Multiple CVEs referenced.

   Remediation:

   Immediately set strong passwords for all DB accounts (no root with empty password), rotate credentials, restrict access by network/firewall and enable least-privilege DB users.

8. **Apache Tomcat AJP RCE (Ghostcat) — AJP connector disclosure**

   Host: 192.168.225.129:8009/tcp

   Severity / CVSS: Critical (9.8) — CVE-2020-1938 referenced

   AJP connector allows reading webapp files (e.g., /WEB-INF/web.xml) and may enable RCE.

   Remediation:

   Disable AJP connector if unused, or apply vendor patches (Tomcat versions fixed); restrict AJP to localhost/firewall and update Tomcat to fixed versions.

9. **PHP CGI (php-cgi) vulnerabilities — multiple CVEs (PHP <5.3.13, 5.4.x <5.4.3)**

   Host: 192.168.225.129:80/tcp (cgi-bin/php)

   Severity / CVSS: Critical (9.8)

   CGI setup allows passing command-line switches to php-cgi, enabling source disclosure and remote code execution (demonstrated phpinfo execution).

   Remediation:

   Patch/upgrade PHP to fixed versions (≥5.3.13 or ≥5.4.3) or migrate away from CGI setup; apply WAF rules and restrict access to CGI endpoints.

10. **vsftpd Compromised Source Package Backdoor (vsftpd 2.3.4)**

    Host: 192.168.225.129:21/tcp and 192.168.225.129:6200/tcp

    Severity / CVSS: Critical (9.8) — CVE-2011-2523 referenced

    Tainted vsftpd package contains a backdoor opening a shell on port 6200; allows arbitrary command execution.

Remediation:
Remove affected vsftpd package, replace with vendor-signed fixed package, verify package signatures, and block the backdoor port; rebuild host if compromise suspected.

Escalation Email

Subject: Urgent Security Escalation – Critical Vulnerabilities Detected on Host 192.168.225.129

Dear Developer Team,

During recent security scanning, host 192.168.225.129 was found to have multiple critical vulnerabilities, including backdoors, unencrypted remote services, an EOL OS, default credentials, RCE-prone services, and weak passwords. These issues collectively expose the host to full system compromise.

Immediate action is required:
Isolate the host from the network.
Conduct a full forensic investigation.
Patch or upgrade all affected services.
Remove insecure or unused applications.
Enforce strong authentication and access controls.
Rebuild compromised systems if needed.

These flaws pose an extreme risk to organizational assets and data integrity. Urgent attention from security operations and IT leadership is recommended.

Regards,
AISWARYA T S
VAPT INTERN