

## Lewistech.co.ke Website Penetration Test

**Results: Found open ports 80 (HTTP) and 443 (HTTPS)**

### 2: Scanning for Vulnerabilities

- Used Burp Suite to scan for **OWASP Top 10** vulnerabilities.
- Identified issues:
  - Password Leak Vulnerability
  - Misconfigured HTTP headers

### Step 3: Exploitation

- Confirmed **password leak** vulnerability via Burp Suite's Repeater tool.
- Demonstrated proof of concept without compromising sensitive data.

### Step 4: Reporting and Fixing

- Shared findings with developers. Collaborated to fix:
  - Enforced strong password policies
  - Fixed misconfigured headers

### Step 5. Findings

| Vulnerability             | Description              | Severity | Status |
|---------------------------|--------------------------|----------|--------|
| Password Leak             | Weak password protection | High     | Fixed  |
| Misconfigured HTTP Header | Missing security headers | Medium   | Fixed  |

### Conclusion

The penetration test successfully identified critical vulnerabilities. Collaboration with developers ensured all issues were fixed, improving the website's security.