Results: Open ports 22 (HTTP) and 443 (HTTPS).

## Step 2: Vulnerability Scanning

- Conducted OWASP vulnerability tests using **Burp Suite**.
- Key Findings:
  - o **SQL Injection Vulnerability** on login form.
  - o **Cross-Site Scripting (XSS)** on search bar.

## Step 3: Exploitation

- Demonstrated how SQL injection can expose sensitive user information.
- Proof of Concept for XSS vulnerability showed risk of script injection.

---

## Step 4. Findings

| Vulnerability | Description | Severity | Status |
|---|---|---|---|
| SQL Injection | Weak input validation on login form | Critical | Reported |
| Cross-Site Scripting | Lack of input sanitization | High | Reported |

---

## Step 5. Recommendations

- **SQL Injection**: Implement parameterized queries and input validation.
- **XSS**: Sanitize all user inputs and encode output properly.

---

## Step 6. Conclusion

The penetration test revealed critical vulnerabilities on **Kai & Karo.com**. Recommendations were provided to developers to mitigate risks.