Problem Statement:

We need to evaluate the security posture of a publicly hosted endpoint. Please perform a comprehensive scan of the following endpoint:

<http://www.itsecgames.com/>

Objectives:

* Identify vulnerabilities on this domain name. You can use any publicly available tools. But you have to pull up the report and show the vulnerability reported by the tool.
* Detect potential vulnerabilities (misconfigurations, outdated software, CVEs).
* Assess SSL/TLS configuration and certificate health.
* Highlight any exposed information that could aid attackers (headers, banners, error messages).
* Provide a prioritized list of findings along with mitigation recommendations.

**Findings:**

**1.DNS Lookup (nslookup)**

* Your DNS requests timed out repeatedly, showing "Unknown" server and no response.
* This could be a local DNS resolver issue or network blockage, as the site is reachable via HTTP.
* Implication: Limited DNS information hinders initial reconnaissance but does not affect live testing.

**2. HTTP Headers (curl -I)**

* Server identified as Apache.
* Headers like Last-Modified, ETag, Accept-Ranges, and Content-Type are present.
* No security headers such as X-Content-Type-Options, Content-Security-Policy, Strict-Transport-Security, X-Frame-Options are detected.
* Website serves content over HTTP only, not HTTPS.

**3.Potential Vulnerabilities Detected**

**Misconfigurations**

* **Missing Security Headers:** The server is missing critical headers like:
  + Content-Security-Policy (CSP)
  + X-Content-Type-Options: nosniff
  + X-Frame-Options
  + Referrer-Policy
  + Permissions-Policy
* **Enabled HTTP OPTIONS Method:** Can enable reconnaissance or probing attacks.
* **Security.txt Missing:** No designated vulnerability disclosure channel.

**Outdated Software & Known CVEs**

* Server software identified as **Apache HTTP Server** (version details not specified but likely outdated due to no recent update headers).
* Use of **Google Font API** scripts.
* No direct CVE data from scans, but exposure to known Apache vulnerabilities is possible if the server is unpatched.

**4. SSL/TLS Configuration and Certificate Health**

* The website only serves content over **HTTP (port 80)** without redirecting to HTTPS.
* SSL certificate presented for <https://www.itsecgames.com/> shows **domain mismatch** and no valid alternate names for the requested domain.
* This causes browser warnings and insecure communication.
* No evidence of HTTP Strict Transport Security (HSTS) headers present.
* Risk from lack of encryption includes interception, manipulation, and credential theft.

**5. Exposed Information that Could Aid Attackers**

* **Server Banner Disclosure:** The Server: Apache header reveals the web server technology.
* **Absence of Security Headers:** Opens risks for Cross-Site Scripting (XSS), Clickjacking, MIME sniffing, and referrer leakage.
* **HTTP Only Communication:** Data transmitted in cleartext vulnerable to man-in-the-middle attacks.
* **Miscellaneous Headers:** Last-Modified, ETag, Accept-Ranges headers allow resource fingerprinting and caching attacks.

**6. Prioritized Findings and Mitigation Recommendations**

| **Priority** | **Finding** | **Risk/Impact** | **Recommended Mitigations** |
| --- | --- | --- | --- |
| High | HTTP only with no HTTPS | Data interception, MITM, credential theft | Obtain and configure a valid SSL certificate, enforce HTTPS redirects |
| High | SSL certificate domain mismatch | User distrust, insecure communication | Install correctly matched SSL certificate for the domain |
| High | Missing Content-Security-Policy | Vulnerable to Cross-Site Scripting (XSS) | Implement robust CSP headers to restrict sources and scripts |
| High | Missing X-Content-Type-Options | Allows MIME sniffing and related attacks | Add X-Content-Type-Options: nosniff header |
| Medium | Missing X-Frame-Options | Vulnerable to clickjacking | Add X-Frame-Options: SAMEORIGIN or equivalent protection |
| Medium | Server header reveals software | Targeted attacks based on known vulnerabilities in server | Remove or obfuscate server headers |
| Medium | Enabled HTTP OPTIONS method | Reconnaissance, potential exploit vector | Disable HTTP OPTIONS method if not required |
| Medium | Missing security.txt file | Delayed vulnerability reporting | Create and publish security.txt per standards |
| Low | Exposure through caching headers | Resource fingerprinting, cache poisoning | Evaluate necessity of ETag and Last-Modified headers |

**Summary**

* The endpoint <http://www.itsecgames.com/> is **intentionally vulnerable** for training purposes and exhibits numerous security weaknesses including lack of encryption, missing important HTTP security headers, and server information exposure.
* Immediate priority should be placed on **implementing HTTPS with a valid certificate** and **adding critical security headers**.
* Secondary priorities include improving disclosure mechanisms with a security.txt file, disabling unnecessary HTTP methods, and removing server identifying headers.
* Addressing these areas will significantly improve the security posture and reduce attack surface.