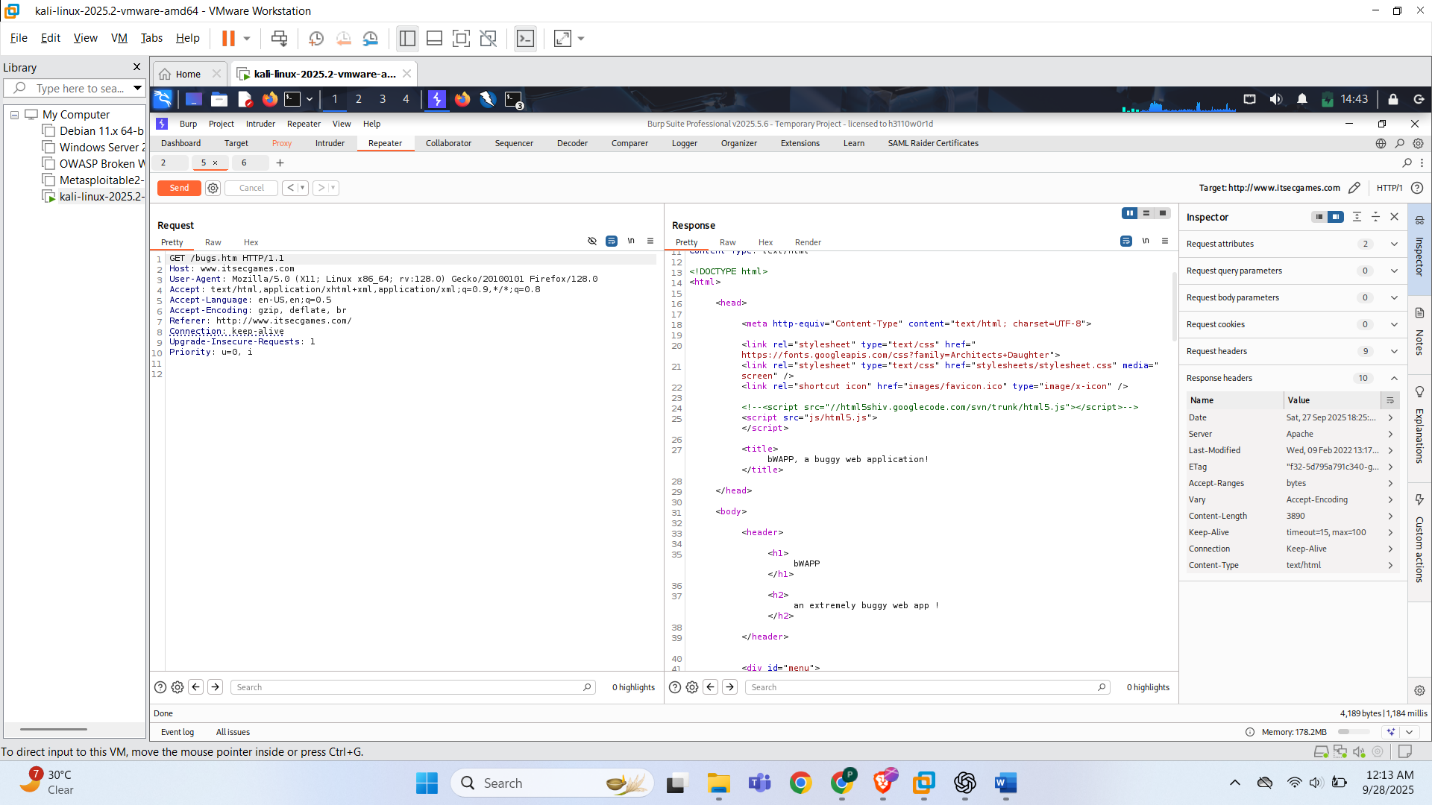
**Job Title: Security Officer Trainee**

* **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/>

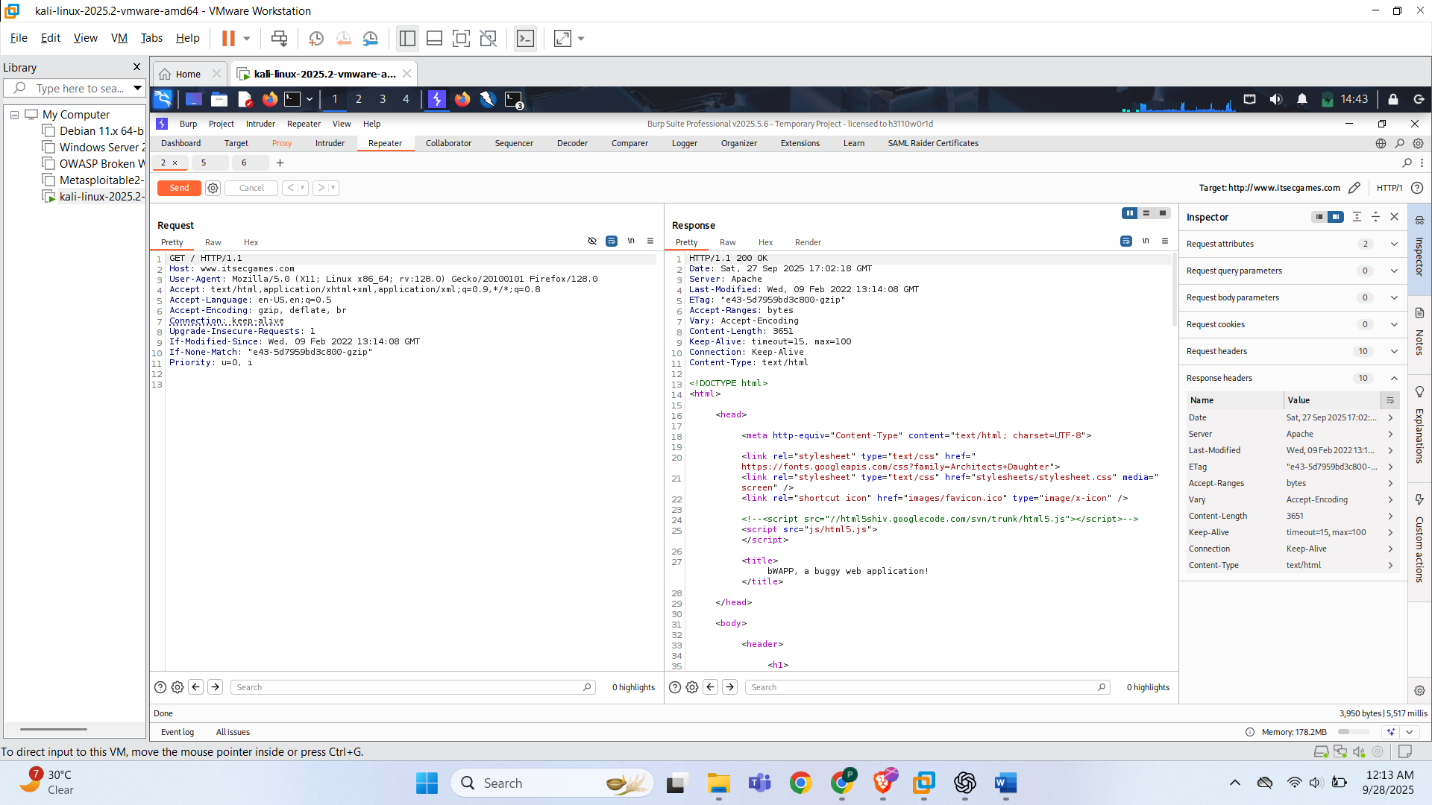
1. **there are no X-Frame-Options header and no Content-Security-Policy header visible**, so the site appears to allow framing. That’s the first required check for a clickjacking/vector framing issue.

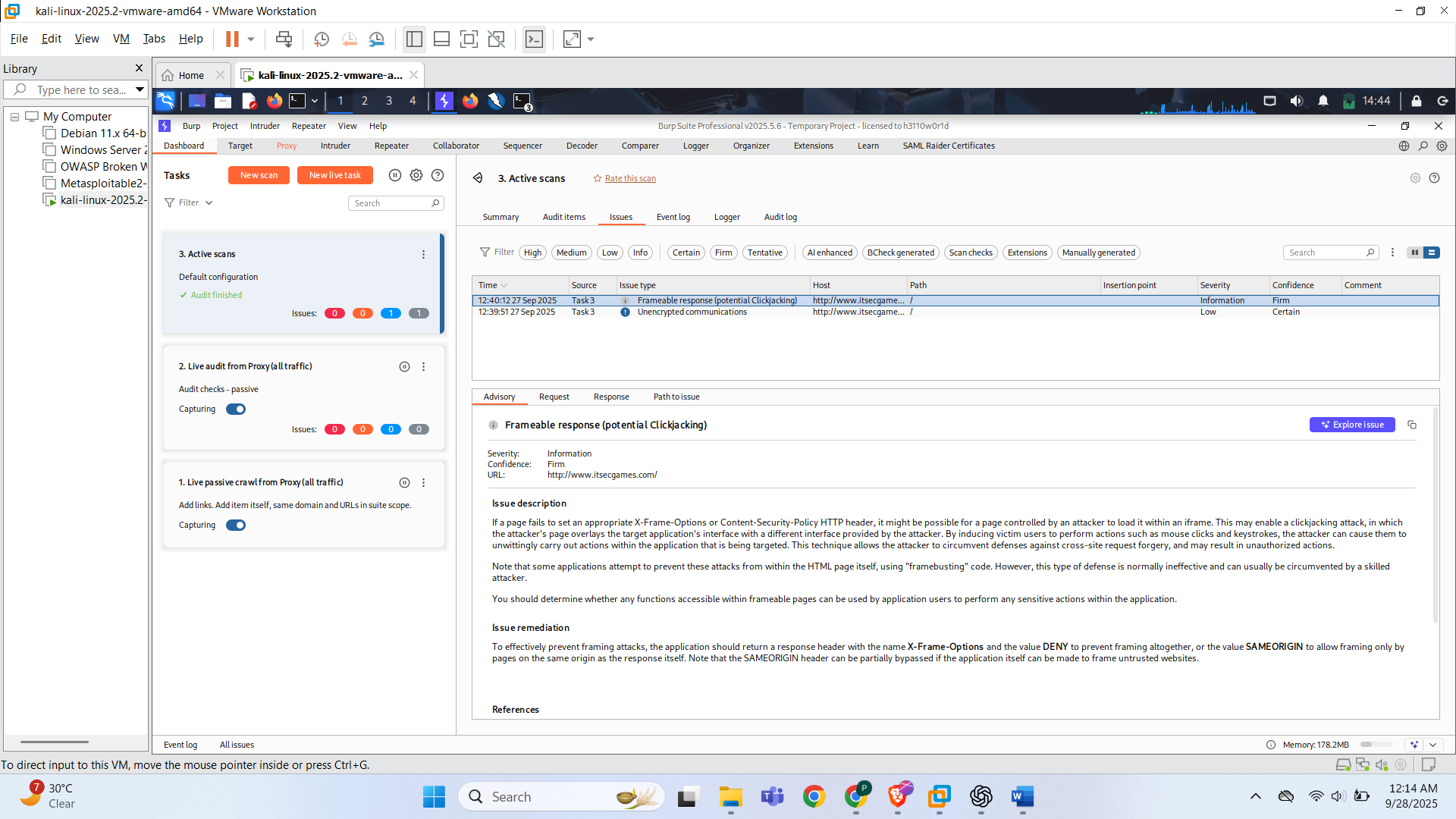
the site does not set X-Frame-Options nor a CSP frame-ancestors directive, so it can be framed. That means framing/clickjacking protection is missing and the site is vulnerable to clickjacking (impact depends on what UI actions exist).



**Title:** Missing frame-ancestors / X-Frame-Options — Clickjacking possible  
**Severity:** Medium

**Impact:** An attacker can embed the site and trick users into performing unintended actions (clicks, form submissions) — risk depends on the functionality available to authenticated users.





**Remediation** (apply one of these server-side headers)

* Content-Security-Policy: frame-ancestors 'self';
* X-Frame-Options: DENY

or

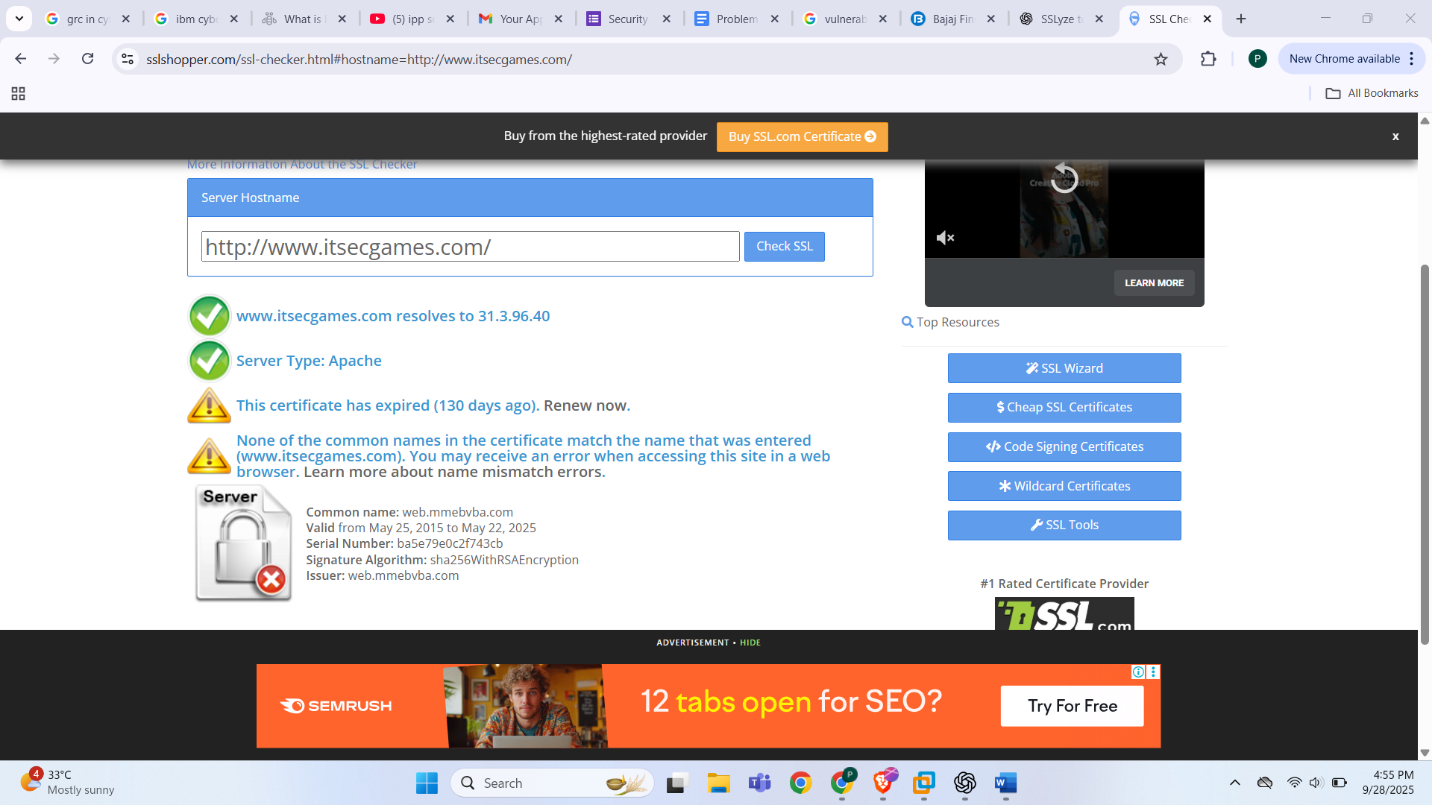
* X-Frame-Options: SAMEORIGIN
* Use always (Apache) / always flag (Nginx add header) so answers from error pages/CDNs still include header.
* Use CSP frame-ancestors for fine-grain control and compatibility with modern browsers; keep X-Frame-Options as a fallback for older browsers.

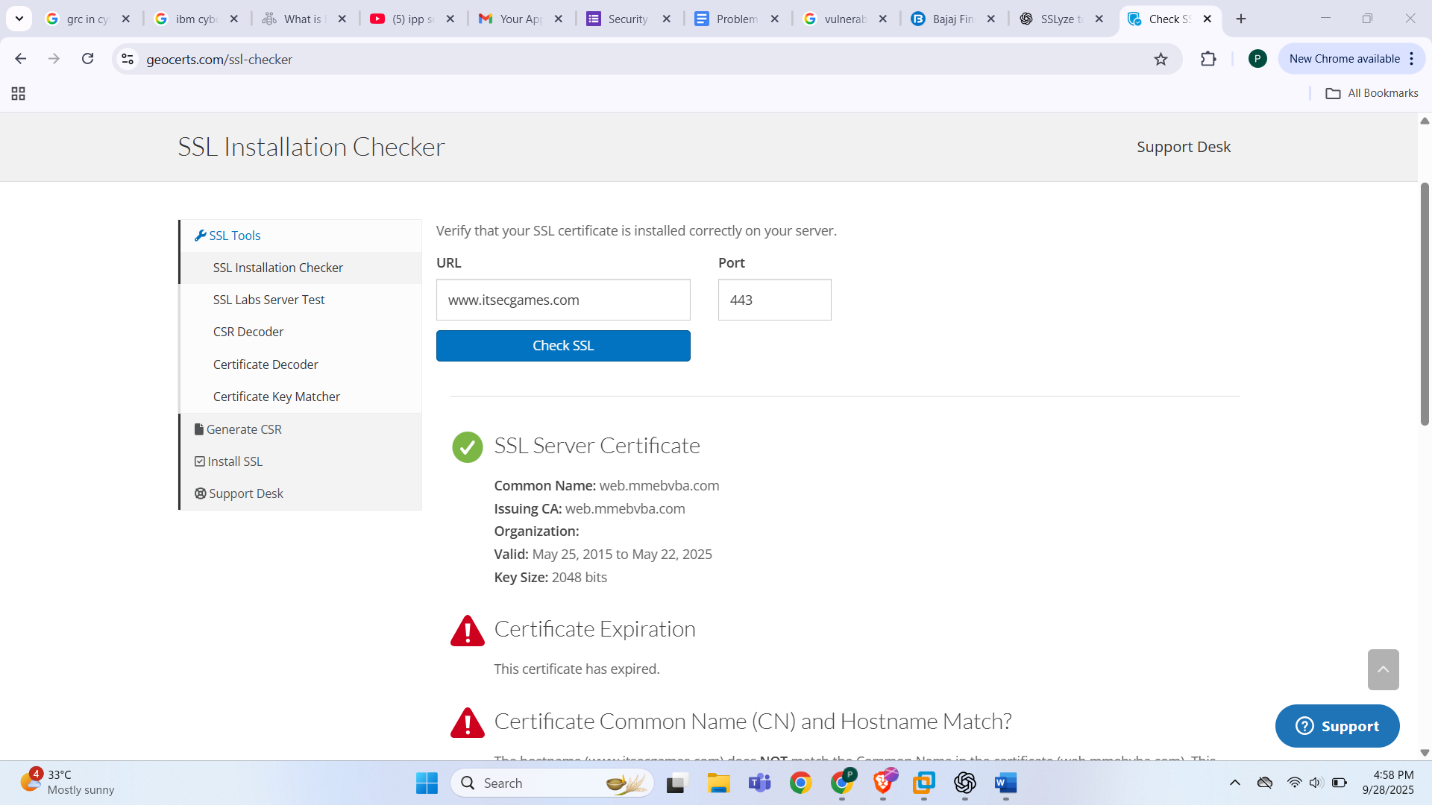
1. **SSL/TLS Certificate Misconfiguration (Self-signed / Expired)**

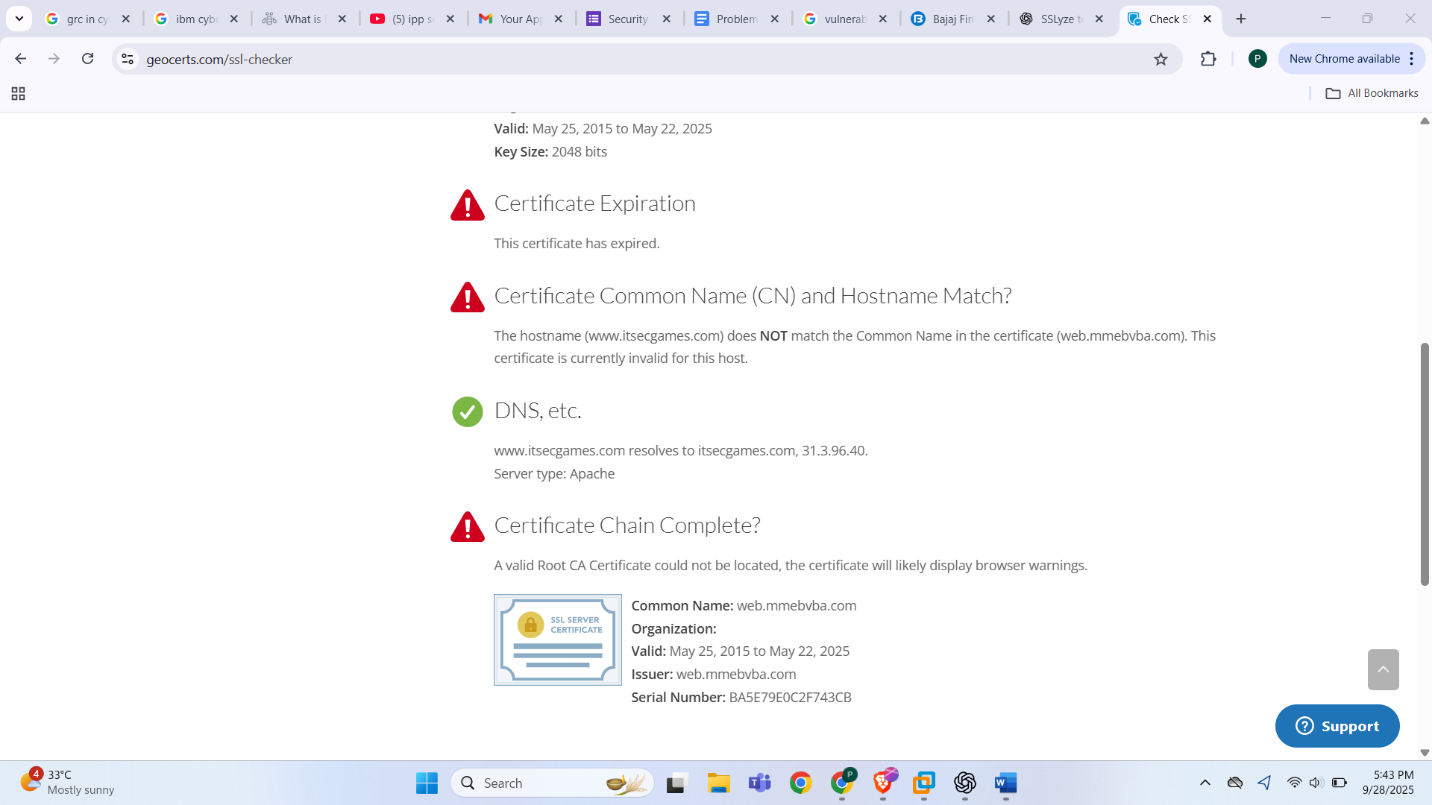
Self-signed and expired TLS certificate; certificate chain untrusted and OCSP stapling not configured — allows browser warnings and enables MITM risk

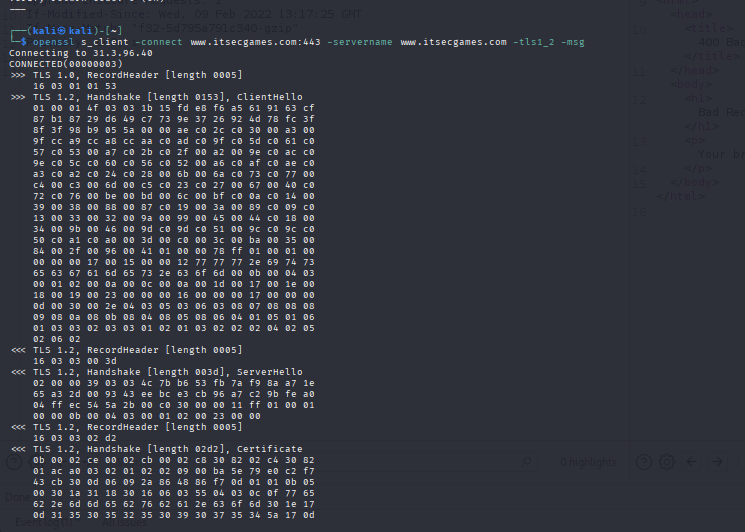
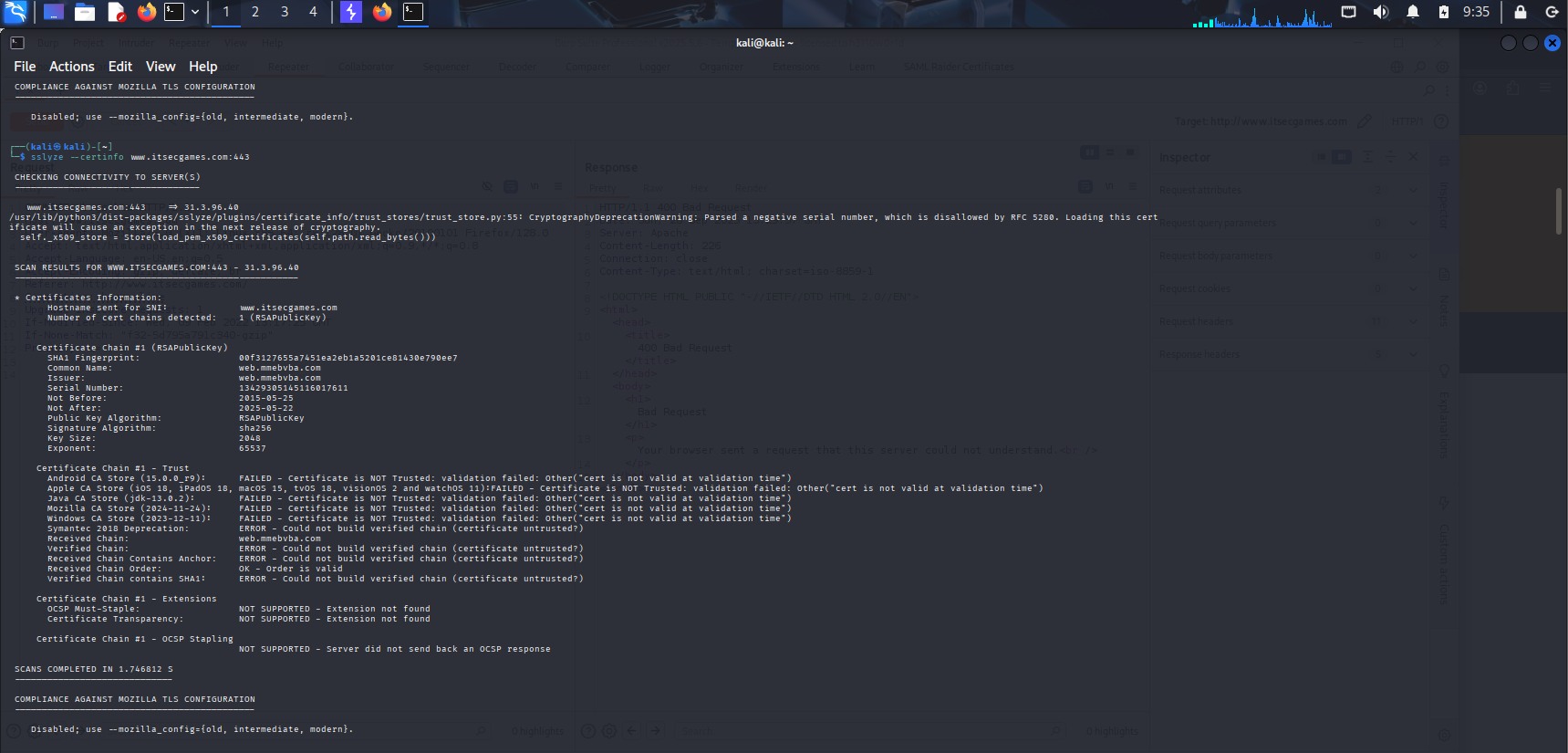
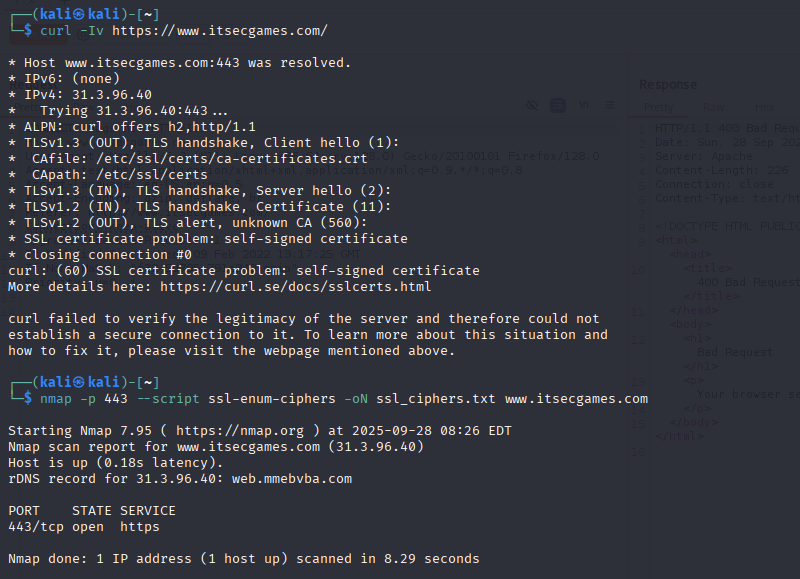
The server presents a certificate that is not trusted by public CA stores (self-signed/issuer = web.mmebvba.com) and the certificate validity ended May 22, 2025. An expired / untrusted certificate breaks HTTPS guarantees (confidentiality, integrity, auth) and exposes users to phishing/MITM and degraded trust. Immediate remediation required.

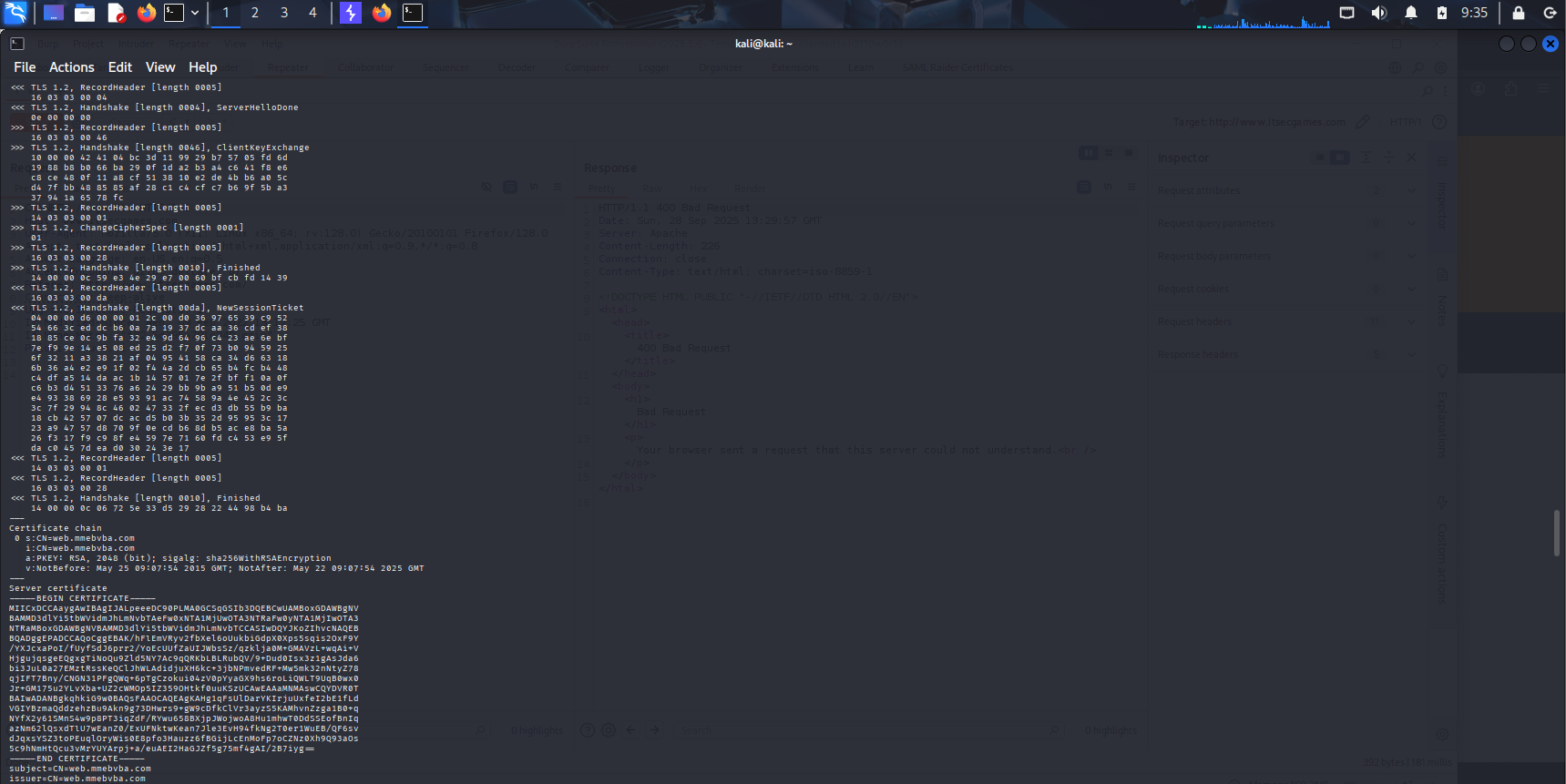
Internet-facing TLS with invalid/untrusted certificate prevents normal TLS validation; attackers can impersonate site; users will receive browser warnings and may ignore them, exposing credentials or session tokens.

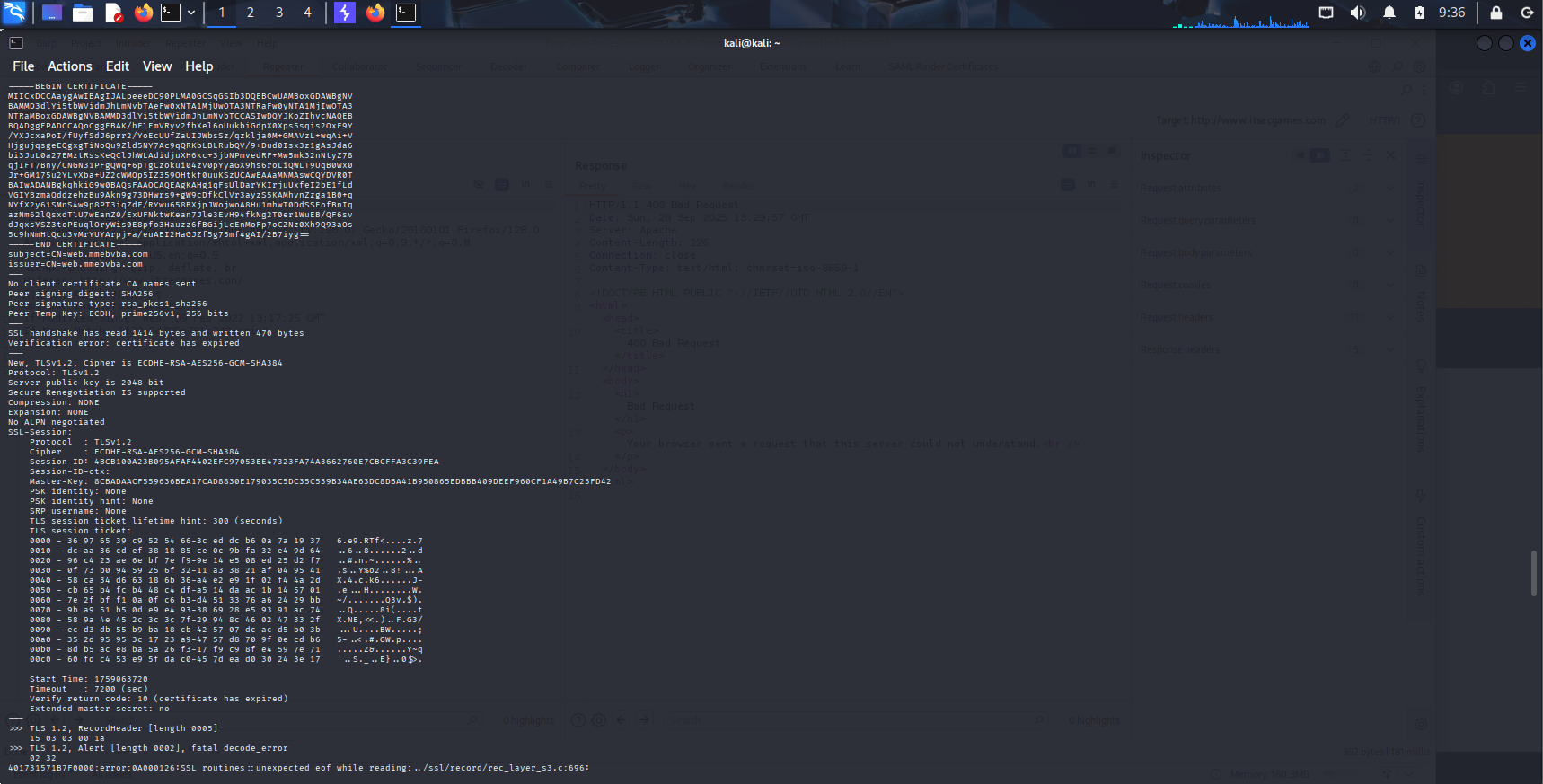












**Impact**

* Authentication broken: Browser cannot verify server identity → users see warnings; attackers can perform MITM attacks (intercept credentials, session cookies, sensitive data) or phish users.
* Trust & user experience: Visitors get security warnings that reduce trust and usage.
* Automated clients / APIs: May fail to connect or silently accept invalid certs if misconfigured.
* Regulatory / compliance: Noncompliant with basic TLS best practices, may violate internal security policies.

**Recommended**

* Install the full certificate chain (include intermediate certificates) in Apache SSLCertificateFile / SSLCertificateChainFile (or combined PEM) so clients can validate the chain.
* Don't use self-signed certs for public/production sites. Use self-signed only for internal dev environments.
* Enable OCSP stapling to improve revocation performance and reliability (sample Apache config below).
* Rotate certs & automate renewal (Let’s Encrypt + cron/systemd timer / certbot auto renewal). Avoid multi-year certificates without automation

1. **Nikto scan**



1. **Zap scan**

Frameable response (Potential Clickjacking)

Unencrypted Communications

**Remediation:**

* Implement HTTPS (TLS 1.2 or TLS 1.3) for all communications.
* Redirect HTTP → HTTPS.
* Configure HSTS (HTTP Strict Transport Security)
* Add security headers in the HTTP response