Vulnerability Assessment Report: toscrape.com

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	http		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 35.211.122.109
+ Target Hostname: toscrape.com
+ Target Port: 80
+ Start Time: 2026-01-31 05:10:53 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Server leaks inodes via ETags, header found with file /, fields: 0x63e40de9 0xf63
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 26 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2026-01-31 05:11:22 (GMT0) (29 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- http://books.toscrape.com
- http://quotes.toscrape.com/js
- http://quotes.toscrape.com/scroll
- http://quotes.toscrape.com
- http://quotes.toscrape.com/js-delayed
- http://quotes.toscrape.com/search.aspx
- http://quotes.toscrape.com/login
- http://quotes.toscrape.com/tableful
- http://quotes.toscrape.com/random
- http://quotes.toscrape.com/

4. Vulnerabilities Detected

- Missing Security Headers

5. Vulnerability Intelligence (CVE Mapping)

Vulnerabilities in nginx
- CVE-2009-2629: Buffer underflow in src/http/ngx_http_parse.c in nginx 0.1.0 through 0.5.37, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.15 allows ...
- CVE-2009-3896: src/http/ngx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x befor...
- CVE-2009-3898: Directory traversal vulnerability in src/http/modules/ngx_http_dav_module.c in nginx (aka Engine X) before 0.7.63, and 0.8.x before 0.8.17, allows rem...
- CVE-2009-4487: nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or ...
- CVE-2010-2263: nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or unparsed content of arbitrary...

6. Attack Possibilities & Mitigation

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.