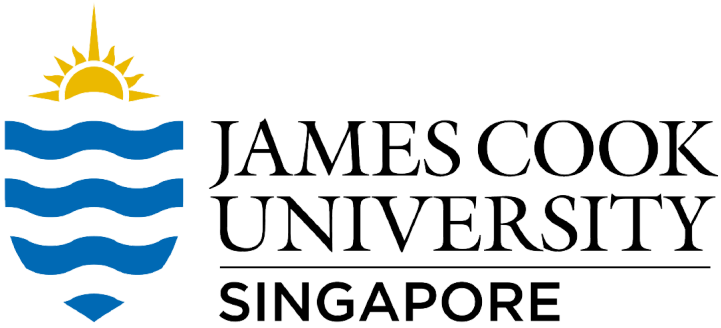


CP3418 - Best Practices in Cybersecurity

Assessment Item 3- Report

Lecturer : Dr.Steve Kerrison & Dr.Hari Krishnan

11th April, 2025

TR1S, 2025

Penetration Testing Report

Target: http://inspectorio.com
Testers: Austin Liandro, Zwe Sett Aung , Bryan Colin
Date: 11th April, 2025

Executive Summary

This report summarizes a black-box penetration test performed against the publicly accessible infrastructure of **Inspectorio.com**, a platform hosted on **Vercel**, a modern frontend cloud provider. The goal was to identify potential vulnerabilities and misconfigurations that could pose security risks to users and data.

1. Reconnaissance

1.1 Target Identification

Tool Used: nslookup.io

IP Address Identified: 76.76.21.21

Speed Scan: `100 packets per second`

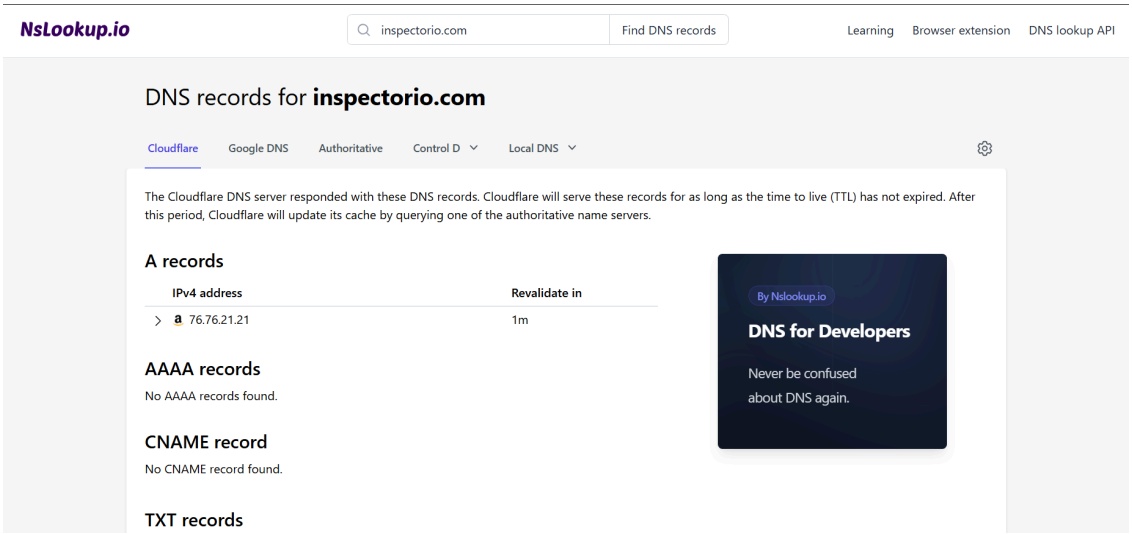
Hosting Provider Identified: Vercel

Other IPs Observed: 66.33.60.66, 76.76.21.98

1.2 SSL Certificate and WHOIS Analysis

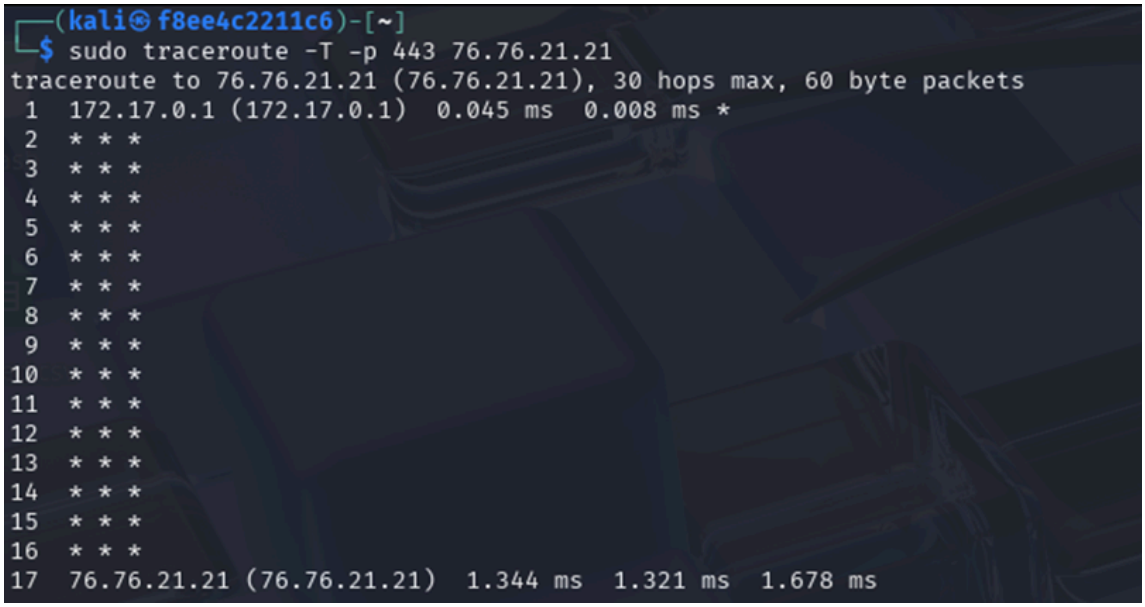
- **SSL Issuer:** Let's Encrypt

- **TLS Versions:** TLSv1.2, TLSv1.3
- Certificate Subject: www.silkworldwide.com



1.3 Traceroute

- Host responds successfully.
- Multiple intermediate hops (2–16) are unresponsive, suggesting firewall or ICMP filtering.
- Confirms Vercel employs layered network security.



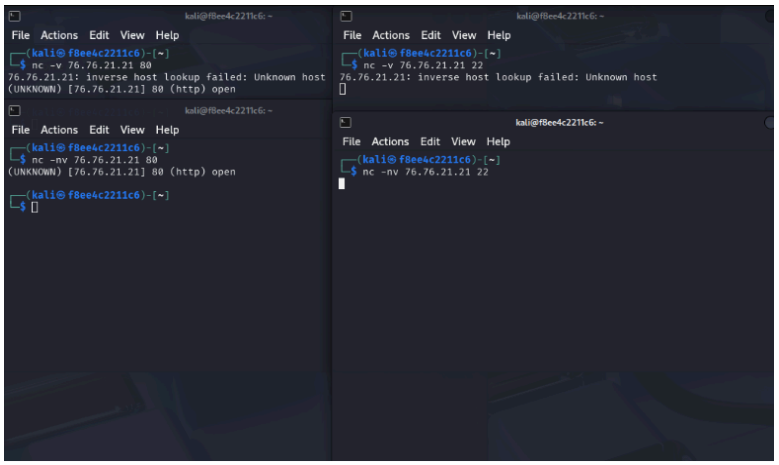
2. Scanning

2.1 Port Scanning (Masscan & Nmap)

- **Only Open Ports:** 80 (HTTP) and 443 (HTTPS)
- **Observation:** 65,533 ports filtered. Likely due to firewall.
- **Conclusion:** Target is hardened against unauthorized access.
- **Version**: Reverse Proxy by Vercel, Golang

2.2 Service Enumeration

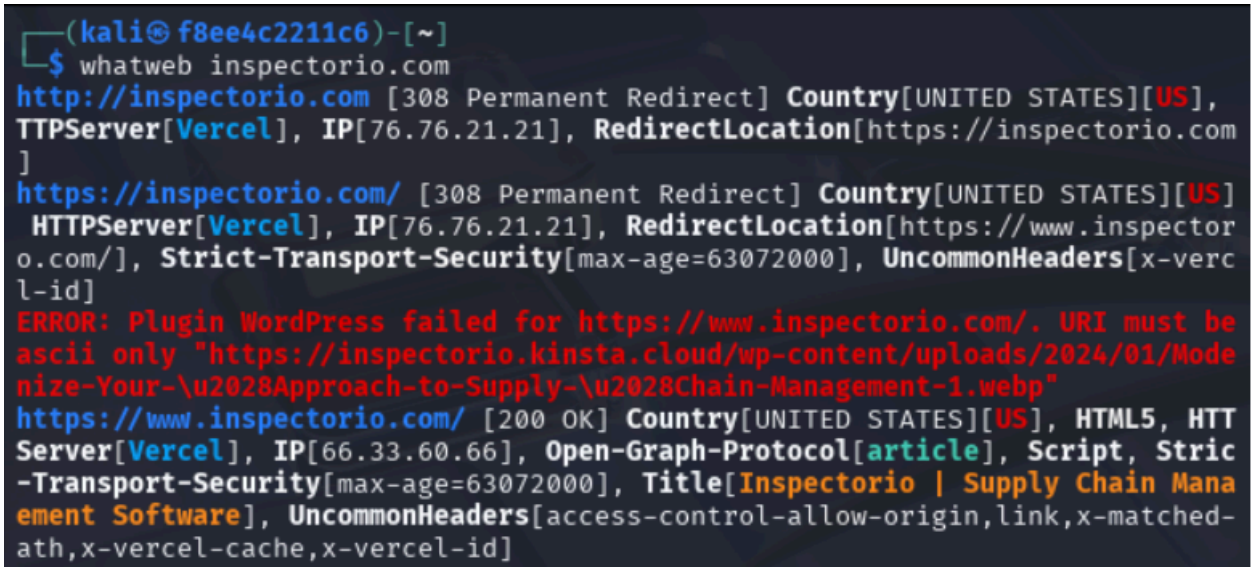
- **Banner Grabbing via Telnet and Netcat:**
    - Port 80: Returns 308 Permanent Redirect to https://vercel.com
    - Port 21, 22, 25: No response (closed/filtered)
- **Server Details:**
    - Server: Vercel
    - X-Vercel-Id suggests Singapore data center.



3. Technology Stack Identification

3.1 WhatWeb Scan

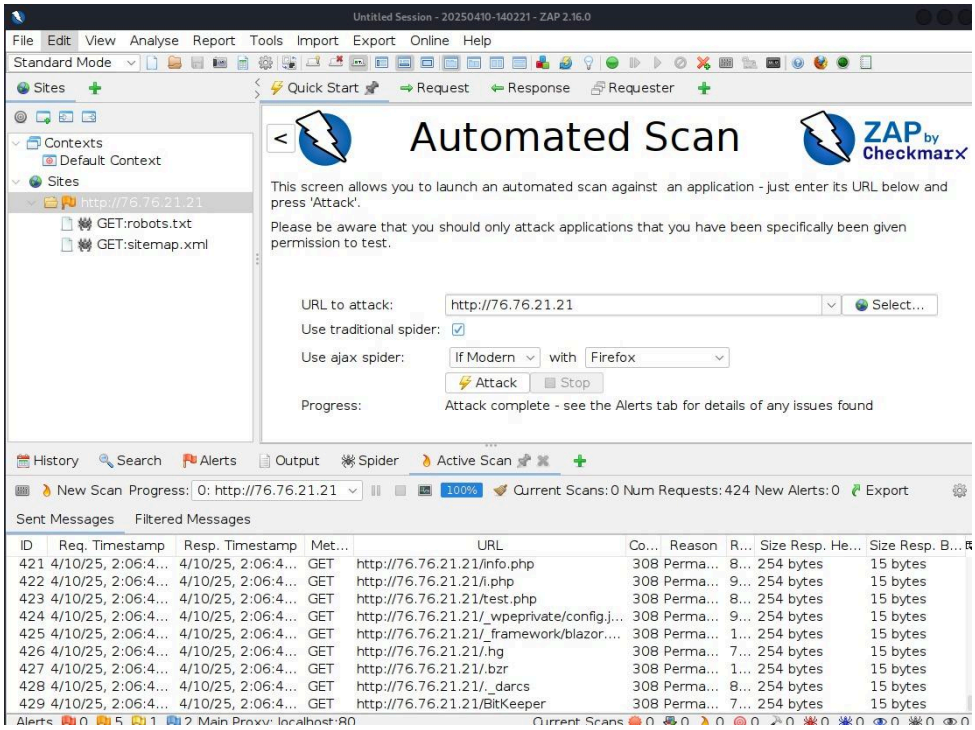
- Hosted on Vercel
- Web Server: HTTPServer[Vercel]
- Technologies Detected: HTML5, JavaScript Modules, possibly WordPress
- Redirects:
    - *http://inspectorio.com → https://inspectorio.com → https://www.inspectorio.com*
- WordPress Evidence: /wp-content/uploads/ URLs on kinsta.cloud

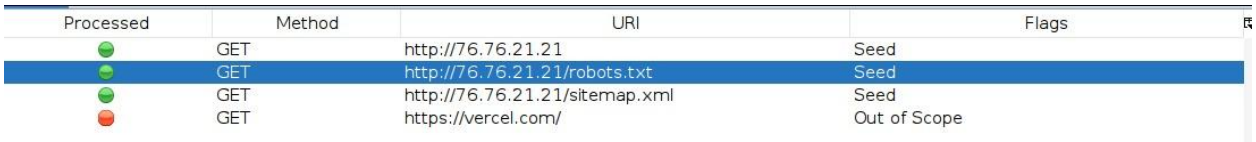


4. Enumeration & Crawling

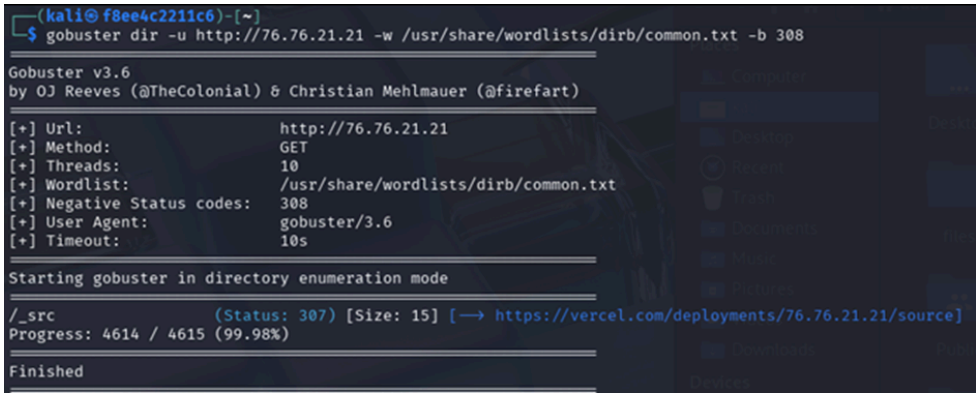
4.1 Directory & File Enumeration

- **Tools:** Gobuster, OWASP ZAP
- */src* redirects to Vercel deployment panel.
- */robots.txt* and */sitemap.xml*: Inaccessible via direct IP.
- Using 307 indicates a temporary redirect.





- Gobuster



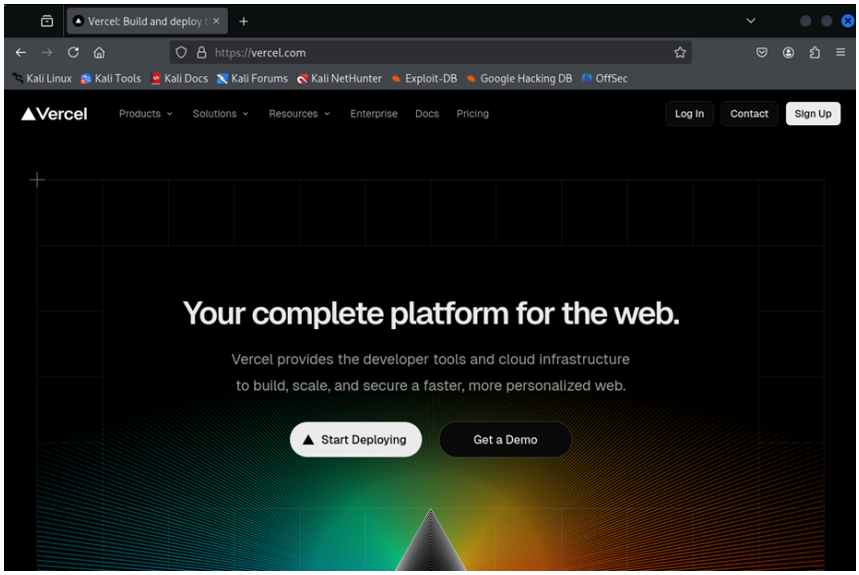
- Result: “src (Status: 307) [Size: 15] [--> https://vercel.com/deployments/76.76.21.21/source]”.

- The site hosted on Vercel and direct access attempts were being redirected to Vercel’s deployment panel.

To confirm website access, Manually Visited:

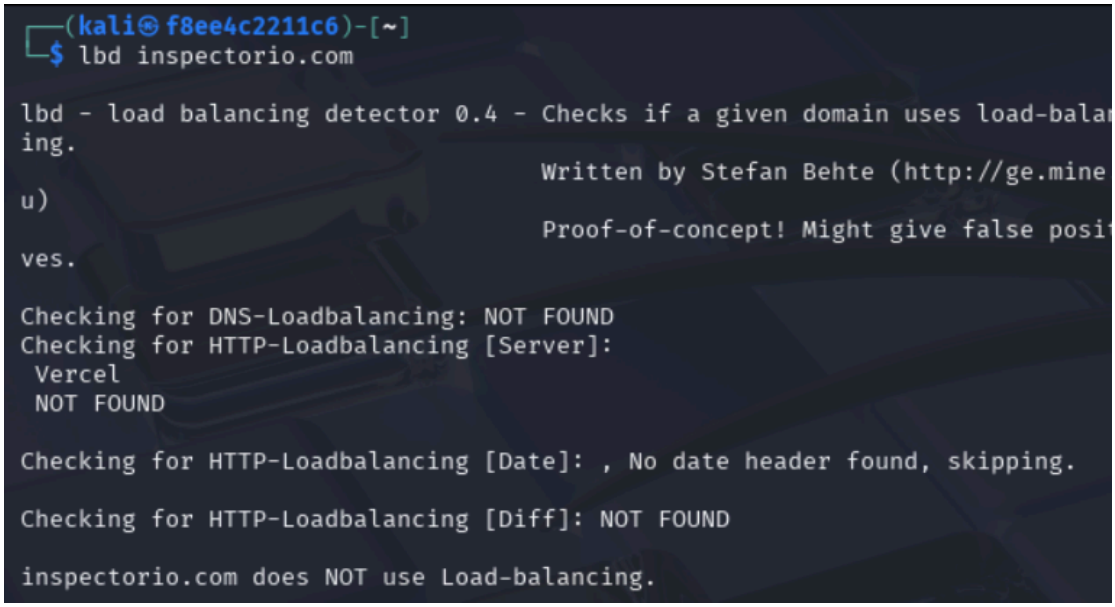
http://76.76.21.21 (Port 80) and https://76.76.21.21 (Port 443)

Both directed to Vercel website without any error:



4.2 DNS Load Balancing Check

- **Tool:** LBD
- **Result:** No DNS or HTTP load balancing detected.



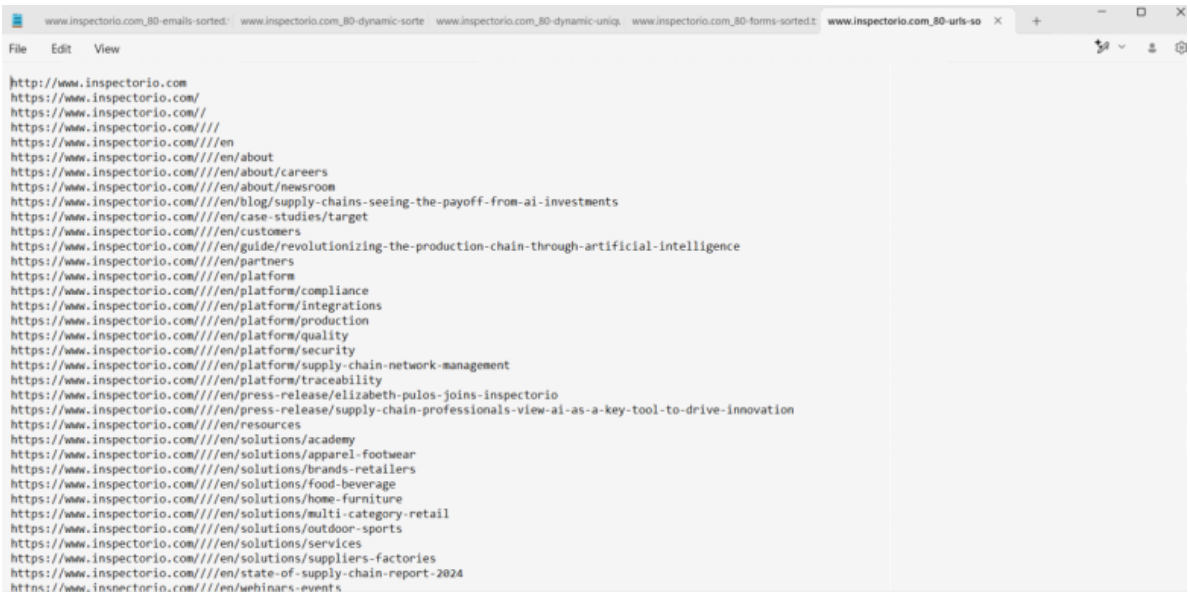
4.3 Crawling

- **Tools:** BlackWidow
- **Identified URLs:** General Site Pages, Dynamic URLs.
- **Email Address Enumeration:**
    - Abby.Nelson@ketnergroup.com
    - contact@inspectorio.com

- **Key Observations from Crawling:**

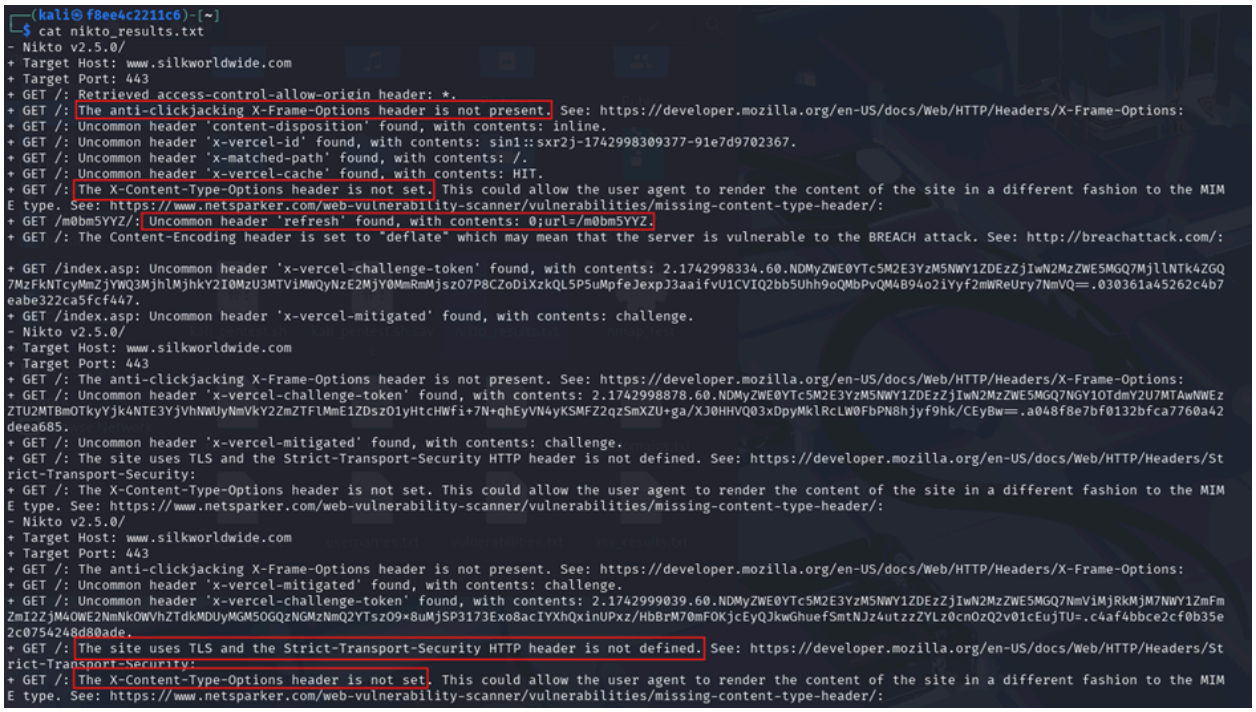
The platform depends significantly on **Vercel** and potentially **Kinsta** for backend services.

- **Redundant or improperly structured URLs** may leave the site vulnerable to:
    - URL-based enumeration
    - Misrouting or cache poisoning
- **Publicly accessible email addresses** represent a risk vector for phishing or impersonation-based attacks.



5. Vulnerability Assessment

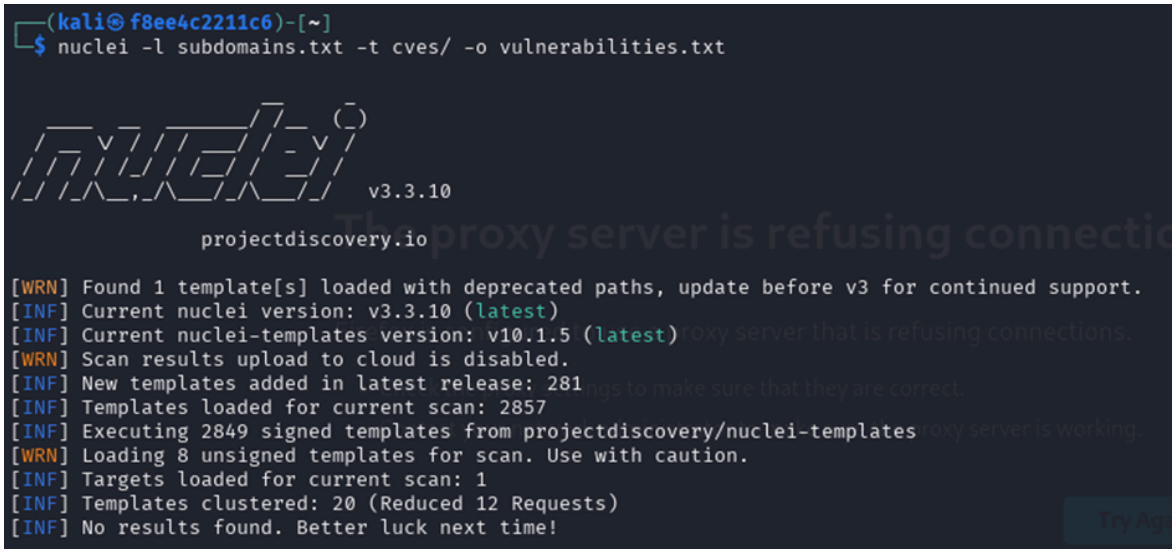
5.1 Nikto Scan



- **Missing Headers:**
    - X-Frame-Options: Vulnerable to clickjacking
    - X-Content-Type-Options: MIME sniffing risk
    - Strict-Transport-Security: Weak HTTPS enforcement
- Other Issues:
    - Content-Encoding: deflate: May enable BREACH attacks
    - Refresh header: Indicates auto-redirect behavior.

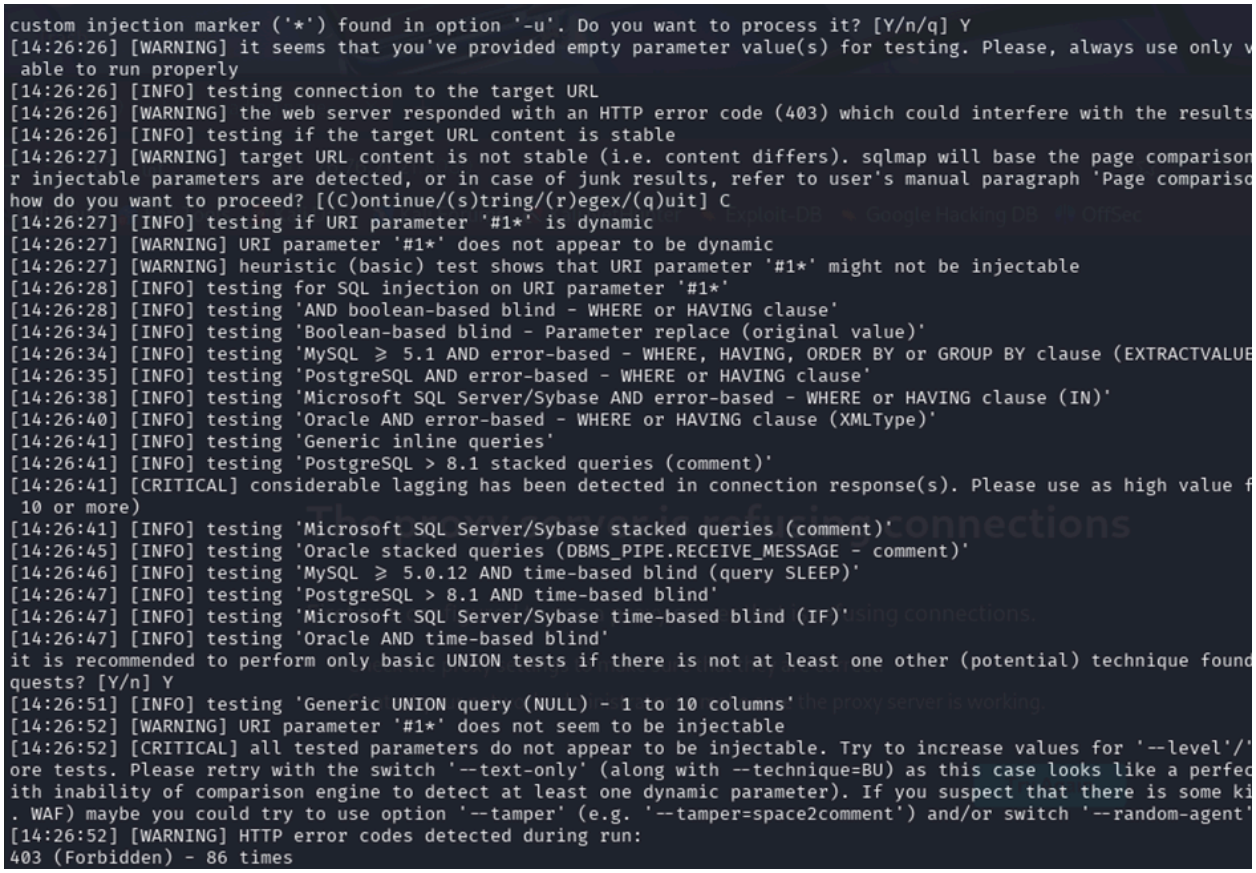
5.2 Nuclei

- Getting SQLMap scanning.
- Getting the tech stack analysis information.
- Didn't get any vulnerability.



5.3 SQLMap

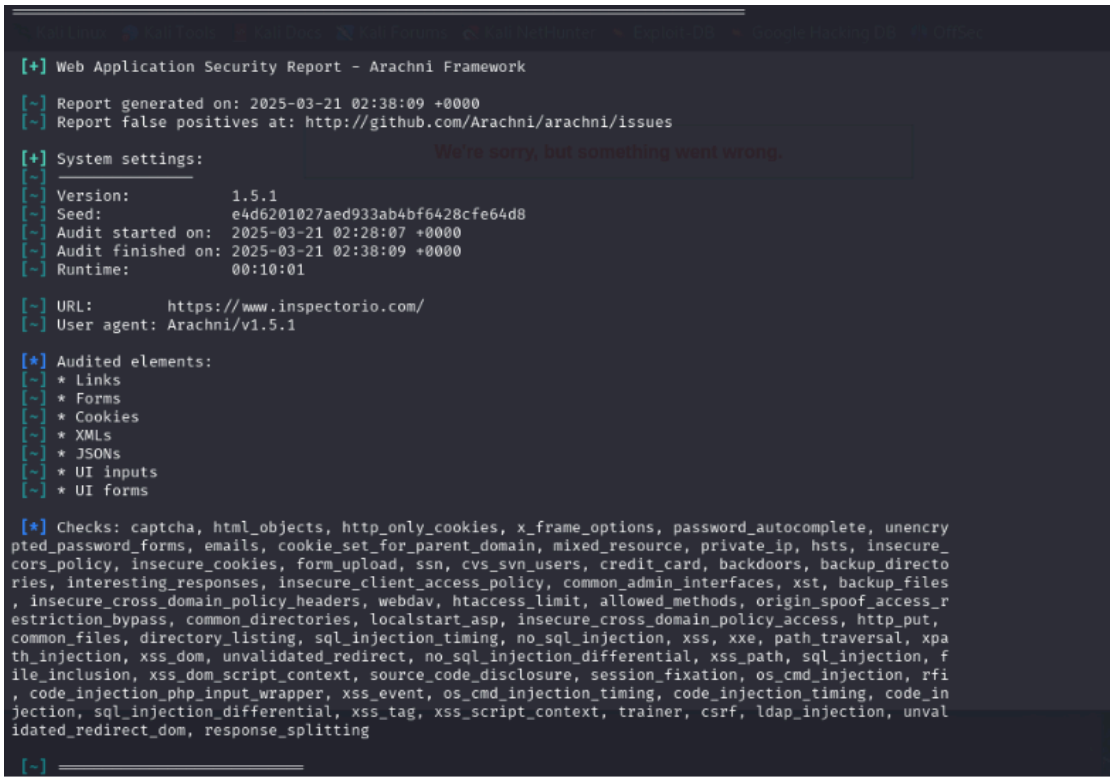
Scan Results:



```
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[14:26:26] [WARNING] it seems that you've provided empty parameter value(s) for testing. Please, always use only v
 able to run properly
[14:26:26] [INFO] testing connection to the target URL
[14:26:26] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results
[14:26:26] [INFO] testing if the target URL content is stable
[14:26:27] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison
r injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page compariso
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
[14:26:27] [INFO] testing if URI parameter '#1*' is dynamic
[14:26:27] [WARNING] URI parameter '#1*' does not appear to be dynamic
[14:26:27] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[14:26:28] [INFO] testing for SQL injection on URI parameter '#1*'
[14:26:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:26:34] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:26:34] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE
[14:26:35] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[14:26:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[14:26:40] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[14:26:41] [INFO] testing 'Generic inline queries'
[14:26:41] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[14:26:41] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value f
 10 or more)
[14:26:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[14:26:45] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[14:26:46] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[14:26:47] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[14:26:47] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[14:26:47] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found
quests? [Y/n] Y
[14:26:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:26:52] [WARNING] URI parameter '#1*' does not seem to be injectable
[14:26:52] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'
ore tests. Please retry with the switch '--text-only' (along with --technique=BU) as this case looks like a perfec
ith inability of comparison engine to detect at least one dynamic parameter). If you suspect that there is some ki
. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[14:26:52] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 86 times
```

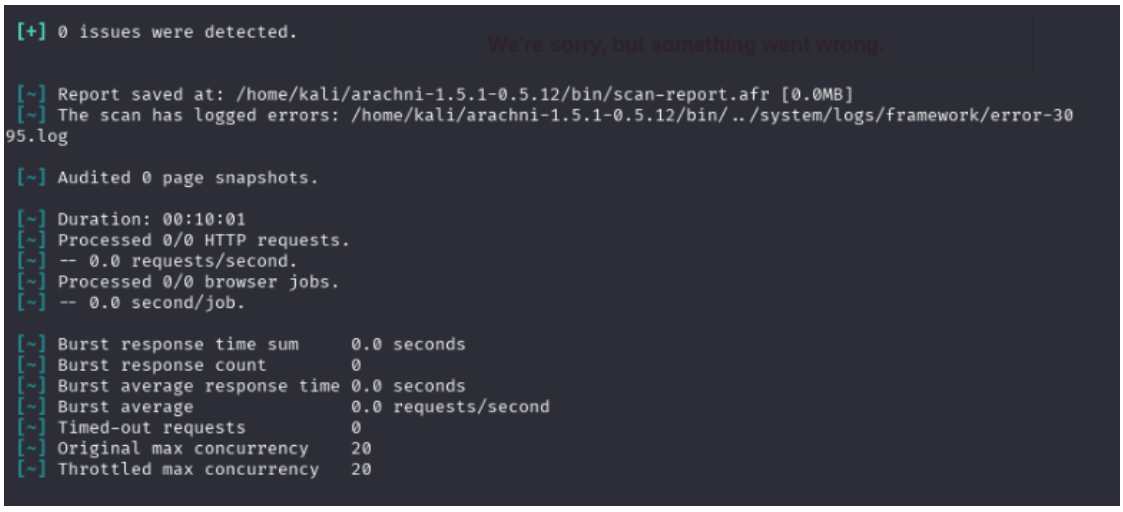
- All requests returned HTTP 403 Forbidden
- Dynamic content interferes with payload testing
- Likely protected by WAF or security restrictions
- The Parameter tested did not appear to be injectable (#1)

5.4 Arachni



```
[+] Web Application Security Report - Arachni Framework

[~] Report generated on: 2025-03-21 02:38:09 +0000
[~] Report false positives at: http://github.com/Arachni/arachni/issues

[+] System settings:
[~] ----------------
[~] Version:          1.5.1
[~] Seed:             e4d6201027aed933ab4bf6428cfe64d8
[~] Audit started on:  2025-03-21 02:28:07 +0000
[~] Audit finished on: 2025-03-21 02:38:09 +0000
[~] Runtime:          00:10:01

[~] URL:        https://www.inspectorio.com/
[~] User agent: Arachni/v1.5.1

[*] Audited elements:
[~] * Links
[~] * Forms
[~] * Cookies
[~] * XMLs
[~] * JSONs
[~] * UI inputs
[~] * UI forms

[*] Checks: captcha, html_objects, http_only_cookies, x_frame_options, password_autocomplete, unencry
pted_password_forms, emails, cookie_set_for_parent_domain, mixed_resource, private_ip, hsts, insecure_
cors_policy, insecure_cookies, form_upload, ssn, cvs_svn_users, credit_card, backdoors, backup_directo
ries, interesting_responses, insecure_client_access_policy, common_admin_interfaces, xst, backup_files
, insecure_cross_domain_policy_headers, webdav, htaccess_limit, allowed_methods, origin_spoof_access_r
estriction_bypass, common_directories, localstart_asp, insecure_cross_domain_policy_access, http_put,
common_files, directory_listing, sql_injection_timing, no_sql_injection, xss, xxe, path_traversal, xpa
th_injection, xss_dom, unvalidated_redirect, no_sql_injection_differential, xss_path, sql_injection, f
ile_inclusion, xss_dom_script_context, source_code_disclosure, session_fixation, os_cmd_injection, rfi
, code_injection_php_input_wrapper, xss_event, os_cmd_injection_timing, code_injection_timing, code_in
jection, sql_injection_differential, xss_tag, xss_script_context, trainer, csrf, ldap_injection, unval
idated_redirect_dom, response_splitting

[~] ========================
```

- The scan completed, but no security issues were found.
- Possible Reasons:
    - WAF/Cloudflare blocked scan requests.
    - Arachni was unable to execute payloads due to JavaScript protections.



```
[+] 0 issues were detected.


[~] Report saved at: /home/kali/arachni-1.5.1-0.5.12/bin/scan-report.afr [0.0MB]
[~] The scan has logged errors: /home/kali/arachni-1.5.1-0.5.12/bin/../system/logs/framework/error-30
95.log

[~] Audited 0 page snapshots.

[~] Duration: 00:10:01
[~] Processed 0/0 HTTP requests.
[~] -- 0.0 requests/second.
[~] Processed 0/0 browser jobs.
[~] -- 0.0 second/job.

[~] Burst response time sum     0.0 seconds
[~] Burst response count        0
[~] Burst average response time 0.0 seconds
[~] Burst average               0.0 requests/second
[~] Timed-out requests          0
[~] Original max concurrency    20
[~] Throttled max concurrency   20
```

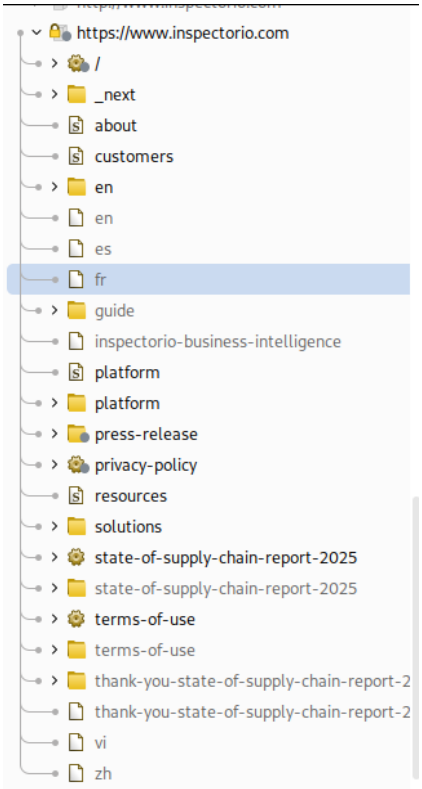
6. Web Application Analysis

6.1 Entry Points Mapping

Using Burp Suite Professional, a full crawl of the web application was performed to enumerate all accessible routes and files on **https://www.inspectorio.com**.

Mapped Entry Points Included:

- Root and common paths: /, /about, /customers
- Language-specific directories: /en, /es, /fr
- Functional modules:
    - /platform, /solutions, /resources
    - /inspectorio-business-intelligence
    - /press-release, /privacy-policy, /guide



Entry Points

These entry points serve as the primary surface for testing user inputs, redirects, enumeration attempts, and injection payloads.

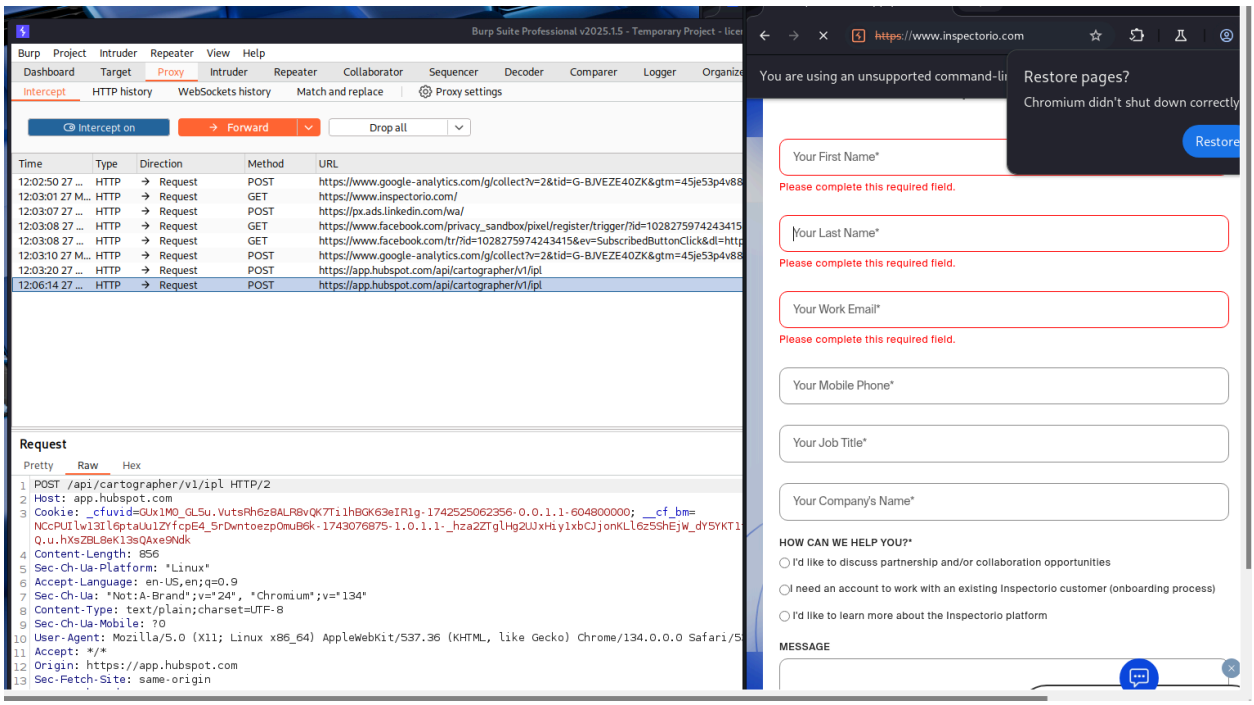
6.2 Input and Form Testing (Burp Suite Pro)

One of the most prominent interactive elements was the **“Request a Demo” form**.

- Location: **https://www.inspectorio.com**
- Submission Endpoint: **https://app.hubspot.com/api/cartographer/v1/ipl**

Form Fields Included:

- Full name
- Work email
- Job title
- Mobile number
- Company name



Observation

Although found on Inspectorio, the form submission is processed by **HubSpot**.

Manual Manipulation:

- The form was intercepted, modified, and replayed.
- Payloads were injected to test for reflected or stored XSS.

Result: No XSS behavior observed; data was sanitized and no content was reflected.

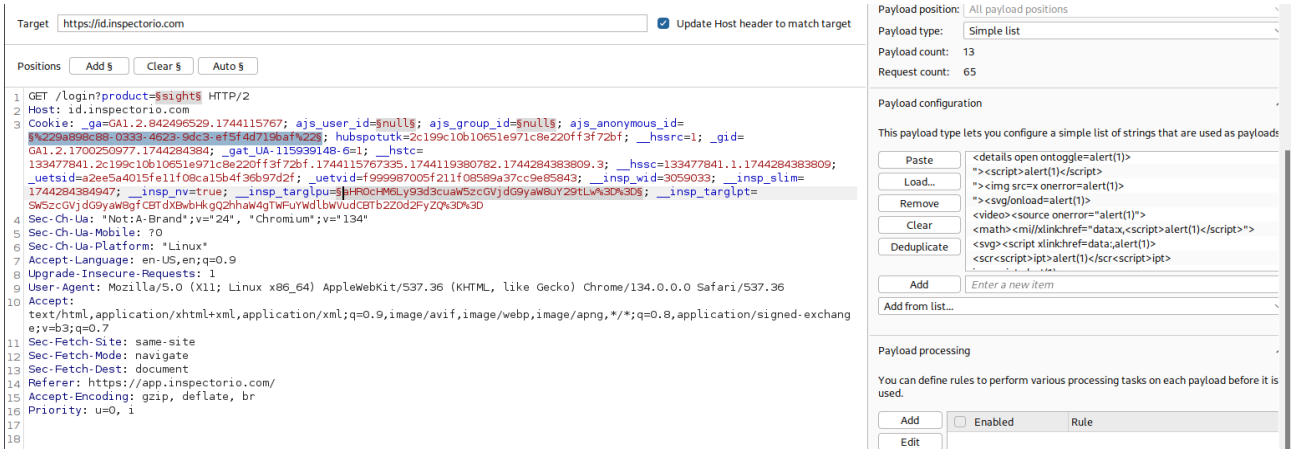
6.3 XSS Injection Testing

Targeted Endpoint:

- GET /login?product=sight
- Host: id.inspectorio.com

Intruder Setup:

- Multiple injection points:
    - **Query Parameter**: product=
    - **Cookies**: ajs_user_id, ajs_group_id, ajs_anonymous_id, _insp_targlpu
- Mode Used: **Cluster Bomb** to try multiple payload combinations



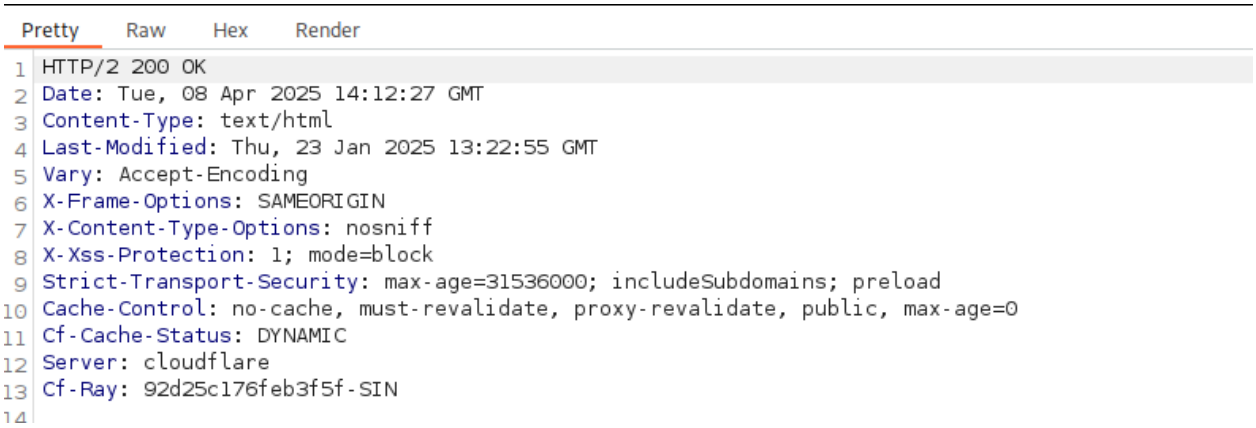
Payload Positions

Payloads Injected Included:

- <script>alert(1)</script>
- <img src=x onerror=alert(1)>
- <svg/onload=alert(1)>
- <iframe src=javascript:alert(1)>
- <details open ontoggle=alert(1)>
- "><script>alert(1)</script>
- "><img src=x onerror=alert(1)>
- "><svg/onload=alert(1)>
- <video><source onerror="alert(1)">
- <math><mi//xlink:href="data:x,<script>alert(1)</script>">
- <svg><script xlink:href=data:,alert(1)>
- <scr<script>ipt>alert(1)</scr<script>ipt>
- javascript:alert(1)

Result: No payloads were reflected or executed. Responses showed:

- X-XSS-Protection: 1; mode=block
- Strong Content-Security-Policy

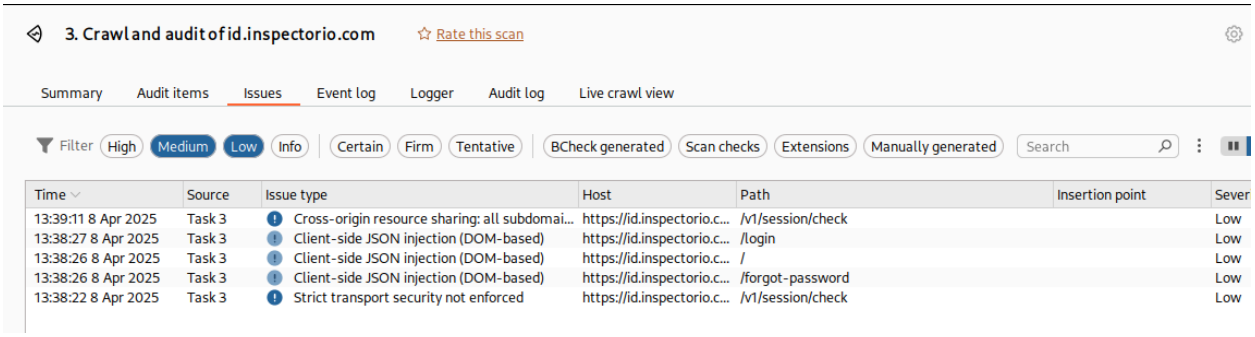


Response

6.4 Crawl & Audit: id.inspectorio.com

A Burp Suite automated audit returned the following **low-severity issues**:

Issue	Path	Risk
CORS misconfiguration	/v1/session/check	All subdomains allowed
JSON injection (DOM based)	/login ,/forgot-password	May lead to XSS
Missing Strict-Transport-Security	/v1/session/check	Weak HTTPS enforcement



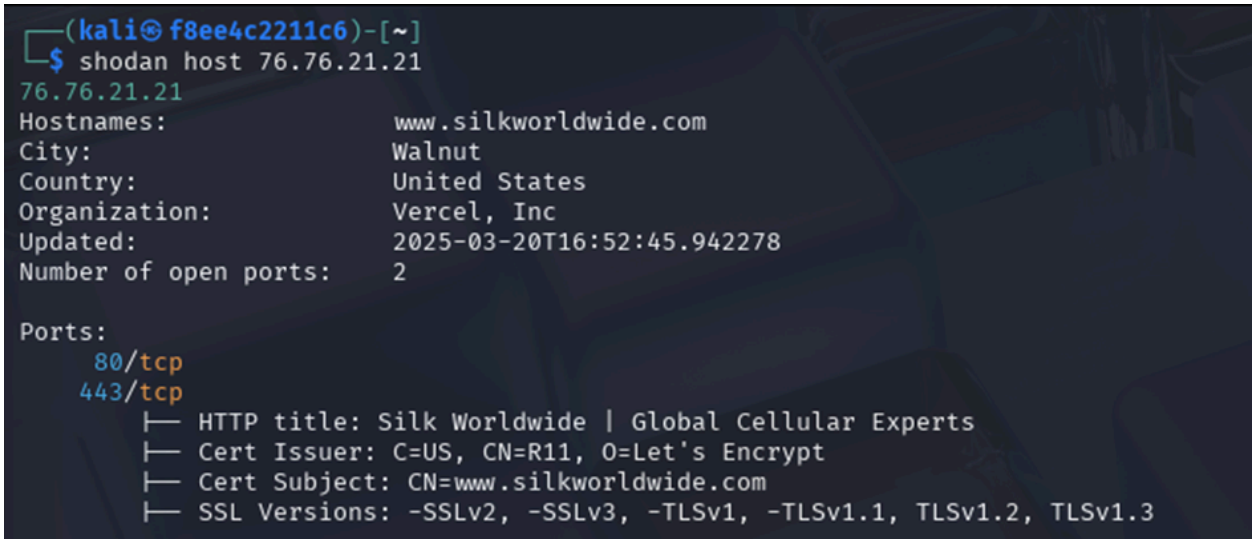
Lightweight Scan Result

These findings do not currently lead to exploitable issues but should be addressed for defense-in-depth.

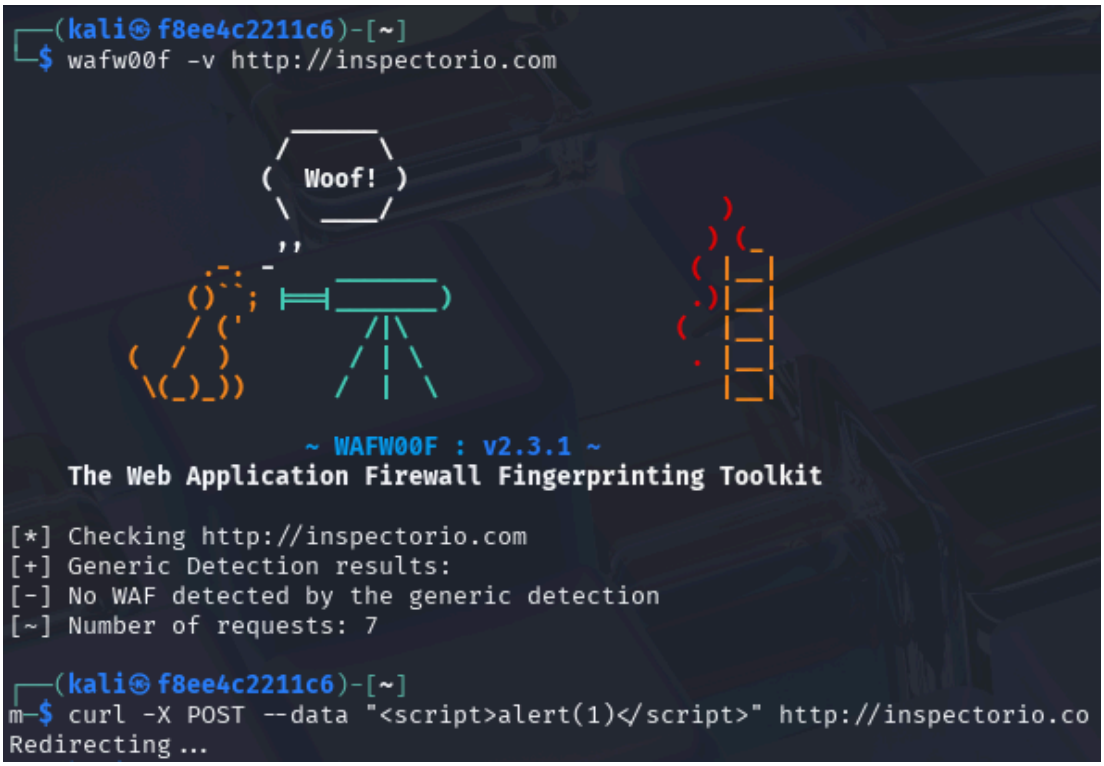
6.5 Scan Valuable Information:

The following scan results from shodan:

Name	Results
Host Name	www.silkworldwide
City	Walnut
Country	United States
Organization	Vercel, Inc
Last updated	2025-03-20T161:52:45.942278
Number of open ports	2 (80, 443)
HTTP Title	Silk World Wide | Global Cellular Experts
Certificate Issuer	C= US, CN = R11, 0= Let's Encrypt
SSL Versions	- SSLv2, -SSLv3, -TLSv1, TLSv1.1, TLSv1.2, TLSv1.3



7. Web Application Firewall (WAF) & Proxy Detection

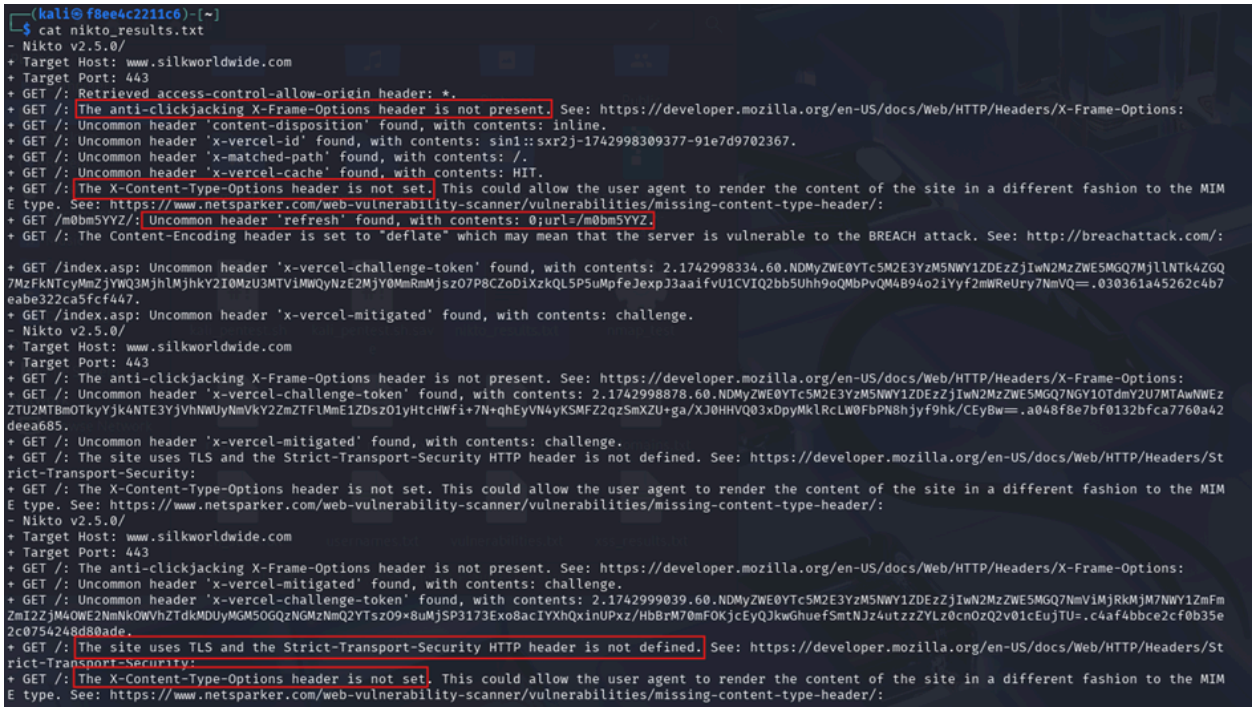


- **Tool:** WAFW00F
- **Observation:** No active WAF detected
- **Manual Analysis:** Responses suggest soft filtering (e.g., redirection, silent sanitization) likely handled by Vercel

8. Finding Vulnerability

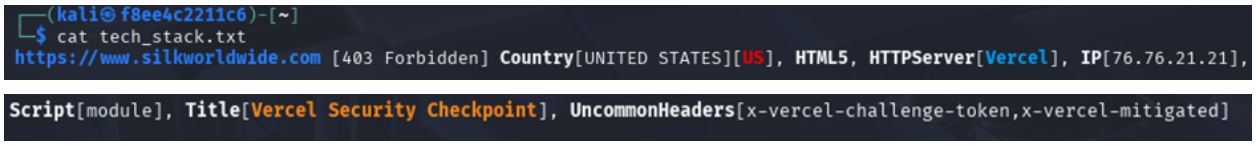
-Tool: Nuclei

Nikto Results Scanning gets missing security headers such as Clickjacking Protection, MIME sniffing protection, Man-in-the-middle-risk, and has a potential vulnerability of breach attack because of compression (content-encoding:deflate) that may expose sensitive data.

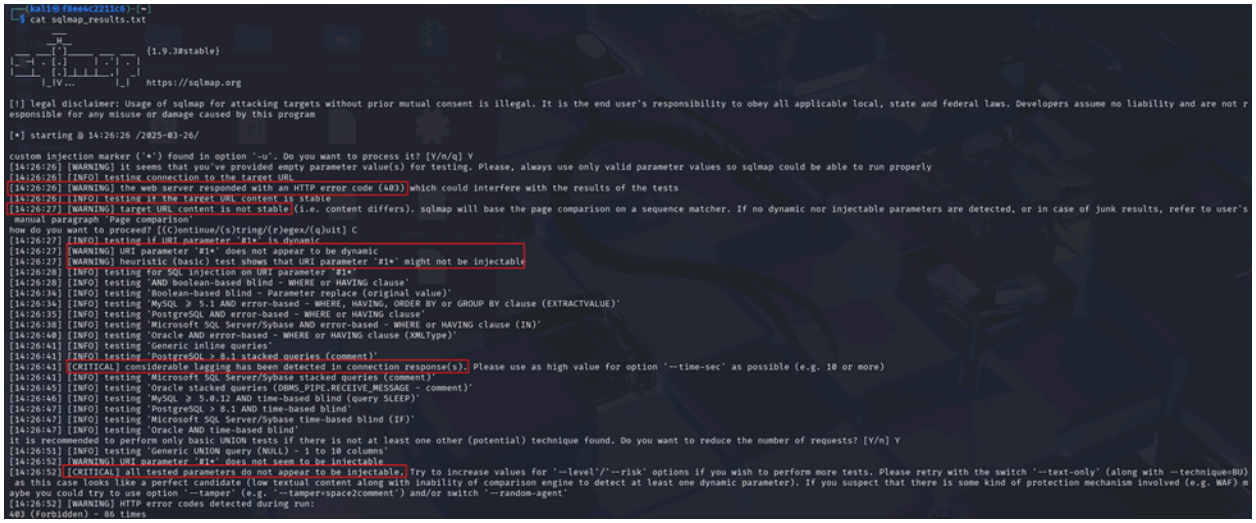


- tech_stack.txt

Technology Detected with HTML5 (Frontend) and Java Script Modules that are likely using ES6 Modules. Moreover, for the security findings, there's a 403 Forbidden Responses meaning that the site has an access restriction that is protected by Vercel security checkpoint.



- SQL Map Result



- The target URL content not stable because of the dynamic content that may affect the SQL injection detection.

- There's no dynamic parameters detected because parameter #1 doesn't appear to be injectable.

- In conclusion, there's no SQL injection vulnerabilities found by scanning.

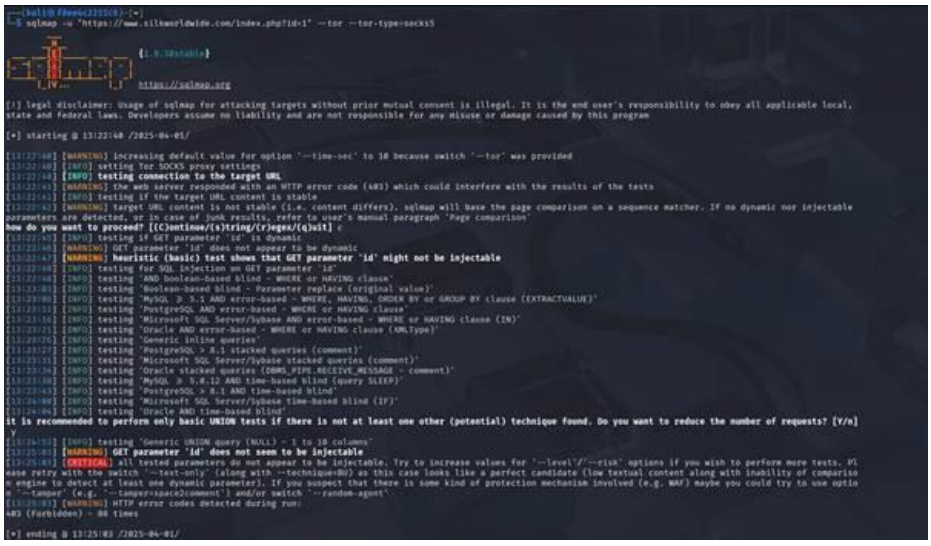
9. Evasion & Bypass Attempts

9.1 Spoofing & Header Manipulation

- Used:
    - User-Agent: Mozilla/5.0
    - Referer: https://www.google.com
    - X-Forwarded-For: 127.0.0.1
- **Result:** Still received 403 Forbidden

9.2 Alternative Routing

- **TOR Browser:** No change in access behavior



10. Tools Summary

Tool	Purpose	Result
nslookup	Domain to IP	Success
Masscan/Nmap	Port Scan	80/443 open
Netcat/Telnet	Port Check	Confirmed HTTP open
Whatweb	Tech Stack	Vercel , JS modules
LBD	Load Balancing	Not found
Nikto	Vulnerability Scan	Missing headers
SQLMap	SQL Injection	Blocked (403)
Nuclei	CVE scan	No vulnerability found
OWASP ZAP	Crawling	Limited by firewall
Burp Suite Professional	Form testing + XSS injection	Inputs sanitized
Shodan	Scan Valuable Information	Host, SSL certificate
Gobuster	Hidden directory enumeration	Success
Nuclei	Web server, frameworks, SQL Map	Security Headers, Findings
Tor	Bypass the SSL connection	Unsuccess
BlackWidow	Identifying Site Functionality	Success
Arachni	Finding Site Vulnerabilities	Unsuccess
Wafw00f	Detecting Firewall	Not found

11. Conclusion & Recommendations

11.1 Summary of Key Findings

- Only HTTP/HTTPS ports are open.
- Vercel enforces strong network restrictions.
- Some minor misconfigurations in HTTP headers.
- No critical vulnerabilities (XSS, SQLi, etc.) found.
- Vercel may silently block scans via reverse proxy.
- Content is highly dynamic, which may affect some scanning reliability such as SQLi detection.
- Missing HTTP security headers (Clickjacking, MIME sniffing, Man-in-the-middle)
- Breach Attack potential detected due to HTTP compression.
- Detected front-end technologies included HTML5 and JavaScript modules using ES6.
- Alternate Scanning attempts via Tor did not reveal additional vulnerabilities.

11.2 Recommendations

1. **Add missing security headers**: X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security
2. **Disable HTTP compression**: Prevent BREACH attacks.
3. **Improve WAF visibility**: Consider adding WAF detection or visible defenses.
4. **Evaluate CORS Policy**: Don’t allow all subdomains.
5. **Rate limiting & CAPTCHA**: Add bot protection on login and demo request forms.
6. **Harden exposed URLs**: Avoid redundant slashes and dynamic parameters without validation.
7. **Account for Dynamic Content in Scans**: Utilize tools that can adapt to JavaScript-heavy or changing content.
8. **Supplement Automation with Manual Testing**: Human analysis can identify logic flaws and nuanced issues that automated may miss.