

CP3418 - Best Practices in Cybersecurity

Assessment Item 3- Report

Lecturer : Dr.Steve Kerrison & Dr.Hari Krishnan

11th April, 2025

TR1S, 2025

Penetration Testing Report	4
1. Reconnaissance	4
1.1 Target Identification	4
1.2 SSL Certificate and WHOIS Analysis	5
1.3 Traceroute	5
2. Scanning	5
2.1 Port Scanning (Masscan & Nmap)	5
2.2 Service Enumeration	6
3. Technology Stack Identification	8
3.1 WhatWeb Scan	8
4. Enumeration & Crawling	8
4.1 Directory & File Enumeration	8
4.2 DNS Load Balancing Check	10
4.3 Crawling	10
5. Vulnerability Assessment	12
5.1 Nikto Scan	12
5.2 Nuclei	13
5.3 SQLMap	14
5.4 Arachni	14
6. Web Application Analysis	15
6.1 Entry Points Mapping	15
Mapped Entry Points Included:	16
6.2 Input and Form Testing (Burp Suite Pro)	16
Form Fields Included:	17
Manual Manipulation:	17
6.3 XSS Injection Testing	18
Targeted Endpoint:	18
Payloads Injected Included:	19
6.4 Crawl & Audit: id.inspectorio.com	20
6.5 Scan Valuable Information:	21
7. Web Application Firewall (WAF) & Proxy Detection	23
8. Finding Vulnerability	23
9. Evasion & Bypass Attempts	25
9.1 Spoofing & Header Manipulation	25
9.2 Alternative Routing	26
10. Tools Summary	26
11. Conclusion & Recommendations	27
11.1 Summary of Key Findings	27
11.2 Recommendations	27

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

DNS records for **inspectorio.com**

A records

IPv4 address	Revalidate in
> a 76.76.21.21	1m

AAAA records
No AAAA records found.

CNAME record
No CNAME record found.

TXT records

By Nslookup.io
DNS for Developers
 Never be confused
 about DNS again.

1.3 Traceroute

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

```
(kali㉿f8ee4c2211c6) [~]
$ sudo traceroute -T -p 443 76.76.21.21
traceroute to 76.76.21.21 (76.76.21.21), 30 hops max, 60 byte packets
 1  172.17.0.1 (172.17.0.1)  0.045 ms  0.008 ms *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  76.76.21.21 (76.76.21.21)  1.344 ms  1.321 ms  1.678 ms
```

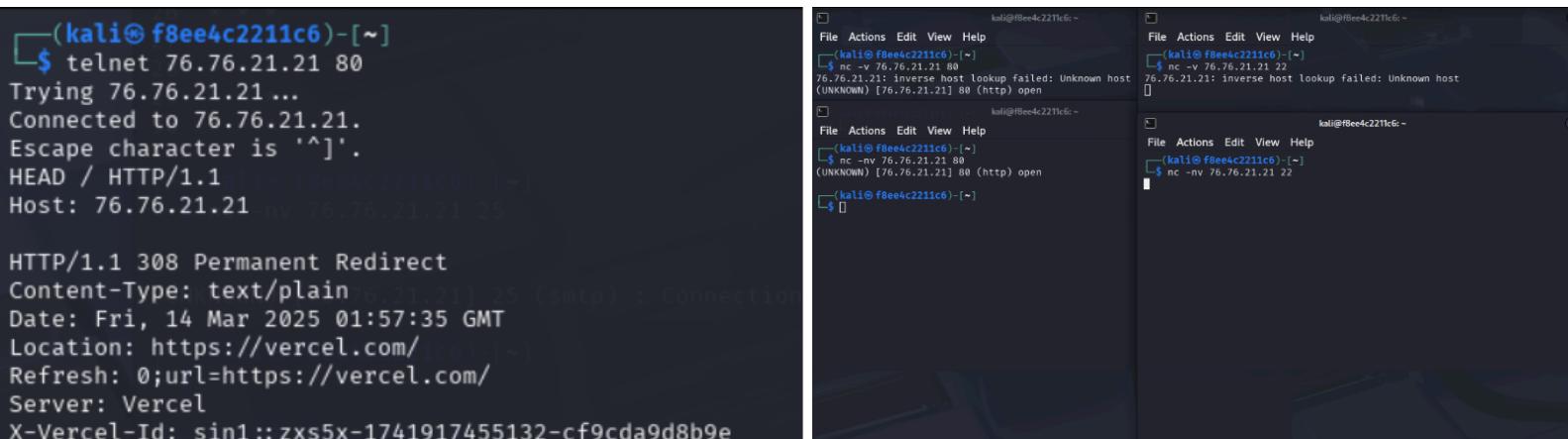
2. Scanning

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.



The image shows three terminal windows side-by-side, all running on a Kali Linux system (indicated by the 'kali' prompt). The left window shows the output of a telnet session to port 80 of the target host (76.76.21.21). It receives a 308 Permanent Redirect response to https://vercel.com. The middle window shows the output of an nc -v scan to port 80, which fails with an inverse host lookup error. The right window shows the output of an nc -v scan to port 22, which also fails with an inverse host lookup error.

```
(kali㉿f8ee4c2211c6)-[~]
$ telnet 76.76.21.21 80
Trying 76.76.21.21 ...
Connected to 76.76.21.21.
Escape character is '^['.
HEAD / HTTP/1.1
HTTP/1.1 308 Permanent Redirect
Content-Type: text/plain
Date: Fri, 14 Mar 2025 01:57:35 GMT
Location: https://vercel.com/
Refresh: 0;url=https://vercel.com/
Server: Vercel
X-Vercel-Id: sin1::zxs5x-1741917455132-cf9cda9d8b9e

(kali㉿f8ee4c2211c6)-[~]
$ nc -v 76.76.21.21 80
76.76.21.21: inverse host lookup failed: Unknown host
(UNKNOWN) [76.76.21.21] 80 (http) open

(kali㉿f8ee4c2211c6)-[~]
$ nc -v 76.76.21.21 22
76.76.21.21: inverse host lookup failed: Unknown host
(UNKNOWN) [76.76.21.21] 22 (ssh) open
```

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

```
(kali㉿f8ee4c2211c6)-[~]
└─$ whatweb inspectorio.com
http://inspectorio.com [308 Permanent Redirect] Country[UNITED STATES][US], 
HTTPServer[Vercel], IP[76.76.21.21], RedirectLocation[https://inspectorio.com]
]
https://inspectorio.com/ [308 Permanent Redirect] Country[UNITED STATES][US]
HTTPServer[Vercel], IP[76.76.21.21], RedirectLocation[https://www.inspectorio.com/], Strict-Transport-Security[max-age=63072000], UncommonHeaders[x-vercel-id]
ERROR: Plugin WordPress failed for https://www.inspectorio.com/. URI must be
ascii only "https://inspectorio.kinsta.cloud/wp-content/uploads/2024/01/Mode
nize-Your-\u2028Approach-to-Supply-\u2028Chain-Management-1.webp"
https://www.inspectorio.com/ [200 OK] Country[UNITED STATES][US], HTML5, HTT
PServer[Vercel], IP[66.33.60.66], Open-Graph-Protocol[article], Script, Stric
-Transport-Security[max-age=63072000], Title[Inspectorio | Supply Chain Mana
gement Software], UncommonHeaders[access-control-allow-origin,link,x-matched-
ath,x-vercel-cache,x-vercel-id]
```

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.

The screenshot shows the OWASP ZAP interface during an automated scan. The main window title is "Untitled Session - 20250410-140221 - ZAP 2.16.0". The left sidebar shows "Contexts" and "Sites" for the URL `http://76.76.21.21`, which contains two entries: `GET:robots.txt` and `GET:sitemap.xml`. The central panel is titled "Automated Scan" and contains fields for "URL to attack" (`http://76.76.21.21`), "Use traditional spider" (checked), "Use ajax spider" (set to "If Modern with Firefox"), and a "Attack" button. Below these fields, a message says "Attack complete - see the Alerts tab for details of any issues found". The bottom pane displays a table of network traffic:

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Co...	Reason	R...	Size	Re...	He...	Size	Re...	B...
421	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/info.php	308	Perma...	8...	254	bytes	15	bytes		
422	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/i.php	308	Perma...	9...	254	bytes	15	bytes		
423	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/test.php	308	Perma...	8...	254	bytes	15	bytes		
424	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/_vpreprivate/config.j...	308	Perma...	9...	254	bytes	15	bytes		
425	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/_framework/blazor....	308	Perma...	1...	254	bytes	15	bytes		
426	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/.hg	308	Perma...	7...	254	bytes	15	bytes		
427	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/.bzr	308	Perma...	1...	254	bytes	15	bytes		
428	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/_darcs	308	Perma...	8...	254	bytes	15	bytes		
429	4/10/25, 2:06:4...	4/10/25, 2:06:4...	GET	http://76.76.21.21/BitKeeper	308	Perma...	7...	254	bytes	15	bytes		

Processed	Method	URI	Flags
Green	GET	http://76.76.21.21	Seed
Green	GET	http://76.76.21.21/robots.txt	Seed
Green	GET	http://76.76.21.21/sitemap.xml	Seed
Red	GET	https://vercel.com/	Out of Scope

- Gobuster

```
(kali㉿f8ee4c2211c6) [~]
$ gobuster dir -u http://76.76.21.21 -w /usr/share/wordlists/dirb/common.txt -b 308
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

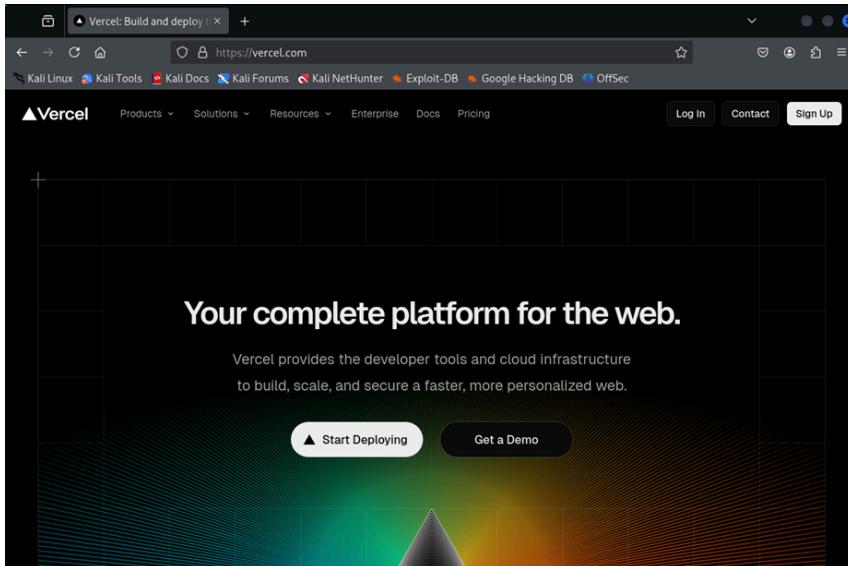
[+] Url:          http://76.76.21.21
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 308
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/_src           (Status: 307) [Size: 15] [→ https://vercel.com/deployments/76.76.21.21/source]
Progress: 4614 / 4615 (99.98%)
=====
Finished
```

- 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.

```
(kali㉿f8ee4c2211c6) - [~]
$ lbd inspectorio.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine
u)
Proof-of-concept! Might give false posi
ves.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
Vercel
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: , No date header found, skipping.

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

inspectorio.com does NOT use Load-balancing.
```

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.

```

File Edit View
http://www.inspectorio.com/
https://www.inspectorio.com/
https://www.inspectorio.com///
https://www.inspectorio.com///en
https://www.inspectorio.com///en/about
https://www.inspectorio.com///en/about/careers
https://www.inspectorio.com///en/about/newsroom
https://www.inspectorio.com///en/blog/supply-chains-seeing-the-payoff-from-ai-investments
https://www.inspectorio.com///en/case-studies/target
https://www.inspectorio.com///en/customers
https://www.inspectorio.com///en/guide/revolutionizing-the-production-chain-through-artificial-intelligence
https://www.inspectorio.com///en/partners
https://www.inspectorio.com///en/platform
https://www.inspectorio.com///en/platform/compliance
https://www.inspectorio.com///en/platform/integrations
https://www.inspectorio.com///en/platform/production
https://www.inspectorio.com///en/platform/quality
https://www.inspectorio.com///en/platform/security
https://www.inspectorio.com///en/platform/supply-chain-network-management
https://www.inspectorio.com///en/platform/traceability
https://www.inspectorio.com///en/press-release/elizabeth-pulos-joins-inspectorio
https://www.inspectorio.com///en/press-release/supply-chain-professionals-view-ai-as-a-key-tool-to-drive-innovation
https://www.inspectorio.com///en/resources
https://www.inspectorio.com///en/solutions/academy
https://www.inspectorio.com///en/solutions/apparel-footwear
https://www.inspectorio.com///en/solutions/brands-retailers
https://www.inspectorio.com///en/solutions/food-beverage
https://www.inspectorio.com///en/solutions/home-furniture
https://www.inspectorio.com///en/solutions/multi-category-retail
https://www.inspectorio.com///en/solutions/outdoor-sports
https://www.inspectorio.com///en/solutions/services
https://www.inspectorio.com///en/solutions/suppliers-factories
https://www.inspectorio.com///en/state-of-supply-chain-report-2024
https://www.inspectorio.com///en/webinars-events

```

5. Vulnerability Assessment

5.1 Nikto Scan

```
(kali㉿f8ee4c2211c6) -[~]
$ cat nikto_results.txt
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: Retrieved access-control-allow-origin header: *.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'Content-Disposition' found, with contents: inline.
+ GET /: Uncommon header 'x-vercel-id' found, with contents: sin1::srxr2j-1742998309377-91e7d7902367.
+ GET /: Uncommon header 'x-matched-path' found, with contents: /.
+ GET /: Uncommon header 'x-vercel-cache' found, with contents: HIT.
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /m0bm5YYZ/: [Uncommon header 'refresh' found, with contents: 0;url=/m0bm5YYZ].
+ GET /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/:

+ GET /index.asp: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742998334.60.NDMyZWE0YTc5M2E3YzM5NWy1ZDEzzjIwN2MzZWE5MGQ7MjllNTk4ZGQ
7MzFkNTcyMmZjYh03MjhkY2I0Mz1MwQyNzE2MjY0MmRmMjsz07P8CzoDiXzkQLSP5uMpfeJexpJ3aaifvU1CVIQ2bbUhh9oQMbPvQM4B94o2iYyf2mWReUry7NmVQ=.a030361a45262c4b7
eabe322ca5fcf447.
+ GET /index.asp: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742998878.60.NDMyZWE0YTc5M2E3YzM5NWy1ZDEzzjIwN2MzZWE5MGQ7GY10Tdm2U7MTAwNWEz
ZTU2MTBmoOtKyYjk4NTE3YjVhNWUyNmVky2ZmZTf1MmE1ZDs01yHtcHWfi+7N+qhEyVn4yKSMFZ2qzMxZU+ga/XJ0HHVQ03xDpyMklRclW0FbPn8hjyf9hk.CEyBw=.a048f8e7bf0132bfca7760a42
deea685.
+ GET /: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ GET /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/St
rict-Transport-Security:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ GET /: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742999039.60.NDMyZWE0YTc5M2E3YzM5NWy1ZDEzzjIwN2MzZWE5MGQ7NmViMjRkMjM7NWy1ZmFm
ZmI22jM40WE2NmNk0WVhzTdkMDUyMGMS0GQzNGMzNmQ2Yts09x8uMjSP3173Exo8aciYXhQxinUPxz/HbBr:M70mfOKjCeYQJkwGhuefSmtNjz4utzzYLz0cn0zQ2v01cEujtU=.c4af4bbcce2cf0b35e
2c0754248d8ade.
+ GET /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/St
rict-Transport-Security:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
```

- 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 validable 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 on injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison 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 for 10 or more)
[14:26:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)' connections
[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)' using connections.
[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' the proxy server is working.
[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 perfect
. 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

The screenshot shows the Arachni Framework's Web Application Security Report interface. At the top, there are several tabs: Kali Linux, Kali Tools, Kali Docs, Kali Rooters, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main window title is "[+] Web Application Security Report - Arachni Framework". Below the title, it says "Report generated on: 2025-03-21 02:38:09 +0000" and "Report false positives at: http://github.com/Arachni/arachni/issues". A large green box contains the message "We're sorry, but something went wrong." To the left of this box, under "[+] System settings:", are details about the version (1.5.1), seed (e4d6201027aed933ab4bf6428cfe64d8), audit start and finish times, runtime (00:10:01), URL (https://www.inspectorio.com/), and user agent (Arachni/v1.5.1). Under "[*] Audited elements:", a list includes Links, Forms, Cookies, XMLs, JSONs, UI inputs, and UI forms. A large blue box at the bottom lists various security checks: captcha, html_objects, http_only_cookies, x_frame_options, password_autocomplete, unencrypted_password_forms, emails, cookie_set_for_parent_domain, mixed_resource, private_ip, hsts, insecure_cors_policy, insecure_cookies, form_upload, ssn, csv_svn_users, credit_card, backdoors, backup_directories, 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_restriction_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, xpath_injection, xss_dom_unvalidated_redirect, no_sql_injection_differential, xss_path, sql_injection, file_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_injection, sql_injection_differential, xss_tag, xss_script_context, trainer, csrf, ldap_injection, unvalidated_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.

The screenshot shows the Arachni Framework's Web Application Security Report interface. At the top, there are several tabs: Kali Linux, Kali Tools, Kali Docs, Kali Rooters, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main window title is "[+] Web Application Security Report - Arachni Framework". Below the title, it says "0 issues were detected." and "Report saved at: /home/kali/arachni-1.5.1-0.5.12/bin/scan-report.afr [0.0MB]". A large green box contains the message "We're sorry, but something went wrong." To the left of this box, under "[~] Audit summary:", it says "Audited 0 page snapshots." and provides statistics: 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), and Throttled max concurrency (20).

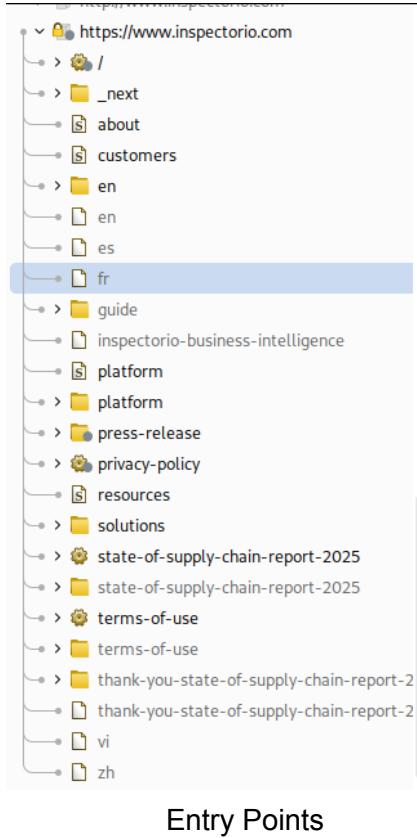
6. Web Application Analysis

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



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

The screenshot shows two windows side-by-side. On the left is the Burp Suite Professional interface, specifically the Intercept tab. It displays a list of network requests and responses. One request is highlighted, showing a POST to the URL <https://app.hubspot.com/api/cartographer/v1/ipl>. The right window is a browser window showing a form titled "Request a Demo". The form has several fields with validation messages: "Your First Name*" (highlighted in red), "Please complete this required field.", "Your Last Name*" (highlighted in red), "Please complete this required field.", "Your Work Email*" (highlighted in red), "Please complete this required field.", "Your Mobile Phone*", "Your Job Title*", and "Your Company's Name*". At the bottom of the form, there is a section titled "HOW CAN WE HELP YOU?" with three radio button options: "I'd like to discuss partnership and/or collaboration opportunities", "I need an account to work with an existing Inspectorio customer (onboarding process)", and "I'd like to learn more about the Inspectorio platform". There is also a "MESSAGE" input field with a blue speech bubble icon.

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

The screenshot shows the OWASP ZAP Intruder tool's payload configuration screen. The target is set to `https://id.inspectorio.com`. The payload position is set to "All payload positions" and the payload type is "Simple list". The payload count is 13 and the request count is 65. The payload configuration section contains a list of various XSS payloads, including standard ones like <script>alert(1)</script> and more complex ones involving SVG and MathML. The payload processing section allows defining rules to perform various processing tasks on each payload before it is used. A rule is currently defined with the name "Enabled Rule" and is set to be enabled.

Line Number	Line Content
1	GET /login?product= sights HTTP/2
2	Host: id.inspectorio.com
3	Cookie: _ga=GAI.2.842496529.1744115767; ajs_user_id=\$null; ajs_group_id=\$null; ajs_anonymous_id=\$%229a098e88033-4623-9d3-e15f4d719bf#223; hubspotutk=2c199c10b10651e971cbe220ff3f72bf; __hsref=1; __gid=GAI.2.1700250977.1744284384; __gat_UA-115939148-6=; __hstc=133477841.1.1744284383809.3; __hssc=133477841.1.1744284383809; __uetid=a2ee5a4015fe11f06ca15b4f36b97d2f; __utvid=f999987005f211f06589a37cc9e85843; __insp_wid=3059033; __insp_slim=1744284384947; __insp_nv=true; __insp_targlpu=\$!FOCCH6Ly93d3cuaw5zcGVjdG9yaW8jY29tLw%3D%3D\$; __insp_targlpt=SW5zcGVjdG9yaW8jOTdxBwhkgQ2hhaWq1TwUvwdlbwudCBfb2Zod2FyZ0%3D%3D\$
4	Sec-Ch-Ua: "Not-A-Brand";v="24", "Chromium";v="134"
5	Sec-Ch-Ua-Mobile: ?0
6	Sec-Ch-Ua-Platform: "Linux"
7	Accept-Language: en-US,en;q=0.9
8	Upgrade-Insecure-Requests: 1
9	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
10	Accept: */*
11	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
12	e;v=0.7;q=0.7
13	Sec-Fetch-Site: same-site
14	Sec-Fetch-Mode: navigate
15	Sec-Fetch-Dest: document
16	Referer: https://app.inspectorio.com/
17	Accept-Encoding: gzip, deflate, br
18	Priority: u=0, i

Payload Positions

Payloads Injected Included:

- <script>alert(1)</script>
-
- <svg/onload=alert(1)>
- <iframe src=javascript:alert(1)>
- <details open ontoggle=alert(1)>
- "><script>alert(1)</script>
- ">
- "><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

Pretty	Raw	Hex	Render
1	HTTP/2 200 OK		
2	Date: Tue, 08 Apr 2025 14:12:27 GMT		
3	Content-Type: text/html		
4	Last-Modified: Thu, 23 Jan 2025 13:22:55 GMT		
5	Vary: Accept-Encoding		
6	X-Frame-Options: SAMEORIGIN		
7	X-Content-Type-Options: nosniff		
8	X-Xss-Protection: 1; mode=block		
9	Strict-Transport-Security: max-age=31536000; includeSubdomains; preload		
10	Cache-Control: no-cache, must-revalidate, proxy-revalidate, public, max-age=0		
11	Cf-Cache-Status: DYNAMIC		
12	Server: cloudflare		
13	Cf-Ray: 92d25c176feb3f5f-SIN		
14			

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

The screenshot shows the Burp Suite interface with the 'Issues' tab selected. The title bar indicates '3. Crawland audit of id.inspectorio.com'. The main area displays a table of findings:

Time	Source	Issue type	Host	Path	Insertion point	Severity
13:39:11 8 Apr 2025	Task 3	ⓘ Cross-origin resource sharing: all subdomai...	https://id.inspectorio.c...	/v1/session/check		Low
13:38:27 8 Apr 2025	Task 3	ⓘ Client-side JSON injection (DOM-based)	https://id.inspectorio.c...	/login		Low
13:38:26 8 Apr 2025	Task 3	ⓘ Client-side JSON injection (DOM-based)	https://id.inspectorio.c...	/		Low
13:38:26 8 Apr 2025	Task 3	ⓘ Client-side JSON injection (DOM-based)	https://id.inspectorio.c...	/forgot-password		Low
13:38:22 8 Apr 2025	Task 3	ⓘ Strict transport security not enforced	https://id.inspectorio.c...	/v1/session/check		Low

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	2025-03-20T16:52:45.942278
Number of open ports	2 (80, 443)
HTTP Title	Silk World Wide Global Cellular Experts
Certificate Issuer	C= US, CN = R11, O= Let's Encrypt
SSL Versions	- SSLv2, -SSLv3, -TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
(kali㉿f8ee4c2211c6)~
$ shodan host 76.76.21.21
76.76.21.21
Hostnames: www.silkworldwide.com
City: Walnut
Country: United States
Organization: Vercel, Inc
Updated: 2025-03-20T16:52:45.942278
Number of open ports: 2

Ports:
  80/tcp
  443/tcp
    HTTP title: Silk Worldwide | Global Cellular Experts
    Cert Issuer: C=US, CN=R11, O=Let's Encrypt
    Cert Subject: CN=www.silkworldwide.com
    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.

```
(kali㉿f8ee4c2211c6) [~]
$ cat nikto_results.txt
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: Retrieved access-control-allow-origin header: *.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'Content-Disposition' found, with contents: inline.
+ GET /: Uncommon header 'x-vercel-id' found, with contents: sin1::srx2j-1742998309377-91e7d9702367.
+ GET /: Uncommon header 'x-matched-path' found, with contents: /.
+ GET /: Uncommon header 'x-vercel-cache' found, with contents: HIT.
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /:obm5YYZ/: Uncommon header 'refresh' found, with contents: 0;url=/#obm5YYZ.
+ GET /: The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/:

+ GET /index.asp: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742998334.60.NDMyZWE0YTc5M2E3Yz5NWY1ZDEzzjIwN2MzWE5MGQ7Mj1lNTk4ZGQ
7MzFkNTcyMmZjYwQ3MjnlMjhkY2I0MzU3MTv1MwQyNzE2MjY0MmRmMjsz07P8Cz0DiXzkl5P5uMpfeJexp3aaifvU1CVIQ2bb5Uh9oQmPvQM4B94o2iYyf2mWReUry7NmVQ=.030361a45262c4b7
eabe322ca5fcf447.
+ GET /index.asp: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742998878.60.NDMyZWE0YTc5M2E3Yz5NWY1ZDEzzjIwN2MzWE5MGQ7NY10Tdm2U0MTAwNWEz
ZTU2MTBm0tKyYjk4NTE3YjVhNWUyNmVky2ZmZTf1MmE1ZDsz01yhHtCHWFi+7N+qhEyV4yKSMF2ZqzSmXZU+ga/XJ0HHVQ03xDpyMkLrclW0FbPN8hjyf9hk/CEyBw=.a048f8e7bf0132bfca7760a42
deea685.
+ GET /: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ GET /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/St
rict-Transport-Security:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
- Nikto v2.5.0/
+ Target Host: www.silkworldwide.com
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ GET /: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1742999039.60.NDMyZWE0YTc5M2E3Yz5NWY1ZDEzzjIwN2MzWE5MGQ7NmViMjRkMjM7NWY1ZmFm
Zm122jM4OWE2NmNk0WVhZTdkMDUyMGM50GQzNGMzNmQ2Yts09xuMjSP3173Exo8aciYXhQxInUPxz/HbBrM70mfOKjCeYQjkwGhuefSmtNJz4utzzYLz0cnzQ2v01cEujtU=.c4af4bbcce2cf0b35e
2c0754248dd8ade.
+ GET /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/St
rict-Transport-Security:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
```

- 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.

```
(kali㉿f8ee4c2211c6) [~]
$ cat tech_stack.txt
https://www.silkworldwide.com [403 Forbidden] Country[UNITED STATES][US], HTML5, HTTPServer[Vercel], IP[76.76.21.21],
Script[module], Title[Vercel Security Checkpoint], UncommonHeaders[x-vercel-challenge-token,x-vercel-mitigated]
```

- SQL Map Result

```
[root@fedorav2316 ~]#
$ cat sqlmap_results.txt
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:26:26 /2025-03-26

custom injection marker ('*) found in option '-u'. Do you want to process it? [Y/n/q] Y
[*] http://sqlmap.org:80/test/1?id=1 OR ... [1.9.3#stable]
[*] http://sqlmap.org:80/test/1?id=1 OR ... https://sqlmap.org

[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:26:26 /2025-03-26

custom injection marker ('*) found in option '-u'. Do you want to process it? [Y/n/q] Y
[*] http://sqlmap.org:80/test/1?id=1 OR ... [1.9.3#stable]
[*] http://sqlmap.org:80/test/1?id=1 OR ... https://sqlmap.org

[*] [INFO] testing connection to the target URL
[*] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[*] [WARNING] target URL content is stable
[*] [WARNING] target URL content is not stable (i.e. content differs), sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual for more information
[*] [INFO] how do you want to proceed? [(C)ontinue/(S)tring/(R)egev/(Q)uit]
[*] [WARNING] URL parameter '#1' appears to be dynamic
[*] [WARNING] static/basic test shows that URL parameter '#1' might not be injectable
[*] [INFO] testing for SQL injection on URL parameter '#1'
[*] [INFO] testing 'AND' boolean-based blind - WHERE or HAVING clause
[*] [INFO] testing 'OR' boolean-based blind - WHERE or HAVING clause
[*] [INFO] testing UNION query - WHERE or HAVING clause (EXTRACTVALUE)
[*] [INFO] testing MySQL's t_1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
[*] [INFO] testing PostgreSQL AND error-based - WHERE or HAVING clause (IN)
[*] [INFO] testing Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (XMLType)
[*] [INFO] testing Oracle AND error-based
[*] [INFO] testing Generic inline queries
[*] [INFO] testing PostgreSQL > 8.1 stacked queries (comment)
[*] [CRITICAL] considerable lagging has been detected in connection response(). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[*] [INFO] testing Microsoft SQL Server/Sybase (comment)
[*] [INFO] testing Oracle standard query (DMS_PIPE.RECEIVE_MESSAGE comment)
[*] [INFO] testing MySQL > 5.0.12 AND time-based blind (query SLEEP)
[*] [INFO] testing PostgreSQL > 8.1 AND time-based blind
[*] [INFO] testing Microsoft SQL Server/Sybase AND time-based blind (IF)
[*] [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. Do you want to reduce the number of requests? [Y/n] Y
[*] [INFO] testing Generic UNION query (NULL) - 1 to 10 columns
[*] [INFO] testing Generic UNION query (NULL) - 11 to 20 columns
[*] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. Please retry with the switch '--text-only' (along with --technique=BU) as this case looks like a perfect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper=space+comment' and/or switch '--random-agent'
[*] [WARNING] HTTP error codes detected during run:
[*] [WARNING] 403 (Forbidden) - 46 times
```

- 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

```
[kali㉿8ee4c2211c0:~] $ sqlmap -u "https://www.silkworldwide.com/index.php?id%31" {1.9.3#stable} https://sqlmap.org [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program [*] starting @ 13:03:23 /2025-04-01/ [13:03:24] [INFO] testing connection to the target URL [13:03:24] [CRITICAL] can't establish SSL connection [*] ending @ 13:03:24 /2025-04-01/
```

9.2 Alternative Routing

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

```

$ sqlmap -u "https://www.siliconwide.com/index.php?id=1" --tor --tor-type-seocks

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:22:48 /2025-04-05

[2025-04-05 13:22:48] [WARNING] increasing default timeout for option '--time-soc' to 30 because switch '--tor' was provided
[2025-04-05 13:22:48] [INFO] setting Tor SOCKS proxy settings
[2025-04-05 13:22:48] [INFO] testing connection to the target URL
[2025-04-05 13:22:48] [INFO] testing if the target URL is stable
[2025-04-05 13:22:48] [INFO] testing if the target URL content is stable
[2025-04-05 13:22:48] [WARNING] Target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable
parameters are detected, or in case of junk results, refer to user's manual paragraph "Page comparison".
[2025-04-05 13:22:48] [INFO] testing if GET parameter 'id' is dynamic
[2025-04-05 13:22:48] [INFO] testing if GET parameter 'id' is dynamic
[2025-04-05 13:22:48] [WARNING] GET parameter 'id' does not appear to be dynamic
[2025-04-05 13:22:48] [INFO] heuristics (basic) test shows that GET parameter 'id' might not be injectable
[2025-04-05 13:22:48] [INFO] testing MySQL error-based blind - WHERE or HAVING clause
[2025-04-05 13:22:48] [INFO] testing MySQL Boolean-based blind - WHERE or HAVING clause
[2025-04-05 13:22:48] [INFO] testing MySQL Boolean-based time-based blind - WHERE or HAVING clause (EXTRACTVALUE)
[2025-04-05 13:22:48] [INFO] testing MySQL Sqli error-based - WHERE or HAVING clause
[2025-04-05 13:22:48] [INFO] testing PostgreSQL Sqli AND error-based - WHERE or HAVING clause (IN)
[2025-04-05 13:22:48] [INFO] testing Oracle AND error-based - WHERE or HAVING clause (IN/TYPE)
[2025-04-05 13:22:48] [INFO] testing Oracle Boolean-based blind - WHERE or HAVING clause
[2025-04-05 13:22:48] [INFO] testing PostgreSQL > 8.1 stacked queries (comment)
[2025-04-05 13:22:48] [INFO] testing Microsoft Sql Server/Sybase stacked queries (comment)
[2025-04-05 13:22:48] [INFO] testing Microsoft Sql Server/Sybase stacked queries (comment,INET)
[2025-04-05 13:22:48] [INFO] testing PostgreSQL > 8.1 AND time-based blind (every SELECT)
[2025-04-05 13:22:48] [INFO] testing Microsoft Sql Server/Sybase time-based blind (IP)
[2025-04-05 13:22:48] [INFO] testing Microsoft Sql Server/Sybase time-based blind (IP)

It is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
y

[2025-04-05 13:22:48] [INFO] testing generic UNION query (MySQL) - 1 to 10 columns
[2025-04-05 13:22:48] [INFO] GET parameter 'id' does not seem to be injectable
[2025-04-05 13:22:48] [WARNING] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. It's
useless with the switch '--test-only' along with '--technique=BDF' as this case looks like a perfect candidate (low textual content along with inability of comparison
of engine output). If you suspect that the target database is protected against such attack, you might suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option
--tamper (e.g. --tamper=executeOnly) and/or switch '--random-agent'.
[2025-04-05 13:22:48] [INFO] HTTP error codes detected during run:
#3 [INFO] forbidden - 88 times

[*] ending @ 13:22:48 /2025-04-05

```

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.