Risk Analysis

SkillsBridge

Stranger Thinks

HIMANSHU MIDHA (34676295)
QINYI LIU (33536988)
CHENJIN QIN (35504900)
JEFFIN THOMAS (33948941)
YING FU (34055436)

Contents

Nmap Risks

Ports	Services	Details	Risk Level
80/tcp	HTTP	Vercel Proxy, Redirects to HTTPS	Low
443/tcp	HTTPS	TLS/SSL configured, but missing HSTS header	High
443/tcp	HTTPS	No stored XSS vulnerabilities detected	Informational
443/tcp	HTTPS	No SQL injection vulnerabilities detected	Informational
443/tcp	HTTPS	DoS risk - Slow HTTP attacks	Medium
443/tcp	HTTPS	Missing X-Frame-Options	High
443/tcp	HTTPS	SSL/TLS Grade A (strong ciphers)	Informational

Nmap Mitigation

- Configure Strict-Transport-Security (HSTS) header with max-age=31536000 to prevent protocol downgrade attacks.
- Add X-Frame-Options: DENY to prevent clickjacking.
- Implement Content-Security-Policy to restrict resource loading.
- Configure X-Content-Type-Options: nosniff to prevent MIME-sniffing.
- Configure connection/request timeouts to limit incomplete requests.
- Apply rate limiting and restrict max concurrent connections per IP.
- Disable older TLS versions if not required (keep TLS 1.2 and 1.3 only).
- Review and remove weak cipher suites.
- Enable OCSP stapling for certificate validation.

Nikto Risks

Findings	Details	Risk Level
Missing HSTS Header	Man-in-the-middle and protocol downgrade attacks possible	High
Missing X-Frame-Options	Clickjacking possible	High
Missing X-Content-Type-Options	Misinterpretation risk	Medium
Private IP Address Disclosure	Attackers gain insight into backend/internal infrastructure	Medium
Vercel Headers Information Disclosure	Reveals internal IDs/tokens useful for reconnaissance	Medium

	and infrastructure fingerprinting	
Archive.zip File Accessible	Source code or sensitive data leakage risk	Medium
Error Message Disclosure (DEPLOYMENT_NOT_FOUND)	Error messages and misconfigured redirects expose environment details (DEPLOYMENT_NOT_FOUND errors visible)	Medium
Uncommon Header 'refresh'	May expose redirect URLs or application logic to attackers	Low
Uncommon Header 'x-vercel-error'	Error messages expose deployment details and environment information	Low
Wildcard SSL Certificate	Increased attack surface if one subdomain is compromised	Low
Cache-Control Suboptimal	May impact performance but secure	Low

Nikto Mitigation

- Add X-Frame-Options: DENY or SAMEORIGIN to block clickjacking attacks.
- Configure X-Content-Type-Options: nosniff to prevent MIME sniffing.
- Implement Strict-Transport-Security: max-age=31536000; includeSubDomains; preload to enforce HTTPS.
- Add Content-Security-Policy: default-src 'self'; script-src 'self' to restrict resource loading.
- Remove or sanitize unnecessary Vercel-specific headers (x-vercel-id, x-vercel-cache, x-vercel-challenge-token, x-vercel-mitigated) from production responses.
- Suppress exposure of internal/private IP addresses in HTTP headers.
- Configure custom error pages to hide deployment and environment details.
- Remove or restrict access to archive files (archive.zip) and backup files
- Use reverse proxy to filter and strip internal headers before reaching clients.
- Implement header filtering rules in Vercel configuration or CDN layer.
- Review wildcard certificate usage and consider dedicated certificates for sensitive applications.

Burpsuite Risks

Findings	**Details**	**Risk Level**
SQL Injection Vulnerabilities	Database protected from unauthorized access	Informational
Input Property	No malicious code execution possible	Informational
WAF Protection	Network-level defense operational	Informational
Error Handling	No SQL errors or stack traces leaked to attackers	Informational

Queries In Use	Single quotes handled without errors	Informational

Burpsuite Mitigation

Continue regular security testing

Monitor WAF logs for attack patterns and adjust rules as needed.

Keep application frameworks and dependencies updated.

Conduct code reviews focusing on database query construction.

Implement security logging and alerting for suspicious activity.