Vulnerability Assessment Report: telehack.com

SECURITY SCORE: 95/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
17	qotd		None
21	ftp		None
23	telnet		None
70	gopher		**fingerprint-strings:** GenericLines: iWelcome to the Telehack Gopher...
79	finger		**fingerprint-strings:** GenericLines: TELEHACK SYSTEM STATUS 2026-Feb...
80	http		**http-title:** Did not follow redirect to https://telehack.com/...
443	http		**http-title:** Telehack... **ssl-cert:** Subject: commonName=*.telehack.com Subject Alterna...
513	login		**fingerprint-strings:** DNSStatusRequestTCP: Connected to TELEHACK po...
2222	ssh		None
6668	ssh		None
6969	acmsoda		**fingerprint-strings:** GetRequest: HTTP/1.0 404 File Not Found C...
7070	realserver		None
8080	telnet		None
31337	telnet		None

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 64.13.139.230
+ Target Hostname: telehack.com
+ Target Port: 80
+ Start Time: 2026-02-23 16:59:05 (GMT0)
---------------------------------------------------------------------------
+ Server: tel/os
+ Uncommon header 'alt-svc' found, with contents: h3=":80"; ma=86400
```

```
+ Uncommon header 'content-security-policy' found, with contents: default-src
'unsafe-inline' 'self' data: http://telehack.com ws://telehack.com
http://*.telehack.com ws://*.telehack.com
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'link' found, with contents: ; rel="canonical"
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Root page / redirects to: https://telehack.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 26 items checked: 4 error(s) and 8 item(s) reported on remote host
+ End Time: 2026-02-23 16:59:41 (GMT0) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled Website Endpoints

- No endpoints found

4. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 60 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

5. Attack Possibilities & Mitigation

[LOW] Attack: Client-side Script Injection
Mitigation: Sanitize all user inputs and use output encoding.