

# SSL/TLS Report - juice-shop.herokuapp.com:443

Generated from juice-shop.herokuapp.com\_ssl\_tls\_2025-09-08\_18-46-03.html

## SSL/TLS Report

### Findings

| # | Issue / Type               | Location | Param | Payload / Vector | Status | Risk | Evidence / Details                     | Mitigation  |
|---|----------------------------|----------|-------|------------------|--------|------|--|---|
| 1 | Broad Wildcard Certificate | -        | -     | -                | OK     | Low  | Wildcard used with minimal SAN entries | Limit wildcard certificates; prefer SAN certificates scoped to required hosts only. |

### TLS Protocol Support

| Protocol | Supported |
|----------|-----------|
| TLSv1.0  | ■         |
| TLSv1.1  | ■         |
| TLSv1.2  | ■         |
| TLSv1.3  | ■         |

### Certificate

|                   |                          |
|-------------------|--------------------------|
| Subject / CN      | *.herokuapp.com          |
| Issuer            | Amazon RSA 2048 M02      |
| Valid From        | Jan 31 00:00:00 2025 GMT |
| Valid To          | Mar 1 23:59:59 2026 GMT  |
| Days Until Expiry | 174                      |
| Wildcard          | Yes                      |
| Self-Signed       | No                       |