# Vulnerability Assessment Report: httpforever.com

# SECURITY SCORE: 95/100

OVERALL RISK LEVEL: LOW

## 1. Network Scan Results (Nmap)

| Port | Service | Version | State |
|---|---|---|---|
| 22 | ssh | 8.9p1 Ubuntu 3ubuntu0.13 | open |
| 25 | smtp | | filtered |
| 80 | http | 1.18.0 | open |
| 135 | msrpc | | filtered |
| 139 | netbios-ssn | | filtered |
| 179 | bgp | | filtered |
| 443 | http | 1.18.0 | open |
| 445 | microsoft-ds | | filtered |
| 7025 | vmsvc-2 | | filtered |

## 2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 146.190.62.39
+ Target Hostname: httpforever.com
+ Target Port: 80
+ Start Time: 2026-02-16 16:32:59 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x641b16b8 0x1404
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'content-security-policy' found, with contents: default-src 'self';
script-src cdnjs.cloudflare.com 'self' 'report-sha256'; style-src cdnjs.cloudflare.com 'self'
fonts.googleapis.com 'unsafe-inline'; font-src fonts.googleapis.com fonts.gstatic.com
cdnjs.cloudflare.com; frame-ancestors 'none'; report-uri
https://scotthelme.report-uri.com/r/d/csp/enforce
+ Uncommon header 'referrer-policy' found, with contents: strict-origin-when-cross-origin
+ Uncommon header 'feature-policy' found, with contents: accelerometer 'none'; camera 'none';
geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none';
usb 'none'
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 26 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-02-16 16:33:27 (GMT0) (28 seconds)
```

```
---------------------------------------------------------------------------
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

## 3. Crawled Website Endpoints

- http://httpforever.com/

## 4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

## 5. Attack Possibilities & Mitigation

**Attack:** Clickjacking Vulnerability
**Mitigation:** Implement X-Frame-Options: SAMEORIGIN or DENY.