

Security

To ensure security Apptimized complies with the following cybersecurity standards:

- ISO 15408;
- ISO/IEC 27001;
- ISO/IEC 27002;
- ANSI/ISA 62443 (Formerly ISA-99);
- IEC 62443;

A military-grade security protocol (TLS/SSL) is used by Apptimized to provide privacy and data integrity between two or more communicating applications.

Apptimized safety audit entails a network scan of its resources to identify vulnerabilities and non-penetration.

The screenshot below shows the vulnerability report provided by **Detectify** for **app.apptimized.com**.

The screenshot displays a vulnerability report from Detectify for the domain **app.apptimized.com**. The report is structured into three main panels:

- Summary Panel:** Features the Detectify logo and the title "VULNERABILITY REPORT app.apptimized.com". It includes scan dates: "Scan Started 2020-02-25T00:06:00+00:00" and "Scan Finished 2020-02-25T00:25:58+00:00".
- 1.1 Fingerprinted Software Panel:** Contains a "Summary" section with "Found at app.apptimized.com" and a "CVSS Score 0". It also lists "References" such as "DETECTIFY - An intelligent way to look for vulnerabilities" and "DETECTIFY - What's under the hood". Below this, several software fingerprints are listed with their vendors, software names, versions, and confidence levels (e.g., "Vendor: microsoft, Software: windows, Confidence: 30").
- Findings Panel:** Titled "Findings" with a link to "All findings summary". It shows a "HIGH" severity finding with "No findings" listed. Below this, a "MEDIUM" severity finding is also shown with "No findings". A "LOW" severity finding is also present with "No findings". An "INFORMATION" section lists several items, including "Fingerprinted Software", "Strict-Transport-Security / Missing Header", "Discovered Host", "Crawled URL's", "Service Providers", and "Recorded User Events Failed using app.apptimized.com-recording-1920x937".


The screenshots below show the SSL report of **app.apptimized.com**.

| Feature | Percentage |
|------------------|------------|
| Certificate | 100% |
| Protocol Support | 100% |
| Key Exchange | 90% |
| Cipher Strength | 90% |

This site works only in browsers with SNI support.

[illegible][illegible]

| | |
|--------------------------------|--|
| OpenSSL version: | Unknown (requires support for at least two protocols, vnd. SSL2) |
| OpenSSL TLS compression | No |
| RC4 | No |
| Heartbleed (vulnerability) | No |
| Heartbleed (vulnerability) | No (more info) |
| Indiscretions (vulnerability) | No |
| OpenSSL CVEs (CVE-2014-0224) | No (more info) |
| OpenSSL Pending CVEs | No |
| CVE-2016-2107 | No (more info) |
| ROBUST (vulnerability) | No (more info) |
| Forward Secrecy | Yes (with more browsers) |
| ALPN | Yes (to http 1.1) |
| NPN | No |
| Session resumption (cookies) | No (NPN assigned but not accepted) |
| Session resumption (tickets) | No |
| CCSP (logging) | No |
| Strict Transport Security | No |
| PSK13 | No |
| HTTPS (Preloading) | Not in Chrome, Edge, Firefox, IE |
| Public Key Pinning (HPKP) | No (more info) |
| Public Key Pinning Report-Only | No |
| Public Key Pinning (Strict) | No (more info) |
| Long Handshake intolerance | No |
| TLS extension intolerance | No |
| TLS version intolerance | No |
| Incorrect SSL alerts | No |
| Handshake compression (DHE) | No, DHE, not supported |
| DTLS public server param | No, DTLS, not supported |
| DTLS | No |
| ECDF public server param | No |
| ECDF | No |
| Supported Named Groups | secp256r1, secp384r1 (server preferred order) |
| SSL 2 handshake | No |



The screenshot shows a web browser window with the address bar displaying 'http://app.apptimed.com/'. The page title is 'My Profile'. The main content area shows a profile card for 'John Doe' with a placeholder image, email 'john.doe@example.com', and phone number '+1 (555) 123-4567'. Below the card is a 'My Profile' section with a table of account details.

| Field | Value |
|-----------------------------|-------------------------|
| First name | John |
| Last name | Doe |
| Email | john.doe@example.com |
| Phone | +1 (555) 123-4567 |
| Account type | Standard |
| Account status | Active |
| Account created | 2023-01-01 10:00:00 UTC |
| Account last login | 2023-01-01 10:00:00 UTC |
| Account last login IP | 192.168.1.1 |
| Account last login device | Chrome |
| Account last login location | New York, NY, USA |

SSL Report v2.1.0

Copyright © 2009-2020 Quanta, Inc. All Rights Reserved.

Try Qvalys for free! Experience the award-winning [Qvalys Cloud Platform](#) and the entire collection of [Qvalys Cloud Apps](#), including certificate security solutions.

[Letter and
card form](#)

10/1/2014

| Protocol Details | |
|---------------------------------------|--|
| DROWN | No, server keys and handshake not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this deeper explanation |
| Secure Negotiation | Yes, server certificate only provided by the Canopy network search engine, original DROWN database here |
| Secure Client-Initiated Negotiation | Supported |
| Insecure Client-Initiated Negotiation | No |
| BRACE attack | Mitigated server-side (more info) |

Revision #1

Created 17 March 2020 09:03:14

Updated 7 June 2021 04:52:31