

# 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:

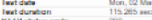
- Summary Panel:** Features the Detectify logo and the title "VULNERABILITY REPORT app.apptimized.com". It includes scan dates: "Scan Started 2020-02-25T00:06:00+00:00" and "Scan Finished 2020-02-25T00:25:58+00:00".
- 1.1 Fingerprinted Software Panel:** Contains a "Summary" section with "Found at app.apptimized.com" 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, it lists several fingerprinted items 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", a "MEDIUM" severity finding with "No findings", and a "LOW" severity finding with "No findings". It also includes an "INFORMATION" section with a list of findings, 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.

	Cipher Suites	
	# TLSv1.2 (available in server-on-demand mode)	
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (dh/anon) ECDH secg2dhe1 (sig. 3072)	256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (dh/anon) ECDH secg2de1 (sig. 3072)	128
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (dh/anon) ECDH secg2dhe1 (sig. 3072)	256
	bbs RSA P-5 WPKAT	
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (dh/anon) ECDH secg2de1 (sig. 3072)	128
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (dh/anon) ECDH secg2dhe1 (sig. 3072)	256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (dh/anon) ECDH secg2dhe1 (sig. 3072)	256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (dh/anon) ECDH secg2de1 (sig. 3072)	128
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (dh/anon) ECDH secg2dhe1 (sig. 3072)	256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (dh/anon) ECDH secg2de1 (sig. 3072)	128

[illegible]

The screenshot shows a web browser window with the title "MIT IDP requests". It displays two requests and their corresponding responses:

- Request 1:** `https://app.appstombed.com/` (MIT IDP:1 202 Found)
- Request 2:** `https://app.appstombed.com/Account/Login?ReturnUrl=%2F` (MIT IDP:1 200 OK)

Below the requests, the **Response** details are shown:

- Time:** Mon, 02 May 2020 08:52:13 UTC
- Content type:** text/html
- Content length:** 115,283 seconds
- MIT IDP status code:** 200
- MIT IDP server signature:** X509
- Server hostname:** (empty)

Copyright © 2009-2020 [Qualys, Inc.](#) All Rights Reserved.

[Letter and  
card form](#)

Protocol Details	
LDAPv3	No, server keys and certificates not seen elsewhere with SSLv2 (1) For a better understanding of this threat, please read <a href="#">this deeper vulnerability analysis</a> (2) Certificates and keys are only provided by the <a href="#">Cisco</a> network search engine, original LDAPv3 website lists (3) Cisco's data is only exclusive, irreversible key and certificate reuse; possibly out-of-date and not complete
Secure Negotiation	Supported
Secure Client-Installed Negotiation	No
Insecure Client-Installed Negotiation	No
Brassica Attack	Mitigated server-side ( <a href="#">more info</a> )

---

Revision #1

Created 17 March 2020 09:03:14

Updated 7 June 2021 04:52:31