

# 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 as follows:

- Summary:** Shows the scan status (Scan Started: 2020-02-25T00:06:00+00:00, Scan Finished: 2020-02-25T00:25:58+00:00) and a CVSS Score of 0.
- 1.1 Fingerprinted Software:** Lists identified software components with their vendors, versions, and confidence levels.


Vendor	Software	Version	Confidence
Microsoft	Windows		30
Microsoft	IS	10.0	100
Microsoft	ASP.NET Core		50
Microsoft	IIS Express		50
Microsoft	ASP.NET Core		50
- Findings:** A summary of all findings, categorized by severity (High, Medium, Low, Information). The report shows several 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.


Renegotiation	no
SSA1 attack	Mitigated server-side ( <a href="#">more info</a> )
POODLE (SSLv3)	No, SSLv3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Just a POODLE	No ( <a href="#">more info</a> )
GOLDENDOODLE	No ( <a href="#">more info</a> )
OpenSSL 0-Length	No ( <a href="#">more info</a> )
Shoring POODLE	No ( <a href="#">more info</a> )
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbleed (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Unsharable (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CVE's vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln.	No ( <a href="#">more info</a> )
(CVE-2016-2107)	No ( <a href="#">more info</a> )
HDOJO (vulnerability)	No ( <a href="#">more info</a> )
Forward Secrecy	Yes (with <a href="#">most browsers</a> ) <a href="#">HDOJO</a> ( <a href="#">more info</a> )
ALPN	Yes (2 http/1.1)
NPN	No
Session resumption (loading)	No (SNI assigned but not accepted)
Session resumption (storing)	No
OCSP stapling	No
Strict Transport Security (STS)	No
H2.1.5 (preloading)	Not in: Chrome, Edge, Firefox, IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No ( <a href="#">more info</a> )
Public Key Pinning (Sticky)	No ( <a href="#">more info</a> )
Long handshake tolerance	No
TLS extension intolerance	No
Incorrect SNI alerts	No
Unknown common DH primes	No, DHPE suites not supported
DH public server param (TA) reuse	No, DHPE suites not supported
EC-ON public server param reuse	No
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No



HTTP Requests

1 <https://app.aphismed.com/> (HTTP/1.1 200 Found)

2 <https://app.aphismed.com/Account/Login?ReturnUrl=%2F> (HTTP/1.1 200 OK)



Metadata/headers

last dateMon, 02 Mar 2020 06:52:13 UTC

last duration115.265 seconds

HTTP status code200

HTTP server signatureKestrel

Server hostname-

SSL Report v2.1.0

Copyright © 2019-2020 [Qualys, Inc.](#) All Rights Reserved.

[Try Qualys for free](#). Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [qualys.com products](#) including [certificate security](#) & [webSSL](#).

---

Revision #1

Created 17 March 2020 09:03:14

Updated 7 June 2021 04:52:31