Pintexx Workplace:

Sicherheitsfaktoren

Inhaltsverzeichnis

1 Allgemeines

Pintexx Workplace „Basic“ ist ein System für den Fern-Zugriff auf einen PC, Terminals Server oder VM.

1.1 Sensible Daten

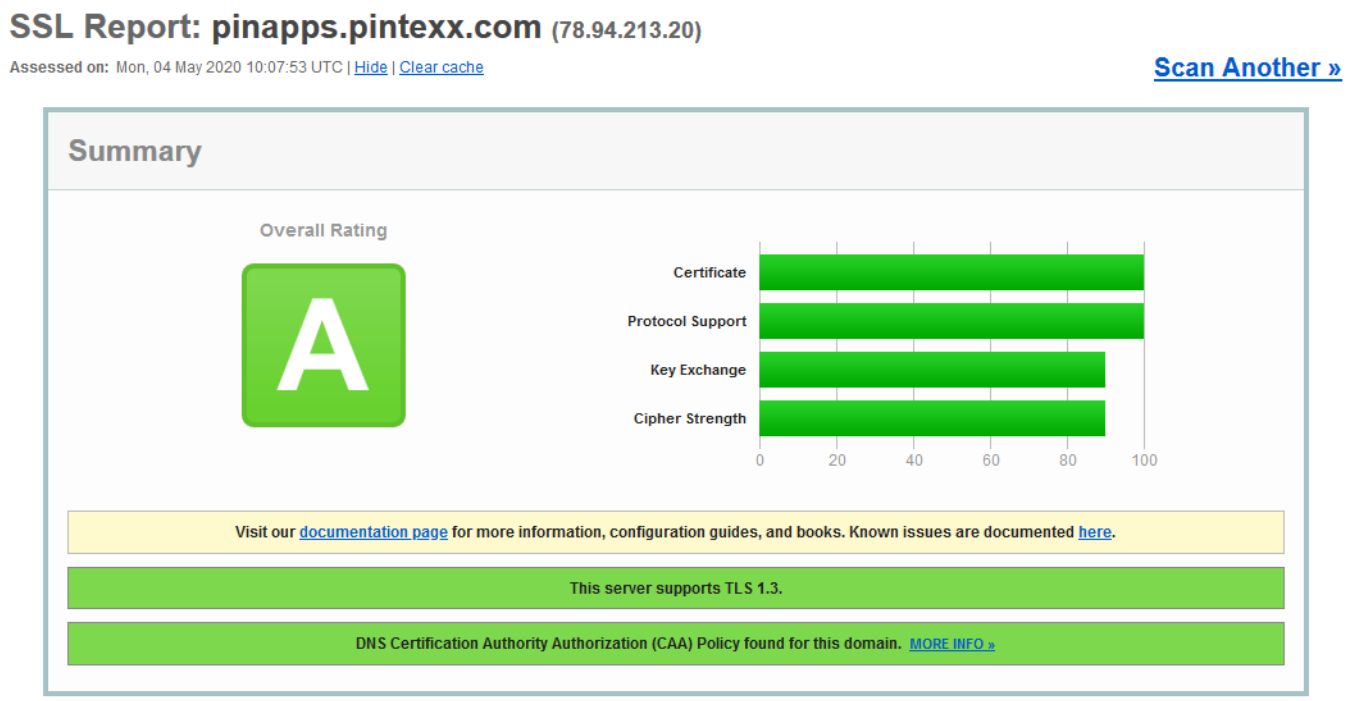
In den meistgenutzten Betriebs-Modi erfolgt die Authentifizierung über ein Drittsystem, i.d.R. ein Active-Directory oder LDAP-System.
In diesen Modi werden KEINE benutzersensitiven Daten im System gespeichert.

Werden diese Modi nicht verwendet, so werden nur ein Anzeige-Name, ein Anmeldekennwort und ein Passwort gespeichert. Eine E-Mail-Adresse ist nur notwendig, wenn eine 2-Faktor-Authentifizierung verwendet wird und die Zusendung des Tokens per E-Mail erfolgt.

1.2 Qualität der Verschlüsselung

Die Qualität der Verschlüsselung wurde mit dem bekannten Tool von SSL Labs durchgeführt.

Das Ergebnis entspricht einer sehr guten Qualität.



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
NPN	Yes http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No

Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

Wie aus den Protokoll-Details zu erkennen ist, werden dadurch bereits bekannte Angriffe von

Poodle

Doodle

BEAST

Ticketbleed

Hartbleed

RC4

ROBOT

abgewehrt.

1.3 Penetrationstests

Ein Penetrations-Test wurde mit dem Tool OWASP ZAP der OWASP Org durchgeführt.

Ergebnis für System App:

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	7
Informational	3

Ergebnis für Applications App:

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	7
Informational	5

Ergebnis für Remote App:

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	5
Informational	2

Die Details der Reports können auf Anfrage mitgeteilt werden.

2 Virtuelle Maschine

Pintexx Workplace wird als virtuelle Maschine ausgeliefert, also als „Black Box“.

Aus diesem Grund ist es grundsätzlich nicht direkt möglich, auf das innere der VM zuzugreifen.

2.1 Firewall

Die virtuelle Maschine besitzt eine eigene Firewall.

Der Zugriff auf die VM ist nur über SSH oder über die Web-Oberfläche möglich

2.2 SSH

Der Zugriff auf die VM kann über einen speziellen Port per SSH für Support-Mitarbeiter von Pintexx erfolgen. Allerdings nur unter Verwendung eines entsprechenden Schlüssels.

2.3 Ports

In der VM Firewall sind nur die notwendigen Ports für den Betrieb der Anwendungen geöffnet.

Dazu gehören die http-Ports 80, 443, die LDAP-Ports 389, 636 sowie ein Kommunikations-Port 6000.

Weitere Ports für z.B. Monitoring (SNMP) werden nur nach Aktivierung des Features geöffnet.

3 OWASP Top 10

Das Online Web Application Security Project (kurz OWASP) hat die neuen Top 10 der häufigsten Sicherheitsrisiken für Webanwendungen veröffentlicht. Die OWASP Top 10 - 2017 sollen Entwickler, Anforderungsingenieure und das Management für Risiken der Webanwendungssicherheit sensibilisieren, und sie sind durch die große Bekanntheit auch zu einer impliziten Sicherheitsrichtlinie in der Web-Industrie geworden.

Die OWASP Top 10 - 2017 beschreiben die zehn häufigsten Sicherheitsrisiken für Webanwendungen, zeigen Angriffsvektoren auf und empfehlen Schutzmaßnahmen, wie man sich vor den Angriffen schützen kann.

3.1 A1:2017 – Injection

Injections entstehen durch die Verarbeitung von nicht vertrauenswürdigen Daten durch eine Anwendung. Diese Daten wurden hierbei nicht oder nur unzureichend validiert und behandelt. In der Vergangenheit wurden häufig SQL-Injections ausgenutzt; dennoch müssen ebenso andere Injections wie gegen LDAP-Verzeichnisse oder das Betriebssystem berücksichtigt werden.

Pintexx Workplace:

Pintexx Workplace verwendet keine SQL-Abfragen. Alle Abfragen sind objektorientiert und mit einer Limit-Anweisung versehen.

LDAP-Abfragen können nur auf vorgegebene Verzeichnisse durchgeführt werden.

3.2 A2:2017 - Fehler im Authentifizierungsmanagement

Die Authentifizierung stellt den Vorgang dar, in dem ein Benutzer seine Identität gegenüber einer Anwendung nachweist. Fehler hierbei können dazu führen, dass Angreifer Identitäten missbrauchen und sich als ein anderer Benutzer ausgeben können.

Pintexx Workplace:

In den Modi Active Directory/LDAP/Radius werden Login/Passwort nur weitergereicht und nicht gespeichert. Die Regeln für Passwort-Komplexität liegen dann bei diesen Systemen.

Die Remote App verfügt über einen Login Schutz (s. Login Schutz).

Die Admin-Zugänge für System, Applications und Remote können nach außen (Internet) komplett abgeschaltet werden.

Das System verfügt über eine 2-Faktor-Authentifizierung über mehrere Optionen.

3.3 A3:2017 - Veröffentlichung sensitiver Informationen

Durch unzureichenden Schutz sensitiver Daten sind in der Vergangenheit schwerwiegende Vorfälle entstanden. In 2016 musste Yahoo einräumen 3,5 Milliarden Nutzerdaten verloren zu haben, wobei in den Daten auch schwach gehashte (MD5) Passwörter enthalten waren. Durch den unzureichenden Schutz sind Milliarden von Passwortkombinationen und anderen sensitiven Informationen wie Bank- und Kreditkartendaten bekannt geworden.

Pintexx Workplace:

Das System speichert in den Modi Active Directory/LDAP keine sensiblen Daten, da diese in Drittsystemen verwaltet werden.

Werden lokale Benutzer verwendet, werden diese vom Administrator angelegt. Es werden nur Login/Passwort und ein Anzeigename gespeichert. Passwörter werden gehasht.

Über SSL und die Einstellung der TLS Levels wird eine perfekte Forward Secrecy erreicht.

Die Sicherheit kann weiter durch Setzen des HSTS Headers erhöht werden.

3.4 A4:2017 - XML External Entities (XXE)

Der XML-Standard sieht es vor externe Daten in ein XML-Dokument nachzuladen. Wer das bei der Verarbeitung dieser Dokumente nicht berücksichtigt, riskiert eine unberechtigte Befehlsausführung, den Abfluss interner Informationen oder Dienstversagen.

Pintexx Workplace:

Das System verwendet XML ausschließlich zur Konfiguration von Parametern. Es werden keine XML-Dateien im- oder exportiert.

3.5 A5:2017 - Fehler im Zugriffsmanagement

Wird das Zugriffsmanagement nicht stringent umgesetzt, können Benutzer auf Daten zugreifen, die nicht für sie freigegeben sind. Beim Design einer Anwendung muss deshalb zwingend und klar definiert werden, wie Benutzer sich gegenüber einer Anwendung authentifizieren (A2:2017) und im Folgeschritt, wenn die Identität festgestellt wurde, wozu der Benutzer berechtigt ist.

Pintexx Workplace:

Das System beinhaltet einen grundsätzlichen Zugriffsschutz. Auf eine Seite innerhalb einer Anwendung kann nur zugegriffen werden, nachdem eine Authentifizierung erfolgt ist.

Ein Benutzer kann keine Daten speichern, nur lesen.

3.6 A6:2017 - Sicherheitsrelevante Fehlkonfiguration

Werden Fehler in der Konfiguration von Systemen wie Firewalls, Webservern oder Webanwendungen gemacht, kann dies weitreichende Folgen haben. Denkbar sind von der Veröffentlichung sensitiver Informationen über unautorisierten Systemzugriff bis hin zu Dienstversagen viele Fälle.

Pintexx Workplace:

Das gesamte System wird bereits als „Black Box“ (VM) mit integrierter Firewall geliefert.

SSL/TLS sowie http-Header können leicht konfiguriert werden.

3.7 A7:2017 - Cross-Site Scripting (XSS)

Bestimmte Zeichen müssen dem Browser als Sonderzeichen übergeben werden, da andernfalls der Browser diese als Befehle interpretiert. Wer das sogenannte Output Escaping nicht beherrscht, riskiert Cross-Site Scripting, wodurch Angreifer möglicherweise Cookie-Informationen abgreifen oder Seiten verunstalten können.

Pintexx Workplace:

Der Benutzer hat keine Möglichkeit, Daten einzugeben.

Die gesamte Administration kann nach außen (Internet) abgeschaltet werden.

Bei den Administratoren werden alle relevanten Eingabe-Felder über Schemen validiert.

3.8 A8:2017 - Unsichere Deserialisierung

Bei einer Serialisierung werden komplexe Datenstrukturen in eine sequentielle Zeichenkette umgewandelt. Der umgekehrte Prozess – die Deserialisierung – kann ausgenutzt werden, um fremde Befehle auszuführen.

Pintexx Workplace:

Deserialisierung wird nur an einer Stelle im Kern der Anwendung verwendet.Diese wird nur nach erfolgter Authentifizierung erreicht.

3.9 A9:2017 - Verwendung unsicherer Komponenten

In der heutigen Welt von Frameworks und Softwarebibliotheken verwenden Entwickler sehr häufig fremden Code. Was Effizienz- und Sicherheitsvorteile bietet, kann gleichfalls zum Einfallstor für Hacker werden. Nachdem Sicherheitslücken von Softwarekomponenten bekannt werden, muss unverzüglich für ein Update gesorgt werden. Das Bewusstsein und die Verwendung sicherer Komponenten stellt eine große Herausforderung dar.

Pintexx Workplace:

Das System verwendet ein eigenes Framework auf Basis von jQuery.

3.10 A10:2017 - Unzureichender Einsatz von Logging und Überwachung

Logging und die Analyse dieser Daten stellen den wichtigsten Weg dar, einen Angriff auf die eigenen Systeme zu erkennen. Ebenso müssen Fehler der Anwendung im laufenden Betrieb protokolliert und an die verantwortlichen Stellen kommuniziert werden.

Pintexx Workplace:

Das System verfügt über ein intensives Logging sämtlicher Aktivitäten. Alle auftretenden Fehler in allen verwendeten Modulen werden festgehalten und dem Administrator zur Verfügung gestellt.

Das System verfügt über eine SNMP- und Zabbix-Schnittstelle zur Systemüberwachung.

4 Sicherer Zugriff

Pintexx Workplace verfügt über die Möglichkeit, eine verschlüsselte Verbindung einzurichten. Dies kann über Konfiguration von Zertifikaten, die Einstellung von Sicherheitsebenen, die Verwendung von Headern und Cookie-Eigenschaften und andere Maßnahmen erfolgen.

4.1 Zertifikate

Pintexx Workplace unterstützt die Verwendung eigener Zertifikate als auch das freie Zertifikats-System „Lets Encrypt“. Dabei wird eine p12-Datei in das System importiert und im zentralen Zugangssystem (Proxy) eingerichtet. Dadurch gilt die Verschlüsselung ausnahmslos allen Browser-Zugriffen.

4.2 TLS Selektion

Über die Möglichkeit den TLS-Level auszuwählen kann eine maßgebliche Steigerung der Zugriffssicherheit erreicht werden. Durch die ausschließliche Verwendung von TLSv1.2 oder TLSv1.3 können die meisten bekannten Angriffe bereits abgewehrt werden.

4.3 Header

Pintexx Workplace verfügt über die Möglichkeit, bestimmte sicherheits-relevante Header zu setzen.

Dazu gehören z.B.

X-Frame-Options
X-Content-Type-Options
X-XSS-Protection
Strict-Transport-Security
Content-Security-Policy

4.4 Cookie

Die verwendeten Cookies verfügen alle über die HttpOnly-Eigenschaft.

4.5 Automatische Umleitung

Eine automatische Umleitung von http auf https kann eingerichtet werden.

4.6 Login Schutz

Wird ein falsches Login eingegeben, dann wird ein Zeitraum von 5 Sekunden serverseitig abgewartet. Mit jedem weiteren falschen Login erhöht sich die Wartezeit um weitere 5 Sekunden. Sobald ein richtiges Login angegeben wird, wird der Zeitraum zurückgesetzt.

4.7 Admin Zugriff

Das System wird über eine Web-Oberfläche von einem Administrator konfiguriert.

Die Zugänge für Benutzer und Administratoren sind grundsätzlich getrennt.
Aus diesem Grund ist es auch möglich, den Administrator-Zugriff über das Internet auf Netzwerk-Ebene abzuschalten.
Somit ist nur noch ein Zugriff über eine lokale IP-Adresse möglich.

4.8 Gateway

Pintexx Workplace verfügt über ein sog. Gateway, welches den Zugriff eines Browsers über Web Sockets auf einen PC über das RDP-Protokoll ermöglicht.

Das Gateway ist ein eigenständiger Web-Server, der unabhängig vom Portal oder Administration arbeitet.

Ist eine korrekte Authentifizierung und Autorisierung am Benutzer-Portal erfolgt, so erfolgt zusätzlich eine Authentifizierung am Gateway.
Diese Authentifizierung kann nur vom Portal über eine lokale IP-Adresse erfolgen und gibt ein Zugriffs-Token zurück. Mit diesem Token kann dann der Zugriff auf den PC erfolgen.

Ein direkter Zugriff über das Internet auf das Gateway zur Erhalt eines Tokens ist somit nicht möglich.

4.9 2-Faktor-Authentifizierung

Pintexx Workplace verfügt über eine 2-Faktor-Authentifizierung für eine zweite Sicherheitsebene.

Für den 2. Faktor stehen mehrere Optionen wie E-Mail, SMS, Google Authenticator oder Radius.
Eine Code-Zahl wird über die genannten Mechanismen dem Benutzer zugänglich gemacht.

Ist die Standard-Authentifizierung über Login/Passwort erfolgt, muss als nächster Schritt die Code-Zahl eingegeben werden.

Erst danach ist ein Zugriff auf das nachfolgende System möglich.