



# **WEB APPLICATION AUDIT "DIGITAL ONBOARDING"**

**Bericht, 02.10.2024**

VERTRAULICH

**Basler Kantonalbank**

Nicolas Bruggmann  
Aeschenvorstadt 41  
4002 Basel  
Schweiz



(+41) 64 266 21 24



[nicolas.bruggmann@bkb.ch](mailto:nicolas.bruggmann@bkb.ch)

# 1 MANAGEMENT SUMMARY

## 1.1 Auftrag und Testrahmen





Der vorliegende Bericht präsentiert die Prüfergebnisse des Web Application Security Audits "Digital Onboarding" des Kunden Basler Kantonalbank (nachfolgend Kunde genannt). Alle technischen Überprüfungen fanden zwischen dem 04.09.2024 und dem 13.09.2024 statt, wobei alle Schritte im Onboarding nach der E-Mail Verifikation erst ab dem 10.09.2024 zum Testen verfügbar waren.

Bei dem durchgeführten Security Audit wurden folgende Ziele getestet:


PRÜFZIEL	BESCHREIBUNG
<b>Webapplikationsaudit</b>	<p>Die Digital Onboarding Webanwendung wurde gemäss des «OWASP Testing Guides», welcher sich als Industriesicherheitsstandard etabliert hat, auf verschiedenste Arten von Schwachstellen überprüft. Zusätzlich wurde der Audit durch weitere Checks der InfoGuard ergänzt.</p> <p>Zu diesem Zweck wurde mittels automatisierter Ansätze (Tools, Scanner) als auch manueller Arbeit Tests an der Webanwendung sowie dem Server durchgeführt. Ziel war es Schwachstellen aus Sicht eines professionellen Angreifers zu identifizieren.</p> <p>Als Teil der Prüfung wurden Defensivmassnahmen, wie die Web Application Firewall (WAF) auf der Hauptseite für den Prüfer deaktiviert, dazu wurde die IP 85.195.223.145 auf der WAF freigeschalten. Auf den externen Einbindungen wurde dies nicht gemacht.</p> <p>Das Digitale Onboarding war unter der <a href="https://zak.int.cler.ch/">https://zak.int.cler.ch/</a> Webadresse (URL) verfügbar und die externen Einbindungen unter folgenden URLs:</p> <ul style="list-style-type: none"> <li>• <a href="https://sandbox-autoid.id-validation.ch/">https://sandbox-autoid.id-validation.ch/</a></li> <li>• <a href="https://go.test.online-ident.ch/">https://go.test.online-ident.ch/</a></li> <li>• <a href="https://ai.test.online-ident.ch/">https://ai.test.online-ident.ch/</a></li> <li>• <a href="https://api.test.online-ident.ch/">https://api.test.online-ident.ch/</a></li> </ul> <p>Vom Prüfrahmen ausgeschlossen waren alle weitere Funktionalitäten von Zak wie auch die Teile der externen Systemen, welche nicht beim Onboarding verwendet werden.</p> <p>Für den Audit wurde ein interner Benutzer <code>ing-ldg</code> erstellt, um die BKB-interne Sicht der Applikation zu betrachten. Der Zugriff dieses Benutzers auf die interne Applikation funktionierte jedoch während des Testzeitraums nicht. Deshalb wurde die BKB-interne Sicht von einigen der erstellten Fällen über Screen-Sharing kurz betrachtet.</p>

## 2 SCHWACHSTELLENKLASSIFIKATION



Die folgende Tabelle listet die verschiedenen Klassen von Schwachstellen auf und gibt eine Standardmassnahme für das Beheben der Sicherheitsrisiken vor. Diese Empfehlung soll aber lediglich als Standardempfehlung verstanden werden. Grundsätzlich sollte für jede Massnahme vor der Umsetzung eine Kosten/Nutzen Analyse durchgeführt werden, sofern dies für das jeweilige Risiko vertretbar ist.




SYMBOL	HINTERGRUNDINFORMATION
 Schwerwiegende Schwachstelle	<b>TECHNISCH</b>  Unmittelbare Bedrohung des Systems: ein Ausnutzen der Schwachstelle kann zur Übernahme der Kontrolle über ein System bzw. zum Abfluss von sensitiven Informationen führen.
	<b>KONZEPTIONELL / ORGANISATORISCH</b>  Grobe Fehler im Design des Netzwerks oder ein komplettes Fehlen von konzeptionellen/organisatorischen Sicherheitsvorkehrung.
 Mittlere Schwachstelle	<b>TECHNISCH</b>  Mittelschwere Schwachstelle: keine direkte Bedrohung des Systems (in Kombination mit anderen mittelschweren Schwachstellen ist eine Bedrohung aber nicht ausgeschlossen).
	<b>KONZEPTIONELL / ORGANISATORISCH</b>  Fehler im Design des Netzwerks oder eine massgebliche Schwächung von konzeptionellen/organisatorischen Sicherheitsvorkehrungen.
 Geringe Schwachstelle	<b>TECHNISCH</b>  Geringfügige Schwachstelle: keine unmittelbare Bedrohung des Systems. Die aktuelle technische Umsetzung entspricht nicht momentanen «Best Practices»
	<b>KONZEPTIONELL / ORGANISATORISCH</b>  Abweichungen von Best Practice Ansätzen bezüglich Konzeption und Organisation.
 Information	Während der Überprüfung wurden keine Sicherheitsprobleme detektiert. Allerdings beinhalte die Antwort Informationen.



## 4.2 Externen Einbindungen

SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
api.test.online-ident.ch	V-0083	<p>Die Webapplikation erlaubt es Angreifern, durch das Besuchen gewissen Webadressen (URL) unauthentifiziert auf Benutzerdaten (Namen, E-Mail, Telefonnummer) zuzugreifen (siehe auch V-0125). Ein Beispiel eines solches URL ist:</p> <ul style="list-style-type: none"> <li><a href="https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR">https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR</a></li> </ul> <p>Dabei ist die Entropie der ID, welche gebraucht wird, um den Benutzer zu identifizieren, ungenügend, da diese einfach aus 8 Grossbuchstaben besteht. Dies ermöglicht es einem Angreifer die möglichen Werte zu erraten, und dadurch Zugriff auf die Informationen der Benutzer zu erhalten. Je mehr Benutzer es gibt, desto effizienter wird dies für den Angreifer.</p> <p>Die URLs bleiben für mehrere Tage, nachdem der Benutzer die Verifikation abgeschlossen hat, gültig. Die genaue Lebensdauer, und ob diese URLs irgendwann nicht mehr gültig sind, konnte aus zeitlichen Gründen im Zuge des Tests nicht identifiziert werden, aber beträgt mindestens 3 Tage.</p> <p>Falls es zum Beispiel 1000 aktive Onboarding Fälle gibt, bei welchen der Zugriff auf die URLs noch möglich ist, würde ein Angreifer mit einem einzelnen System durch</p>	<p>Generell sollte folgendes beachtet werden:</p> <ul style="list-style-type: none"> <li>Falls eine Variable für die Autorisierung verwendet wird, sollte sichergestellt werden, dass sie genügend Entropie hat und dadurch nicht vom Angreifer zufällig erratbar ist. Hierfür könnte zum Beispiel eine UUID verwendet werden.</li> <li>Die Webapplikation sollte dahingehend überprüft werden, dass keinerlei sensitive Informationen in URLs versendet werden. Diese sollten ausschliesslich in den Nutzdaten der HTTP-Anfragen (z.B. mit Hilfe von POST-Parameter, im Authorization Header oder als Cookie) übertragen werden.</li> <li>Für alle Daten, welche das System extern (z.B. mittels einem Web-Requests) verfügbar macht, sollte überprüft werden, dass nur die nötigen Informationen das System verlassen, wie auch das diese nur für den nötigen Zeitraum verfügbar sind. Da extern für den Benutzer nur die Telefonnummer ersichtlich ist, sollte es nur möglich sein auf dies zuzugreifen. Falls ein Onboarding-Case nach einer Stunde nicht mehr vom Benutzer vervollständigt werden kann, so sollten die dazugehörigen Daten auch nur für eine solche Dauer verfügbar sein.</li> </ul> <p>Es sollte nur für authentifizierte Benutzer möglich sein, auf ihre eigenen Daten zuzugreifen. Hierfür, sollte auch für die</p>	<div>  <p>Schwerwiegende Schwachstelle</p> </div>



SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
		<p>einen Brute-Force Angriff im Durchschnitt jede 43 Tage Zugriff auf die Daten eines Zufälligen Benutzers erhalten.</p> <p>Falls die URLs für zwei Wochen lange gültig bleiben, wie von Mesoneer geplant, und es im Jahr etwa 10'000 Self-Onboarding Fälle gibt, so könnte ein Angreifer mit einem einzelnen System im Durchschnitt jede 100 Tage die Information eines Zufälligen Kunde erhalten.</p> <p>Dieser Befund wird aufgrund der Gesetzlichen Anforderungen bei Finanzinstituten und der daraus entstehenden Kritikalität der Daten als Schwerwiegend eingeschätzt. Würden die Informationen, welche herausgegeben werden, auf das für die Webapplikation benötigte Minimum (nur Telefonnummer) reduziert werden, würde dies als Mittlere Schwachstelle gesehen werden.</p>	<p>externen Einbindungen ein robustes Autorisierung-Schema und Authentifizierung-Schema verwendet werden.</p> <p>Für das Digitale Onboarding, und die Übergänge, die darin stattfinden, könnte man wie folgt vorgehen:</p> <p><b>Für die Weiterleitungen im gleichen Browser:</b> Hier könnte man den Übergang mittels einem Post-Request machen. Der Post-Request könnte im Körper entweder ein JSON Web Token (JWT) beinhalten, welches der Empfänger validieren kann, oder einen einmal-gültigen Token, der im Hintergrund zwischen den Seiten, zusammen mit dem Case, kommuniziert wurde. Die Empfängerseite, kann dann diesen Token oder JWT brauchen, um für den Benutzer ein Cookie oder Token zu erstellen, welches mit dem spezifischen Case zusammenhängt. Dann sollte der Zugriff auf Case-spezifischen Daten nur mittels dieses Cookies oder Token möglich sein.</p> <p><b>Für die Weiterleitung mittels QR-Codes:</b> Falls die Weiterleitung via einen QR-Code durchgeführt wird, sollte der Link im QR-Code nur für einen kurzen Zeitraum gültig sein und verwendet werden, um die Browser-Session mit dem Case zu verlinken. Dies kann wieder durch einen einmal-gültigen Token oder einem JWT durchgeführt werden, bei welchen die Seite dann ein Cookie oder Token erstellt, welches gebraucht wird, um den Zugriff auf die Case-spezifischen Daten zu limitieren. Zudem sollten hierfür nur die strikt nötigen Informationen exponiert werden. Im vorliegenden Fall, zum Beispiel, wird nur die Telefonnummer des Benutzers vom Client gebraucht. Die</p>	


SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
			anderen Informationen müssen nicht im Frontend zugänglich sein und können deshalb auch so gesetzt werden, dass sie nie das Backend verlassen. Zusätzlich könnte man auch die Telefonnummer nicht mehr dem Benutzer zeigen, und stattdessen einen Text verwenden, der einfach sagt, dass eine SMS versendet wird.	
sandbox-autoid.id-validation.ch	V-0086	<p>Es wurden die folgenden Information-Disclosure-Mängel identifiziert:</p> <ul style="list-style-type: none"> <li>Der Webserver retourniert Standardfehlerseiten, welche die genaue Versionsnummer (nginx 1.25.5) bekanntgeben.</li> </ul> <p>Einem Angreifer ist es dadurch möglich, effizient in öffentlichen Exploit-Datenbanken nach bekannten Schwachstellen zu dieser Version zu suchen, um diese im Anschluss einfach und schnell auszunutzen.</p>	Die Konfiguration des Webserver sollte gehärtet werden, sodass keine internen Informationen wie zum Beispiel Versionsinformationen über HTTP-Header, Standardfehlerseiten oder Standardwebseiten bekanntgegeben werden.	 <p>Mittlere Schwachstelle</p>
sandbox-autoid.id-validation.ch	V-0090	<p>Die verwendete Webserver Version nginx 1.25.5 ist gemäss der folgenden Webseite veraltet und enthält bekannte Schwachstellen mit mittlerer Kritikalität:</p> <ul style="list-style-type: none"> <li><a href="https://nginx.org/en/security_advisories.html">https://nginx.org/en/security_advisories.html</a></li> </ul> <p>Es wird darauf hingewiesen, dass diese Schwachstelle ausschliesslich auf der bekannten Versionsnummer basiert und daher fehlerhaft sein könnte.</p>	Es sollte überprüft werden, ob der Webserver tatsächlich veraltet ist. Ist dies der Fall, so sollte ein Patch-Management-Prozess implementiert werden, welcher den Webserver berücksichtigt. Falls bereits ein Patch-Management-Prozess existiert, dann sollte der Webserver zum bestehenden Prozess hinzugefügt werden, um sicherzustellen, dass dieser laufend auf die aktuelle Version aktualisiert wird.	 <p>Mittlere Schwachstelle</p>




SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
go.test.online-ident.ch	V-0091	<p>Die folgenden zusätzlichen Netzwerkdienste wurden identifiziert, welche auf dem Webserver betrieben werden und aus dem Internet erreichbar sind:</p> <ul style="list-style-type: none"> <li>TCP-Port 22 (SSH)</li> </ul> <p>Das Exponieren solcher Dienste im Internet erhöht die externe Angriffsfläche und daraus resultierend auch das Sicherheitsrisiko, da eine Schwachstelle in einer der Dienste unmittelbare negative Auswirkungen auf die im Prüfraum befindliche Webapplikation hat.</p>	<p>Um die externe Angriffsfläche zu minimieren, sollten die identifizierten Netzwerkdienste deaktiviert, deinstalliert oder der externe Zugriff aus dem Internet unterbunden oder eingeschränkt werden, da diese nicht für den erfolgreichen Betrieb der im Prüfraum befindlichen Webapplikation benötigt werden.</p> <p>Falls der SSH-Dienst nicht deaktiviert werden kann, dann sollte die Passwort-basierte Authentifizierung unterbunden werden, da diese sonst gegen Brute-Force Angriffe anfällig sein kann.</p>	 <p>Mittlere Schwachstelle</p>
sandbox-autoid.id-validation.ch	V-0097	<p>Auf Basis von Versionsinformationen, welche in JavaScript-Dateien identifiziert wurden, verwendet die Webapplikation die folgenden veralteten JavaScript-Bibliotheken:</p> <ul style="list-style-type: none"> <li>pdf.js 2.14.305 und 3.6.172</li> </ul> <p>Kommen tatsächlich diese Versionen zum Einsatz, so enthält die Webapplikation bekannte Schwachstellen mit hohem Schweregrad. Informationen zu den existierenden Schwachstellen können den folgenden Webadressen entnommen werden:</p> <ul style="list-style-type: none"> <li><a href="https://security.snyk.io/package/npm/pdfjs-dist/2.14.305">https://security.snyk.io/package/npm/pdfjs-dist/2.14.305</a></li> </ul>	<p>Zunächst sollte überprüft werden, ob die betroffene JavaScript-Bibliothek tatsächlich veraltet ist, da die Identifikation dieser Schwachstelle ausschliesslich auf der veröffentlichten Softwareversion basiert. Wenn dies der Fall ist, dann sollte die Bibliothek auf die neueste Version aktualisiert werden.</p>	 <p>Mittlere Schwachstelle</p>
go.test.online-ident.ch	V-0100	<p>Die go.test.online-ident.ch Webanwendung verwendet nicht bei allen Anfragen, in welchen Benutzerdaten involviert sind, einen Cache-Control-Header. Deshalb können alle</p>	<p>Die Webapplikation sollte sicherstellen, dass keine Webseiten mit sensiblen Informationen in Komponenten wie Webproxys oder Webbrowsern im Browser-Cache gespeichert werden</p>	

SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
		<p>Komponenten (z. B. Webproxy oder Webbrowser), die die angeforderten Ressourcen (z. B. eine Webseite) verarbeitet, diese Ressourcen zwischenspeichern.</p> <p>Angreifer, die Zugriff auf eine dieser Komponenten haben, können dann die zwischengespeicherten Daten lesen, um potenziell wertvolle Informationen zu erhalten.</p>	<p>können. Eine solche Anweisung kann in HTTP-Antworten durch Setzen der folgenden Header umgesetzt werden:</p> <pre>Cache-Control: no-cache, no-store Expires: 0 Pragma: no-cache</pre>	<p>Mittlere Schwachstelle</p>
sandbox-autoid.id-validation.ch	V-0119	<p>Die Applikation setzt den HTTP Header "Access-Control-Allow-Origin: *". Dadurch kann ein Angreifer den Browser eines Opfers missbrauchen, um die Applikation zu verwenden.</p> <p>Wenn eine zugriffsberechtigte Person auf eine bösartige Webseite surft, erhält die bösartige Webseite Zugriff auf alle nicht authentisierten Bereiche der Applikation und kann in diesem Bereich auch Schwachstellen ausnutzen.</p>	<p>Es sollten nur vertrauenswürdige Domains zugelassen werden, die wirklich in der CORS Policy benötigt werden.</p> <p>Zum Beispiel:</p> <pre>Access-Control-Allow-Origin: ai.test.online-ident.ch</pre>	<p></p> <p>Mittlere Schwachstelle</p>
go.test.online-ident.ch	V-0088	<p>Die Webapplikation bindet externen JavaScript-Code in die eigenen Webseiten ein. Diese externen Ressourcen werden von den folgenden Webservern bezogen:</p> <ul style="list-style-type: none"> <li><a href="https://api.xs2a.com">https://api.xs2a.com</a></li> <li><a href="https://cdnjs.cloudflare.com/ajax/libs/pdf.js">https://cdnjs.cloudflare.com/ajax/libs/pdf.js</a></li> </ul> <p>Dies stellt ein potentiellles Sicherheitsrisiko dar, da die Kompromittierung einer dieser Webserver unmittelbar negative Auswirkungen auf die Sicherheit der eigenen Webapplikation hat. Zusätzlich wird das Risiko erhöht, dass sensitive Informationen und das Benutzerverhalten</p>	<p>Falls möglich, sollten alle extern gehosteten Ressourcen lokal auf dem Webserver gespeichert werden. In diesem Falle hat die Kompromittierung externer Webserver keine Auswirkungen auf die Sicherheit der Webapplikation.</p>	<p></p> <p>Geringe Schwachstelle</p>



SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
		unabsichtlich den externen Betreibern der Webserver bekanntgegeben werden.		
sandbox-autoid.id-validation.ch  test.online-ident.ch	V-0089	Die Applikation test.online-ident.ch und sandbox-autoid.id-validation.ch benutzten keine <code>Permissions-Policy</code> oder <code>Feature-Policy</code> Header. Dies erlaubt einem Angreifer möglicherweise Zugang zu Ressourcen, die ihm verwahrt bleiben sollten und lässt den Browser Geräte nicht schützen.	Die folgenden Massnahmen sollten getroffen werden: <ul style="list-style-type: none"> <li>• Limitierung der Direktiven, die von der Applikation verwendet werden auf den Scope 'self'.</li> <li>• Entfernen von Direktiven, die von der Applikation nicht verwendet werden (bspw. falls die Kamera nicht benutzt wird: auf 'none' setzen)</li> <li>• 'Feature-Policy' sollte auf 'Permissions-Policy' umbenannt werden.</li> </ul>	 <p>Geringe Schwachstelle</p>
sandbox-autoid.id-validation.ch	V-0092	Die Webapplikation verwendet Standardfehlermeldungen, woraus sich schliessen lässt, dass der Webserver nicht ausreichend gehärtet ist. Nicht gehärtete Systeme sind nicht konform zu Security-Best-Practices und stellen ein potentiellies Sicherheitsrisiko dar, da unter Umständen mitigierende Massnahmen fehlen, die die Gesamtsicherheit erhöhen.	Die Konfiguration des Webserver, der Webapplikation sowie das verwendete Betriebssystem sollten gehärtet werden, um die Widerstandsfähigkeit gegen erfolgreiche Angriffe zu erhöhen. Beispiele solcher Massnahmen sind: <ul style="list-style-type: none"> <li>• Entfernung von Standardfehlermeldungen sowie von Standarddateien, welche Teil der Installation sind.</li> <li>• Deaktivierung von Webservermodulen, welche nicht von der Webapplikation benötigt werden.</li> <li>• Verwendung eines dedizierten Service-Accounts für den Webserver, welcher niedrige Privilegien besitzt.</li> <li>• Zentrale Speicherung der Webserverlogs.</li> </ul>	 <p>Geringe Schwachstelle</p>

SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
			<p>Das Center for Internet Security (CIS) publiziert Hardening Guidelines für eine Vielzahl an Softwareanwendungen inklusive gängiger Webserver und Betriebssysteme. Diese Hardening Guidelines können über die folgende Webseite heruntergeladen werden:</p> <ul style="list-style-type: none"> <li><a href="https://www.cisecurity.org/cis-benchmarks/">https://www.cisecurity.org/cis-benchmarks/</a></li> </ul>	
test.online-ident.ch	V-0093	<p>Bei der Analyse der bestehenden Konfiguration des HTTP Strict Transport Security (HSTS) Headers wurden die folgenden Mängel identifiziert:</p> <ul style="list-style-type: none"> <li>Das Attribut <code>includeSubDomains</code> wird nicht verwendet.</li> </ul>	<p>Um die Sicherheit der Webapplikation zu erhöhen, sollte die Implementierung des HSTS-Headers den folgenden Anforderungen entsprechen:</p> <ol style="list-style-type: none"> <li>Der HSTS-Header sollte vom Webserver bei allen HTTPS-Anfragen retourniert werden.</li> <li>Das Attribut <code>max-age</code> des HSTS-Headers sollte grösser als 10368000 Sekunden (120 Tage) und idealerweise 31536000 Sekunden (ein Jahr) betragen.</li> <li>RFC 6797, Abschnitt 14.4 empfiehlt die Verwendung des Attributs <code>includeSubDomains</code>.</li> <li>Es wird nicht empfohlen, die HSTS-Richtlinie mit dem Attribute <code>http-equiv</code> des Metatags zu setzen, da Browser diese Richtlinie unter Umständen ignorieren.</li> </ol> <p>Aus diesem Grund wird die Implementierung des folgenden HSTS-Headers empfohlen, welcher für ein Jahr gültig ist:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre>	<div>  <p>Geringe Schwachstelle</p> </div>

SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
ai.test.online-ident.ch go.test.online-ident.ch api.test.online-ident.ch	V-0098	<p>Bei der Webapplikation <code>go.test.online-ident.ch</code> kommt der <code>X-Content-Type-Options</code> (XCTO) Header nicht zum Einsatz. Das Fehlen dieses Headers führt dazu, dass bestimmte Browser versuchen, den Inhaltstyp und die Encodierung der Antwort zu erraten, selbst wenn diese Eigenschaften bereits vom Webserver definiert sind. Dieses Verhalten kann von Angreifern u. U. ausgenutzt werden, um einen sogenannten MIME-Type-Sniffing-Angriff durchzuführen.</p> <p>Weitere Informationen zu diesem Header können der folgenden Webseite entnommen werden:</p> <p><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options</a></p>	<p>Die Konfiguration des Webserver sollte aktualisiert werden, sodass der folgende XCTO-Header zum Einsatz kommt:</p> <pre>X-Content-Type-Options: nosniff</pre>	 <p>Geringe Schwachstelle</p>
sandbox-autoid.id-validation.ch	V-0122	<p>Der Dienst beinhaltet TLS Chiffren Sammlungen, welche nicht den AEAD (Authenticated Encryption with Associated Data) Modus verwenden. Dies entspricht nicht mehr den best-practice Empfehlungen.</p>	<p>Die TLS-Version sollte auf TLS v1.2 oder idealerweise TLS v1.3 umgestellt werden. Für TLS v1.2 sollten nur AEAD (Authenticated Encryption with Associated Data) Chiffren Sammlungen verwendet werden.</p>	 <p>Geringe Schwachstelle</p>
api.test.online-ident.ch sandbox-autoid.id-validation.ch	V-0125	<p>Es wurden folgende Webadressen (URLs) identifiziert, welche Session-Informationen im GET-Parameter übertragen.</p> <ul style="list-style-type: none"> <li><a href="https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR">https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR</a></li> </ul>	<p>Die Webapplikation sollte aktualisiert werden, um sicherzustellen, dass keinerlei sensitive Informationen in URLs, sondern ausschliesslich in den Nutzdaten der HTTP-Anfragen (z.B. mit Hilfe von POST-Parameter) übertragen werden.</p>	 <p>Geringe Schwachstelle</p>

SYSTEME	ID	RESULTAT	MASSNAHME	BEWERTUNG
		<ul style="list-style-type: none"> <li><a href="https://sandbox-autoid.id-validation.ch/api/v1/internal/scheduled-cases/ed72bd9e-72c8-42d4-9419-99d4dc55e1f5?idToken=undefined">https://sandbox-autoid.id-validation.ch/api/v1/internal/scheduled-cases/ed72bd9e-72c8-42d4-9419-99d4dc55e1f5?idToken=undefined</a></li> </ul> <p>Solche URLs stellen ein mögliches Sicherheitsrisiko dar, da sie an mehreren Stellen, wie z. B. Webproxy-, Webserver-Logs oder vom Browser selbst während deren Übertragung aufgezeichnet werden können. Ein Angreifer mit Zugriff auf eine dieser Stellen kann die preisgegebenen Informationen im Anschluss missbrauchen, um auf die IDs zuzugreifen. (TST-WCPQTU-LR und ed72bd9e-72c8-42d4-9419-99d4dc55e1f5). Diese erlauben den Zugriff auf Benutzerdaten (Namen, E-Mail, Telefonnummer, Nationalität) zuzugreifen (siehe auch V-0083).</p>	<p>Generauere Empfehlungen, wie das für die Webapplikation umgesetzt werden, können der Schwachstelle mit ID V-0083 entnommen werden.</p>	

## 5 PRÜFKATALOG

---

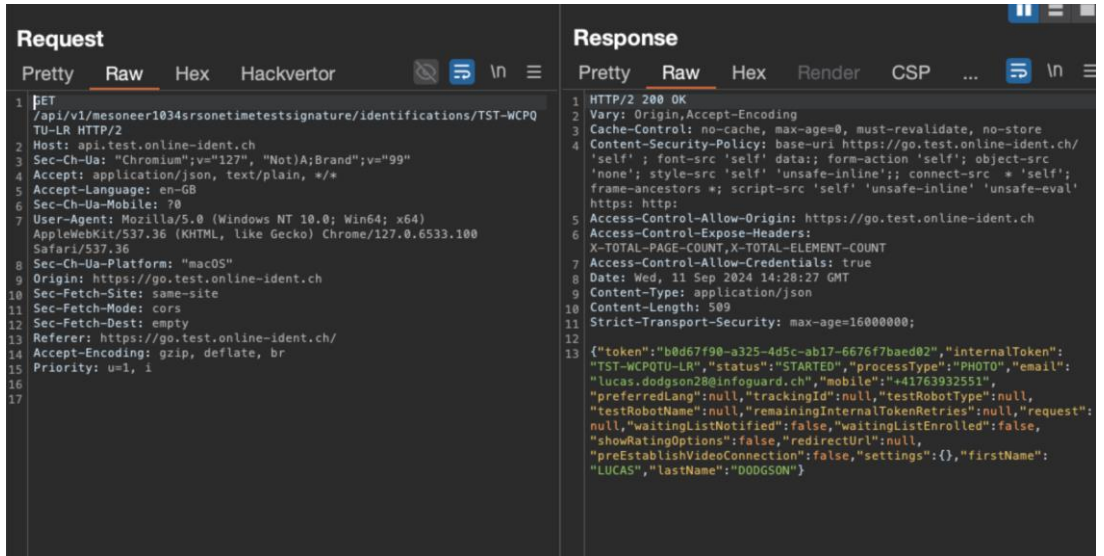

Anhand des Prüfkataloges ist ersichtlich, welche Überprüfungen die InfoGuard vorgenommen hat. Dieser beinhaltet folgenden Punkte:

- **ID:** Details aus Kapitel 4 können mittels dieser ID nachgeschlagen werden.
- **GUID:** Eindeutige Referenz des Checks.
- **Frage:** Die Prüffrage, welche sich der Auditor für die Überprüfung stellt.
- **Resultat:** Das Resultat, welche die Überprüfung ergab sowie eine Beschreibung der daraus resultierenden Risiken.
- **Massnahme:** Massnahmenvorschläge für die Reduzierung der Risiken.
- **PoC:** Beschreibung des Vorgehens, um die Schwachstelle zu reproduzieren.
- **Bewertung:** Das resultierende Risiko der Überprüfung

## 5.2 Externen Einbindungen

ZUSÄTZLICHE CHECKS	
Zugriff auf Ressourcen anderer Benutzer (V-0083)	
GUID	53312a02-fdb8-44ff-8245-2308037c0512
Frage	Können nicht authentifizierte Benutzer auf sensitive Daten zugreifen?
Resultat	<p>Die Webapplikation erlaubt es Angreifern, durch das Besuchen gewissen Webadressen (URL) unauthentifiziert auf Benutzerdaten (Namen, E-Mail, Telefonnummer) zuzugreifen (siehe auch V-0125). Ein Beispiel eines solchen URL ist:</p> <ul style="list-style-type: none"> <li><a href="https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR">https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR</a></li> </ul> <p>Dabei ist die Entropie der ID, welche gebraucht wird, um den Benutzer zu identifizieren, ungenügend, da diese einfach aus 8 Grossbuchstaben besteht. Dies ermöglicht es einem Angreifer die möglichen Werte zu erraten, und dadurch Zugriff auf die Informationen der Benutzer zu erhalten. Je mehr Benutzer es gibt, desto effizienter wird dies für den Angreifer.</p> <p>Die URLs bleiben für mehrere Tage, nachdem der Benutzer die Verifikation abgeschlossen hat, gültig. Die genaue Lebensdauer, und ob diese URLs irgendwann nicht mehr gültig sind, konnte aus zeitlichen Gründen im Zuge des Tests nicht identifiziert werden, aber beträgt mindestens 3 Tage.</p>

	<p>Falls es zum Beispiel 1000 aktive Onboarding Fälle gibt, bei welchen der Zugriff auf die URLs noch möglich ist, würde ein Angreifer mit einem einzelnen System durch einen Brute-Force Angriff im Durchschnitt jede 43 Tage Zugriff auf die Daten eines Zufälligen Benutzers erhalten.</p> <p>Falls die URLs für zwei Wochen lange gültig bleiben, wie von Mesoneer geplant, und es im Jahr etwa 10'000 Self-Onboarding Fälle gibt, so könnte ein Angreifer mit einem einzelnen System im Durchschnitt jede 100 Tage die Information eines Zufälligen Kunde erhalten.</p> <p>Dieser Befund wird aufgrund der Gesetzlichen Anforderungen bei Finanzinstituten und der daraus entstehenden Kritikalität der Daten als Schwerwiegend eingeschätzt. Würden die Informationen, welche herausgegeben werden, auf das für die Webapplikation benötigte Minimum (nur Telefonnummer) reduziert werden, würde dies als Mittlere Schwachstelle gesehen werden.</p>
Massnahme	<p>Generell sollte folgendes beachtet werden:</p> <ul style="list-style-type: none"> <li>Falls eine Variable für die Autorisierung verwendet wird, sollte sichergestellt werden, dass sie genügend Entropie hat und dadurch nicht vom Angreifer zufällig erratbar ist. Hierfür könnte zum Beispiel eine UUID verwendet werden.</li> <li>Die Webapplikation sollte dahingehend überprüft werden, dass keinerlei sensitive Informationen in URLs versendet werden. Diese sollten ausschliesslich in den Nutzdaten der HTTP-Anfragen (z.B. mit Hilfe von POST-Parameter, im Authorization Header oder als Cookie) übertragen werden.</li> <li>Für alle Daten, welche das System extern (z.B. mittels einem Web-Requests) verfügbar macht, sollte überprüft werden, dass nur die nötigen Informationen das System verlassen, wie auch das diese nur für den nötigen Zeitraum verfügbar sind. Da extern für den Benutzer nur die Telefonnummer ersichtlich ist, sollte es nur möglich sein auf dies zuzugreifen. Falls ein Onboarding-Case nach einer Stunde nicht mehr vom Benutzer vervollständigt werden kann, so sollten die dazugehörigen Daten auch nur für eine solche Dauer verfügbar sein.</li> </ul> <p>Es sollte nur für authentifizierte Benutzer möglich sein, auf ihre eigene Daten zuzugreifen. Hierfür, sollte auch für die externen Einbindungen ein robustes Autorisierung-Schema und Authentifizierung-Schema verwendet werden.</p> <p>Für das Digitale Onboarding, und die Übergänge, die darin stattfinden, könnte man wie folgt vorgehen:</p> <p><b>Für die Weiterleitungen im gleichen Browser:</b> Hier könnte man den Übergang mittels einem Post-Request machen. Der Post-Request könnte im Körper entweder ein JSON Web Token (JWT) beinhalten, welches der Empfänger validieren kann, oder einen einmal-gültigen Token, der im Hintergrund zwischen den Seiten, zusammen mit dem Case, kommuniziert wurde. Die Empfängerseite, kann dann diesen Token oder JWT brauchen, um für den Benutzer ein Cookie oder Token zu erstellen, welches mit dem spezifischen Case zusammenhängt. Dann sollte der Zugriff auf Case-spezifischen Daten nur mittels dieses Cookies oder Token möglich sein.</p>

	<p><b>Für die Weiterleitung mittels QR-Codes:</b> Falls die Weiterleitung via einen QR-Code durchgeführt wird, sollte der Link im QR-Code nur für einen kurzen Zeitraum gültig sein und verwendet werden, um die Browser-Session mit dem Case zu verlinken. Dies kann wieder durch einen einmal-gültigen Token oder einem JWT durchgeführt werden, bei welchen die Seite dann ein Cookie oder Token erstellt, welches gebraucht wird, um den Zugriff auf die Case-spezifischen Daten zu limitieren. Zudem sollten hierfür nur die strikt nötigen Informationen exponiert werden. Im vorliegenden Fall, zum Beispiel, wird nur die Telefonnummer des Benutzers vom Client gebraucht. Die anderen Informationen müssen nicht im Frontend zugänglich sein und können deshalb auch so gesetzt werden, dass sie nie das Backend verlassen. Zusätzlich könnte man auch die Telefonnummer nicht mehr dem Benutzer zeigen, und stattdessen einen Text verwenden, der einfach sagt, dass eine SMS versendet wird.</p>
Betroffene Systeme	api.test.online-ident.ch
PoC	<p>Folgender Screenshot zeigt ein Beispiel einer solcher Webanfrage, die ohne weitere Cookies oder Authentifizierung-Information auf die Daten eines Benutzers zugreifen kann.</p> 
Bewertung	<div style="text-align: center;">   Schwerwiegende Schwachstelle </div>

## WEB APPLICATION SECURITY AUDIT

### ALLGEMEINE INFORMATIONEN ZUM SCOPE DES AUDITS

**Scope - Dokumentation des Prüfrahmens (V-0084)**

KUNDE: BASLER KANTONALBANK

DATEI:

WEB APPLICATION AUDIT "DIGITAL ONBOARDING"


ORT, DATUM: BAAR, 02.10.2024

KLASSIFIZIERUNG:


VERTRAULICH

89 | 119



GUID	126ba981-3e69-4960-9003-133c970c4f4e
Frage	Was ist der Prüfraum des Penetration Tests?
Resultat	<p>Dieser Abschnitt beinhaltet alle Befunde, welche für die externen Einbindungen zutreffen:</p> <ul style="list-style-type: none"> <li>• <a href="https://sandbox-autoid.id-validation.ch">https://sandbox-autoid.id-validation.ch</a></li> <li>• <a href="https://go.test.online-ident.ch">https://go.test.online-ident.ch</a></li> <li>• <a href="https://api.test.online-ident.ch">https://api.test.online-ident.ch</a></li> <li>• <a href="https://ai.test.online-ident.ch">https://ai.test.online-ident.ch</a></li> </ul> <p>Die gleichen Testeinschränkungen, wie in V-0002 beschrieben treffen auch hier zu.</p>
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### Scope - Auditlokation (V-0085)

GUID	05b8b7fc-76da-4e6c-ace5-65abd5d663c2
Frage	Wo wurde das Audit durchgeführt und welche Quell-IP-Adresse wurde dabei verwendet?
Resultat	Der Audit wurde aus dem Internet mit der öffentlichen IP-Adresse 85.195.223.145 durchgeführt.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### INFORMATIONSSAMMLUNG (WSTG-INFO)

#### Fingerprint Environment (V-0086)

KUNDE: BASLER KANTONALBANK



DATEI:

WEB APPLICATION AUDIT "DIGITAL  
ONBOARDING"

ORT, DATUM: BAAR, 02.10.2024


KLASSIFIZIERUNG:

VERTRAULICH

GUID	ae8279d6-f174-4c07-897e-8cf832a36120
Frage	Gibt die Webapplikation Informationen über die verwendete Webserverversion, verwendete Webframeworks oder eingesetzte Sicherheitsprodukte bekannt?
Resultat	<p>Es wurden die folgenden Information-Disclosure-Mängel identifiziert:</p> <ul style="list-style-type: none"> <li>Der Webserver retourniert Standardfehlerseiten, welche die genaue Versionsnummer (nginx 1.25.5) bekanntgeben.</li> </ul> <p>Einem Angreifer ist es dadurch möglich, effizient in öffentlichen Exploit-Datenbanken nach bekannten Schwachstellen zu dieser Version zu suchen, um diese im Anschluss einfach und schnell auszunutzen.</p>
Massnahme	Die Konfiguration des Webserver sollte gehärtet werden, sodass keine internen Informationen wie zum Beispiel Versionsinformationen über HTTP-Header, Standardfehlerseiten oder Standardwebseiten bekanntgegeben werden.
Betroffene Systeme	sandbox-autoid.id-validation.ch
PoC	<p>Der folgende Screenshot, zeigt eine Standardfehlerseite, welche eine Detaillierte nginx Version zurückgibt.</p> 
Bewertung	 <p>Mittlere Schwachstelle</p>

#### Informationsabflüsse durch Webseiteninhalte (V-0087)

GUID	e1271b61-8eca-40bb-ad6b-65d9011c224e
------	--------------------------------------

Frage	Enthalten HTML-Kommentare oder Meta-Tags sensible Informationen?
Resultat	HTML-Kommentare und Metatags des Webverkehrs wurden analysiert, um sicherheitsrelevante Informationen (z.B. Benutzernamen, Hostnamen, Passwörter etc.) zu identifizieren. Im Zuge dessen konnten keine sensiblen Informationen identifiziert werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### Verwendung externer Ressourcen in Webapplikation (V-0088)

GUID	061d8532-9ac2-452e-92ff-a0bbaec198cb
Frage	Bindet die Webapplikation externe Ressourcen ein?
Resultat	<p>Die Webapplikation bindet externen JavaScript-Code in die eigenen Webseiten ein. Diese externen Ressourcen werden von den folgenden Webservern bezogen:</p> <ul style="list-style-type: none"> <li>• <a href="https://api.xs2a.com">https://api.xs2a.com</a></li> <li>• <a href="https://cdnjs.cloudflare.com/ajax/libs/pdf.js">https://cdnjs.cloudflare.com/ajax/libs/pdf.js</a></li> </ul> <p>Dies stellt ein potentiellles Sicherheitsrisiko dar, da die Kompromittierung einer dieser Webserver unmittelbar negative Auswirkungen auf die Sicherheit der eigenen Webapplikation hat. Zusätzlich wird das Risiko erhöht, dass sensitive Informationen und das Benutzerverhalten unabsichtlich den externen Betreibern der Webserver bekanntgegeben werden.</p>
Massnahme	Falls möglich, sollten alle extern gehosteten Ressourcen lokal auf dem Webserver gespeichert werden. In diesem Falle hat die Kompromittierung externer Webserver keine Auswirkungen auf die Sicherheit der Webapplikation.
Betroffene Systeme	go.test.online-ident.ch
PoC	Folgende Screenshots zeigt eine Webanfragen, bei welcher die Antworten die externen Seiten referenzieren.

Request	Response
<pre> 1 GET /app/en/mesoneer1034srsonetimetests/signature/identifications/TST-WCPQTU-LR/identification/start HTTP/2 2 Host: go.test.online-ident.ch 3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99" 4 Sec-Ch-Ua-Mobile: ?0 5 Sec-Ch-Ua-Platform: "macOS" 6 Accept-Language: en-GB 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Sec-Fetch-Site: cross-site </pre>	<pre> 47 &lt;script type="text/javascript" src=" ./assets/clientInfo.js"&gt;&lt;/script&gt; 48 &lt;script type="text/javascript" src=" ./assets/identifyInsights.js"&gt;&lt;/script&gt; 49 &lt;script src="https://api.k2a.com/ks2a.js"&gt;&lt;/ script&gt; 50 &lt;link rel="stylesheet" href=" https://api.k2a.com/ks2a_base.css"&gt; 51 &lt;style&gt;:root{--surface-a:#ffffff;--surface-b: #f4f4f4;--surface-c:#eaeaea;--surface-d:#c8c8c8; --surface-e:#ffffff;--surface-f:#ffffff;--text-color: #333333;--text-color-secondary:#848484; --primary-color:#007ad9;--primary-color-text:#ffffff; --font-family:-apple-system, BlinkMacSystemFont, Segoe UI, Roboto, Helvetica, Arial, sans-serif, Apple Color Emoji, Segoe UI Emoji, Segoe UI Symbol; </pre>
Request	Response
<pre> 1 GET /app/997.f914be7b90fb0abf.js HTTP/2 2 Host: go.test.online-ident.ch 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: https://go.test.online-ident.ch/app/en/mesoneer1034srsonetimetests/signature/identifications/TST-VABBG-TMK/identification/facetec 8 Dnt: 1 9 Sec-Gpc: 1 10 Sec-Fetch-Dest: script 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Site: same-origin 13 Te: trailers </pre>	<pre> r[_ngcontent-%COMP%].content-wrapper[_ngcontent-%COMP%]{padding:15px;margin:15px 0}.page-wrapper[_ngcontent-%COMP%].content-wrapper[_ngcontent-%COMP%].btn-wrapper[_ngcontent-%COMP%]{text-align:center}}),t,t(),k=r(5080),q=r(1355),I=r(7899),D=r(8028),S=r(1924),ee=r(6878),te=r(7324),oe=r(7757),F=r.n(oe),z=r(6036),re=function(){var t=function(){function l(o,n){(0,y.Z)(this,l),this.documentUploadService=n,this.document=o;var p="https://cdn.jsdelivr.net/npm/pdf.js/pdf.worker.min.js";z.concat(z.version,"/pdf.worker.min.js");z.GlobalWorkerOptions.workerSrc=p;return(0,b.Z)(l,{key:"pdfToImageDataURLAsync",value:function(n){return function(t,l,o,n){return new o  (o=Promise)}(function(a,c){function i(s){try{d(n.next(s))}catch(m){c(m)}}function u(s){try{d(n.throw(s))}catch(m){c(m)}}function d(s){s.done?a(s.value):function p(a){return a instanceof o?a:new o(function(c){c(a)})(s.value).then(i,u)}d((n=n.apply(t,l  [])).next())}}(this,void 0,void 0,F).mark(function p(){var a,c,i,u,d,s,v,j,l;return F().wrap(function(f){for(;;)switch(f.prev=f.next){case 0:return f.next=2,new Response(n).arrayBuffer();case 2:return a=f.sent,c=this.document.createElement("canvas"),i=c.getContext("2d"),u=a,f.next=6,(0,z.getDocument)(u).promise;case 6:return d=f.sent,f.next=9,d.getPage(1);case 9:return v=(s=f.sent).getViewport({scale:2}),c.height=v.height,c.width=v. </pre>

Bewertung

Geringe Schwachstelle

## KONFIGURATIONS- UND DEPLOYMENT-MANAGEMENT-TESTS (WSTG-CONFIG)

### Permissions-Policy (Old: Feature Policy) (V-0089)

GUID	509f7753-6fba-4e86-bdac-3e32443e99bd
Frage	Ist die Permissions-Policy für die Applikation angemessen?
Resultat	Die Applikation test.online-ident.ch und sandbox-autoid.id-validation.ch benutzten keine Permissions-Policy oder Feature-Policy Header. Dies erlaubt einem Angreifer möglicherweise Zugang zu Ressourcen, die ihm verwahrt bleiben sollten und lässt den Browser

KUNDE: BASLER KANTONALBANK

DATEI:

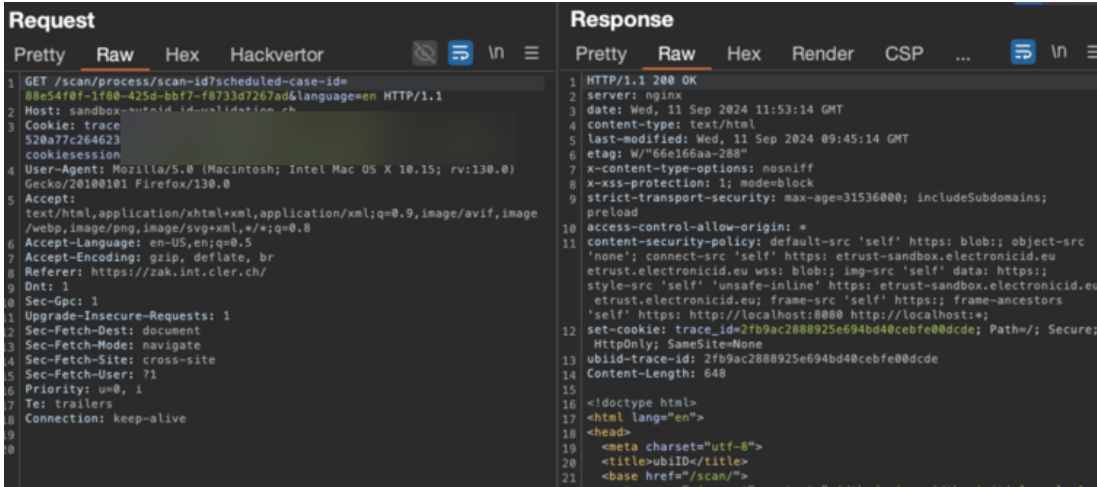
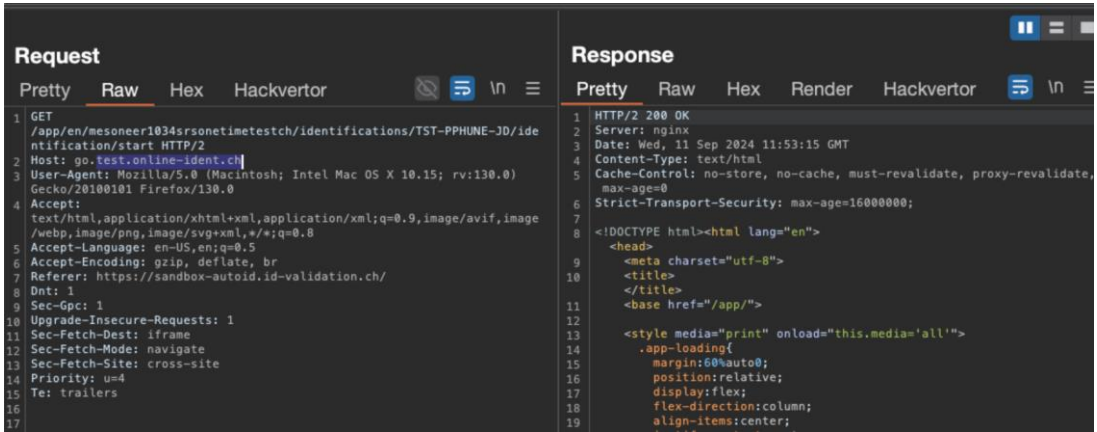
WEB APPLICATION AUDIT "DIGITAL ONBOARDING"


ORT, DATUM: BAAR, 02.10.2024

KLASSIFIZIERUNG:

VERTRAULICH

93 | 119

	Geräte nicht schützen.	
Massnahme	<p>Die folgenden Massnahmen sollten getroffen werden:</p> <ul style="list-style-type: none"> <li>Limitierung der Direktiven, die von der Applikation verwendet werden auf den Scope 'self'.</li> <li>Entfernen von Direktiven, die von der Applikation nicht verwendet werden (bspw. falls die Kamera nicht benutzt wird: auf 'none' setzen)</li> <li>'Feature-Policy' sollte auf 'Permissions-Policy' umbenannt werden.</li> </ul>	
Betroffene Systeme	<p>sandbox-autoid.id-validation.ch</p> <p>test.online-ident.ch</p>	
PoC	<p>Folgende Screenshots zeigen Webanfragen, bei welchen im Antwortheader keine Permissions oder Feature Policy Headers gesetzt sind.</p>  	

Bewertung	 Geringe Schwachstelle
<b>Schwachstellen in Webserver (V-0090)</b>	
GUID	3dc8dba0-e026-4f89-bb1e-4058cd3c128b
Frage	Existieren bekannte Schwachstellen für den im Scope befindlichen Webserver?
Resultat	<p>Die genaue Webserver Version <code>nginx 1.25.5</code> wurde auf standard-Fehlerseiten (V-0086) identifiziert. Gemäss der folgenden Webseite ist diese Version veraltet und enthält bekannte Schwachstellen mit mittleren Kritikalität:</p> <ul style="list-style-type: none"> <li>• <a href="https://nginx.org/en/security_advisories.html">https://nginx.org/en/security_advisories.html</a></li> </ul> <p>Es wird darauf hingewiesen, dass diese Schwachstelle ausschliesslich auf der bekannten Versionsnummer basiert und daher fehlerhaft sein könnte.</p>
Massnahme	Es sollte überprüft werden, ob der Webserver tatsächlich veraltet ist. Ist dies der Fall, so sollte ein Patch-Management-Prozess implementiert werden, welcher den Webserver berücksichtigt. Falls bereits ein Patch-Management-Prozess existiert, dann sollte der Webserver zum bestehenden Prozess hinzugefügt werden, um sicherzustellen, dass dieser laufend auf die aktuelle Version aktualisiert wird.
Betroffene Systeme	sandbox-autoid.id-validation.ch
PoC	Folgender Screenshot zeigt die bekannten Schwachstellen in <code>nginx 1.25.5</code>

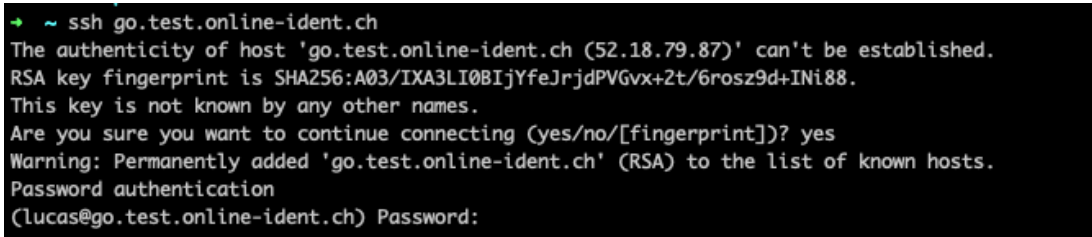

- Buffer overread in the ngx\_http\_mp4\_module  
Severity: low  
[Advisory](#)  
[CVE-2024-7347](#)  
Not vulnerable: 1.27.1+, 1.26.2+  
Vulnerable: 1.5.13-1.27.0  
[The patch](#) [pgp](#)
- Buffer overwrite in HTTP/3  
Severity: medium  
[Advisory](#)  
[CVE-2024-32760](#)  
Not vulnerable: 1.27.0+, 1.26.1+  
Vulnerable: 1.25.0-1.25.5, 1.26.0
- Stack overflow and use-after-free in HTTP/3  
Severity: medium  
[Advisory](#)  
[CVE-2024-31079](#)  
Not vulnerable: 1.27.0+, 1.26.1+  
Vulnerable: 1.25.0-1.25.5, 1.26.0
- NULL pointer dereference in HTTP/3  
Severity: medium  
[Advisory](#)  
[CVE-2024-35200](#)  
Not vulnerable: 1.27.0+, 1.26.1+  
Vulnerable: 1.25.0-1.25.5, 1.26.0
- Memory disclosure in HTTP/3  
Severity: medium  
[Advisory](#)  
[CVE-2024-34161](#)  
Not vulnerable: 1.27.0+, 1.26.1+  
Vulnerable: 1.25.0-1.25.5, 1.26.0

Folgender Screenshot zeigt die Fehlerseite, welche die Version retourniert:




Bewertung




	Mittlere Schwachstelle
<b>Netzwerkconfiguration des Webservers (V-0091)</b>	
GUID	a6aa1219-5d71-4ef7-ad2a-d7ec1cfd4102
Frage	Sind zusätzliche Netzwerkdienste (z.B. FTP) aus dem Internet erreichbar, welche jedoch nicht für den erfolgreichen Betrieb der im Scope befindlichen Webapplikation benötigt werden?
Resultat	<p>Die folgenden zusätzlichen Netzwerkdienste wurden identifiziert, welche auf dem Webserver betrieben werden und aus dem Internet erreichbar sind:</p> <ul style="list-style-type: none"> <li>TCP-Port 22 (SSH)</li> </ul> <p>Das Exponieren solcher Dienste im Internet erhöht die externe Angriffsfläche und daraus resultierend auch das Sicherheitsrisiko, da eine Schwachstelle in einer der Dienste unmittelbare negative Auswirkungen auf die im Prüfraum befindliche Webapplikation hat.</p>
Massnahme	<p>Um die externe Angriffsfläche zu minimieren, sollten die identifizierten Netzwerkdienste deaktiviert, deinstalliert oder der externe Zugriff aus dem Internet unterbunden oder eingeschränkt werden, da diese nicht für den erfolgreichen Betrieb der im Prüfraum befindlichen Webapplikation benötigt werden.</p> <p>Falls der SSH-Dienst nicht deaktiviert werden kann, dann sollte die Passwort-basierte Authentifizierung unterbunden werden, da diese sonst gegen Brute-Force Angriffe anfällig sein kann..</p>
Betroffene Systeme	go.test.online-ident.ch
PoC	<p>Folgender Screenshot zeigt, dass der SSH Dienst exponiert ist.</p> 
Bewertung	 <p>Mittlere Schwachstelle</p>



## Applikationsplattform Konfiguration (V-0092)

GUID	aaeb25a4-5560-475c-809b-4e9689307f3e
Frage	Weist die Konfiguration des verwendeten Applikations-Frameworks Verwundbarkeiten auf?
Resultat	Die Webapplikation verwendet Standardfehlermeldungen, woraus sich schliessen lässt, dass der Webserver nicht ausreichend gehärtet ist. Nicht gehärtete Systeme sind nicht konform zu Security-Best-Practices und stellen ein potentielltes Sicherheitsrisiko dar, da unter Umständen mitigierende Massnahmen fehlen, die die Gesamtsicherheit erhöhen.
Massnahme	<p>Die Konfiguration des Webserver, der Webapplikation sowie das verwendete Betriebssystem sollten gehärtet werden, um die Widerstandsfähigkeit gegen erfolgreiche Angriffe zu erhöhen. Beispiele solcher Massnahmen sind:</p> <ul style="list-style-type: none"> <li>Entfernung von Standardfehlermeldungen sowie von Standarddateien, welche Teil der Installation sind.</li> <li>Deaktivierung von Webservermodulen, welche nicht von der Webapplikation benötigt werden.</li> <li>Verwendung eines dedizierten Service-Accounts für den Webserver, welcher niedrige Privilegien besitzt.</li> <li>Zentrale Speicherung der Webserverlogs.</li> </ul> <p>Das Center for Internet Security (CIS) publiziert Hardening Guidelines für eine Vielzahl an Softwareanwendungen inklusive gängiger Webserver und Betriebssysteme. Diese Hardening Guidelines können über die folgende Webseite heruntergeladen werden:</p> <ul style="list-style-type: none"> <li><a href="https://www.cisecurity.org/cis-benchmarks/">https://www.cisecurity.org/cis-benchmarks/</a></li> </ul>
Betroffene Systeme	sandbox-autoid.id-validation.ch
PoC	<p>Folgender Screenshot zeigt eine Standardfehlerseite:</p> 

Bewertung	 Geringe Schwachstelle
Konfiguration von HTTP Strict Transport Security (HSTS) (V-0093)	
GUID	de49d908-f19a-4cdc-8e92-6a8debce0a7e
Frage	Verwendet die Webapplikation einen HTTP Strict Transport Security (HSTS) Header und ist dieser angemessen konfiguriert?
Resultat	<p>Bei der Analyse der bestehenden Konfiguration des HTTP Strict Transport Security (HSTS) Headers wurden die folgenden Mängel identifiziert:</p> <ul style="list-style-type: none"> <li>Das Attribut <code>includeSubDomains</code> wird nicht verwendet.</li> </ul>
Massnahme	<p>Um die Sicherheit der Webapplikation zu erhöhen, sollte die Implementierung des HSTS-Headers den folgenden Anforderungen entsprechen:</p> <ol style="list-style-type: none"> <li>Der HSTS-Header sollte vom Webserver bei allen HTTPS-Anfragen retourniert werden.</li> <li>Das Attribut <code>max-age</code> des HSTS-Headers sollte grösser als 10368000 Sekunden (120 Tage) und idealerweise 31536000 Sekunden (ein Jahr) betragen.</li> <li>RFC 6797, Abschnitt 14.4 empfiehlt die Verwendung des Attributs <code>includeSubDomains</code>.</li> <li>Es wird nicht empfohlen, die HSTS-Richtlinie mit dem Attribute <code>http-equiv</code> des Metatags zu setzen, da Browser diese Richtlinie unter Umständen ignorieren.</li> </ol> <p>Aus diesem Grund wird die Implementierung des folgenden HSTS-Headers empfohlen, welcher für ein Jahr gültig ist:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre>
Betroffene Systeme	test.online-ident.ch
PoC	Folgender Screenshot zeigt, dass für go.test.online-ident.ch der HSTS-Header das Attribut <code>includeSubDomains</code> nicht verwendet.


Request	Response
<pre> 1 GET /api/v1/resources/00535dab-4e67-4ec4-9ff8-2b64f9da7d1f/font/thin   HTTP/2 2 Host: ai.test.online-ident.ch 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0)   Gecko/20100101 Firefox/130.0 4 Accept:   application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: https://go.test.online-ident.ch/ 8 Origin: https://go.test.online-ident.ch 9 Dnt: 1 10 Sec-Gpc: 1 </pre>	<pre> 1 HTTP/2 200 OK 2 Vary: Origin,Accept-Encoding 3 Content-Security-Policy: script-src 'self'; base-uri 'none'   frame-ancestors 'self'; style-src 'self' 'unsafe-inline';   form-action 'self'; default-src 'self'; object-src 'none' 4 Access-Control-Allow-Origin: https://go.test.online-ident. 5 Access-Control-Expose-Headers:   X-TOTAL-PAGE-COUNT,X-TOTAL-ELEMENT-COUNT 6 Access-Control-Allow-Credentials: true 7 Date: Wed, 11 Sep 2024 12:30:13 GMT 8 Strict-Transport-Security: max-age=16000000; 9 10 @SIG b </pre>

Bewertung




Geringe Schwachstelle

### Content Security Policy (CSP) (V-0094)


GUID	c1efaba5-ef78-4967-a382-68e36bd5cb5a
Frage	Verwendet die Webapplikation einen Content Security Policy (CSP) Header und ist dieser angemessen konfiguriert?
Resultat	Die Webapplikation verwendet einen angemessen konfigurierten Content Security Policy (CSP) Header.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

### Cross-Domain Referrer Leakage (V-0095)

GUID	b7d07ec9-3c48-4900-9af0-677d1d745606
Frage	Gibt die Webapplikation Dritten sensitive Informationen über den HTTP-Header Referrer bekannt?
Resultat	Es wurden keine sensitiven Informationen identifiziert, welche externen Webapplikationen über den HTTP-Header Referrer bekanntgegeben wurden.

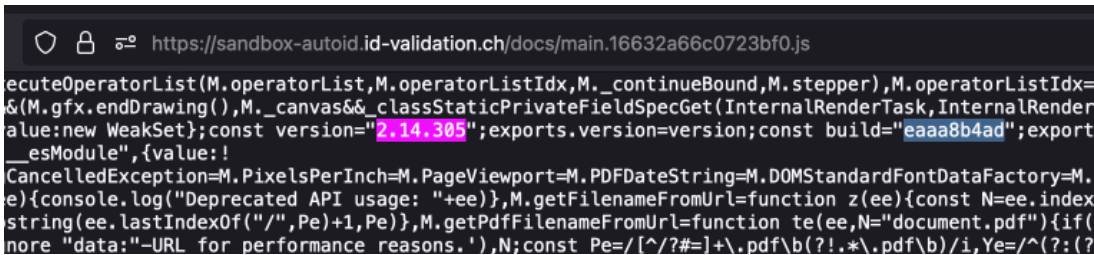
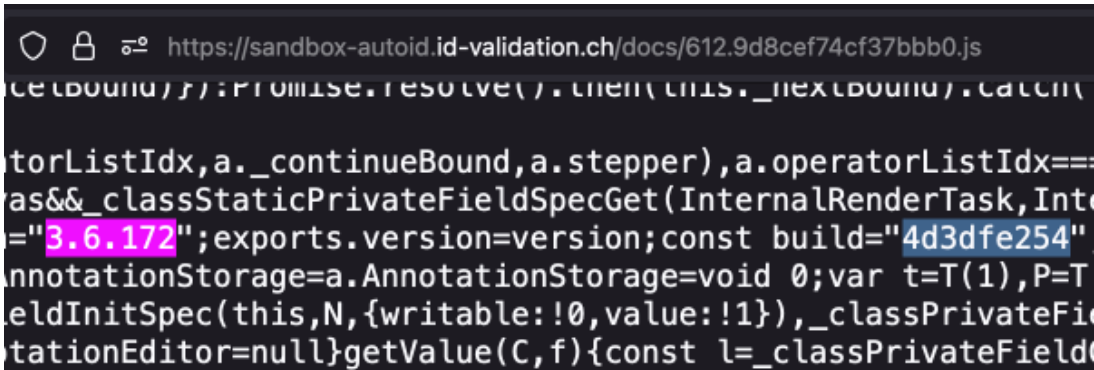
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### GET/POST Interchangeability (V-0096)

GUID	561f404f-eb36-4aa3-9da7-92300096ddba
Frage	Akzeptiert die Webapplikation GET-Parameter die üblicherweise als POST-Parameter übertragen werden?
Resultat	Der Webserver lehnte die Verarbeitung von GET-Parametern ab, die eigentlich als POST-Parameter gesendet werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### Veraltete JavaScript-Bibliotheken in Verwendung (V-0097)

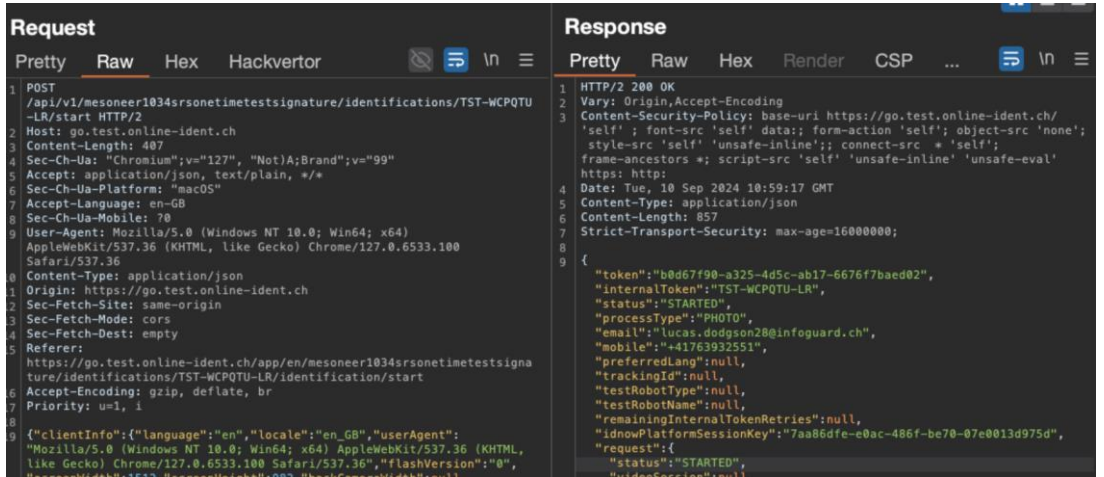
GUID	3a9b5e8b-b225-4f58-a092-c3c83ffd1369
Frage	Sind die verwendeten JavaScript Bibliotheken auf dem aktuellen Stand?
Resultat	<p>Auf Basis von Versionsinformationen, welche in JavaScript-Dateien identifiziert wurden, verwendet die Webapplikation die folgenden veralteten JavaScript-Bibliotheken:</p> <ul style="list-style-type: none"> <li>pdf.js 2.14.305 und 3.6.172</li> </ul> <p>Kommen tatsächlich diese Versionen zum Einsatz, so enthält die Webapplikation bekannte Schwachstellen mit hohem Schweregrad. Informationen zu den existierenden Schwachstellen können den folgenden Webadressen entnommen werden:</p>

	<ul style="list-style-type: none"> <li><a href="https://security.snyk.io/package/npm/pdfjs-dist/2.14.305">https://security.snyk.io/package/npm/pdfjs-dist/2.14.305</a></li> </ul>
Massnahme	<p>Zunächst sollte überprüft werden, ob die betroffene JavaScript-Bibliothek tatsächlich veraltet ist, da die Identifikation dieser Schwachstelle ausschliesslich auf der veröffentlichten Softwareversion basiert. Wenn dies der Fall ist, dann sollte die Bibliothek auf die neueste Version aktualisiert werden.</p>
Betroffene Systeme	<p>sandbox-autoid.id-validation.ch</p>
PoC	<p>Die folgenden Screenshots dokumentieren die Indikatoren, dass die JavaScript-Bibliotheken verwendet werden:</p> <p>pdf.js 2.14.305:</p>  <p>pdf.js 3.6.172:</p>  <p>Gemäss folgendem Screenshot ist diese JavaScript-Bibliothek veraltet und enthalten bekannte Schwachstellen:</p>


	<div> <div> <p><b>pdfjs-dist@2.14.305 vulnerabilities</b></p> <p>Generic build of Mozilla's PDF.js library.</p> </div> <div> <p><b>Direct Vulnerabilities</b></p> <p>Known vulnerabilities in the pdfjs-dist package. This does not include vulnerabilities belonging to this package's dependencies.</p> <p>Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.</p> <p>Fix for free</p> </div> <div> <table> <thead> <tr> <th>VULNERABILITY</th><th>VULNERABLE VERSION</th></tr> </thead> <tbody> <tr> <td> <div> <div>H</div> <p><b>Arbitrary Code Injection</b></p> <p>pdfjs-dist is a Portable Document Format (PDF) library that is built with HTML5.</p> <p>Affected versions of this package are vulnerable to Arbitrary Code Injection in <code>font_loader.js</code>, which passes input to the <code>eval()</code> function when the default <code>isEvalSupported</code> option is in use. An attacker can execute code by convincing a user to open a malicious PDF file.</p> <p>How to fix Arbitrary Code Injection?</p> <p>Upgrade <code>pdfjs-dist</code> to version 4.2.67 or higher.</p> </div> <div>&lt;4.2.67</div> </td><td></td></tr> </tbody> </table> </div> <div> <p>LATEST VERSION</p> <p>4.6.82</p> <hr/> <p>LATEST NON VULNERABLE VERSION</p> <p>4.6.82</p> <hr/> <p>FIRST PUBLISHED</p> <p>10 years ago</p> <hr/> <p>LATEST VERSION PUBLISHED</p> <p>10 days ago</p> <hr/> <p>LICENSES DETECTED</p> <p>Apache-2.0 &gt;=0</p> <hr/> <p><a href="#">View pdfjs-dist package health on Snyk Advisor</a></p> </div> <div> <p>Report a new vulnerability</p> <p>Found a mistake?</p> </div> </div>	VULNERABILITY	VULNERABLE VERSION	<div> <div>H</div> <p><b>Arbitrary Code Injection</b></p> <p>pdfjs-dist is a Portable Document Format (PDF) library that is built with HTML5.</p> <p>Affected versions of this package are vulnerable to Arbitrary Code Injection in <code>font_loader.js</code>, which passes input to the <code>eval()</code> function when the default <code>isEvalSupported</code> option is in use. An attacker can execute code by convincing a user to open a malicious PDF file.</p> <p>How to fix Arbitrary Code Injection?</p> <p>Upgrade <code>pdfjs-dist</code> to version 4.2.67 or higher.</p> </div> <div>&lt;4.2.67</div>	
VULNERABILITY	VULNERABLE VERSION				
<div> <div>H</div> <p><b>Arbitrary Code Injection</b></p> <p>pdfjs-dist is a Portable Document Format (PDF) library that is built with HTML5.</p> <p>Affected versions of this package are vulnerable to Arbitrary Code Injection in <code>font_loader.js</code>, which passes input to the <code>eval()</code> function when the default <code>isEvalSupported</code> option is in use. An attacker can execute code by convincing a user to open a malicious PDF file.</p> <p>How to fix Arbitrary Code Injection?</p> <p>Upgrade <code>pdfjs-dist</code> to version 4.2.67 or higher.</p> </div> <div>&lt;4.2.67</div>					
Bewertung	<div> <div></div> <p>Mittlere Schwachstelle</p> </div>				
Content Sniffing (V-0098)					
GUID	275190e4-f157-46b4-a211-6a06b61ab03a				
Frage	Verwendet die Webapplikation einen X-Content-Type-Options (CTO) Header und ist dieser angemessen konfiguriert?				
Resultat	<p>Bei der Webapplikation <code>go.test.online-ident.ch</code> kommt der X-Content-Type-Options (XCTO) Header nicht zum Einsatz. Das Fehlen dieses Headers führt dazu, dass bestimmte Browser versuchen, den Inhaltstyp und die Enkodierung der Antwort zu erraten, selbst wenn diese Eigenschaften bereits vom Webserver definiert sind. Dieses Verhalten kann von Angreifern u. U. ausgenutzt werden, um einen sogenannten MIME-Type-Sniffing-Angriff durchzuführen.</p> <p>Weitere Informationen zu diesem Header können der folgenden Webseite entnommen werden:</p> <p><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options</a></p>				
Massnahme	<p>Die Konfiguration des Webserver sollte aktualisiert werden, sodass der folgende XCTO-Header zum Einsatz kommt:</p> <pre>X-Content-Type-Options: nosniff</pre>				

Betroffene Systeme	ai.test.online-ident.ch go.test.online-ident.ch api.test.online-ident.ch
PoC	<p>go.test.online-ident.ch verwendet den XCTO Header, wie im folgenden Screenshot ersichtlich, nicht:</p> <div><div><div>Request</div><div><div>PrettyRawHexHackvortor</div><div><div>1GET /api/v1/resources/a5c1352f-68f7-4103-94ac-d28ae0975959/font/medium HTTP/2</div><div>2Host: ai.test.online-ident.ch</div><div>3User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0</div><div>4Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8</div><div>5Accept-Language: en-US,en;q=0.5</div><div>6Accept-Encoding: gzip, deflate, br</div><div>7Referer: https://go.test.online-ident.ch/</div><div>8Origin: https://go.test.online-ident.ch</div><div>9Dnt: 1</div><div>10Sec-Gpc: 1</div><div>11Sec-Fetch-Dest: font</div><div>12Sec-Fetch-Mode: cors</div><div>13Sec-Fetch-Site: same-site</div><div>14Te: trailers</div></div></div></div><div><div>Response</div><div><div>PrettyRawHexRenderMetadat...</div><div><div>1HTTP/2 200 OK</div><div>2Vary: Origin,Accept-Encoding</div><div>3Content-Security-Policy: script-src 'self'; base-uri 'none'; frame-ancestors 'self'; style-src 'self' 'unsafe-inline'; form-action 'self'; default-src 'self'; object-src 'none'</div><div>4Access-Control-Allow-Origin: https://go.test.online-ident.ch</div><div>5Access-Control-Expose-Headers: X-TOTAL-PAGE-COUNT,X-TOTAL-ELEMENT-COUNT</div><div>6Access-Control-Allow-Credentials: true</div><div>7Date: Wed, 11 Sep 2024 09:40:25 GMT</div><div>8Strict-Transport-Security: max-age=16000000;</div><div>9</div><div>10@DSIG;0m1 GP0Si*RIiä:pGSUB ~{Ä=TLTSH:rr-ä0S/24;WE`VDMXyZcE\$'äcmap</div><div>R5 Sucvt</div><div>ä ZT*fgpmW 5Xsgasp .iDglyf;A]Dähdmx)g* B headÿ iL6hhea{ \$hmtxü</div><div>ü x{ loca0IZ6Amaxp'E"</div><div>name ' WAL'p0st0ncRCprepM=0 Y EA"0Ü_&lt;ä0I ä0 "cÜpp#</div></div></div></div></div>
Bewertung	<div><div></div><div>Geringe Schwachstelle</div></div>

ÜBERPRÜFUNG AUTHENTIFIZIERUNG (WSTG-AUTHN)	
Unsichere Übertragung von Passwörtern (V-0099)	
GUID	6d15418b-cc73-4e2b-9957-c6352414a81e
Frage	Stellt die Webapplikation die Authentizität, Integrität und Vertraulichkeit von sensiven Informationen während der Übertragung sicher?
Resultat	Es wurden sämtliche Daten von der Webapplikation mittels Hyper Text Transfer Protocol Secure (HTTPS) sicher übertragen.
Betroffene Systeme	Externen Einbindungen
Bewertung	<div><div></div><div>Information</div></div>


Browser Cache (V-0100)	
GUID	054edf92-36ca-4d8d-8408-d703aea94038
Frage	Darf der Browser sensitive Daten im Browser-Cache speichern?
Resultat	Die go.test.online-ident.ch Webanwendung verwendet nicht bei allen Anfragen, in welchen Benutzerdaten involviert sind, einen Cache-Control-Header. Deshalb können alle Komponenten (z. B. Webproxy oder Webbrowser), die die angeforderten Ressourcen (z. B. eine Webseite) verarbeitet, diese Ressourcen zwischenspeichern. Angreifer, die Zugriff auf eine dieser Komponenten haben, können dann die zwischengespeicherten Daten lesen, um potenziell wertvolle Informationen zu erhalten.
Massnahme	<p>Die Webapplikation sollte sicherstellen, dass keine Webseiten mit sensiblen Informationen in Komponenten wie Webproxys oder Webbrowsern im Browser-Cache gespeichert werden können. Eine solche Anweisung kann in HTTP-Antworten durch Setzen der folgenden Header umgesetzt werden:</p> <pre>Cache-Control: no-cache, no-store Expires: 0 Pragma: no-cache</pre>
Betroffene Systeme	go.test.online-ident.ch
PoC	<p>Folgender Screenshot zeigt ein Beispiel, einer Antwort, die keinen Cache-Control Header hat, jedoch Benutzerdaten beinhaltet.</p> 



Bewertung	 Mittlere Schwachstelle
-----------	---

#### ÜBERPRÜFUNG AUTORISIERUNG (WSTG-AUTHZ)

##### Unautorisierte Datenbankänderungen via Overposting/Mass-Assignment-Angriffe (V-0101)




GUID	eba6f3b2-0356-4cc6-b4b4-a09532adedd4
Frage	Erlaubt die API das unberechtigte Aktualisieren von kritischen Datenbankinhalten?
Resultat	Es wurde keine Overposting- bzw. Mass-Assignment-Schwachstelle identifiziert, die eine unautorisierte Aktualisierung von sensiblen Datenbankinformationen (z. B. Gruppenmitgliedschaften) ermöglicht hätte.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### ÜBERPRÜFUNG AUTORISIERUNG (WSTG-AUTHZ)


##### OAUTH2-SPEZIFISCHE TESTS

##### Signaturprüfung (V-0102)

GUID	54ecce27-1e7a-46b2-825b-95e30bf0c0c4
Frage	Wird die Signatur der Tokens (Access Token, Refresh Token, ID Token etc.) Server-seitig überprüft?
Resultat	Der Server überprüft die Token-Signatur bei jeder Anfrage.
Betroffene Systeme	Externen Einbindungen


Bewertung	 Information
<b>Deaktivierung der Signaturprüfung des WT (V-0103)</b>	
GUID	7534a0a6-f0ce-4063-a57d-fa611ef77716
Frage	Ist es möglich die Validierung der Token-Signatur über den 'alg' Header zu deaktivieren?
Resultat	Die Signaturprüfung wird durch den Server auch bei einem mit "alg": "none" definierten JWT durchgeführt.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information
<b>Überprüfung des Token-Inhalts (V-0104)</b>	
GUID	571a418b-172f-4c3c-acb6-b35c2ae854a9
Frage	Enthält der Token ungewöhnlichen Inhalte?  Dieser Check besteht damit wir den Inhalt des Tokens überprüfen, ob nicht zum Beispiel ein Passwort im Klartext oder ähnliches gesendet wird.
Resultat	Tokens enthalten keine ungewöhnlichen oder potenziell nicht benötigte Parameter.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

### Signing Key (V-0105)

GUID	8d14822a-2b01-4999-a8e1-be85df4aac31
Frage	Ist es möglich den Signing Key zu knacken?
Resultat	Es war nicht möglich den Signing Key zu knacken.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


### ÜBERPRÜFUNG EINGABEÜBERPRÜFUNG (WSTG-INPVAL)

#### Server-Side Request Forgery (SSRF) (V-0106)


GUID	83f96ce4-fd84-426f-af20-ec23aceb4c84
Frage	Können Server-Side Request Forgery (SSRF) Schwachstellen identifiziert werden?
Resultat	Es wurde keine Server-Side Request Forgery (SSRF) Schwachstelle identifiziert.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### Reflected Cross Site Scripting (XSS) (V-0107)


GUID	f05719ea-a52a-4d92-bf31-fb62258b8d5c
Frage	Wurden Reflected Cross Site Scripting (XSS) Schwachstellen gefunden?



Resultat	Es wurde keine Reflected Cross Site Scripting (XSS) Schwachstelle identifiziert.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


#### Stored Cross Site Scripting (XSS) (V-0108)

GUID	18a954aa-feb4-488b-841b-7601a487498a
Frage	Enthält die Webapplikation eine persistente Cross Site Scripting Schwachstelle?
Resultat	Es konnten keine persistente Cross Site Scripting (XSS) Verwundbarkeiten identifiziert werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

#### HTTP Verb Tampering (V-0109)


GUID	94b9ac34-ec44-45c7-9d7d-2c83ce007b64
Frage	Werden Anfragen mit abgeändertem HTTP Methoden korrekt verarbeitet?
Resultat	Der Server verhält sich verhältnismässig, wenn falsche HTTP Methoden verwendet werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	

	Information
<b>HTTP Parameter Pollution (V-0110)</b>	
GUID	896b088c-42c0-46e1-92f3-554f00021be1
Frage	Wie werden HTTP Parameter verarbeitet welche mehrfach vorkommen?
Resultat	Es konnten keine HTTP Parameter Pollution Verwundbarkeiten identifiziert werden. Die Applikation verhält sich bei mehrfach enthaltenen Parameter nicht ungewöhnlich.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information
<b>SQL Injection (V-0111)</b>	
GUID	1655ac40-f05d-4b64-9e2b-c8aadd54d2c2
Frage	Enthält die Webapplikation SQL Injection Schwachstellen?
Resultat	Es konnten keine SQL-Injection Schwachstellen identifiziert werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information
<b>ÜBERPRÜFUNG FEHLERBEHANDLUNG (WSTG-ERR)</b>	
<b>Stacktraces (V-0112)</b>	

GUID	a7ab216c-b69a-44e6-b79d-3c631fdf1f8b
Frage	Können sensitive Informationen wie verwendete Bibliotheken aus Stacktraces ausgelesen werden?
Resultat	Während des Audits wurden keine Stacktraces entdeckt. Auch durch gezielte Aufrufe, die Exceptions auf dem Server auslösen könnten, wurden keine Stacktraces an den Client zurückgeschickt.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


#### ÜBERPRÜFUNG EINSATZ KRYPTOGRAPHISCH SCHWACHER VERFAHREN (WSTG-CRYPST)

##### Sensitive Informationen über unverschlüsselten Kanal (V-0113)

GUID	08abbca9-11c3-4c9c-b35b-78df322729df
Frage	Werden sensitive Informationen über einen unverschlüsselten Kanal versendet?
Resultat	Während dem Audit wurde keine Schwachstelle in der Handhabung von verschlüsselten Übertragungen festgestellt.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


##### Umleitung von HTTP auf HTTPS (V-0114)

GUID	ad91e432-b537-4552-9d03-a3a6cb850a2b
Frage	Wird ein Benutzer mittels eines HTTP 301 "Moved Permanently" Status auf HTTPS umgeleitet?

Resultat	Der Benutzer wird mit HTTP Status 301 auf HTTPS weitergeleitet.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information

### ÜBERPRÜFUNG GESCHÄFTSLOGIK (WSTG-BUSLOGIC)


#### Datenvalidierung Business Logic (V-0115)

GUID	917bc026-4f71-457a-a51a-9d169b5a8409
Frage	Können Probleme in der Business-Logik bezüglich der Validierung von Daten identifiziert werden?
Resultat	Im Zuge des Audits wurden keine Probleme im Verhalten der Datenvalidierung identifiziert.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


### CLIENT-SEITIGE ÜBERPRÜFUNGEN (WSTG-CLIENT)

#### DOM-based Cross Site Scripting (XSS) (V-0117)

GUID	e0d70d61-bee1-4127-8c92-aab14fc75358
Frage	Können DOM-basierende Cross Site Scripting (XSS) Verwundbarkeiten identifiziert werden?
Resultat	Es wurden keine DOM-basierten Cross-Site Scripting (XSS) Schwachstellen identifiziert.
Betroffene	Externen Einbindungen

Systeme	
Bewertung	 Information

#### HTML Injection (V-0118)

GUID	ec80d4f7-20f6-45b2-b66a-75367316078d
Frage	Können HTML Injection Verwundbarkeiten identifiziert werden?
Resultat	Es wurden keine HTML-Injection-Schwachstellen identifiziert.
Betroffene Systeme	Externen Einbindungen
Bewertung	 Information


#### Cross Origin Ressource Sharing (V-0119)

GUID	d58da37d-271c-4076-ba42-0ce855254e7e
Frage	Wird CORS verwendet und falls ja, ist es sicher implementiert?
Resultat	<p>Die Applikation setzt den HTTP Header "Access-Control-Allow-Origin: *". Dadurch kann ein Angreifer den Browser eines Opfers missbrauchen, um die Applikation zu verwenden.</p> <p>Wenn eine zugriffsberechtigte Person auf eine bösartige Webseite surft, erhält die bösartige Webseite Zugriff auf alle nicht authentisierten Bereiche der Applikation und kann in diesem Bereich auch Schwachstellen ausnutzen.</p>
Massnahme	<p>Es sollten nur vertrauenswürdige Domains zugelassen werden, die wirklich in der CORS Policy benötigt werden.</p> <p>Zum Beispiel:</p>



	Access-Control-Allow-Origin: ai.test.online-ident.ch
Betroffene Systeme	sandbox-autoid.id-validation.ch
PoC	<div>Folgender Screenshot zeigt den gesetzten CORS Header:</div> <div><div><div>Request</div><div><div>PrettyRawHexHackvortor</div><div><pre>POST /api/v1/internal/2988441f-fa00-435f-a181-9938361994d4/id-cases/82bb8725-0ccd-49af-8fbf-49176b9e2246/resume HTTP/1.1 Host: sandbox-autoid.id-validation.ch Cookie: trace_id=520a77c26462346b; cookiesession1=6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0 Accept: application/json, text/plain, */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Referer: https://sandbox-autoid.id-validation.ch/scan/process/channel-selection?scheduled-case-id=82bb8725-0ccd-49af-8fbf-49176b9e2246&amp;language=en Idtoken: undefined Content-Type: application/json</pre></div></div></div><div><div>Response</div><div><div>PrettyRawHexRenderHackvortor</div><div><pre>1 HTTP/1.1 200 2 server: nginx 3 date: Thu, 12 Sep 2024 08:28:50 GMT 4 content-type: application/json 5 x-content-type-options: nosniff 6 x-xss-protection: 0 7 cache-control: no-cache, no-store, max-age=0, must-revalidate 8 pragma: no-cache 9 expires: 0 10 x-frame-options: DENY 11 x-content-type-options: nosniff 12 x-xss-protection: 1; mode=block 13 strict-transport-security: max-age=31536000; includeSubdomains; preload 14 access-control-allow-origin: * 15 set-cookie: trace_id=520a77c26462346b; cookiesession1=6; HttpOnly; SameSite=None</pre></div></div></div></div>
Bewertung	<div><div></div><div>Mittlere Schwachstelle</div></div>



WebSockets (V-0120)	
GUID	84029cc8-880c-4f8b-bac1-77d00fbfa77a
Frage	Gibt es Schwachstellen in der WebSockets Kommunikation?
Resultat	Es konnten keine Schwachstellen in der WebSockets Kommunikation identifiziert werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	<div><div></div><div>Information</div></div>
Lokaler Speicher (V-0121)	


GUID	2fad63d9-ee76-4da4-be8d-2a961033b7f5
Frage	Sind sensitive Informationen im lokalen Browser Storage gespeichert?
Resultat	Es wurden keine sensitiven Informationen identifiziert, die im lokalen Browserspeicher abgelegt werden.
Betroffene Systeme	Externen Einbindungen
Bewertung	<div>  <p>Information</p> </div>

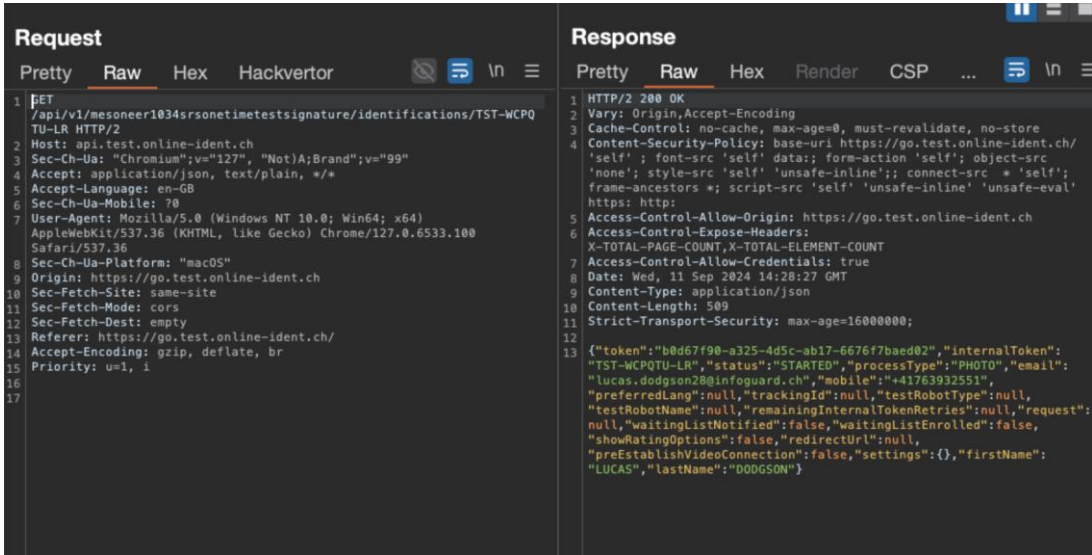
#### ZUSÄTZLICHE TESTS



#### TLS Konfiguration (V-0122)

GUID	f7d86b3c-8077-475a-833f-8375e9575f2a
Frage	Wird eine sichere TLS-Konfiguration verwendet?
Resultat	Der Dienst beinhaltet TLS Chiffren Sammlungen, welche nicht den AEAD (Authenticated Encryption with Associated Data) Modus verwenden. Dies entspricht nicht mehr den best-practice Empfehlungen.
Massnahme	Die TLS-Version sollte auf TLS v1.2 oder idealerweise TLS v1.3 umgestellt werden. Für TLS v1.2 sollten nur AEAD (Authenticated Encryption with Associated Data) Chiffren Sammlungen verwendet werden.
Betroffene Systeme	sandbox-autoid.id-validation.ch

PoC	<pre> ----- sandbox-autoid.id-validation.ch:443 The following weak cipher suites are supported: TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_CAMELLIA_256_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_256_GCM [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_256_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_256_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_128_GCM [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_RSA_WITH_AES_128_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_256_GCM [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_256_CBC_SHA [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_128_GCM [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 [TLSv1.2] (AEAD Mode not supported) TLS_DHE_RSA_WITH_AES_128_CBC_SHA [TLSv1.2] (AEAD Mode not supported) </pre>
Bewertung	 <p>Geringe Schwachstelle</p>
Überprüfung TLS Zertifikat (V-0123)	
GUID	0c943870-a068-411e-bbc7-cdf65cb3dbf9
Frage	Wird ein sicheres TLS Zertifikat verwendet?
Resultat	Die Überprüfung der TLS Zertifikate hat keine wesentlichen Fehlkonfigurationen identifiziert.
Betroffene Systeme	Externen Einbindungen
Bewertung	

	Information
<b>Einsatz einer Web Application Firewall (WAF) (V-0124)</b>	
GUID	98e2f8de-8649-4dec-9169-696048f18feb
Frage	Werden am Perimeter exponierte Webapplikationen zusätzlich durch eine "Web Application Firewall" (WAF) geschützt?
Resultat	<p>Es konnte eine "Web Application Firewall" (WAF) identifiziert werden.</p> <p>Eine WAF fungiert als zusätzliche Sicherheitsmassnahme und erschwert das erfolgreiche Ausnutzen allfällig vorhandener Schwachstellen.</p>
Betroffene Systeme	Externen Einbindungen
Bewertung	 <p>Information</p>
<b>Sensitive Informationen in URLs (V-0125)</b>	
GUID	4eb52008-824f-4a0c-84e1-60c60fb29f3e
Frage	Werden sensitive Informationen mit Hilfe von GET-Parameter übertragen?
Resultat	<p>Es wurden folgende Webadressen (URLs) identifiziert, welche Session-Informationen im GET-Parameter übertragen.</p> <ul style="list-style-type: none"> <li><a href="https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR">https://api.test.online-ident.ch/api/v1/mesoneer1034srsonetimetestssignature/identifications/TST-WCPQTU-LR</a></li> <li><a href="https://sandbox-autoid.id-validation.ch/api/v1/internal/scheduled-cases/ed72bd9e-72c8-42d4-9419-99d4dc55e1f5?idToken=undefined">https://sandbox-autoid.id-validation.ch/api/v1/internal/scheduled-cases/ed72bd9e-72c8-42d4-9419-99d4dc55e1f5?idToken=undefined</a></li> </ul> <p>Solche URLs stellen ein mögliches Sicherheitsrisiko dar, da sie an mehreren Stellen, wie z. B. Webproxy-, Webserver-Logs oder vom Browser selbst während deren Übertragung aufgezeichnet werden können. Ein Angreifer mit Zugriff auf eine dieser Stellen kann die preisgegebenen Informationen im Anschluss missbrauchen, um auf die IDs zuzugreifen. (TST-WCPQTU-LR und ed72bd9e-72c8-42d4-9419-99d4dc55e1f5). Diese erlauben den Zugriff auf Benutzerdaten</p>

	(Namen, E-Mail, Telefonnummer, Nationalität) zuzugreifen (siehe auch V-0083).
Massnahme	<p>Die Webapplikation sollte aktualisiert werden, um sicherzustellen, dass keinerlei sensitive Informationen in URLs, sondern ausschliesslich in den Nutzdaten der HTTP-Anfragen (z.B. mit Hilfe von POST-Parameter) übertragen werden.</p> <p>Generauere Empfehlungen, wie das für die Webapplikation umgesetzt werden, können der Schwachstelle mit ID V-0083 entnommen werden.</p>
Betroffene Systeme	<p>api.test.online-ident.ch</p> <p>sandbox-autoid.id-validation.ch</p>
PoC	<p>Folgender Screenshot zeigt ein Beispiel einer solcher Webanfrage, die ohne weitere Cookies oder Authentifizierung-Information auf die Daten eines Benutzers zugreifen kann.</p>  <p>Folgender Screenshot zeigt die Antwort des zweiten URLs:</p>

	<div><div>sandbox-autoid.id-validation.ch/api/ X +</div><div>← → ↻  https://sandbox-autoid.id-validation.ch/api/v1/internal/scheduled-cases/ed72bd9e-72c8-42d4-9419-99d4dc55e1f5?idToken=undefined ☆</div><div>This XML file does not appear to have any style information associated with it. The document tree is shown below.</div><div><pre>&lt;ScheduledCaseResponse&gt;   &lt;tenantId&gt;2988441f-fa00-435f-a181-9938361994d4&lt;/tenantId&gt;   &lt;tenantDisplayName&gt;2_1034b Zak INT&lt;/tenantDisplayName&gt;   &lt;tenantStatus&gt;ACTIVE&lt;/tenantStatus&gt;   &lt;caseStatus&gt;VERIFICATION_CONFIRMED&lt;/caseStatus&gt;   &lt;availableIdTypes&gt;     &lt;lastName&gt;asd&lt;/lastName&gt;     &lt;firstName&gt;xtesthappy&lt;/firstName&gt;     &lt;birthdate&gt;     &lt;mobileCountryCode&gt;41&lt;/mobileCountryCode&gt;     &lt;mobilePhoneNumber&gt;763932551&lt;/mobilePhoneNumber&gt;     &lt;issuerCountry&gt;     &lt;nationality&gt;AT&lt;/nationality&gt;     &lt;email&gt;lucas.dodgson@infoguard.ch&lt;/email&gt;   &lt;/availableIdTypes&gt;   &lt;qtspIntegration&gt;false&lt;/qtspIntegration&gt;   &lt;signingIntegration&gt;false&lt;/signingIntegration&gt;   &lt;signingQuality&gt;AES&lt;/signingQuality&gt;   &lt;legalStepDisplayed&gt;true&lt;/legalStepDisplayed&gt;   &lt;startSigningImmediately&gt;false&lt;/startSigningImmediately&gt;   &lt;personDataStepDisplayed&gt;false&lt;/personDataStepDisplayed&gt;   &lt;personDataCompletelyProvidedByApi&gt;false&lt;/personDataCompletelyProvidedByApi&gt;   &lt;mobileStepDisplayed&gt;false&lt;/mobileStepDisplayed&gt;   &lt;mobileProvidedByApi&gt;false&lt;/mobileProvidedByApi&gt;   &lt;identificationVerification&gt;true&lt;/identificationVerification&gt;   &lt;animationStepDisplayed&gt;false&lt;/animationStepDisplayed&gt;   &lt;introductionStepDisplayed&gt;false&lt;/introductionStepDisplayed&gt;   &lt;scanningIntroductionStepDisplayed&gt;false&lt;/scanningIntroductionStepDisplayed&gt;   &lt;emailStepDisplayed&gt;false&lt;/emailStepDisplayed&gt;   &lt;guidanceStepDisplayed&gt;false&lt;/guidanceStepDisplayed&gt;   &lt;emailProvidedByApi&gt;false&lt;/emailProvidedByApi&gt;   &lt;ubidProductType&gt;INTRUM_AUTO_3&lt;/ubidProductType&gt;   &lt;updatedPermissionCheck&gt;11ba77c4-530d-4316-a22a-3882e7f69868&lt;/updatedPermissionCheck&gt; &lt;/ScheduledCaseResponse&gt;</pre></div></div>
Bewertung	<div></div> <div>Geringe Schwachstelle</div>