هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار التطوير الآمن للتطبيقات

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لحماية تطوير البرمجيات والتطبيقات الخاصة ب<اسم الجهة> وذلك لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC ٢٠١٨ :١ –)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق المعيار

يطبق هذا المعيار على جميع أنشطة ومشاريع وممارسات تطوير البرمجيات والتطبيقات والأصول المعلوماتية والتقنية الخاصة بها في <اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	التطوير الآمن للتطبيقات
الهدف	توفير متطلبات الأمن السيبراني لضمان حماية أنشطة تطوير البرمجيات والتطبيقات وضوابط الأمن السيبراني لحماية البرمجيات التي يتم تطويرها.
المخاطر المحتملة	يمكن أن يؤدي تطوير التطبيقات غير الآمن إلى إيجاد ثغرات أمنية يمكن استغلالها لتهديد سرية بيانات <اسم الجهة> وسلامتها وتوافرها، والتأثير في سير عملها.
الإجراءات المطلوبة	
١-١	تطوير عملية دورة حياة تطوير البرمجيات الآمنة (SSDLC) وتطبيقها.
١-٢	تطوير منهجية وعملية "التطوير والأمن والعمليات" (DevSecOps) واتباعها.
١-٣	ضمان توفير متطلبات الأمن السيبراني في المراحل الأولية من تطوير البرمجيات ودمجها في دورة حياة تطوير البرمجيات الآمنة (SSDLC).
١-٤	ضمان اختبار الأمن السيبراني في مراحل اختبار تطوير البرمجيات ودمجه في دورة حياة تطوير البرمجيات الآمنة (SSDLC).
١-٥	تطوير آلية تلقائية في مراحل اختبار تطوير البرمجيات اتجاه البرمجيات والاختراقات الضارة المعروفة.

١-٦	يجب استخدام الطرق المختلفة للاختبارات الأمنية في مراحل تطوير البرمجيات مثل (طريقة التشويش، اختبار الصندوق الأسود) وغيرها.
١-٧	تصميم وإعداد بيئة آمنة لغايات التطوير والاختبار وضمان الجودة.
١-٨	تطبيق إرشادات تطوير التطبيقات الآمن وفقاً للجدول (أ).
١-٩	يجب استخدام لغة ذاكرة آمنة ويجب اختبار التطبيق ضد هجمات اختراقات الذاكرة.
١-١٠	تطبيق إجراءات التخفيف على أعلى ١٠ مخاطر تهدد أمن تطبيقات الويب وفقاً للمشروع المفتوح لأمن تطبيقات الويب (OWASP) فيما يخص الأنظمة والتطبيقات الحساسة.
١-١١	تطبيق آليات لتقييد صلاحيات التعديل على الشفرة المصدرية أو بيانات بيئات الإنتاج.
١-١٢	إلزام الموردين الخارجيين بالالتزام بسياسات ومعايير الأمن السيبراني المعتمدة في <اسم الجهة>.
١-١٣	استخدام المصادر الحديثة والموثوق بها والمرخصة فقط لأدوات تطوير البرمجيات والمكتبات والمكونات.
١-١٤	ضمان تطبيق ضوابط حماية تطبيقات الويب وفقاً لسياسة ومعيار حماية تطبيقات الويب المعتمدين في <اسم الجهة>.
١-١٥	استخدام خوارزميات تشفير موحدة ومراجعة بدقة وفقاً للمعايير والإجراءات ذات العلاقة.
١-١٦	التحقق من أن إصدارات كافة البرمجيات التي تم شراؤها من خارج <اسم الجهة> مدعومة من المطور ومحصنة بصورة ملائمة بناءً على التوصيات الأمنية للمطور.
١-١٧	تدريب جميع العاملين في تطوير البرمجيات على كتابة الشفرات المصدرية المناسبة للغة البرمجة وبيئة التطوير المستخدمة.
١-١٨	يجب التأكد من أن جميع العاملين داخل أو خارج <اسم الجهة> لمن له علاقة في دورة حياة تطوير البرمجيات على استعداد لتنفيذ مهامهم ومسؤولياتهم خلال دورة حياة تطوير التطبيق.
١-١٩	<اسم الجهة> يجب أن تطبق آليات الحماية والتحصين على أجهزة مطوري التطبيقات مثل (الأجهزة المحمولة لمصممي التطبيقات، مطوري التطبيقات، مختبري التطبيقات، الخ) لتنفيذ المهام التطويرية باستخدام المنهجية القائمة على المخاطر.
١-٢٠	يجب على <اسم الجهة> ضمان التغييرات الآمنة المصرح بها للشفرة لتقييد مصادر الوصول لبيئة التطوير وتفعيل خاصية تسجيل الأحداث والتغييرات.

٢	مستودع الشفرة المصدرية
الهدف	توفير ضوابط الأمن السيبراني لضمان حماية الشفرة المصدرية والمكتبات ومستودع الشفرة المصدرية.
المخاطر المحتملة	في حال عدم توفير حماية كافية ومناسبة للشفرة المصدرية والمكتبات، يمكن أن تتعرض الشفرة المصدرية في <اسم الجهة> للخطر أو يتم التلاعب بها أو الوصول غير المصرح به لها.
الإجراءات المطلوبة	
٢-١	استخدام مستودع شفرة مصدرية آمن يمتاز بتطبيق إجراءات التحقق من الهوية والإصدار والرقابة وتسجيل الدخول.
٢-٢	تطبيق إجراءات منع وصول أي شخص إلى الشفرة المصدرية ومستودع الشفرة المصدرية باستثناء مطوري التطبيقات والجهات المسؤولة عنها عند الحاجة.
٢-٣	استخدام خطة ترقيم موحدة لضوابط الإصدار بحيث تبين تاريخ تثبيت الإصدارات المحدثة من البرمجيات.
٢-٤	أرشفة الإصدارات القديمة من الشفرة المصدرية دورياً.
٢-٥	فصل الشفرة المصدرية للتطبيقات قيد التطوير عن الشفرة المصدرية للتطبيقات في بيئة الإنتاج.
٢-٦	أرشفة الشفرة المصدرية للتطبيقات التي انتهت صلاحيتها بحيث يمكن استرجاعها عند الحاجة.
٢-٧	الحصول على نسخة من الشفرة المصدرية لكافة التطبيقات التي طورتها أطراف خارجية لـ<اسم الجهة> وتخزينها في مستودع الشفرة المصدرية.
٢-٨	تطوير معايير تحصين وأمن الحاويات والنسخ الافتراضية للنظام (Docker) وإرشادات الممارسات الأمنية المثلى وتطبيقها.
٢-٩	تثبيت آليات إدارة الأسرار وذلك من أجل إدارة الأسرار والمفاتيح والشهادات ومنع تخزين الأسرار في الحاويات.
٢-١٠	استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة.
٢-١١	استخدام سجل حاويات خاص لضمان تنزيل نسخ الحاويات المعتمدة والآمنة فقط على النظام بحيث يمكن فحص كل نسخة بحثاً عن الثغرات المعروفة والشائعة.
٢-١٢	عدم إدارة الحاويات من خلال حسابات المستخدمين عالية الصلاحية والامتيازات.

اختر التصنيف

٣	مراجعة واختبار الشفرة المصدرية
الهدف	توفير ضمان بشأن تطبيق ضوابط الأمن السيبراني على تطوير التطبيقات الآمن وكشف نقاط الضعف والثغرات والمشكلات في البرمجيات.
المخاطر المحتملة	يمكن أن تتعرض <اسم الجهة> إلى مخاطر أمنية كبيرة في حال عدم اختبار الشفرة المصدرية وأنشطة تطوير الشفرات ومراجعتها بانتظام لغايات الكشف عن الثغرات الأمنية والإعدادات الخاطئة ونقاط الضعف، يمكن أن تتعرض <اسم الجهة> إلى مخاطر أمنية كبيرة.
الإجراءات المطلوبة	
١-٣	إجراء عملية مراجعة الشفرة المصدرية بانتظام لتطبيقات الويب المطورة داخلياً.
٢-٣	تطبيق أدوات التحليل الثابتة والديناميكية للتحقق من الالتزام بممارسات تطوير التطبيقات الآمن بالنسبة للبرمجيات المطورة داخلياً.
٣-٣	القيام بمراجعة أمنية الشفرة المصدرية بانتظام لكافة التطبيقات المطورة لـ<اسم الجهة> من قبل أطراف خارجية.
٤-٣	مراجعة واعتماد الضوابط الأمنية للتطبيقات المطورة داخلياً قبل تثبيتها في بيئة الإنتاج.
٥-٣	إعادة تقييم التطبيقات الحالية المطورة داخلياً وإعادة اعتمادها بعد إجراء تغيير رئيسي عليها أو بعد مرور فترة زمنية محددة.
٦-٣	إجراء تقييم المخاطر لكافة التطبيقات قيد التطوير أو التي يتم شراؤها لتحديد الضوابط المطلوبة لتقليل مخاطر التطبيقات إلى مستويات مقبولة قبل التثبيت في بيئة الإنتاج (يرجى الرجوع إلى سياسة إدارة المخاطر المعتمدة في <اسم الجهة>).
٧-٣	إجراء اختبار الالتزام بالأمن السيبراني للبرمجيات بناءً على سياسات الأمن السيبراني المعتمدة في <اسم الجهة> قبل التثبيت في بيئة الإنتاج.
٨-٣	استخدام معيار التحقق من حماية التطبيقات الصادر عن المشروع المفتوح لأمن تطبيقات الويب (OWASP) كدليل إرشادي لتحديد المتطلبات الأمنية وعمل حالات اختبار لمراجعة الأنظمة والتطبيقات الحساسة.
٩-٣	إجراء مراجعة لإعدادات البرمجيات بما في ذلك مراجعة الإعدادات والتحصين وحزم التحديثات قبل التثبيت في بيئة الإنتاج.
١٠-٣	إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق ومراجعة تطوير التطبيقات الآمن، قبل التثبيت في بيئة الإنتاج.

اختر التصنيف

الإصدار <١,٠>

٣-١١	إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق، بعد التثبيت في بيئة الإنتاج.
٣-١٢	معالجة كافة المشاكل الأمنية في التطبيقات المطورة التي يتم اكتشافها خلال مراجعة تطوير التطبيقات الآمن قبل التثبيت في بيئة الإنتاج.
٣-١٣	اختبار التطبيقات المطورة لضمان تطبيق ضوابط فصل المهام بالصورة الملائمة.
٣-١٤	إلغاء وحذف حسابات وبيانات الاختبار الموجودة في بيئة غير بيئة الإنتاج قبل نقل التطبيقات إلى بيئة الإنتاج.
٣-١٥	فصل بيئة الاختبار والتطوير منطقياً عن بيئة الإنتاج والبيئات الأخرى باستخدام محددات الشبكة عن طريق إعداد وتثبيت قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية.
٣-١٦	إجراء مراجعة النظير للشفرة المصدرية من قبل مطور لم يشارك في كتابة أي شفرة قبل التثبيت في بيئة الإنتاج في <اسم الجهة>.
٣-١٧	استخدام الشفرة المصدرية وأدوات تقييم أمن البرمجيات المعتمدة والمرخصة.
٣-١٨	إجراء الاختبارات الأمنية للتطبيقات المطورة في كافة مراحل اختبار دورة حياة تطوير البرمجيات (SDLC)، بما في ذلك الاختبارات غير الوظيفية، واختبار الوحدات (UT) واختبار تكامل الأنظمة (SIT)، واختبار قبول المستخدم (UAT).
٣-١٩	استحداث عملية لإدارة العيوب البرمجية في البرمجيات والثغرات والمشكلات الأمنية ووضع سجل خاص بها ومتابعتهما.
٣-٢٠	إدراج الاختبارات كجزء من عمليات التحسين المستمر والتطوير المستمر (CI/CD).

الجدول أ - إرشادات تطوير التطبيقات الآمن

A١	التحكم بالوصول (OWASP:A١:٢٠٢١ - إجراءات التحكم بالوصول غير الآمنة)
A١-١	التحقق من أن المستخدمين يمكنهم الوصول فقط إلى الوظائف أو الخدمات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.
A١-٢	التحقق من أن المستخدمين يمكنهم الوصول فقط إلى العناوين الآمنة (Secured URLs) التي يملكون تصاريح وصلاحيات خاصة لها.
A١-٣	التحقق من أن المستخدمين يمكنهم الوصول فقط إلى ملفات البيانات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.
A١-٤	التحقق من عدم تجاوز ضوابط الوصول.
A١-٥	التحقق من أن مرجعيات العناصر المباشرة محمية بحيث يمكن الوصول فقط إلى العناصر المصرح بها لكل مستخدم.
A١-٦	التحقق من إلغاء تفعيل تصفح الدليل (Directory Browsing) إلا إذا كان ذلك مطلوباً.
A١-٧	التحقق من أن المستخدم يمكنه الوصول فقط إلى المعلومات المحمية التي يملك تصاريح وصلاحيات خاصة لها (على سبيل المثال، من خلال تطبيق ضوابط لحماية مرجعيات الكائنات من التلاعب المباشر والوصول غير المصرح به إلى البيانات).
A١-٨	التحقق من إخفاق ضوابط الوصول بصورة آمنة.
A١-٩	التحقق من أن نفس قواعد التحكم بالوصول المتضمنة في طبقة العرض مطبقة على الخادم بحسب دور المستخدم، بحيث لا يمكن إعادة تفعيل الضوابط والمعايير أو إعادة إضافتها من مستخدمين يمتلكون مزايا وصلاحيات أعلى.
A١-١٠	التحقق من أن كافة خصائص المستخدمين والبيانات ومعلومات السياسة المستخدمة من قبل ضوابط الوصول لا يمكن التلاعب بها من قبل المستخدمين إلا إذا كان مصرحاً لهم بذلك تحديداً.
A١-١١	التحقق من أن كافة ضوابط الوصول فعالة من جهة الخادم.
A١-١٢	التحقق من أن قرارات التحكم بالوصول يمكن تسجيلها وأن كافة القرارات غير الناجحة قد تم تسجيلها.
A١-١٣	التحقق من أن التطبيق أو إطار العمل يصدر رموزاً تعريفية عشوائية معقدة مضادة لتزوير الطلب عبر المواقع (Cross-Site Request Forgery "CSRF")، وتكون هذه

اختر التصنيف

	الرموز خاصة بالمستخدم باعتبارها جزءاً من كافة المعاملات عالية القيمة أو الوصول إلى المعلومات المحمية، وأن التطبيق يتحقق من وجود هذه الرموز التعريفية بالقيمة الملائمة للمستخدم الحالي عند معالجة هذه الطلبات.
A١-١٤	الحماية التراكمية للتحكم بالوصول- التحقق من أن النظام يستطيع توفير الحماية من الوصول التراكمي أو المستمر للوظائف المحمية أو المصادر أو البيانات، وذلك من خلال استخدام ضابط مصادر (Resource Governor) على سبيل المثال، للحد من عدد حالات التسجيل لكل ساعة أو منع مستخدم فردي من سحب بيانات قاعدة البيانات بأكملها.
A١-١٥	التحقق من وجود آلية مركزية (بما في ذلك المكتبات التي تستدعي خدمات تصاريح وصلاحيات خارجية) للتحكم بالوصول إلى كل نوع من المصادر المحمية.
A١-١٦	التحقق من الفصل بين المنطق الذي يتمتع بمزايا وصلاحيات عن شفرات التطبيق الأخرى.
A١-١٧	تطبيق ضوابط الوصول الملائمة إلى المعلومات المحمية المخزنة على الخادم. وتشمل هذه المعلومات البيانات المخزنة والملفات المؤقتة والبيانات التي يمكن الوصول إليها فقط من قبل مستخدمين نظام محددين.
A١-١٨	التحقق من أن حسابات الخدمة أو الحسابات التي تدعم الاتصالات من الأنظمة الخارجية أو إليها تمتلك الحد الأدنى من الصلاحيات والامتيازات.
A١-١٩	التحقق من تطبيق تدقيق الحسابات وإلغاء تفعيل الحسابات غير المستخدمة (على سبيل المثال، بعد مرور أكثر من ٣٠ يوماً من تاريخ انتهاء صلاحية كلمة مرور الحساب، حساب غير مستخدم).
A١-٢٠	في حال السماح بالجلسات الطويلة المصادق عليها، يجب إعادة التحقق دورياً من تصاريح وصلاحيات المستخدم لضمان عدم تغير مزاياه، وفي حال تغيرها، يجب تسجيل خروج المستخدم وإجباره على إجراء عملية إعادة التحقق من الهوية (مثل الرسائل النصية، أو رموز تعريفية، أو غيرها) .
A١-٢١	التحقق من أن التطبيق يدعم إلغاء تفعيل الحسابات وإنهاء الجلسات عند توقف التصاريح والصلاحيات (على سبيل المثال، عند حدوث تغيير في الدور، أو في حالة التوظيف، أو إجراءات الأعمال، أو غيرها). , employment status, business process, etc.).
A٢	التشفير (OWASP:A٢:٢٠٢١ – فشل التشفير)
A٢-١	التحقق من أن كافة دالات التشفير المستخدمة لحماية الأسرار من مستخدم التطبيق مطبقة على الخادم.
A٢-٢	التحقق من أن كافة وحدات التشفير تفشل بصورة آمنة.

A٢-٣	التحقق من حماية أي أسرار رئيسية من الوصول غير المصرح به (السر الرئيسي هو بيانات اعتماد التطبيق المخزنة كنص غير مشفر على القرص والتي تستخدم لحماية الوصول إلى معلومات الإعدادات الأمنية).
A٢-٤	التحقق من أن كافة الأرقام العشوائية، وأسماء الملفات العشوائية، والمعرفات الموحدة (GUIDs)، وسلاسل الحروف العشوائية (Strings) صادرة من مولد الأرقام العشوائية المعتمد لنموذج التشفير، وذلك عندما يكون الهدف من هذه القيم العشوائية هو جعل الجهة المهاجمة غير قادرة على تخمينها.
A٢-٥	التحقق من أن نماذج التشفير المستخدمة في التطبيق قد تم التحقق منها وفقاً للسياسات والإجراءات ذات العلاقة.
A٢-٦	التحقق من أن نماذج التشفير تعمل بنظامها المعتمد وفقاً للسياسات والإجراءات ذات العلاقة.
A٢-٧	التحقق من وجود سياسة صريحة حول كيفية إدارة مفاتيح التشفير (مثل كيفية إصدارها وتوزيعها وإلغائها وانتهاء صلاحيتها) والتحقق من تطبيق هذه السياسة بصورة ملائمة.
A٢-٨	التحقق من وجود عدم الإنكار(Non-Repudiation) من خلال التشفير (التوقيع الرقمي) للمعاملات الحساسة مثل (المعاملات المالية والتجارة الإلكترونية والسجلات، وغيرها).
A٢-٩	التحقق من حماية كافة مفاتيح التشفير بصورة ملائمة. في حال تعرض المفتاح لانتهاك أمني، فإنه لا يمكن الوثوق به ويجب استبداله أو إلغاؤه.
A٢-١٠	التحقق من تشفير المعلومات القابلة لتحديد الهوية (PII) والمعلومات المحمية والبيانات المخزنة عندما لا تكون قيد الاستخدام.
A٢-١١	التحقق من إلغاء تفعيل تخزين النماذج التي تتضمن معلومات محمية لدى العميل، بما في ذلك خصائص الإكمال التلقائي.
A٢-١٢	التحقق من إرسال كافة المعلومات المحمية إلى الخادم في متن رسالة بروتوكول نقل النص التشعبي (HTTP)، (أي منع استخدام معايير شريط العنوان "URL" لإرسال البيانات المحمية).
A٢-١٣	التحقق من أن كافة النسخ المخزنة أو المؤقتة للمعلومات المحمية المخزنة على الخادم محمية من الوصول غير المصرح به، والتأكد من حذف الملفات العاملة المؤقتة بمجرد انقضاء الحاجة لها.
A٢-١٤	إلغاء تفعيل التخزين أو حفظ النسخ المؤقتة للصفحات التي تتضمن معلومات محمية لدى العميل، والتحقق من أن هذه النسخ محمية من الوصول غير المصرح به أو مسحها أو إلغاء صلاحيتها بعد وصول المستخدم المصرح له إليها. (يمكن استخدام "Cache-Control: no-store" مع ضابط عنوان بروتوكول نقل

	النص التشعبي "HTTP". "Pragma: no-cache"، وهو أقل فاعلية، ولكنه متوافق مع النسخ الأقدم "١,٠" من بروتوكول نقل النص التشعبي "HTTP").
A٢-١٥	التحقق من تحديد قائمة بالمعلومات المحمية التي يعالجها التطبيق، والتأكد من وجود سياسة صريحة حول كيفية التحكم بالوصول إلى هذه المعلومات، ومتى يجب تشفيرها (أثناء عدم الاستخدام وأثناء النقل والاستخدام)، والتحقق من تطبيق هذه السياسة بصورة ملائمة.
A٢-١٦	التحقق من وجود طريقة لحذف كل أنواع المعلومات المحمية الموجودة في التطبيق عند نهاية فترة الاحتفاظ المطلوبة.
A٢-١٧	التحقق من أن التطبيق يقلل عدد المعايير المرسلة إلى الأنظمة غير الموثوقة مثل الحقول المخفية ومتغيرات "Ajax" وملفات الارتباط وقيم العناوين.
A٢-١٨	التحقق من قدرة التطبيق على كشف الأرقام غير الطبيعية لطلبات المعلومات والتنبيه بشأنها، أو معالجة المعاملات عالية القيمة لدور المستخدم مثل سحب الشاشة، أو الاستخدام التلقائي لاستخلاص خدمات الويب، أو منع فقدان البيانات. على سبيل المثال، يجب ألا يكون المستخدم العادي قادراً على الوصول إلى أكثر من ٥ سجلات في الساعة أو أكثر من ٣٠ سجلاً في اليوم.
A٢-١٩	التحقق من أن بيانات الاعتماد التي يستخدمها التطبيق على الخادم، مثل اتصال قاعدة البيانات، وكلمة المرور، والمفاتيح السرية للتشفير، ليست مثبتة في الشفرة. ويجب تخزين أي بيانات اعتماد في ملف إعدادات منفصل على نظام موثوق وتشفيرها.
A٢-٢٠	التحقق من أن خصائص الإكمال التلقائي غير مفعلة على النماذج باستثناء النماذج التي تتضمن معلومات محمية، بما في ذلك التحقق من الهوية.
A٣	**اعتماد المدخلات (OWASP:A٣:٢٠٢١ - الحقن والإدخال)**
A٣-١	التحقق من أن بيئة التشغيل غير معرضة لتجاوز سعة المخزن المؤقت، وأن ضوابط الأمن تمنع تجاوز سعة المخزن المؤقت.
A٣-٢	التحقق من أن بيئة التشغيل غير معرضة لحقن تعليمات الاستعلام البنيوية (SQL Injection)، وأن ضوابط الأمن تمنع حقن تعليمات الاستعلام البنيوية (SQL Injection).
A٣-٣	استخدام ضوابط لتقييد تعليمات الاستعلام البنيوية (SQL) مثل (LIMIT) للحماية والتقليل من خطر وضرر الافصاح الكبير للمعلومات والسجلات.
A٣-٤	التحقق من أن بيئة التشغيل غير معرضة لحقن النصوص البرمجية عبر المواقع (XSS)، وأن ضوابط الأمن تمنع حقن النصوص البرمجية عبر المواقع (XSS).

A٣-٥	التحقق من أن بيئة التشغيل غير معرضة لحقن بروتوكول النفاذ إلى الدليل البسيط LDAP (Injection) وأن ضوابط الأمن تمنع حقن بروتوكول النفاذ إلى الدليل البسيط (LDAP Injection).
A٣-٦	التحقق من أن بيئة التشغيل غير معرضة لحقن أوامر نظام التشغيل (OS (Command Injection، وأن ضوابط الأمن تمنع حقن أوامر نظام التشغيل (OS (Command Injection.
A٣-٧	التحقق من نوع البيانات ونطاقها وطولها (إذا أمكن).
A٣-٨	عند الحاجة إلى السماح برموز خطرة محتملة كمدخلات، يجب التأكد من تطبيق ضوابط إضافية مثل ترميز المدخلات، وحماية واجهات برمجة التطبيقات الخاصة بالمهام، ومعرفة الجهات التي تستخدم تلك البيانات طوال فترة استخدام التطبيق. وتشمل الأمثلة على الرموز الخطرة الشائعة الآتي: (< > " ' % ( ) & + \ \'\ \").
A٣-٩	التأكد من أن جميع عمليات التحقق من صحة المدخلات تتم بواسطة روتين مركزي للتحقق من صحة المدخلات للتطبيق.
A٣-١٠	التحقق من أن كافة عمليات التحقق الفاشلة تؤدي إلى رفض المدخلات أو تدقيقها.
A٣-١١	التحقق من تنفيذ كافة إجراءات التحقق أو إجراءات تطوير التطبيقات وإنفاذها على الخادم.
A٣-١٢	التحقق من إزالة من كافة البيانات غير الموثوقة والتي تعتبر مخرجات بالنسبة للغة "HTML" (بما في ذلك عناصر لغة "HTML" وخصائصها، وقيم بيانات لغة "JavaScript"، وكتل الصفحات النمطية المتسلسلة "CSS Blocks"، وخصائص شريط العنوان "URL") بصورة ملائمة لمحتوي التطبيق.
A٣-١٣	التحقق من أن مجموعات الرموز، مثل "UTF-٨"، محددة لكافة مصادر المدخلات.
A٣-١٤	التحقق من أن كافة البيانات المدخلة موحدة لكافة برمجيات فك تشفير أو برمجيات تفسير البيانات المرسلة إلى العميل قبل مصادقتها.
A٣-١٥	إذا كان إطار عمل التطبيق يسمح بالتخصيص التلقائي الضخم للمعايير (ويسمى أيضاً ربط المتغيرات التلقائي) من طلب وارد إلى نموذج، فيجب التحقق من أن الحقول الحساسة أمنياً مثل "رصيد الحساب" أو "الدور" أو "كلمة المرور" محمية من الربط التلقائي الخبيث.
A٣-١٦	التحقق من أن التطبيق محمي من هجمات تلوث متغيرات بروتوكول نقل النص التشعبي (HTTP)، خصوصاً إذا كان إطار عمل التطبيق لا يميز بين مصادر متغيرات الطلب (مثل طلب "GET"، وطلب "POST"، وملفات الارتباط، والعناوين، والبيئة، وغيرها).
A٣-١٧	التحقق من أن التطبيق يستخدم ضوابط تحقق من المدخلات لكل نوع من البيانات التي يتم قبولها.

A٣-١٨	التحقق من تسجيل كافة حالات الإخفاق في التحقق من المدخلات.
A٣-١٩	التحقق من أن كل نوع من عمليات ترميز المخرجات أو إزالة منها التي يقوم بها التطبيق له ضابط أمني واحد للوجهة المقصودة.
A٤	**التصميم الغير آمن (OWASP:A٤:٢٠٢١- التصميم الغير آمن)**
A٤-١	التحقق من عمليات التطبيق ومن كافة تدفقات قواعد العمل عالية القيمة في بيئة موثوقة مثل الخادم المحمي والمراقب.
A٤-٢	التحقق من أن التطبيق لا يسمح بمعاملات عالية القيمة منتحلة، مثل السماح للمستخدم المهاجم (أ) بمعالجة معاملة باعتباره المستخدم الضحية (ب) من خلال التلاعب أو إعادة إعداد الجلسة أو حالة المعاملة أو هوية المستخدم أو المعاملة.
A٤-٣	التحقق من أن التطبيق لا يسمح بالتلاعب بمعايير قواعد العمل عالية القيمة والتي تشمل، على سبيل المثال لا الحصر، السعر، والفائدة، والخصومات، والمعلومات القابلة لتحديد الهوية (PII)، والأرصدة، وهويات الأسهم، وغيرها.
A٤-٤	التحقق من وجود إجراءات دفاعية في التطبيق للحماية من هجمات الإنكار، حيث تشمل هذه الإجراءات سجلات المعاملات المحمية والقابلة للتحقق، وسجلات التدقيق أو سجلات النظام، وفي الأنظمة ذات القيمة الأعلى، المراقبة المباشرة لأنشطة المستخدم والمعاملات بحثاً عن أي أنشطة غير طبيعية.
A٤-٥	التحقق من أن التطبيق يوفر الحماية من هجمات الإفصاح عن المعلومات مثل مرجعيات العناصر المباشرة، والتلاعب، واستخدام الهجمات التخمينية لاختراق الجلسة، وأنواع الهجمات الأخرى.
A٤-٦	التحقق من وجود ضوابط كشف وضبط كافية في التطبيق للحماية من الهجمات التخمينية (مثل الاستخدام المستمر لدالة معينة) أو هجمات حجب الخدمة.
A٤-٧	التحقق من وجود ضوابط وصول كافية في التطبيق لمنع هجمات رفع مستوى المزايا والصلاحيات، وتشمل هذه الضوابط منع المستخدمين المجهولين من الوصول إلى البيانات المحمية أو الدالات المحمية، أو منع المستخدمين من الوصول إلى معلومات المستخدمين الآخرين، أو استخدام وظائف ذات مزايا وصلاحيات هامة وحساسة.
A٤-٨	التحقق من أن التطبيق يعالج دفعات قواعد العمل في خطوات متتالية فقط، بحيث تتم معالجة كافة الخطوات مباشرة، وتجنب المعالجة بطريقة غير منتظمة أو التجاوز عن أي خطوات، أو معالجة خطوات مستخدم آخر أو المعاملات المقدمة بسرعة.

A٤-٩	التحقق من أن التطبيق يتضمن تصاريح وصلاحيات إضافية (مثل تحقق الإعداد أو التحقق من الهوية المتغير) لأنظمة القيم المتدنية و/أو فصل المهام للتطبيقات ذات القيم المرتفعة لفرض ضوابط مكافحة الاحتيال وفقاً لمخاطر التطبيق وعمليات الاحتيال السابقة.
A٤-١٠	التحقق من أن للتطبيق حدود عمل يطبقها في موقع موثوق (كتطبيقها على خادم محمي) على كل مستخدم أو بشكل يومي، والتي تتضمن تنبيهات قابلة للإعداد واستجابات تلقائية للهجمات التلقائية أو غير الاعتيادية.
A٤-١١	يجب تطبيق واستخدام آلية أمنية في تطوير دورة حياة التطبيقات بواسطة مطوري التطبيقات المحترفين بالوظائف والخصائص الأمنية.
A٤-١٢	يجب تطوير واستخدام المكتبات لأنماط التصميم الآمن.
A٤-١٣	يجب استخدام نمذجة التهديد في المصادقات الهامة، التحكم في الوصول، منطق الأعمال، وتدفقات المفاتيح.
A٤-١٤	يجب دمج لغة الأمان وعناصر التحكم في حالات المستخدم أو العميل.
A٤-١٥	يجب دمج الفحص لكل طبقة في التطبيق من الواجهة الأمامية للتطبيق الى الواجهة الخلفية للتطبيق.
A٤-١٦	يجب كتابة اختبارات الوحدة والتحقق من أن جميع التدفقات الحرجة مقاومة لنموذج التهديد. كما يجب تجميع الحالات وحالات سوء الاستخدام لكل طبقة في التطبيق.
A٤-١٧	يجب أن تكون طبقات التطبيق منفصلة في الأنظمة وشبكات الإنترنت بناءً على احتياجات التعرض والحماية.
A٤-١٨	يجب أن يكون التصميم للتطبيق بناءً على فصل المشتركين أو العملاء على مدار كل الطبقات.
A٤-١٩	يجب تقييد استهلاك المصدر من قبل المستخدم أو الخدمة.
A٥	**أمن الاتصالات (OWASP:A٥:٢٠٢١ - الإعدادات الأمنية الخاطئة)**
A٥-١	التحقق من أنه يمكن بناء مسار من جهة إصدار شهادات موثوقة لكل شهادة تشفير خادم أمن طبقة النقل (TLS)، وأنه قد تم التحقق من صلاحية شهادة كل خادم.
A٥-٢	التحقق من استخدام أحدث إصدار من أمن طبقة النقل (TLS) في كافة الاتصالات (بما في ذلك الاتصالات الخارجية واتصالات أجهزة النقطة النهائية) التي تم مصادقتها أو التي تتضمن معلومات أو وظائف محمية.
A٥-٣	التحقق من تسجيل حالات إخفاق اتصالات أمن طبقة النقل (TLS) بأجهزة النقطة النهائية.

اختر التصنيف

الإصدار <١,٠>

A٥-٤	التحقق من المصادقة على كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية.
A٥-٥	التحقق من أن كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية تستخدم حساباً تم إعداده ومنحه الحد الأدنى من المزايا والصلاحيات اللازمة ليعمل التطبيق بالشكل الصحيح.
A٥-٦	التحقق من أن اتصالات أمن طبقة النقل (TLS) الفاشلة لا ينتج عنها اتصال غير آمن (غير مشفر).
A٥-٧	التحقق من أن مسارات شهادات التشفير قد تم بناؤها والتحقق منها لكافة شهادات التشفير الخاصة بالعميل باستخدام جهات الصلاحيات الموثوقة ومعلومات الإلغاء.
A٥-٨	التحقق من وجود تنفيذ أمن طبقة النقل (TLS) موحد يتم استخدامه في التطبيق وتم إعداده ليعمل في نظام عمل معتمد.
A٥-٩	التحقق من أن ترميز الرموز المحددة معرف لكافة الاتصالات (مثل "UTF-٨").
A٥-١٠	التحقق ومراجعة الإعدادات دورياً بما يتوافق مع أحدث الإعدادات الأمنية.
A٥-١١	التحقق من أن التطبيق يقبل مجموعة محددة فقط من طرق طلب بروتوكول نقل النص التشعبي (HTTP) مثل طلب "GET" وطلب "POST" وأن الطرق غير المستخدمة محظورة.
A٥-١٢	التحقق من أن كل استجابة لبروتوكول نقل النص التشعبي (HTTP) تتضمن عنوان نوع محتوى يحدد مجموعة رموز آمنة (مثل "UTF-٨").
A٥-١٣	التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) و/أو الآليات الأخرى للمتصفحات الأقدم تم تضمينها من أجل الحماية من هجمات الخطف بالنقر (Click Jacking).
A٥-١٤	التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) في الطلبات والاستجابات تتضمن فقط رموز المدونة الموحدة الأمريكية لتبادل المعلومات القابلة للطباعة.(ASCII)
A٥-١٥	التحقق من استخدام صيغ بيانات أقل تعقيداً مثل جافا سكريبت (JSON)، وتجنب جعل المعلومات المحمية متسلسلة.
A٥-١٦	تحديث وإصلاح أو ترقية معالجات لغة الترميز القابلة للامتداد (XML) والمكتبات قيد الاستخدام في التطبيق أو نظام التشغيل الأساسي، واستخدام عمليات التحقق من الاعتماديات، وتحديث البروتوكول البسيط للوصول إلى الكائنات (SOAP) إلى إصدار ١,٢ أو إصدار أحدث.

اختر التصنيف

الإصدار <١,٠>

A٥-١٧	إلغاء تفعيل لغة الترميز القابلة للامتداد لجهات خارجية ومعالجة "DTD" في كافة محللات لغة الترميز القابلة للامتداد (XML) في التطبيق وفقاً لتوجيهات المشروع المفتوح لأمن تطبيقات الويب "XXE Prevention".
A٥-١٨	تطبيق التحقق الإيجابي من المدخلات على الخادم (السماح بقائمة محددة) أو التصفية أو التدقيق لمنع البيانات العدائية ضمن وثائق أو عناوين أو عُقد لغة الترميز القابلة للامتداد (XML).
A٥-١٩	التحقق من أن وظيفة رفع الملف بلغة الترميز القابلة للامتداد (XML) أو بلغة الأسلوب الموسع (XSL) تتحقق من لغة الترميز القابلة للامتداد (XML) باستخدام تحقق لغة كتابة الملفات المرافقة للغة (XSD) أو طريقة تحقق مشابهة.
A٥-٢٠	استخدام أدوات اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST) للمساعدة في كشف لغة الترميز القابلة للامتداد لجهات خارجية (XXE) في الشفرة المصدرية، مع الأخذ بعين الاعتبار أن مراجعة الشفرة يدوياً هي الطريقة التي يفضل اتباعها في التطبيقات الكبيرة والمعقدة ذات العديد من التداخلات.
A٥-٢١	إذا كان من غير الممكن تطبيق هذه الضوابط، يجب دراسة استخدام حزم التحديثات الافتراضية، أو البوابات الأمنية لواجهات برمجة التطبيقات، أو جدار الحماية لتطبيقات الويب لكشف هجمات لغة الترميز القابلة للامتداد لجهات خارجية (XXE) ومراقبتها وحجبها.
A٥-٢٢	التحقق من استخدام الاستفسارات المضبوطة بمعايير لمنع حقن تعليمات الاستعلام البنيوية (SQL Injection).
A٥-٢٣	التحقق من استخدام بيانات اعتماد معقدة وآمنة للوصول إلى قواعد البيانات.
A٥-٢٤	التحقق من أن التطبيق الذي يصل إلى قواعد البيانات يمتلك أدنى مستوى ممكن من الامتيازات والصلاحيات المطلوبة.
A٥-٢٥	التحقق من أن سلاسل الحروف العشوائية (Strings) للاتصال ليست مثبتة في الشفرة ضمن التطبيق، خصوصاً بيانات اعتماد التحقق من الهوية من قاعدة البيانات.
A٥-٢٦	التحقق من إغلاق الاتصال بقاعدة البيانات بأسرع ما يمكن.
A٥-٢٧	التحقق من حذف كافة وظائف قاعدة البيانات غير اللازمة أو غير المستخدمة أو إلغاء تفعيلها، بما في ذلك محتوى المورد التلقائي، وتثبيت الحد الأدنى من الخصائص والخيارات اللازمة لعمل التطبيق. على سبيل المثال، إلغاء تفعيل الإجراءات أو الخدمات المخزنة وحزم الخصائص المفيدة غير اللازمة.

A٥-٢٨	التحقق من إلغاء تفعيل أي حسابات تلقائية أو غير ضرورية والتي يمكن من خلالها الوصول إلى قواعد البيانات غير اللازمة لدعم متطلبات الأعمال.
A٥-٢٩	التحقق من أن التطبيق يستخدم بيانات اعتماد مختلفة لكل ميزة وصلاحية (مثل مستخدم، ومستخدم للقراءة فقط، وضيف، ومشرفين) عند اتصاله بقاعدة البيانات.
A٥-٣٠	التحقق من إلغاء تفعيل تسجيل الدخول عن بعد والجلسات المجهولة إذا لم يكن هناك حاجة إليها.
A٥-٣١	بالنسبة للتطبيقات التي تعتمد على قاعدة بيانات، يجب استخدام قوالب الإعداد والتحصين الموحدة، واختبار جميع الأنظمة التي تعتبر جزءاً من إجراءات العمل الحساسة.
A٦	**الشفرة الخبيثة والثغرات (OWASP:A٦:٢٠٢١ - المكونات القديمة والتي تحتوي على ثغرات)**
A٦-١	التحقق من عدم وجود شفرات خبيثة في أي شفرة تم تطويرها أو تعديلها بهدف إنشاء التطبيق.
A٦-٢	التأكد من أن سلامة الشفرة المفسرة والمكتبات والأوامر التنفيذية وملفات الإعدادات قد تم التحقق منها باستخدام المجموعات الاختبارية أو عمليات حساب ملخص النص المميز.
A٦-٣	التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من الهوية أو تستخدمها لم تتأثر بأي شفرات خبيثة.
A٦-٤	التحقق من أن كافة الشفرات التي تطبق إدارة الجلسات أو تستخدمها لم تتأثر بأي شفرات خبيثة.
A٦-٥	التحقق من أن كافة الشفرات التي تطبق ضوابط الوصول أو تستخدمها لم تتأثر بأي شفرات خبيثة.
A٦-٦	التحقق من أن كافة ضوابط التحقق من المدخلات لم تتأثر بأي شفرات خبيثة.
A٦-٧	التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من المخرجات أو تستخدمها لم تتأثر بأي شفرات خبيثة.
A٦-٨	التحقق من أن كافة الشفرات التي تطبق نموذج التشفير أو تستخدمه لم تتأثر بأي شفرات خبيثة.
A٦-٩	التحقق من أن كافة الشفرات التي تطبق ضوابط التعامل مع الأخطاء وتسجيلها أو تستخدمها لم تتأثر بأي شفرات خبيثة.
A٦-١٠	التحقق من أن كافة الأنشطة الخبيثة قد خضعت لتقنية الحماية المعزولة (Sandboxing).

اختر التصنيف

الإصدار <١,٠>

A٦-١١	تحديث المكونات بأحدث التحديثات والإصلاحات عند معرفة المستخدم بالثغرات المنشورة.
A٦-١٢	إلغاء الاعتماديات غير المستخدمة والخصائص غير اللازمة والمكونات والملفات والوثائق.
A٦-١٣	عمل قائمة جرد مستمرة لإصدارات المكونات من طرف العميل والخادم (مثل أطر العمل والمكتبات) واعتمادياتها باستخدام أدوات مثل الإصدارات، و" Dependency Check"، و"retire.js"، وغيرها، والمراقبة المستمرة للمصادر مثل تعداد الثغرات الشائعة (CVE) وقاعدة بيانات الثغرات الوطنية (NVD) بحثاً عن الثغرات في المكونات، إلى جانب استخدام أدوات تحليل تكوين البرمجيات من أجل أتمتة العملية، والاشتراك في تنبيهات البريد الإلكتروني من أجل الثغرات الأمنية ذات العلاقة بالمكونات قيد الاستخدام.
A٦-١٤	الحصول على المكونات من مصادر رسمية وعبر روابط محمية فقط، وتفضيل الحزم الموقعة لتقليل فرص وجود مكون خبيث معدل.
A٦-١٥	مراقبة المكتبات والمكونات التي لا تتوافر لها صيانة أو ليس للإصدارات القديمة منها تحديثات وإصلاحات أمنية. إذا كان تثبيت حزم التحديثات غير ممكناً، يجب دراسة تثبيت التحديثات والإصلاحات الافتراضية لمراقبة المشكلات المكتشفة أو كشفها أو الحماية منها.
A٦-١٦	التحقق من أن إعادة التوجيه والإرسال في شريط العنوان (URL) لا تتضمن بيانات غير مصرحة.
A٦-١٧	التحقق من توحيد أسماء الملفات وبيانات المسارات التي يتم الحصول عليها من مصادر غير موثوقة لإلغاء هجمات تجاوز المسار.
A٦-١٨	التحقق من فحص الملفات التي يتم الحصول عليها من مصادر غير موثوقة من خلال برامج مكافحة الفيروسات لمنع تحميل برمجيات خبيثة معروفة.
A٦-١٩	التحقق من عدم استخدام المعايير التي تم الحصول عليها من مصادر غير موثوقة للتلاعب في أسماء الملفات أو أسماء المسارات أو ملفات وكائنات النظام دون توحيدها أولاً والتحقق من مدخلاتها لمنع هجمات إدراج الملفات المحلية.
A٦-٢٠	التحقق من توحيد المعايير التي تم الحصول عليها من مصادر غير موثوقة والتحقق من مدخلاتها وترميز مخرجاتها لمنع هجمات إدراج الملفات عن بعد، خصوصاً عندما يكون من الممكن تنفيذ المدخلات مثل العناوين أو المصادر أو إدراج القوالب.
A٦-٢١	التحقق من عدم السماح بإدراج محتوى عشوائي عن بعد عند مشاركة موارد "IFRAMEs" و"HTML ٥" عبر النطاقات.
A٦-٢٢	التحقق من تخزين الملفات التي تم الحصول عليها من مصادر غير موثوقة خارج "Webroot".

اختر التصنيف

الإصدار <١,٠>

A٦-٢٣	التحقق من إعداد وضبط خادم الويب أو التطبيق تلقائياً لحجب الوصول إلى المصادر البعيدة أو الأنظمة خارج خادم الويب أو التطبيق.
A٦-٢٤	التحقق من أن شفرة التطبيق لا تنفذ بيانات مرفوعة تم الحصول عليها من مصادر غير موثوقة.
A٦-٢٥	التحقق من ضبط إعدادات مشاركة مصادر تطبيقات "Flash" أو "Silverlight" أو غيرها من تطبيقات الإنترنت الغنية (RIA) عبر النطاقات بحيث تمنع الوصول غير المصرح به أو الوصول عن بعد غير المعتمد.
A٦-٢٦	التحقق من أن كافة أنواع الملفات المسموح برفعها مقتصرة على غايات العمل وحسب الحاجة (مثل ملفات "PDF" ومستندات برامج "Office").
A٦-٢٧	التأكد من أن التحقق من نوع الملف يتم من خلال التحقق من عناوين الملفات وليس من خلال اسم امتداد الملفات فقط.
A٦-٢٨	التحقق من عدم تفعيل امتيازات وصلاحيات التنفيذ في أدلة تحميل الملفات.
A٦-٢٩	التحقق من ضبط إعدادات ملفات ومصادر التطبيق تلقائياً على وضعية القراءة فقط.
A٦-٣٠	التحقق من إلغاء كافة أنواع المشاركات والمشاركات الإدارية غير اللازمة، وتقييد الوصول إلى المشاركات أو جعله يتطلب التحقق من الهوية.
A٦-٣١	طلب التحقق من الهوية قبل السماح برفع الملفات.
A٦-٣٢	وضع حد على حجم الملفات التي يمكن رفعها والذي يجب ألا يتجاوز الحجم المطلوب لغايات العمل (على سبيل المثال، ١ ميغابايت كحد أعلى)، وإضافة ملاحظة على صفحة الويب تخص أحجام الملفات المقبولة.
A٧	**عمليات التحقق من الهوية (OWASP:A٧:٢٠٢١ - إجراءات فشل التحقق من الهوية)**
A٧-١	التحقق من أن كافة الصفحات والمصادر تقتضي التحقق من الهوية باستثناء المحددة خصوصاً لتكون عامة (مبدأ التحقق التام والمتكامل).
A٧-٢	التحقق من أن حقول كلمات المرور لا تُظهر كلمات مرور المستخدمين عند إدخالها وأن خاصية الإكمال التلقائي في حقول كلمات المرور (أو الأشكال التي تتضمنها) غير مفعلة.
A٧-٣	التحقق من أن كافة ضوابط التحقق من الهوية تخفق بصورة آمنة لضمان عدم قدرة الجهات المهاجمة على تسجيل الدخول.
A٧-٤	التحقق من أن بيانات الاعتماد وكافة معلومات الهوية الأخرى التي يتعامل معها التطبيق لا تمر عبر روابط غير مشفرة أو مشفرة بصورة غير آمنة.

اختر التصنيف

الإصدار <١,٠>

A٧-٥	التحقق من أن مسار "نسيت كلمة المرور" ومسارات الاستعادة الأخرى لا ترسل كلمات المرور الحالية أو الجديدة من غير تشفير إلى المستخدم.
A٧-٦	التحقق من أن تنفيذ هجمات تعداد اسم المستخدم (User Enumeration) غير ممكن عن طريق وظائف "تسجيل الدخول" أو "إعادة ضبط كلمة المرور" أو "نسيت الحساب".
A٧-٧	التحقق من عدم وجود كلمات مرور افتراضية قيد الاستخدام لإطار عمل التطبيق أو أي مكونات مستخدمة من قبل التطبيق (مثل "admin/password").
A٧-٨	التحقق من وجود ضابط مصادر (Resource Governor) لتوفير الحماية من الهجوم التخميني العمودي (Vertical Brute Forcing) (وهو هجوم يحاول اختراق حساب واحد باستخدام كافة كلمات المرور المحتملة) والهجوم التخميني الأفقي Horizontal (Brute Forcing) (وهو هجوم يحاول اختراق جميع الحسابات باستخدام كلمة مرور واحدة مثل "Password١"). ويجب ألا يكون هناك تأخير في إدخال بيانات الاعتماد الصحيحة. فعلى سبيل المثال، يجب ضبط إعدادات عنوان بروتوكول الإنترنت لمصدر الهجوم التخميني بحيث يتم إغلاقه بعد ٦٠ دقيقة، ويتم إغلاق الحساب بعد ١٥ دقيقة. ويجب أن تكون آليتا الضبط فاعلتين بشكل متزامن للحماية من الهجمات التشخيصية والموزعة.
A٧-٩	التحقق من أن كافة ضوابط التحقق من الهوية فعالة من جهة الخادم.
A٧-١٠	التحقق من أن حقول كلمات المرور تسمح باستخدام عبارات مرور، ولا تمنع استخدام عبارات مرور طويلة أو معقدة للغاية، وتوفر حماية كافية من استخدام كلمات المرور الدارجة.
A٧-١١	التحقق من أن كافة وظائف إدارة الحسابات، (مثل التسجيل، أو تحديث الملف التعريفي، أو "نسيت اسم المستخدم"، أو "نسيت كلمة المرور"، أو رمز التعريف غير المفعل/المفقود، أو مكتب المساعدة، أو الاستجابة الصوتية التفاعلية "IVR")، والتي يمكن أن تستعيد صلاحية الوصول إلى الحساب، قادرة على مقاومة الهجمات بنفس مستوى الآلية الأساسية للتحقق من الهوية.
A٧-١٢	التحقق من أن المستخدمين يمكنهم تغيير بيانات اعتمادهم باستخدام آلية مقاومة للهجمات تتمتع بنفس قدرة الآلية الأساسية للتحقق من الهوية على مقاومة الهجمات (مثل الرسائل النصية، أو رموز تعريفية، أو تطبيقات الهواتف المحمولة، أو غيرها). عند تغيير كلمات المرور، يجب إدخال كلمة المرور الحالية قبل إدخال كلمة المرور الجديدة وأن يتبع ذلك عملية إعادة تحقق من المستخدم.
A٧-١٣	التحقق من انتهاء صلاحية بيانات الاعتماد بعد مرور فترة زمنية يتم إعدادها إدارياً. ويجب أن تكون فترة انتهاء صلاحية كلمة المرور قصيرة بناءً على حساسية التطبيق، مما يفرض بالتالي تغيير كلمة المرور بشكل أسرع.

A٧-١٤	التحقق من تسجيل كافة قرارات التحقق من الهوية بما في ذلك "المباعدات الخطية" و"الأقفال المؤقتة".
A٧-١٥	التحقق من أن كلمات مرور الحسابات مجزئة عشوائياً باستخدام طريقة تجزئة عشوائية خاصة لكل حساب (مثل هوية مستخدم الإنترنت أو إنشاء الحساب) واختزالها قبل التخزين.
A٧-١٦	التحقق من أن كافة بيانات اعتماد التحقق من الهوية للوصول للخدمات الخارجية بالنسبة للتطبيق مشفرة ومخزنة في موقع محمي (وليس في شفرة مصدرية).
A٧-١٧	التحقق من أن نسيان كلمة المرور ومسارات الاستعادة ترسل رمز تفعيل أو تحقّق من الهوية متعدّد العناصر له وقت محدد (مثل الرسائل النصية، أو رموز تعريفية، أو تطبيقات الهواتف المحمولة، أو غيرها) بدلاً من إرسال كلمة المرور.
A٧-١٨	التحقق من أن وظيفة "نسيت كلمة المرور" لا تغلق الحساب أو تلغي تفعيله إلا بعد أن ينجح المستخدم في تغيير كلمة المرور.
A٧-١٩	التحقق من عدم وجود أسئلة وإجابات معرفية مشتركة (ما يسمى بالأسئلة والإجابات "السرية").
A٧-٢٠	التحقق من إمكانية إعداد النظام وضبطه بحيث لا يسمح باستخدام أرقام قابلة للإعداد من كلمات مرور سابقة.
A٧-٢١	التحقق من تنفيذ كافة ضوابط التحقق من الهوية مركزياً (بما في ذلك المكتبات التي تستدعي خدمات تحقق خارجية).
A٧-٢٢	التحقق من طلب إعادة التحقق من الهوية أو تحقق الإعداد أو التحقق من الهوية المتغير، أو الرسالة النصية أو التطبيق ثنائي العوامل أو توقيع المعاملة قبل السماح بأي عمليات حساسة على التطبيق وفقاً للملف التعريفي للمخاطر الخاصة بالتطبيق.
A٧-٢٣	التحقق من وجود وظيفة لإلغاء تفعيل بيانات اعتماد المستخدم أو إبطالها في حال وقوع انتهاك أمني.
A٧-٢٤	التحقق من تشفير كلمة المرور وفقاً للمعايير والإجراءات ذات العلاقة.
A٧-٢٥	إذا كان تطبيق <اسم الجهة> يدير مخزن بيانات اعتماد، فإنه يجب أن يضمن تخزين قيمة الاختزال باتجاه واحد وبطريقة مشفرة بدرجة تعقيد عالية لكلمات المرور، وأن الجدول والملف الذي يخزن كلمات المرور والمفاتيح يمكن الكتابة عليه فقط عن طريق التطبيق. (يجب عدم استخدام خوارزمية "MD٥" قدر الإمكان).
A٧-٢٦	فصل منطق التحقق من الهوية عن المصدر الذي يتم طلبه، واستخدام إعادة التوجيه من وإلى مراقبة التحقق من الهوية المركزي.

A٧-٢٧	يجب ألا تشير رسائل فشل التحقق من الهوية إلى الجزء غير الصحيح من بيانات التحقق من الهوية. فعلى سبيل المثال، بدلاً من استخدام "اسم مستخدم غير صحيح" أو "كلمة مرور غير صحيحة"، يجب استخدام "اسم مستخدم غير صحيح أو كلمة مرور غير صحيحة" لكلا الحالتين. ويجب أن تكون رسائل الأخطاء متطابقة في الشفرة المصدرية وعند عرضها.
A٧-٢٨	التحقق من قوة كلمة المرور والتأكد من عدم تطابقها مع كلمات المرور الضعيفة الدارجة.
A٧-٢٩	يجب تطبيق متطلبات درجة طول وتعقيد كلمة المرور الواردة في السياسة أو اللائحة المعتمدة لدى <اسم الجهة>، كما يجب أن تكون بيانات اعتماد التحقق من الهوية كافية لمواجهة الهجمات التي تعتبر شائعة بالنسبة للتهديدات الموجودة في بيئة التثبيت. ويجب التحقق من أن كلمة المرور تتضمن كحد أدنى ما يلي: • حرف كبير واحد على الأقل (A-Z). • حرف صغير واحد على الأقل (a-z). • رقم واحد على الأقل (٠-٩). • رمز خاص واحد على الأقل مثل:(!"#$%&'()*+,- ./:;<=>?@[\]^_`{|}~"). كما يجب التحقق من أن كلمة المرور لا تتضمن على الأقل ما يلي: • أكثر من رقمين أو رمزين متطابقين متتاليين (مثل "١١١" و"aa"). • أرقام أو رموز متسلسلة (مثل "١٢٣"، أو "٧٨٩"، أو"abc"). • نفس اسم المستخدم. • كلمات قاموسية ("password"، أو "p@ssw٠rd"، أو "secret١٢٣").
A٧-٣٠	إنفاذ إلغاء تفعيل الحساب بعد عدد محدد من محاولات تسجيل الدخول غير الصحيحة (على سبيل المثال، خمس محاولات للتطبيقات غير الهامة وثلاث محاولات للتطبيقات الحساسة). ويجب إلغاء تفعيل الحساب لفترة زمنية معينة تكون كافية لإحباط محاولات الهجوم التخميني لبيانات الاعتماد شريطة ألا تكون هذه المدة طويلة بحيث تسمح بتنفيذ هجمات حجب الخدمة (مثلاً إلغاء التفعيل لمدة ٣٠ دقيقة فقط).
A٧-٣١	يجب إبلاغ المستخدم بآخر استخدام للحساب (سواءً كان ناجحاً أم لا) عند تسجيله الدخول بنجاح.
A٧-٣٢	التحقق من استخدام التطبيق لتنفيذ التحكم بإدارة الجلسة التلقائية الخاصة بإطار العمل.
A٧-٣٣	التحقق من إبطال الجلسات عند تسجيل خروج المستخدم.
A٧-٣٤	التحقق من انتهاء وقت الجلسات بعد مرور فترة معينة من عدم النشاط.

اختر التصنيف

A٧-٣٥	التحقق من أن كافة الصفحات التي تقتضي التحقق من الهوية للوصول إليها تتضمن روابط لتسجيل الخروج.
A٧-٣٦	التحقق من أن هوية الجلسة غير مكشوفة أبداً إلا في عناوين ملفات الارتباط (Cookie Headers)، وتحديداً في شريط العنوان (URL) أو رسائل الخطأ أو السجلات. ويتضمن هذا التحقق من أن التطبيق لا يدعم قيام شريط العنوان (URL) بإعادة كتابة جلسات الملفات التعريفية.
A٧-٣٧	التحقق من تغيير هوية الجلسة أو مسحها عند تسجيل الخروج.
A٧-٣٨	التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية باستخدام آلية "HttpOnly" (عدم عرض ملفات الارتباط عند المستخدم).
A٧-٣٩	التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية بخاصية "Secure" وأن عناوين أمن النقل المقيد موجودة (مثل: "Strict-Transport-Security: max-age=٦٠٠٠٠; includeSubDomains").
A٧-٤٠	التحقق من تغيير هوية الجلسة عند تسجيل الدخول لمنع سرقة بيانات الجلسة.
A٧-٤١	التحقق من تغيير هوية الجلسة عند إعادة التحقق من الهوية.
A٧-٤٢	التحقق من أن الرموز التعريفية للجلسات المصادق عليها طويلة وعشوائية بالقدر الكافي لمواجهة الهجمات التي تعتبر تهديدات شائعة في بيئة التثبيت.
A٧-٤٣	التحقق من أن الرموز التعريفية للجلسات المصادق عليها والتي تستخدم ملفات الارتباط لها مسار محدد بقيمة حصرية ملائمة لذلك الموقع. ويجب عدم تحديد تقييد خاصية ملف ارتباط النطاق إلا إذا كانت الأعمال تقتضي ذلك، كعملية تسجيل دخول موحد.
A٧-٤٤	التحقق من أن التطبيق لا يسمح بجلسات مستخدم متزامنة مكررة صادرة من أجهزة مختلفة.
A٧-٤٥	التحقق من انتهاء وقت الجلسات بعد مرور الحد الأقصى لفترة زمنية تم إعدادها إدارياً بغض النظر عن النشاط (أي وقت انتهاء مطلق).
A٧-٤٦	إصدار هوية جديدة للجلسة في حال تغيير أمن الاتصال من بروتوكول نقل النص التشعبي (HTTP) إلى بروتوكول نقل النص التشعبي الآمن (HTTPS)، والذي قد يحدث خلال عملية التحقق من الهوية. من المستحسن استخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) باستمرار في التطبيق بدلاً من التنقل بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS).

اختر التصنيف

الإصدار <١,٠>

A٨	إلغاء التسلسل غير الآمن (OWASP:A٨:٢٠٢١- فشل سلامة البرامج والبيانات)
A٨-١	تطبيق عمليات التحقق من سلامة المعلومات، مثل التواقيع الرقمية، لأي كائنات متسلسلة لمنع إنشاء كائنات عدائية أو التلاعب بالبيانات.
A٨-٢	إنفاذ قيود محددة خلال إلغاء التسلسل قبل إنشاء الكائن لأن الشفرة تتوقع عادة مجموعة فئات قابلة للتحديد. من غير المستحسن الاعتماد على هذا الأسلوب فقط نظراً إلى وجود طرق لتجاوزه.
A٨-٣	عزل الشفرة التي يتم إلغاء تسلسلها وتشغيلها في بيئات متدنية المزايا والصلاحيات حيثما أمكن.
A٨-٤	تسجيل استثناءات إلغاء التسلسل وحالات الإخفاق، مثل الحالات التي لا يكون فيها النوع الوارد هو النوع المتوقع أو التي يحدد فيها إلغاء تسلسل الاستثناءات.
A٨-٥	تقييد أو مراقبة الربط البيني الوارد والصادر في الشبكة من الحاويات أو الخوادم التي تم إلغاء تسلسلها.
A٨-٦	مراقبة إلغاء التسلسل والتنبيه إذا كان المستخدم يلغي التسلسل باستمرار.
A٩	التعامل مع الأخطاء وتسجيلها (OWASP:A٩:٢٠٢١ – فشل أمن السجلات والمراقبة)
A٩-١	ضمان إجراء التحقق الصريح من الأخطاء للبرمجيات المطورة داخلياً، وتوثيقه لكافة المدخلات، بما في ذلك الحجم ونوع البيانات والنطاقات أو الصيغ المسموحة.
A٩-٢	التحقق من أن التطبيق لا يظهر رسائل خطأ أو يكدس آثاراً تتضمن معلومات محمية، بما في ذلك هوية الجلسة والمعلومات الشخصية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها.
A٩-٣	التحقق من تنفيذ جميع عمليات التعامل مع الأخطاء على أجهزة موثوقة.
A٩-٤	التحقق من تطبيق كافة ضوابط التسجيل على الخادم.
A٩-٥	التحقق من أن منطق التعامل مع الأخطاء في الضوابط الأمنية يحجب الوصول تلقائياً.
A٩-٦	التحقق من أن ضوابط التسجيل الأمنية تسمح بتسجيل أحداث النجاح والإخفاق التي تم تحديدها باعتبارها مهمة أمنياً.
A٩-٧	التحقق من أن كل حدث في السجل يتضمن ختماً زمنياً من مصدر موثوق، ومستوى شدة الحدث، ومؤشراً على أن الحدث مهم أمنياً (إذا كان مختلطاً مع سجلات أخرى)، وهوية المستخدم الذي تسبب بالحدث (إذا كان هناك مستخدم مرتبط بالحدث)، ومصدر عنوان

	بروتوكول الإنترنت للطلب المصاحب للحدث سواءً كان الحدث ناجحاً أو فاشلاً، ووصفاً للحدث.
A٩-٨	التحقق من أن كافة السجلات محمية من الوصول غير المصرح به والتعديل.
A٩-٩	التحقق من أن التطبيق لا يسجل معلومات محمية خاصة بالتطبيق، بما في ذلك هوية الجلسة والمعلومات الشخصية أو المحمية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها.
A٩-١٠	التحقق من توفر أداة تحليل السجل مما يسمح للمحلل بالبحث عن أحداث السجل بناءً على تركيبة من معايير البحث في كافة الحقول في صيغة السجل المدعومة من النظام.
A٩-١١	التحقق من عدم تنفيذ كافة الأحداث التي تتضمن بيانات غير موثوقة باعتبارها شفرة في برمجيات استعراض السجلات المعنية.
A٩-١٢	التحقق من وجود تنفيذ تسجيل موحد مستخدم في التطبيق.
A٩-١٣	التحقق من أن السجلات لها إجراء منتظم موحد للنسخ الاحتياطية أو الأرشفة.
A٩-١٤	تطبيق "التعامل مع الاستثناءات في الشفرات" حيثما أمكن.
A٩-١٥	التحقق من أن السجلات أدناه مفعلة: • سجل يشمل كل حالات الإخفاق في التحقق من المدخلات. • سجل يشمل كل محاولات التحقق من الهوية، وخصوصاً حالات الإخفاق. • سجل يشمل كل حالات الإخفاق في التحكم بالوصول. • سجل يشمل كل أحداث التلاعب الظاهرة، بما في ذلك التغييرات غير المتوقعة على حالة البيانات. • سجل يشمل كل محاولات الاتصال بالرموز التعريفية لجلسة منتهية الصلاحية أو غير صحيحة. • سجل يشمل كل استثناءات النظام. • سجل يشمل كل الوظائف الإدارية، بما في ذلك التغييرات على إعدادات الضبط والتهيئة الأمنية. • سجل يشمل كل حالات إخفاق اتصال أمن طبقة النقل بأجهزة النقطة النهائية. • سجل يشمل كل حالات إخفاق نموذج التشفير.
A١٠	**تزوير الطلب عبر الخوادم (OWASP:A١٠:٢٠٢١– SSRF)**
A١٠-١	وظائف الوصول عن بعد للمصادر يجب أن تكون مفصولة داخل شبكات الإنترنت لتقليل التأثير من اختراقات تزوير الطلب عبر الخوادم.

A١٠-٢	<اسم الجهة> يجب أن تطبق سياسات "المنع بشكل افتراضي" في جدار الحماية أو في نقاط وصول شبكات الإنترنت لمنع جميع التحركات داخل الشبكة الداخلية الغير ضرورية.
A١٠-٣	جميع مدخلات العملاء يجب أن تتم تصفيتها وفحصها.
A١٠-٤	التحقق من صحة المخطط للرابط الإلكتروني (URL)، مع تحديد المنفذ والوجهة النهائية مع قائمة السماح المحددة.
A١٠-٥	<اسم الجهة> يجب منع ارسال الاستجابات والردود للعميل على هيئتها الأصلية.
A١٠-٦	<اسم الجهة> يجب تعطيل إعادة التوجيه بروتوكول (HTTP).
A١٠-٧	<اسم الجهة> يجب أن تتأكد من أن العاملين لديهم الوعي الكافي لفهم تناسق وخصائص الرابط الإلكتروني (URL) لتجنب الاختراقات مثل اختراق إعادة الربط لنظام اسم المجال (DNS) و "وقت الفحص، وقت الاستخدام" (TOCTOU).
A١٠-٨	عدم تثبيت خدمات أمنية أخرى على أنظمة الواجهة مثل خدمة الهوية المفتوحة (OpenID). تقييد حركات المرور الداخلية على هذه الأنظمة مثل المضيف المحلي.
A١٠-٩	يجب استخدام وظائف وتقنيات تشفير الإنترنت مثل شبكات الخصوصية الافتراضية (VPNs) على الأنظمة المستقلة.
A١١	**التحقّق من الهاتف المحمول**
A١١-١	التأكد من تحقق العميل من شهادات تشفير طبقة المنافذ الآمنة (SSL).
A١١-٢	التحقق من عدم استخدام قيم رقم تعريف الجهاز المميز (UDID) كضوابط أمنية.
A١١-٣	التحقق من أن تطبيق الهاتف المحمول لا يخزن المعلومات المحمية على المصادر المشتركة على الجهاز (مثل بطاقة "SD" أو المجلدات المشتركة).
A١١-٤	التحقق من أن المعلومات المحمية ليست مخزنة في قاعدة بيانات "SQLite" على الجهاز.
A١١-٥	التحقق من أن المفاتيح السرية وكلمات المرور ليست مثبتة في الشفرة في البرامج التنفيذية.
A١١-٦	التحقق من أن تطبيق الهاتف المحمول يمنع تسرب المعلومات المحمية عن طريق خاصية التصوير التلقائي في نظام تشغيل "iOS".
A١١-٧	التحقق من أن التطبيق لا يمكن تشغيله على جهاز تم إلغاء القيود الموجودة عليه (Jailbroken) أو جهاز يتمتع بصلاحيات ومزايا هامة وحساسة (Rooted).
A١١-٨	التحقق من أن وقت انتهاء الجلسة له قيمة منطقية.

اختر التصنيف

A١١-٩	التحقق من التصاريح التي يتم طلبها ومن المصادر التي يتم منح تصاريح الوصول إليها (AndroidManifest.xml، وiOS Entitlements).
A١١-١٠	التحقق من أن سجلات انهيار النظام لا تتضمن معلومات محمية.
A١١-١١	التحقق من عدم وضوح النظام الثنائي في التطبيق.
A١١-١٢	التحقق من أن كافة بيانات الاختبار قد تم إزالتها من حاوية التطبيق (.apk .bar .ipa).
A١١-١٣	التحقق من أن التطبيق لا يقوم بتسجيل المعلومات المحمية على سجل النظام أو ملفات النظام.
A١١-١٤	التحقق من أن التطبيق لا يتيح الإكمال التلقائي للنصوص الحساسة في حقول المدخلات مثل حقول كلمات المرور أو المعلومات الشخصية أو بطاقات الائتمان.
A١١-١٥	التحقق من أن تطبيق الهاتف المحمول يطبق عملية تثبيت الشهادات (Certificate Pinning) لمنع إدارة حركة البيانات في التطبيق بالوكالة.
A١١-١٦	التحقق من عدم وجود إعدادات خاطئة في ملفات الإعدادات (مجموعة العلامات التصحيحية، وتصاريح قابلة للقراءة وللكتابة العالمية).
A١١-١٧	التحقق من تحديث مكتبات الأطراف الخارجية قيد الاستخدام وعدم احتوائها على أي ثغرات معروفة.
A١١-١٨	التحقق من عدم تخزين بيانات الويب مثل حركة بيانات بروتوكول نقل النص التشعبي الآمن (HTTPS).
A١١-١٩	التحقق من عدم استخدام سلسلة الأحرف للاستفسار (Query String) مع المعلومات المحمية. بدلاً من ذلك، يجب استخدام طلب "POST" عبر طبقة المنافذ الآمنة (SSL) مع رمز تعريفي للحماية من تزوير الطلب عبر المواقع (CSRF).
A١١-٢٠	التحقق، إن أمكن، من أن أرقام الحسابات الشخصية متقطعة قبل تخزينها على الجهاز.
A١١-٢١	التحقق من أن التطبيق يستفيد من خاصية التوزيع العشوائي لمخطط مساحات العناوين (ASLR).
A١١-٢٢	التحقق من أن البيانات المسجلة عن طريق لوحة المفاتيح (iOS) لا تتضمن بيانات اعتماد أو معلومات مالية أو معلومات محمية أخرى.
A١١-٢٣	في تطبيقات الأندرويد، التحقق من أن التطبيق لا ينشئ ملفات بتصاريح " MODE_WORLD_READABLE " أو " MODE_WORLD_WRITABLE ".

اختر التصنيف

الإصدار <١,٠>

A١١-٢٤	التحقق من تخزين المعلومات المحمية بطريقة مشفرة وآمنة (حتى عند تخزينها في سلسلة مفاتيح "iOS").
A١١-٢٥	التحقق من تطبيق آليات مكافحة التصحيح والهندسة العكسية في التطبيق.
A١١-٢٦	التحقق من أن التطبيق لا يستورد أنشطة حساسة أو مزودي محتوى أو غيرهم على الأندرويد.
A١١-٢٧	التحقق من استخدام هيكليات متغيرة لسلاسل الحروف العشوائية (Strings) الحساسة مثل أرقام الحسابات، والكتابة فوقها عند عدم استخدامها (لتقليل الأضرار الناجمة عن هجمات تحليل الذاكرة).
A١١-٢٨	التأكد من تنفيذ التحقق الكامل من البيانات على المدخلات لأي رسائل أنشطة ومزودي محتوى ومتلقي بث معرضين للمخاطر (الأندرويد).

الأدوار والمسؤوليات

١- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة وتحديث المعيار:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ وتطبيق المعيار:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار باستمرار.

٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

٣- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.