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:

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

# اعتماد الوثيقة

| الدور | الاسم | التاريخ | التوقيع |
|---|---|---|---|
| اختر الدور | <أدخل الاسم الكامل للشخص> | اضغط هنا لإضافة نص | <أدخل التوقيع> |
| | | | |

# نسخ الوثيقة

| النسخة | التاريخ | عُدلَ بواسطة | أسباب التعديل |
|---|---|---|---|
| <أدخل رقم النسخة> | اضغط هنا لإضافة نص | <أدخل الاسم الكامل للشخص> | <أدخل وصف التعديل> |
| | | | |

اختر التصنيف

الإصدار 1.0

# قائمة المحتويات

## الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتطوير البرمجيات والتطبيقات وحمايتها من التهديدات الداخلية والخارجية في <اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-٣-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018).

## نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة أنشطة ومشاريع وممارسات تطوير البرمجيات والتطبيقات والأصول المعلوماتية والتقنية الخاصة بها في <اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

## المعايير

| 1 | التطوير الآمن للتطبيقات (Secure Code Development) |
|---|---|
| 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 | |
| 1-1 | تطوير عملية دورة حياة تطوير البرمجيات الآمنة (SSDLC) وتطبيقها.<br>A Secure Software Development Life Cycle (SSDLC) process Shall be developed and implemented. |
| 2-1 | تطوير منهجية وعملية "التطوير والأمن والعمليات" (DevSecOps) واتباعها.<br>A DevSecOps methodology and process shall be developed and adopted. |
| 3-1 | ضمان توفير متطلبات الأمن السيبراني في المراحل الأولية من تطوير البرمجيات ودمجها في دورة حياة تطوير البرمجيات الآمنة (SSDLC). |

| | |
|---|---|
| Cybersecurity requirements shall be provided in the initial phases of software development and incorporated in the SSDLC process. | |
| ضمان اختبار الأمن السيبراني في مراحل اختبار تطوير البرمجيات ودمجه في دورة حياة تطوير البرمجيات الآمنة (SSDLC).<br>Cybersecurity testing shall be conducted in the testing phases of software development and incorporated in the SSDLC process. | 4-1 |
| تصميم وإعداد بيئة آمنة لغايات التطوير والاختبار وضمان الجودة.<br>A secure environment shall be designed and configured for development, testing and quality assurance purposes. | 5-1 |
| تطبيق إرشادات تطوير التطبيقات الآمن وفقاً للجدول (أ).<br>The secure coding guidelines under Table (A) shall be implemented. | 6-1 |
| تطبيق إجراءات التخفيف على أعلى 10 مخاطر تهدد أمن تطبيقات الويب وفقاً للمشروع المفتوح لأمن تطبيقات الويب (OWASP) فيما يخص الأنظمة والتطبيقات الحساسة.<br>Mitigations to the Open Web Application Security Project (OWASP) Top 10 Application Security Risks shall be implemented for critical systems and applications. | 7-1 |
| تطبيق آليات لتقييد صلاحيات التعديل على الشفرة المصدرية أو بيانات بيئات الإنتاج.<br>Mechanisms to restrict modification of production source code or production data shall be implemented. | 8-1 |
| إلزام الموردين الخارجيين بالالتزام بسياسات ومعايير الأمن السيبراني المعتمدة في <اسم الجهة>.<br>Third party vendors shall be required to adhere to <entity name>'s cybersecurity policies and standards. | 9-1 |
| الحصول عليجب استخدام المصادر الحديثة والموثوق بها والمرخصة فقط لأدوات تطوير البرمجيات والمكتبات والمكونات<br>Only up-to-date, trusted and licensed sources of software development tools, libraries and components shall be used. | 10-1 |

| | |
|---|---|
| 11-1 | ضمان تطبيق ضوابط حماية تطبيقات الويب وفقاً لسياسة ومعيار حماية تطبيقات الويب المعتمدين في <اسم الجهة>.<br>Web application security controls shall be implemented as per <entity name>'s Web Application Security Policy and Standard. |
| 12-1 | استخدام خوارزميات تشفير موحدة ومراجعة بدقة وفقاً للمعايير والإجراءات ذات العلاقة.<br>Standardized and extensively reviewed encryption algorithms shall be used only as per relevant standards and procedures. |
| 13-1 | التحقق من أن إصدارات كافة البرمجيات التي تم شراؤها من خارج <اسم الجهة> مدعومة من المطور ومحصنة بصورة ملائمة بناءً على التوصيات الأمنية للمطور.<br>All versions of all software acquired from outside <entity name> shall be verified to be still supported by the developer and appropriately hardened based on the developer's security recommendations. |
| 14-1 | تدريب جميع العاملين في تطوير البرمجيات على كتابة الشفرات المصدرية المناسبة للغة البرمجة وبيئة التطوير المستخدمة.<br>Conduct training on writing secure code appropriate to the programming language and development environment being used for all software development personnel. |
| 2 | مستودع الشفرة المصدرية (Source Code Repository) |
| 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 | |
| 1-2 | استخدام مستودع شفرة مصدرية آمن يمتاز بتطبيق إجراءات التحقق من الهوية والإصدار والرقابة وتسجيل الدخول. |

| | |
|---|---|
| A secure source code repository that has authentication, version control, and logging enabled shall be used. | |
| تطبيق إجراءات منع وصول أي شخص إلى الشفرة المصدرية ومستودع الشفرة المصدرية باستثناء مطوري التطبيقات والجهات المسؤولة عنها.<br>Deny access to source code and source code repository for anyone except application developers and owners. | 2-2 |
| استخدام خطة ترقيم موحدة لضوابط الإصدار بحيث تبين تاريخ تثبيت الإصدارات المحدثة من البرمجيات.<br>A unified version control numbering scheme shall be used to reflect when updated versions of the software are installed. | 3-2 |
| أرشفة الإصدارات القديمة من الشفرة المصدرية دورياً.<br>Outdated versions of source code shall be archived periodically. | 4-2 |
| فصل الشفرة المصدرية للتطبيقات قيد التطوير عن الشفرة المصدرية للتطبيقات في بيئة الإنتاج.<br>Source code for applications under development shall be segregated from source code for applications in production. | 5-2 |
| أرشفة الشفرة المصدرية للتطبيقات التي انتهت صلاحيتها بحيث يمكن استرجاعها عند الحاجة.<br>The source code of end of life applications shall be archived to ensure that it can still be retrieved if needed. | 6-2 |
| الحصول على نسخة من الشفرة المصدرية لكافة التطبيقات التي طورتها أطراف خارجية لـ<اسم الجهة> وتخزينها في مستودع الشفرة المصدرية.<br>A copy of the source code for all applications developed by third parties specifically for <entity name> shall be acquired and stored in a secure source code repository. | 7-2 |
| تطوير معايير تحصين وأمن الحاويات والنسخ الافتراضية للنظام (Docker) وإرشادات الممارسات الأمنية المثلى وتطبيقها. | 8-2 |

اختر التصنيف

| | |
|---|---|
| | Container and docker security hardening standards and security best practices guidelines shall be developed and implemented. |
| 9-2 | تثبيت آليات إدارة الأسرار وذلك من أجل إدارة الأسرار والمفاتيح والشهادات ومنع تخزين الأسرار في الحاويات.<br>Secret management mechanisms shall be deployed to manage secrets, keys and certifications and prevent storing secrets in containers. |
| 10-2 | استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة.<br>Container images shall be used from trusted or approved sources. |
| 11-2 | استخدام سجل حاويات خاص لضمان تنزيل نسخ الحاويات المعتمدة والآمنة فقط على النظام بحيث يمكن فحص كل نسخة بحثاً عن الثغرات المعروفة والشائعة.<br>A private container registry shall be used to ensure only verified and safe container images are downloaded to <entity name>'s system, and that every image is scanned for common known vulnerabilities. |
| 12-2 | عدم إدارة الحاويات من خلال حسابات المستخدمين عالية الصلاحية والامتيازات.<br>Containers shall not be run with superuser accounts. |
| 3 | مراجعة واختبار الشفرة المصدرية (Secure Code Review and Testing) |
| 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 | |
| 1-3 | إجراء عملية مراجعة الشفرة المصدرية بانتظام لتطبيقات الويب المطورة داخلياً.<br>A secure code review process shall be conducted regularly for internally developed web applications. |

| | |
|---|---|
| 2-3 | تطبيق أدوات التحليل الثابتة والديناميكية للتحقق من الالتزام بممارسات تطوير التطبيقات الآمن بالنسبة للبرمجيات المطورة داخلياً.<br><br>Static and dynamic analysis tools shall be applied to verify that secure coding practices are being adhered to for internally developed software. |
| 3-3 | القيام بمراجعة أمنية الشفرة المصدرية بانتظام لكافة التطبيقات المطورة لـ<اسم الجهة> من قبل أطراف خارجية.<br><br>Conduct a secure code review process regularly for all applications developed by third parties specifically for <entity name>. |
| 4-3 | مراجعة واعتماد الضوابط الأمنية للتطبيقات المطورة داخلياً قبل تثبيتها في بيئة الإنتاج.<br><br>Security controls of new internally developed applications shall be reviewed and approved prior to application deployment into the production environment. |
| 5-3 | إعادة تقييم التطبيقات الحالية المطورة داخلياً وإعادة اعتمادها بعد إجراء تغيير رئيسي عليها أو بعد مرور فترة زمنية محددة.<br><br>Existing internally developed applications shall be re-evaluated and re-approved after a significant change is made to the application, or after a predetermined period. |
| 6-3 | 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>).<br><br>Risk assessments for all applications under development, or which are purchased, shall be conduced to determine the controls required to mitigate application risks to acceptable limits prior to deployment into production environment (refer to <entity name>'s Risk Management Policy). |
| 7-3 | إجراء اختبار الالتزام بالأمن السيبراني للبرمجيات بناءً على سياسات الأمن السيبراني المعتمدة في <اسم الجهة> قبل التثبيت في بيئة الإنتاج.<br><br>Cybersecurity compliance testing shall be conducted for software against <entity name>'s cybersecurity policies and standards prior to deployment into production environment. |

اختر التصنيف

| | |
|---|---|
| 8-3 | 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.<br>OWASP Application Security Verification Standard shall be employed as a guide to define security requirements and generate test cases to review critical systems and applications. |
| 9-3 | إجراء مراجعة لإعدادات البرمجيات بما في ذلك مراجعة الإعدادات والتحصين وحزم التحديثات قبل التثبيت في بيئة الإنتاج.<br>Configurations review of software, including secure configuration hardening and patching, shall be conducted prior to deployment into production environment. |
| 10-3 | إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق ومراجعة تطويرالتطبيقات الآمن، قبل التثبيت في بيئة الإنتاج.<br>Cybersecurity testing; including vulnerability assessment, penetrating testing and secure code review; shall be conducted prior to deployment into production environment. |
| 11-3 | إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق، بعد التثبيت في بيئة الإنتاج.<br>Cybersecurity testing, including vulnerability assessment and penetrating testing, shall be conducted after deployment into production environment. |
| 12-3 | معالجة كافة المشاكل الأمنية في التطبيقات المطورة التي يتم اكتشافها خلال مراجعة تطوير التطبيقات الآمن قبل التثبيت في بيئة الإنتاج.<br>All developed application security issues discovered during the secure code review shall be remediated prior to implementation into production environment. |
| 13-3 | اختبار التطبيقات المطورة لضمان تطبيق ضوابط فصل المهام بالصورة الملائمة.<br>Developed applications shall be tested to ensure that Segregation of duties controls are appropriately implemented. |

| | |
|---|---|
| 14-3 | إلغاء حسابات الاختبار الموجودة في بيئة غير بيئة الإنتاج قبل نقل التطبيقات إلى بيئة الإنتاج.<br>Test accounts that are used in non-production environments shall be removed before the application is moved into production. |
| 15-3 | 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.<br>Test and development environment shall be logically separated from production and other environments using network restrictions by configuring Access-Control Lists (ACLs) and security policies on firewalls. |
| 16-3 | إجراء مراجعة النظير للشفرة المصدرية من قبل مطور لم يشارك في كتابة أي شفرة قبل التثبيت في بيئة الإنتاج في <اسم الجهة>.<br>Source code peer-review shall be conducted by a developer who did not write any of the code prior to its deployment into <entity name>'s production environment. |
| 17-3 | استخدام الشفرة المصدرية وأدوات تقييم أمن البرمجيات المعتمدة والمرخصة.<br>Only approved and licensed source code and software security assessment tools shall be used. |
| 18-3 | 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).<br>Security testing for developed applications shall be performed in all testing phases of SDLC including non-functional testing, Unit Testing (UT), System Integration Testing (SIT), and User Acceptance Testing (UAT). |
| 19-3 | استحداث عملية لإدارة العيوب البرمجية في البرمجيات والثغرات والمشكلات الأمنية ووضع سجل خاص بها ومتابعتهما.<br>A process and registry shall be developed and maintained to manage software bugs, vulnerabilities and security issues. |
| 20-3 | إدراج الاختبارات كجزء من عمليات التحسين المستمر والتطوير المستمر (CI/CD). |

اختر التصنيف

| | |
|---|---|
| Testing shall be embedded as part of the Continuous Improvement/Continuous Development (CI/CD) pipeline. | |

## الجدول أ - إرشادات تطوير التطبيقات الآمن

| 1 | علميات التحقق من الهوية (OWASP:A2:2017 - إجراءات التحقق من الهوية غير الآمنة)<br>Authentication (OWASP:A2:2017 – Broken Authentication) |
|---|---|
| 1-1 | التحقق من أن كافة الصفحات والمصادر تقتضي التحقق من الهوية باستثناء المحددة خصوصاً لتكون عامة (مبدأ التحقق التام والمتكامل).<br>It shall be verified that all pages and resources require authentication except those specifically intended to be public (Principle of Complete Mediation). |
| 2-1 | 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.<br>It shall be verified that all password fields do not show users' passwords when entered, and that password fields (or the forms that contain them) have autocomplete disabled. |
| 3-1 | التحقق من أن كافة ضوابط التحقق من الهوية تخفق بصورة آمنة لضمان عدم قدرة الجهات المهاجمة على تسجيل الدخول.<br>It shall be verified that all authentication controls fail securely to ensure that attackers cannot log in. |
| 4-1 | التحقق من أن بيانات الاعتماد وكافة معلومات الهوية الأخرى التي يتعامل معها التطبيق لا تمر عبر روابط غير مشفرة أو مشفرة بصورة غير آمنة.<br>It shall be verified that credentials and all other identity information handled by the application do not traverse unencrypted or through weakly encrypted links. |
| 5-1 | التحقق من أن مسار "نسيت كلمة المرور" ومسارات الاستعادة الأخرى لا ترسل كلمات المرور الحالية أو الجديدة من غير تشفير. |

| | |
|---|---|
| It shall be verified that forgot password and other recovery paths do not send the existing or new passwords in clear text to the user. | |
| 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".<br>It shall be verified that performing username enumeration is not possible via login, password reset, or forgot account functionalities. | 6-1 |
| التحقق من عدم وجود كلمات مرور افتراضية قيد الاستخدام لإطار عمل التطبيق أو أي مكونات مستخدمة من قبل التطبيق (مثل "admin/password").<br>It shall be verified that there are no default passwords in use for the application framework or any components used by the application (such as “admin/password”). | 7-1 |
| 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 "Password1"). 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 60 دقيقة، ويتم إغلاق الحساب بعد 15 دقيقة. ويجب أن تكون آليتا الضبط فاعلتين بشكل متزامن للحماية من الهجمات التشخيصية والموزعة.<br>It shall be verified that a resource governor is in place to protect against vertical brute forcing (i.e., when a single account is tested against all possible passwords) and horizontal brute forcing (i.e., when all accounts are tested with the same password, such as “Password1”). A correct credential entry shall incur no delay. For example, brute force source IP address lockout shall be configured to 60 minutes and account lockout to 15 minutes. Both these governor mechanisms shall be active simultaneously to protect against diagonal and distributed attacks. | 8-1 |
| التحقق من أن كافة ضوابط التحقق من الهوية فعالة من جهة الخادم. | 9-1 |

| | |
|---|---|
| It shall be verified that all authentication controls are enforced on the server side. | |
| 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 الدراجة.<br><br>It shall be verified that password entry fields allow or encourage the use of passphrases, and do not prevent the entry of long passphrases or highly complex passwords, and provide a sufficient minimum strength to protect against the use of commonly chosen passwords. | 10-1 |
| 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.<br><br>It shall be verified that all account management functions (such as registration, update profile, forgot username, forgot password, disabled/lost token, help desk or IVR) that might regain access to the account are at least as resistant to attacks as the primary authentication mechanism. | 11-1 |
| التحقق من أن المستخدمين يمكنهم تغيير بيانات اعتمادهم باستخدام آلية مقاومة للهجمات تتمتع بنفس قدرة الآلية الأساسية للتحقق من الهوية على مقاومة الهجمات. عند تغيير كلمات المرور، يجب إدخال كلمة المرور الحالية قبل إدخال كلمة المرور الجديدة وأن يتبع ذلك عملية إعادة تحقق من المستخدم.<br><br>It shall be verified that users can safely change their credentials using a mechanism that is at least as resistant to attacks as the primary authentication mechanism. Password changes shall require the existing password to be entered prior to entering a new password, followed by re-authentication of the user. | 12-1 |
| 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. | 13-1 |

| | |
|---|---|
| It shall be verified that authentication credentials expire after an administratively configurable period of time. The password expiry duration shall be shorter based on the criticality of the application, thus ensuring a quicker password change. | |
| التحقق من تسجيل كافة قرارات التحقق من الهوية بما في ذلك "المباعدات الخطية" و"الأقفال المؤقتة".<br>It shall be verified that all authentication decisions are logged, including linear back offs and soft-locks. | 14-1 |
| 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.<br>It shall be verified that account passwords are salted using a salt that is unique to each account (e.g., internal user ID, account creation, etc.) and hashed before storing. | 15-1 |
| التحقق من أن كافة بيانات اعتماد التحقق من الهوية للوصول للخدمات الخارجية بالنسبة للتطبيق مشفرة ومخزنة في موقع محمي (وليس في شفرة مصدرية).<br>It shall be verified that all authentication credentials for accessing external services for the application are encrypted and stored in a protected location (not in source code). | 16-1 |
| 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.<br>It shall be verified that forgot password and other recovery paths send a time-limited activation token or use multi-factor authentication (e.g., SMS, tokens, mobile application, etc.) instead of a password. | 17-1 |
| التحقق من أن وظيفة "نسيت كلمة المرور" لا تغلق الحساب أو تلغي تفعيله إلا بعد أن ينجح المستخدم في تغيير كلمة المرور.<br>It shall be verified that “forget password” functionality does not lock or otherwise disable the account until after the user has successfully changed their password. | 18-1 |

| | |
|---|---|
| 19-1 | التحقق من عدم وجود أسئلة وإجابات معرفية مشتركة (ما يسمى بالأسئلة والإجابات "السرية").<br>It shall be verified that there are no shared knowledge questions/answers (Also called "secret" questions and answers). |
| 20-1 | التحقق من إمكانية إعداد النظام وضبطه بحيث لا يسمح باستخدام أرقام قابلة للإعداد من كلمات مرور سابقة.<br>It shall be verified that the system can be configured to disallow the use of a configurable number of previous passwords. |
| 21-1 | التحقق من تنفيذ كافة ضوابط التحقق من الهوية مركزياً (بما في ذلك المكتبات التي تستدعي خدمات تحقق خارجية).<br>It shall be verified that all authentication controls (including libraries that call external authentication services) have a centralized implementation. |
| 22-1 | 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.<br>It shall be verified that re-authentication, step up or adaptive authentication, SMS or other two-factor application, or transaction signing is required before any application-specific sensitive operations are permitted as per the risk profile of the application. |
| 23-1 | التحقق من وجود وظيفة لإلغاء تفعيل بيانات اعتماد المستخدم أو إبطالها في حال وقوع انتهاك أمني.<br>It shall be verified that a functionality to invalidate or disable user credentials in the event of a compromise is in place. |
| 24-1 | التحقق من تشفير كلمة المرور وفقاً للمعايير والإجراءات ذات العلاقة.<br>It shall be verified that password encryption is implemented in accordance with relevant standards and procedures. |
| 25-1 | إذا كان التطبيق 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 "MD5" قدر الإمكان).<br><br>If <entity name>'s application manages a credential store, it shall ensure that only cryptographically strong one-way salted hashes of passwords are stored and that the table/file that stores the passwords and keys is write-able only by the application. (If possible, MD5 algorithm shall not be used). |
| 26-1 | فصل منطق التحقق من الهوية عن المصدر الذي يتم طلبه، واستخدام إعادة التوجيه من وإلى مراقبة التحقق من الهوية المركزي.<br><br>Authentication logic shall be segregated from the resource being requested, and redirection to and from the centralized authentication control shall be used. |
| 27-1 | 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.<br><br>Authentication failure responses shall not indicate which part of the authentication data is incorrect. For example, instead of "Invalid username" or "Invalid password," "Invalid username and/or password" shall be used for both. Error responses shall be truly identical in both display and source code. |
| 28-1 | يجب تطبيق متطلبات درجة تعقيد كلمة المرور الواردة في السياسة أو اللائحة، 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:<br>• حرف كبير واحد على الأقل (A-Z).<br>• حرف صغير واحد على الأقل (a-z).<br>• رقم واحد على الأقل (0-9).<br>• رمز خاص واحد على الأقل مثل: ( !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~").<br>كما يجب التحقق من أن كلمة المرور لا تتضمن على الأقل ما يلي: |

اختر التصنيف

| | |
|---|---|
| | • أكثر من رقمين أو رمزين متطابقين متتاليين (مثل "111" و"aa").<br>• أرقام أو رموز متسلسلة (مثل "123"، أو "789"، أو"abc").<br>• نفس اسم المستخدم.<br>• كلمات قاموسية ("password"، أو "p@ssw0rd"، أو "secret123").<br><br>Password complexity requirements established by a policy or regulation shall be enforced. Authentication credentials shall be sufficient to withstand attacks that are typical of the threats in the deployed environment.<br><br>Additionally, it shall be verified that passwords contain:<br><br>• At least 1 upper case character (A-Z)<br>• At least 1 lower case character (a-z)<br>• At least 1 digit (9-0)<br>• At least 1 special character (e.g.,-,+*()'&%$#"! “ ”~{\|}`_^[\]@?<=>;:/)<br><br>It shall be verified that passwords do not contain:<br><br>• More than 2 identical digits or characters in a row (e.g., 111, aa, etc.)<br>• Sequential digits or characters (e.g., 123, 789, and abc)<br>• The same username<br>• Dictionary words (e.g., password, p@ssw0rd, secret123, etc.) |
| 29-1 | 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 30 دقيقة فقط).<br><br>Accounts shall be disabled after an established number of invalid login attempts (e.g., five attempts for non-critical applications and three attempts for critical applications). Accounts shall be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so |

| | |
|---|---|
| long as to allow for a denial-of-service attack to be performed. (For example, disabled for 30 minutes). | |
| يجب إبلاغ المستخدم بآخر استخدام للحساب (سواءً كان ناجحاً أم لا) عند تسجيله الدخول بنجاح.<br>The last use (successful or unsuccessful) of a user account shall be reported to the user at their next successful login. | 30-1 |
| إدارة الجلسات (OWASP:A2: 2017 - إجراءات التحقق من الهوية غير الآمنة)<br>Session Management (OWASP:A2:2017 – Broken Authentication) | 2 |
| التحقق من استخدام التطبيق لتنفيذ التحكم بإدارة الجلسة التلقائية الخاصة بإطار العمل.<br>It shall be verified that the framework's default session management control implementation is used by the application. | 1-2 |
| التحقق من إبطال الجلسات عند تسجيل خروج المستخدم.<br>It shall be verified that sessions are invalidated when the user logs out. | 2-2 |
| التحقق من انتهاء وقت الجلسات بعد مرور فترة معينة من عدم النشاط.<br>It shall be verified that sessions timeout after a specified period of inactivity. | 3-2 |
| التحقق من أن كافة الصفحات التي تقتضي التحقق من الهوية للوصول إليها تتضمن روابط لتسجيل الخروج.<br>It shall be verified that all pages that require authentication to access them have logout links. | 4-2 |
| 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.<br>It shall be verified that the session ID is never disclosed other than in cookie headers, particularly in URLs, error messages, | 5-2 |

| | |
|---|---|
| or logs. This includes verifying that the application does not support URL rewriting of session cookies. | |
| التحقق من تغيير هوية الجلسة أو مسحها عند تسجيل الخروج.<br>It shall be verified that the session ID is changed or cleared on logout. | 6-2 |
| التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية باستخدام آلية "HttpOnly" (عدم عرض ملفات الارتباط عند المستخدم).<br>It shall be verified that authenticated session tokens using cookies are protected by the use of "HttpOnly". | 7-2 |
| 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=60000; includeSubDomains").<br>It shall be verified that authenticated session tokens using cookies are protected with the "Secure" attribute and strict transport security headers (such as Strict-Transport-Security: max-age=60000; includeSubDomains) is present. | 8-2 |
| التحقق من تغيير هوية الجلسة عند تسجيل الدخول لمنع سرقة بيانات الجلسة.<br>It shall be verified that the session ID is changed on login to prevent session fixation. | 9-2 |
| التحقق من تغيير هوية الجلسة عند إعادة التحقق من الهوية.<br>It shall be verified that the session ID is changed on re-authentication. | 10-2 |
| التحقق من أن التطبيق يتعرف على هويات الجلسات الصادرة عن طريق إطار عمل التطبيق نفسه ويعتبر هذه الهويات فقط صحيحة.<br>It shall be verified that only session IDs generated by the application framework are recognized as valid by the application. | 11-2 |
| التحقق من أن الرموز التعريفية للجلسات المصادق عليها طويلة وعشوائية بالقدر الكافي لمواجهة الهجمات التي تعتبر تهديدات شائعة في بيئة التثبيت. | 12-2 |

| | |
|---|---|
| It shall be verified that authenticated session tokens are sufficiently long and random to withstand attacks that are typical threats in the deployment environment. | |
| 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.<br>It shall be verified that authenticated session tokens using cookies have their path set to an appropriately restrictive value for that site. The domain cookie attribute restriction shall not be set except for a business requirement, such as a single sign on. | 13-2 |
| التحقق من أن التطبيق لا يسمح بجلسات مستخدم متزامنة مكررة صادرة من أجهزة مختلفة.<br>It shall be verified that the application does not permit duplicate concurrent user sessions, originating from different machines. | 14-2 |
| التحقق من انتهاء وقت الجلسات بعد مرور الحد الأقصى لفترة زمنية تم إعدادها إدارياً بغض النظر عن النشاط (أي وقت انتهاء مطلق).<br>It shall be verified that sessions timeout after an administratively configurable maximum time period regardless of the performed activity (i.e., an absolute timeout). | 15-2 |
| 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).<br>A new session identifier shall be generated if the connection security is changed from HTTP to HTTPS, as can occur during authentication. Within an application, it is recommended to consistently utilize HTTPS rather than switching between HTTP to HTTPS. | 16-2 |
| التحكم بالوصول (OWASP:A5:2017 - إجراءات التحكم بالوصول غير الآمنة) | 3 |

اختر التصنيف

| Access Control (OWASP:A5:2017 – Broken Access Control) | |
|---|---|
| التحقق من أن المستخدمين يمكنهم الوصول فقط إلى الوظائف أو الخدمات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.<br>It shall be verified that users can only access secured functions or services for which they possess specific authorization. | 1-3 |
| التحقق من أن المستخدمين يمكنهم الوصول فقط إلى العناوين الآمنة (Secured URLs) التي يملكون تصاريح وصلاحيات خاصة لها.<br>It shall be verified that users can only access secured URLs for which they possess specific authorization. | 2-3 |
| التحقق من أن المستخدمين يمكنهم الوصول فقط إلى ملفات البيانات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.<br>It shall be verified that users can only access secured data files for which they possess specific authorization. | 3-3 |
| التحقق من أن مرجعيات الكائنات المباشرة محمية بحيث يمكن الوصول فقط إلى الكائنات المصرح بها لكل مستخدم.<br>It shall be verified that direct object references are protected in a way that ensures only authorized objects are accessible to each user. | 4-3 |
| التحقق من إلغاء تفعيل تصفح الدليل (Directory Browsing) إلا إذا كان ذلك مطلوباً.<br>It shall be verified that directory browsing is disabled unless required. | 5-3 |
| 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).<br>It shall be verified that users can only access protected data for which they possess specific authorization (for example, by implementing controls to protect against direct object reference tampering and prevent unauthorized access to data). | 6-3 |

| | |
|---|---|
| 7-3 | التحقق من إخفاق ضوابط الوصول بصورة آمنة.<br>It shall be verified that access controls fail securely. |
| 8-3 | 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.<br>It shall be verified that the same access control rules implied by the presentation layer are enforced on the server side for that user role, and that controls and parameters cannot be re-enabled or re-added by users with higher privileges. |
| 9-3 | 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.<br>It shall be verified that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized. |
| 10-3 | التحقق من أن كافة ضوابط الوصول فعالة من جهة الخادم.<br>It shall be verified that all access controls are enforced on the server side. |
| 11-3 | التحقق من أن قرارات التحكم بالوصول يمكن تسجيلها وأن كافة القرارات غير الناجحة قد تم تسجيلها.<br>It shall be verified that all access control decisions can be logged and all failed decisions are logged. |
| 12-3 | التحقق من أن التطبيق أو إطار العمل يصدر رموزاً تعريفية عشوائية معقدة مضادة لتزوير الطلب عبر المواقع (Cross-Site Request Forgery "CSRF")، وتكون هذه 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.<br>It shall be verified that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing protected data, and that the application verifies the presence of such tokens with |

| | |
|---|---|
| the proper value for the current user when processing these requests. | |
| 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.<br>Aggregate access control protection – It shall be verified that the system can protect against aggregate or continuous access of secured functions, resources, or data, possibly by the use of a resource governor, for example, to limit the number of registrations per hour or to prevent the entire database from being scraped by an individual user. | 13-3 |
| التحقق من وجود آلية مركزية (بما في ذلك المكتبات التي تستدعي خدمات تصاريح وصلاحيات خارجية) للتحكم بالوصول إلى كل نوع من المصادر المحمية.<br>It shall be verified that a centralized mechanism (including libraries that call external authorization services) is in place to control access to each type of protected resource. | 14-3 |
| التحقق من الفصل بين المنطق الذي يتمتع بمزايا وصلاحيات عن شفرات التطبيق الأخرى.<br>It shall be verified that there is segregation between privileged logic and other application code. | 15-3 |
| 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.<br>Appropriate access controls shall be implemented for protected data stored on the server. This includes cached data, temporary files and data accessible only by specific system users. | 16-3 |
| التحقق من أن حسابات الخدمة أو الحسابات التي تدعم الاتصالات من الأنظمة الخارجية أو إليها تمتلك الحد الأدنى من الصلاحيات والامتيازات. | 17-3 |

| | |
|---|---|
| It shall be verified that service accounts or accounts supporting connections to or from external systems have the least privilege possible. | |
| التحقق من تطبيق تدقيق الحسابات وإلغاء تفعيل الحسابات غير المستخدمة (على سبيل المثال، بعد مرور أكثر من 30 يوماً من تاريخ انتهاء صلاحية كلمة مرور الحساب).<br>It shall be verified that account auditing is implemented and that unused accounts are disabled (for example, after more than 30 days from the expiration of an account's password). | 18-3 |
| 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.<br>If long authenticated sessions are allowed, a user's authorization shall be periodically re-validated to ensure that their privileges have not changed. In case their privileges have changed, the user shall be logged out and forced to re-authenticate. | 19-3 |
| 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).<br>It shall be verified that the application supports disabling of accounts and terminating sessions when authorization ceases (for example, upon changes to role, employment status, business process, etc.). | 20-3 |
| اعتماد المدخلات (OWASP:A1:2017 - الحقن والإدخال و OWASP:A7:2017 - البرمجة النصية عبر المواقع)<br>Input validation (OWASP:A1:2017 – Injection & OWASP:A7:2017 – Cross-Site Scripting) | 4 |
| التحقق من أن بيئة التشغيل غير معرضة لتجاوز سعة المخزن المؤقت، وأن ضوابط الأمن تمنع تجاوز سعة المخزن المؤقت.<br>It shall be verified that the runtime environment is not susceptible to buffer overflows, and that security controls prevent buffer overflows. | 1-4 |

اختر التصنيف

| | |
|---|---|
| 2-4 | التحقق من أن بيئة التشغيل غير معرضة لحقن تعليمات الاستعلام البنيوية (SQL Injection)، وأن ضوابط الأمن تمنع حقن تعليمات الاستعلام البنيوية (SQL Injection).<br>It shall be verified that the runtime environment is not susceptible to SQL Injection, and that security controls prevent SQL Injection. |
| 3-4 | التحقق من أن بيئة التشغيل غير معرضة لحقن النصوص البرمجية عبر المواقع (XSS)، وأن ضوابط الأمن تمنع حقن النصوص البرمجية عبر المواقع (XSS).<br>It shall be verified that the runtime environment is not susceptible to Cross Site Scripting (XSS), and that security controls prevent XSS. |
| 4-4 | 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).<br>It shall be verified that the runtime environment is not susceptible to LDAP Injection, and that security controls prevent LDAP Injection. |
| 5-4 | 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).<br>It shall be verified that the runtime environment is not susceptible to OS Command Injection, and that security controls prevent OS Command Injection. |
| 6-4 | التحقق من نوع البيانات ونطاقها وطولها (إذا أمكن).<br>Data type, range and length shall be verified (if possible). |
| 7-4 | 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: (< > " ' % ( ) & + \ \' \"\).<br>If any potentially hazardous characters must be allowed as input, additional controls; such as output encoding, secure task specific APIs, and accounting for the utilization of that data throughout the application; shall be implemented. |

اختر التصنيف

| | |
|---|---|
| Examples of common hazardous characters include: ( " < > : "\ '\\ + & ( ) % '). | |
| التأكد من أن جميع عمليات التحقق من صحة المدخلات تتم بواسطة روتين مركزي للتحقق من صحة المدخلات للتطبيق.<br>It shall be verified that all input validation is carried out by a centralized input validation routine for the application. | 8-4 |
| التحقق من أن كافة عمليات التحقق الفاشلة تؤدي إلى رفض المدخلات أو تدقيقها.<br>It shall be verified that all input validation failures result in input rejection or input sanitization. | 9-4 |
| التحقق من تنفيذ كافة إجراءات التحقق أو إجراءات تطوير التطبيقات وإنفاذها على الخادم.<br>It shall be verified that all input validation or encoding routines are performed and enforced on the server side. | 10-4 |
| التحقق من التخلص 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.<br>It shall be verified that all untrusted data that is output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URL attributes) is properly discarded for the applicable context. | 11-4 |
| التحقق من أن مجموعات الرموز، مثل "UTF-8"، محددة لكافة مصادر المدخلات.<br>It shall be verified that a character set, such as UTF-8, is specified for all sources of input. | 12-4 |
| التحقق من أن كافة البيانات المدخلة موحدة لكافة برمجيات فك تشفير أو برمجيات تفسير البيانات المرسلة إلى العميل قبل مصادقتها.<br>It shall be verified that all input data is canonicalized for all downstream decoders or interpreters prior to validation. | 13-4 |
| 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 | 14-4 |

| | |
|---|---|
| | الحساسة أمنياً مثل "رصيد الحساب" أو "الدور" أو "كلمة المرور" محمية من الربط التلقائي الخبيث.<br>If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, it shall be verified that security sensitive fields such as “accountBalance”, “role” or “password” are protected from malicious automatic binding. |
| 15-4 | 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).<br>It shall be verified that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.) |
| 16-4 | التحقق من أن التطبيق يستخدم ضابط تحقق من المدخلات واحد لكل نوع من البيانات التي يتم قبولها.<br>It shall be verified that a single input validation control is used by the application for each type of data that is accepted. |
| 17-4 | التحقق من تسجيل كافة حالات الإخفاق في التحقق من المدخلات.<br>It shall be verified that all input validation failures are logged. |
| 18-4 | التحقق من أن كل نوع من عمليات ترميز المخرجات أو التخلص منها التي يقوم بها التطبيق له ضابط أمني واحد للوجهة المقصودة.<br>It shall be verified that for each type of output encoding/escaping performed by the application, there is a single security control for that type of output for the intended destination. |
| 5 | إلغاء التسلسل غير الآمن (OWASP:A8:2017- إلغاء التسلسل غير الآمن)<br>Insecure Deserialization (OWASP:A8:2017 – Insecure Deserialization) |

| | |
|---|---|
| 1-5 | تطبيق عمليات التحقق من سلامة المعلومات، مثل التواقيع الرقمية، لأي كائنات متسلسلة لمنع إنشاء كائنات عدائية أو التلاعب بالبيانات.<br>Integrity checks, such as digital signatures, shall be implemented on any serialized objects to prevent hostile object creation or data tampering. |
| 2-5 | 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.<br>Strict type constraints during deserialization shall be enforced before object creation as the code typically expects a definable set of classes. Bypasses to this technique have been demonstrated; therefore, reliance solely on this technique is not advisable. |
| 3-5 | عزل الشفرة التي يتم إلغاء تسلسلها وتشغيلها في بيئات متدنية المزايا والصلاحيات حيثما أمكن.<br>Code that deserializes shall be isolated and run in low privilege environments whenever possible. |
| 4-5 | تسجيل استثناءات إلغاء التسلسل وحالات الإخفاق، مثل الحالات التي لا يكون فيها النوع الوارد هو النوع المتوقع أو التي يحدد فيها إلغاء تسلسل الاستثناءات.<br>Deserialization exceptions and failures; such as the cases in which the incoming type is not the expected type, or the deserialization throws exceptions; shall be logged. |
| | تقييد أو مراقبة الربط البيني الوارد والصادر في الشبكة من الحاويات أو الخوادم التي تم إلغاء تسلسلها.<br>Incoming and outgoing network connectivity from containers or servers that deserialize shall be restricted or monitored. |
| | مراقبة إلغاء التسلسل والتنبيه إذا كان المستخدم يلغي التسلسل باستمرار.<br>Deserialization shall be monitored, and an alert shall be issued if a user deserializes constantly. |
| 6 | التشفير (OWASP:A3:2017 - تعرض المعلومات المحمية للمخاطر)<br>Cryptography (OWASP:A3:2017 – Protected Data Exposure) |

اختر التصنيف

| | |
|---|---|
| 1-6 | التحقق من أن كافة دالات التشفير المستخدمة لحماية الأسرار من مستخدم التطبيق مطبقة على الخادم.<br>It shall be verified that all cryptographic functions used to protect secrets from the application user are implemented on the server side. |
| 2-6 | التحقق من أن كافة وحدات التشفير تخفق بصورة آمنة.<br>It shall be verified that all cryptographic modules fail securely. |
| 3-6 | 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).<br>It shall be verified that any master secret(s) is protected from unauthorized access (A master secret is an application credential stored as plaintext on disk that is used to protect access to security configuration information). |
| 4-6 | 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.<br>It shall be verified that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved random number generator when these random values are intended to be unguessable by an attacker. |
| 5-6 | التحقق من أن نماذج التشفير المستخدمة في التطبيق قد تم التحقق منها وفقاً للسياسات والإجراءات ذات العلاقة.<br>It shall be verified that cryptographic modules used by the application have been validated as per relevant policies and procedures. |
| 6-6 | التحقق من أن نماذج التشفير تعمل بنظامها المعتمد وفقاً للسياسات والإجراءات ذات العلاقة. |

| | |
|---|---|
| It shall be verified that cryptographic modules operate in their approved mode in accordance with relevant policies and procedures. | |
| التحقق من وجود سياسة صريحة حول كيفية إدارة مفاتيح التشفير (مثل كيفية إصدارها وتوزيعها وإلغائها وانتهاء صلاحيتها) والتحقق من تطبيق هذه السياسة بصورة ملائمة.<br>It shall be verified that there is an explicit policy for how cryptographic keys are managed (for example, generated, distributed, revoked, or expired), and that this policy is properly enforced. | 7-6 |
| التحقق من وجود عدم الإنكار(Non-Repudiation) من خلال التشفير (التوقيع الرقمي) للمعاملات المالية والتجارة الإلكترونية والسجلات.<br>It shall be verified that non-repudiation through cryptography (digital signing) is present for financial or e-commerce transactions and records. | 8-6 |
| التحقق من حماية كافة مفاتيح التشفير بصورة ملائمة. في حال تعرض المفتاح لانتهاك أمني، فإنه لا يمكن الوثوق به ويجب استبداله أو إلغاؤه.<br>It shall be verified that all cryptographic keys are adequately protected. If a key has been compromised, it shall no longer be trusted and shall be replaced or revoked. | 9-6 |
| التحقق من تشفير المعلومات القابلة لتحديد الهوية (PII) والمعلومات المحمية والبيانات المخزنة عندما لا تكون قيد الاستخدام.<br>It shall be verified that Personally Identifiable Information (PII) and protected information and data are stored encrypted at rest. | 10-6 |
| التعامل مع الأخطاء وتسجيلها (OWASP:A10:2017 - عدم كفاية وفاعلية التسجيل والمراقبة)<br>Error Handling and Logging (OWASP:A10:2017 – Insufficient Logging & Monitoring) | 7 |
| ضمان إجراء التحقق الصريح من الأخطاء للبرمجيات المطورة داخلياً، وتوثيقه لكافة المدخلات، بما في ذلك الحجم ونوع البيانات والنطاقات أو الصيغ المسموحة. | 1-7 |

| | |
|---|---|
| For in-house developed software, explicit error checking shall be performed and documented for all input, including size, data type, and acceptable ranges or formats. | |
| 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.<br>It shall be verified that the application does not output error messages or stack traces containing protected data that could assist an attacker, including a session ID and personal information. | 2-7 |
| التحقق من تنفيذ جميع عمليات التعامل مع الأخطاء على أجهزة موثوقة.<br>It shall be verified that error handling is performed on trusted devices. | 3-7 |
| التحقق من تطبيق كافة ضوابط التسجيل على الخادم.<br>It shall be verified that all logging controls are implemented on the server. | 4-7 |
| التحقق من أن منطق التعامل مع الأخطاء في الضوابط الأمنية يحجب الوصول تلقائياً.<br>It shall be verified that error handling logic in security controls denies access by default. | 5-7 |
| التحقق من أن ضوابط التسجيل الأمنية تسمح بتسجيل أحداث النجاح والإخفاق التي تم تحديدها باعتبارها مهمة أمنياً.<br>It shall be verified that security logging controls provide the ability to log both success and failure events that are identified as security-relevant. | 6-7 |
| 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.<br>It shall be verified that each log event includes a time stamp from a reliable source, severity level of the event, an indication that the event is a security relevant event (if mixed | 7-7 |

| | |
|---|---|
| with other logs), the identity of the user that caused the event (if there is a user associated with the event), the source IP address of the request associated with the event, whether the event succeeded or failed, and a description of the event. | |
| التحقق من أن كافة السجلات محمية من الوصول غير المصرح به والتعديل.<br>It shall be verified that all logs are protected from unauthorized access and modification. | 8-7 |
| 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.<br>It shall be verified that the application does not log application-specific protected data that could assist an attacker, including user's session IDs and personal or protected information. | 9-7 |
| 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.<br>It shall be verified that a log analysis tool is available which allows an analyst to search for log events based on a combination of search criteria across all fields in the log record format supported by this system. | 10-7 |
| التحقق من عدم تنفيذ كافة الأحداث التي تتضمن بيانات غير موثوقة باعتبارها شفرة في برمجيات استعراض السجلات المعنية.<br>It shall be verified that all events that include untrusted data will not execute as code in the intended log viewing software. | 11-7 |
| التحقق من وجود تنفيذ تسجيل موحد مستخدم في التطبيق.<br>It shall be verified that there is a single logging implementation that is used by the application. | 12-7 |
| التحقق من أن السجلات لها إجراء منتظم موحد للنسخ الاحتياطية أو الأرشفة.<br>It shall be verified that logs have a standard regular procedure for backing up or archiving. | 13-7 |
| تطبيق "التعامل مع الاستثناءات في الشفرات" حيثما أمكن. | 14-7 |

| | |
|---|---|
| “Try catch” shall be implemented where applicable. | |
| التحقق من أن السجلات أدناه مفعلة:<br>• سجل يشمل كل حالات الإخفاق في التحقق من المدخلات.<br>• سجل يشمل كل محاولات التحقق من الهوية، وخصوصاً حالات الإخفاق.<br>• سجل يشمل كل حالات الإخفاق في التحكم بالوصول.<br>• سجل يشمل كل أحداث التلاعب الظاهرة، بما في ذلك التغييرات غير المتوقعة على حالة البيانات.<br>• سجل يشمل كل محاولات الاتصال بالرموز التعريفية لجلسة منتهية الصلاحية أو غير صحيحة.<br>• سجل يشمل كل استثناءات النظام.<br>• سجل يشمل كل الوظائف الإدارية، بما في ذلك التغييرات على إعدادات الضبط والتهيئة الأمنية.<br>• سجل يشمل كل حالات إخفاق اتصال أمن طبقة النقل بأجهزة النقطة النهائية.<br>• سجل يشمل كل حالات إخفاق نموذج التشفير.<br>It shall be verified that all the below logs are enabled:<br>• Log of all input validation failures<br>• Log of all authentication attempts, especially failures<br>• Log of all access control failures<br>• Log of all apparent tampering events, including unexpected changes to data status.<br>• Log of attempts to connect with invalid or expired session tokens<br>• Log of all system exceptions<br>• Log of all administrative functions, including changes to the security configuration settings<br>• Log of all backend TLS connection failures<br>• Log of cryptographic module failures | 15-7 |
| حماية المعلومات (OWASP:A3:2017 - تعرض المعلومات المحمية للمخاطر)<br>Data Protection (OWASP:A3:2017 – Protected Data Exposure) | 8 |
| التحقق من إلغاء تفعيل تخزين النماذج التي تتضمن معلومات محمية لدى العميل، بما في ذلك خصائص الإكمال التلقائي. | 1-8 |

| | |
|---|---|
| It shall be verified that all forms containing protected information have disabled client side caching, including autocomplete features. | |
| 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).<br><br>It shall be verified that all protected data is sent to the server in the HTTP message body (i.e., URL parameters shall never be used to send protected data). | 2-8 |
| 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.<br><br>It shall be verified that all cached or temporary copies of protected data stored on the server are protected from unauthorized access, and that those temporary working files are purged a soon as they are no longer required. | 3-8 |
| 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 "1.0" من بروتوكول نقل النص التشعبي "HTTP").<br><br>Client-side caching or temporary copies of pages containing protected data shall be disabled. Additionally, it shall be verified that such copies are protected from unauthorized access or purged/invalidated after an authorized user accesses the protected data). (Cache-Control: no-store, may be used in conjunction with HTTP header control "Pragma: no-cache," which is less effective, but is HTTP/1.0 backward compatible). | 4-8 |
| 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. | 5-8 |

| | |
|---|---|
| It shall be verified that the list of protected data processed by the application is identified, and that there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). Additionally, it shall be verified that such policy is properly enforced. | |
| التحقق من وجود طريقة لحذف كل أنواع المعلومات المحمية الموجودة في التطبيق عند نهاية فترة الاحتفاظ المطلوبة.<br>It shall be verified that there is a method to remove each type of protected data from the application at the end of its required retention period. | 6-8 |
| التحقق من أن التطبيق يقلل عدد المعايير المرسلة إلى الأنظمة غير الموثوقة مثل الحقول المخفية ومتغيرات "Ajax" وملفات الارتباط وقيم العناوين.<br>It shall be verified that the application minimizes the number of parameters sent to untrusted systems, such as hidden fields, Ajax variables, cookies and header values. | 7-8 |
| 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 أن لا يكون المستخدم العادي قادراً على الوصول إلى أكثر من 5 سجلات في الساعة أو أكثر من 30 سجلاً في اليوم.<br>It shall be verified that the application has the ability to detect and alert on abnormal numbers of requests for information, or on the processing of high value transactions for a user's role, such as screen scraping, automated use of web service extraction, or data loss prevention. For example, the average user shall not be able to access more than 5 records per hour or 30 records per day. | 8-8 |
| 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.<br>It shall be verified that credentials used by the application on the server side; such as database connection, password and encryption secret keys; are not hard coded. Any credentials | 9-8 |

| | |
|---|---|
| shall be stored in a separate configuration file on a trusted system and shall be encrypted. | |
| التحقق من أن خصائص الإكمال التلقائي غير مفعلة على النماذج باستثناء النماذج التي تتضمن معلومات محمية، بما في ذلك التحقق من الهوية.<br>It shall be verified that autocomplete features are disabled on forms expected to contain protected information, including authentication. | 10-8 |
| أمن الاتصالات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة)<br>Communication Security (OWASP:A6:2017 – Security Misconfiguration) | 9 |
| 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.<br>It shall be verified that a path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and that each server certificate is valid. | 1-9 |
| 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.<br>It shall be verified that the latest version of TLS is used for all connections (including both external and backend connections) that are authenticated or involve protected data or functions. | 2-9 |
| التحقق من تسجيل حالات إخفاق اتصالات أمن طبقة النقل (TLS) بأجهزة النقطة النهائية.<br>It shall be verified that backend TLS connection failures are logged. | 3-9 |
| التحقق من المصادقة على كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية.<br>It shall be verified that all connections to external systems that involve protected information or functions are authenticated. | 4-9 |

| | |
|---|---|
| 5-9 | 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.<br>It shall be verified that all connections to external systems that involve protected information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly. |
| 6-9 | التحقق من أن اتصالات أمن طبقة النقل (TLS) الفاشلة لا ينتج عنها اتصال غير آمن (غير مشفر).<br>It shall be verified that failed TLS connections do not fall back to an insecure connection. |
| 7-9 | التحقق من أن مسارات شهادات التشفير قد تم بناؤها والتحقق منها لكافة شهادات التشفير الخاصة بالعميل باستخدام جهات الصلاحيات الموثوقة ومعلومات الإلغاء.<br>It shall be verified that certificate paths are built and verified for all client certificates using configured trust anchors and revocation information. |
| 8-9 | التحقق من وجود تنفيذ أمن طبقة النقل (TLS) موحد يتم استخدامه في التطبيق وتم إعداده ليعمل في نظام عمل معتمد.<br>It shall be verified that there is a single standard TLS implementation that is used by the application and configured to operate in an approved mode of operation. |
| 9-9 | التحقق من أن ترميز الرموز المحددة معرف لكافة الاتصالات (مثل "UTF-8").<br>It shall be verified that specific character encodings are defined for all connections (e.g., UTF-8). |
| 10 | أمن البروتوكول (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة و OWASP:A4:2017 لغة الترميز القابلة للامتداد لجهات خارجية)<br>Protocol Security (OWASP:A6:2017 – Security Misconfiguration & OWASP:A4:2017 XML External Entities) |
| 1-10 | 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. |

اختر التصنيف

| | |
|---|---|
| It shall be verified that the application accepts only a defined set of HTTP request methods, such as GET and POST, and that unused methods are explicitly blocked. | |
| التحقق من أن كل استجابة لبروتوكول نقل النص التشعبي (HTTP) تتضمن عنوان نوع محتوى يحدد مجموعة رموز آمنة (مثل "UTF-8").<br>It shall be verified that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8). | 2-10 |
| التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) و/أو الآليات الأخرى للمتصفحات الأقدم متضمنة من أجل الحماية من هجمات الخطف بالنقر ( Click Jacking).<br>It shall be verified that HTTP headers and/or other mechanisms for older browsers have been included to protect against click jacking attacks. | 3-10 |
| التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) في الطلبات والاستجابات تتضمن فقط رموز المدونة الموحدة الأمريكية لتبادل المعلومات القابلة للطباعة (ASCII).<br>It shall be verified that HTTP headers in both requests and responses contain only printable ASCII characters. | 4-10 |
| التحقق من استخدام صيغ بيانات أقل تعقيداً مثل جافا سكريبت (JSON)، وتجنب جعل المعلومات المحمية متسلسلة.<br>The use of less complex data formats, such as JSON, shall be verified, and serialization of protected data shall be avoided. | 5-10 |
| 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 1.2 أو إصدار أحدث.<br>All XML processors and libraries in use by the application or on the underlying operating system shall be patched or upgraded. Additionally, dependency checkers shall be used, and SOAP shall be updated to SOAP 1.2 or higher. | 6-10 |

| | |
|---|---|
| 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".<br>XML external entity and DTD processing shall be disabled in all XML parsers in the application, as per OWASP Cheat Sheet "XXE Prevention". | 7-10 |
| 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).<br>Positive server-side input validation (whitelisting), filtering, or sanitization shall be implemented to prevent hostile data within XML documents, headers, or nodes. | 8-10 |
| 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.<br>It shall be verified that XML or XSL file upload functionality validates incoming XML using XSD validation or similar. | 9-10 |
| 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.<br>SAST and DAST tools shall be used to help detect XXE in source code, although manual code review is the best alternative in large and complex applications with many integrations. | 10-10 |
| 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.<br>If the implementation of these controls is not possible, the use of virtual patching, API security gateways, or Web Application Firewalls (WAFs) shall be considered to detect, monitor, and block XXE attacks. | 11-10 |

اختر التصنيف

| الشفرة الخبيثة والثغرات (OWASP:A9:2017 - استخدام المكونات مع الثغرات المعروفة)<br>Malicious Code and Vulnerabilities (OWASP:A9:2017 – Using Components with Known Vulnerabilities) | 11 |
|---|---|
| التحقق من عدم وجود شفرات خبيثة في أي شفرة تم تطويرها أو تعديلها بهدف إنشاء التطبيق.<br>It shall be verified that no malicious code is in any code that was either developed or modified in order to create the application. | 1-11 |
| التأكد من أن سلامة الشفرة المفسرة والمكتبات والأوامر التنفيذية وملفات الإعدادات قد تم التحقق منها باستخدام المجموعات الاختبارية أو عمليات حساب ملخص النص المميز.<br>It shall be ensured that the integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes. | 2-11 |
| التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من الهوية أو تستخدمها لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code implementing or using authentication controls is not affected by any malicious code. | 3-11 |
| التحقق من أن كافة الشفرات التي تطبق إدارة الجلسات أو تستخدمها لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code implementing or using session management controls is not affected by any malicious code. | 4-11 |
| التحقق من أن كافة الشفرات التي تطبق ضوابط الوصول أو تستخدمها لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code implementing or using access controls is not affected by any malicious code. | 5-11 |
| التحقق من أن كافة ضوابط التحقق من المدخلات لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all input validation controls are not affected by any malicious code. | 6-11 |

| | |
|---|---|
| 7-11 | التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من المخرجات أو تستخدمها لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code implementing or using output validation controls is not affected by any malicious code. |
| 8-11 | التحقق من أن كافة الشفرات التي تطبق نموذج التشفير أو تستخدمه لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code supporting or using a cryptographic module is not affected by any malicious code. |
| 9-11 | التحقق من أن كافة الشفرات التي تطبق ضوابط التعامل مع الأخطاء وتسجيلها أو تستخدمها لم تتأثر بأي شفرات خبيثة.<br>It shall be verified that all code implementing or using error handling and logging controls is not affected by any malicious code. |
| 10-11 | التحقق من أن كافة الأنشطة الخبيثة قد خضعت لتقنية الحماية المعزولة (Sandboxing).<br>It shall be verified all malicious activity is adequately sandboxed. |
| 11-11 | التحقق من التخلص من المعلومات المحمية المخزنة في الذاكرة بسرعة عند عدم الحاجة لها.<br>It shall be verified that protected data is rapidly sanitized from memory as soon as it is no longer needed. |
| 12-11 | تحديث المكونات بأحدث التحديثات والإصلاحات عند معرفة المستخدم بالثغرات المنشورة.<br>Components shall be updated with the latest patches as soon as a user knows about published vulnerabilities. |
| 13-11 | إلغاء الاعتماديات غير المستخدمة والخصائص غير اللازمة والمكونات والملفات والوثائق.<br>Unused dependencies, unnecessary features, components, files, and documentation shall be removed. |
| 14-11 | عمل قائمة جرد مستمرة لإصدارات المكونات من طرف العميل والخادم (مثل أطر العمل والمكتبات) واعتمادياتها باستخدام أدوات مثل الإصدارات، |

اختر التصنيف

| | |
|---|---|
| | و"DependencyCheck"، 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.<br><br>Versions of both client-side and server-side components, (e.g., frameworks and libraries), and their dependencies shall be continuously inventoried using tools such as versions, DependencyCheck, retire.js, etc. Additionally, sources such as CVE and NVD, shall be continuously monitored for vulnerabilities in the components, and software composition analysis tools shall be used to automate the process. Subscription to email alerts for security vulnerabilities related to the used components shall be ensured as well. |
| 15-11 | الحصول على المكونات من مصادر رسمية وعبر روابط محمية فقط، وتفضيل الحزم الموقعة لتقليل فرص وجود مكون خبيث معدل.<br><br>Components shall be obtained from official sources and over secure links only. Signed packages shall be preferred to reduce the chance of including a modified, malicious component. |
| 16-11 | 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.<br><br>Libraries and components that are unmaintained or do not create security patches for older versions shall be monitored. If patching is not possible, deploying a virtual patch to monitor, detect, or protect against the discovered issue shall be considered. |
| 12 | قواعد العمل (Business Logic) |
| 1-12 | التحقق من عمليات التطبيق ومن كافة تدفقات قواعد العمل عالية القيمة في بيئة موثوقة مثل الخادم المحمي والمراقب. |

| | |
|---|---|
| Application processes and all high value business logic flows shall be verified in a trusted environment, such as on a protected and monitored server. | |
| 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.<br>It shall be verified that the application does not allow spoofed high value transactions, such as allowing Attacker User A to process a transaction as Victim User B, by tampering with or replaying session, transaction state, transaction or user IDs. | 2-12 |
| 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.<br>It shall be verified that the application does not allow high value business logic parameters to be tampered with, which include, but are not limited to, price, interest, discounts, PII, balances, stock IDs, etc. | 3-12 |
| 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.<br>It shall be verified that the application has defensive measures; such as verifiable and protected transaction logs, audit trails or system logs, and, in the highest value systems, real time monitoring of user activities and transactions for anomalies; to protect against repudiation attacks. | 4-12 |
| التحقق من أن التطبيق يوفر الحماية من هجمات الإفصاح عن المعلومات مثل مرجعيات الكائنات المباشرة، والتلاعب، واستخدام الهجمات التخمينية لاختراق الجلسة، وأنواع الهجمات الأخرى.<br>It shall be verified that the application protects against information disclosure attacks, such as direct object reference, tampering, session brute force or other attacks. | 5-12 |

| | |
|---|---|
| 6-12 | التحقق من وجود ضوابط كشف وضبط كافية في التطبيق للحماية من الهجمات التخمينية (مثل الاستخدام المستمر لدالة معينة) أو هجمات حجب الخدمة.<br>It shall be verified that the application has sufficient detection and governor controls to protect against brute force (such as the continuous use of a particular function) or denial of service attacks. |
| 7-12 | 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.<br>It shall be verified that the application has sufficient access controls to prevent elevation of privilege attacks. Such controls shall include preventing anonymous users from accessing secured data or secured functions, and preventing users from accessing each other's details or using privileged functions. |
| 8-12 | 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.<br>It shall be verified that the application processes business logic flows in sequential steps only, with all steps being processed directly. Additionally, the application shall be verified not to process out of order, skip steps, process steps from another user, or process transactions submitted quickly. |
| 9-12 | 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 لإنفاذ ضوابط مكافحة الاحتيال وفقاً لمخاطر التطبيق وعمليات الاحتيال السابقة.<br>It shall be verified that the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and/or segregation of duties for high value applications, to enforce anti-fraud controls as per the risk of application and past fraud. |

| | |
|---|---|
| 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.<br><br>It shall be verified that the application has business limits and enforces them in a trusted location (e.g., on a protected server) on a per user or per day basis, with configurable alerting and automated reactions to automated or unusual attack. | 10-12 |
| الملفات والمصادر (OWASP:A9:2017 - استخدام المكونات تحتوي ثغرات معروفة)<br><br>Files and Resources (OWASP:A9:2017 – Using Components with Known Vulnerabilities) | 13 |
| التحقق من أن إعادة التوجيه والإرسال في شريط العنوان (URL) لا تتضمن بيانات غير مصرحة.<br><br>It shall be verified that URL redirects and forwards do not include unvalidated data. | 1-13 |
| التحقق من توحيد أسماء الملفات وبيانات المسارات التي يتم الحصول عليها من مصادر غير موثوقة لإلغاء هجمات تجاوز المسار.<br><br>It shall be verified that filenames and path data obtained from untrusted sources are canonicalized to eliminate path traversal attacks. | 2-13 |
| التحقق من فحص الملفات التي يتم الحصول عليها من مصادر غير موثوقة من خلال برامج مكافحة الفيروسات لمنع تحميل برمجيات خبيثة معروفة.<br><br>It shall be verified that files obtained from untrusted sources are scanned by antivirus scanners to prevent the upload of known malicious content. | 3-13 |
| 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.<br><br>It shall be verified that parameters obtained from untrusted sources are not used in manipulating filenames, pathnames | 4-13 |

| | |
|---|---|
| or any file system object without first being canonicalized and input validated to prevent local file inclusion attacks. | |
| 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.<br>It shall be verified that parameters obtained from untrusted sources are canonicalized, input validated, and output encoded to prevent remote file inclusion attacks, particularly where input could be executed, such as header, source, or template inclusion. | 5-13 |
| التحقق من عدم السماح بإدراج محتوى عشوائي عن بعد عند مشاركة موارد "IFRAMEs" و"HTML 5" عبر النطاقات.<br>It shall be verified that sharing remote IFRAMEs and HTML 5 resources across domains does not allow the inclusion of arbitrary remote content. | 6-13 |
| التحقق من تخزين الملفات التي تم الحصول عليها من مصادر غير موثوقة خارج "Webroot".<br>It shall be verified that files obtained from untrusted sources are stored outside the webroot. | 7-13 |
| التحقق من إعداد وضبط خادم الويب أو التطبيق تلقائياً لحجب الوصول إلى المصادر البعيدة أو الأنظمة خارج خادم الويب أو التطبيق.<br>It shall be verified that web or application server is configured by default to deny access to remote resources or systems outside the web or application server. | 8-13 |
| التحقق من أن شفرة التطبيق لا تنفذ بيانات مرفوعة تم الحصول عليها من مصادر غير موثوقة.<br>It shall be verified the application code does not execute uploaded data obtained from untrusted sources. | 9-13 |

| | |
|---|---|
| 10-13 | 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.<br><br>It shall be verified that Flash, Silverlight or other Rich Internet Application (RIA) cross-domain resource sharing configuration is set to prevent unauthenticated or unauthorized remote access. |
| 11-13 | التحقق من أن كافة أنواع الملفات المسموح برفعها مقتصرة على غايات العمل وحسب الحاجة (مثل ملفات "PDF" ومستندات برامج "Office").<br>It shall be verified that file types allowed for upload are limited to business purpose and needs only (e.g., PDF and office documents). |
| 12-13 | التأكد من أن التحقق من نوع الملف يتم من خلال التحقق من عناوين الملفات وليس من خلال اسم امتداد الملفات فقط.<br>It shall be verified that file type validation is performed not only by checking file headers but also by checking file extension names. |
| 13-13 | التحقق من عدم تفعيل امتيازات وصلاحيات التنفيذ في أدلة تحميل الملفات.<br>It shall be verified that execution privileges are turned off on file upload directories. |
| 14-13 | التحقق من ضبط إعدادات ملفات ومصادر التطبيق تلقائياً على وضعية القراءة فقط.<br>It shall be verified that application files and resources are read-only by default. |
| 15-13 | التحقق من إلغاء كافة أنواع المشاركات والمشاركات الإدارية غير اللازمة، وتقييد الوصول إلى المشاركات أو جعله يتطلب التحقق من الهوية.<br>It shall be verified that all unnecessary shares and administrative shares are removed, and that access to required shares is either restricted or requires authentication. |
| 16-13 | طلب التحقق من الهوية قبل السماح برفع الملفات. |

| | |
|---|---|
| Authentication shall be required before allowing a file to be uploaded. | |
| وضع حد على حجم الملفات التي يمكن رفعها والذي يجب ألا يتجاوز الحجم المطلوب لغايات العمل (على سبيل المثال، 1 ميغابايت كحد أعلى)، وإضافة ملاحظة على صفحة الويب تخص أحجام الملفات المقبولة.<br>Size of files that can be uploaded shall be limited to the size that is needed for business purposes only (for example, maximum 1 MB), and a note shall be added on the web page for the accepted file sizes. | 17-13 |
| التحقّق من الهاتف المحمول (Mobile Verification) | 14 |
| التأكد من تحقق العميل من شهادات تشفير طبقة المنافذ الآمنة (SSL).<br>It shall be verified that the client validates SSL certificates. | 1-14 |
| التحقق من عدم استخدام قيم رقم تعريف الجهاز المميز (UDID) كضوابط أمنية.<br>It shall be verified that Unique Device ID (UDID) values are not used as security controls. | 2-14 |
| التحقق من أن تطبيق الهاتف المحمول لا يخزن المعلومات المحمية على المصادر المشتركة على الجهاز (مثل بطاقة "SD" أو المجلدات المشتركة).<br>It shall be verified that the mobile application does not store protected data on shared resources on a device (for example, on SD card or shared folders). | 3-14 |
| التحقق من أن المعلومات المحمية ليست مخزنة في قاعدة بيانات "SQLite" على الجهاز.<br>It shall be verified that protected data is not stored on SQLite database on the device. | 4-14 |
| التحقق من أن المفاتيح السرية وكلمات المرور ليست مثبتة في الشفرة في البرامج التنفيذية.<br>It shall be verified that secret keys or passwords are not hard coded in the executable. | 5-14 |

| | |
|---|---|
| 6-14 | التحقق من أن تطبيق الهاتف المحمول يمنع تسرب المعلومات المحمية عن طريق خاصية التصوير التلقائي في نظام تشغيل "iOS".<br>It shall be verified that the mobile application prevents the leakage of protected data via iOS autosnapshot feature. |
| 7-14 | التحقق من أن التطبيق لا يمكن تشغيله على جهاز تم إلغاء القيود الموجودة عليه (Jailbroken) أو جهاز يتمتع بصلاحيات ومزايا هامة وحساسة (Rooted).<br>It shall be verified that the application cannot be run on a jailbroken or rooted device. |
| 8-14 | التحقق من أن وقت انتهاء الجلسة له قيمة منطقية.<br>It shall be verified that the session timeout is of a reasonable value. |
| 9-14 | التحقق من التصاريح التي يتم طلبها ومن المصادر التي يتم منح تصاريح الوصول إليها (AndroidManifest.xml، وiOS Entitlements).<br>Requested permissions, as well as the resources authorized to be accessed (i.e., AndroidManifest.xml, iOS Entitlements), shall be verified. |
| 10-14 | التحقق من أن سجلات انهيار النظام لا تتضمن معلومات محمية.<br>It shall be verified that crash logs do not contain protected data. |
| 11-14 | التحقق من عدم وضوح النظام الثنائي في التطبيق.<br>It shall be verified that the application binary has been obfuscated. |
| 12-14 | التحقق من أن كافة بيانات الاختبار قد تم إزالتها من حاوية التطبيق ( .apk .bar .ipa).<br>It shall be verified that all test data has been removed from the application container (.ipa .apk .bar). |
| 13-14 | التحقق من أن التطبيق لا يقوم بتسجيل المعلومات المحمية على سجل النظام أو ملفات النظام.<br>It shall be verified that the application does not log protected data to the system log or filesystem. |

اختر التصنيف

| | |
|---|---|
| 14-14 | التحقق من أن التطبيق لا يتيح الإكمال التلقائي للنصوص الحساسة في حقول المدخلات مثل حقول كلمات المرور أو المعلومات الشخصية أو بطاقات الائتمان.<br>It shall be verified that the application does not enable autocomplete for sensitive text input fields, such as password, personal information or credit card fields. |
| 15-14 | التحقق من أن تطبيق الهاتف المحمول يطبق عملية تثبيت الشهادات ( Certificate Pinning) لمنع إدارة حركة البيانات في التطبيق بالوكالة.<br>It shall be verified that the mobile application implements certificate pinning to prevent the proxying of application traffic. |
| 16-14 | التحقق من عدم وجود إعدادات خاطئة في ملفات الإعدادات (مجموعة العلامات التصحيحية، وتصاريح قابلة للقراءة وللكتابة العالمية).<br>It shall be verified that no misconfigurations are present in the configuration files (Debugging flags set, world readable/writable permissions). |
| 17-14 | التحقق من تحديث مكتبات الأطراف الخارجية قيد الاستخدام وعدم احتوائها على أي ثغرات معروفة.<br>It shall be verified that all third party libraries in use are up to date, and contain no known vulnerabilities. |
| 18-14 | التحقق من عدم تخزين بيانات الويب مثل حركة بيانات بروتوكول نقل النص التشعبي الآمن (HTTPS).<br>It shall be verified that web data, such as HTTPS traffic, is not cached. |
| 19-14 | 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).<br>It shall be verified that the query string is not used for protected data. Instead, a POST request via SSL shall be used with a CSRF token. |
| 20-14 | التحقق، إن أمكن، من أن أرقام الحسابات الشخصية متقطعة قبل تخزينها على الجهاز. |

| | |
|---|---|
| It shall be verified that, if applicable, any personal account numbers are truncated prior to storing them on a device. | |
| التحقق من أن التطبيق يستفيد من خاصية التوزيع العشوائي لمخطط مساحات العناوين (ASLR).<br>It shall be verified that the application makes use of Address Space Layout Randomization (ASLR). | 21-14 |
| التحقق من أن البيانات المسجلة عن طريق لوحة المفاتيح (iOS) لا تتضمن بيانات اعتماد أو معلومات مالية أو معلومات محمية أخرى.<br>It shall be verified that data logged via the keyboard (iOS) does not contain credentials, financial information or other protected data. | 22-14 |
| في تطبيقات الأندرويد، التحقق من أن التطبيق لا ينشئ ملفات بتصاريح " MODE_WORLD_READABLE " أو " MODE_WORLD_WRITABLE ".<br>For Android applications, it shall be verified that the application does not create files with permissions of MODE_WORLD_READABLE or MODE_WORLD_WRITABLE. | 23-14 |
| التحقق من تخزين المعلومات المحمية بطريقة مشفرة وآمنة (حتى عند تخزينها في سلسلة مفاتيح "iOS").<br>It shall be verified that protected data is stored in a cryptographically secure manner (even when stored on iOS keychain). | 24-14 |
| التحقق من تطبيق آليات مكافحة التصحيح والهندسة العكسية في التطبيق.<br>It shall be verified that anti-debugging and reverse engineering mechanisms are implemented in the application. | 25-14 |
| التحقق من أن التطبيق لا يستورد أنشطة حساسة أو مزودي محتوى أو غيرهم على الأندرويد.<br>It shall be verified that the application does not export sensitive activities, intents, content providers, etc. on Android. | 26-14 |

| | |
|---|---|
| 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).<br>It shall be verified that mutable structures have been used for sensitive strings such as account numbers and are overwritten when not used, (to mitigate damage from memory analysis attacks). | 27-14 |
| التأكد من تنفيذ التحقق الكامل من البيانات على المدخلات لأي رسائل أنشطة ومزودي محتوى ومتلقي بث معرضين للمخاطر (الأندرويد).<br>It shall be verified that any exposed intents, content providers and broadcast receivers perform full data validation on input (Android). | 28-14 |
| أمن قواعد البيانات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة)<br>Database Security (OWASP:A6:2017 – Security Misconfiguration) | 15 |
| التحقق من استخدام الاستفسارات المضبوطة بمعايير لمنع حقن تعليمات الاستعلام البنيوية (SQL Injection).<br>It shall be verified that parameterized queries are used to prevent SQL Injection. | 1-15 |
| التحقق من استخدام بيانات اعتماد معقدة وآمنة للوصول إلى قواعد البيانات.<br>It shall be verified that strong and secure credentials are used for database access. | 2-15 |
| التحقق من أن التطبيق الذي يصل إلى قواعد البيانات يمتلك أدنى مستوى ممكن من الامتيازات والصلاحيات المطلوبة.<br>It shall be verified that the application accessing the database uses the lowest possible level of privileges required. | 3-15 |
| التحقق من أن سلاسل الحروف العشوائية (Strings) للاتصال ليست مثبتة في الشفرة ضمن التطبيق، خصوصاً بيانات اعتماد التحقق من الهوية من قاعدة البيانات.<br>It shall be verified that connection strings are not hard coded within the application, especially database authentication credentials. | 4-15 |

اختر التصنيف

| | |
|---|---|
| 5-15 | التحقق من إغلاق الاتصال بقاعدة البيانات بأسرع ما يمكن.<br>It shall be verified that the connection to the database is closed as soon as possible. |
| 6-15 | 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.<br>It shall be verified that all unnecessary and unused database functionalities, including default vendor content, have been turned off or disabled. Only the minimum set of features and options required for the application to function shall be installed. For example, unnecessary stored procedures or services and utility packages, shall be disabled. |
| 7-15 | التحقق من إلغاء تفعيل أي حسابات تلقائية أو غير ضرورية والتي يمكن من خلالها الوصول إلى قواعد البيانات غير اللازمة لدعم متطلبات الأعمال.<br>It shall be verified that any default or unnecessary accounts with access to databases that are not required to support business requirements are disabled. |
| 8-15 | التحقق من أن التطبيق يستخدم بيانات اعتماد مختلفة لكل ميزة وصلاحية (مثل مستخدم، ومستخدم للقراءة فقط، وضيف، ومشرفين) عند اتصاله بقاعدة البيانات.<br>It shall be verified that the application connects to the database with different credentials for every trust distinction and accountability (for example, user, read-only user, guest, administrators). |
| 9-15 | التحقق من إلغاء تفعيل تسجيل الدخول عن بعد والجلسات المجهولة إذا لم يكن هناك حاجة إليها.<br>It shall be verified that remote logons and null sessions are disabled if not needed. |
| 10-15 | بالنسبة للتطبيقات التي تعتمد على قاعدة بيانات، يجب استخدام قوالب الإعداد والتحصين الموحدة، واختبار جميع الأنظمة التي تعتبر جزءاً من إجراءات العمل الحساسة. |

| | |
|---|---|
| For applications that rely on a database, standard hardening configuration templates shall be used, and all systems that are part of critical business processes shall be tested. | |

## الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

## الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذا المعيار باستمرار.

2- يجب على <إدارة تقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني> في <اسم الجهة> الالتزام بهذا المعيار.

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