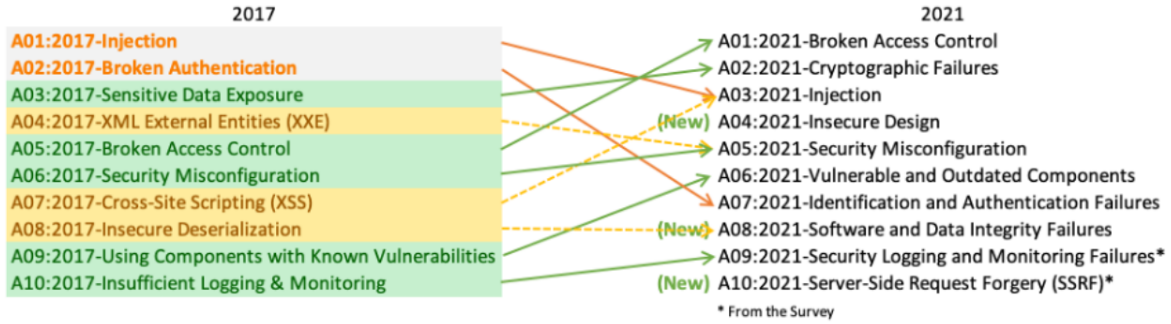
# OWASP Top Ten

## Top 10 Web Application Security Risks

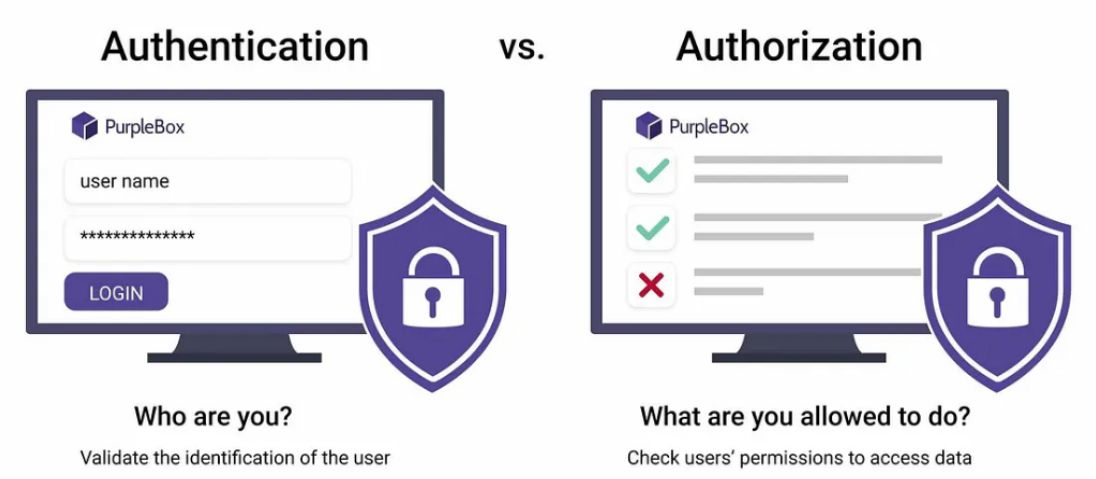
There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.




1. **Broken Access Control**

   (التحكم في الوصول)

   في البداية عليك التفريق بين:




Authentication:

المصادقة هي عملية التحقق من هوية المستخدم(يوزرنيم و باسوورد)

Authorization:

بينما التخويل هو عملية التحقق من ما الذي لديهم صلاحية الوصول إليه(يوزر عادي أو ادمن)

اذا مشكله التحكم في الوصول تعني انه المخترق يحاول اخذ صلاحيات اكثر مما لديه مثل ان يأخذ صلاحيات الادمن , وممكن أن تكون نوعان :أفقي اي ان يأخذ صلاحيات يوزر بنفس درجته, أو عمودي أي يأخذ صلاحيات يوزر أكبر من درجته

2. **Cryptographic Failures**

فشل التشفير هو المجال الذي يستهدف فيه المهاجمون بشكل شائع البيانات الحساسة مثل كلمات المرور وأرقام بطاقات الائتمان والمعلومات الشخصية، عندما لا تحميها بشكل صحيح. وهذا هو السبب الجذري لتعرض البيانات الحساسة للمخاطر.

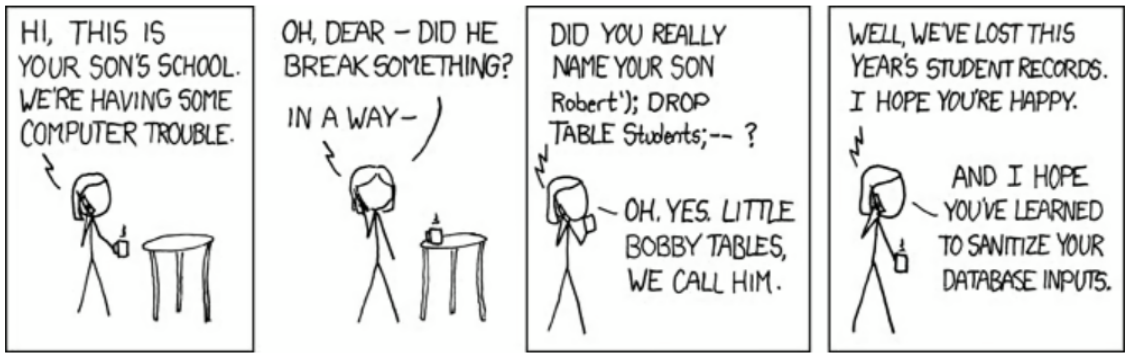
3. **Injection**

الحقن, هو محاولة من قبل المهاجم لإرسال بيانات إلى تطبيق بطريقة من شأنها تغيير معنى الأوامر

أنواعه:

**SQL injection attacks**

هجمات حقن SQL
تتضمن إدخال رمز خبيث في الاوامر من خلال إدخال المستخدم، ثم يتم تنفيذه من قبل خادم قاعدة بيانات التطبيق الخلفي. يمكن أن تؤدي استغلالات الحقن الناجحة إلى فقدان بيانات هائل واضطراب حيث يحصل المهاجم على الوصول إلى قاعدة البيانات ويتلاعب بها مثل قراءة وتعديل الجداول



https://tryhackme.com/room/sqlilab

**Cross-site scripting attacks**

ثغرات Cross-site scripting (XSS)
تشكل تهديدًا خطيرًا لتطبيقات الويب لأنها تتيح للمهاجمين حقن نصوص خبيثة في مواقع الويب  وخداع المستخدمين غير المشبوهين لتنفيذها. يمكن أن يؤدي ذلك إلى سرقة البيانات الحساسة، مثل بيانات تسجيل الدخول أو المعلومات المالية، أو حتى السيطرة الكاملة على جلسة الويب للضحية. في بعض الحالات، يمكن أن تفتح هذه الهجمات الباب أمام أنواع أخرى من الهجمات، مثل توزيع البرمجيات الخبيثة أو استغلال الثغرات الأخرى في تطبيق الويب.

**XML external entity (XXE)**

حقن الكيان الخارجي في XML (المعروفة أيضًا باسم XXE)
هي ثغرة أمنية على الويب تتيح للمهاجم التدخل في معالجة التطبيق للبيانات XML. غالبًا ما تتيح للمهاجم عرض الملفات على نظام ملفات خادم التطبيق، والتفاعل مع أي أنظمة خلفية أو خارجية يمكن للتطبيق الوصول إليها.

في بعض الحالات، يمكن للمهاجم تصعيد هجوم XXE لاختراق الخادم الأساسي أو البنية التحتية الخلفية الأخرى، من خلال استغلال ثغرة XXE لتنفيذ هجمات التزوير على الخادم الجانبي (SSRF).

4. **Insecure Design**

الضعف في التصميم غير الآمن يشمل مجموعة واسعة من النقاط الضعيفة ويصف الضوابط التصميمية المفقودة أو غير الفعّالة. عندما يحاول الشخص فهم معناه، فإنه من الأساسي فهم الحقيقة التي تقول إن التصميم غير الآمن يختلف كثيرًا عن التنفيذ غير الآمن

يمكن لتصميم آمن أن يتضمن حوادث تنفيذ غير آمنة. بالمثل، يمكن أن يؤدي تنفيذ آمن إلى ثغرات لأن التصميم لم يكن آمنًا أو خاليًا من العيوب.

5. **Security Misconfiguration**

تعد التهيئة الأمنية غير الصحيحة ثغرة تحدث عندما يتم تجاهل ممارسات الأمان الأفضل، مما يتيح للمهاجمين الوصول إلى النظام باستخدام الثغرات.

6. **Vulnerable and Outdated Components**

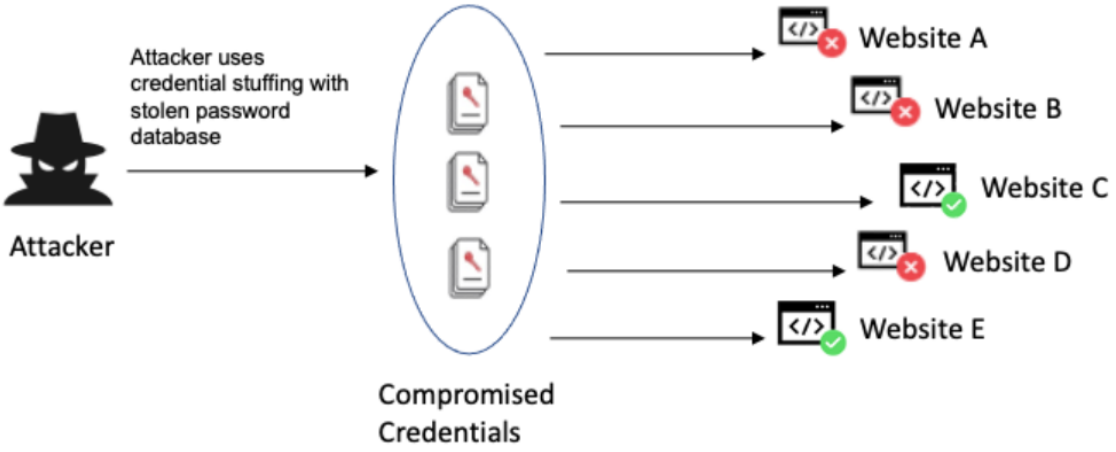
   المكونات الضعيفة والقديمة تشير إلى المكتبات أو الإطارات من الأطراف الثالثة المستخدمة في تطبيقات الويب التي تحتوي على ثغرات معروفة أو لم يعد يتم دعمها من قبل مطوريها. يمكن استغلال هذه المكونات من قبل المهاجمين للحصول على وصول غير مصرح به إلى البيانات الحساسة أو للسيطرة على النظام.

7. **Identification and authentication failures**

   فشل التعرف والمصادقة يمكن أن يحدث عندما لا تُنفذ وظائف تتعلق بهوية المستخدم، أو المصادقة، أو إدارة الجلسة بشكل صحيح أو لا تُحمى بشكل كافٍ من قبل التطبيق. يمكن للمهاجمين استغلال فشل التعرف والمصادقة عن طريق الاستيلاء على كلمات المرور، أو المفاتيح، أو رموز الجلسة، أو استغلال عيوب التنفيذ الأخرى ليتولى هويات مستخدمين آخرين، إما بشكل مؤقت أو دائم.

   امثلة:

   - Brute force/credential stuffing
   - Session hijacking
   - Session fixation
   - Cross-Site Request Forgery (CSRF)
   - Execution After Redirect (EAR)
   - One-click attack



8. **software and data integrity failures**

   فشل السلامة والنزاهة في البرمجيات والبيانات يحدث عندما يتمكن المهاجم من تعديل أو حذف البيانات بطريقة غير مصرح بها. يمكن أن يحدث هذا بسبب الثغرات في البرمجيات أو الممارسات البرمجية الضعيفة. يمكن للمهاجمين استغلال هذه الثغرات للوصول إلى معلومات حساسة أو لتسبب الضرر في النظام.

9. **Security Logging and Monitoring Failures**

   فشل التسجيل والمراقبة الأمنية ليس لديه ثغرات مباشرة يمكن استغلالها، ولكن هذا لا يعني أن التسجيل والمراقبة أقل أهمية بأي شكل من الأشكال.

   قد تؤثر التسجيل والمراقبة غير الكافية للأنظمة على الرؤية، والإنذار بالحوادث، وفشل تسجيل الدخول، وفشل الأنظمة، وانتهاكات الأمان. وهذا يجعل من الضروري أن يكون لديك نظام تسجيل ومراقبة مشغل بالكامل لجمع السجلات وإصدار التنبيهات لموظفي مركز عمليات الأمان
   (SOC)
   والمسؤولين. كما أنه من المهم أيضًا إجراء فحوصات بشكل منتظم لضمان تسجيل جميع الأنظمة الصحيحة كما هو متوقع — فلا تريد أن تفتقد السجلات القيمة من جدار الحماية الخاص بك.

10. **Server-Side Request Forgery (SSRF)**

    هو نوع من الهجمات السيبرانية حيث يستفيد المهاجم الماهر من الثغرة الموجودة مسبقًا على الخادم ويستخدمها ضد الخادم. اعتمادًا على نية المهاجم، يستخدم المهاجم SSRF لتعديل بيانات الخادم الحرجة للمهمة (المخزنة أو المارة) عن طريق إدخال رمز/رابط معطوب.