Misconfiguration و Information Disclosure

الهجمات السيبرانية من أخطر التهديدات التي تواجه الأنظمة الحديثة، وتتنوع طرق المهاجمين في استغلال الثغرات الأمنية للوصول إلى البيانات أو تعطيل الخدمات. ومن بين هذه الثغرات **إفشاء المعلومات (Information Disclosure)** و **سوء التهيئة(Misconfiguration)** ، حيث تمثلان أحد أبرز العوامل التي تساهم في اختراق الأنظمة بشكل غير مباشر نتيجة إهمال أو ضعف في إعدادات الأمان.

أولا : إفشاء المعلومات Information Disclosure

هو حدوث تسريب أو كشف غير مقصود للمعلومات الحساسة أو البيانات السرية نتيجة خطأ في تصميم النظام أو في تكوينه.

أمثلة :

١. **رسائل الخطأ التفصيلية** :ظهور تفاصيل قاعدة البيانات أو إصدار السيرفر عند حدوث خطأ.

٢. **ملفات النسخ الاحتياطية** :وجود ملفات مثل backup.zipأو config.old يمكن الوصول إليها.

٣. **إعدادات السيرفر المكشوفة** :مثل ملفات /.git أو.env التي تحتوي على كلمات مرور.

٤. **الكشف عن المسارات الداخلية** :ظهور مسار النظام (C:\xampp\htdocs...) في رسائل الخطأ.

المخاطر:

- تمكين المهاجم من فهم بنية النظام الداخلية.
- تسهيل تنفيذ هجمات أخرى مثل SQL Injection أوLFI
- سرقة بيانات حساسة ككلمات مرور أو مفاتيحAPI

ثانيا: سوء التهيئة Misconfiguration

يقصد به ضعف أو خطأ في إعدادات النظام أو الخدمات أو الشبكات، يؤدي إلى فتح ثغرات أمنية يمكن استغلالها.

أمثلة شائعة:

١. **استخدام بيانات دخول افتراضية** (admin:admin)

٢. **عدم تعطيل Directory Listing** مما يسمح برؤية محتويات المجلدات.

٣. **السماح بالوصول لملفات التكوين** مثل config.phpأو web.config

٤. **عدم تفعيل HTTPS** والاكتفاء بـHTTP.

٥. **صلاحيات زائدة للمستخدمين** مثال: منح مستخدم عادي صلاحيات مسؤول

المخاطر:

- منح المهاجم وصولًا غير مصرح به إلى الموارد.
- إمكانية استغلال الثغرات لتسريب بيانات حساسة.
- تعطيل الخدمات أو تغيير إعدادات الخادم.

العلاقة بين Information Disclosure وMisconfiguration

- غالبًا ما يؤدي **سوء التهيئة** إلى **إفشاء المعلومات**.
- مثال: ترك Directory Listing مفعلًا ← يمكن للمهاجم رؤية ملفات حساسة.
- بالتالي فالعلاقتان تكاملية Misconfiguration :سبب، و Information Disclosure نتيجة.

أساليب الوقاية

١. **تفعيل وضع الإنتاج (Production Mode)** بدلًا من وضع التطوير.

٢. **إخفاء رسائل الخطأ** وعرض رسائل عامة فقط للمستخدم النهائي.

٣. **منع الوصول لملفات التكوين** عبر إعدادات السيرفر.(Apache/Nginx)

٤. **تعطيل Directory Listing.**

٥. **استخدام جدران نارية (WAF) للكشف عن الطلبات المشبوهة.**

٦. **إجراء اختبارات اختراق دورية** باستخدام أدوات مثل .**Burp Suite, OWASP ZAP**

أمثلة واقعية

- تسريب بيانات موقع شهير بسبب وجود ملف env.يحتوي على بيانات قاعدة البيانات.
- خطأ تكوين في S3 Bucket لشركة عالمية أدى إلى كشف ملايين السجلات للعامة.
- Misconfigured Elasticsearchسماح بالوصول غير المصرح به إلى بيانات حساسة.