الفصل الرابع و العشرين (والأخير)
تلخيص لثغرات تطبيقات الويب

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

تلخيص لثغرات تطبيقات الويب

اسم الثغرة	مكان وجودها	كيفية اكتشافها
XSS	فى اى inputs موجودة داخل صفحة ال HTML سواء كانت تتعامل مع ال DB او لا	تجربة Payloads كثيرة فى جميع ال inputs لمعرفة من هو مصاب او لا
SQLI	فى اى Inputs او Parameters تتعامل مع ال DB فقط و هذا على حسب فهمك لل inputs, parameters على انها تتعامل مع ال DB او لا	اضافة ' لل input او parameter المصاب لاكتشاف SQLI Error Based او اضافة جملة True/False لاكتشاف SQLI Blind Based
CSRF	فى حالة عدم وجود CSRF Token فى ال HTTP Headers	انشئ Form بقيم جديدة و محاولة اقناع الهدف بالضغط عليها (بالهندسة الاجتماعية)
RCE	فى اى Inputs او Parameters لا تتعامل مع ال DB و يكون نظام التشغيل Linux	تجربة Payloads كثيرة
SSRF	فى اى Inputs او Parameters لا تتعامل مع ال DB و يكون نظام التشغيل Linux	تجربة Payloads كثيرة
XPath Injection	فى اى Inputs او Parameters تتعامل مع ملفات من نوع XML فقط	تجربة Payloads كثيرة

تلخيص لثغرات تطبيقات الويب (تكمله...)

اسم الثغرة	مكان وجودها	كيفية اكتشافها
XXE	فى اى Inputs او Parameters تتعامل مع ملفات من نوع XML فقط	تجربة Payloads كثيرة
Open/URL Redirect	فى اى Parameters تقوم بتحويل الصفحة الحالية لصفحة اخرى او لموقع اخر	اختبار هذا parameter المصاب بصفحة جديدة هل سيحولنى لها ام لا
LFI/RFI	فى اى Parameters تقوم بتحويل الصفحة الحالية لصفحة اخرى داخلية او لصفحة اخرى من موقع خارجى	اختبار هذا parameter المصاب بصفحة داخلية اخرى او بصفحة من موقع اخر خارجى هل سيحولنى لها ام لا
Path Traversal	فى اى Parameters تتعامل مع ملفات الموقع الداخلية و يكون نظام التشغيل Linux	تجربة ../../.../../etc/passwd
Insecure Deserialization	فى اى inputs او parameters يتم عمل Deserialization لها و هى فى المواقع المكتوبة بال Java	تجربة Payloads كثيرة
CORS	فى HTTP Response Headers	اختبار access-control-allow-origin و اختبار access-control-allow-credentials

تلخيص لثغرات تطبيقات الويب (تكمله...)

اسم الثغرة	مكان وجودها	كيفية اكتشافها
Click Jacking	فى HTTP Response Headers	اختبار X-frame-options
Session Hijacking	فى HTTP Request Headers	اختبار ال Session هل هى ثابتة لا تتغير او غير مشفرة أو يمكن تخمينها
Rate Limit (DoS attack)	فى اى inputs او parameters يحب ان يكون له limit مثل login و reset و password و كمان على حسب فهمك للموقع اية اللى هيسبب Brute Force او DoS attacks او لا	التجربة عدة مرات فى هذه inputs و parameters حتى تعرف وجود الثغرة من عدمها
IDOR	على حسب فهمك للموقع فهى ثغرة منطقية و لسيت تقنية مثل باقى الثغرات	التغيير فى قيم parameters الحساسة زى parameter خاص بال user-id و محاولة تغييره ب user-id اخر و غير ذلك من السيناريوهات
Subdomain Takeover	فى CNAME الخاص بالموقع	التأكد ان CNAME موجود و منتهى الصلاحية و انك تقدر تشترية من جديد
JWT	فى ال HTTP Request Headers	اختبار Authorization Bearer

تلخيص لثغرات تطبيقات الويب (تكمله...)

اسم الثغرة	مكان وجودها	كيفية اكتشافها
HTTP Splitting	فى HTTP Response Headers	اختبار ال HTTP Response Headers هل فيهم header بيحتوى على URL الصفحة المطلوبة بالتحديد
Authentication	فى صفحات الدخول Login	تخمين ال UserName و اختبار الرسائل التى تظهر

تم بحمد الله انتهاء الفصل الأخير
دمتم في أمان الله