الفصل الرابع عشر
نصائح عند اختبار تطبيقات الويب

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

نصائح عند اختبار تطبيقات الويب

1- مرحلة ال Information Gathering

- فهم تطبيق الويب و طريقة عمله و الغرض منه جيداااااااا
- جمع المعلومات مثلا اية اللغة المستخدمة، معرفة كل الصفحات اللى شغالة فى التطبيق. بعض الادوات المهمة لذلك Wapplayzer – Dirsearch – check index source code
- حاول تفهم نوعية المستخدمين فى التطبيق و انشئ 2 User من كل نوع

2- مرحلة ال Scanning

- لازم تكون عارف ان الثغرات موجودة فى ال inputs و ال Parameters المتغيرة لذلك عليك اولا بجمع الصفحات التى تحتوى على inputs و parameters و ذلك باستخدام web crawler زى ده (https://dataminer.io/) و (Chrome Extension Scraper) ثانيا بما ان لكل ثغرة payloads مختلفة عن الثغرات الاخرى فلذلك (اشتغل بذكاء و ليس بجهد كبير) معنى ذلك اشتغل على الثغرات اللى مش ممكن يشتغل عليها ال Scanners مثل BurpSuite و غيره ألا و هى الثغرات المنطقية مثل ثغرات Authentication – Authorization – Access Control لان بطبيعة الحال ال Scanners ما هى الا أداة و ليست عنصرى بشرى يفكر و يفهم

نصائح عند اختبار تطبيقات الويب (تكمله...)

- فلذلك استخدام ال pluginsالموجودة فى BurpSuite لاختبار ال inputs و ال parameters من الثغرات التقنية مثل SQLI – XSS – Path Traversal – Open Redirect و غيرها من الثغرات اللى بتستخدم Payloads لاختبارها

3- مرحلة ال Exploitation

- فى حالة اكتشافك لثغرة معينة قم بمحاولة استغلالها بطريقة لا تضر الموقع ليكون لديك دليل كافى على وجود الثغرة

4- مرحلة ال Reporting

- دائما قم بكتابة و حفظ كل ما تجده فسوف تحتاجة

- ملحوظات هاااااامة:

- ليس عليك بأن تبدأ بإختبار المواقع الكبيرة مثلا على المنصات المشهورة زى – HackerOne BugCrowd و غيرها و لكن عليك اولا اختبار المواقع العامة على Google ثم عليك بالتدوير على مواقع تعرض Bug Bounty من على Google ثم بعد اتقان تام لجميع الثغرات المذكورة مسبقا عليك الدخول على منصات HackerOne و غيرها للمنافسة مع كثير من مختبرى الاختراق المحترفين.
- لا نتشغل بكم تستغرق من الوقت فى اكتشاف الثغرات فمن الممكن ان تستغرق فى اكتشاف ثغرة واحدة او بعض الثغرات اسبوع او شهر او شهرين او سنة فليس لها وقت محدد كل ما عليك هو اختبار كل inputs و parameters من الثغرات سواء كانت ثغرات منطقية او تقنية (التى تحتاج Payloads)

تم بحمد الله انتهاء الفصل الرابع عشر