طريقتي في عمل إختبار إختراق ل WEB APPLICATION

EBRAHEM HEGAZY

WHAT IS THIS VIDEO ABOUT, AND WHAT IT IS NOT

الفيديو ده الغرض منه شرح طريقتي في عمل اختبار اختراق لويب أبلكيشن من ناحية ازاي بنظم شغلي وبركز علي ايه وبفكر ازاي لما اشوف صفحة معينه او برامتر معين

الفيديو ده مش لشرح نوع معين من الثغرات ولا لشرح طريقة البج هانتنج ولا خاص باكتشاف الثغرات اصلا. يتم شرح درس منفصل لكل نوع من الثغرات

لو في شئ مش واضح GOOGLE IS YOUR FRIEND

TESTING WEBSITE

- http://testphp.vulnweb.com/

أشهر الأسئلة

ازاي اعرف ان الأبلكيشن الفلاني مصاب بالثغرة الفلانية

ازاي اعرف انه البرامتر ده مصاب او لا وازاي اعرف مصاب بانهي ثغرة

ايه الفرق بين الريكون وال information gathering

أزاي لما اشوف صفحة معينة ابقي عارف اني لازم اجرب عليها الثغرة الفلانية؟

أعمل ايه لما احس اني مشتت؟

امتي اقول كفاية كدة علي الأبلكيشن ده؟

METHODOLOGY

WORK SMART NOT HARD

1) SCOPING AND INFORMATION GATHERING
   - إفهم الأبلكيشن وطريقة عملة والغرض منه
   - جمع المعلومات(WAPPALYZER, DIRSEARCH, INDEX SOURCE CODE, GITHUB)
   - حاول تفهم نوعية المستخدمين في الموقع وانشئ اتنين يوزر من كل نوع مستخدم

2) SCANNING
- ركز علي ثغرة واحدة, الا لو لقيت حاجة واضح جدا انها مصاب
- شخصيا بركز فقط علي ال LOGICAL & ACCESS CONTROL VULNERABILITIES
- شغل البرب سكانر واشتغل انت بشكل يدوي
- دايما خلي عندك خطوات واضحة لإيه اللي محتاج تعمله تست في الويب أبلكيشن وأنواع الثغرات اللي هتدور عليها

3) EXPLOITATION
- في حالة إكتشافك لثغرة معينة, قم بمحاولة إستغلالها بطريقة لا تضر بالموقع, ليكون لديك دليل كافي علي وجود الثغرة

4) REPORTING

دائما قم بحفظ وكتابة كل ما تجده فسوف تحتاجة

Before we start

- OneNote
- AutoHotKey (Demo?)
- Burp plugins (J2EEScan, Upload tester)

تطبيق عملي

REFERENCES

HackerOne Hacktivity
https://hackerone.com/hacktivity

Bug Bounty Cheat Sheet
https://github.com/EdOverflow/bugbounty-cheatsheet

Awesome Bug Bounty List
https://github.com/djadmin/awesome-bug-bounty

Bug Bounty Reference
https://github.com/ngalongc/bug-bounty-reference

Payload all the things
https://github.com/swisskyrepo/PayloadsAllTheThings/