ملخص اللقاء الأول – Bug Bounty and Penetration Testing

تنويه:

إن هذا الملف وضع لتسهيل عملية وصولك لمرفقات اللقاء ولن يغنيك عن المحتوى الوارد فيه.

هذا اللقاء سيكون كل يوم أحد عند الساعة السابعة والنصف مساءً وقد يتم تحديث المواعيد دوريًا لذلك عليك متابعتنا على الديسكورد.

https://twitter.com/MAlajab/status/1287489064069992449?s=20

في البداية حتى تستطيع الانضمام لمكتشفي الثغرات يجب أن يكون لديك خلفية في المجال أو المسار الذي تميل إليه.

نصائح عامة لك ك صائد ثغرات Bug bounty hunter أو مختبر اختراق penetration tester :

1- **التركيز بالشكل الصحيح على مسارك التعليمي وعدم التشتت.**
2- **أخذ المعلومة من مصدرها الأساسي ولابد أن تكون جودتها عالية وموثوقة.**
3- **يجب التروي في البحث وتجنب الطرق المختصرة حتى يظهر التقرير الذي تعده بشكل جيد. والأهم من ذلك حتى تكون أنت ملم بجميع ماحصل خلال البحث (أنصحك بمتابعة هذه الدورة كمقدمة) https://youtu.be/BjfCWSFmIFI**
4- **إذا كان لديك خبرة في مجال معين مثلا تطوير المواقع أو التطبيقات فأستمر في هذا المسار لأنك سوف تكون متميز ومتمكن أكثر من غيرك في نفس مجالك.**
5- **فيما يخص مرحلة بحثك عن الثغرات إذا كنت تواجه مشكلة عدم قبول التقرير بسبب التكرار (duplicated) انصحك بالبحث في توقيت بداية نزول القوائم (مثلا Hakerone يتم عرض برامج جديدة في أول أسبوع من بداية كل شهر).**
6- **في اصطياد الثغرات (Bug Bounty) تحتاج فقط إلى إثبات ولست ملزم بعمل dump**

لمعرفة منصات البحث عن ثغرات تابع هذا الرابط:

https://github.com/Malajab/incyber/blob/master/assets/bugbountyplatfrom.md

الآن نأتي لأهم الأدوات التي نحتاجها وسوف نقوم بتثبيتها على نظام كالي لينكس.

قبل البدء بسرد ما سوف نقوم بتثبيته هذا اليوم قمت بجمع العديد منها في هذا الرابط يمكن الاطلاع عليه:

https://github.com/Malajab/incyber/blob/master/assets/tools.md

الأداة الأولى:

📣 خادم الوكيل Proxy والتنصت على الشبكات

اسم الاداة	الوصف	اللغة المستخدمة	الموقع
اداة Burp Suite	تقوم الاداة بعتراض الاتصال والتعديل عليه قبل ارساله الى الخادم	لغة الجافا	https://portswigger.net/burp

جدها مباشرة لاتحتاج إلى تحميل وكونك مبتدىء فستكون كافية ولكن يوجد منها نسخة professional بمبلغ 300 دولار سنويًا تستطيع عمل إضافات تساعد في الأتمتة وتجنب عمل الخطوات يدويا.
على سبيل المثال

اضافة Mind Map Exporter	وظيفة هذه الاداة رسم الخارطة الذهنية لجيمع الروابط الخاصة بالموقع الذي يتم فحصة	لغة الجافا	https://portswigger.net

سوف نقوم بشرح هذه الأداة في لقاء قادم.

الأداة الثانية:

فحص خوادم تطبيقات الويب

اسم الاداة	الوصف	اللغة المستخدمة	الموقع
اداة FFuF	من الادوات التي استخدمها بشكل يومي وهي تقوم بمحاولة تخمين الامتدادات الخاصةبالمواقع وكما يميز هذه الاداة هي امكانية تخصيصها حسب رغبتك	لغة Go	https://github.com/ffuf/ffuf

تعتبر من الأدوات الرائعة جدًا حيث تقوم بعمل مسح (Scan) على موقع الويب كاملًا وتعطيك نتائج منظمة ولديها المزيد من المزايا.
في البداية نقوم بتحميل الأداة من هذا الرابط

https://github.com/ffuf/ffuf

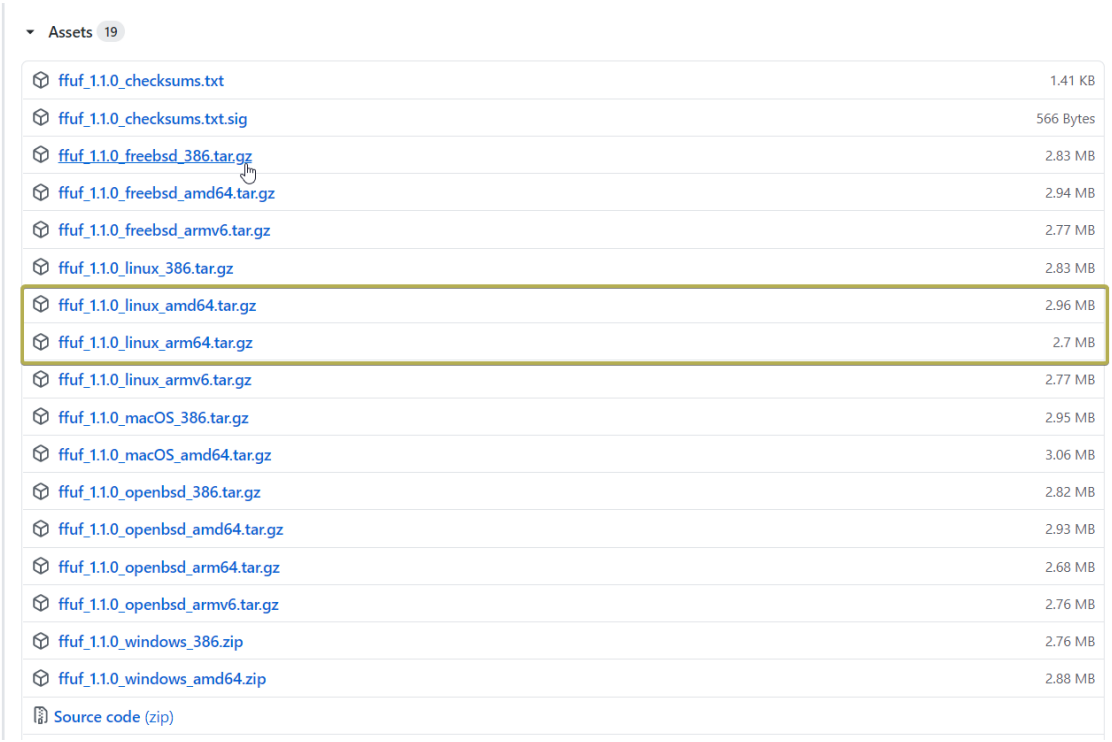
ثم من قائمة التحميل

Installation

- Download a prebuilt binary from releases page, unpack and run! or
- If you have go compiler installed: `go get github.com/ffuf/ffuf`

The only dependency of ffuf is Go 1.11. No dependencies outside of Go standard library are needed.

تقوم باختيار النسخة المناسبة.. هاتين النسختين مناسبتين لنظام كالي



من مميزات هذه الأداة فمجرد التحميل تحصل عليها دون الحاجة للتثبيت.

لمعرفة متطلبات الأداة ضع الأمر:

```
./ffuf
```

ستجد الكثير من الأوامر لكني سوف أذكر اثنين منها:

- u- .. يستخدم لوضع رابط الهدف.
- c- .. سوف يعطيك تنسيق بالألوان للنتائج.

وهنا أود الإشارة إلى أنه ومن الأمور المهمة التي يجب أن تركز عليها هو تصفية نتائج البحث قبل ظهورها وهذا ممكن من خلال الأوامر فمثلا إذا أردت تقليل عدد الكلمات اكتب w-

حينما نقوم بتشغيل الأداة ضع هذا الأمر

```
./ffuf -c -u http://www.tesla.com/FUZZ -w
```

تابع الآن شرح لهذه الأداة

https://youtu.be/Boq9oJ1mdto?t=3000

قد تسأل ماهي قائمة الكلمات (word list) التي تفيدني خلال عملية الاصطياد؟

سيفيدك المصدر (Seclist) كثيرًا .. حيث تم عمل مستودع كامل تجد في الكثير من الثغرات والمنصات التي قد تواجهها.
سأذكر هنا أن ذلك سيفيدك في حال كنت تعمل tracking لموضوع misconfiguration الذي يستخدمه المبرمج و system administrator مثلا يقوم بتثبيت ssh قد ينسى أن يحذف الملفات وهكذا.

مصادر متعددة

المصدر	الوصف	الموقع
مصدر SecLists	مصدر يحتوى على قوائم متعددة تستخدم في اختبار الاختراق واصطياد الثغرات وانصح باستخدامها	https://github.com/danielmiessler/SecLists

رابط المصدر على GitHub:

https://github.com/danielmiessler/SecLists

قبل تحميل الأداة عليك أن تتأكد أن لديك فك الضغط للملفات
إذهب إلى الترمنيال وأكتب الأمر:

```
unzip
```

تابع هنا لتعرف كيفية تحميل Seclists والعمل عليها.
https://youtu.be/Boq9oJ1mdto?t=3786

البعض يأتي إلي يسأل أن XSS – SQLi – LFI لاتعمل لديه؟
السبب في ذلك أن أغلبية المواقع تجد واجهاتها أو هي مستضافة لدى شبكات مثل أكاماي (Akamai) أو كلاود فلير(Cloudflare) (هذه الشبكات لتوزيع محتوى نطاقات ومقدم للخدمات السحابية) تقوم مثل هذه الشبكات بعمل قائمة سوداء لمثل Seclists من هنا لن تسفيد منها. لذلك إذا كنت تريد العمل بنصيحتي اخلق شيء خاص بك أو تتبع بعض الهاشتاقات في تويتر مثل #bugbountytips يضع البعض خطوات تستطيع من خلالها تخطي الحماية.

أضافة بالانجليزية لمن أراد معرفة المقصود بـ misconfiguration؟

https://www.coursera.org/lecture/cyber-threats-attack-vectors/misconfiguration-4Pvmi

الأداة الثالثة:

وهي من أدوات فحص خوادم تطبيقات الويب.

اداة dirsearch	تقوم هذه الاداة بمحاولة تخمين الامتدادات الخاصة بالموقع المستهدف وهي اداة سهلة الاستخدام وكذلك قوية الاداء	لغة python	https://github.com/maurosoria/dirsearch

رابط تحميل الأداة:

https://github.com/maurosoria/dirsearch

شرح تثبيت الأداة:

https://youtu.be/Boq9oJ1mdto?t=4347

فيما يخص الأداوت التي يتم عملها بلغة البايثون تستطيع التعامل معها بصيغتين من الأوامر:

```
python3 dirsearch.py

chomd +x dirsearch.py
```

تطبيق على أداة (dirsearch)ويجب أن أنوه هنا إلى أن الأداة حتى تعمل تحتاج إلى امتداد (extension e.g .php) إذا لم تكن تعرفه يمكن الاكتفاء بوضع علامة / (Slash).

https://youtu.be/Boq9oJ1mdto?t=5102

في جانب Bug Bounty أريد أن أعطيك هذه نصيحة استخدم user agent مستخدم كثيرًا في عملية التصفح من أجل أن تتفادى اكتشافك ومن ثم عمل حظر لك.
إذا كنت تبحث عن user agents اكتب في محركات البحث List of User Agents

https://developers.whatismybrowser.com/useragents/explore/

وللحديث والتطبيق أكثر تابع هذا الجزء.
https://youtu.be/Boq9oJ1mdto?t=5353

إذا كنت Bug Bounty hunter انصحك بالاطلاع على:
https://tools.ietf.org/html/rfc2616

الأداة الأخيرة:

وهي من أدوات فحص خوادم تطبيقات الويب.

اداة Sublist3r	تقوم هذه الاداة بحصر وجمع جميع النطاقات الفرعية الخاصة بالموقع المستهدف مستعينة بالخدمات العامة مثل قوقل ياهو وغيرها	لغة python	/https://github.com/aboul3la/Sublist3r

رابط تحميل الأداة:
/https://github.com/aboul3la/Sublist3r

شرح الأداة:
https://youtu.be/Boq9oJ1mdto?t=6204

بالمناسبة تستطيع تثبيت هذه الأداة على نظام الويندوز.

من الأشياء المفيدة والتي أود ذكرها في نهاية هذا اللقاء:

DNSdumpster موقع يفيدك كثيرا في maping domain https://dnsdumpster.com/

كذلك موقع viroustotal مفيد لأنك ستجد نتائج جاهزة تستطيع أنت استخدامها كذلك عموما مفيد في فحص الملفات والبرمجيات الخبيثة. https://www.virustotal.com/gui/home/upload

يوجد كذلك أداة AssetFinder
https://github.com/tomnomnom/assetfinder

أخيرًا ستجد هنا نموذج لكيفية عمل التقرير.

https://github.com/Malajab/incyber/blob/master/Template/bug-report.md

ماهو المطلوب للقاء القادم:

- التأكد من تثبيت جميع الأدوات التي تم ذكرها.
- التسجيل في موقع https://tryhackme.com/signup سنقوم بعمل الدروس في نطاق الجزء المجاني.