# اكتشاف الثغرات

مقدمة حول تقنيات اكتشاف الثغرات وكيفية البدء في مجال البق باونتي

تقديم: صالح لرضي

# Keywords

مصطلحات في المادة التدريبية:
ما بين القوسين [] يشير إلى مصطلح البحث في جوجل للاستزادة في الموضوع.

# مالذي سنتعلمه اليوم؟

١. ما هو اصطياد الثغرات؟
٢. أهميته
٣. الفرق بين الاختراق الأخلاقي وصيد الثغرات
٤. الفرق بين VDP و BBP
٥. اختيار البرنامج المناسب لك
٦. منصات اكتشاف الثغرات الأمنية
٧. متطلبات Bug Bounty
٨. الأدوات المستخدمة
٩. الفحص اليدوي والاوتوماتيكي
١٠. حيل وأفكار

# ما هو اصطياد الثغرات؟

هي عملية فحص التطبيقات بأنواعها (ويب|اندرويد|أيفون) بحثًا عن الثغرات الأمنية.

الهدف: المال.
الكيفية: حيل وأدوات.

# ما هو اصطياد الثغرات؟

هناك ٣ عناصر أساسية في أي هجوم الكتروني ناجح - الطريقة - والفرصة - والدافع

Method—Opportunity--Motive


مجال البق باونتي يتركز على الدافع المالي - ادفع المال لتحمي نفسك

# أين المشكلة؟؟

تخيل معي أن بنك وصل إلى مليون عميل مع تقديم خدمات الكترونية تحويل إلى حسابات ووو، جميل صحيح؟

لكن دعونا ننظر من جانب آخر، ماذا لو استطاع شخص الدخول إلى قاعدة البيانات وتنزيلها! هل هذا ممكن؟

هذه النقطة بالذات تؤرق الشركات الكبيرة، فمجرد غض البصر عن جانب من جوانب الخدمة الالكترونية قد تخسر وتغرق في ديون.

# أين المشكلة؟؟

حينها ستبدأ الشركة في اتخاذ قرارات لتأمين معلوماتها وهي:

- توظيف مختبري اختراق وتقسيم المهام بين فريق احمر وازرق.
- التدقيق الأمني ومراقبة العمليات في النظام.
- الحماية من الهجمات الالكترونية:

توعية.

تثبيت حلول الحماية (EndpointSecurity | CloudSecurity | PasswordManagment | LogManagment | Patch and vulnerability Management | SEIM) :

وغيرها الكثير...

# أين المشكلة؟؟

لكن تبقى هذه الحلول هذه غير كافية 100%، فمن الصعب جدًا معرفة جميع الثغرات الأمنية في موقع ما، فحتى الشركات الكبرى يعثر فيها على ثغرات أمنية عالية الخطورة Criticalبين فترة وأخرى.

هنا تكمن الفكرة! بدل أن تحرك عقول فريق لا يتجاوز 20شخص، افتح المجال للجميع !!وذلك بالاشتراك في برامج bugbountyالتي يزورها آلآف الهاكرز كل يوم.

# أين تكمن أهميته؟

بغض النظر فيما إذا كنت باحث أو شركة مستضيفة ففوائد البق باونتي عديدة منها:

**كباحث أمني**

- فرصة لربح المال
- فرصة لتطوير المهارات
- فرصة سانحة للتسويق للذات والحصول على فرصة عمل - على اقل تقدير مع الجهات التي تجد فيها ثغرات خطيرة.

**كشركة أو مؤسسة**

- توفير حماية عالية للموقع والعملاء.
- الحفاظ على سمعة الشركة.
- توفير الوقت والمال.
- الحفاظ على الثقة والولاء للعملاء.
- جذب المواهب المتخصصة.

# أهمية البق باونتي؟؟

قد يتسآل البعض عن أهمية هذا للشركة التي تستضيف باحثين أمنيين، حيث تكمن الأهمية في الآتي:

- الحد من الثغرات الأمنية الخطيرة
- الحفاظ على حقوق المستخدمين والعملاء
- الحد من التسريبات التي قد تتسبب في كارثة أو تؤدي إلى إفلاس الشركة

# الفرق بين الاختراق الأخلاقي وصيد الثغرات

**الاختراق الأخلاقي:** يشير إلى عملية اختبار أمني تُجرى على نظام حاسوبي أو تطبيق للكشف عن الثغرات الأمنية والتي يتم العمل على إصلاحها. يتم تنفيذ الاختبارات الأمنية بموافقة صاحب النظام أو المؤسسة المعنية، ويتم العمل على تقديم تقرير يوضح الثغرات المكتشفة والتوصيات اللازمة لإصلاحها، ويتم العمل على إصلاح هذه الثغرات.

أما **صيد الثغرات - bug bounty**، فهو برنامج يقدمه صاحب النظام أو الموقع للمكتشفين المحتملين للثغرات الأمنية، ويتم تحديد مكافأة مالية محددة للمكتشفين الذين يقدمون بلاغا عن ثغرات أمنية محددة. يمكن أن يشارك في البرنامج أي شخص يهتم بالأمان السيبراني ويمتلك المهارات اللازمة لاكتشاف الثغرات، ولا يتطلب منهم الحصول على موافقة صاحب النظام قبل البحث عن الثغرات.(إذا كانت برامج عامة)

# الفرق بين الاختراق الأخلاقي وصيد الثغرات

| الميزة | الاختراق الاخلاقي | البق باونتي |
|---|---|---|
| الغرض | الإبلاغ عن الثغرة وإصلاحها كمسؤولية في المؤسسة | الحصول على مكافئات من خلال البحث عن الثغرات |
| النطاق | غير محدد على منصة أو تطبيق. | غالبًا ما يكون محدد وفق سياسة محددة |
| الحافز الرئيسي | تعزيز الأمن في المؤسسة بشكل عام | المال أو السمعة |
| الطريقة | استخدام المعرفة وتقنيات black hat hackers | استخدام المعرفة وتقنيات black hat hackers |
| علاقة الباحث بالمؤسسة | يعمل الباحث في المؤسسة | لا يرتبط الباحث بالمؤسسة |

# قبل البدء

هناك القليل ما بين ٩٥-٩٩ من المواقع لا تملك برامج أمنية
هذا يعني التأكد من الجهة قبل فحصها.

لأن هناك محركات بحث تظهر لك مواقع مصابة مثل جوجل دورك، و موقع Shodanو FOFAو
hunter.howو ip criminal.

متوسط دخل ال bug hunters هو 3000$ شهريًا.

# لماذا يناسبنا كيمنيين؟

- مصادر التعلم مجانية.
- قلة الرواتب في اليمن.
- مرونة ساعات العمل.

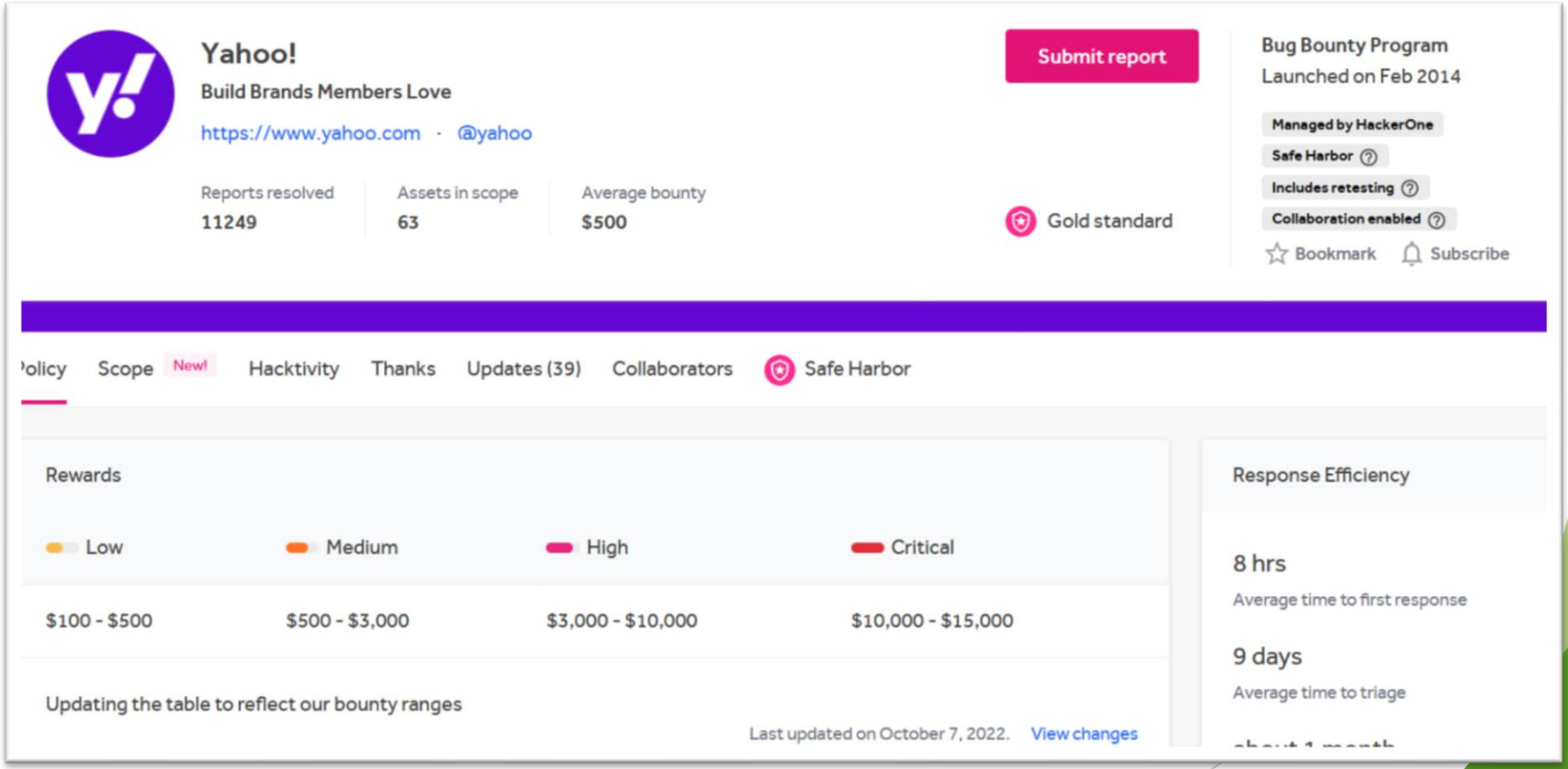
# VDP vs BBP

يوجد نوعين من برامج اكتشاف الثغرات الأمنية وهي:

VDP: Vulnerability Disclosure Program
BBP: Bug Bounty Program

الأولى محبذه للمبتدئين وذلك لسهولة العثور على ثغرات فيها والسكوب الواسع.


MTN Group
https://www.mtn.com/
Submit report
Vulnerability Disclosure Program
Launched on Dec 2019
Reports resolved
4258
Assets in scope
376
Bookmarked
Subscribed
Policy
Scope
New!
Hacktivity
Thanks
Updates (0)


Yahoo!
Build Brands Members Love
https://www.yahoo.com · @yahoo
Submit report
Bug Bounty Program
Launched on Feb 2014
Managed by HackerOne
Safe Harbor
Includes retesting
Collaboration enabled
Bookmark
Subscribe
Reports resolved
11249
Assets in scope
63
Average bounty
$500
Gold standard
olicy
Scope
New!
Hacktivity
Thanks
Updates (39)
Collaborators
Safe Harbor
Rewards
Low
Medium
High
Critical
$100 - $500
$500 - $3,000
$3,000 - $10,000
$10,000 - $15,000
Updating the table to reflect our bounty ranges
Last updated on October 7, 2022.
View changes
Response Efficiency
8 hrs
Average time to first response
9 days
Average time to triage

# Looking for VDP & BBP

عند البحث عن برنامج مناسب لك، اجعل في عين الاعتبار النقاط التالية:

١. إمكانياتك وخبرتك - ex. لغة البرمجة والسيرفر - ويب أم تطبيق أم نظام تشغيل
٢. أهدافك - وكم مدى هتبقى في البروقرام.
٣. تحليل المنافسة.
٤. عدد التقارير والسكوب.

# طرق اختيار البرنامج

منصات اكتشاف الثغرات Intigrity -YesWeHack -Hackerone -BugCrowd.
عن طريق جوجل دورك. [google dorks for bug bounty]

# منصات تدير اكشاف الثغرات

تعمل هذه المنصات كوسيط بين الهاكر والشركة وتشرف على عملية التبليغ، أبرز هذه المنصات هي Hackeroneو Bugcrowd .

هذا الرابط https://github.com/disclose/bug-bounty-platforms يحتوي على قائمة بكافة المنصات.

# متطلبات قبل الإبحار إلى رحلة التعلم
# - مرحلة الإعداد

تتلخص مرحلة الإعداد من جانبين:

- الإعداد المعرفي.
- تنصيب بيئة عمل مناسبة.

# الإعداد المعرفي

**الأساسيات:**

١. أساسيات أمن تطبيقات الويب، كفهم عمل الثغرات الشائعة.
٢. فهم كيفية عمل تطبيقات الويب.
٣. الإرادة والتعلم المستمر.

**إضافي:**

- لغة إنجليزية ممتازة.
- تعلم كتابة التقارير (يمكنك الاستعانة مع ب .ChatGPT)
- تعلم كيفية التعامل مع الشركات عند تقديم الثغرة. (قراءة التقارير السابقة).

....

# الإعداد المعرفي

**إضافي:**

- التعامل مع سطر أوامر لينكس.
- اساسيات البرمجة.
- أساسيات الشبكات.

# مصادر رئيسية للتعلم

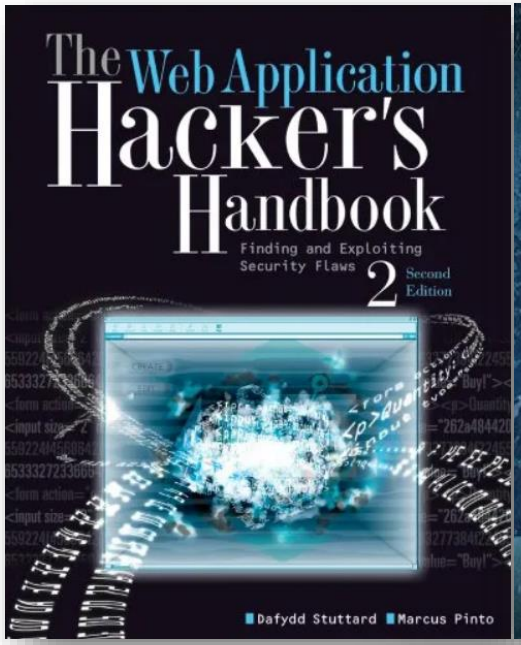
١- الكتب.

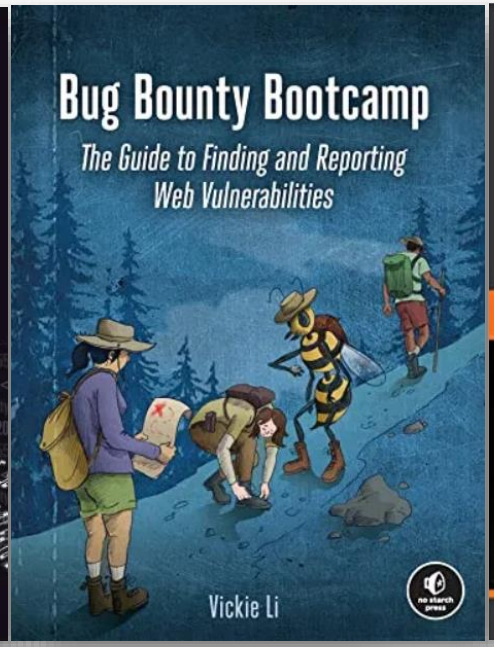
٢- التقارير المنشورة Disclosed reports

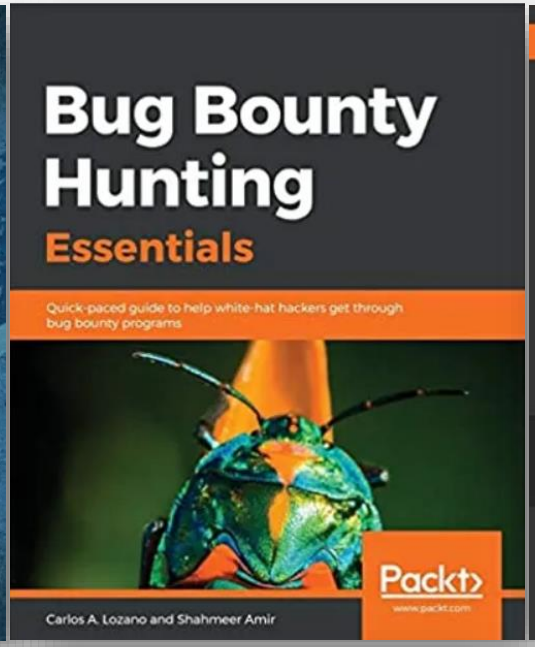
٣- الرايت اب على موقع Medium.com
[site:*.medium.com | site:medium.com "Keyword"]

٤- الحيل الهاكرز على وسائل التواصل مثل تويتر ولينكد إن...

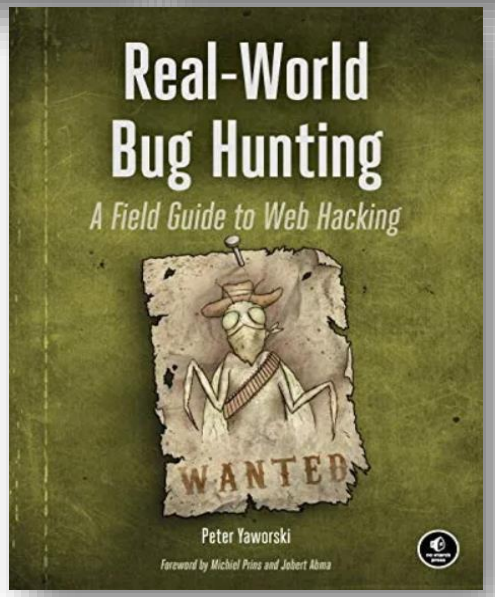
# الكتب

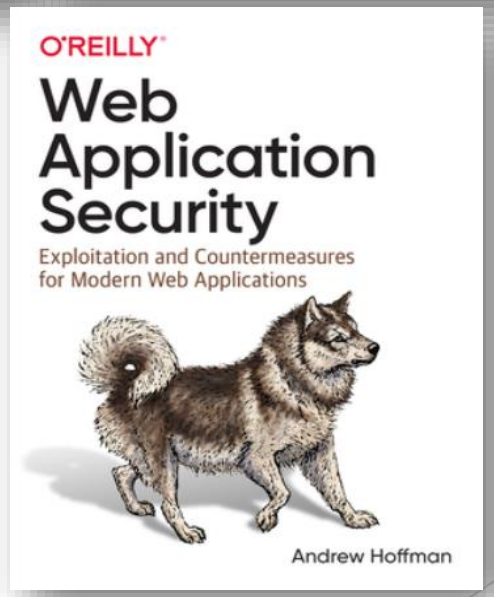

The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto


Bug Bounty Bootcamp
The Guide to Finding and Reporting Web Vulnerabilities
Vickie Li


Bug Bounty Hunting
Essentials
Quick-paced guide to help white-hat hackers get through bug bounty programs
Carlos A. Lozano and Shahmeer Amir
Packt


Prakhar Prasad
Mastering
Modern Web Penetration Testing
Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does!
Packt


Real-World Bug Hunting
A Field Guide to Web Hacking
WANTED
Peter Yaworski


O'REILLY
Web Application Security
Exploitation and Countermeasures for Modern Web Applications
Andrew Hoffman

# التقارير المنشورة

1. https://hackerone.com/hacktivity/overview

2- https://huntr.dev/bounties/hacktivity

....

# الرايت ابس Write-ups

**الرايت اب: هي المقالات التي يحكي فيها الهاكرز تجاربهم عند اكتشاف الثغرات الأمنية.**

**ابرز المواقع التي يكتبون فيها:**

1. **Medium.com**
2. **https://infosecwriteups.com/**

**site:*.medium.com | site:medium.com**
**Site:infosecwriteups.com**
**…..**

# حيل الهاكرز على وسائل التواصل

١. الهاشتاق #bugbountytips على منصة X (تويتر).

٢. المنشورات على لينكد إن.

Bug_Bounty_Career @Library_Sec @LibrarySecBackups.pdf

# إعداد بيئة الاختراق

**من على الاندرويد:**

تطبيق تيرمكس أو استخدام VPS أو RDP

**جهاز الحاسوب:**

تثبيت أحد توزيعات لينكس المخصصة لأختبار الأختراق مثل كالي لينكس أو Parrot Sec OS. ....

# إعداد بيئة الاختراق

**تنزيل تطبيق تيرمكس**

يجب تنزيله من على الموقع الرئيسي وليس المتجر، لأنه توقف عن نشر التحديثات في المتجر.

الموقع الرئيسي: https://github.com/termux/termux-app

التنزيل: https://f-droid.org/en/packages/com.termux

# الأدوات التي ستحتاجها في رحلتك

1. Burpsuite.
2. Nuclei.
3. Nmap.

# ثغرات شائعة

هناك عدد كبير جدًا من الثغرات الشائعة منها:

1. XSS
2. Information Disclosure
3. SQLi
4. Business Login Errors
5. Broken Access Control
6. SSRF
7. Open Redirection
8. RCE
9. OS command injection
10. Race Conditions
11. Cache Vulns: Cache Deception and Poisoning
12. Subdomain Takeover
13. IDOR - Insecure Direct Object References

READ OWASP 10: https://owasp.org/www-community/vulnerabilities/

# تحديد الهدف

- تحديد الموقع الالكتروني: من خلال جوجل دورك أو من أحد المنصات - integrity HackerOne - BugCrowd
- قراءة الpolicy الخاصة بالبرنامج. كمثال Yahooأو DoD.
- وضع خطة زمنية محكمة للفحص.

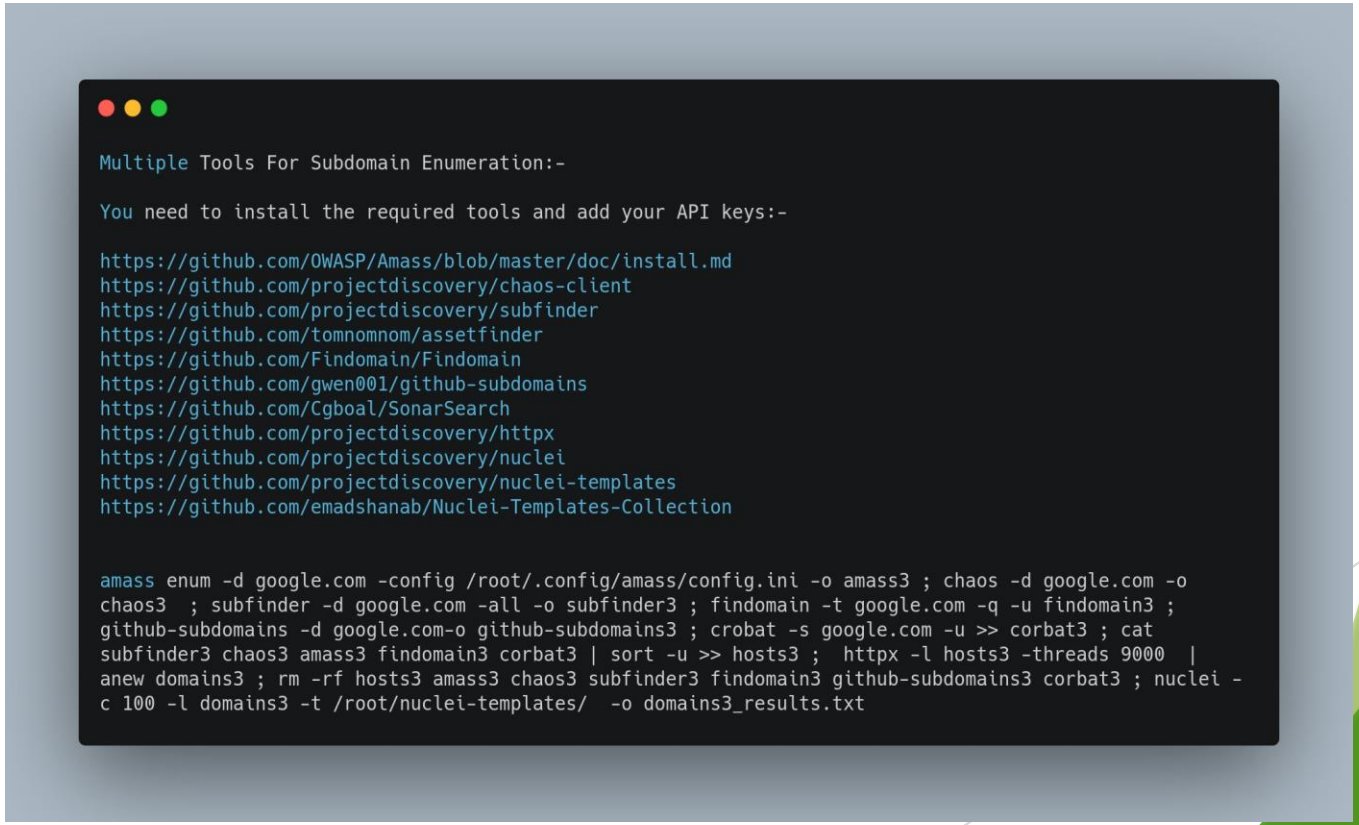
# تقنيات الاستطلاع Recon

١. جمع النطاقات الفرعية للهدف المحدد
٢. جمع ملفات الجافا سكريب للتطبيقات
٣. قراءة تعليمات الموقع الالكتروني
٤. أهداف الموقع
٥. البحث عنه في الانترنت
٦. جمع كافة الروابط gauو waybackurls
٧. النشرات على التواصل الاجتماعي - منشورات التوظيف ستعطيك فكرة عن backend
٨. التقارير السابقة وأولويات المؤسسة أمنيًا - سياسة الخصوصية
٩. البحث عن معلومات مكشوفة او مسربة أو ومحاولة الحصول إلى الكود المصدري

# جمع النطاقات الفرعية

Try to use multiple tools as possible, such as:

1- Amass
2- Subfinder
3- Sublist3r
4- AssetFinder



# جمع النطاقات الفرعية

Tip: The better you get more subdomains, the better you have a chance to find vulnerabilities! Use more than one tool!

# جمع المعلومات

بعد عملية جمع النطاقات الفرعية نجمع المعلومات عن هذه النطاقات، مثل التقنيات باستخدام موقع .whatcms.org

اي فاير وول تعمل عليه ؟ ما هي الصفحات الغير مخولة للدخول 401 - 403؟

أداة Httpx

# البحث عن الثغرات

هناك طريقتين للفحص:

- الطريقة الأوتوماتيكية، أي بأدوات اكتشاف الثغرات.
- اليدوية: وتعتمد على التجربة وتحليل الردود.

فهمك العميق لـ OWSAP 10 سيمكنك من العثور على ثغرات أكثر...

# الفرق بين البحث الاوتوماتيكي واليدوي

لنعطي مثال على ذلك: لقيت فورم في موقع تحاول تحقن فيه reflected xss:

**السينارو الاوتوماتيكي:** تحميل أداة اختبار xss مع تنزيل حزمة payloads

النتيجة: تجربة أكثر من ١٠٠٠ بايلود بدون نتيجة – حظر الايبي – حدوث ترافيك غير عادي

**السيناريو اليدوي:** تجربه البايلود الاعتيادي وتحليل الرد:

<script>alert(“successful”)</script>

# الفرق بين البحث الاوتوماتيكي واليدوي

لاحظت بعد ذلك أن ال WAF حذف <script> و </script> في الرد:
alert(“successful”)

هذا يعني أن الجدار الحماية عنده قائمة سوداء تضمن تلك الكيوردز

كيف ممكن ان اتجاوزه؟؟ (سؤال للعامة).

# الاختبار اليدوي

أغلب الثغرات المكتشفة تكون من خلال الاختبار اليدوي ٩٠-١٠٠%

أغلبية عمل الهاكرز ١٠٠% يدوي - أفضل من يستخدم الAutomation يكون بين ٨٠-٩٠% مثل badcracker.

بعض الثغرات لا يمكن برمجة أدوات لاكتشافها مثل IDORو Account TakeOver و Business Logic Errors.

# الإبلاغ عن الثغرات

بعد عملية الفحص، هل وجدت شيء؟

إذا وجدت ثغرة أمنية وتمكنت من تطبيقها والتأكد من ضررها، فقد حان البدء بكتابة تقرير مفصّل عنها لإبلاغ الشركة عنها بالطرق القانونية.

# ثغرات ال ZeroDay

وهي الثغرات في المنتجات الرقمية والتي لم يتم إصدار تقريع لها من قبل الشركة المالكة بعد أو أنها لا تعلمها حتى، إذا وجدتها واحدة أمامك خيارين:

- ما سينصحك به أي هاكر: إبلاغ الشركة عن الثغرة – قد تتلقى مكافأة وقد لا
- ما سأنصحك به: ابحث شركة zerodium.com واطلع على نطاق عملهم، حينها يمكنك بيع استغلالك المميز بمعدل قد يصل إلى ١٠٠ ألف دولار أمريكي أو أكثر.

# كتابة التقارير والنقاط المهمة

ملاحظة: قد ترفع تقرير وتتلقى Informative
وينجح هاكر آخر في الإبلاغ بنفس الثغرة، والسبب يعود إلى جودة التقرير ومدى خبرتك في إثبات الثغرة والإقناع بالتأثير وصياغة الكلمات فكتابة التقارير "فن".

عناصر التقرير على هاكر ون:

1. Title:
2. Summary:
3. Technical Details: PoC (vid or pic) , Step-by-step reproduction
4. Impact:
5. References:
6. Suggested remediation:

# حيّل

الإدارة: تنظيم الوقت والتعلّم.
محاولة استهداف أصول الشركة الحساسة - التركيز على الإضرار في: العملاء - الموظفين

أي هذه العناوين أفضل؟؟؟

Reflected XSS Poc = <script>alert(“xss”)</script>
Steal cookies via Reflected XSS Poc = <script>alert(document.cookie)</script>

# حيّل

أضف إلى التقرير لمستك الخاصة ولا تقلّد الآخرين، ابذل جهدك فيه!!

أي هذه العناوين أفضل؟؟؟

Dos attack on … endpoint
No rate limit on … lead to server out of service

# بناء سمعتك كباحث أمني

الالتزام بالأخلاق حتى مع تعنت بعض Triagers.

في هاكرون تزداد فرصة أن تتلقى دعوات من برامج بق باونتي خاصة إذا عثرت على ثغرات أكثر حتى على vdp .

حاول أن تكون أفضل ١٠ هاكرز في برنامج ما.

لا تهتم بجمع المال في أو ٦ أشهر لك، ركز على صقل المهارات وبناء سمعة حسنة.

الاستمرار وعدم الانقطاع عن التبليغ.

# مستقبل صيد الثغرات

مع تغلغل التكنولوجيا في حياتنا، ستزداد عدد الأصول، وبالمقابل ستزداد الهجمات الالكترونية

دعنا نقارن الامس باليوم:
سابقًا كانت الشركات تدفع ٥ دولارات مقابل ثغرات مثل XSSوقليل جدًا من هو مهتم في مجال bug hunting.
أما اليوم فتنفق ملايين الدولارات، كرم فريق هاكرون هاكر كندي لوصوله إلى 3 مليون دولار.

شركة MatterMost تمنح هاكر ٧٥٠ دولار وتضع درجة خطورة الثغرة High وعنوانها:
Password Reset Link Uses http protocol!

# أفكار ونصائح

...

If you have the SKILLS, go for it.

If not, it’s NEVER too late to learn!!