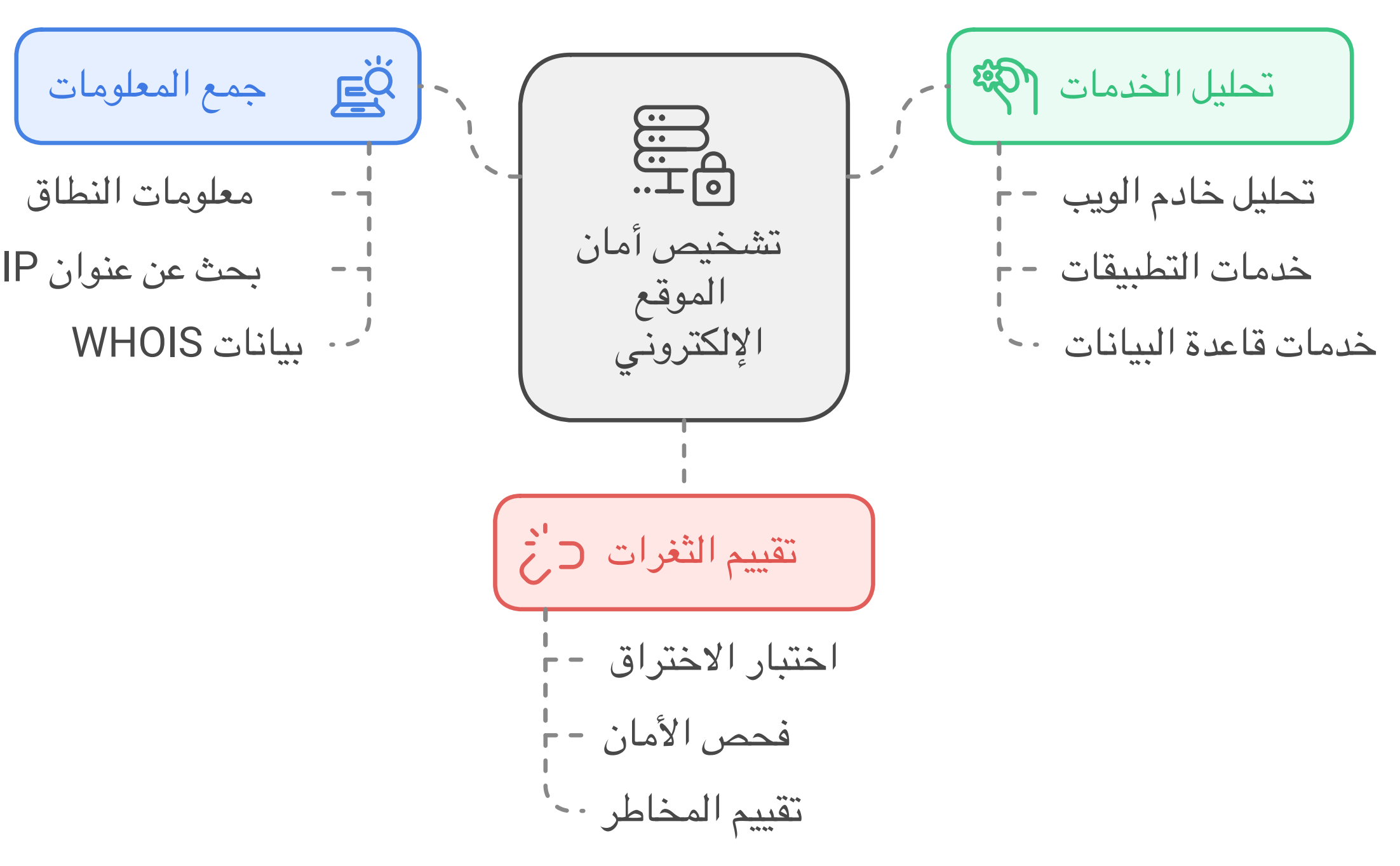
تحليل وتشخيص ألمواقع الأكترونية

لتشخيص هدف)موقع إلكتروني(وفهم الهيكل الأمني الخاص به بشكل كامل، تحتاج إلى المرور بعدة مراحل متكاملة لجمع المعلومات وتحليل الخدمات والثغرات. سأتناول معك الخطوات الأساسية التي تساعدك في تشخيص الموقع المستهدف:

.1جمع المعلومات: (Reconnaissance)
أ. معلومات أساسية عن النطاق: (Domain Information)



ابدأ بجمع معلومات عن النطاق باستخدام أدوات متخصصة:

Whois Lookup

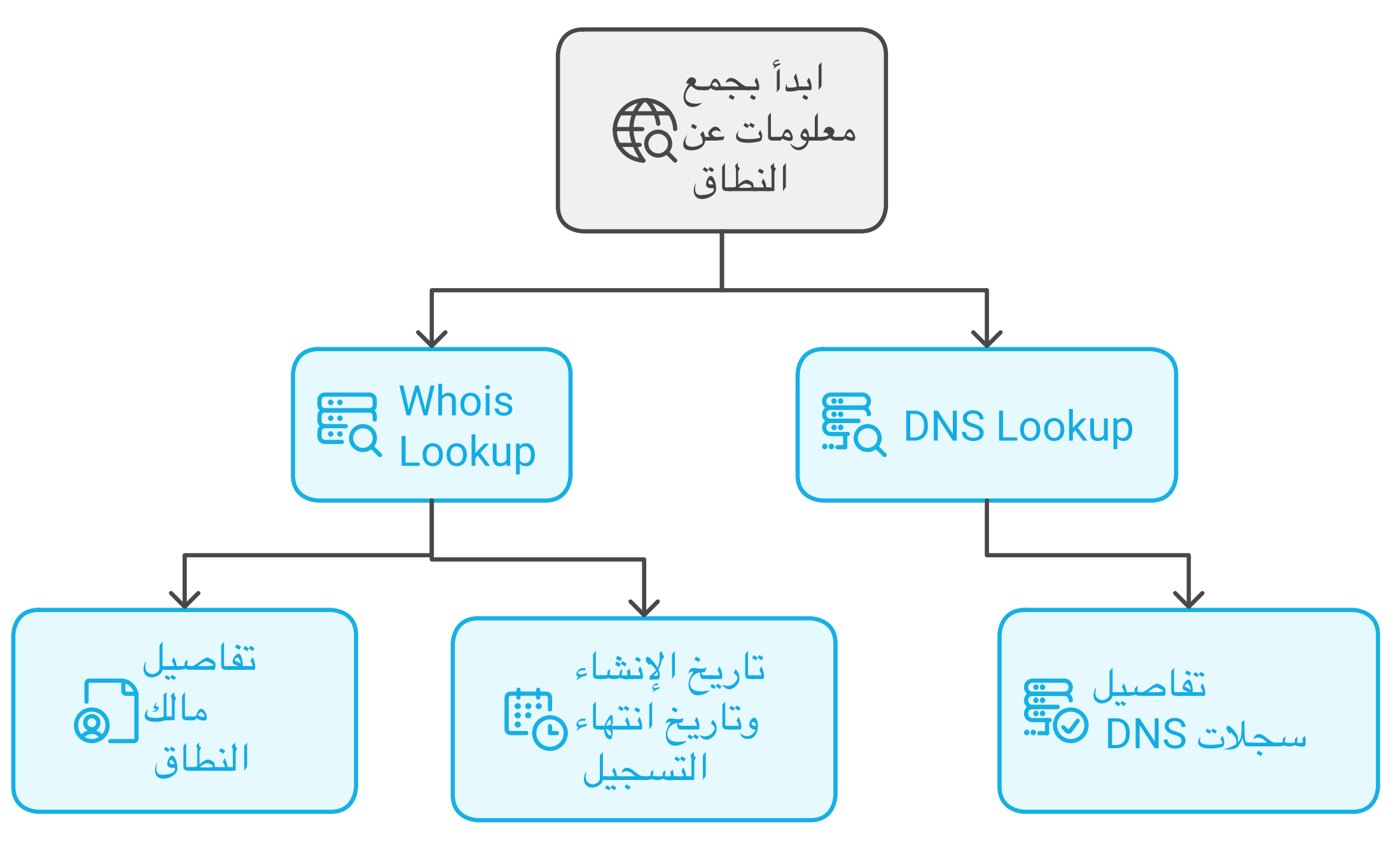
يوفر معلومات عن مالك النطاق، تاريخ الإنشاء، وانتهاء التسجيل. استخدم الأمر

```
whois example.com
```

DNS Lookup

لمعرفة تفاصيل سجلات DNS الخاصة بالموقع المستهدف. أداة مثل **dig** أو **nslookup** توفر هذه المعلومات.

```
dig example.com
nslookup example.com
```



ب. فحص النطاقات الفرعية: (Subdomain Enumeration)
قد تكون بعض النطاقات الفرعية غير معلنة، وتحتوي على خدمات حساسة. أدوات مثل Sublist3r وAmass تستخدم لجمع هذه المعلومات.

```
sublist3r -d example.com
amass enum -d example.com
```

ج. فحص البنية التحتية: (Infrastructure Analysis)
يمكنك استخدام أدوات للكشف عن مزود خدمة الاستضافة ونظام التشغيل المستخدم في الخوادم.

Netcraft:

للحصول على معلومات عن تكنولوجيا الخادم ونظام التشغيل.

د. جمع بيانات عامة من الويب: (Google Dorking)
استخدام عمليات بحث متقدمة لاستخراج بيانات غير مؤمنة من الموقع باستخدام محركات البحث مثل .Google

.2فحص المنافذ والخدمات: (Port Scanning and Service Enumeration)
أ. فحص المنافذ المفتوحة: (Open Ports)
باستخدام أداة Nmap، يمكنك فحص المنافذ المفتوحة على الخادم واكتشاف الخدمات التي تعمل.

```
nmap -sV -O example.co
```

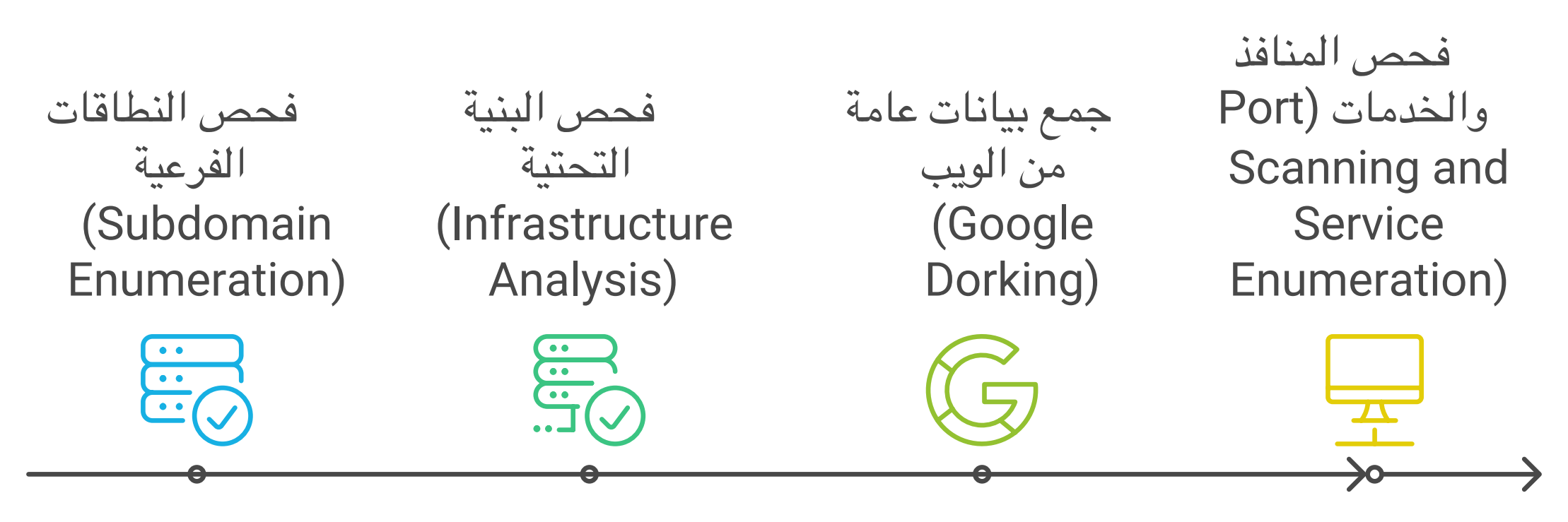
لاكتشاف نسخ الخدمة التي تعمل على المنفذ

-sV:

لتحديد نظام التشغيل

-O:

جمع المعلومات عن الهدف (Information Gathering)



ب. فحص البروتوكولات والخدمات:
بعد فحص المنافذ، يمكن استخدام أدوات متخصصة لفحص الخدمات مثل:اكتشاف الاعدادات الخاطئة بمثل HTTP
- FTP - SSH :

تم استخدام ادوات مثل - Nikto Nmap-scripts

```
nmap: --script=ftp-anon,ssh2-enum-algos,http-enum example.com
```

ج. فحص الشهادات الأمنية: (SSL/TLS Scan)
للتحقق من أمان الاتصال عبر :HTTPS
لتحليل قوة الشهادة SSLScan :

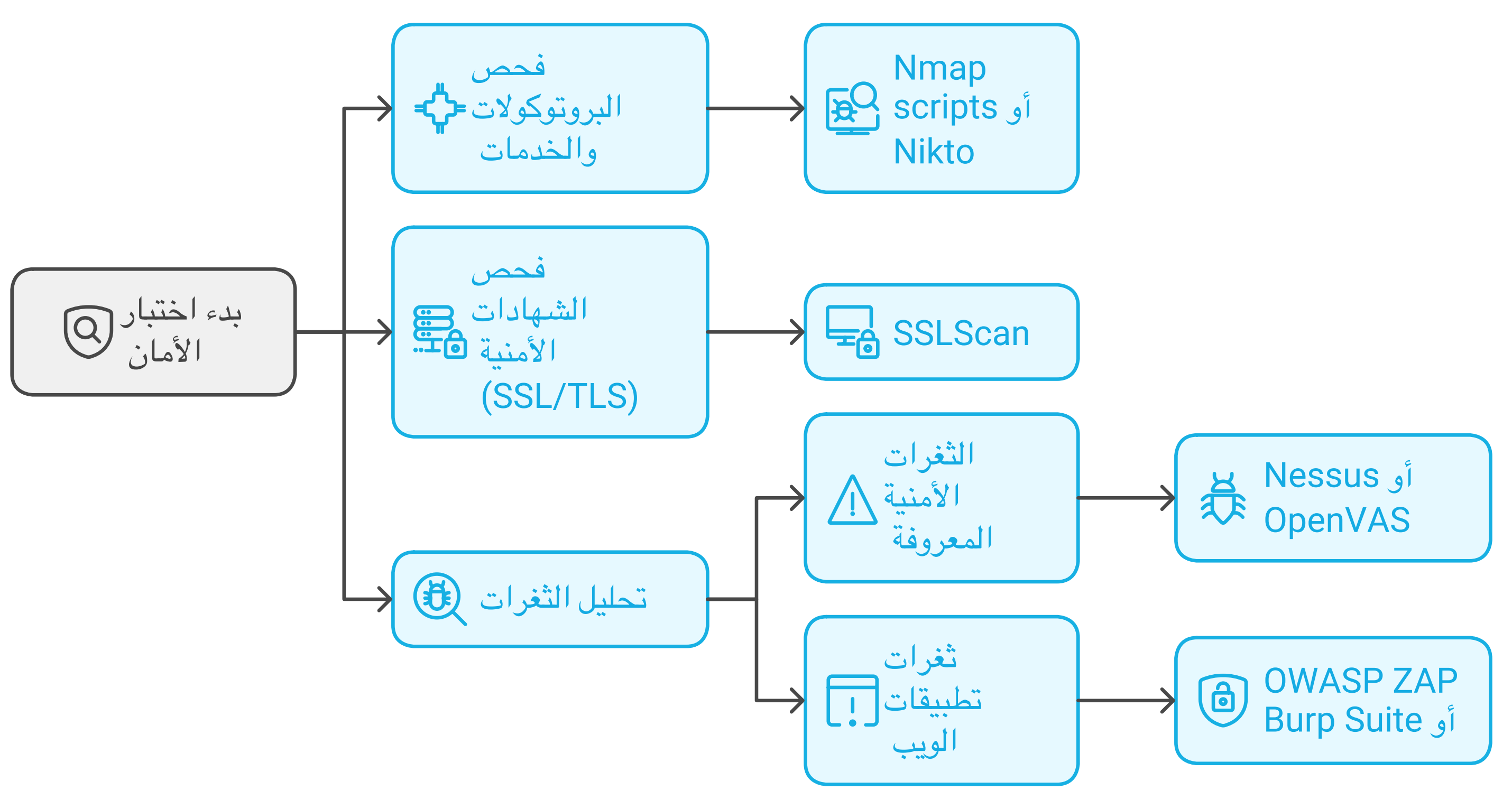
```
sslscan example.com
```

.3تحليل الثغرات: (Vulnerability Scanning)
أ. فحص الثغرات الأمنية المعروفة:
استخدام أدوات تلقائية مثل:
هذه الأدوات تقوم بفحص الثغرات على نطاق واسع، بما في ذلك الثغرات في

Nessus or OpenVAS:

أنظمة التشغيل، التطبيقات، وتكوين الخادم.
ب. فحص تطبيقات الويب: (Web Application Scanning)
لفحص الثغرات الشائعة في التطبيقات او الويب مثل

OWASP ZAP - Burp Suite - SQL Injection - XSS - CSRF:



يمكنك أيضًا تجربة أدوات أخرى مثل:
لفحص ثغرات :SQL Injection

```
sqlmap -u "http://example.com/page?id=1"
```

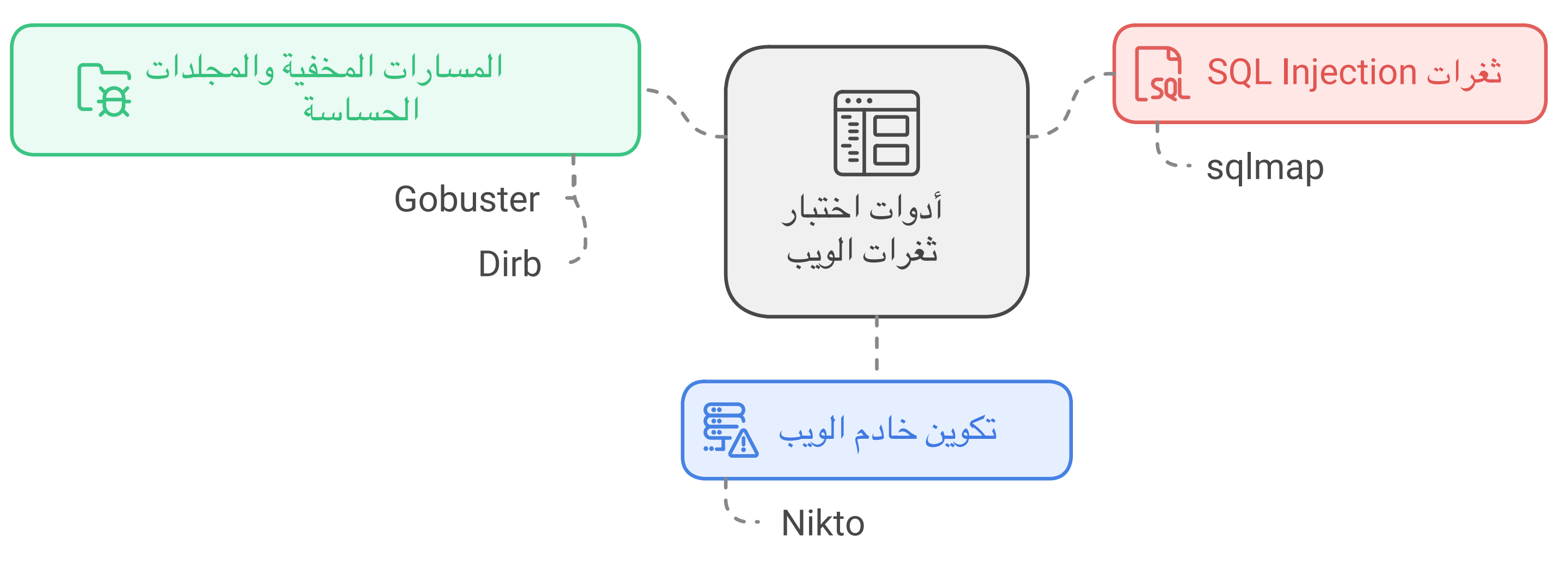
لفحص ثغرات تكوين خادم الويب

```
nikto -h http://example.com
```

ج. فحص المسارات المخفية والمجلدات الحساسة:
استخدام أدوات مثل:
لاكتشاف المجلدات المخفية والملفات المهمة التي قد تحتوي على بيانات حساسة.

Gobuster أو Dirb:

```
gobuster dir -u http://example.com -w /usr/share/wordlists/dirb/common.txt
```

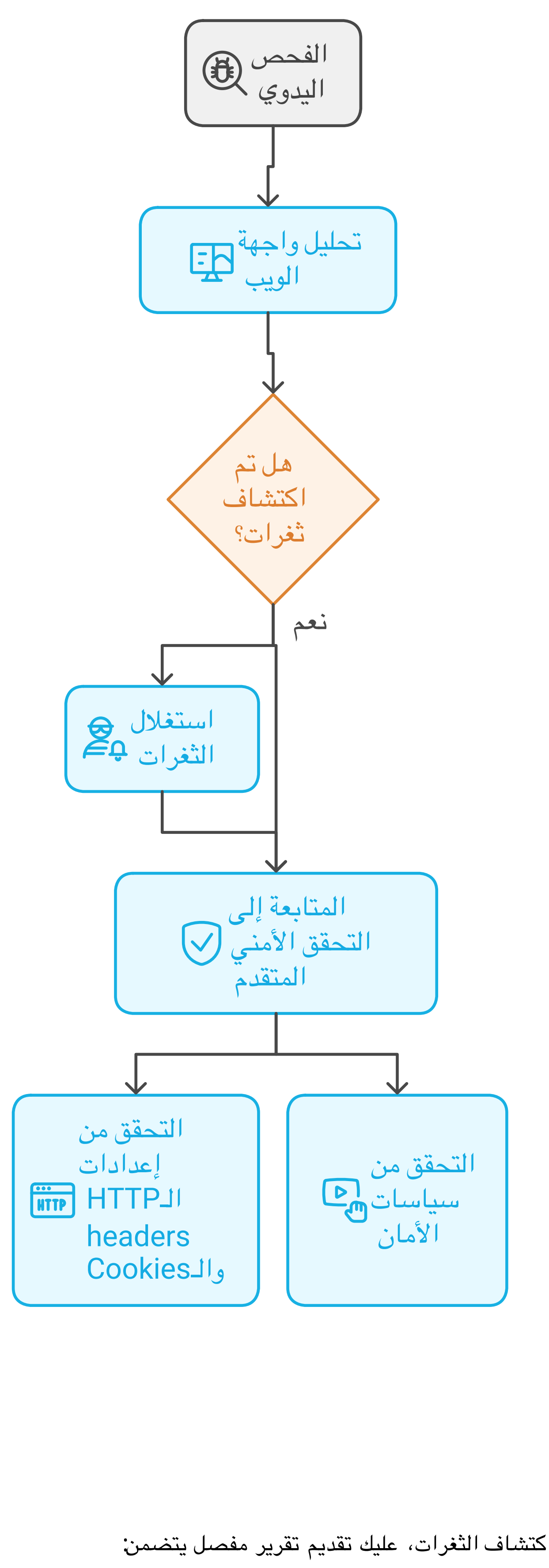


.4الفحص اليدوي: (Manual Testing)
أ. تحليل تطبيقات الويب:
قم بتحليل يدوي لواجهة الموقع لاكتشاف أخطاء في إدارة الجلسات، رفع الملفات، أو إدخال البيانات غير المصححة.

ب. استغلال الثغرات المكتشفة:
في حال اكتشاف ثغرات، استخدم أدوات مثل Metasploit أو ExploitDB لاختبار استغلالها بشكل آمن.
.5التحقق الأمني المتقدم: (Advanced Security Check)
أ. التحقق من الـ Headers والأمن المتعلق بالـ:Cookies
تفحص إعدادات الـ HTTP headers و الـ cookies لضمان عدم وجود أي نقاط ضعف.
استخدم أدوات مثل
تحليل:Headers

```
curl -I http://example.com
```

ب. التحقق من إعدادات السياسات الأمنية:
تفحص سياسات أمان المحتوى (CSP) لمنع الـ XSS والـClickjacking
أدوات مثل CSP Evaluator أو SecurityHeaders.io.



.6إنشاء تقرير شامل:
بعد الانتهاء من الفحص واكتشاف الثغرات، عليك تقديم تقرير مفصل يتضمن:
مقدمة: نظرة عامة عن الهدف، الأدوات المستخدمة، والإطار الزمني للفحص.
نتائج الفحص: قائمة بالثغرات المكتشفة مرتبة حسب مستوى الخطورة.
تفاصيل كل ثغرة: شرح كيفية اكتشافها، دليل إثبات المفهوم (PoC)، التوصيات للإصلاح.
الاستنتاج: ملخص عام حول حالة الأمان في الموقع.

تقرير أمني شامل

- قام بتصميم هذا الملف: م/مشاري الشراري

- حسابات التواصل:
  - منصة X: VXV10_Q
  - منصة Threads: _F5X9
- مكان رفع الملف: **GITHUB**

- رابط الملف: **URL**: https://github.com/HACK-MR-B/Target-Analysis