Subdomain Enumeration 1

Sundomain

- يعني ايه اصلا Subdomain طبعا احنا عارفين الDomain ده بقي الSub منو هههههه بهزر
- بص مثلا انت لو عندك موقع زي الفيسبوك بيبقي الدومين بتاعه كده `facebook.com` ده اسمه Domain عادي جدا بص ده كده `mail.facebook.com` `help.facebook.com` `support.facebook.com` كل دول Subdomains بقي
- ده هيفدنا عمتا لما نيجي نهانت علي موقع عشان انا بقدر اجمع معلومات اكتر عن الموقع اللي بهانت عليه وده مهم جده وحتي في Bug Bounty Programs بتشرط عليك انت تجيب اكتر عدد من ال Subdomains وحتي اصلا ممكن تجيب ثغرات فالSubdomain عادي وده بيحصل عادي
- طب هل الSubdomains دول كل صب دومين بيكون ليه Ip زي الدومين الرئيسي اقولك لأ كلهم بيكونو علي سيرفر واحد بنفس الip عن طريق ال Virtual Host اللي درسناه قبل كده والدومين الواحد يقدر يشيل الاف الsubdomains

ازاي نقدر نجمع Subdomains بتاع موقع؟

مواقع

- securitytrails.com
- subdomainfinder.c99.nl
- shrewdeye.app/search
  -ال Subdomains كل دي مواقع تقدر من خلالها تجمع اكتر عدد من

ادوات

Subfinder

```
subfinder -d <website-domain>
subfinder -d facebook.com
subfinder -d facebook.com -all --recursive
```

- بص `-d` اختصار لكلمة Domain
- خلي بالك `recursive` دي يعني يقدر يجبلك subdomain من ال Subdomain `facebook.com` Main Domain

`mail.facebook.com` Subdomain

`api.help.facebook.com` Subdomain of Subdomain

Assetfinder

```
echo "<website-domain>" | assetfinder --subs-only
```

```
echo "mars.com" | assetfinder--subs-only
```