

Subdomain Enumeration 4

Advanced Method with Certificates

- طبعا اتعلمنا طرق كثير عشان نجيب ال subdomains لحد ماز هقتا بس في فكره كويسه برا الصندوق تعالى اقولك عليها
- قبل ما اقولك حبيب اعرفك حاجه اكيد انت عارف ان ال ssl وال tls certs بيكونو خاصين للاسم الشركه او البراند مش للموقع مش فاهم؟ تعالى افهمك
- تخيل معايا لو في شركه اسمها x.com ساعات هيا بيكون عندها a.com و b.com وساعات subdomains ده اكيد بس هنا هما كلهم تحت نفس الاداره او نفس اسم الشركه اللي هو x فا ساعتها كل ال subdomains والمواقع التابعه ليها فا هما كل دول هيكونو ليهم نفس ال ssl cert زي ما قولتلك فوق
- يعني مثلا wikipedia ده اسم الشركه تمام؟ عندها مواقع زي wikipedia.com او wikimedia.com هنا الشهاده لاسم wikimedia مش للموقع اي حاجه تابعه ليك يا باشا تاخد نفس شهادتك

س

ازاي اعرف ابحت عن ال subdomains باستخدام ال certificates

- عندنا موقع جميل اوي اسمه crt.sh ده يا باشا بتحتطلو اسم الشركه اللي واخده الشهاده تعالي هوريك ازاي

www.aa.com		Entrust EV TLS Issuing RSA CA 1	SSL.com TLS RSA Root CA 2022
Subject Name			
Country	US		
State/Province	Texas		
Locality	Fort Worth		
Organization	American Airlines Inc		
Serial Number	332421		
Common Name	www.aa.com		
Business Category	Private Organization		
Inc. State/Province	Delaware		
Inc. Country	US		
Issuer Name			
Country	US		
Organization	SSL Corporation		
Common Name	Entrust EV TLS Issuing RSA CA 1		
Validity			
Not Before	Wed, 07 May 2025 16:48:57 GMT		
Not After	Thu, 07 May 2026 16:58:07 GMT		
Subject Alt Names			
DNS Name	www.aa.com		
DNS Name	aa.com		
DNS Name	aa.com.br		

- دي مثلا شهادة لشركة america airlines بص فوق كده عند خانة ال organization مكتوب فيها اسم الشركه ودي اللي هتكتبها فالسيرش علي موقع crt.sh وهو هيجيبلك اي حاجه مرتبطه بالشركه