Web Application Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

Subdomains enumeration

What is sub-domain enumeration?

- ✓ Subdomain enumeration is the process of identifying **all subdomains for a given domain.**
- ✓ This can be useful for a variety of purposes, such as **identifying potential targets for an attack**, or simply for organizational purposes.
- ✓ It also helps to broader the attack surface, find **hidden applications, and forgotten subdomains**.

✓ Importance of Subdomain:

There are several reasons why you might want to enumerate all subdomains for a given domain:

- To identify potential targets for an attack:
- By enumerating all subdomains, you may be able to find subdomains that are **less well protected than the root domain or the target organization**, making them more vulnerable to attack.

What is sub-domain enumeration?

- **To gain insights into the organization:** Subdomain enumeration can give you insights into how an organization is structured, what services they offer, and so on.
- This information can be valuable when performing reconnaissance for a penetration test or security assessment.

What is sub-domain enumeration?

- **To find misconfigured DNS entries:**

In some cases, organizations may have **misconfigured DNS** entries that reveal sensitive information, such as internal IP addresses.

Why sub-domain enumeration?

- Sub-domain enumeration can reveal a lot of domains/sub-domains that are in scope of a security assessment which in turn increases the chances of finding vulnerabilities
- Finding applications running on hidden, **forgotten sub-domains may lead to uncovering critical vulnerabilities**
- Often times the same vulnerabilities tend to be present across different domains/applications of the same organization

Sub-domain enumeration techniques

- Search engines like **Google and Bing supports** various advanced search operators to refine search queries. These operators are often referred to as “Google dorks”.
- We can use **“site:”** operator in Google search to find all the sub-domains that Google has found for a domain. Google also supports additional minus operator to exclude sub-domains that we are not interested in “**site:*.wikimedia.org -www -store -jobs -uk**”

- **Bing search engine** supports some advanced search operators as well. Like Google, Bing also supports a **"site:"** operator that you might want to check for any additional results apart from the Google search.
- VirusTotal runs its own passive **DNS replication service**, built by storing DNS resolutions performed when visiting URLs submitted by users. In order to retrieve the information of a domain you just have to put **domain name in the search bar**

- **DNSdumpster** is another interesting tools that can find potentially large number of sub-domains for a given domain
- The **OWASP Amass tool** suite obtains subdomain names by scraping data sources, recursive brute forcing, crawling web archives, permuting/altering names and reverse DNS sweeping.

amass --passive -d appsecco.com # Amass 2.x

amass enum --passive -d appsecco.com # Amass 3.x

References

- ✓ https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6
- ✓ https://medium.com/@rajeevranjancom/subdomain-enumeration-2d5c80a14d32

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in