

SUBDOMAIN TAKEOVER



BROKEN LINK HIJACKING



Guide : Mr Kuldeep L M

Jayashankar P _ Spyder 9

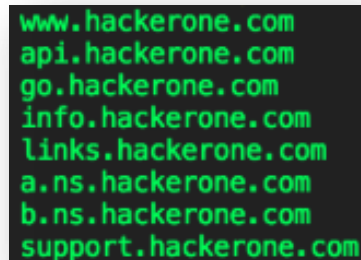
Red Team Intern @ Cyber Sapiens

12.12.2024

SUBDOMAIN TAKEOVER

WHAT IS SUBDOMAIN

A domain that is part of a larger domain in the DNS hierarchy. It's a way to organize and separate different sections of a website under the same main domain, allowing for easy categorization and navigation.



```
www.hackerone.com
api.hackerone.com
go.hackerone.com
info.hackerone.com
links.hackerone.com
a.ns.hackerone.com
b.ns.hackerone.com
support.hackerone.com
```

WHAT IS SUBDOMAIN TAKEOVER

A subdomain takeover is a type of cyber attack where an attacker gains control over a subdomain of a legitimate domain.

This typically occurs when a subdomain is misconfigured or left unmaintained, allowing attackers to exploit orphaned DNS records or expired services.

TESTING FOR SUBDOMAIN TAKEOVER

- ✚ Subdomain Enumeration
- ✚ Identify Service Providers
- ✚ Checking for Dangling DNS Records
- ✚ Attempt to Claim Resources

1. Subdomain Enumeration

Subdomain enumeration is the process of identifying all subdomains associated with a domain. It's a critical process for researchers, security professionals, and enthusiasts who want to: Uncover digital footprints, Strengthen cyber defenses, and Gain insights into web architecture.

Subdomain enumeration can be useful for a variety of purposes, including: Identifying potential targets for an attack, creating a scope of security assessment, Finding forgotten or unattended web applications, and Revealing technical information or data leaks.

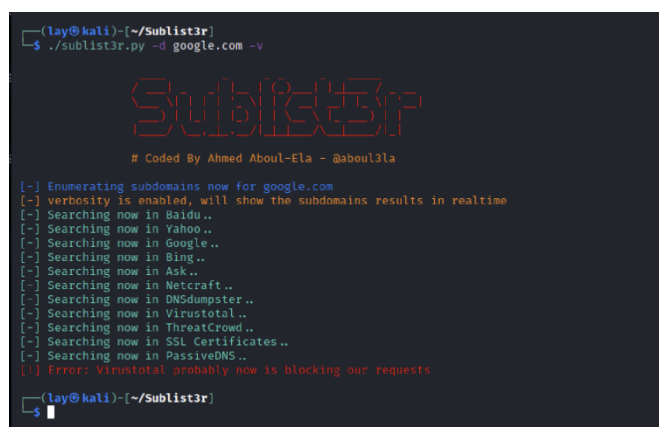
Some tools for subdomain enumeration include:

- **Google Dorking**

A passive technique that uses Google's search operators to find publicly accessible subdomains

- **Sublist3r**

A Python-based tool that uses OSINT to gather information from various search engines and third-party services



```
(lay@kali)~/Sublist3r
$ ./sublist3r.py -d google.com -v

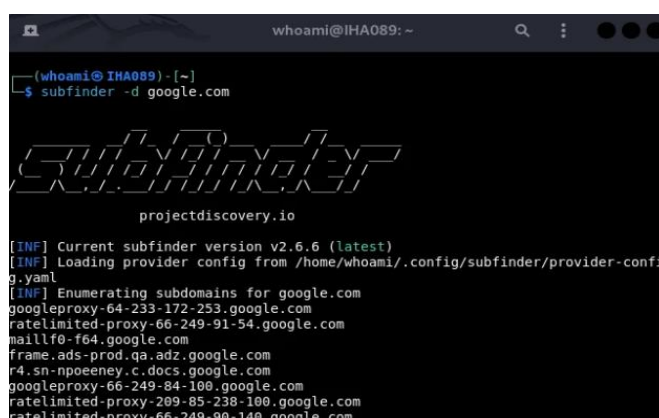
Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[~] Enumerating subdomains now for google.com
[~] verbosity is enabled, will show the subdomains results in realtime
[~] Searching now in Baidu..
[~] Searching now in Yahoo..
[~] Searching now in Google..
[~] Searching now in Bing..
[~] Searching now in Ask..
[~] Searching now in Netcraft..
[~] Searching now in DNSdumpster..
[~] Searching now in VirusTotal..
[~] Searching now in ThreatCrowd..
[~] Searching now in SSL Certificates..
[~] Searching now in PassiveDNS..
[!] Error: VirusTotal probably now is blocking our requests

(lay@kali)~/Sublist3r
$
```

- **Subfinder**

A subdomain discovery tool that uses passive online sources to return valid subdomains for websites



```
(whoami@IHA089)~
$ subfinder -d google.com

Subfinder
projectdiscovery.io

[INF] Current subfinder version v2.6.6 (latest)
[INF] Loading provider config from /home/whoami/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for google.com
googleproxy-64-233-172-253.google.com
ratelimited-proxy-66-249-91-54.google.com
mailf0-f64.google.com
frame.ads-prod.qa.adz.google.com
r4.sn-npoeney.c.docs.google.com
googleproxy-66-249-84-100.google.com
ratelimited-proxy-209-85-238-100.google.com
ratelimited-proxy-66-249-90-140.google.com
```

- **Findomain**

A fast subdomain enumeration tool with a paid version that supports monitoring, integration with nuclei, and reporting

2. Identifying Service Providers

Once subdomains are identified, it's crucial to determine the service providers associated with them. This information can provide insights into the organization's infrastructure and potential vulnerabilities.

Some tools for identifying service providers:

- **WHOIS Lookup:**

Query WHOIS databases to find registrant information, including the hosting provider.



- **DNS Records:**

Analyze DNS records to identify the IP addresses of servers hosting the subdomain.

- **IP Address Lookup:**

Use IP geolocation tools to determine the physical location of the server.

- **Reverse DNS Lookup:**

Find the domain name associated with an IP address.

Type	Name ↑	Value ↑	TTL ↑
A	localhost	192.168.0.1 hosting	4 Hours
A	mail	10.0.0.1 hosting	4 Hours
A	autodiscover	172.16.0.1 hosting	4 Hours
A	whm	198.51.100.1 hosting	4 Hours
A	webdisk	172.31.255.255 hosting	4 Hours

3. Checking for Dangling DNS Records

Dangling DNS records point to nonexistent or removed resources. They can be exploited by attackers to redirect traffic to malicious websites or to launch phishing attacks.

Some tools for Checking for Dangling DNS Records:

- **DNS Lookups:**

Use tools to query DNS servers for the resolution of subdomains.

- **HTTP Requests:**

Send HTTP requests to the subdomain's IP address to check for responses.

- **Web Scraping:**

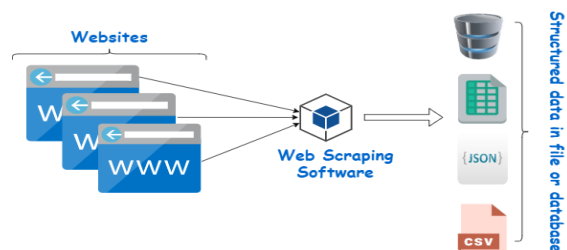
Analyze the website's content to identify links to other subdomains.

```
Microsoft Windows [Version 10.0.17134.472]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\support>nslookup wikipedia.org

Server: UnKnown
Address: 192.168.122.1

Non-authoritative answer:
Name: wikipedia.org
Addresses: 2620:0:863:ed1a::1
          198.35.26.96
```



4. Attempting to Claim Resources

In some cases, attackers may attempt to claim resources associated with subdomains, such as email addresses or domain names. This can be done through phishing attacks, social engineering, or technical exploits.

Some factors to preventing Resource Claims:

- **Strong Password Policies:**

Enforce strong, unique passwords for all accounts.

- **Two-Factor Authentication (2FA):**

Implement 2FA to add an extra layer of security.

- **Regular Security Audits:**

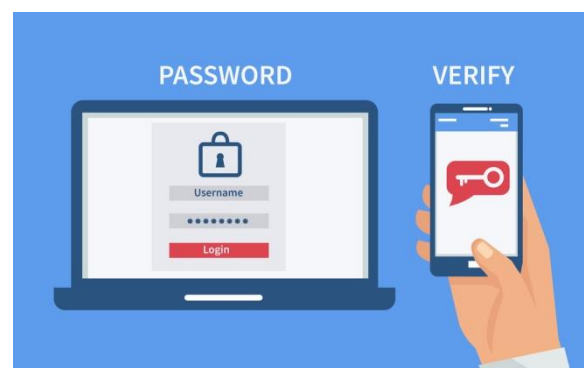
Conduct regular security audits to identify and address vulnerabilities.

- **Monitoring and Alerting:**

Monitor for suspicious activity and set up alerts for potential threats.

- **Staying Informed:**

Keep up-to-date with the latest security threats and best practices.



WHY IS SUBDOMAIN ENUMERATION IMPORTANT ?

- ✚ **Expanding Attack Surface:** By identifying subdomains, attackers can discover additional potential targets for exploitation.
- ✚ **Finding Hidden Services:** Subdomains may host less-known or internal services that might have security vulnerabilities.
- ✚ **Identifying Misconfigurations:** Misconfigurations in subdomain DNS records can lead to information leakage or unauthorized access.

IMPACT OF SUBDOMAIN TAKEOVER

1. Data Breaches:

- ✓ Sensitive Data Exposure: Attackers can access and steal sensitive user data such as personal information, financial details, and login credentials.
- ✓ Data Manipulation: Malicious actors can modify or delete critical data, leading to operational disruptions and financial losses.

2. Reputational Damage:

- ✓ Loss of Trust: A subdomain takeover can erode user trust in the organization's security practices.
- ✓ Brand Tarnish: Malicious content or phishing attacks hosted on the compromised subdomain can damage the organization's reputation.

3. Financial Loss:

- ✓ Direct Costs: Incident response, legal fees, and remediation efforts can incur significant costs.
- ✓ Indirect Costs: Loss of revenue due to decreased customer trust and potential legal liabilities.

4. Further Attacks:

- ✓ Pivot Point: The compromised subdomain can serve as a launchpad for further attacks on the main domain or internal systems.
- ✓ Lateral Movement: Attackers can exploit the compromised subdomain to gain access to other parts of the organization's network.

5. Phishing Attacks:

- ✓ Credential Theft: Attackers can create phishing websites that mimic legitimate services to trick users into revealing their login credentials.
- ✓ Malware Distribution: Malicious content, such as malware or ransomware, can be distributed through the compromised subdomain.

HOW TO MITIGATE THE SUBDOMAIN TAKEOVER ?

- **Inventory Management:**
Up-to-date inventory of all domain names and subdomains, including those registered with third-party services.
- **Use Domain Registrar Security Features:** Enable security features such as DNSSEC (Domain Name System Security Extensions)
- **DNS Record Housekeeping:**
Remove any A, CNAME, or NS records that point to external services that are no longer in use.
- **Regular Security Assessments:**
PenTesting and Vulnerability Scanning, to identify & remediate potential vulnerabilities before they can be exploited by attackers.
- **DNS Configuration Review:**
Ensure proper configuration of DNS records and avoid dangling DNS records.

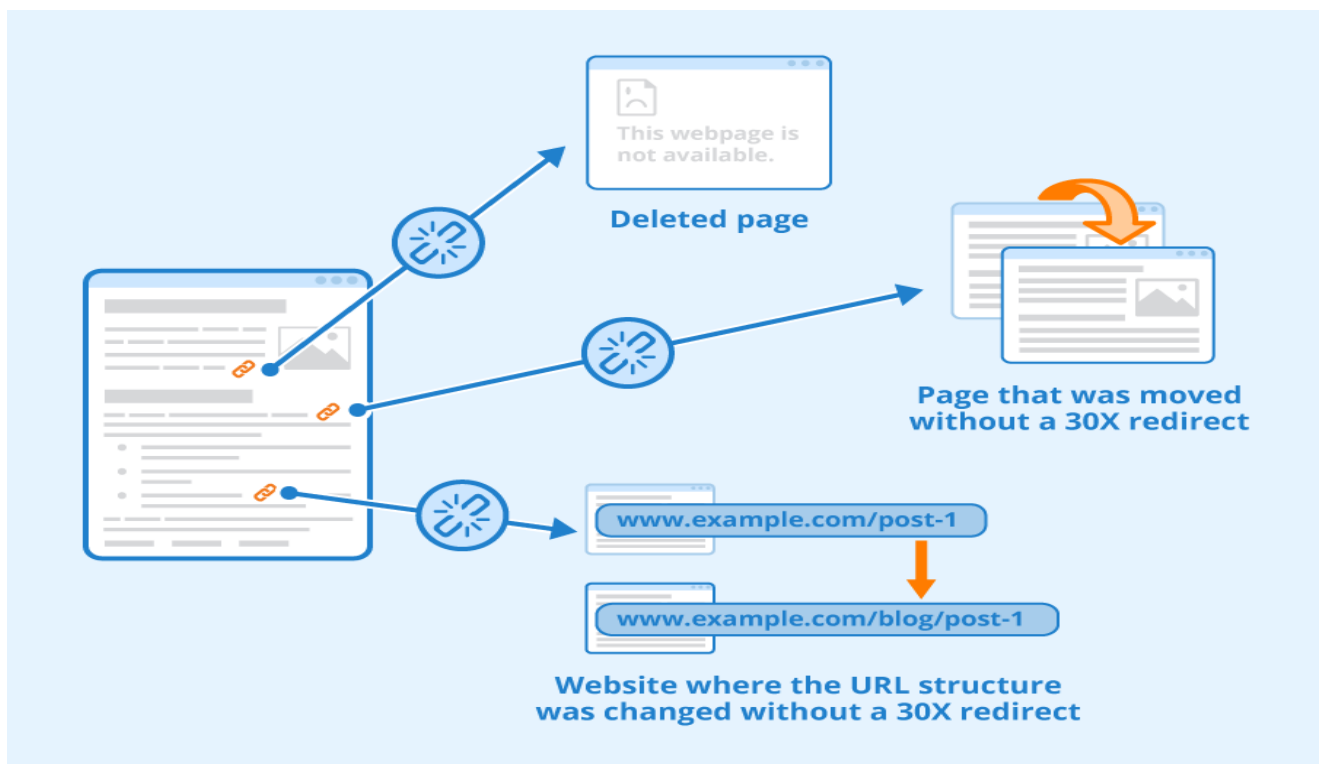
CITATIONS FROM

1. <https://www.hackerone.com/hackerone-community-blog/guide-subdomain-takeovers>
2. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/10-Test_for_Subdomain_Takeover
3. <https://stobes.co/blog/how-to-protect-your-website-from-subdomain-takeovers/>

BROKEN LINK HIJACKING

WHAT IS BROKEN LINK ?

A broken link, also known as a dead link, is a hyperlink that points to a webpage or resource that no longer exists or is unreachable. When you click on a broken link, you typically encounter an error message, most commonly a "404 Not Found" page.



WHAT IS BROKEN LINK HIJACKING ?

Broken link hijacking (BLH) is a type of cyberattack where an attacker takes advantage of invalid external links on a website or web application. These links often point to resources that are no longer available, such as expired domains or deleted pages.

WHY BROKEN LINK HIJACKING IS DANGEROUS ?

Attackers can exploit broken link hijacking to launch a variety of attacks, most commonly to propagate malware or perform phishing using your domain authority. If the attack is specifically targeted at your company, BLH may be used for defacement or impersonation. Finally, BLH can result in stored cross-site scripting.

HOW BROKEN LINK HIJACKING WORKS ?

Expired domains are the cause of the two most popular types of broken link hijacking attacks. These could include domains once owned by an organization or domains belonging to less common redirection/link-shortening services, file hosting services, or content delivery networks (CDNs).

For example, your company could be using an external link-shortening service to improve the user experience by shortening URLs in tweets or LinkedIn posts. If the link shortener goes out of business and loses control of the domain, any published links that utilized this service will stop working. If an attacker then obtains the domain used by the defunct third-party service, they can redirect users to their own harmful sites instead of your original content, for example, to distribute malware. It's worth noting that Twitter and other social media platforms often automatically parse links and provide previews of any visual material, such as a video. As a result, a successful attack may embed offensive content in all of your prior postings in order to deface your brand.

For expired domains that used to belong to your company, the most serious risk is impersonation. If you hold a domain and do not renew its registration, an attacker who takes over that domain may exploit new and existing links that include that domain name to elicit sensitive information via spoofed web pages, conduct phishing attacks based on your reputation, or take over email and social media accounts registered using the expired domain.

XSS attacks are another major risk associated with broken link hijacking. Many websites and web apps use scripts loaded from external sources, including scripts that integrate with an external traffic analyzer (like Google Analytics). If the traffic analyzer company goes out of business or otherwise loses control of its domain, your pages will have a broken JavaScript link. If an attacker then gains control of the traffic analyzer's domain, they will be able to inject malicious scripts that are automatically loaded by your web pages with each visit instead of the analyzer. This results in a stored cross-site scripting attack with potentially significant repercussions.

HOW TO DETECT BROKEN LINKS ?

Broken links, or dead links, can negatively impact your website's security. Here are several methods to detect them:

- ✓ **Visual Check:** Manually click on links on your website to see if they lead to the intended destination.
- ✓ **Review Sitemaps:** Check your XML sitemap for any broken links.
- ✓ **Google Search Console:** This free tool can identify broken links and other website issues.
- ✓ **SEMrush:** Another comprehensive SEO tool that can detect broken links.
- ✓ **Dead Link Checker:** A free online tool that scans your website for broken links.
- ✓ **Dr. Link Check:** Another free tool that checks for broken links, redirects, and other issues.
- ✓ **Check My Links:** A browser extension that highlights broken links on a webpage.

HOW TO BROKEN LINKS IMPACT ?

- **Reputational Damage:** The compromised website can suffer significant damage to its reputation.
- **Financial Loss:** The organization may face financial losses due to lost business, legal fees, and remediation costs.
- **Data Breaches:** Sensitive user data may be exposed if the attacker successfully steals information.
- **Loss of User Trust:** Users may lose trust in the website and its security practices.
- Increased Vulnerability to Phishing Attacks
- Malware Distribution
- SEO Penalties

HOW TO MITIGATE BROKEN LINKS ?

- **Regular Audits:**
To identify and fix broken links. Tools like Screaming Frog SEO Spider, OWASP ZAP, and Google Webmaster Tools can automate this process.
- **Automated Monitoring:**
To alert when a linked domain becomes unavailable or when the domain registration is nearing expiration.
- **Implement Safe Redirects & Error Handling:**
To prevent users from being exposed to malicious content through broken links.
- **404 Page Best Practices:**
To guide users back to safe areas of website, reducing the chance of users navigating to malicious sites.

CITATIONS FROM

1. <https://ahrefs.com/seo/glossary/broken-link>
2. <https://www.semrush.com/blog/broken-link/>
3. <https://www.geeksforgeeks.org/what-is-a-broken-link-identifying-and-fixing-broken-link/>
4. <https://nobleintentstudio.com/blog/why-broken-links-are-bad-for-your-website-and-how-to-fix-them/#:~:text=Broken%20links%20cause%20a%20poor,or%20kept%20up%20to%20date.>

