SUBDOMAIN TAKEOVER

KARTHIK

WHAT IS SUBDOMAIN?

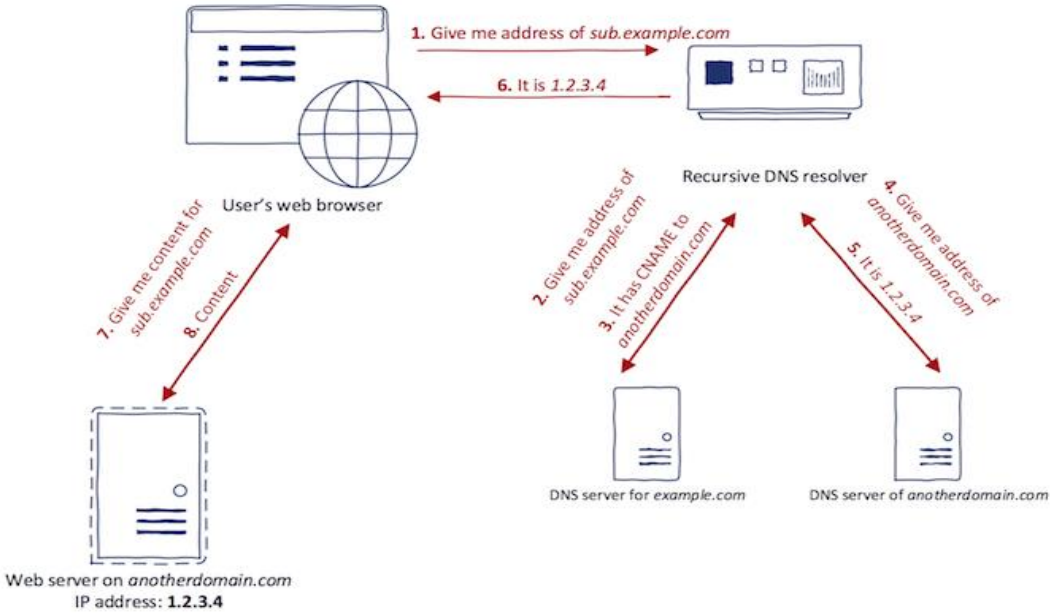
A subdomain is a subset of a larger domain, allowing for further organization and delegation within the domain name system (DNS). It appears as a prefix to the primary domain name, separated by a dot. Subdomains can be used to designate specific sections or services of a website, providing a structured hierarchy for navigation and management. For example, in "blog.example.com," "blog" is the subdomain, typically used to host a blog section separate from the main website content.

WHAT IS SUBDOMAIN TAKEOVER?

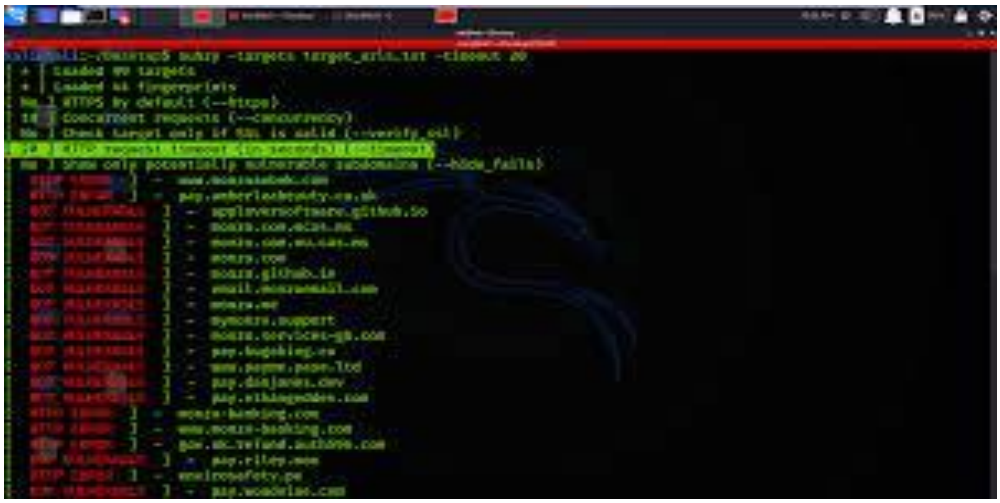
A subdomain takeover occurs when a malicious actor seizes control of a subdomain within a targeted domain. Typically, this occurs when the subdomain is listed in the Domain Name System (DNS) with a canonical name (CNAME) but lacks a host serving content. This situation can arise either because a virtual host has not yet been activated or because it has been removed. Exploiting this vulnerability, an attacker can assume control of the subdomain by establishing their own virtual host and hosting their own content.

By exploiting a subdomain takeover, an attacker can potentially intercept cookies set by the main domain, execute cross-site scripting attacks, or bypass content security policies. This could enable them to gather sensitive information, such as login credentials, or deliver malicious content to unsuspecting users.

To draw an analogy, a subdomain is akin to an electrical outlet. When your own appliance (host) is plugged in, everything functions as intended. However, if the appliance is unplugged or has not been connected yet, someone else could plug in a different appliance. To prevent unauthorized access, it's necessary to disable the outlet at the breaker or fuse box (DNS).



SUBDOMAIN TAKEOVER TOOLS:



- **SubOver:** Identifies potential subdomain takeovers by analyzing CNAME records and other DNS-related information.
- **Sublist3r:** A reconnaissance tool that enumerates subdomains using various techniques like search engine scraping, DNS brute forcing, and certificate transparency logs.
- **Subjack:** Scans for subdomain takeover vulnerabilities by checking for misconfigurations in CNAME and NS records.

- Knock: Uses brute-force techniques to check for subdomain takeovers by testing various DNS records.
- **Nmap:** Although primarily a network mapping tool, Nmap can also discover open ports and services associated with subdomains, aiding in the identification of potential takeover opportunities.
- **Subfinder:** A subdomain discovery tool that can help identify subdomains vulnerable to takeover.
- **Subdomain Takeover Scanner:** A tool developed by EdOverflow for scanning and identifying potential subdomain takeover vulnerabilities.
- **Sub-domain enumeration suite:** A collection of subdomain enumeration tools that can be used for identifying potential takeover opportunities.
- **Subdomain Bruteforcer:** A tool designed to brute force subdomains, which can be useful for discovering potential takeover targets.
- **Massdns:** A high-performance DNS stub resolver that can be used for passive subdomain enumeration, which may uncover potential takeover vulnerabilities.

These tools can aid security professionals and researchers in identifying and mitigating subdomain takeover risks within their organization's domain infrastructure. However, it's crucial to use them responsibly and within legal boundaries.

IMPACTS OF SUBDOMAIN TAKEOVER:

Subdomain takeover can lead to substantial adverse effects on an organization's digital infrastructure, security, and reputation. It's imperative to grasp these potential consequences to implement proactive measures aimed at reducing the associated risks.

Some of the key impacts of subdomain takeover include:

Unauthorized Content or Services: Once a subdomain takeover occurs, attackers can use it to host malicious content or services, such as phishing sites, malware distribution platforms, or other fraudulent activities. Visitors who trust the legitimate domain may unknowingly interact with this malicious content, resulting in potential data breaches, financial losses, or other security incidents.

Data Breaches: Subdomain takeover can lead to unauthorized access to sensitive data or user information. Attackers may exploit the subdomain to deceive users into sharing confidential information like login credentials, personal data, or financial details. This stolen information can be utilized for identity theft, fraud, or other malicious purposes.

SEO and Brand Reputation Damage: Hosting malicious content on a subdomain can harm an organization's search engine rankings and online reputation. Search engines might associate the legitimate domain with malicious activities, diminishing its visibility and trustworthiness. Consequently, this can lead to reduced website traffic and erosion of customer trust.

Phishing and Social Engineering: Attackers often leverage subdomain takeovers to create convincing phishing sites that mimic legitimate services or websites. These fraudulent sites aim to deceive users into divulging sensitive information. The legitimacy added by a subdomain takeover complicates users' ability to differentiate between genuine and fake sites.

Blacklisting and Blocked Services: If a subdomain is identified for malicious activity, it could be blacklisted by security companies, browsers, or email providers. Consequently, legitimate communications, services, or emails linked to the subdomain may be prevented from reaching their intended recipients. Such actions can disrupt business operations and communication channels.

Financial Loss and Legal Consequences: Subdomain takeover incidents can result in financial losses due to data breaches, disrupted services, and potential legal liabilities.

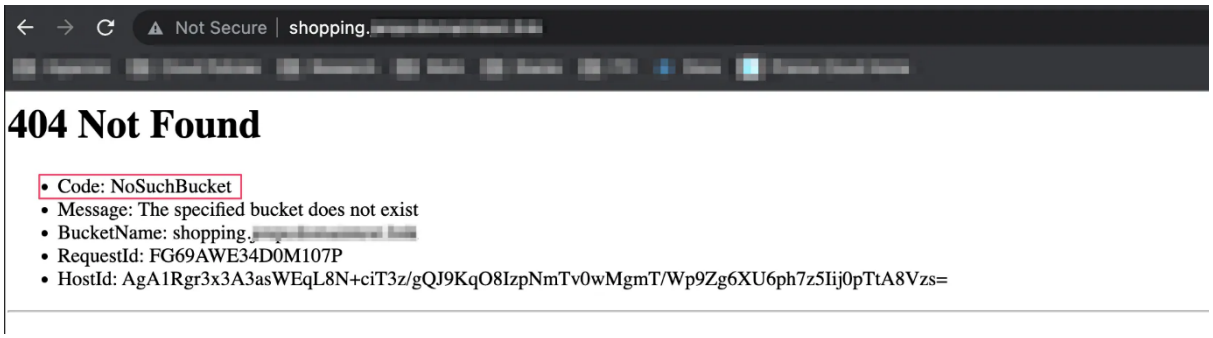
Organizations may face accountability for security breaches and failure to safeguard user data, potentially leading to legal repercussions, regulatory fines, and diminished customer trust.

Loss of Control and Downtime: In cases of subdomain takeover, the legitimate owner forfeits control over the affected digital asset. Attackers can manipulate the subdomain's content, services, or settings, potentially causing downtime, disruptions, and loss of access to vital resources.

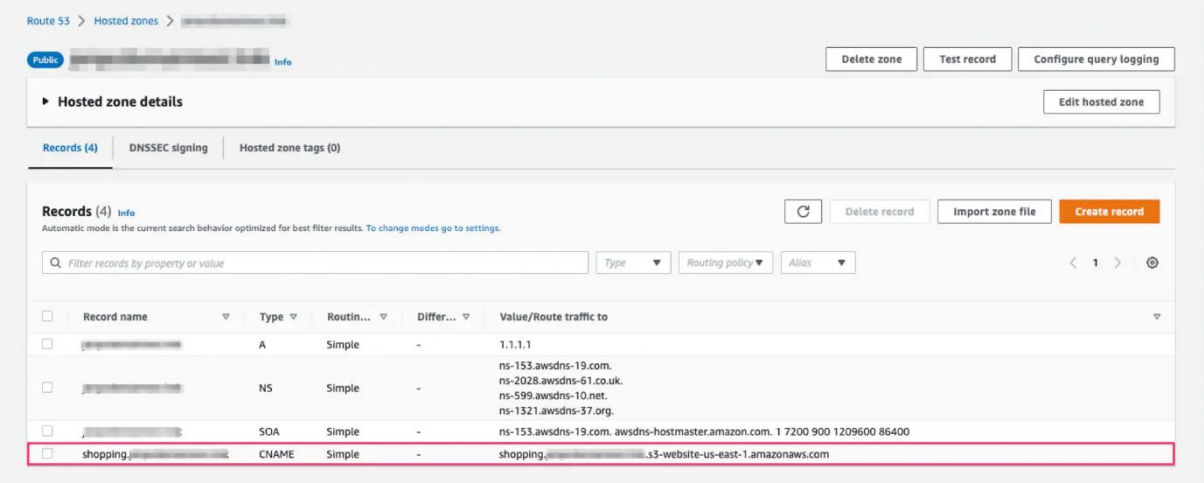
Supply Chain Attacks: If a subdomain takeover impacts a third-party service used by an organization, it can trigger supply chain attacks. Attackers exploit vulnerabilities in the compromised third-party service to compromise the organization's systems, data, or operations.

DETECTION FOR SUBDOMAIN TAKEOVER

Identifying potential subdomain takeover opportunities can be straightforward. For instance, let's consider a scenario where a company employs AWS Route 53 to manage its domain DNS entries. If a subdomain is directed towards a non-existent cloud resource, like an AWS S3 bucket, via its CNAME records, the subdomain will eventually resolve to the S3 bucket endpoint URL. However, since the bucket does not exist, accessing the subdomain will result in a 404 status code accompanied by a generic error message from AWS. This discrepancy in resource availability can signal a potential subdomain takeover opportunity.



This is because the DNS entries were not updated when the bucket was deleted and the CNAME record is still present.



In such a scenario, a subdomain takeover can be exploited by setting up an S3 bucket with an identical name and in the same region. Consequently, the "Route Traffic To" value in the CNAME record will redirect to this newly created S3 bucket. However, unlike the previous case, this S3 bucket is now controlled by an anonymous cloud user, possibly an attacker, rather than the company itself.

Should the anonymous cloud user harbor malicious intentions, they can effectively take over the subdomain until the company identifies the incident and removes the CNAME entry directing traffic to that resource. During this period, the attacker can potentially misuse the subdomain for their own purposes.

MITIGATION FOR SUBDOMAIN TAKEOVER:

Preventing subdomain takeover vulnerabilities necessitates a blend of preventive actions, diligent surveillance, and swift reactions. Adhering to these recommended strategies enables organizations to notably diminish the likelihood of subdomain takeover occurrences.

Key mitigations to consider:

- Regular Subdomain Inventory:
    - Keep an updated list of all subdomains linked to your organization's domain.
    - Document the purpose, owner, and responsible party for each subdomain.
- DNS Monitoring and Cleanup:

    - Regularly check DNS records for subdomains directing to third-party or outdated services.
    - Remove DNS entries for unused subdomains or those associated with terminated services.
- DNS Configuration Best Practices:
    - Set up proper DNS configuration, including CNAME records, to prevent takeover vulnerabilities.
    - Employ robust access controls and authentication methods for DNS management.
- Subdomain Enumeration Tools:
    - Utilize tools like Sublist3r, Amass, and Subfinder to find active subdomains and potential takeover targets.
    - Periodically scan for new subdomains and evaluate their security status.
- Vulnerability Scanning:
    - Conduct routine vulnerability assessments and penetration tests to uncover subdomain takeover risks.
    - Address vulnerabilities promptly based on their severity.
- Collaboration with Third Parties:
    - Communicate with third-party service providers to ensure timely removal of DNS entries for terminated services.
    - Define clear terms for managing subdomains in third-party contracts.
- Subdomain Takeover Scanners:
    - Use automated tools like SubOver and Subjack to detect subdomain takeover vulnerabilities.
    - Regularly scan subdomains for CNAME or NS records pointing to external services.
- Secure Development Practices:
    - Follow secure coding practices when deploying new applications or services using subdomains.
    - Validate and handle user-generated content properly to prevent subdomain takeover.
- Response and Remediation Plan:

    - Create an incident response plan for dealing with subdomain takeover incidents.
    - Define roles and responsibilities for addressing vulnerabilities and security breaches.
- Employee Training and Awareness:
    - Educate employees and users about subdomain takeover and phishing risks.
    - Encourage prompt reporting of suspicious subdomains and activities.
- HTTPS and SSL/TLS:
    - Implement HTTPS for all subdomains to ensure encrypted communication and prevent attacks.
    - Regularly update SSL/TLS certificates to avoid potential vulnerabilities.
- Monitoring and Alerts:
    - Set up monitoring and alerts for DNS changes and subdomain activities to detect unauthorized modifications.
- Backup and Recovery:
    - Maintain backups of critical subdomain configurations and data to aid recovery in case of compromise.
- Patch and Update:
    - Keep software and systems updated to minimize potential vulnerabilities.
- Incident Reporting:
    - Establish clear reporting channels for subdomain takeover vulnerabilities and collaborate with security researchers for responsible disclosure.

REFERENCES:

- https://www.paloaltonetworks.com/blog/prisma-cloud/subdomain-takeover/
- https://medium.com/@aka.0x4C3DD/subdomain-takeover-understanding-the-risks-tools-impact-mitigations-e24f83bd8a59#:~:text=To%20mitigate%20the%20impact%20of,and%20implementing%20strong%20access%20controls.
- https://github.com/martinvw/subdomain-takeover-tools
- https://book.hacktricks.xyz/pentesting-web/domain-subdomain-takeover
- https://developer.mozilla.org/en-US/docs/Web/Security/Subdomain_takeovers
- **https://0xpatrik.com/subdomain-takeover-basics/**