EyeQ Dot Net

LEARN FROM REAL HACKERS

# TASK 8

## Broken Link Hijacking


**ABSTRACT**

This attack leverages the redirection of user traffic intended for legitimate content to malicious destinations. This paper delves into the mechanisms of broken link hijacking, discussing the various methods employed by attackers to identify and manipulate broken links. Furthermore, it explores the potential consequences of such attacks, including the compromise of user privacy, propagation of malware, and the spread of misinformation. The study also highlights preventive measures that web administrators can adopt to mitigate the risks associated with broken link hijacking, emphasizing the importance of regular link maintenance, proactive monitoring, and the implementation of security best practices. In an era where the digital landscape plays a vital role in communication and information dissemination, understanding and addressing the threats posed by broken link hijacking is crucial to maintaining the integrity and security of online content and user experiences.



**SUBMITTED BY**

**BIBITHA V R | 23-08-2023**

# *Report on Broken Link Hijacking*

1. What is open redirection?
2. What are the parameters to look for?
3. Impact of the vulnerability

---

# Introduction:

In the rapidly evolving digital landscape, cyber threats continue to diversify. One such threat gaining prominence is Broken Link Hijacking, which exploits overlooked vulnerabilities in websites. This report delves into the intricacies of Broken Link Hijacking, its methods, potential consequences, and the crucial mitigation strategies that can preserve the integrity of online content and user experiences.

# 1. What is Broken Link Hijacking?

Broken Link Hijacking involves the exploitation of non-functional or outdated links present on websites. Attackers manipulate these links to redirect user traffic to unintended, often malicious, destinations. This process leverages the unnoticed digital footprints that are left behind by abandoned or forgotten web assets. Broken Link Hijacking capitalizes on the trust users place in legitimate websites, leading to unauthorized access and potential security breaches.

# 2. Various Methods to Find This Bug:

Detecting Broken Link Hijacking requires a comprehensive understanding of website architecture and vulnerability identification. Attackers employ several methods to exploit broken links, including:

**a) Crawling and Scanning:** Attackers use automated tools to scan websites for inactive links, identifying entry points for their malicious activities.

**b) Link Poisoning:** Attackers manipulate URLs in previously broken links to direct users to malicious domains, tricking users and search engines alike.

**c) Domain Expiry**: Expired domain names, once linked to a website, can be acquired by attackers to redirect traffic to their own destinations.

**d) Third-party Compromise:** Attackers compromise third-party links embedded on websites, leading to redirection of users to their intended destinations.

# 3. Impact and Mitigation:

The repercussions of Broken Link Hijacking are multifaceted and potentially severe:

**a) Privacy Breaches**: User data can be harvested on malicious sites, leading to privacy breaches and identity theft.

**b) Malware Dissemination**: Malicious content can be injected into the hijacked links, spreading malware among unsuspecting users.

**c) Reputation Damage:** Website credibility can be compromised, leading to a loss of user trust and potential business repercussions.

To mitigate Broken Link Hijacking risks, several proactive measures can be adopted:

**a) Regular Link Maintenance**: Periodic scanning and fixing of broken links can thwart potential attackers.

**b) Vigilant Monitoring:** Implement continuous monitoring systems to promptly identify and respond to broken link hijacking attempts.

**c) Security Best Practices:** Employ security mechanisms like HTTPS, strong authentication, and access controls to fortify your website.

# Conclusion:

Broken Link Hijacking poses a significant threat in the modern digital landscape, with potentially devastating consequences for both users and website owners. By understanding its methods, impacts, and mitigation strategies, individuals and organizations can take proactive steps to safeguard their digital assets and ensure a safer online experience for all.

# References:


- https://www.upguard.com/
- https://www.ecpi.edu/
- https://www.simplilearn.com/
- https://www.sans.org/in_en/
- https://portswigger.net/