Volume 2 Issue 21

Date: 01.02.2026

Cybersecurity Digest

Bi-Weekly update by O/o CISO of Meghalaya Rural Bank

URL Poisoning

In today's hostile Internet, URL poisoning poses a significant threat to web users, their computers, and their data. This malicious technique—also known as URL manipulation attack, URL redirection attack, or URL interpretation attack—allows attackers to deceive users to the true destination of a URL by altering that URL to redirect them to harmful websites. By understanding how URL poisoning works, its impact on businesses, and preventive measures, you can safeguard yourself and your user population against a wide variety of impacts.

Most URLs are human-readable because they begin with a fully-qualified domain name (FQDN) such as "search.google.com." Even to an inexperienced reader, this FQDN is mostly understandable as being the Google search page. As such, we might ignore the rest of the URL and simply trust it based on the domain or FQDN.

URL poisoning is a cyberattack method where attackers modify URLs to manipulate user behaviour or access unauthorized resources. By changing parameters, fragments, or domain names, attackers can redirect users to phishing sites, install malware, or steal sensitive information. This technique exploits the trust users place in familiar web addresses, making it difficult to detect and prevent.

A variation of URL poisoning is search engine poisoning, or SEO poisoning. Cybercriminals optimize their malware-laden pages to get them to the top of search engine results where users can only see the beginning of the URL and not the query strings.

How Does URL Poisoning Happen?

URL poisoning often begins with attackers identifying vulnerabilities or predictable patterns within web applications. By exploiting these weaknesses, attackers can modify URL parameters to bypass security mechanisms or inject malicious code.

For instance, if a URL carries user data or session information as part of its structure, altering these details might grant unauthorized access to service areas or confidential data. Attackers may employ social engineering tactics, sending doctored links under the guise of trusted sources. This manipulation may include altering path segments, query strings, or exploiting poorly configured URL shorteners, making their malicious intent hidden or seemingly benign.

Techniques such as URL encoding or obfuscation tools might also be used to disguise the true nature of the changes, leaving users unaware of the impending danger.

Contd...

Small URL Changes, Big Cybersecurity Impacts

Understanding URL poisoning and its implications is crucial for maintaining a secure online environment. By addressing vulnerabilities, businesses can protect their data, reputation, and customers from the damaging effects of URL manipulation

How URL Poisoning Impacts Your Business

URL poisoning via phishing inside email, SMS, or other messaging application is frequently used as the initial exploit to gain access inside of a larger attack campaign. As such, it can lead to severe consequences for businesses. It compromises user trust, damages brand reputation, and exposes sensitive information. Customers may fall victim to phishing attacks, leading to financial losses and identity theft. Furthermore, businesses may face legal repercussions and regulatory fines for failing to protect user data. The financial and reputational damage caused by compromises that are aided by URL poisoning can be devastating, underscoring the need for proactive measures.

Without proper awareness and defense mechanisms, businesses and individuals are left vulnerable to the myriad threats URL poisoning introduces.

URL redirection attacks can also be a form of URL poisoning. Sometimes, web applications are built as a redirect URL to collect user metrics with the real destination in a query string field. The user is then redirected on to the real destination. This is very common in marketing campaigns.

Examples of URL Poisoning

URL shortening services are widely used and very popular. Users can submit a URL and receive a shorter version that is easier to share in messaging applications. However, they use URL poisoning by design. When someone clicks on the shortened URL, the service redirects them to the original destination. However, recipients cannot determine the final destination from the shortened URL alone, which can allow malicious URLs to be concealed.

In a different scenario, an attacker registers a domain that closely resembles a well-known website. They then design a URL that appears authentic but directs unsuspecting users to a phishing page. By altering parameters, such as usernames or account numbers in URLs, attackers can access confidential user data or administrative controls.

Preventing URL Poisoning

Preventing URL poisoning involves a comprehensive approach to web and messaging security.

Implementing Protective DNS (Domain Name System) is a robust strategy to safeguard against URL poisoning to protect endpoints such as desktops, laptops, and mobile devices. Protective DNS helps mitigate threats by filtering out malicious domains and preventing users from inadvertently connecting to harmful websites. This is accomplished by monitoring DNS queries and applying security policies in real-time, thereby thwarting access to potentially dangerous sites before any damage can occur.

It is essential to implement strong input validation and output encoding practices in web applications to ensure that URLs and the inputs inside of them are properly sanitized and cannot be altered or used in redirects. This reduces the risk that your web applications could be used in URL poisoning attacks.

Educating employees and users on the risks associated with URL manipulation is also vital. Encouraging vigilance when interacting with unfamiliar URLs or operating system popups can prevent potential threats.

By employing these strategies, organizations can significantly reduce the risk of URL poisoning