

Sri Lanka Institute of Information Technology



Bug Bounty Report - 03

Module: IE2062

Web Security

Year 2, Semester 2

Aazaf Ritha. J – IT23151710

B.Sc. (Hons) in Information Technology

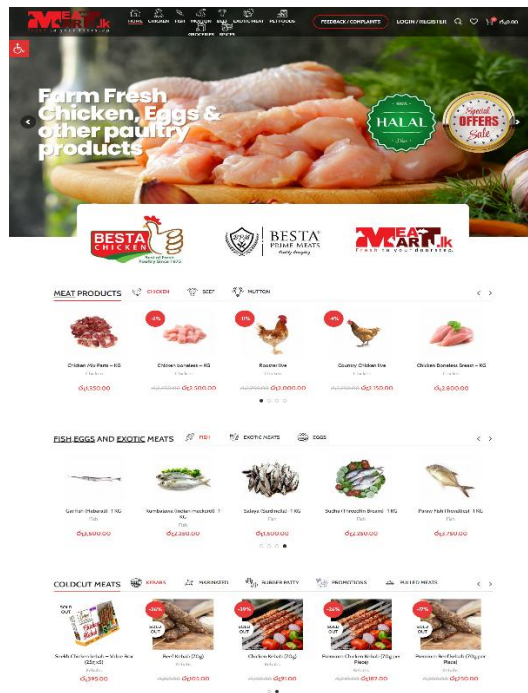
Specialized in Cyber Security

Table of Contents

| | |
|--------------------------------------|----|
| Introduction | 3 |
| Vulnerability Title | 5 |
| Description..... | 6 |
| Affected Component..... | 7 |
| Impact Assessment | 8 |
| Steps to Reproduce..... | 9 |
| Proof of Concept (Screenshots) | 10 |
| Proposed Mitigation or Fix..... | 13 |
| Conclusion..... | 14 |

Introduction

This report outlines a vulnerability discovered on a Sri Lankan e-commerce website, <https://meatmart.lk>. During security testing, a Clickjacking vulnerability was identified on multiple pages of the site. The issue was confirmed through both manual and automated methods, and this report provides technical details, reproduction steps, and mitigation recommendations.



Meat Mart Sri Lanka
Farm Fresh Chicken, Eggs & other poultry products

HALAL **Special Offers**

MEAT PRODUCTS

| CHICKEN | EGG | HUTTON |
|-------------------------|--------------------------|--------------------------|
| Chicken Hot Sale - 450g | Chicken Breast - 450g | Chicken Drumstick - 450g |
| Chicken Breast - 450g | Chicken Drumstick - 450g | Chicken Breast - 450g |

FISH EGGS AND EXOTIC MEATS

| FISH | EXOTIC MEATS | EGG |
|-----------------------|-----------------------|-----------------------|
| Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g |

COLD CUT MEATS

| MEAT | EGG | MEAT | EGG |
|-----------------------|-----------------------|-----------------------|-----------------------|
| Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g |

Best prices in Sri Lanka for Meat and Fish Products

Experience the ultimate value for your money with the best prices in Sri Lanka. Our high quality meat and fish products are delivered to your doorstep with a commitment to quality and freshness. We offer a wide range of products at competitive prices, ensuring you get the best value for your money.

Our Commitment:
At Meat Mart Sri Lanka, we are committed to providing you with the highest quality meat and fish products. We source our products from trusted suppliers and ensure they are delivered to you in the best condition possible. We also offer a wide range of products at competitive prices, ensuring you get the best value for your money.

Consistency and Delivery:
We understand that consistency and delivery are key to your satisfaction. We ensure that our products are delivered to you on time and in the best condition possible. We also offer a wide range of products at competitive prices, ensuring you get the best value for your money.



VIEW MORE **WIDGET VIDEO**

GROCERIES

| MEAT | EGG | MEAT | EGG | MEAT | EGG |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g | Chicken Breast - 450g |

LATEST FROM THE BLOG AND RECIPES

Read the latest news from our blog

| | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Authentic Sri Lankan Chicken Curry Recipe - A Taste of Tradition</p> <p>Discover the secrets of this traditional Sri Lankan dish, featuring tender chicken and aromatic spices. Perfect for a family meal or a special occasion.</p> <p>READ MORE</p> | <p>Catering to Your Tummy: A Guide to Choosing the Right Pet Food</p> <p>Learn how to choose the best pet food for your furry friend. We cover everything from nutrition to ingredients, ensuring your pet stays healthy and happy.</p> <p>READ MORE</p> | <p>The Incredible Nutritional Powerhouse: Eggs and Their Many Health Benefits</p> <p>Eggs are a versatile and nutritious food that can be part of a healthy diet. Discover the many health benefits of eggs and how to incorporate them into your meals.</p> <p>READ MORE</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | | |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <p>YOUR ORDER</p> <p>Thank you for your order. We will process it as quickly as possible and deliver it to you.</p> | <p>WE CONFIRM</p> <p>We confirm your order and will deliver it to you as soon as possible.</p> | <p>DELIVERY AND PAYMENT</p> <p>We offer a wide range of delivery options and payment methods to suit your needs.</p> |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|

MEAT MART SRI LANKA

LOGO LINKS

PRODUCT RANGE

CONTACT DETAILS

LOCATIONS

SECURE DELIVERY

Vulnerability Title

Title – Clickjacking Vulnerability

Risk Level- Medium

Domain - <https://meatmart.lk/>

Description

Clickjacking is a type of attack where a malicious website can trick a user into interacting with a page element (like a button or link) on a website that the user is unaware of. This can be done by embedding the legitimate website inside an iframe or another HTML element, which the attacker controls. The attacker may then "overlay" transparent or misleading elements over the embedded content, making it appear as if the user is clicking on a harmless interface, while in reality, they are triggering actions on the legitimate website. The vulnerability arises when a website allows itself to be embedded within an iframe without protections in place to prevent this behavior. In particular, Clickjacking attacks can exploit the absence of security headers like **X-Frame-Options** or **Content-Security-Policy (CSP)** that are designed to prevent websites from being embedded in iframes. The main risk of a clickjacking attack is that it can lead to unintended actions, such as unwitting users performing actions on behalf of the attacker (e.g., changing account settings, transferring money), or exposing sensitive data by tricking users into interacting with hidden elements. This vulnerability relates to **OWASP Top 10 A05:2021 – Security Misconfiguration**, as it stems from insufficient or missing security configurations that allow dangerous behaviors like iframe embedding, which should be explicitly disallowed.

Affected Component

Web Application: The vulnerability primarily affects web application or sites that allow their content to be embedded within an iframe without any restrictions.

/cart/

/blog/

/category/

/compare/

Browser Security Features: The vulnerability depends on whether the website implements the necessary security headers, such as **X-Frame-Options** or **Content-Security-Policy**.

Embedded Content (iframe): The use of **iframes** without proper security controls is the primary attack vector.

Impact Assessment

User Trust Erosion: If an attacker successfully carries out a clickjacking attack, it can undermine user trust in the affected website, as the user may unknowingly perform actions that harm their account or data.

Account Takeover: Clickjacking can lead to **unauthorized actions** like changing account settings, performing financial transactions, or enabling malicious configurations, which can lead to account takeovers or financial losses.

Loss of Sensitive Data: In some cases, the attacker might collect sensitive information if the victim interacts with the page unintentionally, leading to data breaches.

Reputation Damage: A website with clickjacking vulnerabilities can cause severe damage to its reputation and cause legal and compliance-related issues, especially if personal or financial data is involved.

Malicious Actions: Potential actions that can be performed unknowingly by the victim include:

- Clicking "Like" or "Share" on social media without realizing it.
- Unsubscribing from services.
- Modifying profile settings or making purchases.

Steps to Reproduce

Step 01: Identify the Target Website:

Identify the website that does not implement any clickjacking protection, particularly those that allow their pages to be embedded in an iframe.

- <https://meatmart.lk/>

Step 02: Create a Malicious Page:

Create an HTML page with an embedded iframe targeting the vulnerable site

```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4  <meta charset="UTF-8">
5  <meta name="viewport" content="width=device-width, initial-scale=1.0">
6  <title>Clickjacking Attack</title>
7  </head>
8  <body>
9  <h2>Clickjacking Test</h2>
10 <button onclick="alert('You clicked the button!')">Click Me</button>
11 <iframe src="https://meatmart.lk/" width="800" height="400"></iframe>
12 </body>
13 </html>
```

Step 03: Trigger the Attack:

When a user visits the malicious page, they will see the "Click Me!" button. However, clicking the button will actually trigger a click event on the vulnerable website embedded in the iframe, such as making an unintended purchase or changing account settings.

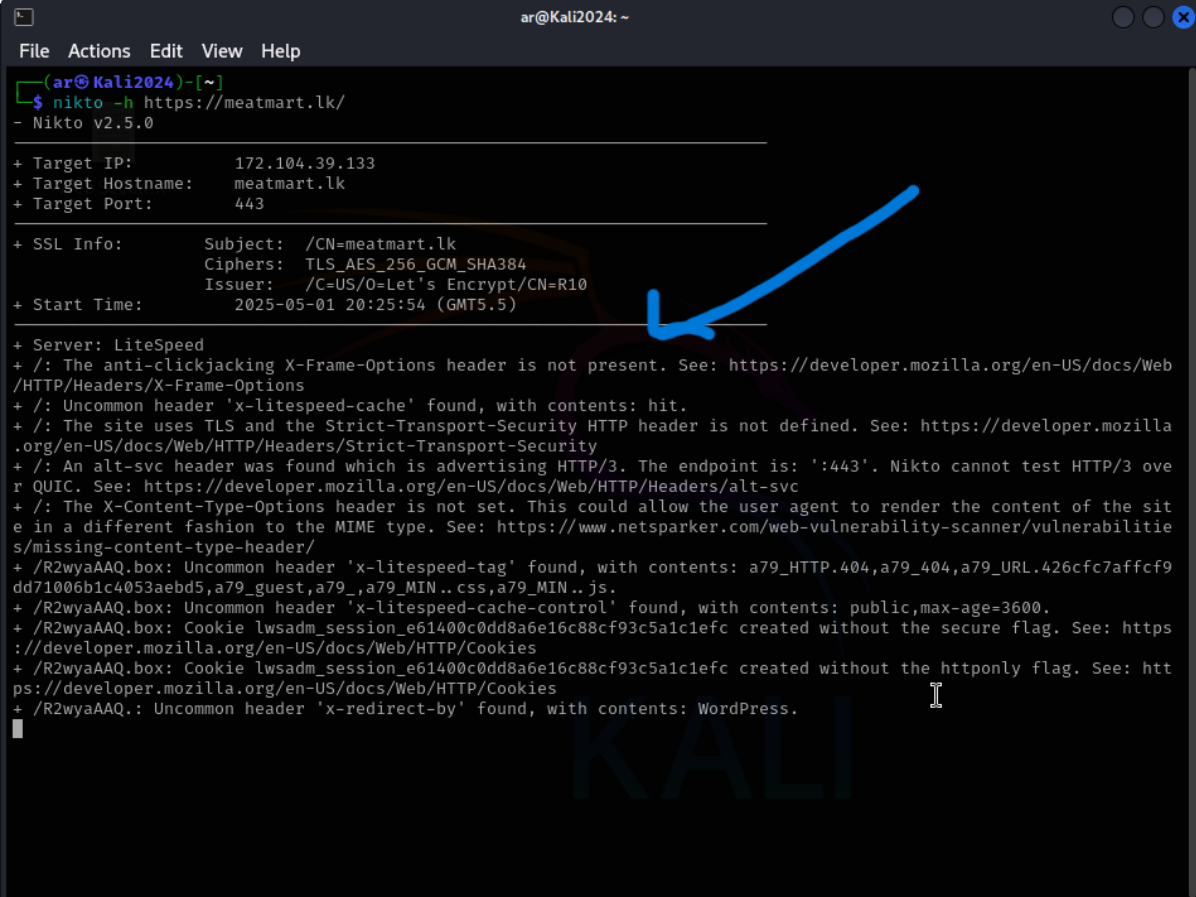
Step 04: Verify the Action:

Verify that the user performs the action on the underlying iframe (such as submitting a form or clicking a link) without realizing it.

Proof of Concept (Screenshots)

Nikto Scan

This screenshot shows the output of a Nikto scan against <https://meatmart.lk>. The scan reveals that the X-Frame-Options header is missing, confirming that the site does not implement basic protection against iframe-based attacks like Clickjacking.



```

ar@Kali2024: ~
File Actions Edit View Help
(ar@Kali2024)-[~]
$ nikto -h https://meatmart.lk/
- Nikto v2.5.0

+ Target IP: 172.104.39.133
+ Target Hostname: meatmart.lk
+ Target Port: 443

+ SSL Info: Subject: /CN=meatmart.lk
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=Let's Encrypt/CN=R10
+ Start Time: 2025-05-01 20:25:54 (GMT5.5)

+ Server: LiteSpeed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-litespeed-cache' found, with contents: hit.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /R2wyaAAQ.box: Uncommon header 'x-litespeed-tag' found, with contents: a79_HTTP.404,a79_404,a79_URL.426cfc7affcf9dd71006b1c4053aebd5,a79_guest,a79_,a79_MIN..css,a79_MIN..js.
+ /R2wyaAAQ.box: Uncommon header 'x-litespeed-cache-control' found, with contents: public,max-age=3600.
+ /R2wyaAAQ.box: Cookie lwsadm_session_e61400c0dd8a6e16c88cf93c5a1c1efc created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /R2wyaAAQ.box: Cookie lwsadm_session_e61400c0dd8a6e16c88cf93c5a1c1efc created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /R2wyaAAQ.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
  
```

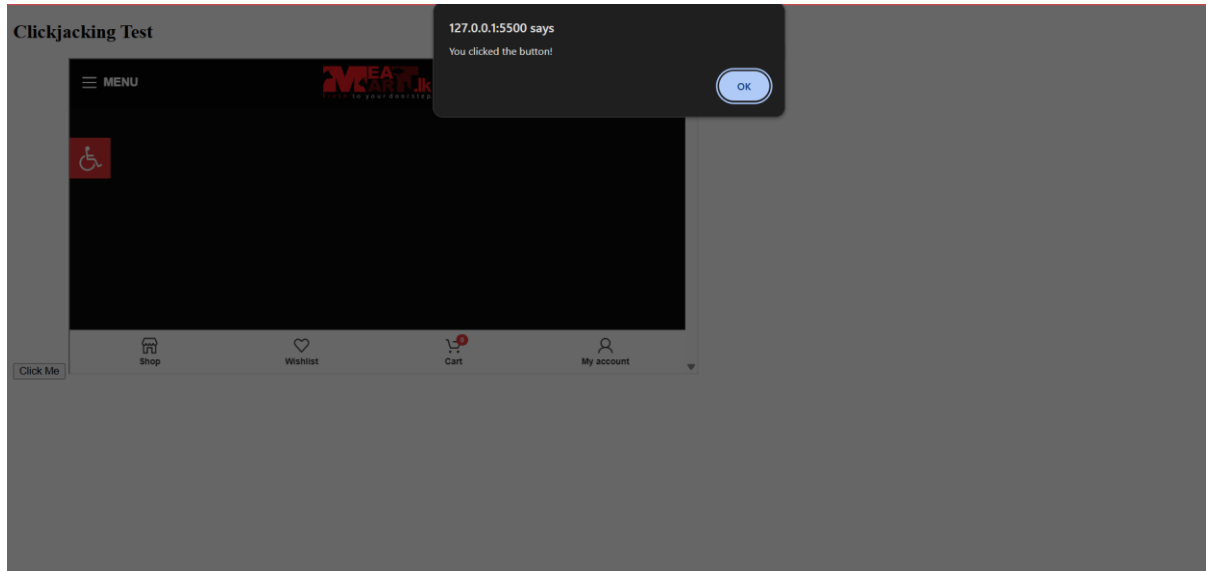
OWASP ZAP scan

The OWASP ZAP scan result highlights the absence of both X-Frame-Options and Content-Security-Policy headers. This indicates the website does not restrict where its content can be embedded, making it vulnerable to Clickjacking.



Manual Verification via iframe (Browser Screenshot)

This screenshot demonstrates a live test in which <https://meatmart.lk> is embedded inside an iframe on a separate domain. The site loads successfully, confirming that it can be iframed without restriction—validating the Clickjacking vulnerability.



Used Malicious code

```
<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Clickjacking Attack</title>

</head>

<body>

<h2>Clickjacking Test</h2>

<button onclick="alert('You clicked the button!')">Click Me</button>

<iframe src="https://meatmart.lk/" width="800" height="400"></iframe>

</body>

</html>
```

Proposed Mitigation or Fix

To mitigate the **Clickjacking** vulnerability, the following steps should be implemented:

Use X-Frame-Options Header:

This header can be used to prevent the website from being embedded in an iframe. Set the header to **DENY** or **SAMEORIGIN**:

- **DENY**: Prevents the page from being embedded in any iframe.
- **SAMEORIGIN**: Allows the page to be embedded only within iframes from the same origin.

Use Content-Security-Policy (CSP):

The **CSP** header provides an additional layer of protection. The frame-ancestors directive can be used to control where your content can be embedded.

JavaScript Clickjacking Protection:

Implement client-side defenses, such as using JavaScript to detect if the page is being loaded inside an iframe. If it is, you can force the top-level window to navigate to your site.

Test for Vulnerabilities:

Use security tools like **OWASP ZAP** or **Burp Suite** to test your website for potential clickjacking vulnerabilities. Additionally, running a **penetration test** periodically can help ensure that your site remains protected.

Conclusion

The Clickjacking vulnerability identified on <https://meatmart.lk> poses a moderate risk to users and the site's reputation. Without proper frame restrictions, attackers can exploit this flaw to trick users into performing unintended actions. This type of issue is associated with "**Security Misconfiguration**," which is listed in the OWASP Top 10 most critical web application security risks. Immediate implementation of security headers like X-Frame-Options and Content-Security-Policy is recommended to mitigate this issue and improve the site's overall security posture.