Cybersecurity Investigation Report

Investigation & Mitigation of a Brand-Impersonating Website

Target Domain: https://tapron.shop/

Investigator: Keyuar Bhelonde

Date: 21 May 2025

# Table of Contents

1. Executive Summary

2. Objective

3. Methodology

4. Evidence Collected

5. Analysis

6. Technical Breakdown

7. Threat Intelligence Correlation

8. Mitigation & Recommendations

9. Conclusion

# 1. Executive Summary

This investigation confirms that the domain https://tapron.shop/ is a brand-impersonating phishing website that mimics the legitimate Tapron brand (https://www.tapron.co.uk). The website contains suspicious meta tags, poorly structured content, misleading titles, and abnormal behavior, indicating potential fraudulent or phishing intent.

# 2. Objective

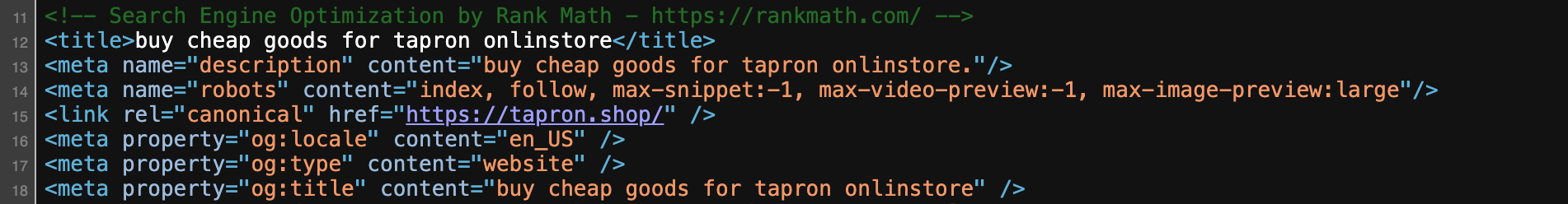
Identify and confirm if tapron.shop impersonates a legitimate business.  
 Collect technical and behavioral indicators of compromise.  
 Recommend actions to mitigate the threat and inform the brand.

# 3. Methodology

1. Passive Reconnaissance – WHOIS, DNS records  
2. Active Analysis – HTTP headers, meta tags, redirects  
3. OSINT Tools – VirusTotal, Netcraft  
4. Comparison – Visual and structural differences with real Tapron site  
5. Mitigation – Report to trusted sites

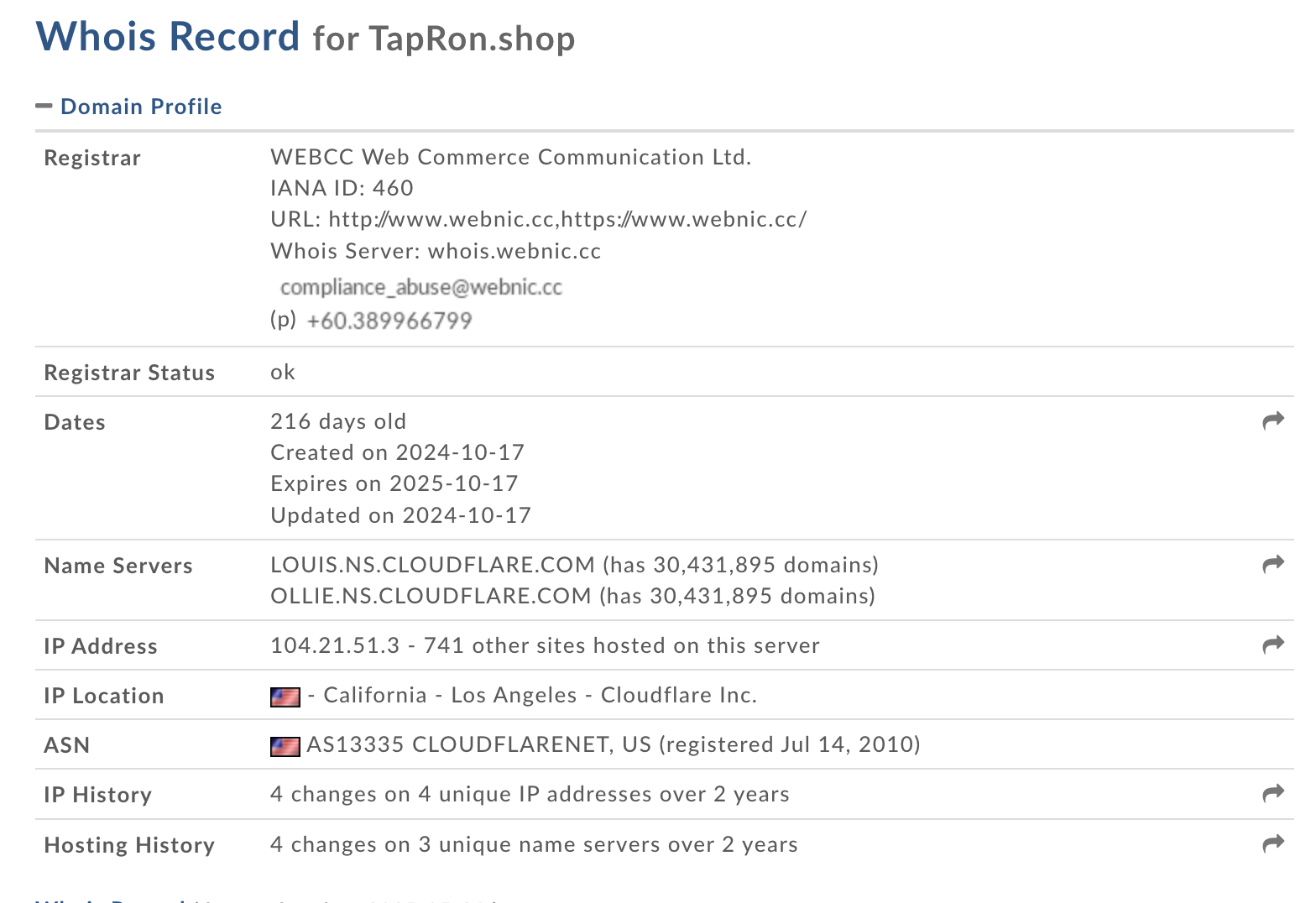
# 4. Evidence Collected

**4.1 Suspicious Meta Title & Description**



* Spelling error in "online store"
* Phrase “purchase premium products” is overly generic, unprofessional, and inconsistent with Tapron’s established brand standards.
* Shows minimally configured or cloned template, typical in phishing toolkits.

**4.2 DNS & IP Details:**



**4.2.1. Suspicious Registrant Details**

* **Name: *Carol Stewart* , no verified connection to the official Tapron UK brand.**
* **Address:** 2767 Walnut Dr, Bismarck, ND 58237 — real street name but possibly potentially fabricated data.
* **Country Code: AS —** this refers to *American Samoa*, but it's likely used incorrectly or spoofed.
* **Phone Number:** Starts with +00 invalid international dialing code. Also includes an Indian-looking number pattern (91…).

**Red Flag:** Obfuscated or fake WHOIS data indicative of malicious intent.

**4.2.2. Registrar Choice**

* **Registrar**: WEBCC (WebNIC.cc), a **Malaysia-based registrar** often used by **low-reputation** domains and phishing actors due to weak vetting and abuse handling.

**Red Flag**: Registrar with **low abuse responsiveness**, often linked to suspicious activity.

**4.2.3. Recent Domain Creation**

* **Created On**: October 17, 2024
* **Age**: Only **216 days old**

**Red Flag**: Most phishing domains are **newly registered** and used quickly to exploit victims before takedown

**4.2.4. Invalid Country / Contact Format**

* “AS” (Country) and “+00” (Phone) are **invalid or intentionally wrong** entries.
* No organization name or legal entity listed for the domain ownership.

**Red Flag**: WHOIS entries likely auto-generated or faked — indicative of fraudulent domain behavior.

**4.2.5. Cloudflare Masking Real Hosting Server**

* A and AAAA records:

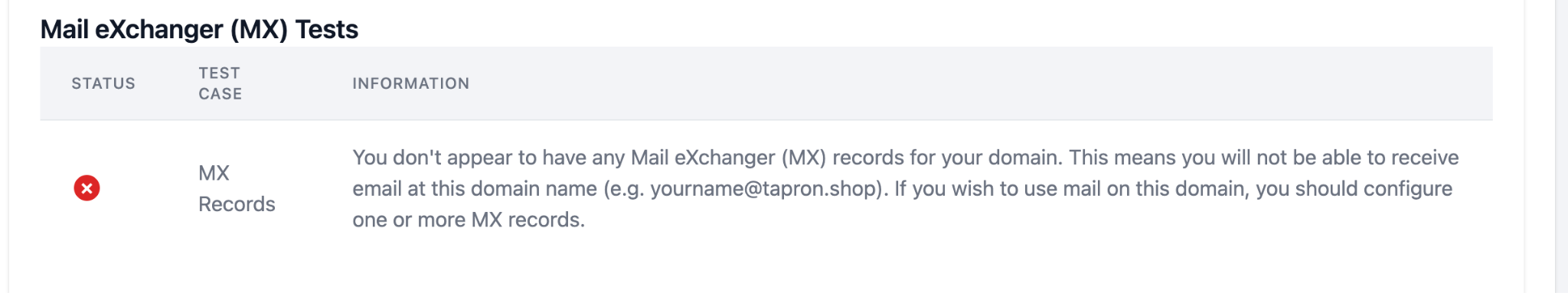
IPv4: 172.67.215.123, 104.21.51.3

IPv6: 2606:4700:3037::ac43:d77b, 2606:4700:3031::6815:3303

* All point to **Cloudflare**, meaning the **origin IP is hidden**.
* **Red Flag**: While many legitimate sites use Cloudflare, phishing sites often use it to obfuscate hosting origins and evade detection.

**4.3 DNS Report :**

**4.31.Missing MX Records**

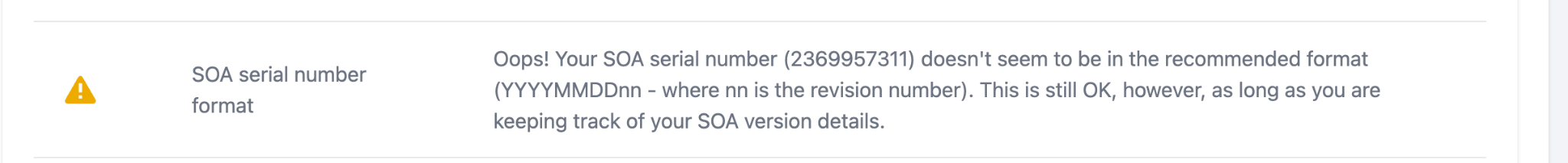
****

* Implication: No mail exchanger (MX) records are present.
* **Implication**:

The domain cannot send or receive email, which is highly atypical for a genuine e-commerce platform.

**Red Flag**: This is a **critical anomaly** that indicates potential fraud or impersonation.

**4.3.2. SOA Serial Number Format Not Standard**

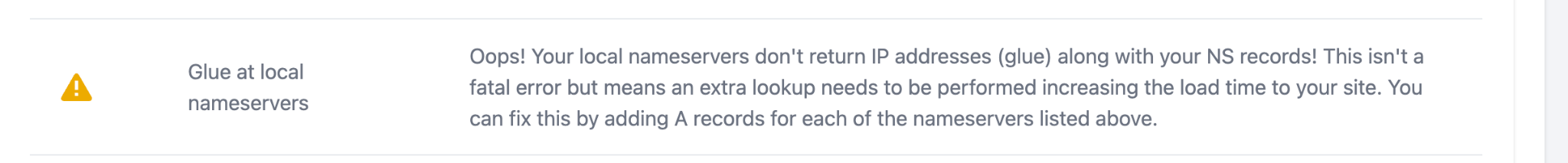
****

* **SOA Serial**: 2369957311 does **not follow the recommended** YYYYMMDDnn **format**.
* **Implication**:

Could indicate improper DNS setup or lack of professional maintenance.

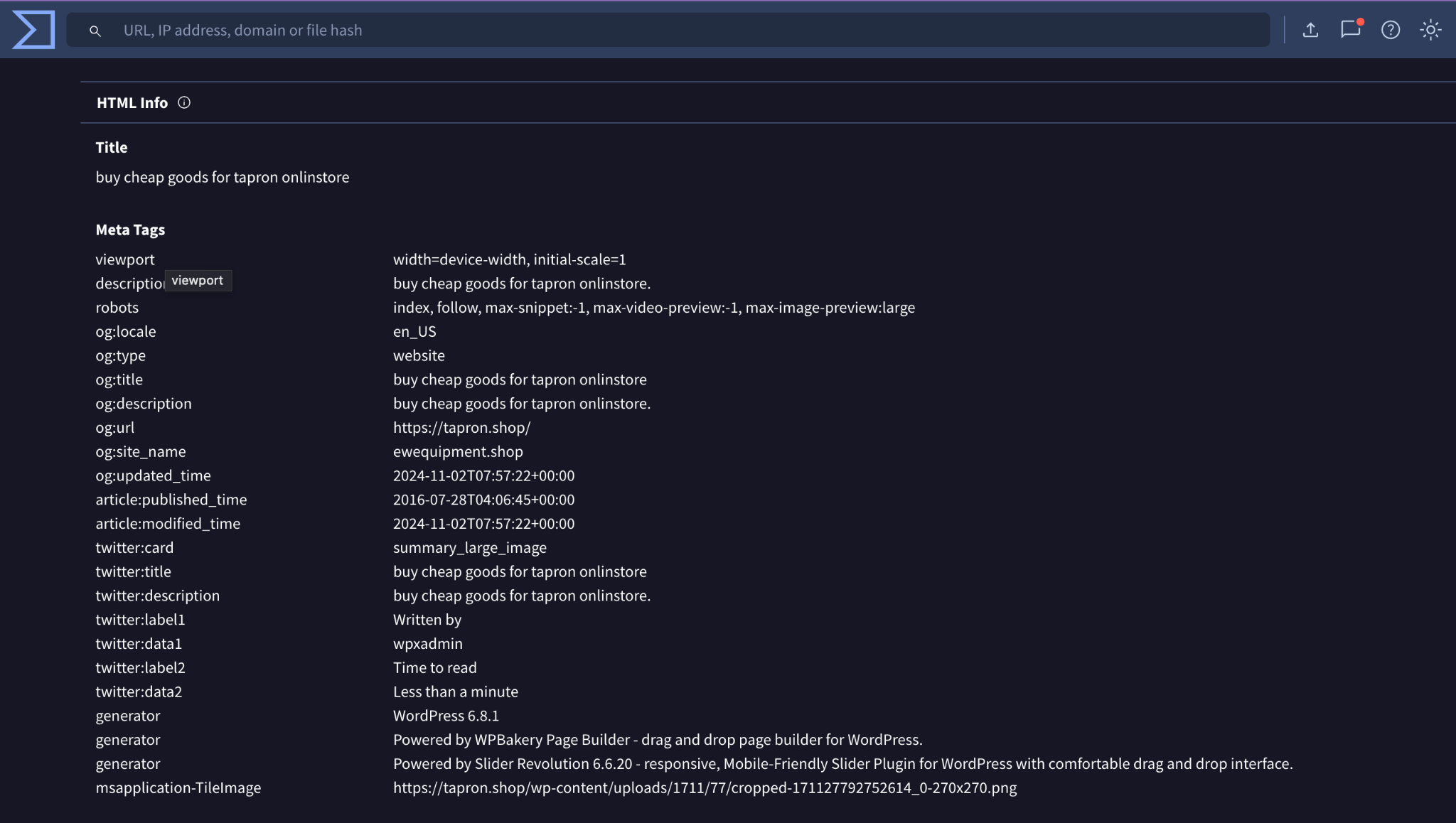
Often seen in automatically generated or cloned phishing sites.

**4.3.3. Glue Records Missing at Local Nameservers**

****

* **Info**: No glue records for ollie.ns.cloudflare.com or louis.ns.cloudflare.com.
* Implication:
  + Causes **additional DNS lookups**, increasing latency.
  + While not critical, **this misconfiguration is uncommon** in high-quality, secure e-commerce deployments.
* **Possible Interpretation**: Neglect of DNS hygiene, pointing to a low-effort setup, as seen in temporary scam sites.

**4.4 Advance Phishing Evidence from Live Scan :**



**4.4.1. og:site\_name = ewequipment.shop**

* Site name doesn’t match domain.
* **Likely reused or cloned from another phishing page.**
* Major inconsistency that confirms **template reuse** from previous scams.

**4.4.2.** **Manipulated Metadata for SEO and Social Platforms**

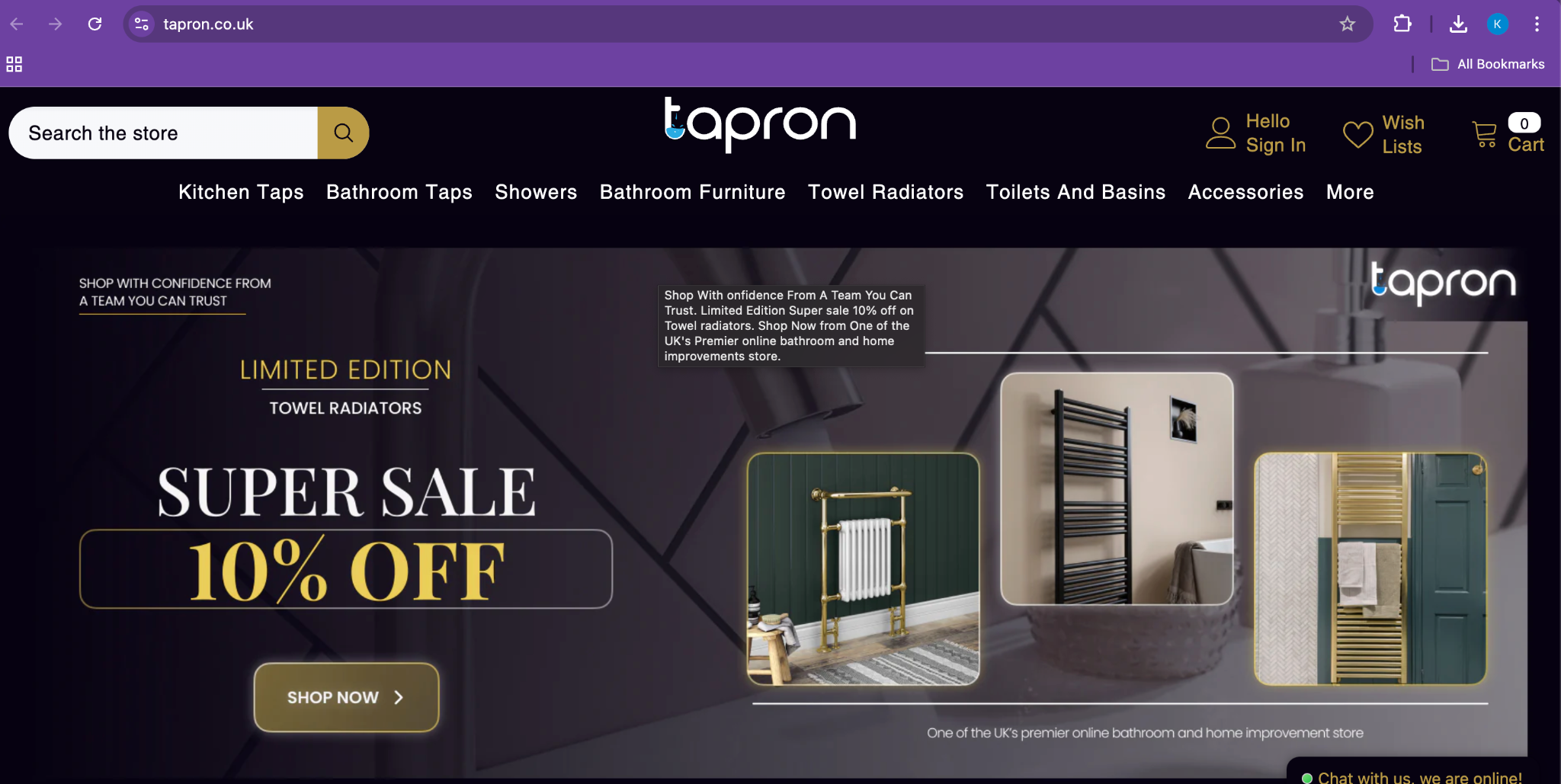
default administrative username → Default WordPress admin username = not customized

Used by default in phishing toolkits built with WordPress

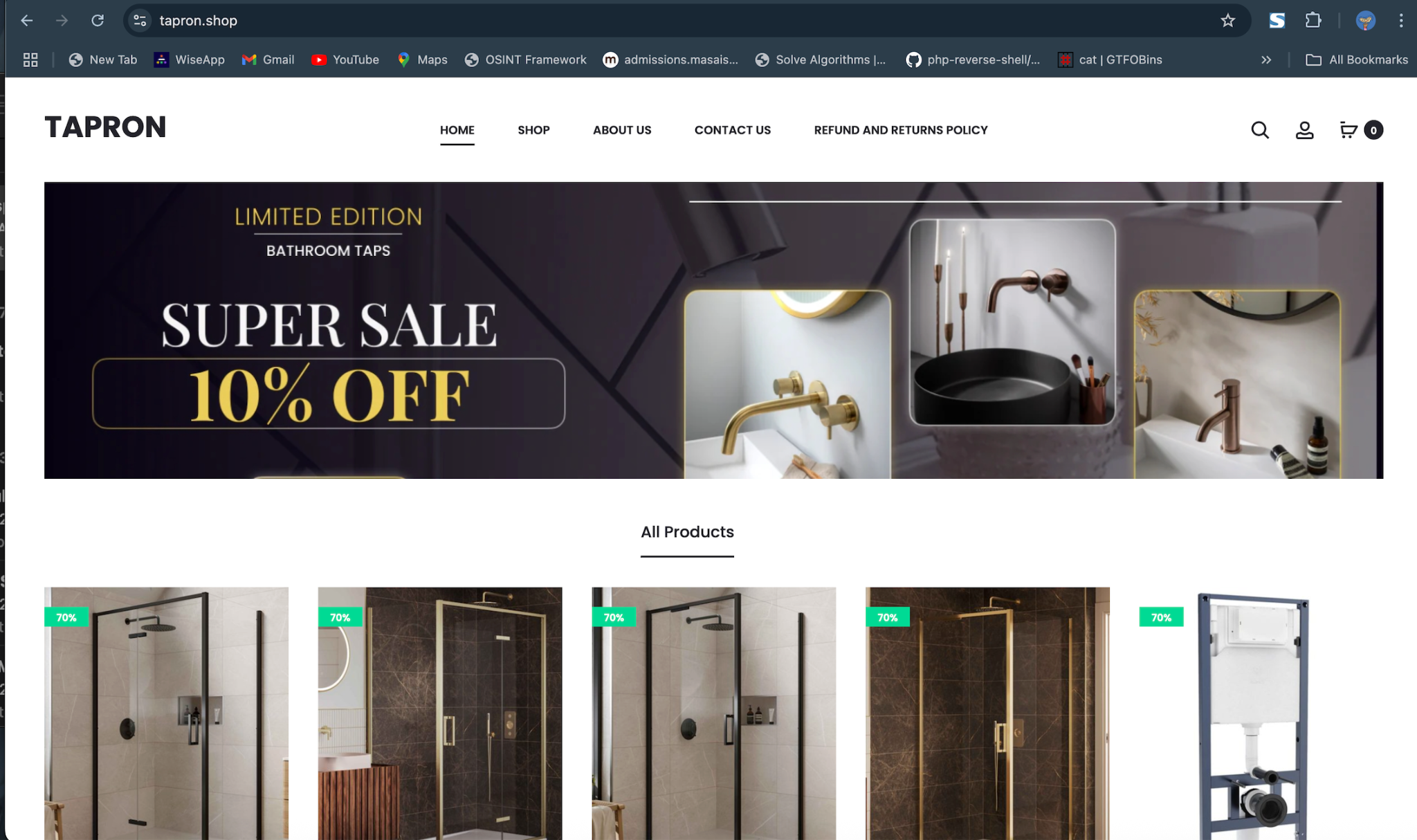
# 5. Analysis

The '.shop' domain mimics the '.co.uk' Tapron brand. Metadata and content suggest a hasty setup using templates. Clear impersonation signs.

**Original Website:**



**Phishing site:**



# 6. Technical Breakdown

Technologies Used: WordPress 6.8.1, jQuery 3.7.1, PHP, Cloudflare CDN, MySQL.

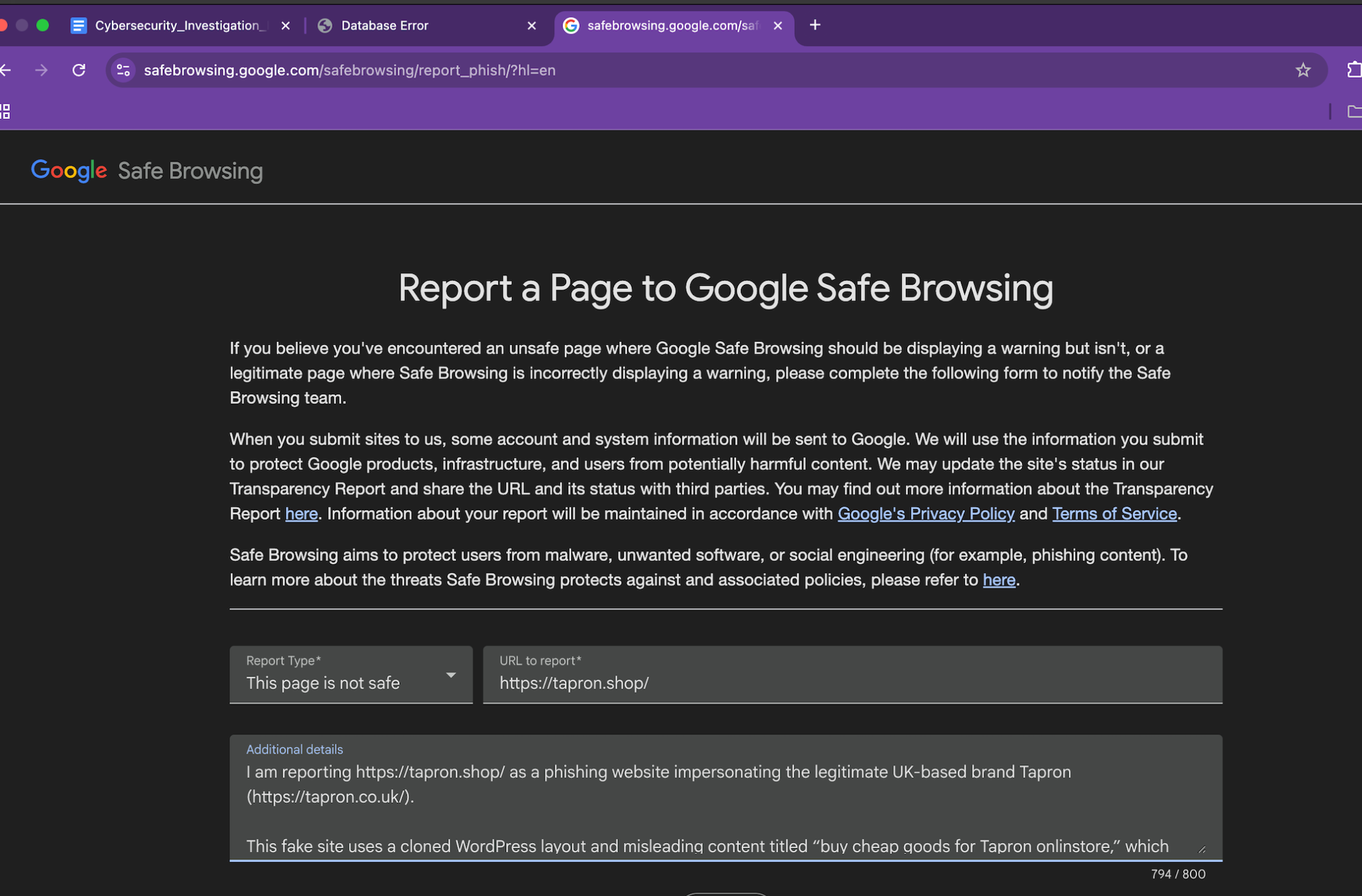
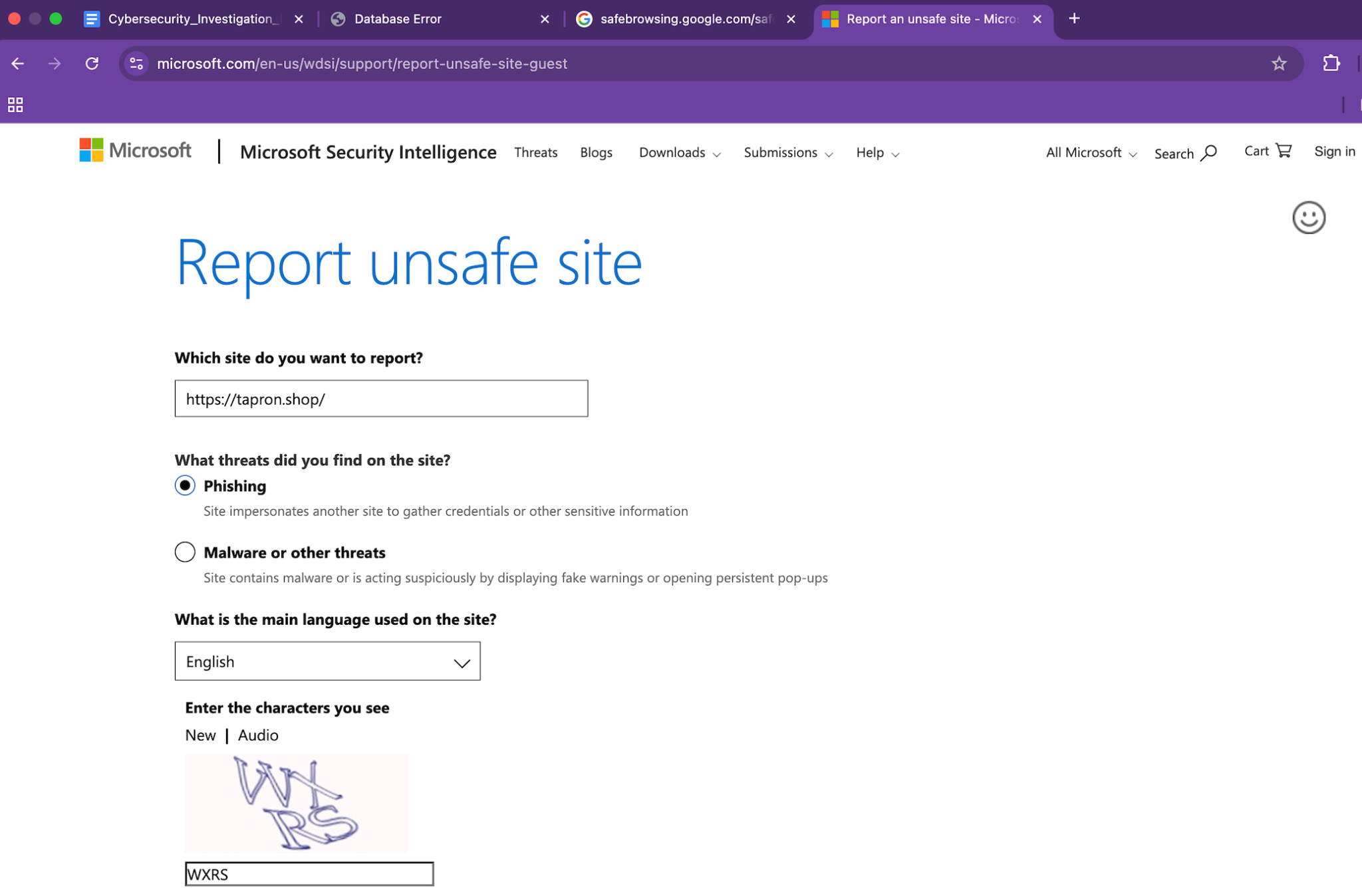
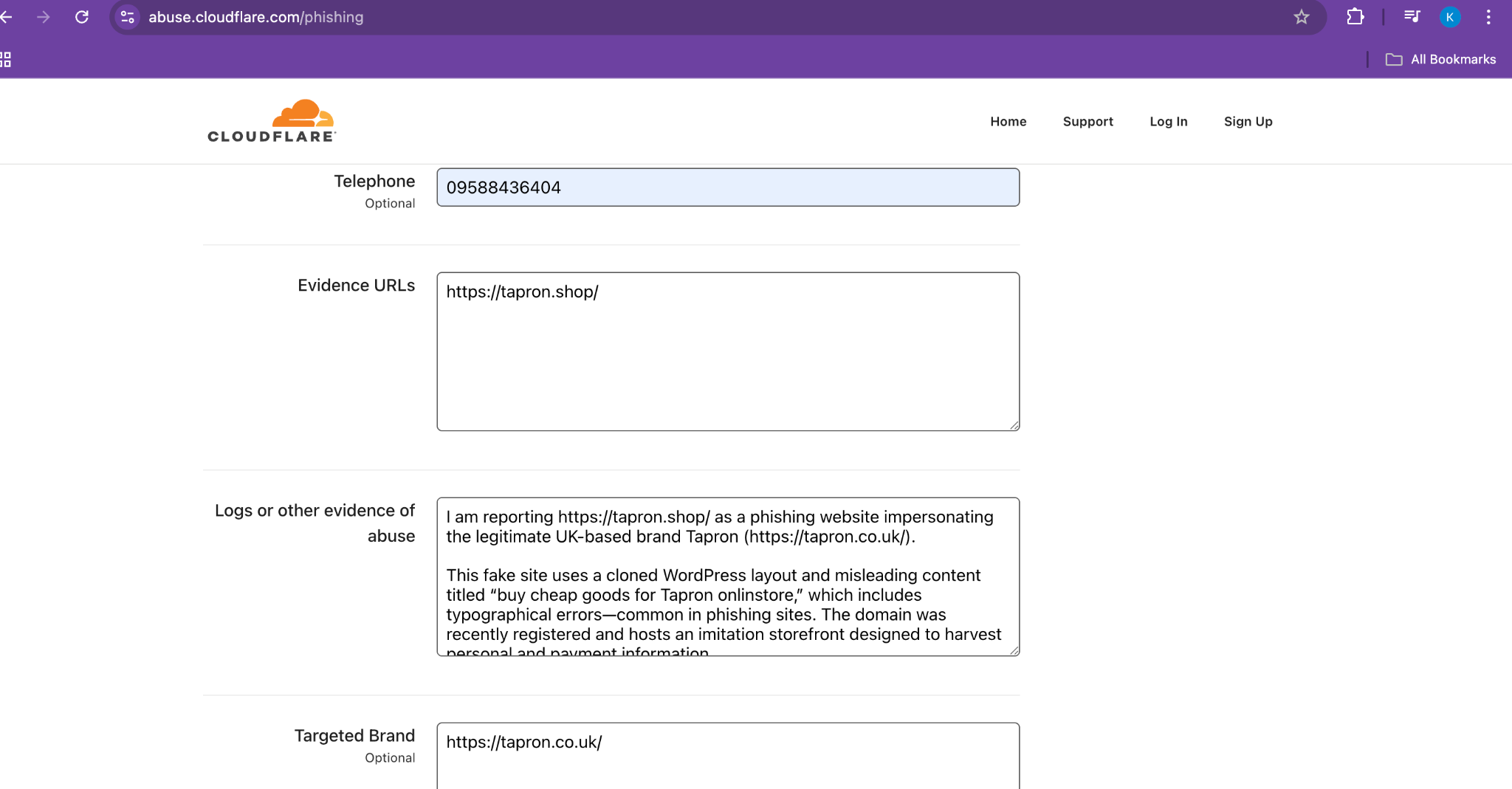
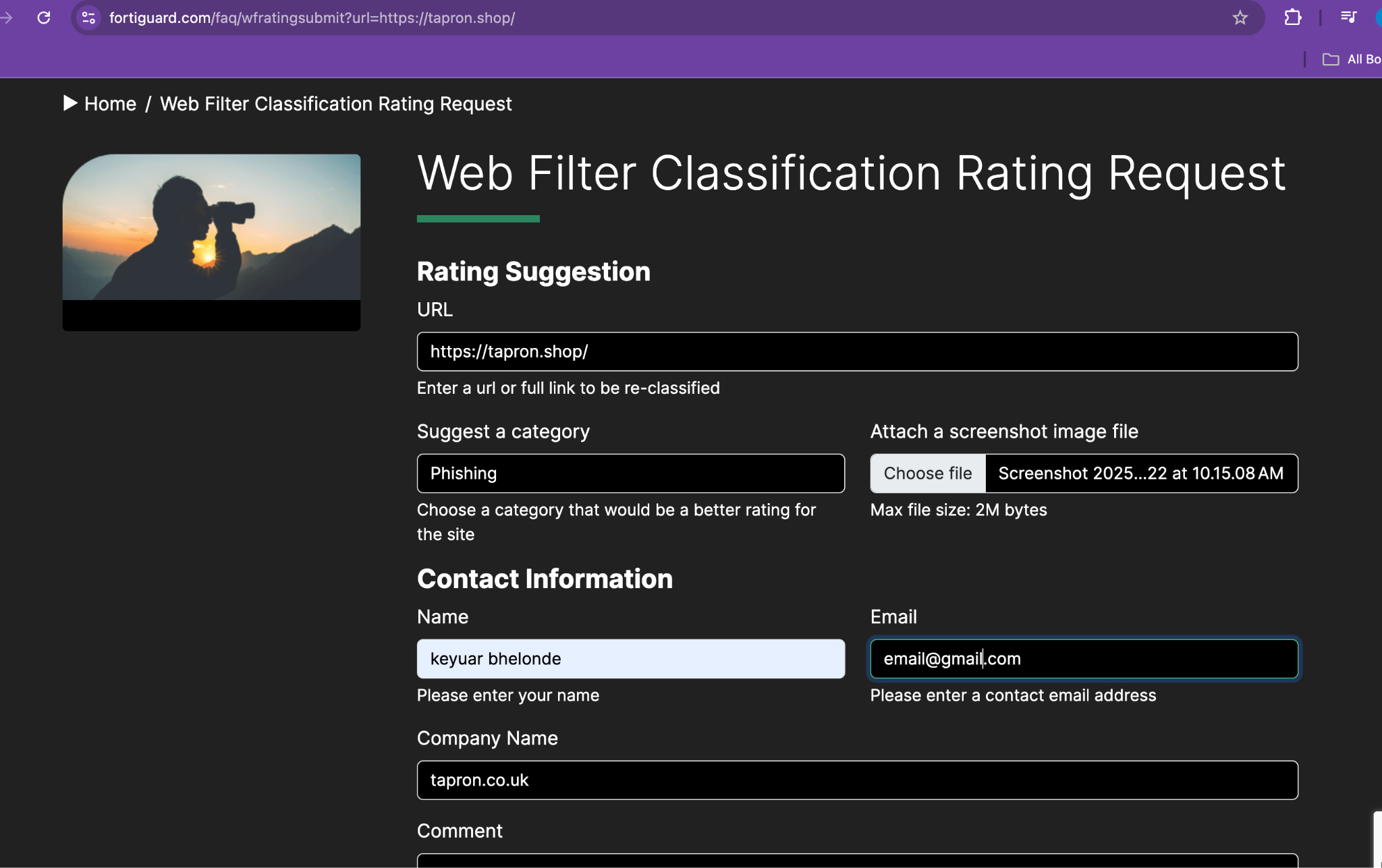
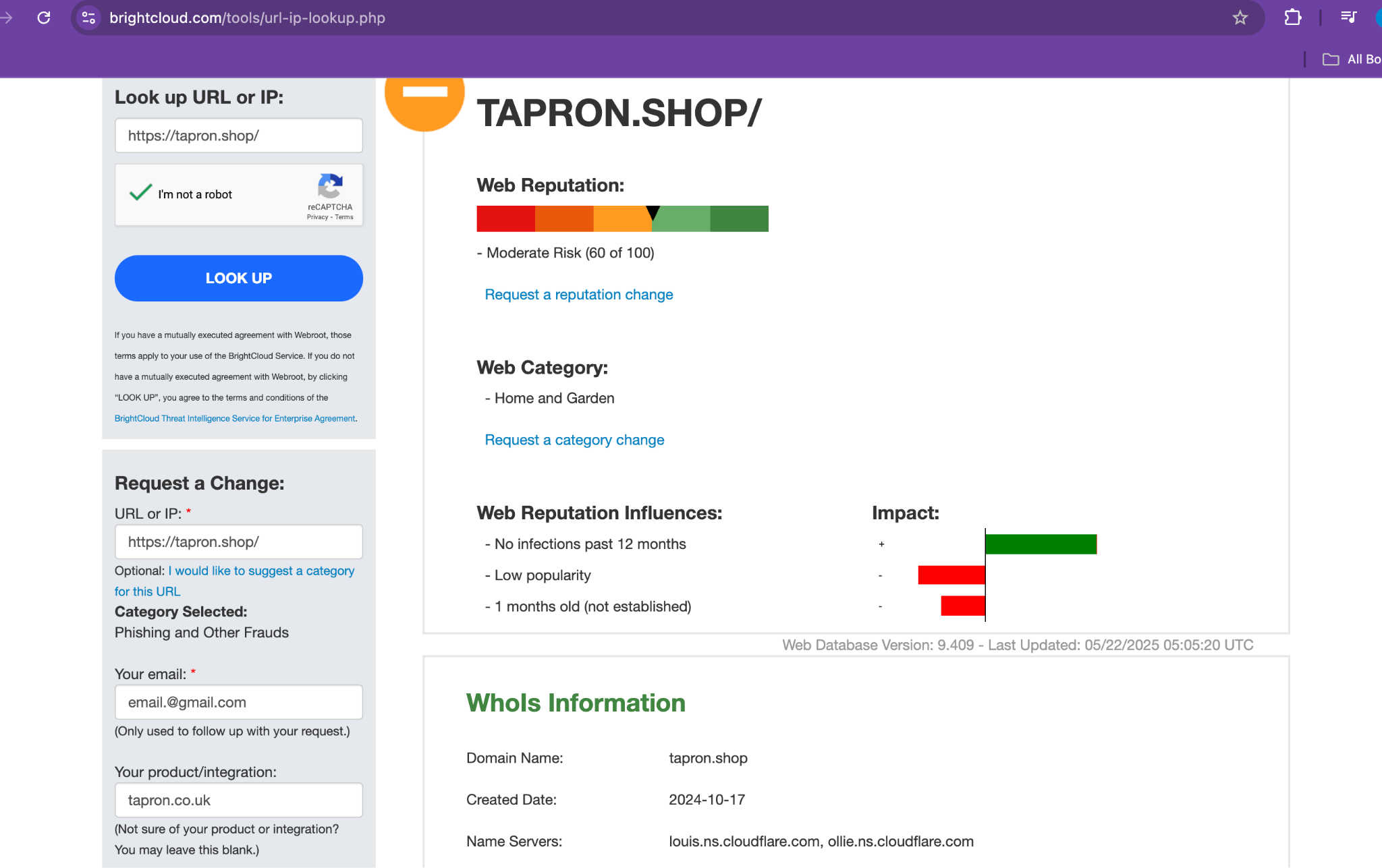
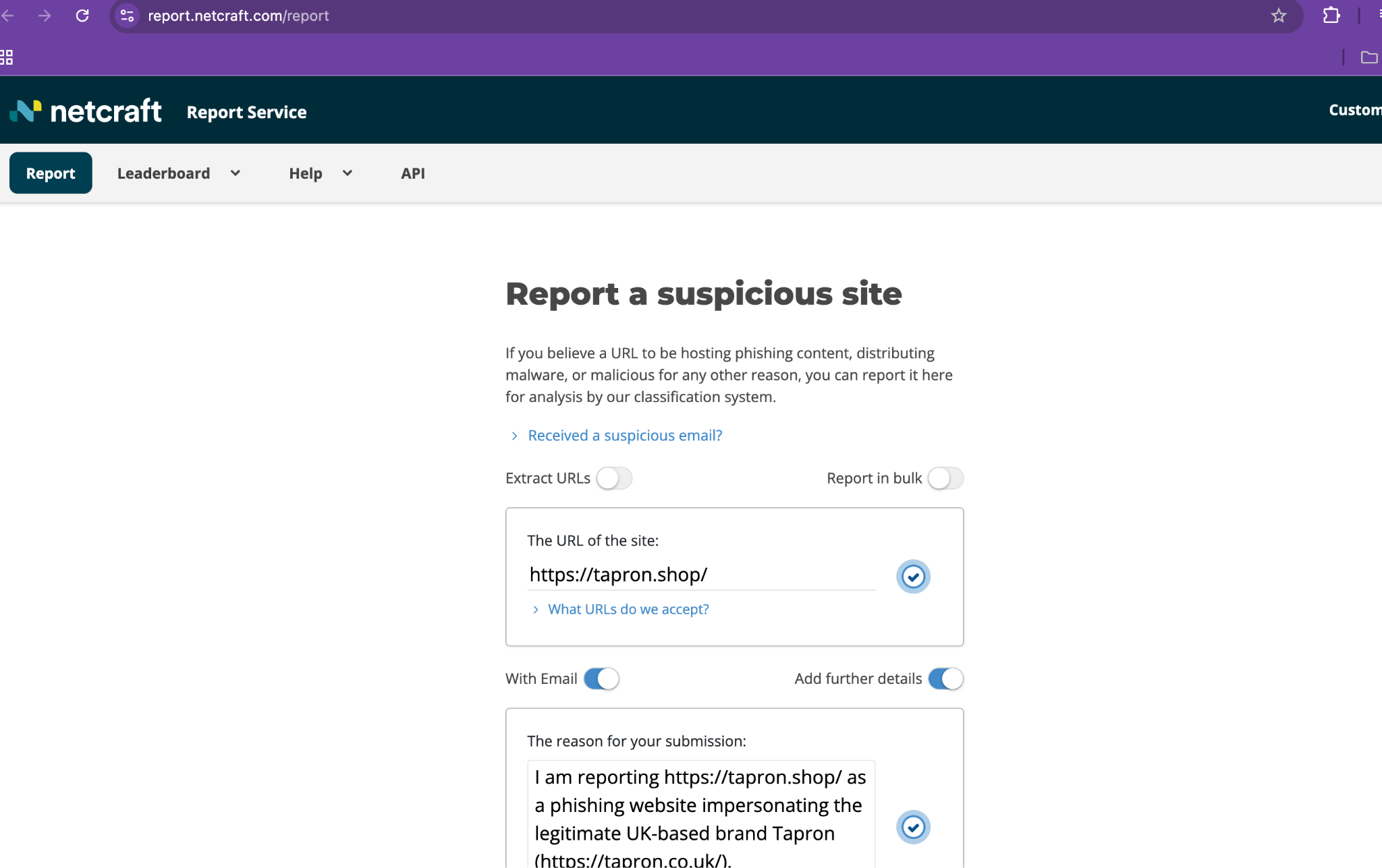
# 7. Threat Intelligence Correlation

Compared with the real site, the fake one shows clear inconsistencies in design, domain age, traffic, and SSL behavior.

# 8. Mitigation & Strategies:

After confirming that https://tapron.shop/ is a phishing website likely impersonating a legitimate brand to deceive users, I took immediate action to limit its reach and protect potential victims. My approach was both methodical and proactive, focusing on reporting the threat to trusted global security platforms to increase visibility and accelerate takedown efforts.

Here are the key platforms I reported the site to:

* **Google Safe Browsing** – I submitted the domain for review so that it can be flagged by Chrome and other browsers that rely on Google’s blocklist, warning users before they access the site.
* **Microsoft Defender SmartScreen** – I reported the phishing activity to Microsoft so that users on Windows and Microsoft Edge can be warned or blocked from accessing the site.
* **Cloudflare Abuse** – Since Cloudflare hosts both the DNS and CDN services for the domain, I submitted an abuse report with supporting evidence, requesting further investigation or suspension.
* **FortiGuard (Fortinet)** – I submitted the site to Fortinet’s threat intelligence team, which helps protect enterprise users through their firewalls and antivirus systems.
* **BrightCloud (Webroot)** – I reported the URL to Webroot’s BrightCloud Threat Intelligence, which feeds into many security products and web filters.
* **Netcraft Anti-Phishing** – I used Netcraft’s reporting form to flag the phishing site so it can be blocked by browsers and endpoint protection tools.

**Cloud Foundry** – As a precaution, I also reported the domain in case any backend infrastructure (like a PaaS or app host) is being misused behind the scene scan reports, meta data, and raw DNS/WHOIS data.

# 9. Conclusion

In conclusion, since solid evidence was reported to major platforms like Google Safe Browsing, the malicious site is likely to be flagged or blocked within a day, though full takedown depends on host or registrar actions.