Subdomain Takeover *of* Nigeria Police Service Commission Website

A Technical Incident Report

By

David Odes

Web Security Lab

1. Executive Summary

In December 2025, the subdomain recruitment.psc.gov.ng, associated with the **Nigeria Police Service Commission (PSC)**, began serving pornographic and search-engine-optimised spam content. The incident coincided with the public announcement of a major police recruitment exercise, significantly increasing the visibility and potential impact of the misuse.

The subdomain had historically been used as an official recruitment portal and remained publicly resolvable despite having been operationally inactive for an extended period. Although the service itself was no longer in use, its DNS A record remained active within the authoritative DNS zone for psc.gov.ng.

On 1 December 2025, the DNS A record for recruitment.psc.gov.ng was modified to point to infrastructure hosted on DigitalOcean. Shortly thereafter, the subdomain began serving purpose-built adult content designed to exploit the reputational trust and search-engine authority associated with a government domain. A TLS certificate was issued for the subdomain on **11 December 2025** via Let's Encrypt, confirming that the operator of the destination server had effective control over the domain at that time.

Based on publicly observable evidence, it is not possible to determine whether the DNS change was authorised or unauthorised, nor whether the hosting environment was legitimate infrastructure that was subsequently compromised. The facts are consistent with multiple scenarios, including unauthorised DNS modification, application-level compromise following an authorised DNS change, or inappropriate use of access by a party with legitimate credentials. Regardless of the initiating mechanism, effective control over what the subdomain served was lost.

The compromised subdomain achieved substantial exposure. Search engine analysis indicates that hundreds of pages were indexed, with traffic increasing from negligible levels in November 2025 to approximately **30,000 visits** in December 2025. The content ranked for thousands of keywords, leveraging the implicit trust and ranking advantage of a .gov.ng domain.

The incident was discovered through external monitoring on **20 December 2025** and responsibly disclosed to the Police Service Commission on **24 December 2025**. After no response was received, the issue was escalated on **12 January 2026** to Galaxy Backbone, the authoritative DNS operator for psc.gov.ng.

On **13 January 2026**, the DNS A record for recruitment.psc.gov.ng was removed, rendering the subdomain offline.

This incident highlights systemic weaknesses in subdomain lifecycle management, access control over DNS and hosting infrastructure, and the absence of continuous monitoring for government web assets. It demonstrates how legacy services, when not formally decommissioned and actively governed, can be repurposed for abuse without requiring exploitation of core systems or sophisticated attack techniques.

1.1 Timeline

1 December 2025: DNS A record for recruitment.psc.gov.ng changed from **143.198.250.115** to **139.59.165.47**

11 December 2025:

- Police Service Commission announces major recruitment exercise
- TLS certificate issued for recruitment.psc.gov.ng via Let's Encrypt

20 December 2025: Incident discovered by Web Security Lab

24 December 2025: Police Service Commission notified via email

12 January 2026: Incident escalated to Galaxy Backbone, the authoritative DNS operator for psc.gov.ng, following a lack of response from the Police Service Commission.

13 January 2026: Galaxy Backbone removed the A record for recruitment.psc.gov.ng, rendering the subdomain offline.

2. Scope and Disclosure

This investigation was conducted externally using publicly available data sources. No access to internal systems, credentials, logs, or cloud accounts was obtained or attempted. All findings are derived solely from passive observation and publicly accessible technical artefacts.

The investigation focused on:

- DNS configuration and historical changes
- Hosting infrastructure and web stack analysis
- TLS certificate issuance and validation
- Web archive content history
- Search engine indexing and traffic patterns
- Application fingerprinting

The Police Service Commission was notified of the incident via email on **24 December 2025.**

3. Domain and Infrastructure Overview

3.1 Domain Registration and DNS Authority

Primary domain: psc.gov.ng
Subdomain: recruitment.psc.gov.ng
Registrar: Galaxy Backbone
Authoritative DNS operator: Galaxy Backbone

Authoritative name servers: ns1.galaxybackbone.com, ns2.galaxybackbone.com

The subdomain recruitment.psc.gov.ng has no independent name server (NS) records and is not a delegated DNS zone. Galaxy Backbone operates authoritative DNS for psc.gov.ng and, by extension, all subdomains, including recruitment.psc.gov.ng. Galaxy Backbone, therefore, controls domain registration, DNS zone hosting, and all subdomain record management.

NS records

Name server	Revalidate in
ns2.galaxybackbone.com.	3m
ns1.galaxybackbone.com.	3m

Fig 1: Name Server record of psc.gov.ng

3.1.1 Domain Governance Context

The .gov.ng domain is a restricted top-level domain managed by the National Information Technology Development Agency (NITDA) in consultation with the Nigeria Internet Registration Association (NiRA). Registration under .gov.ng is limited to federal, state, and local government entities and requires formal authorisation from the head of the registering institution. Domain management policy requires that all government websites use the .gov.ng extension exclusively, and that each domain or service maintain documented ownership and continuing responsibility for quality and security.

3.2 Hosting Infrastructure

The recruitment.psc.gov.ng subdomain currently resolves to infrastructure operated by cloud provider, **DigitalOcean,** at IP address: **139.59.165.47**

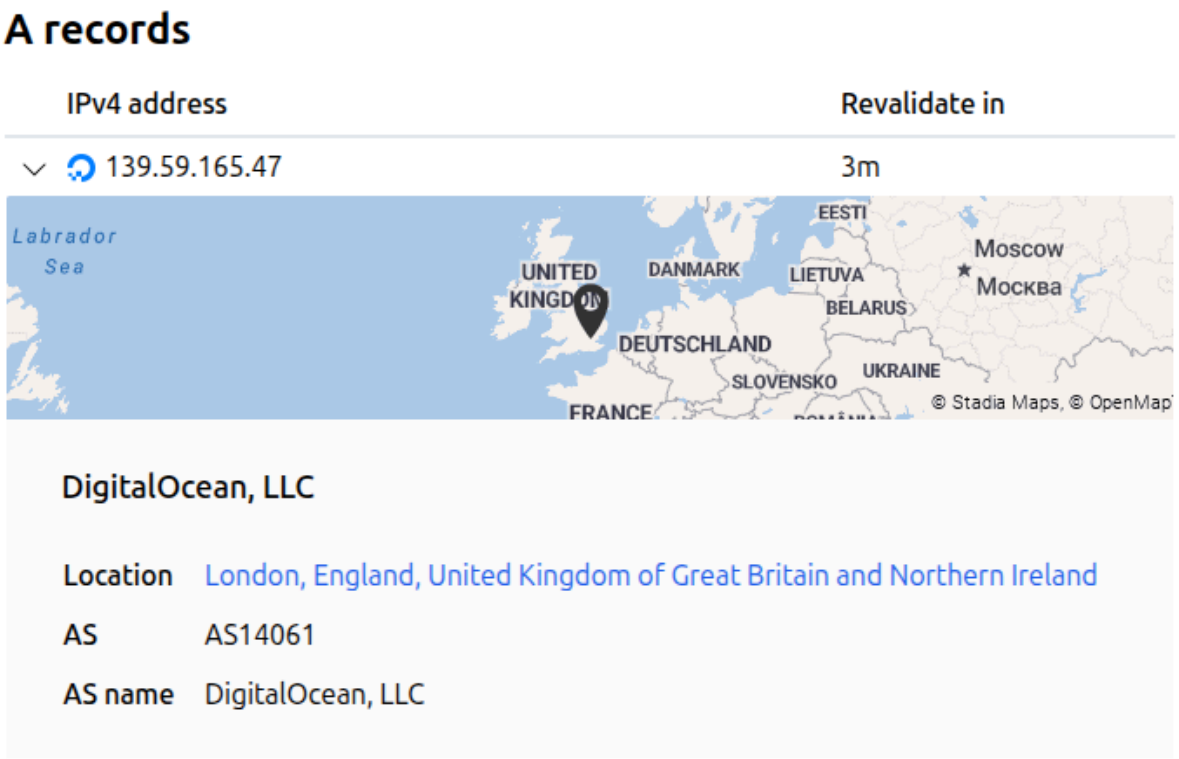

Fig 2: *A record* of recruitment.psc.gov.ng showing IP Information.

3.2.1 Web Stack Identification

Web stack identification shows that the subdomain resolves to a cleanly deployed nginx-based environment with enforced HTTPS and HSTS enabled. The site serves purpose-built content with SEO and metadata optimisations, and does not display characteristics of a defaced or repurposed government system. This is consistent with a deliberately deployed environment rather than an opportunistic defacement.

Fig 3: Web server and hosting characteristics of recruitment.psc.gov.ng

3.3 TLS Certificate Analysis

- **Certificate Authority:** Let's Encrypt
- **Issuance date:** 11 December 2025
- **Validation method:** Domain control validation (HTTP/DNS)

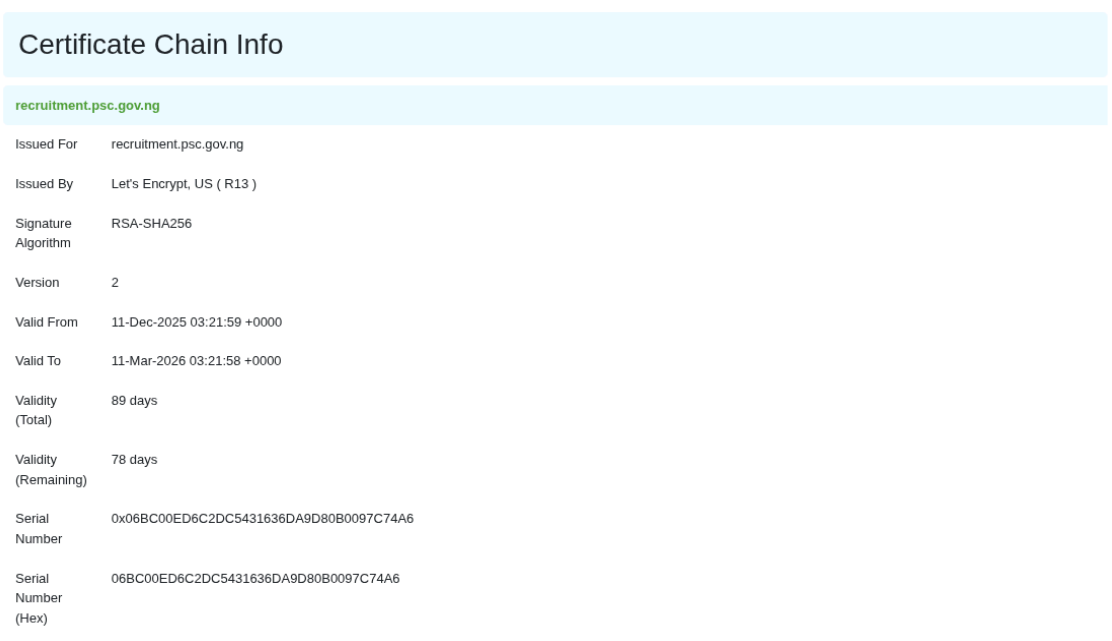

Fig 4: Certificate Chain Information

Certificate issuance confirms that, at the time of issuance, the operator of the DigitalOcean server had effective control of the subdomain and DNS resolution was already correctly configured.

3.4 Impact Assessment

Search engine data indicates significant exposure of the compromised subdomain:

Search engine presence: Over 30 pages of search results on Google, representing hundreds of indexed pages

Traffic surge: Traffic analytics (Ahrefs) show an increase from 4 visits in November 2025 to approximately 30,000 visits in December 2025

Keyword ranking: Search engine optimisation tracking (Semrush) indicates the subdomain ranked for over 7,800 keywords during the active period

Given the timing of the incident during an announced police recruitment exercise, the misuse of the subdomain carried heightened reputational and public trust implications. Members of the public searching for official recruitment information were plausibly exposed to inappropriate content under a trusted government domain, creating risk of reputational harm, misinformation, and erosion of confidence in official digital channels

Current status: As of 4 February 2026, the subdomain is no longer responsive and appears to have been taken offline.

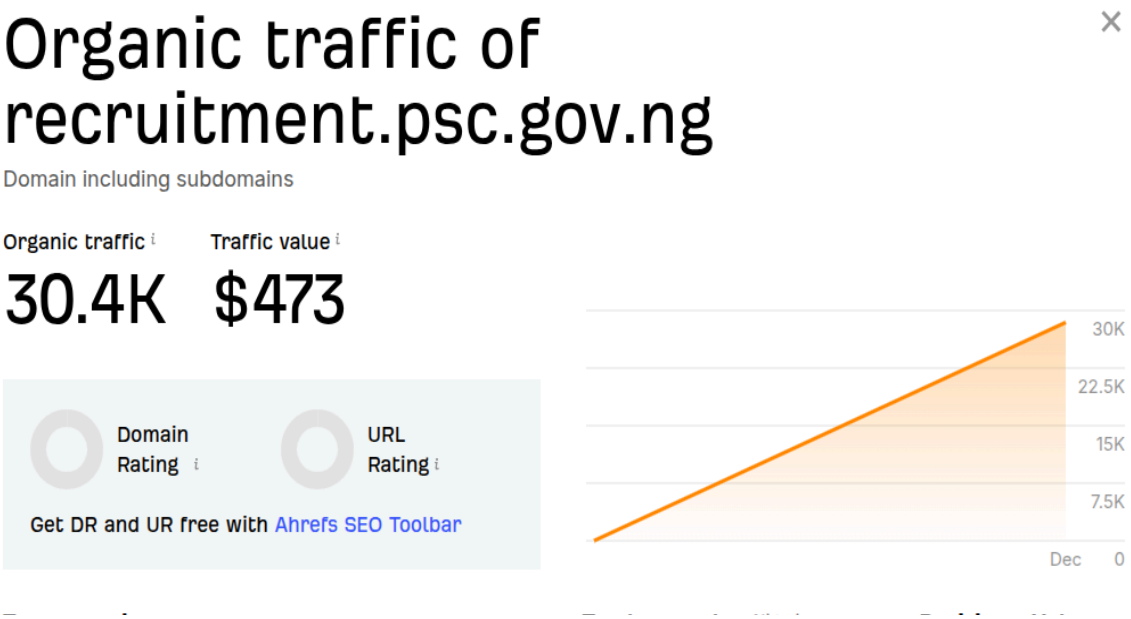

Fig 5: Ahrefs traffic data showing the November to December spike

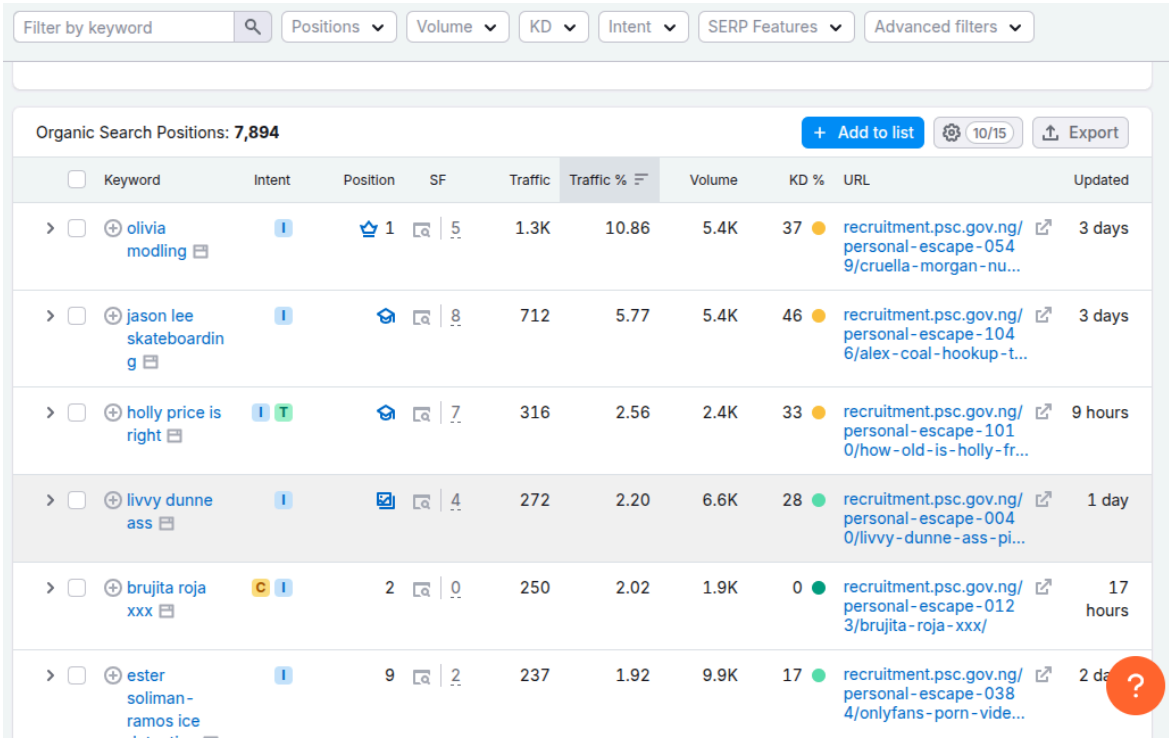

Fig 6: Semrush keyword ranking data

4. Historical Use of recruitment.psc.gov.ng

4.1 Content History

Analysis of **Internet Archive** data shows the subdomain served as a functional recruitment portal up to **2022**.

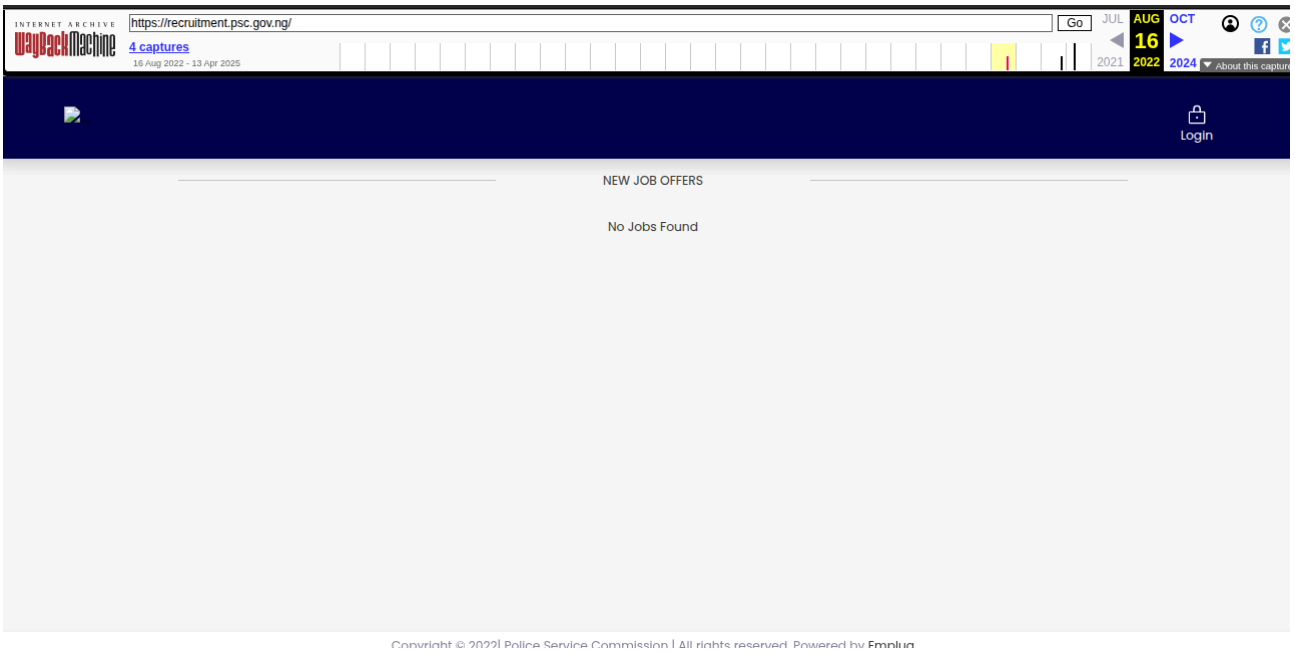

Fig 7: Archive Snapshot from Aug 2022

After 2022, snapshots show “Website Unavailable” states.

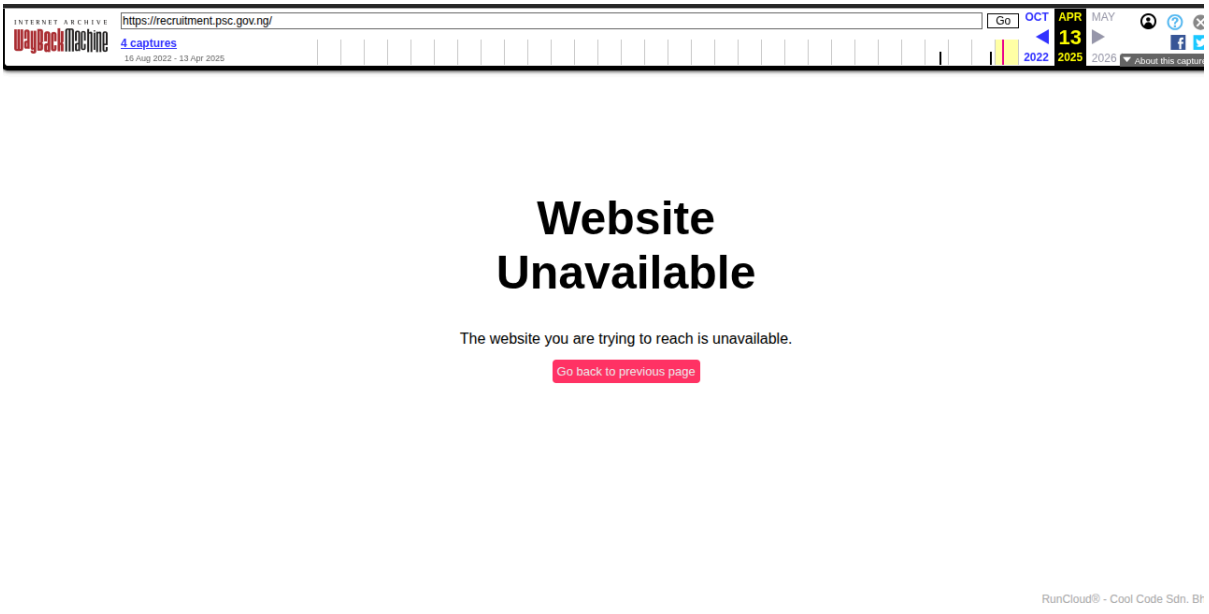

Fig 8: Archive Snapshot from April 2025

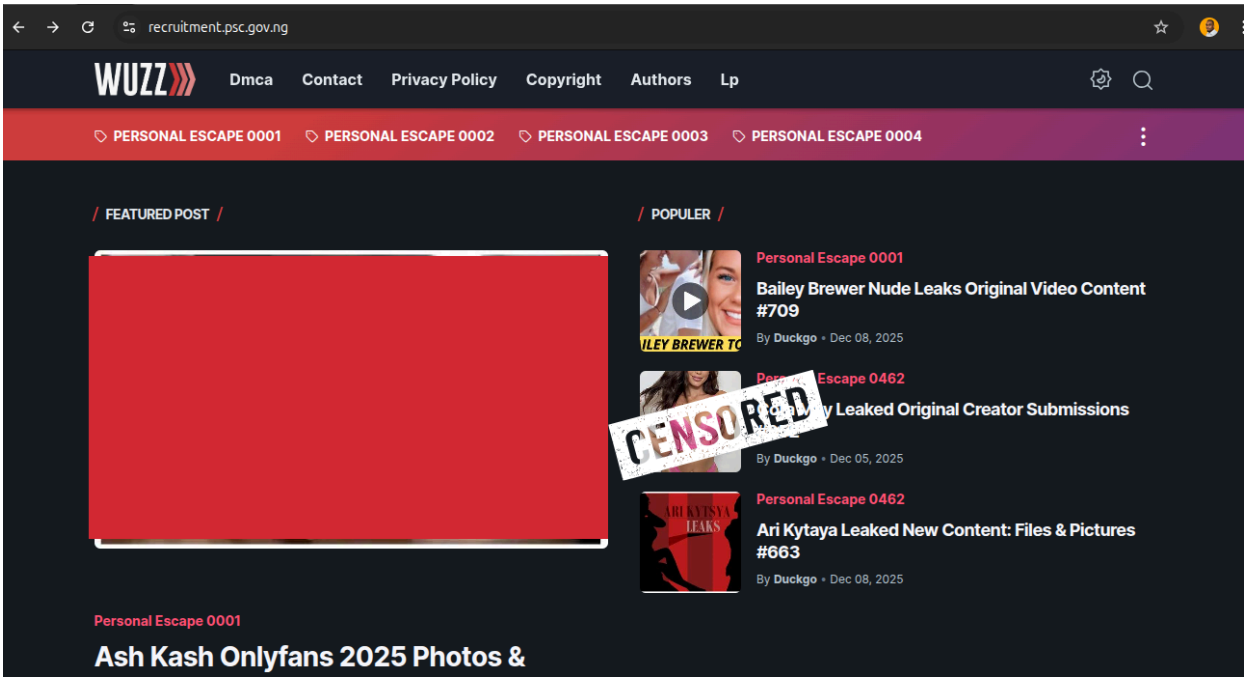

Fig 9: Snapshot of the website taken on December 22, 2025.

Police Service Commission
https://recruitment.psc.gov.ng › personal-escape-0942 › l...

Lyciafaith Creator-Made Video Media #941

4 days ago — **Explore lyciafaith themed streaming in ultra-HD clarity** for a remarkably compelling viewing. Join our digital hub today to see exclusive prime ... Read more

9.7/10 ★★★★★ (991)

psc.gov.ng
https://recruitment.psc.gov.ng › personal-escape-0151

Lexi Gray Onlyfans Pictures & Videos From 2025 #646

4 days ago — Uncover **lexi gray onlyfans** chosen streaming in breathtaking quality for a absolutely mesmerizing adventure. Enroll in our digital hub today to ... Read more

Police Service Commission
https://recruitment.psc.gov.ng › personal-escape-0331

Krivoshapka Exclusive Media Updates #905

3 days ago — See It **Instantly exclusive krivoshapka in gorgeous HD**. With frequent updates and entirely cost-free on our exclusive media page.

8.1/10 ★★★★☆ (907)

Fig 10: Public search engine results for recruitment.psc.gov.ng

5. DNS History and Change Analysis

5.1 Historical DNS Resolution

Passive DNS data shows that the subdomain resolved to one stable IP: 143.198.250.115 for about 3 years before changing on 1 December 2025 to the current IP address: 139.59.165.47.

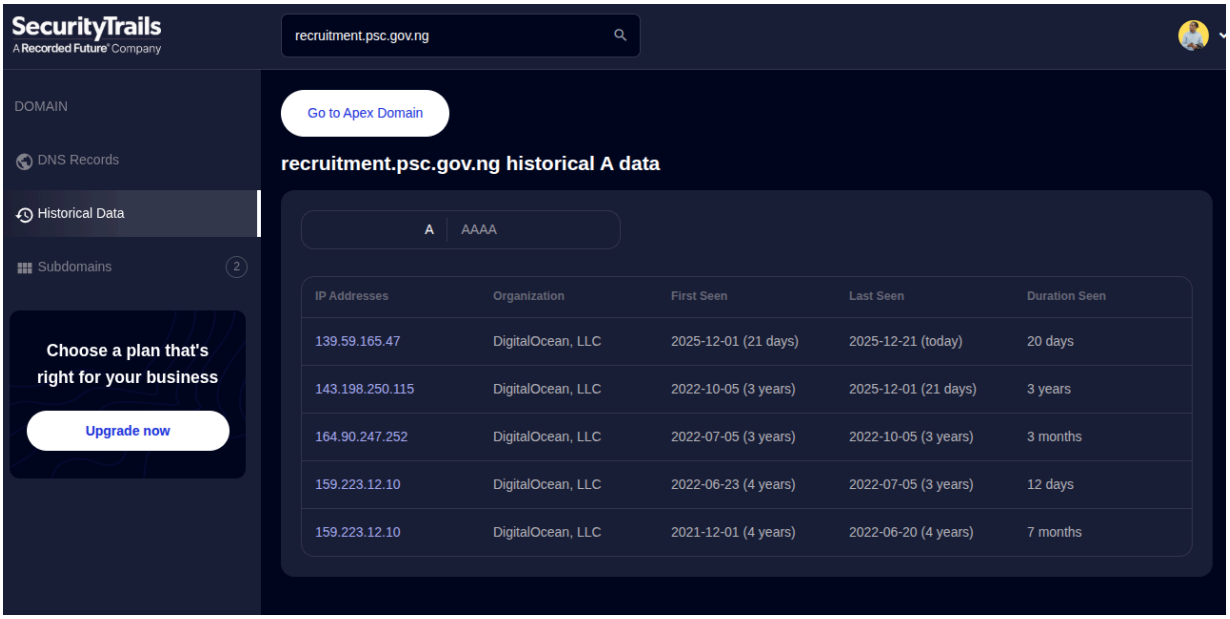

Fig 7: DNS history showing A record changes.

An *A record* change requires administrative action within the DNS management environment. The change itself is documented and observable. However, external investigation cannot determine whether this DNS change was authorised or unauthorised, or whether the hosting environment to which it pointed was legitimate infrastructure that was subsequently compromised.

5.2 Possible Attack Vectors

The following scenarios are non-exhaustive and represent plausible explanations consistent with observed evidence:

DNS-level compromise: Unauthorised access to DNS management systems, allowing an attacker to repoint the subdomain to infrastructure under their control. In this scenario, both the DNS change and the hosting would be unauthorised.

Application-level compromise: Authorised DNS change to legitimate hosting, followed by compromise of the web application, content management system, or hosting environment itself. Modern web applications, particularly those using content management systems, can be compromised through vulnerable themes, plugins, or other application-layer attacks that allow attackers to serve entirely different content while the underlying infrastructure remains legitimately controlled.

Authorised but inappropriate action: DNS change and hosting setup authorised through proper channels but used inappropriately, either through misunderstanding, poor judgment, or malicious intent by someone with legitimate access.

6. Legal and Regulatory Context

This report does not make a finding of legal liability or criminal conduct. It outlines the applicable statutory and regulatory framework relevant to incidents of this nature. Any determination of responsibility would require internal access to systems, logs, and administrative records not available to this investigation.

This incident occurs within a defined regulatory framework. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, establishes legal obligations for the protection of government information infrastructure and provides for penalties related to unauthorised access, system interference, and misuse of computer systems. Section 6 of the Act addresses unauthorised access to computer systems, while provisions relating to tampering with critical infrastructure carry significant penalties.

The .gov.ng Domain Management Policy, administered by the National Information Technology Development Agency (NITDA), requires that government websites use the .gov.ng domain exclusively and maintain documented ownership and responsibility for each registered service. The policy framework assumes active management and security oversight of government web assets.

Beyond this specific case, subdomain compromise and defacement affecting Nigerian government domains is not isolated. Multiple .gov.ng properties currently serve defaced content, host malware, or contain unpatched vulnerabilities, indicating a broader pattern of insufficient maintenance, monitoring, and security discipline across government digital infrastructure.

7. Recommendations

I. Immediately neutralise the affected subdomain

Remove recruitment.psc.gov.ng from DNS or permanently redirect it to the officially designated recruitment portal. The subdomain should not remain active or configurable under any circumstances.

II. Conduct a focused internal investigation into the DNS change and access path

Conduct a targeted internal investigation to determine how control of recruitment.psc.gov.ng was exercised, with specific review of:

- DNS change history and initiating accounts or roles
- Access controls and permissions for DNS administration at the time of the change
- Whether the change followed an approved operational process
- Hosting account ownership and access history for the destination server

- Any third-party vendors, contractors, or service providers with delegated DNS or hosting access

III. Audit and decommission legacy subdomains and public-facing services, with access controls enforced

Identify all legacy subdomains and public-facing services previously operated by the organisation and confirm that each is either:

- Actively used, clearly owned, and appropriately secured, or
- Fully decommissioned, with associated DNS records removed, redirected, or safely parked

Legacy subdomains and services that are no longer in use should not remain active or editable within authoritative DNS. Continued DNS or hosting access for any service should require explicit approval, documented ownership, and role-based access controls.

IV. Implement continuous monitoring of domains, subdomains, and public-facing services

Establish continuous monitoring for all organisational domains, subdomains, and public-facing services to detect unauthorised changes or misuse. This should include:

- Ongoing monitoring of DNS records and resolution for unexpected changes
- Regular review of web content and page titles for unauthorised or anomalous updates
- Monitoring of search engine indexing and keyword associations (e.g. through tools such as Google Search Console)
- Review of traffic sources and referral patterns for indicators of abuse, monetisation, or SEO manipulation

V. Establish formal subdomain lifecycle ownership

Assign explicit business and technical ownership for every registered subdomain, including inactive or legacy services. Ownership should include responsibility for periodic review, security posture, and decommissioning decisions. Subdomains without a named owner should not remain configurable in authoritative DNS.

8. Conclusion

This incident demonstrates how legacy government services, when left active and insufficiently monitored, can be repurposed for abuse through relatively straightforward means. The compromise of `recruitment.psc.gov.ng` subdomain did not rely on exploiting a software vulnerability or breaching the core Police Service Commission website. Instead, it resulted from the continued existence and controllability of a legacy subdomain, combined with a lack of effective oversight once that subdomain ceased legitimate use.

Abuse of this nature is commonly associated with search engine optimisation (SEO) manipulation and advertising monetisation. High-traffic content categories, including adult content, are frequently used to generate visibility, drive referral traffic, and feed advertising or affiliate networks. Domains with strong reputational signals—such as government domains—are particularly attractive targets because they tend to rank well in search results and are implicitly trusted by users and automated systems alike. In this context, the misuse of a .gov.ng subdomain represents a predictable exploitation of trust rather than an isolated anomaly.

More broadly, this incident highlights a recurring weakness in the management of government web infrastructure: legacy services are often retired operationally but not fully decommissioned. Combined with limited maintenance and monitoring, fragmented ownership, and reliance on third-party vendors, this creates an environment in which web assets remain exposed and can be abused for extended periods before detection.

The incident should therefore be understood not as a singular technical failure, but as a governance and maintenance issue affecting public-facing digital services. Without systematic inventory management, enforced decommissioning, access control discipline, and active monitoring, similar misuse, whether for SEO abuse, advertising, phishing, or fraud, is likely to recur across other government assets.