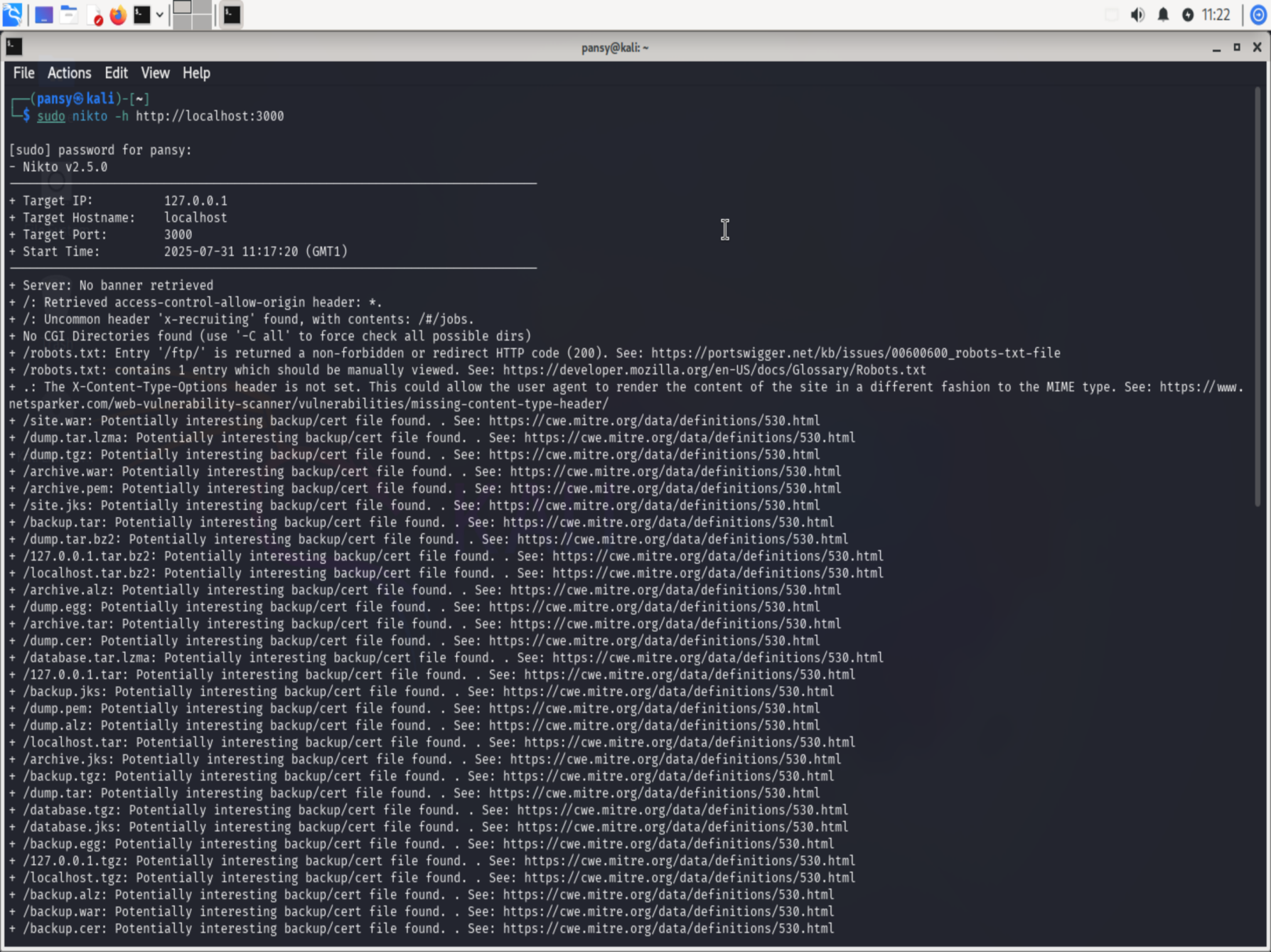
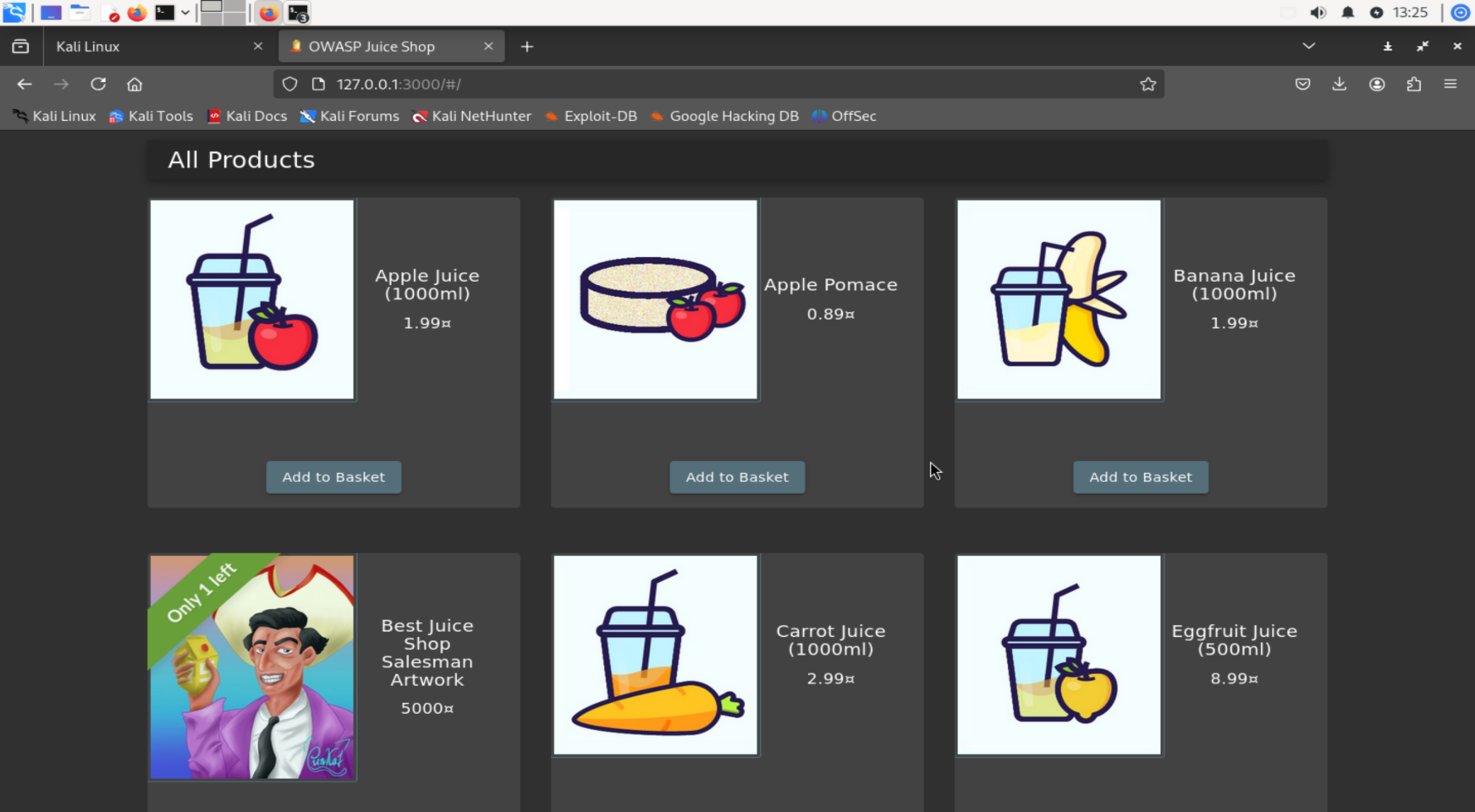
## Web Application Vulnerability Assessment Report

**Security Analyst: Ariyo OluwajomilojuPansy**

**Target:** OWASP Juice Shop  
**Assessment Date:** July 2025  
**Scanner Used:** Nikto.



1. **Vulnerability : Missing X-Content-Type- Options Header**

Description**:**

The server does not include the 'X-Content-Type-Options: nosniff' header, allowing browsers to MIME-sniff

content and possibly execute unintended code

Impact Level**:** Medium

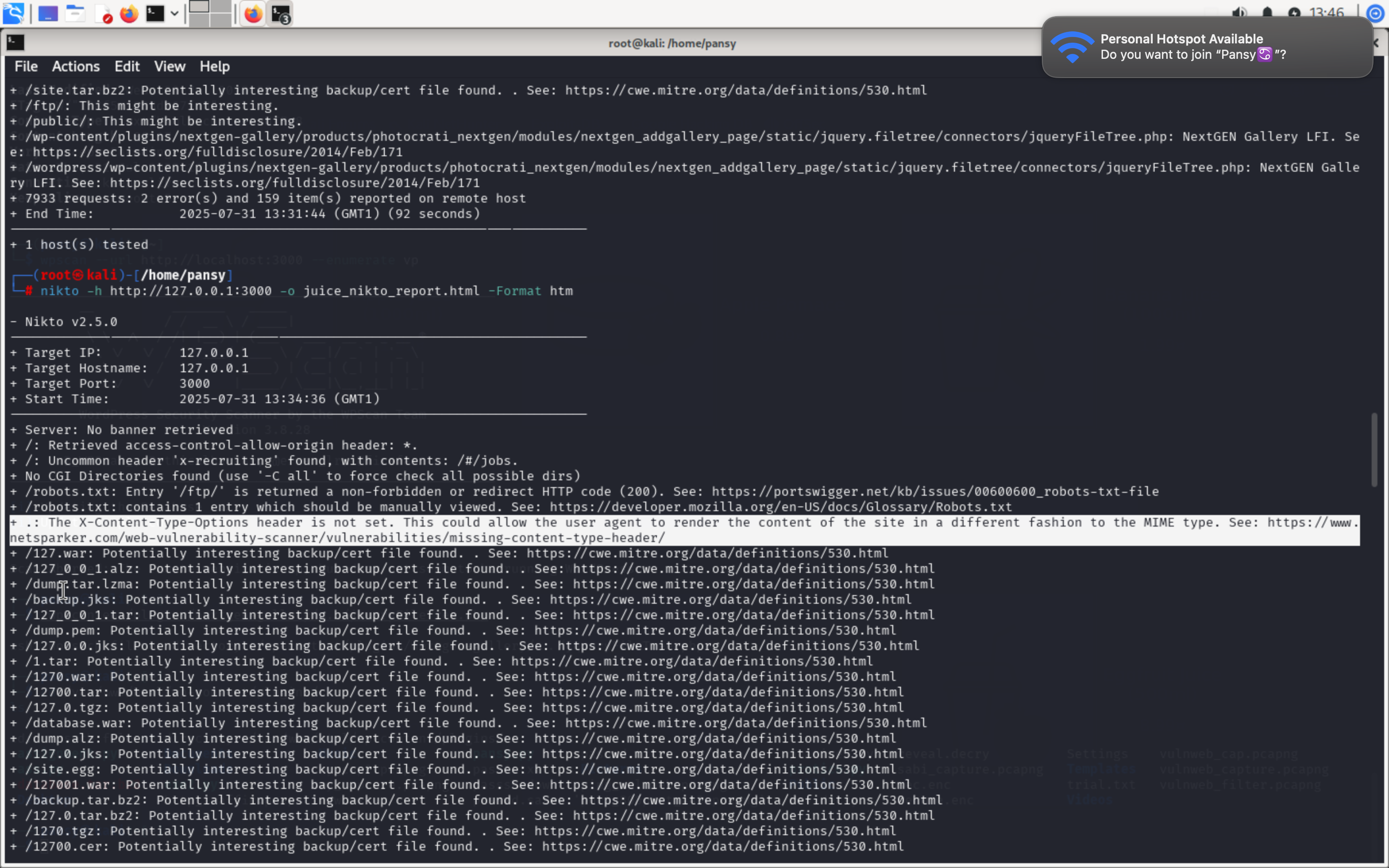
OWASP Mapping: A05:2021 - Security Misconfiguration

Risks:

* Cross-Site Scripting (XSS)
* Content Spoofing
* File Upload Exploits

Mitigation:

* Add the header: X-Content-Type-Options: nosniff
* Configure this in Apache, Nginx, or Node.js with helmet.js.



1. **Retrieved Access-Control-Allow-Origin Header:**

Description**:**

The server includes 'Access-Control-Allow-Origin: \*', allowing unrestricted cross-origin requests.

Impact Level**:** Medium to High

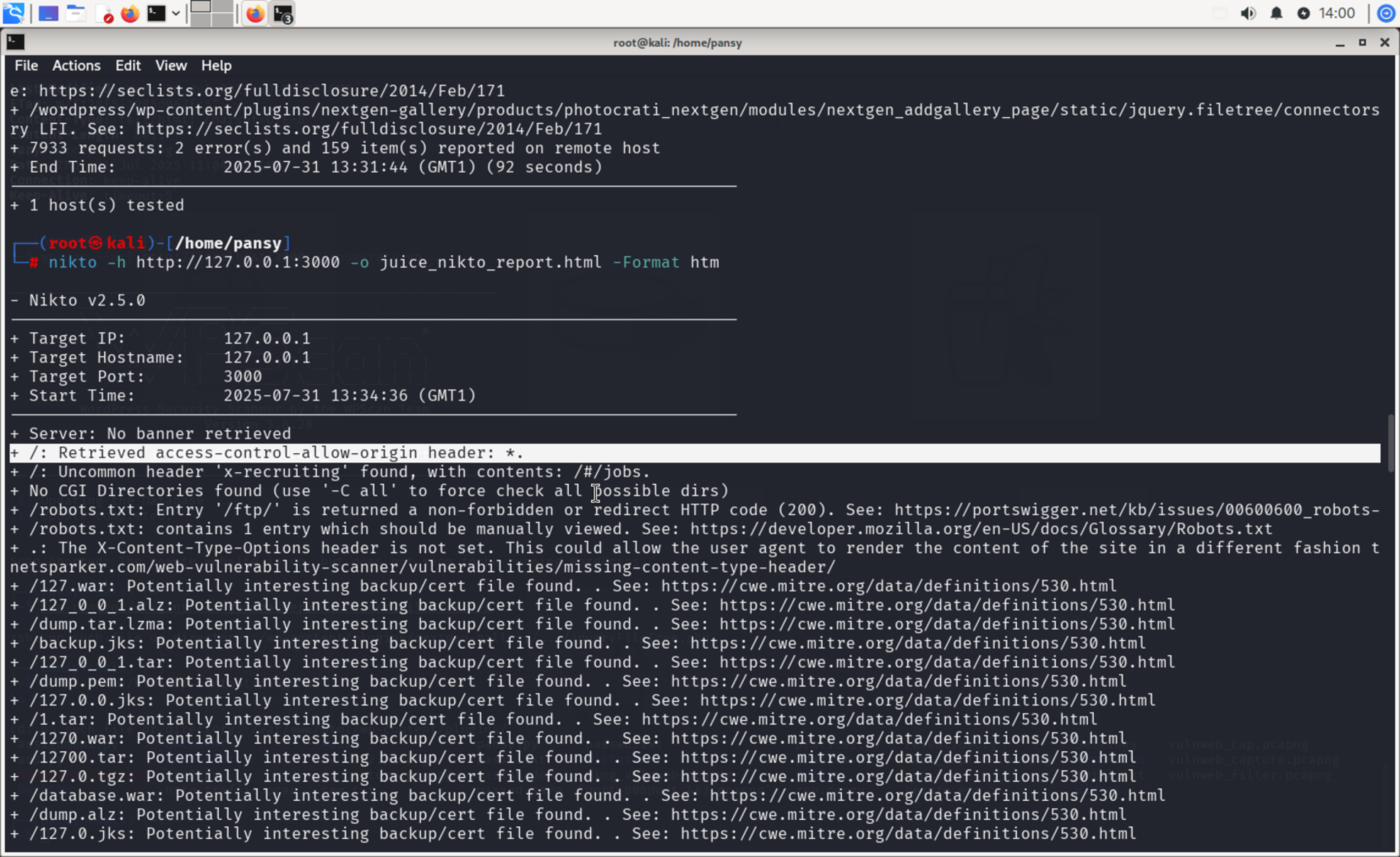
OWASP Mapping: A06:2021 - A05:2021 - Security Misconfiguration

Risks:

* Cross-Origin API Abuse
* Session Hijacking

Mitigation:

* Avoid using '\*' if authentication is used
* Use middleware to validate origins.

****

1. **Vulnerability: Local File Inclusion (LFI) in NextGEN Gallery Plugin**

Description**:**

LFI vulnerability in 'jqueryFileTree.php'. Exploitable via the 'dir' parameter to read arbitrary files.

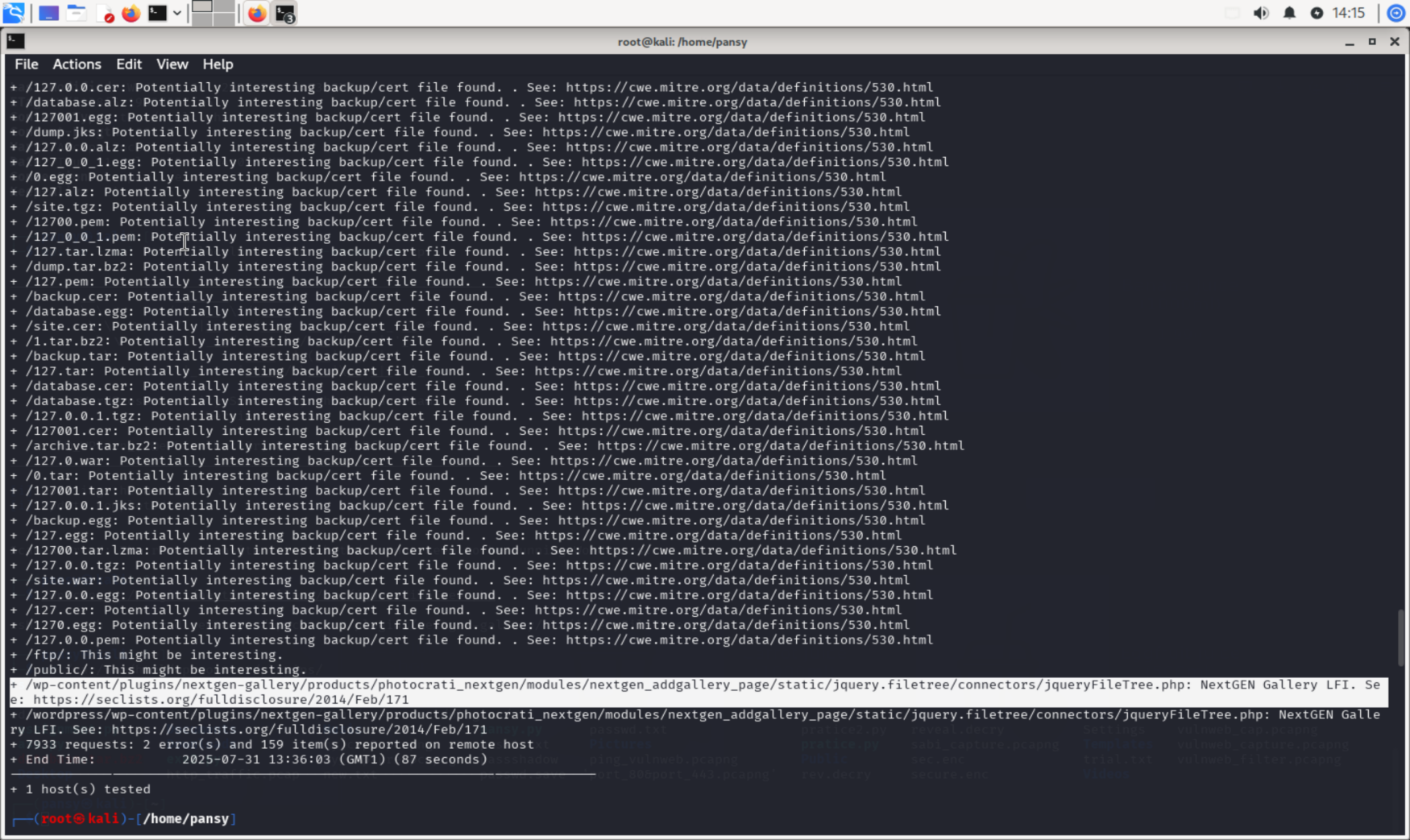
Impact Level**:** Critical

OWASP Mapping: A01:2021 - Broken Access Control

Risks:

* Cross-Origin API Abuse
* Session Hijacking

Mitigation:

* Avoid using '\*' if authentication is used
* Use middleware to validate origins.

1. **Vulnerability: Uncommon HTTP Header - X-Recruiting**

Description**:**

Found uncommon header 'X-Recruiting: /#/jobs'. Could disclose internal routes.

Impact Level**:** Low to High

OWASP Mapping: A06:2021 - Vulnerable and Outdated Components

Risks:

* Information Disclosure
* Application Fingerprinting

Mitigation:

* Remove or sanitize custom headers.
* Secure internal paths with authentication.

