2/26/2026

Challenge-04

Solving CTF Labs on ThunderCipher

YUVARAJ M

ThunderCipher – A02-Misconfig Writeup

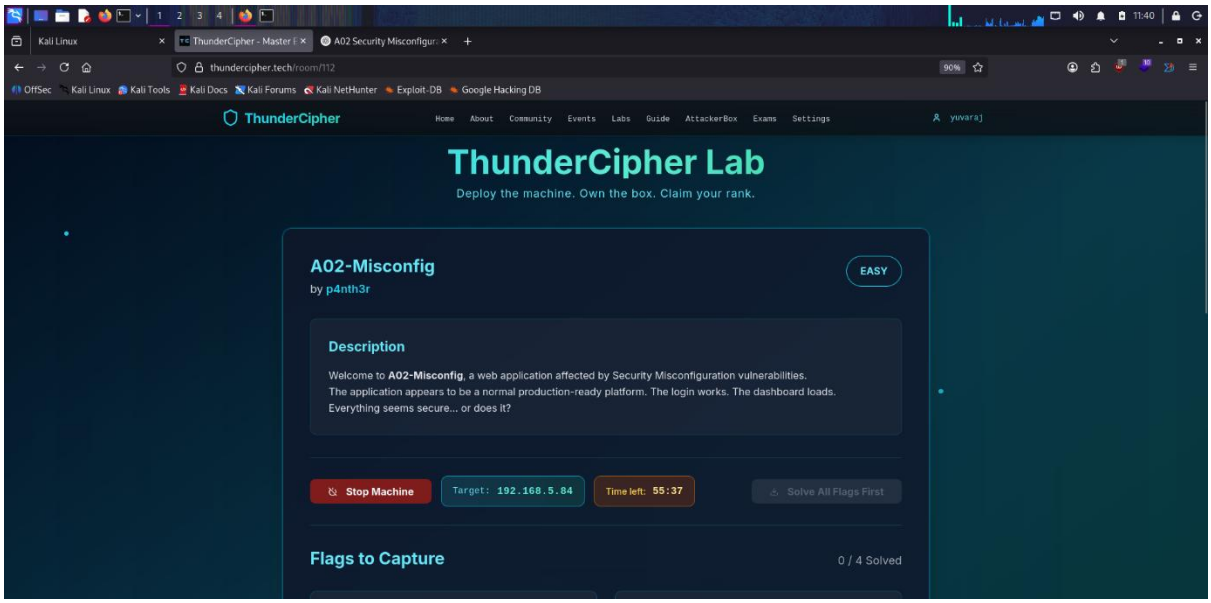
Difficulty: Easy

Category: Web Exploitation

Vulnerability: OWASP A02 – Security Misconfiguration

Target IP: 192.168.5.84

Port: 80



Challenge Description

Welcome to A02-Misconfig, a web application affected by Security Misconfiguration vulnerabilities.

The application appears to be a normal production-ready platform. The login works. The dashboard loads. Everything seems secure… or does it?

The objective of this challenge was to enumerate the application and identify security misconfigurations leading to sensitive information disclosure and privilege escalation.

Methodology

- **Port Scanning**
- **Service Enumeration**
- **Directory Brute Forcing**
- **Sensitive File Analysis**
- **Source Code Inspection**
- **Credential Exploitation**
- **Admin Panel Access**

Phase 1 – Port Scanning

Tool Used: **Nmap**

Command Used: **nmap 192.168.5.84 -sV -A**

Explanation:

- **-sV → Service version detection**
- **-A → OS detection, script scanning, traceroute**

Results:

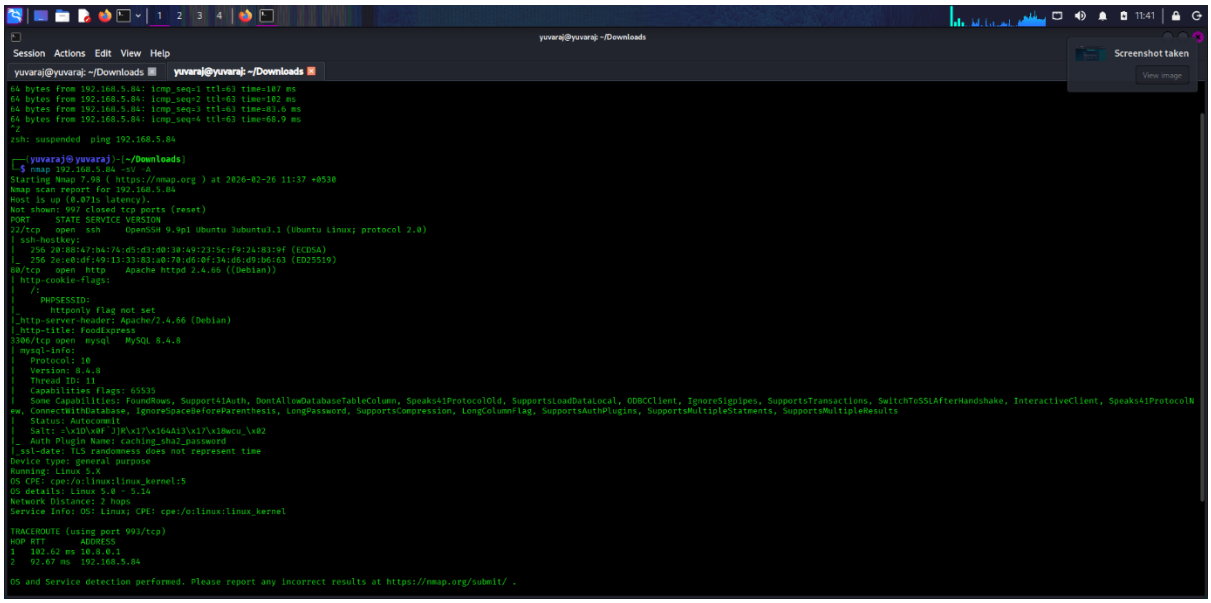
Open Ports:

• 22/tcp – SSH

• 80/tcp – HTTP (Apache 2.4.66 Debian)

Port 80 was identified as the primary attack surface.

Screenshot 1 – Nmap Scan Output



Phase 2 – Directory Enumeration

Tool Used: **Gobuster**

Command Used:

**gobuster dir -u http://192.168.5.84 **

**-w /usr/share/wordlists/dirb/common.txt **

-x php,txt,zip,bak,env

Explanation:

- dir → Directory mode
- -u → Target URL
- -w → Wordlist
- -x → File extension brute-forcing

Extensions searched:

php, txt, zip, bak, env

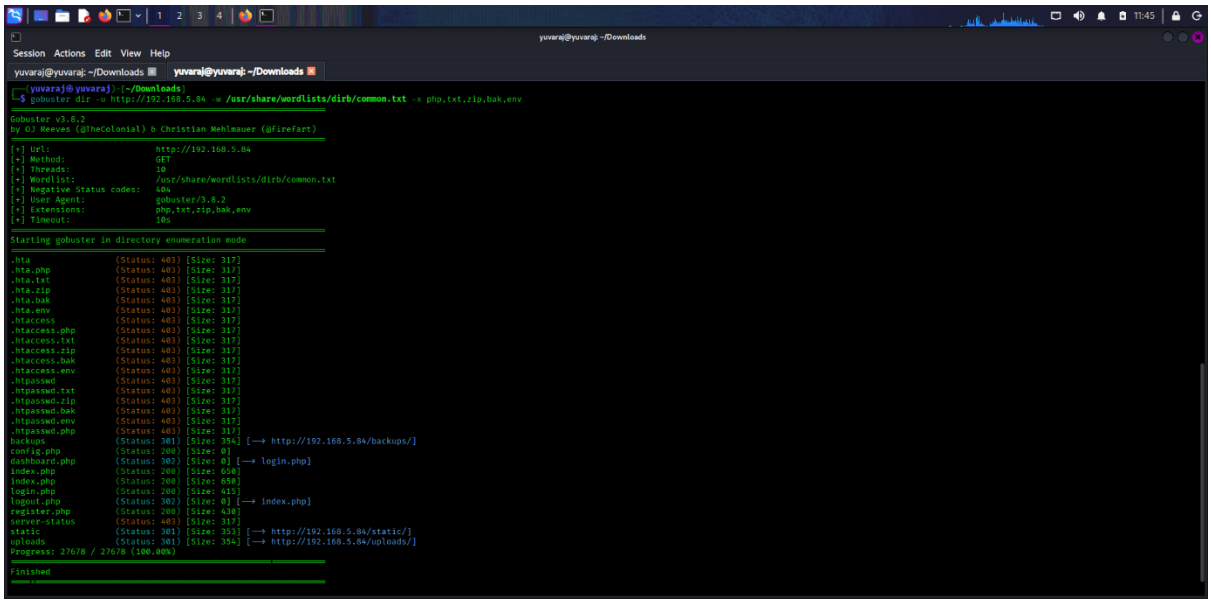
Discovered Endpoints

- **/login.php**
- **/register.php**
- **/.env**
- **/backups**
- **/config.php**

Critical findings:

- **/.env**
- **/backups**

Screenshot 2 – Gobuster Output Showing Discovered Files



Phase 3 – Exposed Environment File

Accessed: http://192.168.5.84/.env

- The environment file was publicly accessible.

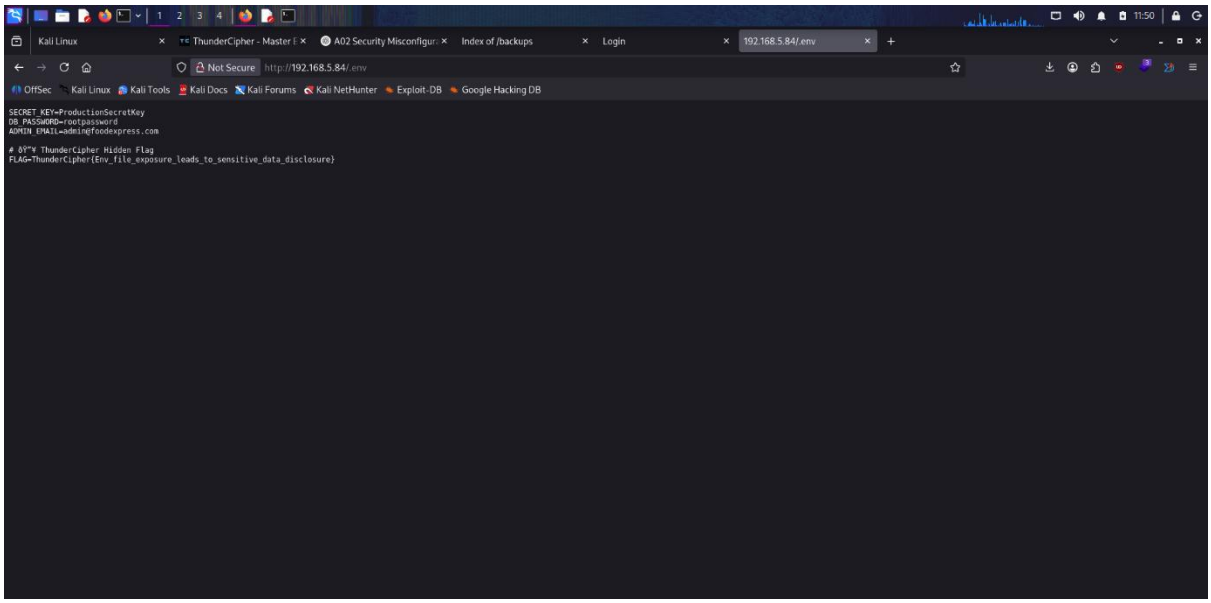
Sensitive information exposed:

- SECRET_KEY
- DB_PASSWORD
- ADMIN_EMAIL
- FLAG

Flag 1

ThunderCipher{Env_file_exposure_leads_to_sensitive_data_disclosure}

Screenshot 3 – .env File Contents with Flag Visible



Phase 4 – Backup File Exposure

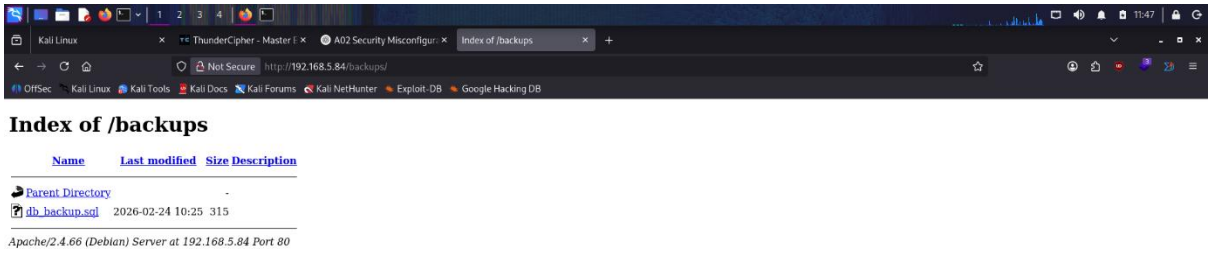
Accessed: http://192.168.5.84/backups/

- Backup files were publicly accessible.
- Sensitive internal data was retrieved.

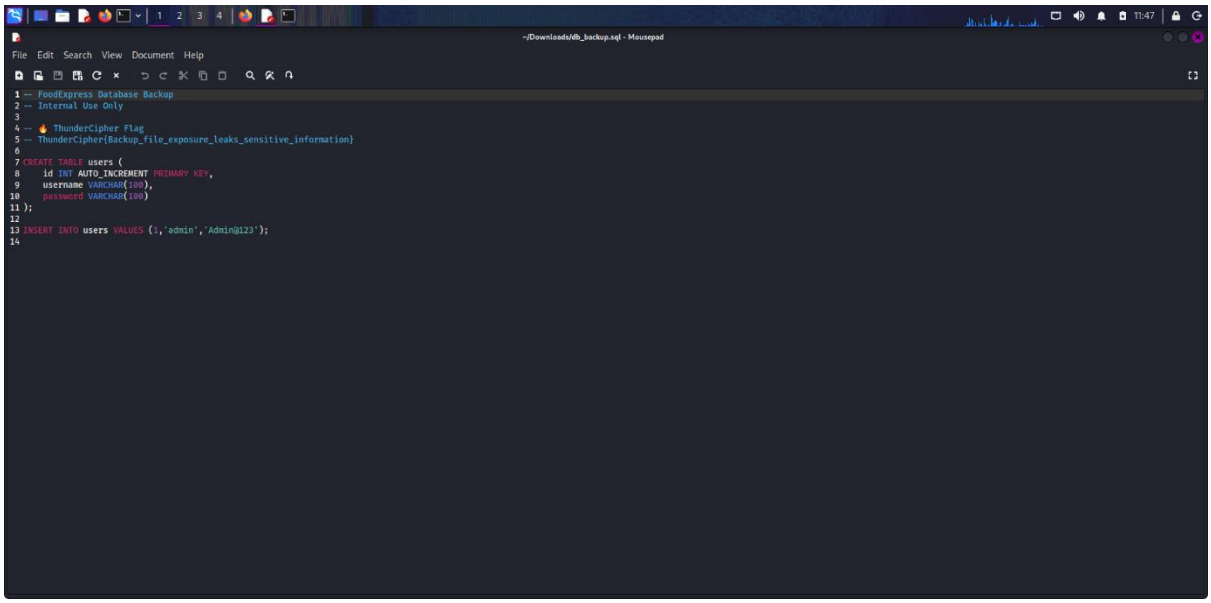
Flag 2

ThunderCipher{Backup_file_exposure_leaks_sensitive_information}

Screenshot 4 – Backup Directory Listing



Screenshot 5 – Extracted Backup File Showing Flag



Phase 5 – Source Code Inspection

- Viewed page source of the application.

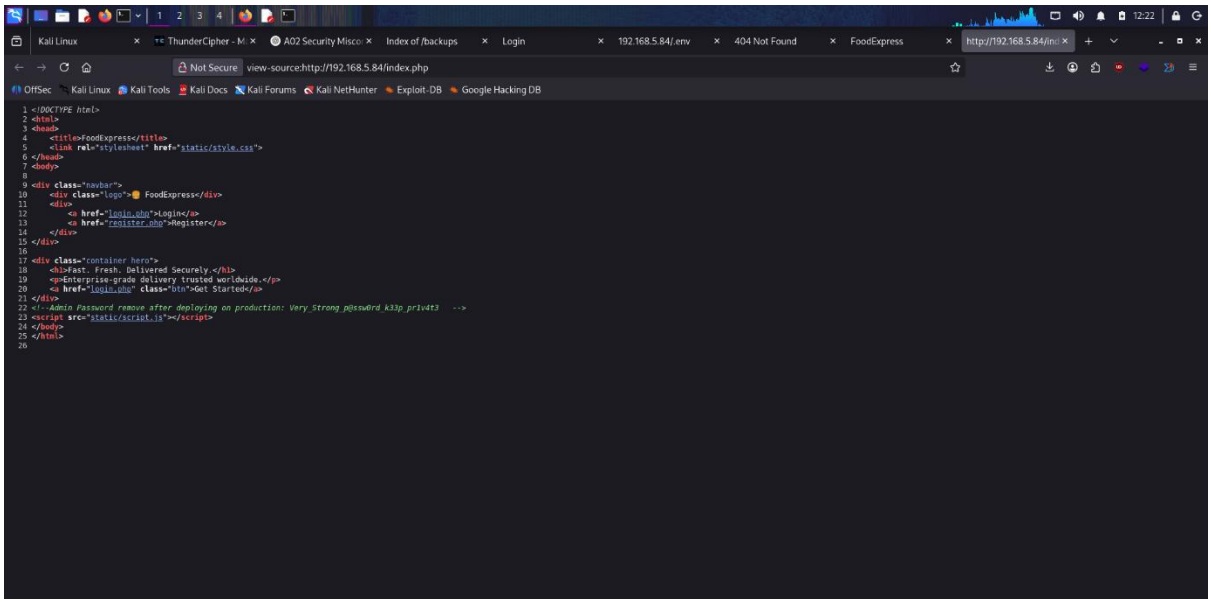
Discovered HTML comment containing admin credentials:

<!--Admin Password remove after deploying on production:

Very_Strong_p@ssw0rd_k33p_pr1v4t3-->

This indicates poor deployment practices.

Screenshot 6 – Page Source Showing Hardcoded Password



Phase 6 – Admin Login

Accessed: http://192.168.5.84/login.php

Credentials used:

Username: **admin**

Password: Very_Strong_p@ssw0rd_k33p_pr1v4t3

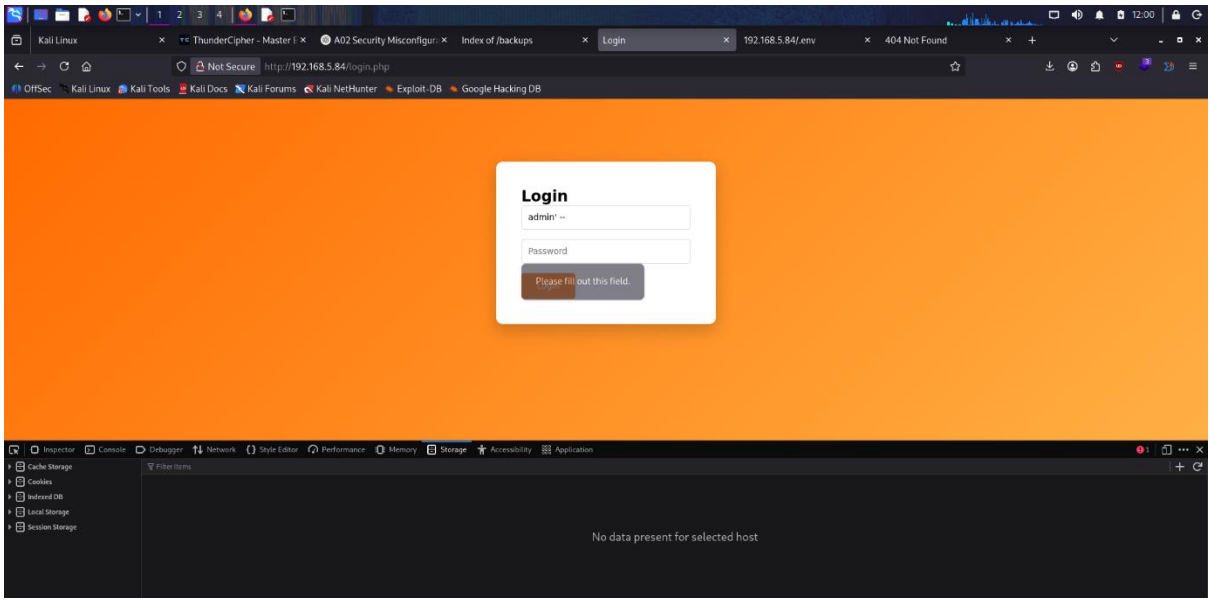
Login successful.

Admin panel revealed final flag.

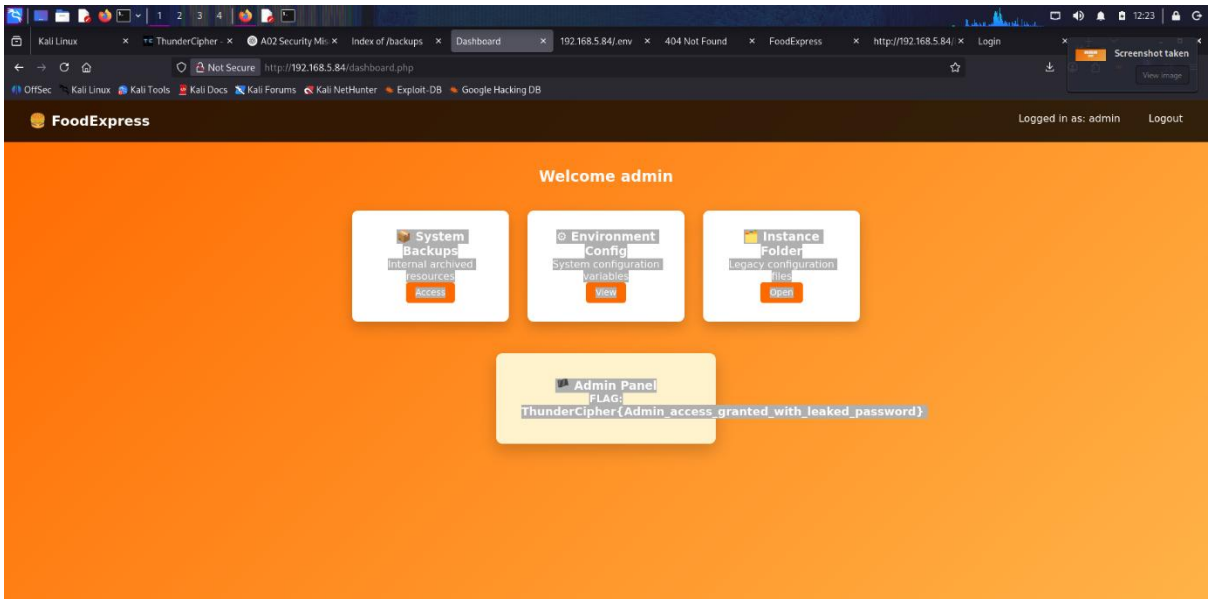
Final Flag

ThunderCipher{Admin_access_granted_with_leaked_password}

Screenshot 7 – Admin Login Page



Screenshot 8 – Admin Dashboard with Final Flag



Vulnerability Analysis

Vulnerability Type

- OWASP Top 10 – A02: Security Misconfiguration

Issues Identified

• Publicly accessible .env file

• Exposed backup directory

• Hardcoded credentials in HTML comments

• Sensitive data exposed in production

Impact

• **Credential disclosure**

• **Database compromise**

• **Privilege escalation**

• **Full administrative takeover**

In real-world applications, this could lead to:

• Data breach

• System compromise

• Reputation damage

Remediation

- Block access to sensitive files via web server configuration
- Store .env files outside web root
- Remove backup files from public directories
- Remove debug information before deployment
- Conduct configuration audits before production

Attack Flow Summary

- **Performed Nmap scan → Identified open services**
- **Used Gobuster → Found hidden endpoints**
- **Accessed .env → Retrieved Flag 1**
- **Accessed backups → Retrieved Flag 2**
- **Inspected source code → Found admin credentials**
- **Logged in as admin → Retrieved Final Flag**

Final Flags Collected

ThunderCipher{Env_file_exposure_leads_to_sensitive_data_disclosure}

ThunderCipher{Backup_file_exposure_leaks_sensitive_information}

ThunderCipher{Admin_access_granted_with_leaked_password}