HUNTER X HUNTER

# Web App Pentesting

hunterxhunter.com

# Agenda

1 Introduction

2 Methodology

3 Recon

4 Key Findings

5 Recommendations

6 Conclusion

# Introduction

This penetration testing engagement was conducted on nahamstore.thm with the objective of identifying vulnerabilities and assessing the overall security posture of the web application.

The scope of the test included a comprehensive evaluation of the site's external and internal vulnerabilities, focusing on areas such as authentication, data handling, and overall infrastructure security

Back to Agenda

# Methodology

The testing followed industry-standard methodologies, including OWASP Top 10 and other commonly known attack vectors, to ensure a thorough analysis of the potential risks.

**Target: nahamstore.thm**

**Testing Type: Black-box**

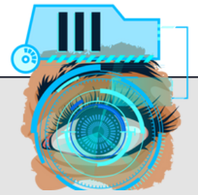
Back to Agenda

# Testing Phases

This penetration test on nahamstore.thm followed a structured and systematic approach based on industry-standard frameworks to thoroughly identify

## Reconnaissance

Objective: Map the application's architecture, identify potential attack vectors
Outcome: Open port 8000 was identified, hosting an admin panel, which was vulnerable due to weak credentials.



## Scanning

Objective: Identify misconfigurations, insecure coding practices, and exposure to known OWASP Top 10 risks.
Outcome: SQLi, XSS, CSRF, IDOR, and SSRF vulnerabilities were identified


## Exploitation

Once vulnerabilities were confirmed, exploitation attempts were made to assess the depth of impact.

## Reporting

Objective: Provide a clear, actionable report with reproducible steps for each vulnerability.
Outcome: Comprehensive recommendations for improving security posture.

Back to Agenda

# Recon

Tools Utilized:

This phase involved both passive and active reconnaissance techniques to gather intelligence about the target's infrastructure and applications. Subdomain enumeration using tools like sublist3r and subfinder provided a comprehensive list of domains.
Directory brute-forcing with gobuster and ffuf revealed hidden endpoints and directories that could be leveraged for further exploitation.

**Directory Enumeration**

**gobuster , ffuf**

---

**Subdomain Enumeration**

**sublist3r , subfinder**

---

**Wordlists**

**SecLists**

---

**Port Scan**

**nmap**

Back to Agenda

# Outcome

## Subdomains

marketing.nahamstore.thm
metric.12345678.nahamstore.thm
nahamstore-2020.nahamstore.thm
nahamstore.thm
shop.nahamstore.thm
stock.nahamstore.thm
www.nahamstore.thm

## Open port

port 8000 was identified, hosting an admin panel

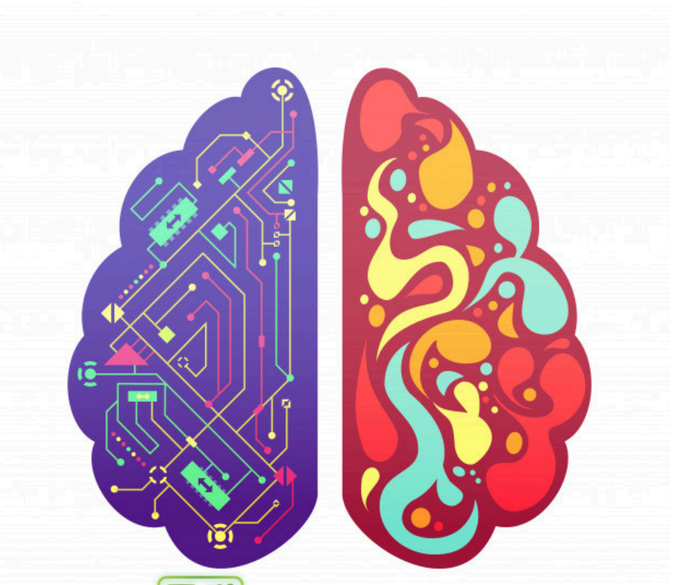
## Hidden Parameter

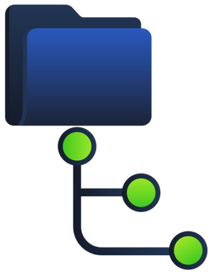
q , r , error , name

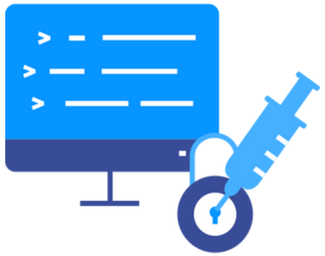
Back to Agenda

# Key Findings:

During the engagement, several vulnerabilities were discovered, with the key issues outlined below






## CSRF

2 csrf vulnerabilities that can lead to account take over in change password function and change e-mail function

## LFI

lfi vulnerability that lead the attacker to read sensitive files

## SQLI

sqli that led attacker to see all data of the app database

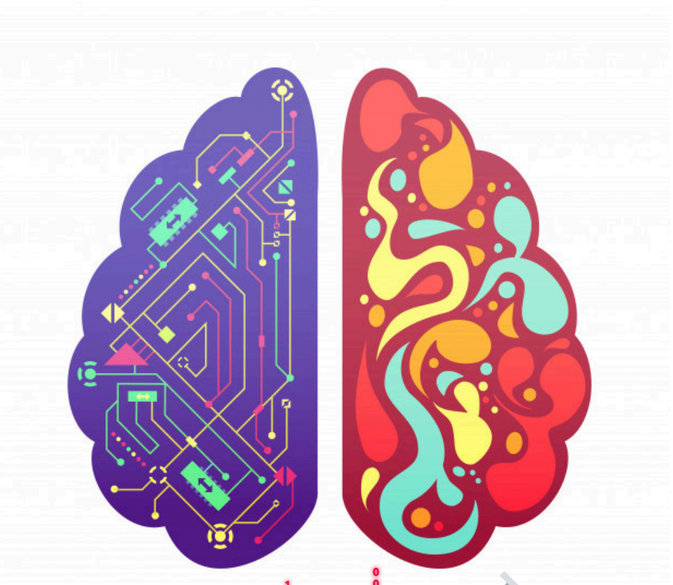
## SSRF

allows an attacker to manipulate server-side requests to interact with internal resources

Back to Agenda

# Key Findings:

During the engagement, several vulnerabilities were discovered, with the key issues outlined below

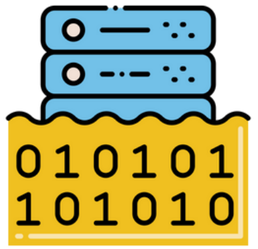


## XSS

many xss that the attacker cloud use it in different scenarios

## Open Redirect

open redirect that the attacker could use it in to redirect users to website the attacker control it




## Idor

discovered an Insecure Direct Object Reference vulnerability that allows unauthorized access to other users' information

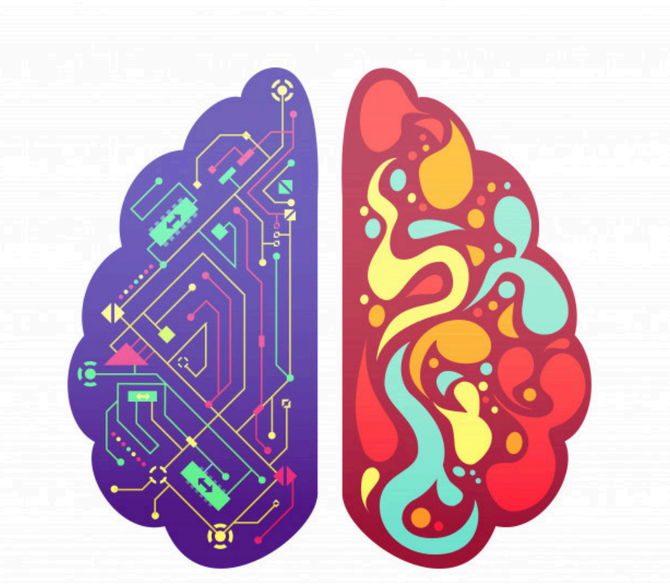

## XXE

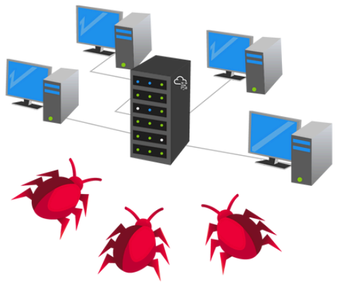
discovered an XML External Entity vulnerability in the application that allowed me to read sensitive server files

Back to Agenda

# Key Findings:

During the engagement, several vulnerabilities were discovered, with the key issues outlined below





## RCE

Discovered a Remote Code Execution vulnerability which allowed me to gain access to the server's machine.

## Maintain Access

after achieving (RCE) in a penetration test, create a persistent backdoor to access user privileges and deploying a hidden service in server machine

Back to Agenda


# Recommendations

Comprehensive recommendations for improving security posture, including enforcing strong credentials, fixing input validation issues

Implement CSRF Tokens: Use anti-CSRF tokens to protect all forms and state-changing actions from forged requests

---

Fix XSS: Sanitize and encode all user inputs and outputs to prevent script injection.
Use Content Security Policy (CSP) headers to mitigate XSS attacks.

---

Patch XXE Vulnerabilities: Disable or properly configure XML parsers to disallow external entity processing.

---

Prevent SQL Injection: Use parameterized queries or prepared statements to avoid direct execution of user inputs in SQL queries

---

Back to Agenda


# Recommendations

Comprehensive recommendations for improving security posture, including enforcing strong credentials, fixing input validation issues

Secure Object Access (IDOR):Implement proper access control mechanisms (such as Role-Based Access Control) to ensure users can only access their own resources.

---

Mitigate SSRF:Validate and sanitize all external URLs. Restrict requests to internal services and use allowlists.

---

Patch RCE:Validate and sanitize all inputs used in system commands or code execution functions. Restrict functionality to only trusted inputs.

---

Fix Open Redirect:Validate all redirect URLs and ensure that external redirects are properly flagged or avoided altogether

---

Back to Agenda


# Recommendations

Comprehensive recommendations for improving security posture, including enforcing strong credentials, fixing input validation issues

Mitigate LFI: Avoid direct inclusion of user-supplied file paths. Ensure only allowed files can be included and use proper validation techniques.

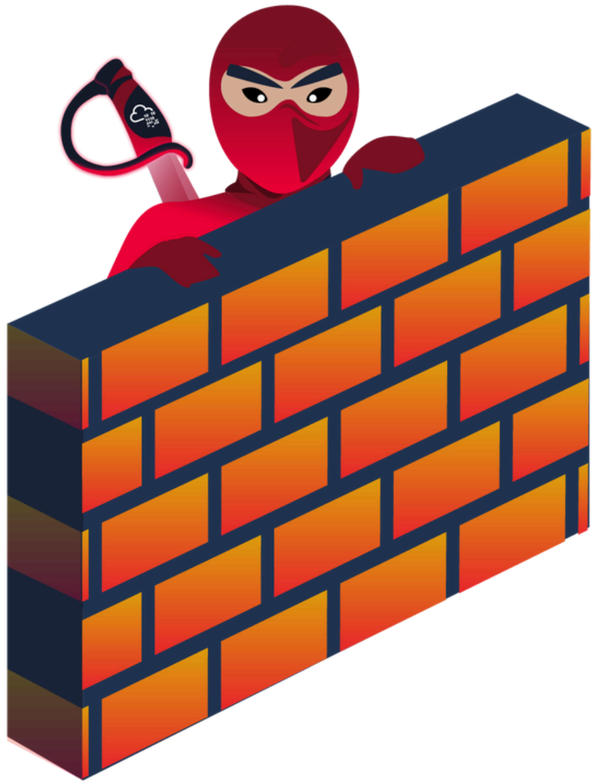
---

Strengthen Admin Panel Security: Close unnecessary open ports.

- Enforce strong password policies and remove default credentials.
- Implement two-factor authentication (2FA) for all administrative logins.

---

Back to Agenda



# General Security Recommendations:

**Conduct Regular Security Audits**: Perform regular vulnerability assessments and penetration testing.

**Use Web Application Firewalls (WAFs)**: Deploy a WAF to detect and block malicious traffic.

Keep Software Updated: Ensure all systems, software, and dependencies are regularly updated to prevent exploitation of known vulnerabilities.

Monitor for Suspicious Activity: Implement logging and monitoring solutions to detect unauthorized access and anomalies in real-time.

Back to Agenda

# Conclusion

In this assessment of the Naham Store web application, we uncovered several critical vulnerabilities that pose a significant risk to both the system's security and its users. The most severe issue, a Remote Code Execution (RCE) vulnerability, grants attackers full control over the system, allowing them to manipulate the website and access sensitive data. Additionally, the XML External Entity (XXE) vulnerability exposed crucial server files, while the Server-Side Request Forgery (SSRF) flaw allowed unauthorized internal network access.

These vulnerabilities demonstrate the importance of implementing strict security measures, such as enforcing stronger authentication methods, disabling unnecessary features, and properly validating user input. Immediate remediation is crucial to prevent exploitation and safeguard sensitive information. By addressing these issues and adhering to best practices, the Naham Store can significantly reduce its security risks and protect both its infrastructure and users from future attacks.

Back to Agenda

# Our Team

# Hunter X Hunter

**Yassen Alsayed**

Penetration tester

**Mahmoud Kroush**

Penetration tester

Back to Agenda

HUNTER X HUNTER

# Connect with us.


Email

**yassenalsayed91@gmail.com**

**kroush333@gmail.com**

Call-Us

**+20 1027610405**

**+20 1556139906**



# Thank You