Specialty Coffee Corporation
Security Assessment Findings Report

Business Confidential

Date: May 16, 2024
Project: DC-001
Version 1.0

Table of Contents

Table of Contents

Confidentiality Statement

This document is the exclusive property of Coffee Specialty Corporation and KOH Security (KOHS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Coffee Specialty Corporation and KOHS.

Coffee Specialty Corporation may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. KOHS prioritized the assessment to identify the weakest security controls an attacker would exploit. KOHS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

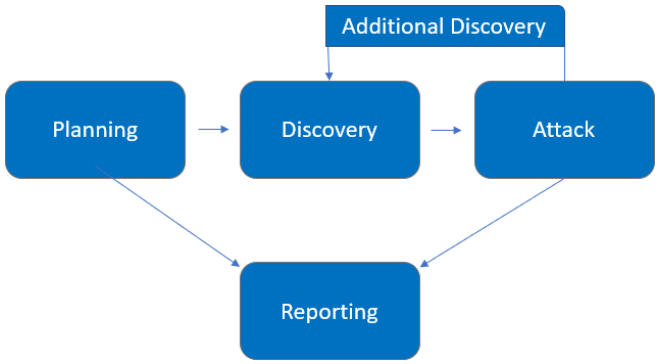
Name	Title	Contact Information
Specialty Coffee Corporation		
John Smith	Global Information Security Manager	Email: jsmith@specialtycoffee.com
KOH Security		
Jayden Koh	Lead Penetration Tester	Email: jkoh@jkoh.dev

Assessment Overview

From May 6, 2024, to May 16, 2024, Coffee Specialty Corporation engaged KOHS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Web Application Penetration Test

A web application penetration test emulates the role of an attacker from outside the network through the main website. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced web application network attacks, such as: SQL injection, cross-site scripting, code injection, insecure file upload, authentication attacks, XML entity injection, and broken object level authentication on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Web Application Penetration Test	http://localhost/capstone/*

Scope Exclusions

Per client request, KOHS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Coffee Specialty Corporation.

Client Allowances

Coffee Specialty Corporation provided KOHS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

KOHS evaluated Coffee Specialty Corporation's web application security posture through penetration testing from May 6, 2024, to May 16, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Web application network penetration testing was permitted for ten (10) business days.

Testing Summary

The website application assessment evaluated Coffee Specialty Corporation's internal network security posture. From an internal perspective, the KOHS team performed vulnerability scanning against all IPs provided by Coffee Specialty Corporation to evaluate the overall patching health of the network. The security team performed common web application-based attacks, such as SQL injection, cross-site scripting, code injection, insecure file upload, authentication attacks, XML entity injection, and broken object level authentication on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The KOHS team discovered the main website was vulnerable to a critical SQL injection (IPT-001) attack in the URL, when accessing different objects. This attack granted the team unlimited access to the entire database which included usernames and passwords for all registered users. This attack in combination with a weak password policy (IPT-004) resulted in the compromise of an admin account and multiple user accounts. The compromise of the admin account allowed the team to gain arbitrary code execution to the server through unrestricted file upload (IPT-002) through a weak file upload authentication service.

Another critical finding was stored Cross Site Scripting (Finding IPT-003), allowing malicious actors to exfiltrate sensitive client data such as session tokens and cookies. In addition to the critical compromises listed above, the KOHS team also found Reflected Cross Site Scripting (IPT-005) which can be used in combination with other attacks such as social engineering and phishing to exfiltrate sensitive client data. They also discovered a weak user authentication policy that did not include account lockouts, IP bans, or Multifactor Authentication (IPT-006) which would allow accounts to become compromised more easily. Another vulnerability was the lack of client-side brute force protection allowing unrestricted subdirectory busting (IPT-007).

Ultimately, the KOHS team was able to get arbitrary code execution on the web server through the multiple web application vulnerabilities and weak internal security protocols. For a full walkthrough of the path to arbitrary code execution, please see Finding IPT-008.

For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of the Coffee Specialty Corporation network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are vulnerabilities on the main website that come enabled by default, SQL injection, Cross Site Scripting, and weak authentication protocols.

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network. The presence of a weak password policy is backed up by the evidence of our testing team cracking over half of registered users' passwords through basic dictionary attacks.

We recommended that Coffee Specialty Corporation re-evaluates their current password policy and consider a policy of 15 characters or more for their regular user accounts and 30 characters or more for their administrator accounts. We also recommend that Coffee Specialty Corporation explore password blacklisting and supply a list of cracked user passwords for the team to evaluate.

The lack of user input sanitization through default configurations led to the compromise of the entire web server. We believe that with the use of basic input sanitization many of the critical vulnerabilities, SQL injection and Cross Site Scripting, would be mitigated. We believe the number of compromised machines would have been significantly larger, however the KOHS and Coffee Specialty Corporation teams agreed it was not necessary to attempt to exploit any remote code execution (RCE) based vulnerabilities as the web server had already been compromised and the teams did not want to risk any denial of service through failed attacks.

We recommend that the Coffee Specialty Corporation team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that Coffee Specialty Corporation improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The Coffee Specialty Corporation Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the Coffee Specialty Corporation network performed as expected for a first-time penetration test. We recommend that the Coffee Specialty Corporation team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus).
2. Proper access control of user privileges.

The following identifies the key weaknesses identified during the assessment:

1. Password policy was found to be insufficient.
2. User input was not sanitized properly.
3. Default configurations were used.
4. User authentication was not secured.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Web Application Penetration Test Findings

4	0	3	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Web Application Penetration Test		
IPT-001: SQL Injection	Critical	Sanitize database queries.
IPT-002: Unrestricted File Upload	Critical	Sanitize file uploads.
IPT-003: Stored Cross Site Scripting	Critical	Sanitize user input.
IPT-004: Insufficient Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-005: Reflected Cross Site Scripting	Moderate	Generate login messages from server side.
IPT-006: Weak Authentication Policy	Moderate	Enable Multifactor Authentication and lockout accounts.
IPT-007: Poor Access Policy	Moderate	Enable rate limiting and brute forcing detection
IPT-008: Steps to server compromise	Informational	Review action and remediation steps.

Technical Findings

Web Application Penetration Test Findings
IPT-001 SQL Injection (Critical)

Finding IPT-001: SQL Injection (Critical)

Description:	Coffee Specialty Corporation is vulnerable to SQL injection in the "coffee" parameter when viewing different objects. KOHS was able to retrieve the entire database with 6 user accounts and 3 admin accounts. The cracked accounts were used to leverage further access that led to the compromise of the webserver.
Risk:	Likelihood: High – This attack is effective in environments that don't sanitize input queries. Impact: Very High – SQL injection permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
System:	All
Tools Used:	Burpsuite, SQLMap
References:	OWASP Guidelines - Explanation of SQL injection SQL Injection Remediation – Explanation of SQL injection sanitization

Evidence

```
Table: users
[9 entries]
+---------+---------+------------------------------------------------------------+----------+
| user_id | type    | password                                                   | username |
+---------+---------+------------------------------------------------------------+----------+
| 1       | admin   | $2y$10$F9bvqz5eoawl                                        | jeremy   |
| 2       | admin   | $2y$10$meh2WXtPZgz                                         | jessamy  |
| 3       | admin   | $2y$10$cCXaMFLC.ym                                         | raj      |
| 4       | user    | $2y$10$ojC8YCMKX2r/                                        | bob      |
| 5       | user    | $2y$10$EPM4Unjn4wn                                         | maria    |
| 6       | user    | $2y$10$qAXjb233b7CM                                        | amir     |
| 7       | user    | $2y$10$37gojoTFmj8                                         | xinyi    |
| 8       | user    | $2y$10$5sVvPfZOjzR                                         | kofi     |
| 9       | user    | $2y$10$aG2kv15AqN5y                                        | bobby    |
+---------+---------+------------------------------------------------------------+----------+
```

Figure 1: Captured hash of "users" table.

```
┌──(kali㉿kali)-[~/peh/capstone]
└─$ hashcat -m 3200 hash /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt --show
$2y$10$F9bvqz5e                                                              :captain1
```

Figure 2: Cracked hash of "production".

Remediation

Blacklist certain characters like ";", "-", and "#", or whitelist only numeric characters. For full mitigation and detection guidance, please reference the OWASP guidance here.

Additionally, the cracked hashes demonstrate a deficient password complexity policy.

IPT-002 Unrestricted File Upload (Critical)

Finding IPT-002: Unrestricted File Upload (Critical)

Description:	KOHS utilized local administrator hashes to gain access to the admin panel at “admin.php” which was found through IPT-007. The local administrator hashes were obtained by dropping the users table via SQL injection in IPT-001. KOHS had unrestricted file upload permission because of weak image file checking. This led to the further compromise of the entire web server through remote code execution.
Risk:	Likelihood: High – The exploit was not difficult to craft. Impact: Very High – This attack is effective once attackers have access to the admin panel and will result in the compromise of the entire webpage.
System:	All
Tools Used:	Burpsuite
References:	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Evidence

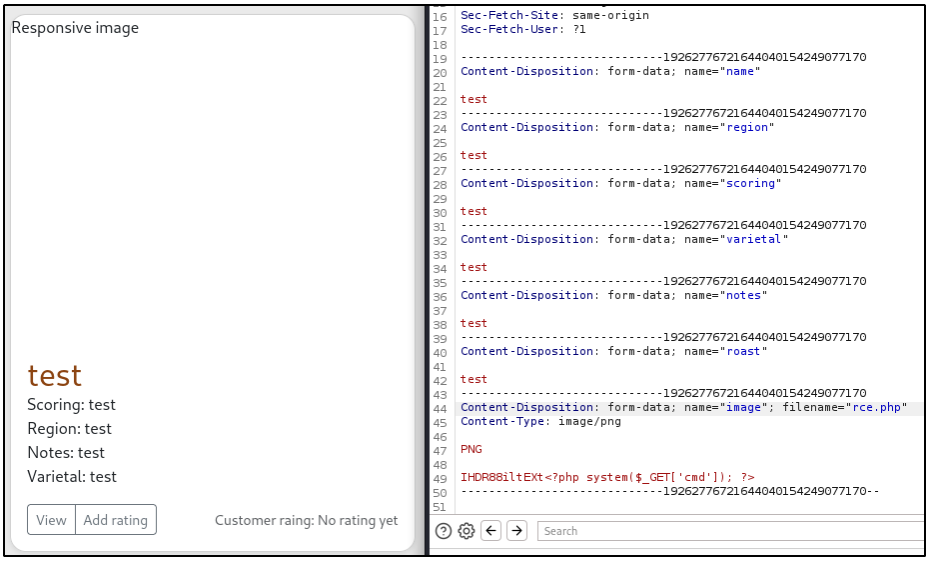


Figure 3: Uploading a PHP script as a picture through the admin panel.

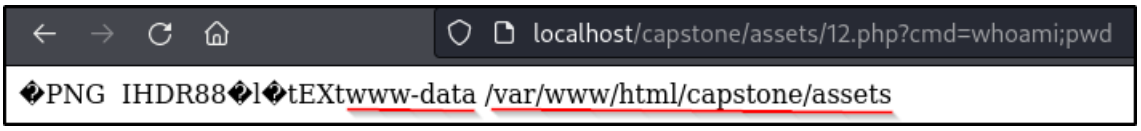


Figure 4: Remote code execution on the webserver.

Remediation

Sanitize file uploads, even from admin accounts, through whitelists of acceptable files and file extensions. For full mitigation and detection guidance, please reference the OWASP guidance here.

IPT-003 Stored Cross Site Scripting (Critical)

Finding IPT-003: Stored Cross Site Scripting (Critical)

Description:	Coffee Specialty Corporation permitted users to upload JavaScript code to the database which allowed for the exfiltration of multiple users' cookies and session tokens, compromising their accounts. KOHS leveraged account access gained to move laterally throughout the database and led to the discovery of a weak password policy (IPT-004).
Risk:	Likelihood: High – This attack is effective in all user input fields. Impact: Very High – Stored Cross Site Scripting affects any users who visit a vulnerable webpage (which is all of the pages).
System:	All
Tools Used:	Firefox
References:	https://owasp.org/www-community/attacks/xss/

Evidence

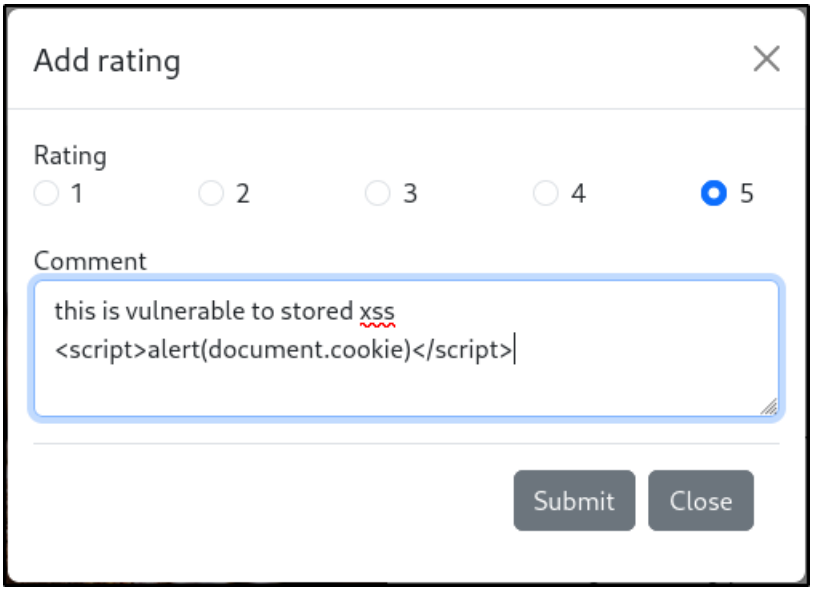


Figure 5: Submitting a malicious payload through the rating service.

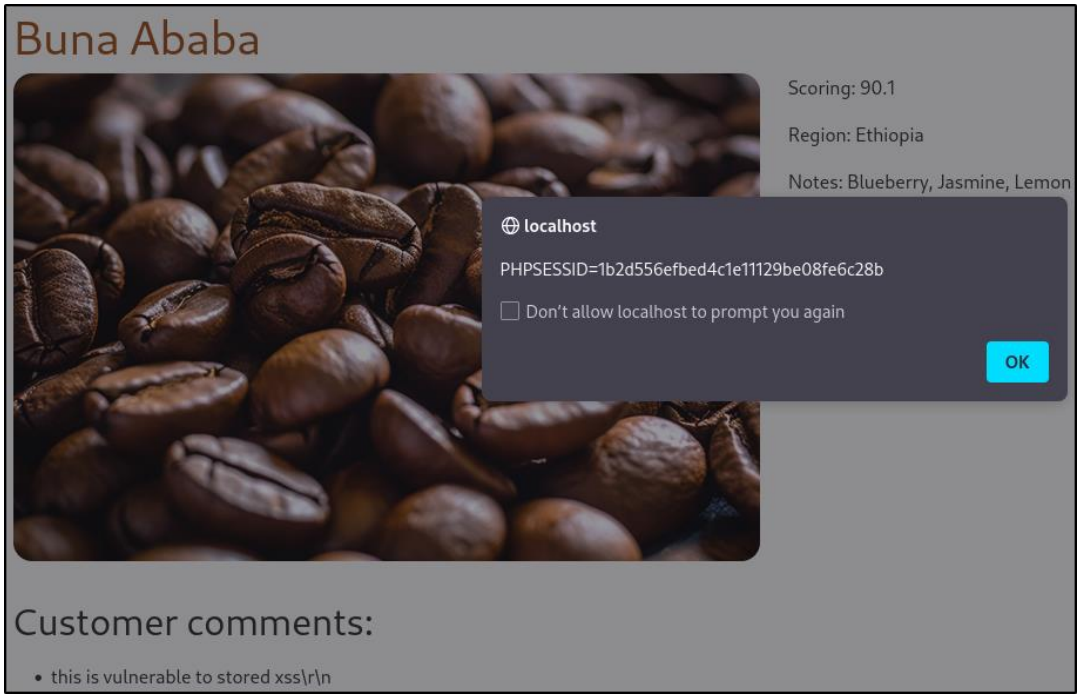


Figure 6: Effects of stored cross site scripting.

Remediation

Sanitize user input. For full mitigation and detection guidance, please reference the OWASP guidance here.

IPT-004 Insufficient Password Complexity (Critical)

Finding IPT-004: Insufficient Password Complexity (Critical)

Description:	KOHS dumped hashes from the database and proceeded to attempt common password guessing attacks against all users. KOHS cracked 5 passwords using basic password list guessing attacks and low effort brute forcing attacks. 1 cracked account had administrator rights.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords. Impact: Very High - Admin accounts with weak passwords could lead to an adversary critically impacting Coffee Specialty Corporation ability to operate.
System:	All
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

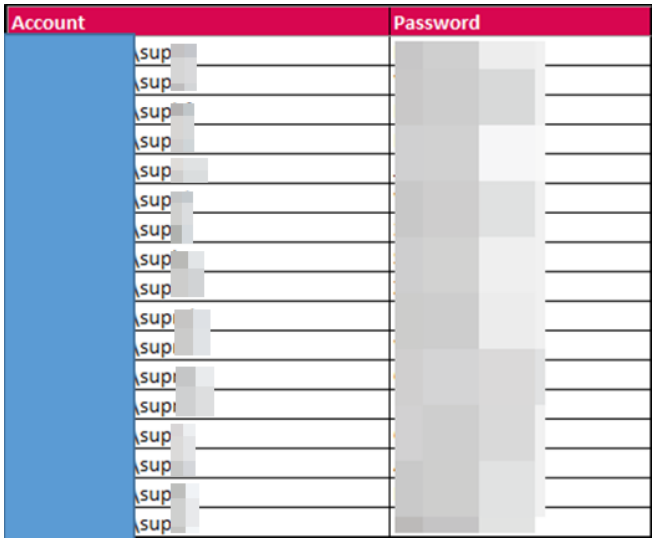


Figure 7: Excerpt of cracked hashes.

Remediation

Implement CIS Benchmark password requirements / PAM solution. KOHS recommends that Coffee Specialty Corporation enforce industry best practices around password complexity and management. A password filter to prevent users from using common and easily guessable passwords is also recommended. Additionally, KOHS recommends that Coffee Specialty

Corporation enforce stricter password requirements for Domain Administrator and other sensitive accounts.

IPT-005 Reflected Cross Site Scripting (Moderate)

Finding IPT-005: Reflected Cross Site Scripting (Moderate)

Description:	Coffee Specialty Corporation permitted users to upload JavaScript code to the database which allowed for the exfiltration of multiple users' cookies and session tokens, compromising their accounts. KOHS leveraged account access gained to move laterally throughout the database and led to the discovery of a weak password policy (IPT-004).
Risk:	Likelihood: High – This attack is effective in all user input fields. Impact: Moderate –Reflected Cross Site Scripting affects any users who visit a vulnerable webpage from a malicious source such as phishing.
System:	All
Tools Used:	Firefox
References:	https://owasp.org/www-community/attacks/xss/

Evidence

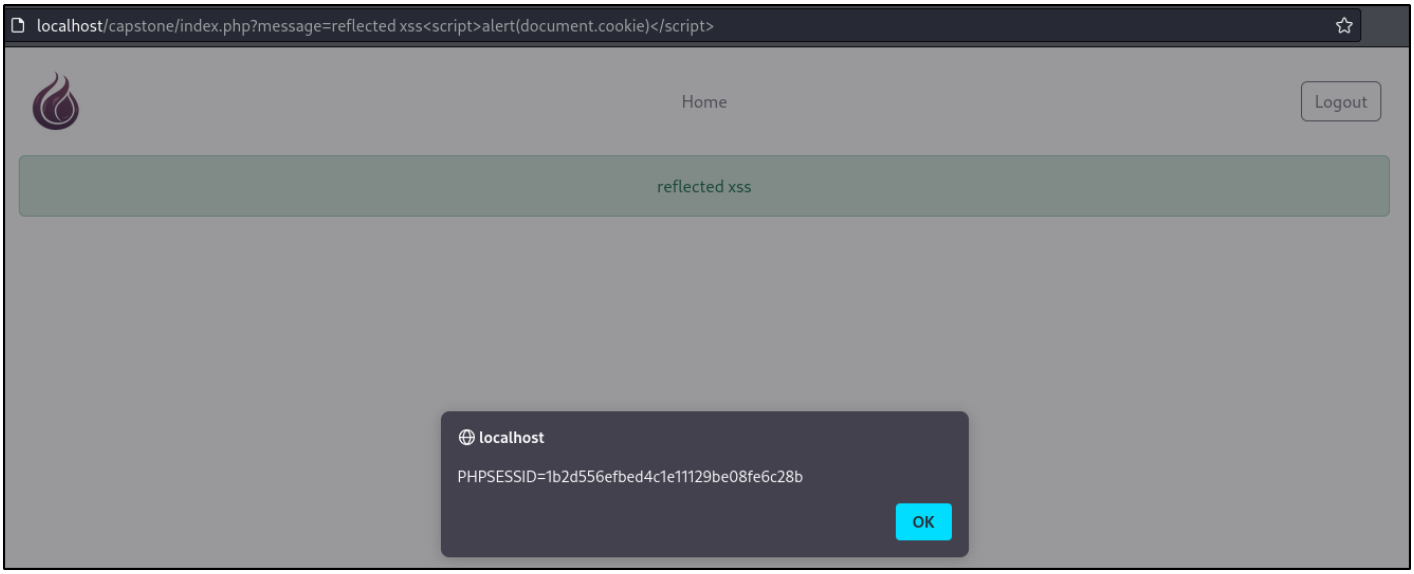


Figure 8: Reflecting a user's cookie to themself.

Remediation

Sanitize user input or generate login messages from server side. For full mitigation and detection guidance, please reference the OWASP guidance here.

IPT-006 Weak Authentication Policy (Moderate)

Finding IPT-006: Weak Authentication Policy (Moderate)

Description:	Coffee Specialty Corporation failed to implement secure authentication protocols allowing attackers to brute force multiple services.
Risk:	Likelihood: High – Relaying password hashes is a basic technique not requiring offline cracking. Impact: Moderate – Weak authentication policies in conjunction with other attacks such as acquiring breached data and weak password policies could lead to the compromise of user accounts.
System:	All
Tools Used:	Burpsuite, Hydra
References:	https://www.loginradius.com/blog/identity/authentication-vulnerabilities-security/

Evidence

A device's IP wasn't banned after 10+ failed account logins. There was also no multifactor authentication when valid credentials were supplied.

Remediation

Enable multifactor authentications for all accounts. Add a lockout policy for IPs and accounts to prevent brute forcing. For full mitigation and detection guidance, please reference the MITRE guidance here.

IPT-007 Poor Access Policy (Moderate)

Finding IPT-007: Poor Access Policy (Moderate)

Description:	KOHS was able to directly brute force all subdirectories on the webpage leading to the discovery of the admin panel.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: Moderate – If exploited, an attacker could possibly gain unauthorized access to services reserved for server admins.
Tools Used:	FFUF
References:	https://owasp.org/www-community/attacks/Brute_force_attack

Evidence

```
└─$ ffuf -u http://localhost/capstone/FUZZ -w /usr/share/wordlists/dirb/common.txt -recursion

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://localhost/capstone/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 14275, Words: 2458, Lines: 109, Duration: 92ms]
admin                   [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 4ms]
[INFO] Adding a new job to the queue: http://localhost/capstone/admin/FUZZ

assets                  [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 2ms]
[INFO] Adding a new job to the queue: http://localhost/capstone/assets/FUZZ

index.php               [Status: 200, Size: 14275, Words: 2458, Lines: 109, Duration: 66ms]
.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1004ms]
.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1136ms]
.hta                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1289ms]
[INFO] Starting queued job on target: http://localhost/capstone/admin/FUZZ

.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 4ms]
.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 6ms]
.hta                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 11ms]
                        [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 35ms]
admin.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 57ms]
[INFO] Starting queued job on target: http://localhost/capstone/assets/FUZZ

.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 6ms]
.hta                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 11ms]
.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 12ms]
                        [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 15ms]
:: Progress: [4614/4614] :: Job [3/3] :: 3846 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

Figure 9: Finding the admin panel through subdirectory brute forcing.

Remediation

Enable active scanning crawling detection. For full mitigation and detection guidance, please reference the MITRE guidance here.

IPT-008 Steps to Remote Code Execution (Informational)

Finding IPT-008: Steps to Remote Code Execution (Informational)

The steps below describe how the penetration tester obtained remote code execution. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Dropped database from SQL injection with SQLmap.	IPT-001
2	Crack admin password with Hashcat.	IPT-004
3	Find admin panel with FFUF.	IPT-007
4	Upload malicious PHP payload with Burpsuite.	IPT-002
5	Render PHP payload from an image.	Disable PHP from loading.

Remediation

Review action and remediation steps.

Additional Scans and Reports

KOHS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by KOH Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

Last Page