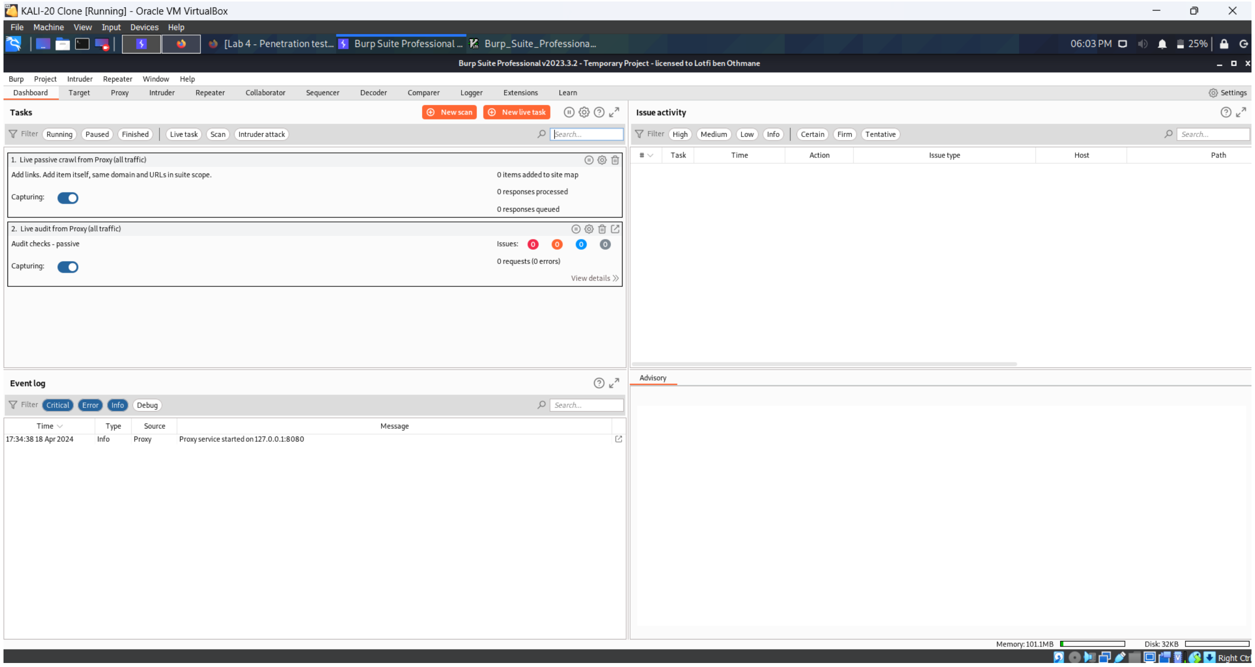
Lab 4: Penetration Testing

Team Members:

Nife Teye
Sowmya Reddy Tukakula

April 9, 2024

Q1 : Attach the screenshot of the login screen of BurpSuite Professional


KALI-20 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Lab 4 - Penetration test...
Burp Suite Professional ...
Burp_Suite_Professiona...
06:03 PM
25%
Burp Suite Professional v2023.3.2 - Temporary Project - licensed to Lotfi ben Othmane
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
# Task Time Action Issue type Host Path
Advisory
Event log
Filter Critical Error Info Debug
Search...
Memory: 101.1MB
Disk: 32KB
Right Ctrl

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing:

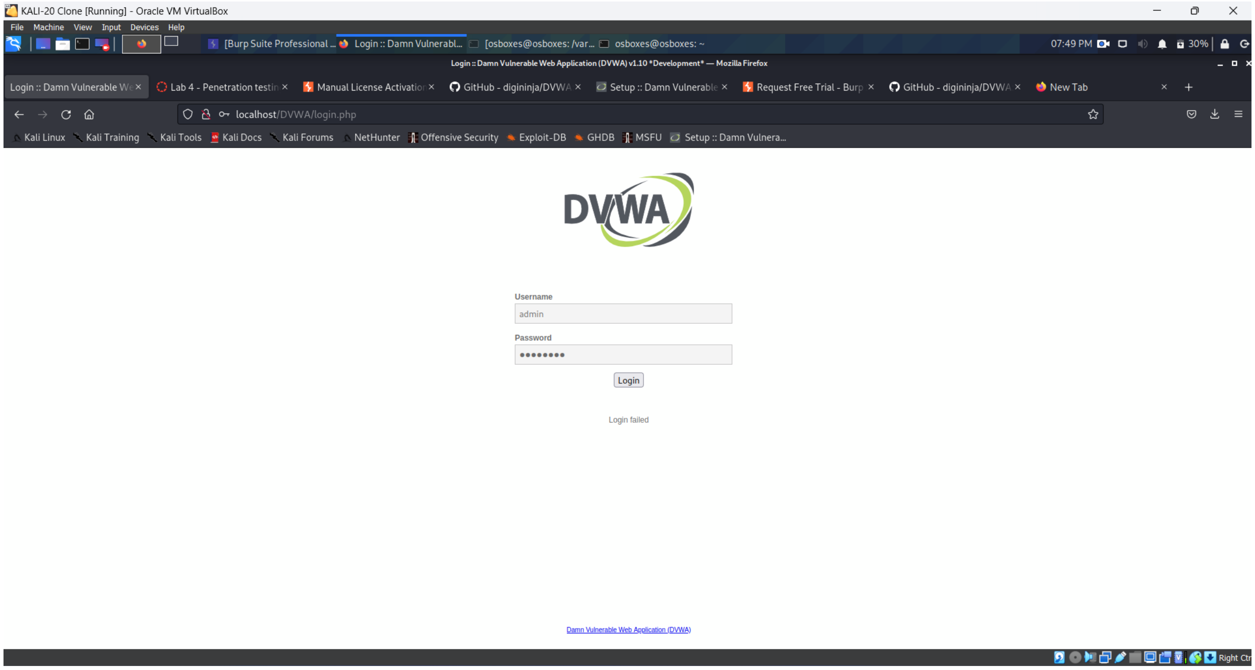
Issues: 0 0 0 0

0 requests (0 errors)

View details »

Time	Type	Source	Message
17:34:38 18 Apr 2024	Info	Proxy	Proxy service started on 127.0.0.1:8080

Q2. Attach the screenshot of login page of DVWA


KALI-20 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Burp Suite Professional ... Login :: Damn Vulnerabl... [osboxes@osboxes: /var... osboxes@osboxes: ~
07:49 PM 30%
Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* — Mozilla Firefox
Login :: Damn Vulnerable We
Lab 4 - Penetration testin
Manual License Activatio
GitHub - digininja/DVWA
Setup :: Damn Vulnerable
Request Free Trial - Burp
GitHub - digininja/DVWA
New Tab
localhost/DVWA/login.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Setup :: Damn Vulnera...
DVWA
Login
Damn Vulnerable Web Application (DVWA)
Right Ctrl

Username: admin

Password: ••••••••

Login failed

Q3: Attach the file output.html report to your submission.

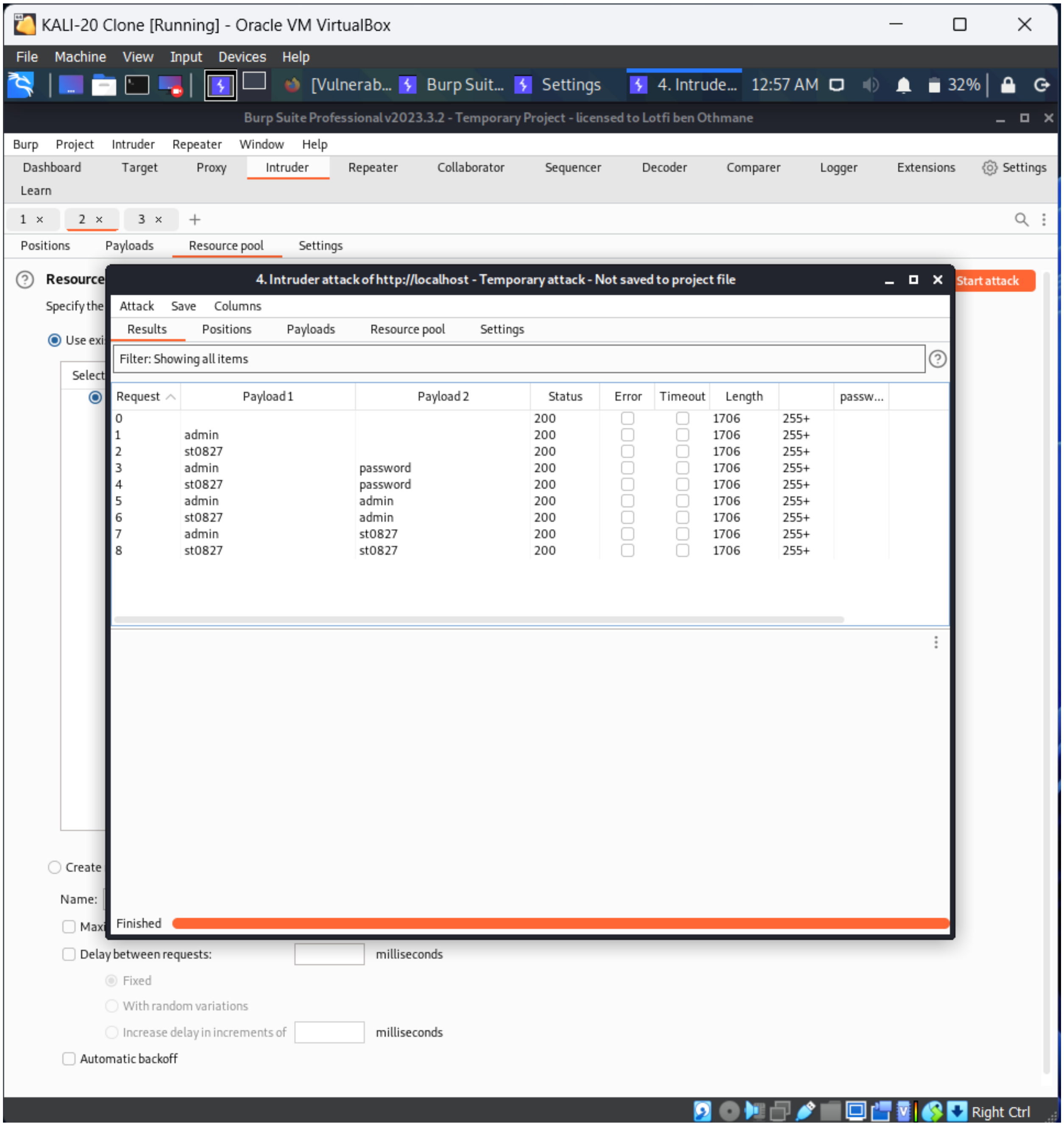
Attached the file

Q4 Reflect on the content of the report and provide your observations in one or two paragraphs.

The Burp Scanner Report provides a summary of identified security issues, categorized by severity and confidence level. The document outlines one high-severity issue with certain confidence related to the cleartext submission of passwords, which is a critical vulnerability as it can allow attackers to easily intercept passwords. Furthermore, there are other vulnerabilities identified, including one low-severity issue with certain confidence and multiple informational issues with varying degrees of confidence. This mixture of issues highlights the importance of a comprehensive approach to security, where even seemingly minor vulnerabilities should not be overlooked.

The detailed issues include unencrypted communications and path-relative stylesheet import attacks, indicating potential areas for improvement in securing data transmission and code integrity. It's also worth noting the inclusion of a potential clickjacking issue, which, while only informational, should be taken seriously. This report serves as a stark reminder of the multifaceted nature of web application security and the need for diligent, continuous testing and improvement to mitigate the risks of data breaches and unauthorized access.

Q5: Please attach the screenshot as above.


KALI-20 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Vulnerab... Burp Suit... Settings 4. Intrude... 12:57 AM 32%
Burp Suite Professional v2023.3.2 - Temporary Project - licensed to Lotfi ben Othmane
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Settings
Learn
1 × 2 × 3 × +
Positions Payloads Resource pool Settings
Start attack
Attack Save Columns
Results Positions Payloads Resource pool Settings
Right Ctrl

4. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length		passw...
0			200	☐	☐	1706	255+	
1	admin		200	☐	☐	1706	255+	
2	st0827		200	☐	☐	1706	255+	
3	admin	password	200	☐	☐	1706	255+	
4	st0827	password	200	☐	☐	1706	255+	
5	admin	admin	200	☐	☐	1706	255+	
6	st0827	admin	200	☐	☐	1706	255+	
7	admin	st0827	200	☐	☐	1706	255+	
8	st0827	st0827	200	☐	☐	1706	255+	

Finished

Q6: Reflect on your experience and describe your observations in two paragraphs.

This Lab is showing how cybersecurity issues and solutions work in the real world. By using Burp Suite, a tool for testing website security, learners get a hands-on chance to see how data requests can be intercepted, changed, and analyzed. The tasks of setting up a security scan and trying out different hacking techniques like brute force attacks help illustrate the complex interactions between a website's weaknesses and the strategies security experts use to test or secure them. This practical use of what's usually learned in theory helps bridge the gap between studying and applying knowledge, highlighting the need for strong security measures on websites.

The lab also underlines the importance of understanding both the tools and the thought processes of potential attackers. Setting up the testing environment, adjusting the proxy settings, and carrying out various attacks not only improve technical skills but also develop a strategic way of thinking about security. It's about thinking critically and solving problems, where you need to predict potential security gaps and act ahead of time to address them. The step-by-step nature of the lab ensures that learners can grasp why each security step or attack method is used, which helps build a deeper understanding of how to find, exploit, and fix security weaknesses. Seeing both the attacker's and defender's points of view gives a full picture of cybersecurity, which is essential for anyone looking to work in this area.