Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Table of Contents

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Contact Information

Company Name	DEEPFAKE LLC
Contact Name	Nickson Njau
Contact Title	Penetration tester

Document History

Version	Date	Author(s)	Comments
001	03/10/2024	Nickson Njau	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

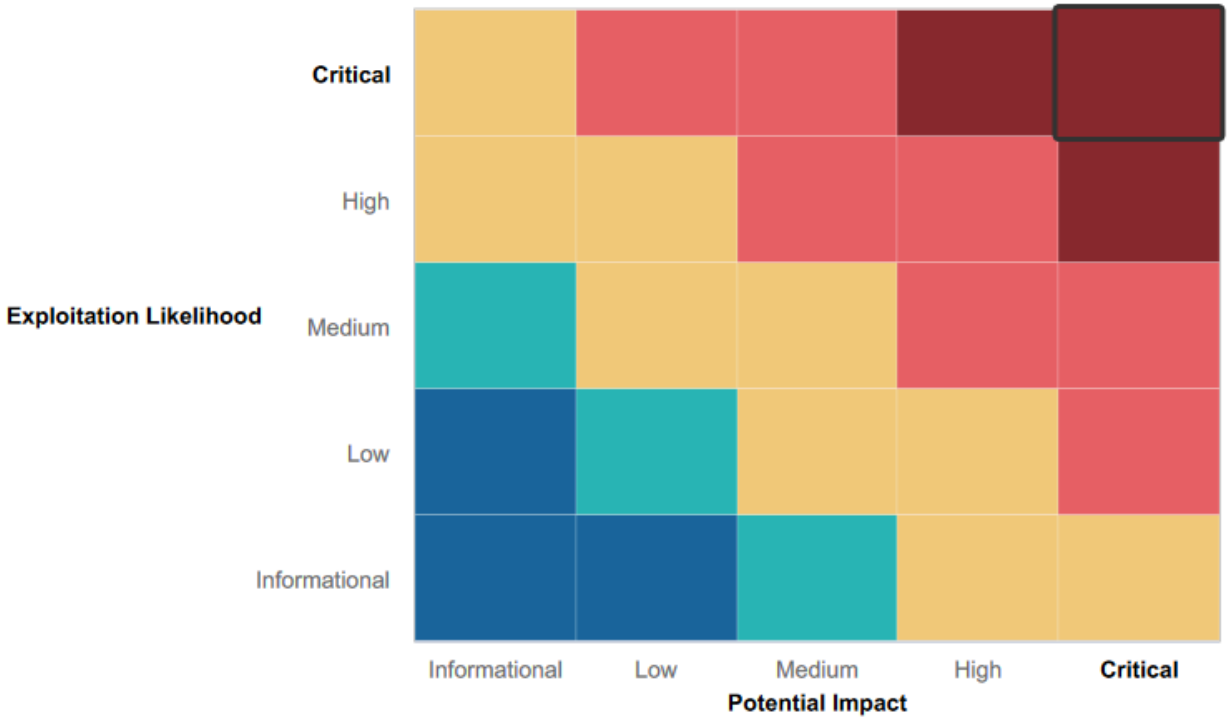
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Most input fields on the Rekall website use proper input validation.
- It took several attempts to find an input field that would accept a command injection.
- 6 exploitation scripts through Metasploit were run against the Apache server before one was successful.
- DEEPFAKE LLC did not have success attempting basic SQL injections against the web page and had to use advanced methods
- Forward-thinking defensive and offensive strategy
- Current and continuing penetration testing to identify vulnerabilities for mitigation

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- The Welcome.php and Memory-Planner.php(First field) pages are vulnerable to reflected XSS payload(1 and 2)
- The Comments.php page is vulnerable to Stored XSS(3)
- The Memory-Planner.php page is vulnerable to Local file inclusion(LFI) (5 and 6)
- The login.php(First field) page is vulnerable to SQL injection(7)
- The login.php(Second field) and robots.php pages are vulnerable to sensitive data exposure(8 and 9)
- The About-Rekall.php page has sensitive data exposure in HTTP response header(4)
- The webpage networking.php(First and second field) is vulnerable to command injection(10 and 11)
- The login.php page is vulnerable to brute force attacks (12)
- The souvenirs.php page is vulnerable to PHP injection(13)
- The disclaimer.php page is vulnerable to directory traversal(15)

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Executive Summary

As the lead pentestester at Deepfake LLC, I spearheaded an extensive security assessment to evaluate the resilience of our systems against potential cyber threats. Our comprehensive penetration testing journey involved probing various components of our infrastructure, including the Rekall web application, Linux servers, and Windows machines.

Our exploration began with the Rekall web application hosted at 192.168.14.35. Leveraging our expertise, we systematically navigated through the application, scrutinizing each component for vulnerabilities. We quickly identified critical weaknesses, such as Cross-Site Scripting (XSS) vulnerabilities on the welcome.php and Memory-Planner.php pages. These vulnerabilities allowed for the injection of malicious scripts, posing significant risks to user data and system integrity.

Moreover, our investigation revealed Stored XSS vulnerabilities on the Comments.php page, further emphasizing the application's susceptibility to exploitation. Additionally, a Local File Inclusion (LFI) vulnerability on the Memory-Planner.php page raised concerns about unauthorized file uploads and execution, highlighting the need for immediate remediation efforts.

Transitioning to our Linux servers, we uncovered a myriad of vulnerabilities that could potentially compromise our system's security. From the Apache Tomcat Remote Code Execution vulnerability (CVE-2017-12617) to the Shellshock vulnerability, each discovery underscored the importance of proactive security measures. Through meticulous analysis and exploitation, we gained unauthorized access to sensitive information, illustrating the severity of these vulnerabilities.

Turning our attention to the Windows machines within our network, we encountered vulnerabilities ranging from Sudo vulnerabilities to Cached credentials exploitation. By exploiting weaknesses in authentication mechanisms and leveraging known vulnerabilities, we successfully infiltrated the systems, demonstrating the critical need for robust security protocols.

Throughout our assessment, we prioritized thorough documentation of each vulnerability, including detailed descriptions, affected hosts, and recommended remediation measures. Our findings underscore the importance of proactive security measures, continuous monitoring, and adherence to best practices to safeguard our infrastructure against evolving threats.

In conclusion, our penetration testing endeavor revealed critical vulnerabilities across our web application, Linux servers, and Windows machines. By diligently documenting our findings and recommendations, we are better equipped to strengthen our security posture and mitigate potential risks in the future.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Summary Vulnerability Overview

Vulnerability	Severity
The Welcome.php and Memory-Planner.php(First field) pages are vulnerable to reflected XSS payload(1 and 2)WebApp	Critical
The Comments.php page is vulnerable to Stored XSS(3)WebApp	Critical
The Memory-Planner.php page is vulnerable to Local file inclusion(LFI) (5 and 6)WebApp	Critical
The login.php(First field) page is vulnerable to SQL injection(7)WebApp	Critical
The login.php(Second field) and robots.php pages are vulnerable to sensitive data exposure(8 and 9)WebApp The About-Rekall.php page has sensitive data exposure in HTTP response header(4)WebApp	Critical
The webpage networking.php(First and second field) is vulnerable to command injection(10 and 11)WebApp	Critical
The login.php page is vulnerable to brute force attacks (12)WebApp	High
The souvenirs.php page is vulnerable to PHP injection(13)WebApp	Critical
The disclaimer.php page is vulnerable to directory traversal(15)WebApp	High
Open source exposed data(1,2 and 3)	Critical
The Apache server(192.168.13.10) has the Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
The Linux server(192.168.13.11) has a Shellshock	Critical
The Linux server(192.168.13.12) has the Struts - CVE-2017-5638 vulnerability	Critical
The Linux(192.168.13.13) server has the Drupal - CVE-2019-6340	High
The Linux server(192.168.13.14) has a Sudo vulnerability(CVE-2019-14287)	High
The Windows10 PC allows anonymous FTP login	Critical
The Windows10 PC is running SLMail service which is exploitable	High
Cached credentials(lsa_dump) on Windows 10 reveal ADMBob and his hash	High
Windows10 pc is vulnerable to psexec	High
Using kiwi to DCsync the administrator reveals the NTLM hash	High

The following summary tables represent an overview of the assessment findings for this penetration test:

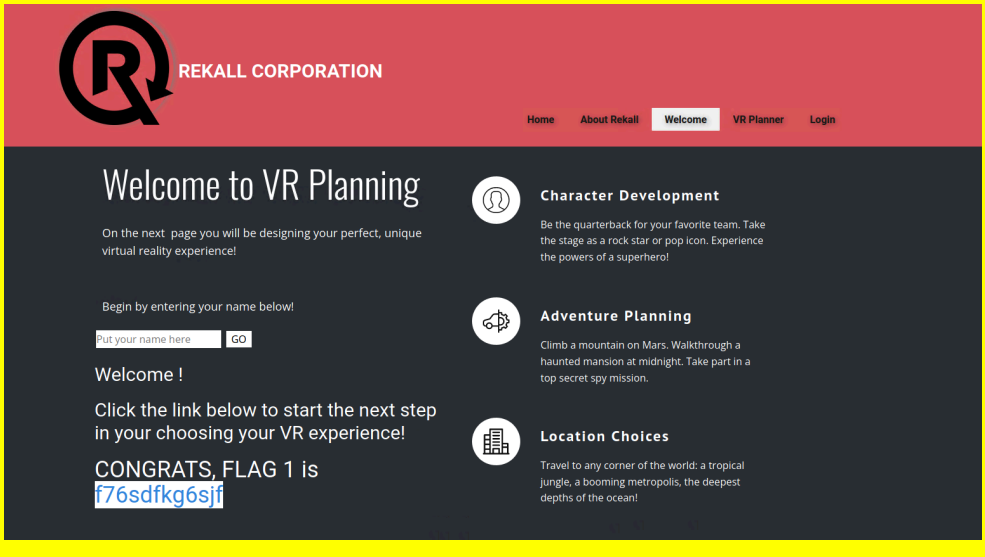
Scan Type	Total
Hosts	192.168.14.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Ports	80 (HTTP) 21(FTP), 25(SMTP), 110 (POP3), 135 (RPC), 8009 (TCP), 8080

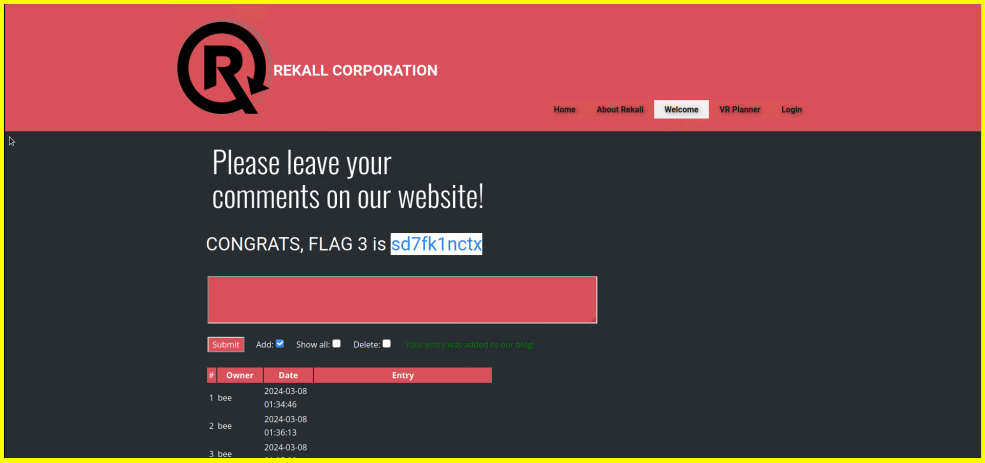
Exploitation Risk	Total
Critical	11
High	9
Medium	0
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS payload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Entering <script>alert(Document.cookie)</Script> enters a reflected XSS payload on welcome.php that reveals 1 The Memory-Planner.php filters out the script tag so it has to be split between another script word to work. Entering <SCRIPscriptT>alert("Hi")</SCRIPscriptT> enters the reflected XSS payload that reveals 2
Images	

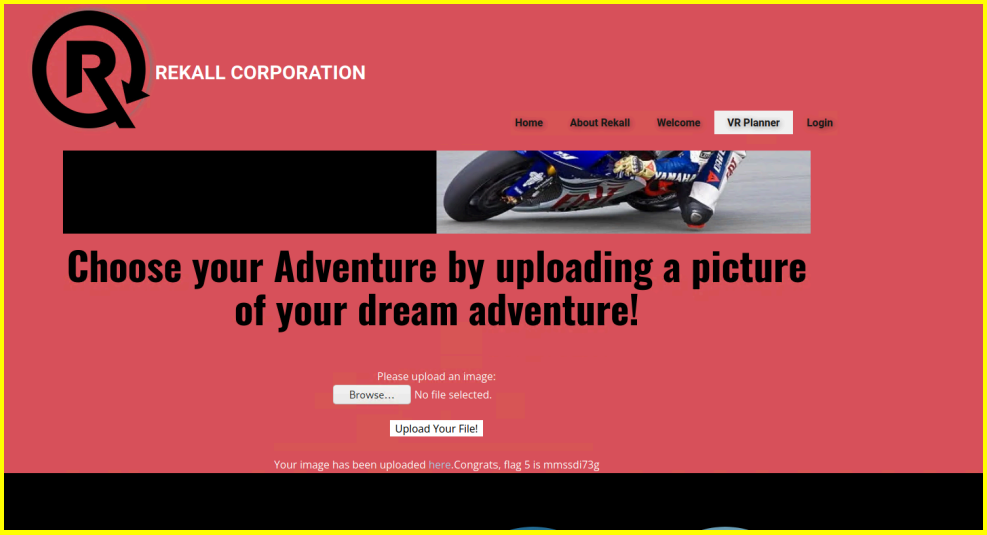
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.14.35 (Welcome.php, Memory-Planner.php)
Remediation	- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc) - Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input that fails the validation should be rejected, not sanitized.

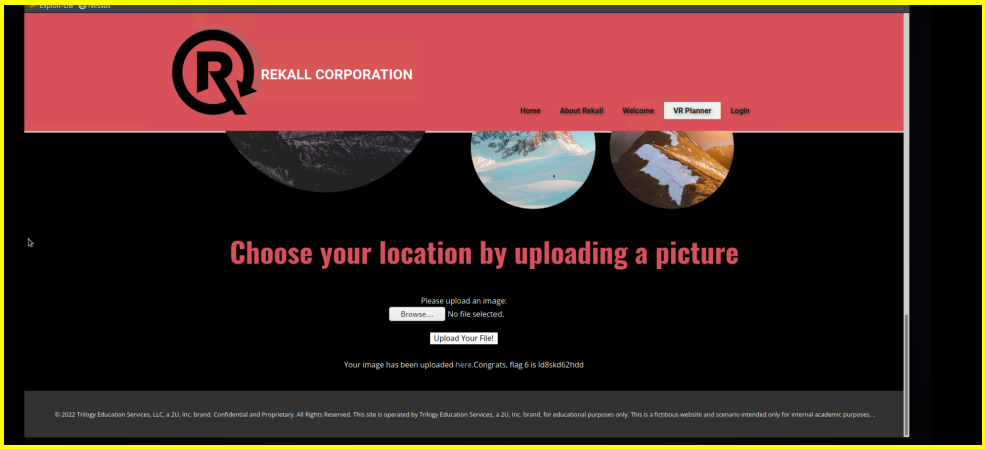
Vulnerability 2	**Findings**
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Webapp
Risk Rating	**Critical**
Description	The Comments.php page is vulnerable to stored XSS. Entering <script>alert(“hi”)</script> as a comment causes a popup which reveals 3
Images	
Affected Hosts	192.168.14.35(comments.php)
Remediation	- Input should be validated as strictly as possible on arrival, given the

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input that fails the validation should be rejected, not sanitized. - User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

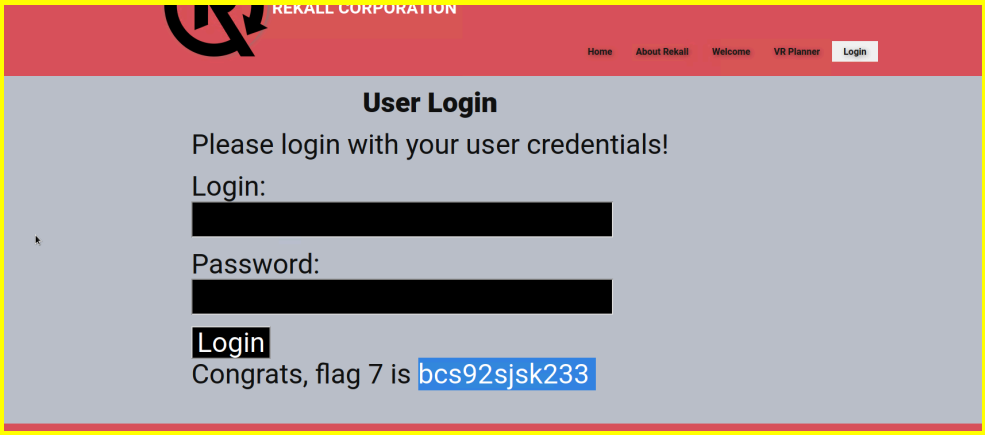
Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Webapp
Risk Rating	**Critical**
Description	The Memory-Planner.php page is vulnerable to Local File inclusion. Field two requires you to make a file and name it test.php and upload it and it gives you 5.Field three required me to make a file named test.php.jpg and upload it and it gave 6
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.14.35(Memory-Planner.php)
Remediation	- ID assignation – save your file paths in a secure database and give an ID for every single one, this way users only get to see their ID without viewing or altering the path - Whitelisting – use verified and secured whitelist files and ignore everything else - Use databases – don't include files on a web server that can be compromised, use a database instead - Better server instructions – make the server send download headers automatically instead of executing files in a specified directory

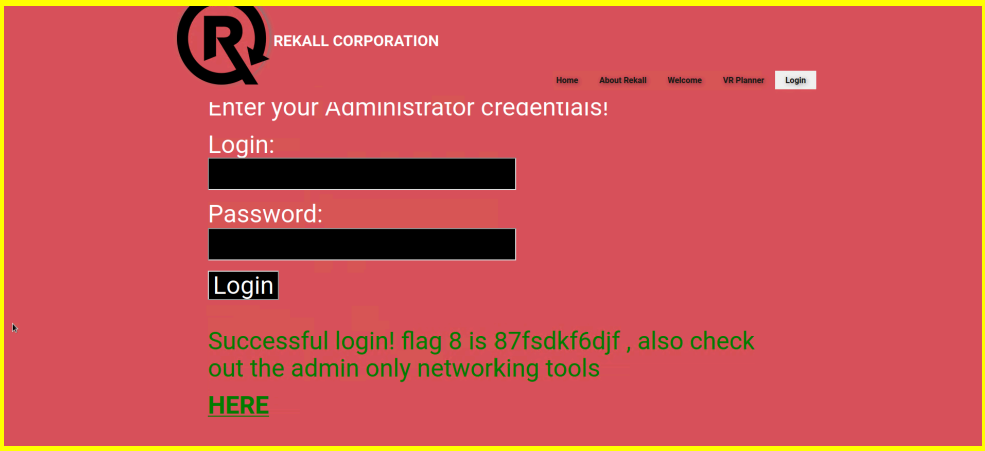
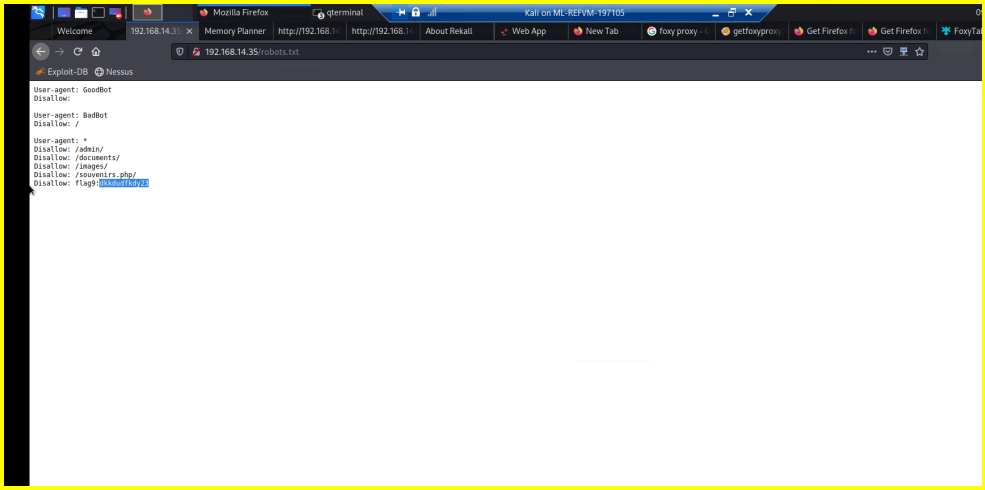
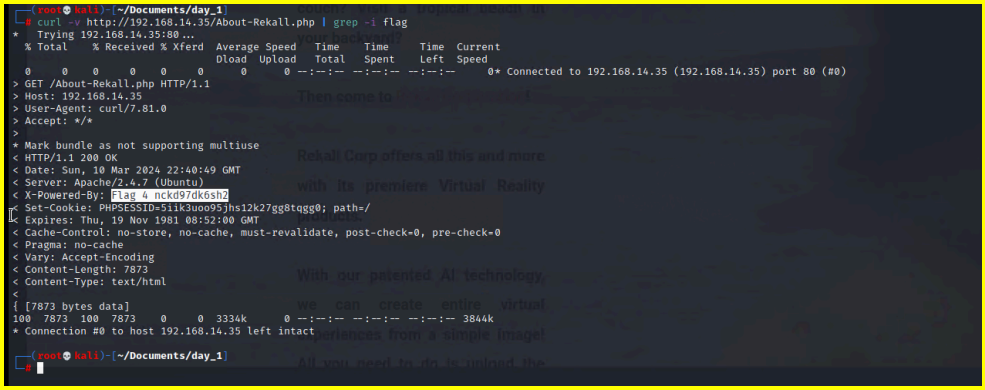
Vulnerability 4	Findings
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	Webapp
Risk Rating	**Critical**
Description	Entering `admin' 1=1--` in the password field with a random username reveals 7. This first command `admin' 1=1` gave an error so I added the -- which behaves as a comment thus avoiding errors

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

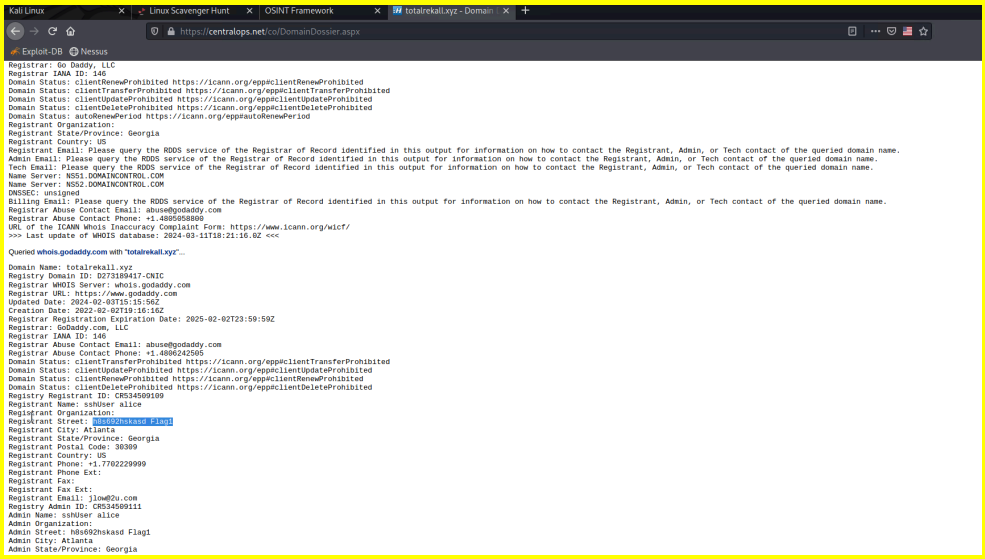
Images	
Affected Hosts	192.168.14.35(Login.php)
Remediation	- The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder.

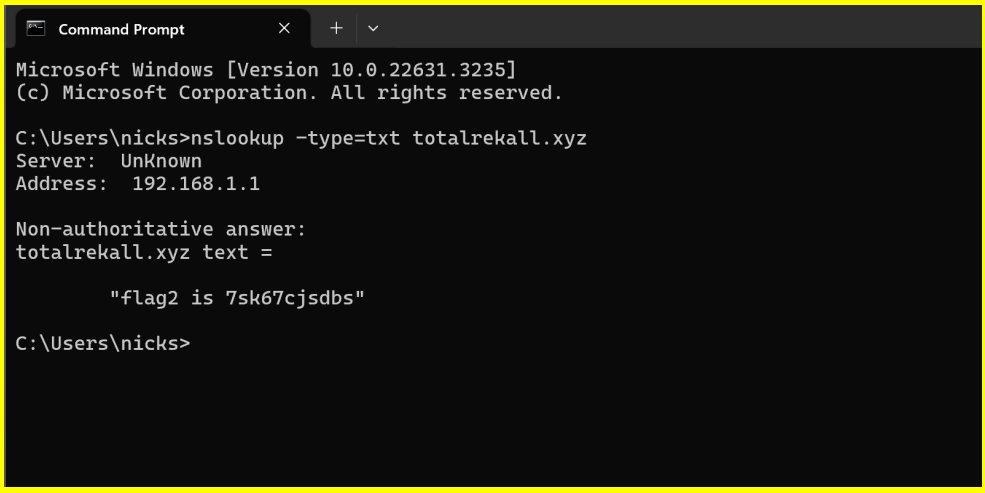
Vulnerability 5	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Webapp Linux OS Windows OS
Risk Rating	**Critical**
Description	Webapp - The login.php(Second field) page is vulnerable to sensitive data exposure. By viewing the page source code, you can see the username and password in the HTML code. Once neutered, the reveal 8. - The robots.txt(A robots.txt file tells search engine crawlers which URLs the crawler can access on your site. This is used mainly to avoid overloading your site with requests) page is accessible from the web which reveals 9 - The About-Rekall.php page exposes sensitive data in the HTTP response header. I got it by `curl -v http://192.168.14.35/About-Rekall.php` and grepped for the 4 LINUX OS - On the Domain Dossier webpage, I viewed the WHOIS data for totalrekall.xyz - The txt information of the domain name totalrekall.xyz contains sensitive information - On crt.sh, the SSL certificate reveals sensitive information Windows OS

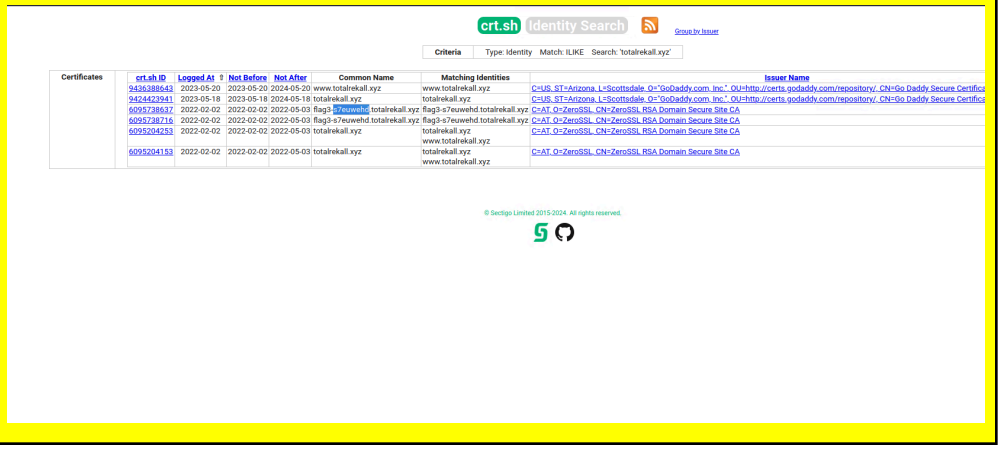
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	- The totalrekall.xyz github page contains credentials for trivera and her hash which I cracked using john. I used it to login to the Windows10 PC http page. - The file 7.txt is stored in the public folder
Images	  

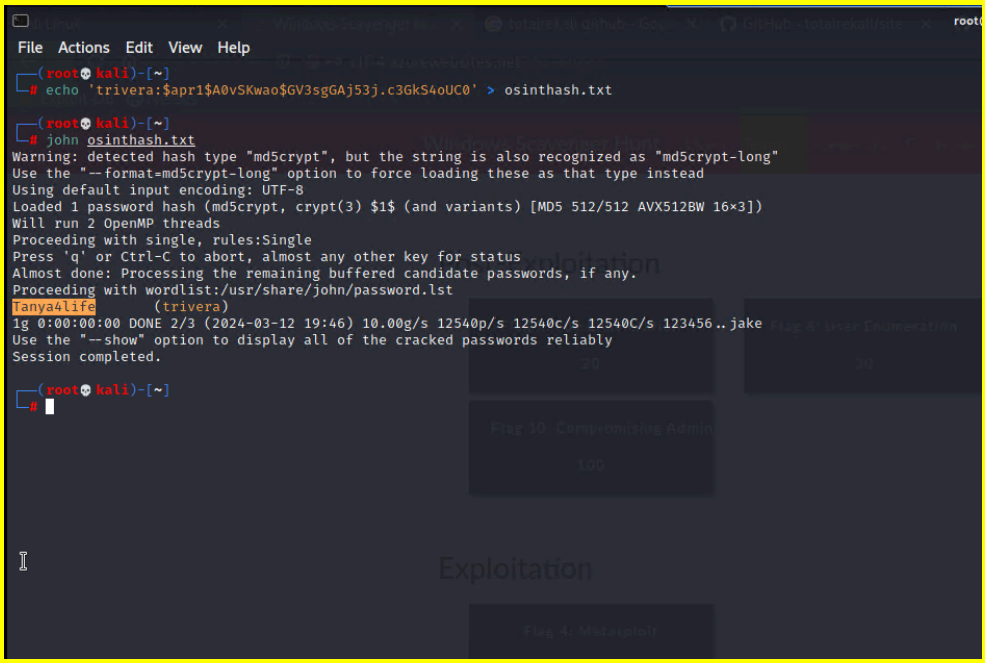
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

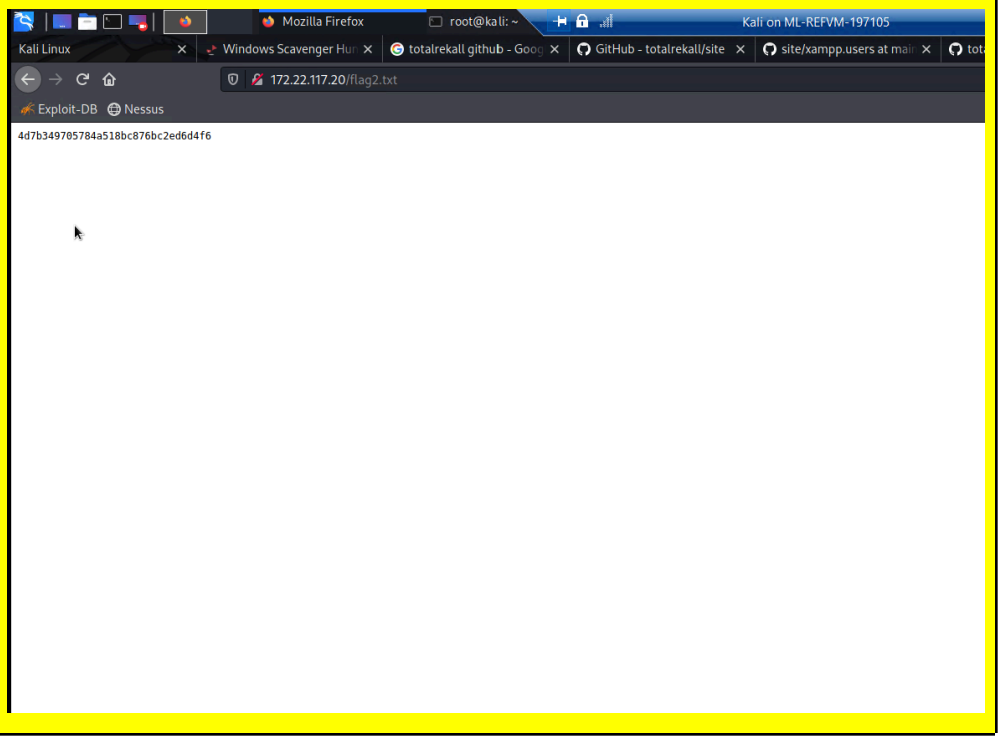




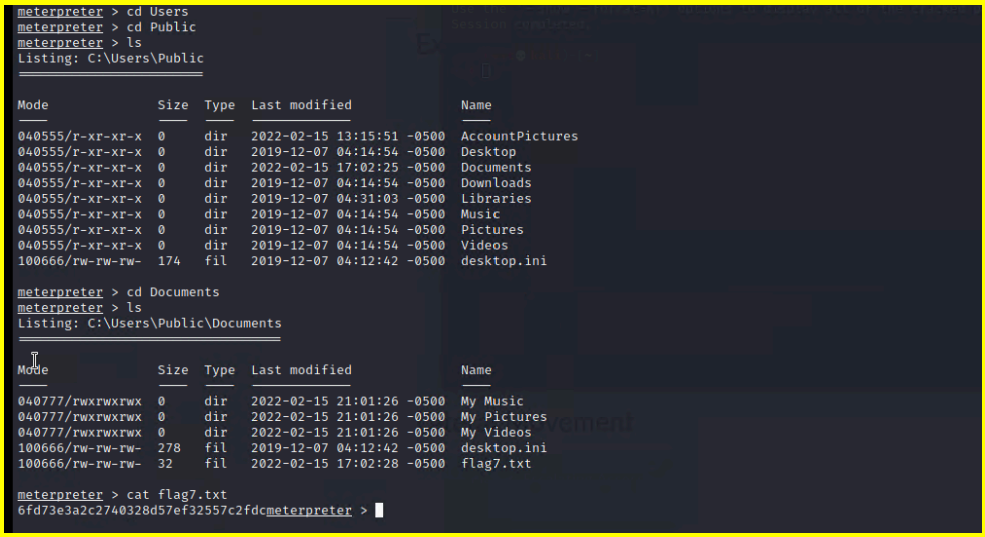


© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.





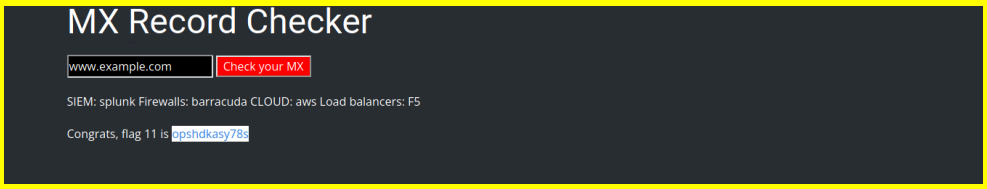
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



Affected Hosts	192.168.14.35, totalrekall.xyz
Remediation	* Classify data processed, stored or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs. * Apply controls as per the classification. * Don’t store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen. * Make sure to encrypt all sensitive data at rest. * Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management. * Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS). * Disable caching for response that contain sensitive data. * Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2. * Verify independently the effectiveness of configuration and settings. * If WHOIS data contains sensitive information, such as personal contact details, consider updating the domain registration information to remove or obscure sensitive details. * If the SSL certificate contains sensitive information, such as private keys or other confidential data, you should revoke the existing certificate and generate a new one. Ensure that sensitive information is not included in the certificate's metadata or text fields.

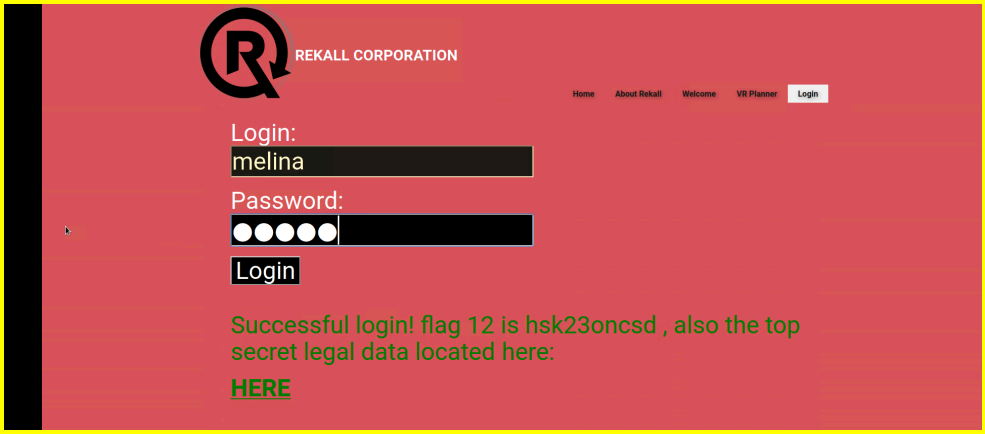
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Webapp
Risk Rating	**Critical**

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Description	The webpage networking.php(First and second field) is vulnerable to command injection. Entering www.example.com && cat /etc/passwd in first field reveals the passwd file thus revealing 10. The second field sanitizes the && characters so I used | or ; Entering www.example.com | cat /etc/passwd reveals the passwd file thus revealing
Images	 
Affected Hosts	192.168.14.35
Remediation	- The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used. Otherwise, only short alphanumeric strings should be accepted. Input containing any other data, including any conceivable shell metacharacter or whitespace, should be rejected. - The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection. For example, the Java API Runtime.exec and the ASP.NET API Process.Start do not support shell metacharacters. This defense can mitigate the impact of an attack even in the event that an attacker circumvents the input validation defenses.

Vulnerability 7	Findings
Title	Brute Force Attacks
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	The login.php page is vulnerable to brute force attacks. Using the command injection vulnerability, I accessed the /etc/passwd and figured out a user

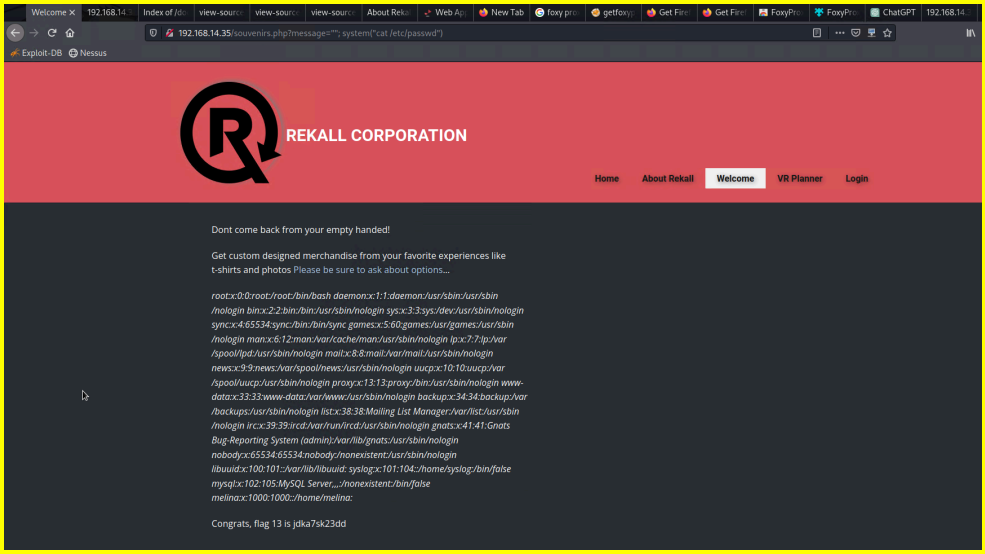
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	named melina whose password is the same as the name; melina. I used it to login and revealed 12.
Images	
Affected Hosts	192.168.14.35(Login.php)
Remediation	- Account Lockout Policy: Implement an account lockout policy that temporarily locks user accounts after a certain number of failed login attempts. This helps prevent attackers from making multiple attempts to guess passwords. - Rate Limiting: Introduce rate-limiting mechanisms to restrict the number of login attempts within a specific time frame. This prevents rapid and continuous attempts at authentication. - Strong Password Policies: Enforce strong password policies, including minimum length, complexity requirements, and regular password changes. Strong passwords make it more challenging for attackers to guess or crack passwords through brute force. - Multi-Factor Authentication (MFA): Implement multi-factor authentication to add an additional layer of security. Even if an attacker manages to guess a password, they would still need a second form of verification. - Captcha and Challenge-Response Tests: Integrate captchas or challenge-response tests during the login process. These tests are designed to distinguish between automated scripts and legitimate users, making it harder for automated brute force attacks. - IP Whitelisting/Blacklisting: Implement IP whitelisting to allow access only from known and trusted IP addresses. Alternatively, maintain a blacklist of known malicious IP addresses to block access attempts from those sources. - Logging and Monitoring: Implement robust logging mechanisms to track login attempts and monitor for unusual patterns or multiple failed login attempts. This enables early detection of potential brute force attacks. - User Notification: Notify users of failed login attempts and provide them with information about the source of the attempts. This empowers users to take action if they notice suspicious activity.

Add any additional vulnerabilities below.

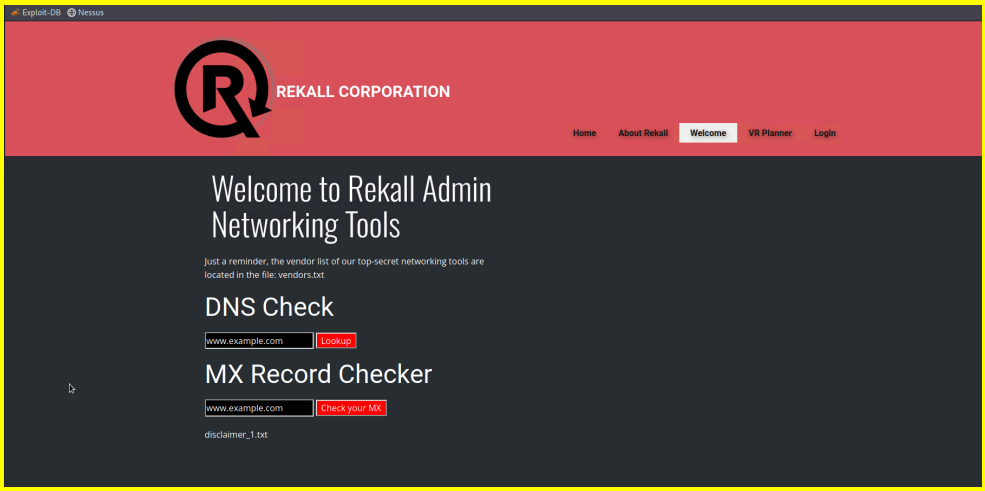
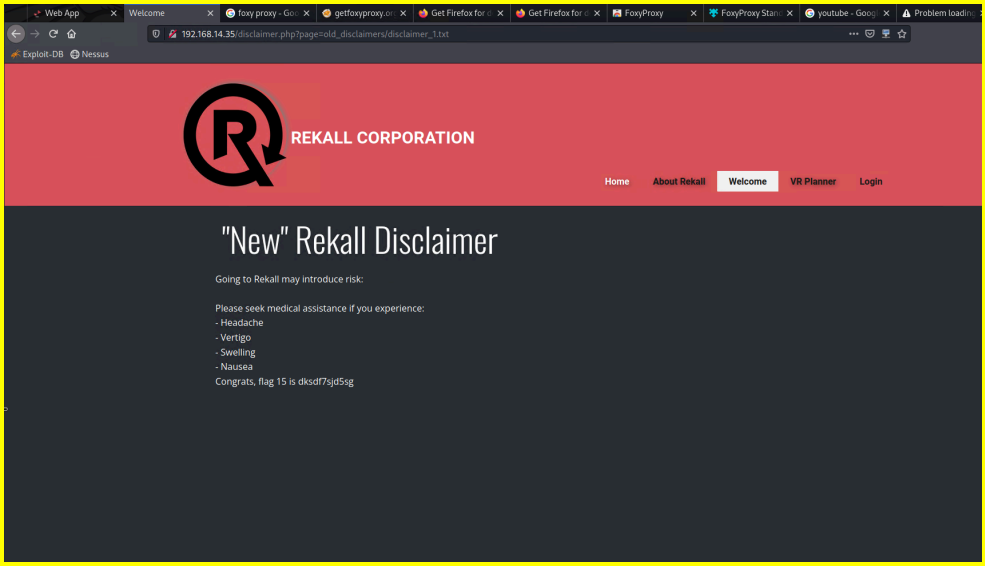
Vulnerability 8	Findings

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Title	PHP INJECTION
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The souvenirs.php page is vulnerable to PHP injection. After accessing the robots.txt file, I saw the souvenirs.php page which reveals a message based on the URL. I entered the payload `http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')` Reveals 13
Images	
Affected Hosts	192.168.14.35(souvenirs.php)
Remediation	Whenever possible, applications should avoid incorporating user-controllable data into dynamically evaluated code. In almost every situation, there are safer alternative methods of implementing application functions, which cannot be manipulated to inject arbitrary code into the server's processing.

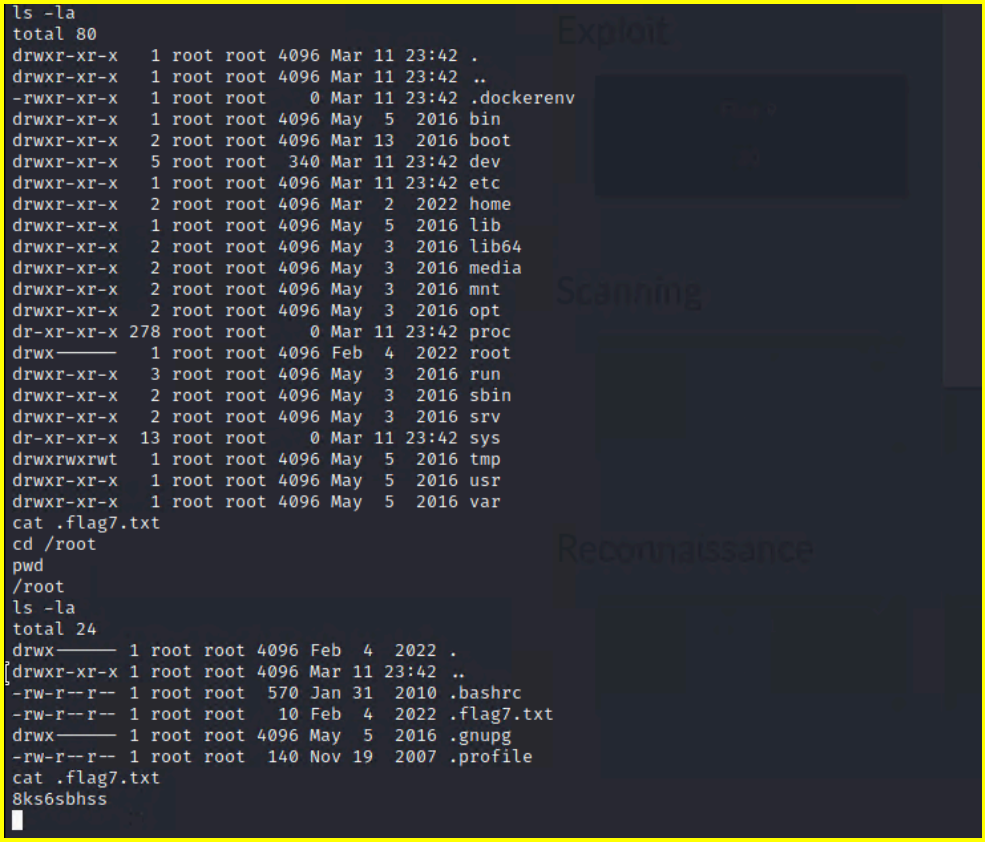
Vulnerability 9	Findings
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	The disclaimers.php page is vulnerable to directory traversal. By using the command injection in 10 or 11, I found a directory named old_disclaimers and listed whatever was in it and discovered disclaimer_1.txt. I then changed my url to '192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt' which revealed the old disclaimer plus 15

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	- Validate user-supplied input: Make sure the application always validates used-supplied input before processing it. The validation can be conducted by either comparing the user-submitted input to a whitelist of acceptable values, or by verifying the input contains only acceptable content (e.g. purely alphanumeric characters). - You must implement a mechanism to ensure that the canonicalized path starts with the expected base directory: It is critical that your application validates that the base directory at the beginning of the canonicalized path is correct.

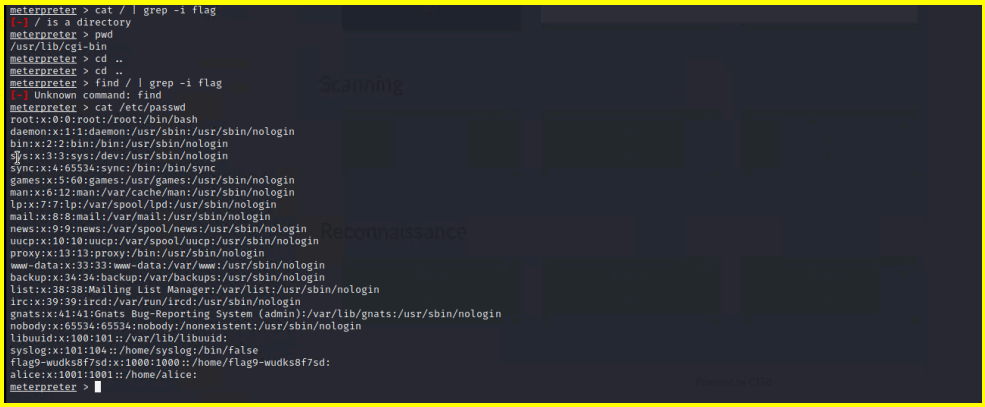
Vulnerability 10	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	LINUX OS
Risk Rating	**Critical**

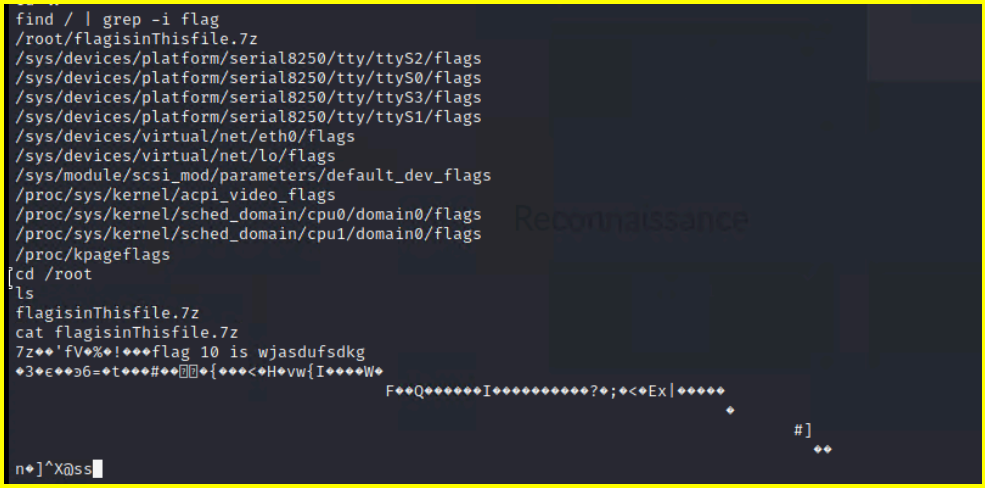
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Description	I figured out the Apache server is running Tomcat and used metasploit to find a jsp exploit(multi/http/tomcat_jsp_upload_bypass) and gained a meterpreter shell. Enter “SHELL” to gain command line and listed to find 7
Images	
Affected Hosts	192.168.13.10
Remediation	- Update Tomcat to latest version where the vulnerability is fixed. - The readonly init-param should not be set to false.

Vulnerability 11	Findings
Title	The Linux server(192.168.13.11) has a Shellshock
Type (Web app / Linux OS / WIndows OS)	LINUX OS
Risk Rating	High
Description	192.168.13.11 was prone to shell shock so using the metasploit module exploit/multi/http/apache_mod_cgi_bash_env_exec and target URI(The vulnerable webpage): /cgi-bin/shockme.cgi, I got a meterpreter shell then accesses the /etc/sudoers file

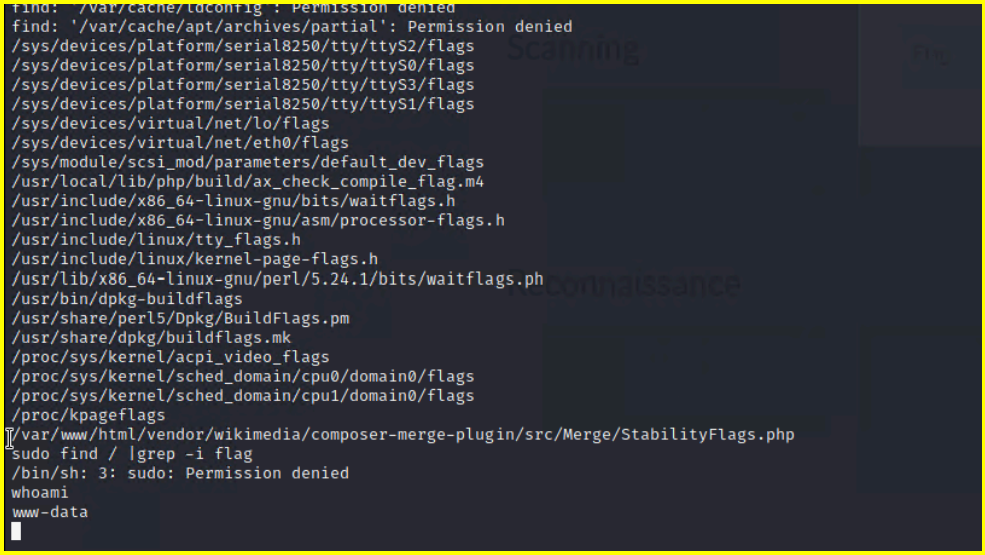
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.13.11
Remediation	- Shellshock type attacks can be avoided by not processing user data directly as variables in web/bash code. An example of this could be to base64 encode user input as it is stored in a variable. - By sanitizing user input and removing un-needed characters, developers can disrupt an attack before it takes place. bash example: x=$(echo “$1”| tr -d “\(\) { :. }”) export x

Vulnerability 12	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	LINUX OS
Risk Rating	**Critical**
Description	The Nessus scan revealed that the server was vulnerable to the CVE-2017-5638. I Using the metasploit module multi/http/struts2_content_type_ognl, I got a meterpreter shell and got 10
Images	

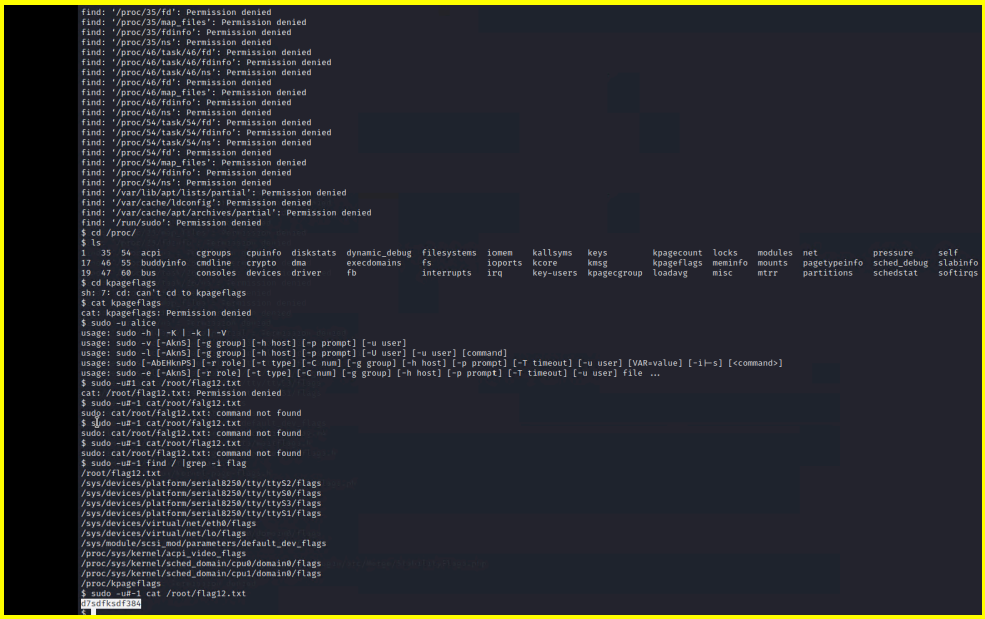
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Affected Hosts	192.168.13.12
Remediation	Web application firewalls such as mod_security could mitigate this attack if the rules are set to approve valid content types or ban OGNL expressions. An alternative mitigation to upgrading Struts is to switch to using Jason Pells multipart parser. This plugin replaces the vulnerable Struts component and can be installed by copying the plugin jar into your application's /WEB-INF/lib directory. The library will need to be included in your application as well.

Vulnerability 13	**Findings**
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	LINUX OS
Risk Rating	High
Description	The nmap scan revealed that 192.168.13.13 is running Drupal, which is vulnerable. Using the metasploit module unix/webapp/drupal_restws_unserialize
Images	
Affected Hosts	192.168.13.13
Remediation	- If you are using Drupal 8.6.x, upgrade to Drupal 8.6.10. - If you are using Drupal 8.5.x or earlier, upgrade to Drupal 8.5.11.

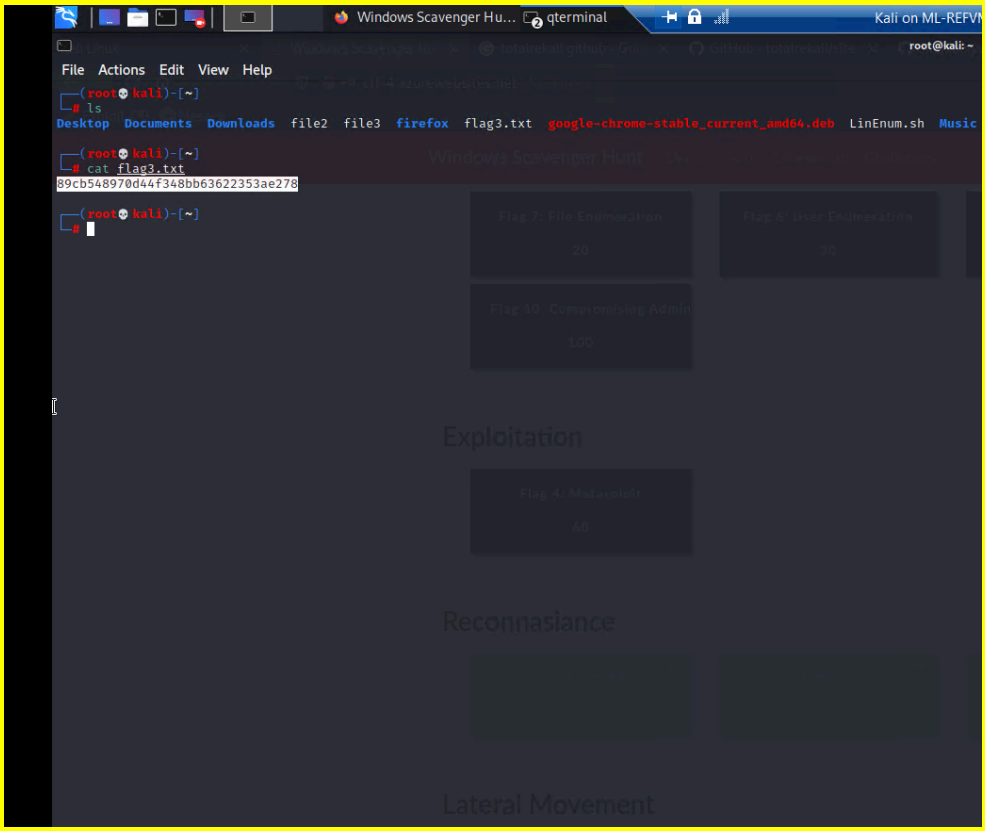
Vulnerability 14	**Findings**
Title	Sudo vulnerability(CVE-2019-14287)

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Type (Web app / Linux OS / WIndows OS)	LINUX OS
Risk Rating	High
Description	The WHOIS data reveals the SSH user Alice. I guessed the password. I used: sudo -u#-1 cat /root/12.txt to reveal the
Images	
Affected Hosts	192.168.13.14
Remediation	To ensure your sudoers configuration is not affected by this vulnerability, we recommend examining each sudoers entry that includes the `!` character in the runas specification, to ensure that the root user is not among the exclusions. These can be found in the /etc/sudoers file or files under /etc/sudoers.d.

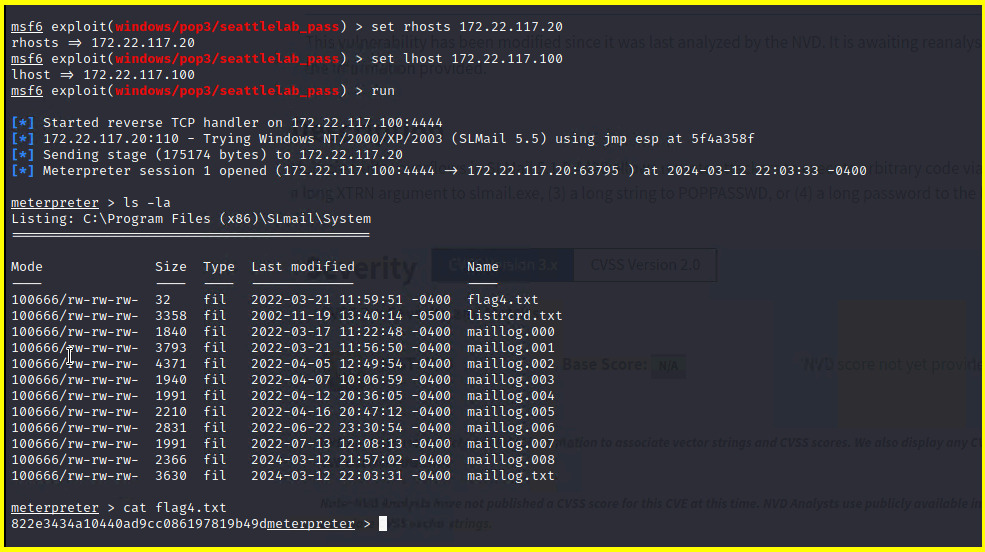
Vulnerability 15	Findings
Title	Anonymous FTP login
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	The nmap scan reveals that the Windows10 PC has anonymous ftp login allowed. I logged in using the anonymous ftp login and downloaded the to my computer

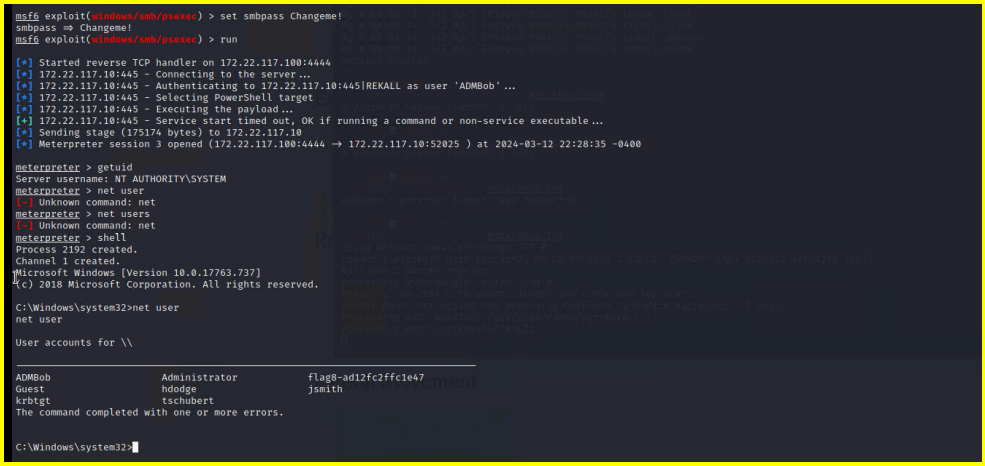
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.

Vulnerability 16	Findings
Title	SLMail service vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	The nmap scan revealed that the Windows 10 PC was running the SLMailservice which is vulnerable. I loaded the SLMail module on metapsloit and run it thus gaining a meterpreter shell

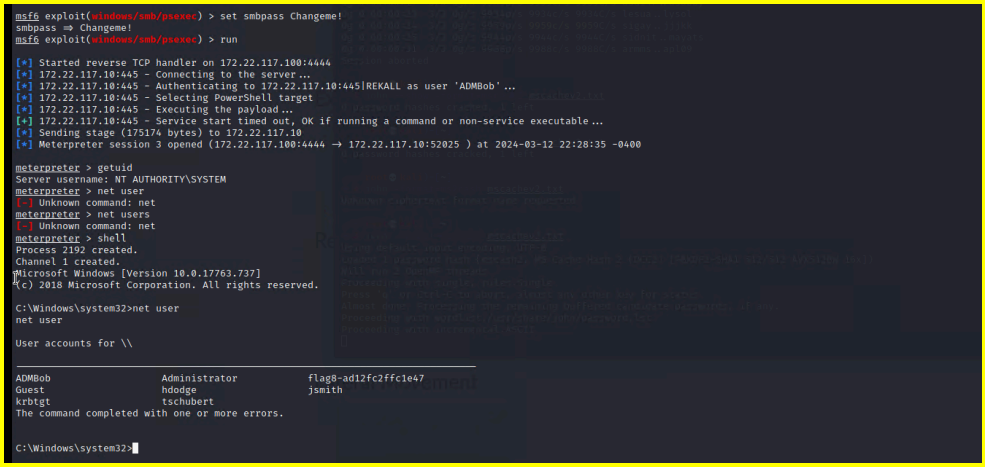
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Upgrade to SLMail 5.5. If it is not possible to upgrade immediately, then disable ESMTP in the SLMail configuration utility, and block access to ports 106/TCP (poppasswd) and 110/TCP (pop3) at the network perimeter.

Vulnerability 17	Findings
Title	Cached credentials(lsa_dump)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	The command lsa_dump::cache reveals ADMBob and his NTLM hash. I cracked it using john and used the psexec module to laterally move
Images	
Affected Hosts	172.22.117.20
Remediation	By default Windows are caching the last 10 password hashes. It is

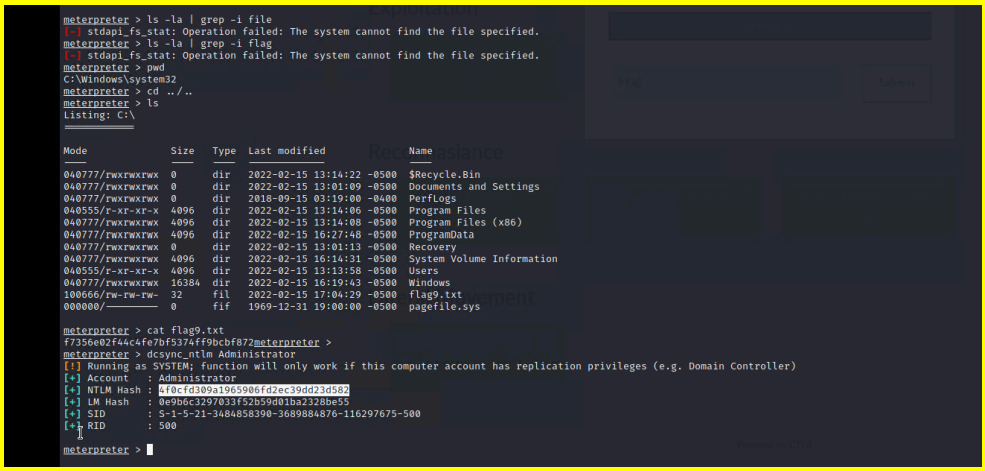
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	recommended to prevent local caching of password by changing the following security setting to 0. Computer Configuration -> Windows Settings -> Local Policy -> Security Options -> Interactive Logon: Number of previous logons to cache -> 0

Vulnerability 18	Findings
Title	PS exec
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	The command lsa_dump::cache reveals ADMBob and his NTLM hash. I cracked it using john and used the psexec module to escalate privileges and laterally move to the WindowsDC
Images	
Affected Hosts	172.22.117.10
Remediation	Upgrade PsExec to version 2.33 or later.

Vulnerability 19	Findings
Title	DCSync vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using DCSync and the administrator, I was able to get the administrator's password hash

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.10
Remediation	- As a mitigation strategy, security administrators can manage the access control lists (ACLs) for “Replicating Directory Changes” and other permissions associated with DC replication. - Security administrators can remove unusual accounts set with replication permissions or deny the permissions for the specified user accounts. - Security administrators can also look for the members of the Administrators and Domain Controller groups that have Replicate Directory Changes permissions by default, as shown below, and enforce the least privileges to reduce the risk of attackers escalating them.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.