

PSP0201

Week 2

Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

DAY 3: Web Exploitation Christmas Chaos

Tool used: kali Linux, Firefox, burp suite

Solution/Walkthrough:

Q1

The screenshot shows a Kali Linux virtual machine running VMware Workstation 16. The browser is open to the TryHackMe room 'AoC Day 3' at <https://tryhackme.com/room/learnpython25days>. The room details show the title 'AoC Day 3', IP address '10.10.178.31', and an expiration time of '1h 26m 30s'. The room content includes a task 'Bypass a login form using BurpSuite' and sections on 'Authentication' and 'Default Credentials'. The 'Authentication' section explains the process of verifying a user's identity. The 'Default Credentials' section discusses the risks of using default credentials, citing examples like Starbucks and the US Department of Defense. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 10:16 PM on 6/16/2022.

Title	IP Address	Expires
AoC Day 3	10.10.178.31	1h 26m 30s

- Bypass a login form using BurpSuite

Authentication

Authentication is a process of verifying a users' identity, normally by credentials (such as a username, user id or password); to put simply, authentication involves checking that somebody really is who they claim to be. Authorization (which is fundamentally different to authentication, but often used interchangeably) determines what a user can and can't access; authorization is covered in tomorrow walkthrough, today's task focuses on authentication and some common flaws.

Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called [Mirai](#) took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid \$250 for the reported issue):

- <https://hackerone.com/reports/195163> - Starbucks, bug bounty for default credentials.
- <https://hackerone.com/reports/804548> - US Dept Of Defense, admin access via default credentials.

In 2017, it was [reported](#) that 15% of all IoT devices still use default passwords.

Read from the text in THM.

Q2

The screenshot shows a VMware Workstation 16 Player window titled "PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)". Inside the VM, a web browser is open to the URL <https://tryhackme.com/room/learncyberin25days>. The page content includes a table with the following data:

Title	IP Address	Expires
AoC Day 3	10.10.178.31	1h 25m 42s

Below the table, the text reads: "You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials."

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called [Mirai](#) took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid \$[50](#) for the reported issue):

- <https://hackerone.com/reports/195163> - Starbucks, bug bounty for default credentials.
- <https://hackerone.com/reports/804548> - US Dept Of Defense, admin access via default credentials.

In 2017, it was [reported](#) that 15% of all IoT devices still use default passwords.

[SecLists](#) is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

Dictionary Attacks using BurpSuite

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most common) usernames and passwords, you can loop through each of them in hopes that one of the combinations is successful.

You can use a number of tools to perform a dictionary attack, one notable one being Hydra (a fast network logon cracker) and BurpSuite, an industry-standard

Read from text in THM.

Q3

The screenshot shows the Hackerone website interface. The top navigation bar includes links for Login, Contacted by a hacker?, and Contact Us. The main header features the Hackerone logo and navigation tabs for SOLUTIONS, PRODUCTS, PARTNERS, COMPANY, HACKERS, and RESOURCES.

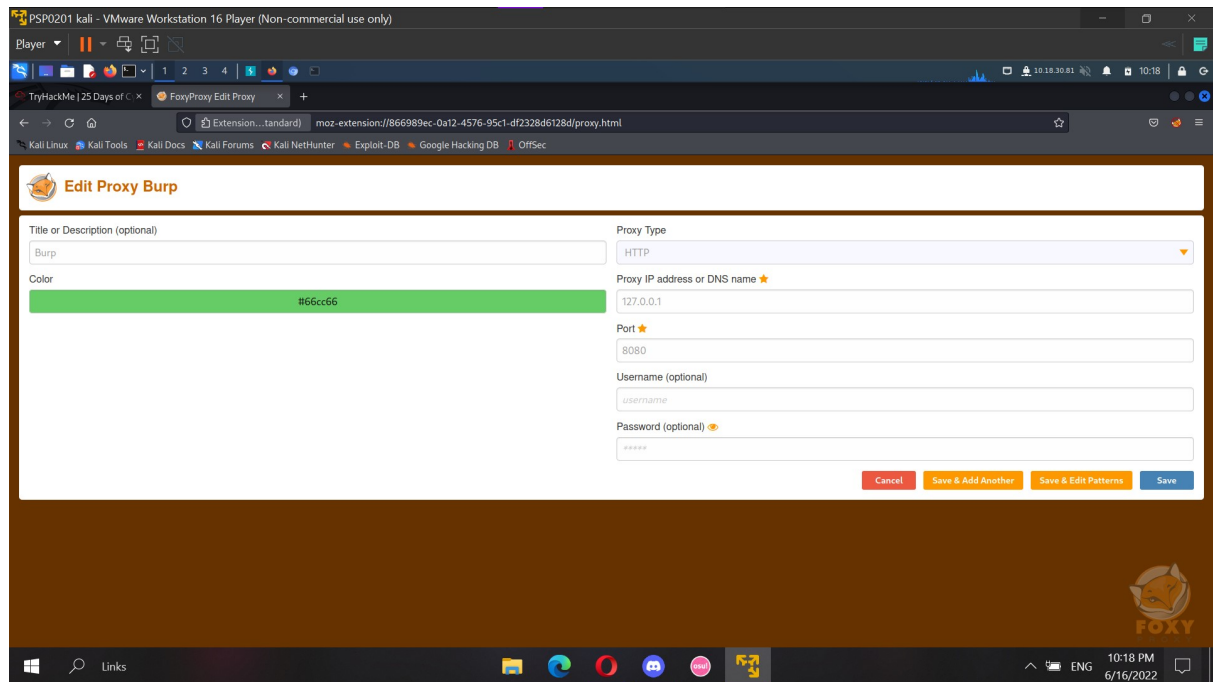
The main content area displays a list of reports. The selected report is titled "U.S. Dept Of Defense staff" and is in a "Resolved" state. The report details include:

- Disclosed:** June 25, 2020 9:38pm +0800
- Severity:** Critical (9 ~ 10)
- Weakness:** Improper Access Control - Generic
- CVE ID:** None
- Account de...:** None

The report history shows several updates, including comments from arm4nd0, agentt2, and agent-l8, and a final disclosure by ag3nt-j1.

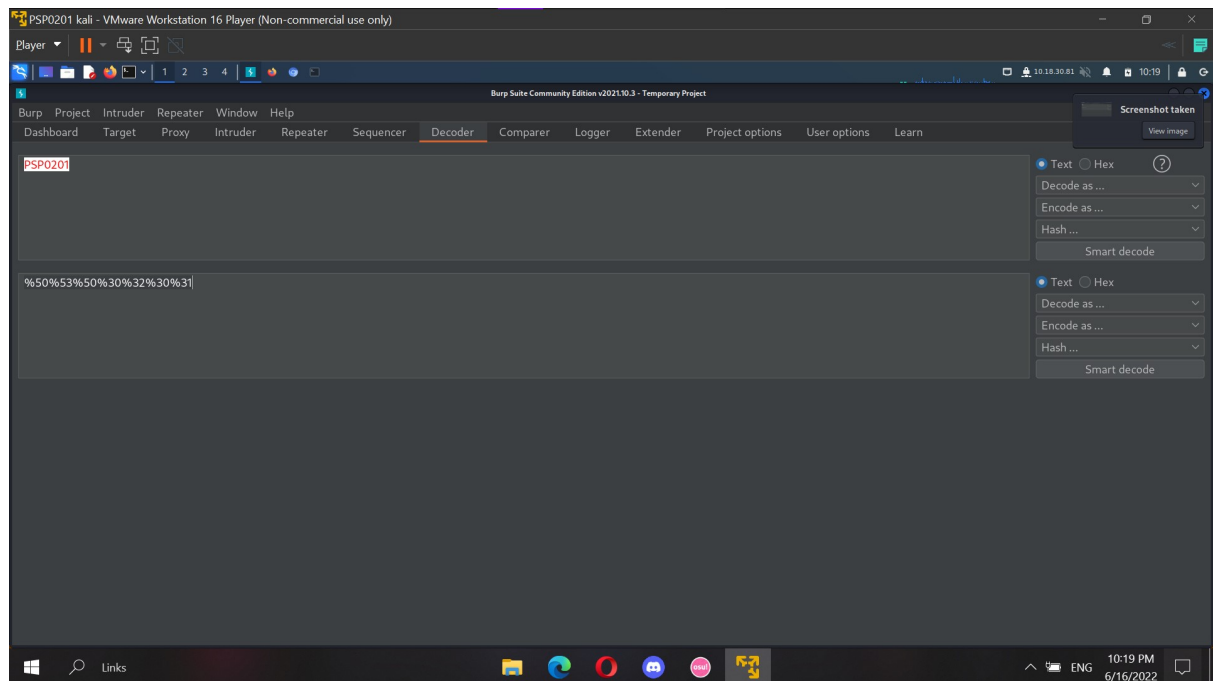
Copy and paste from the Hackerone.com report.

Q4 & Q5



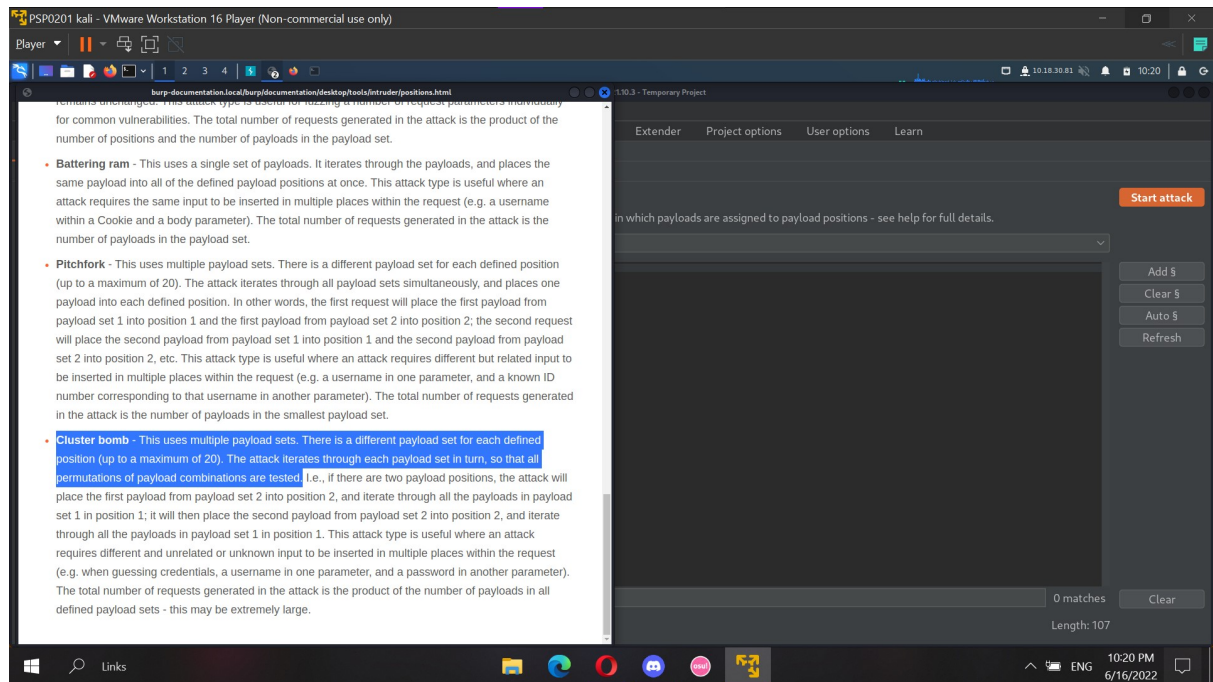
Open the foxy proxy in the firefox and choose the options of Burp. Click on the edit button and the proxy type and port number can be found.

Q6



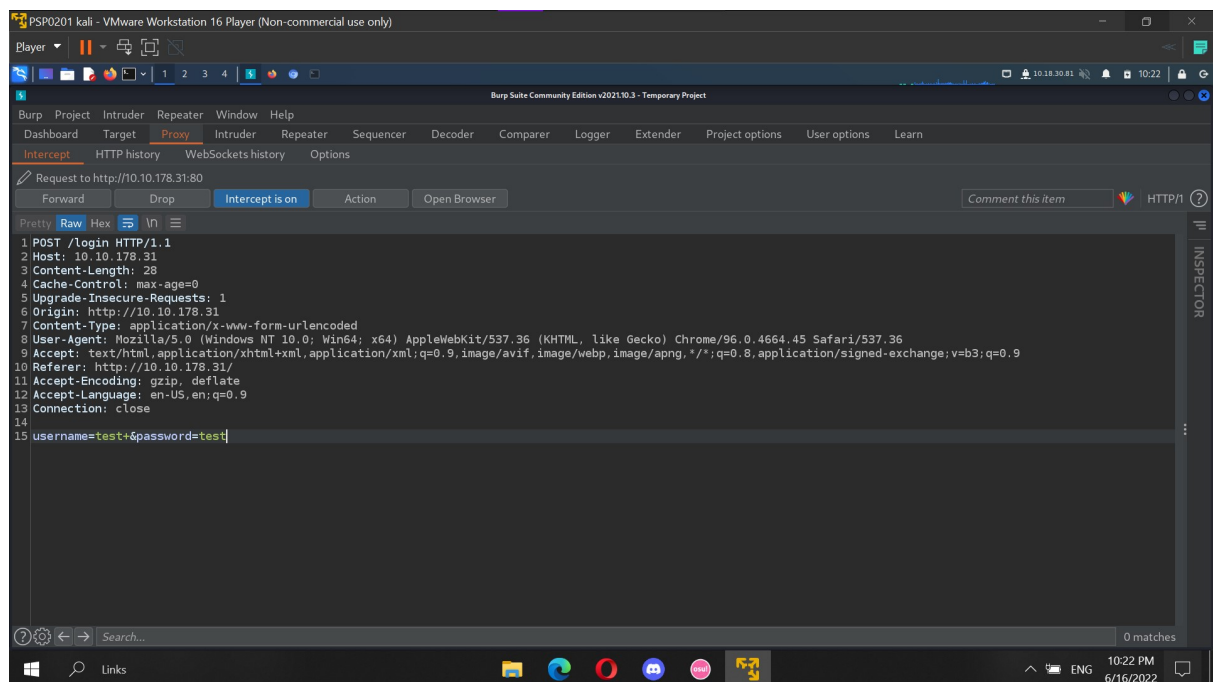
Open burp suite. Choose the decoder options and paste the text PSP0201. Change the encode as options to url and decode. The output then can be get.

Q7



Attack type that matches with the question. Found in the list of attack type options on intruder.

Q8



Turn on the intercept option in burp suite and type in a random input to the site and let burp suite to hold the request. Change the attack type to cluster bomb.

Payload set: Payload count: 3
Payload type: Request count: 0

? **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are u

Paste

Load ...

Remove

Clear

admin

root

user

Add

Add from list ... [Pro version only]

Payload set: Payload count: 3
Payload type: Request count: 9

? **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

password

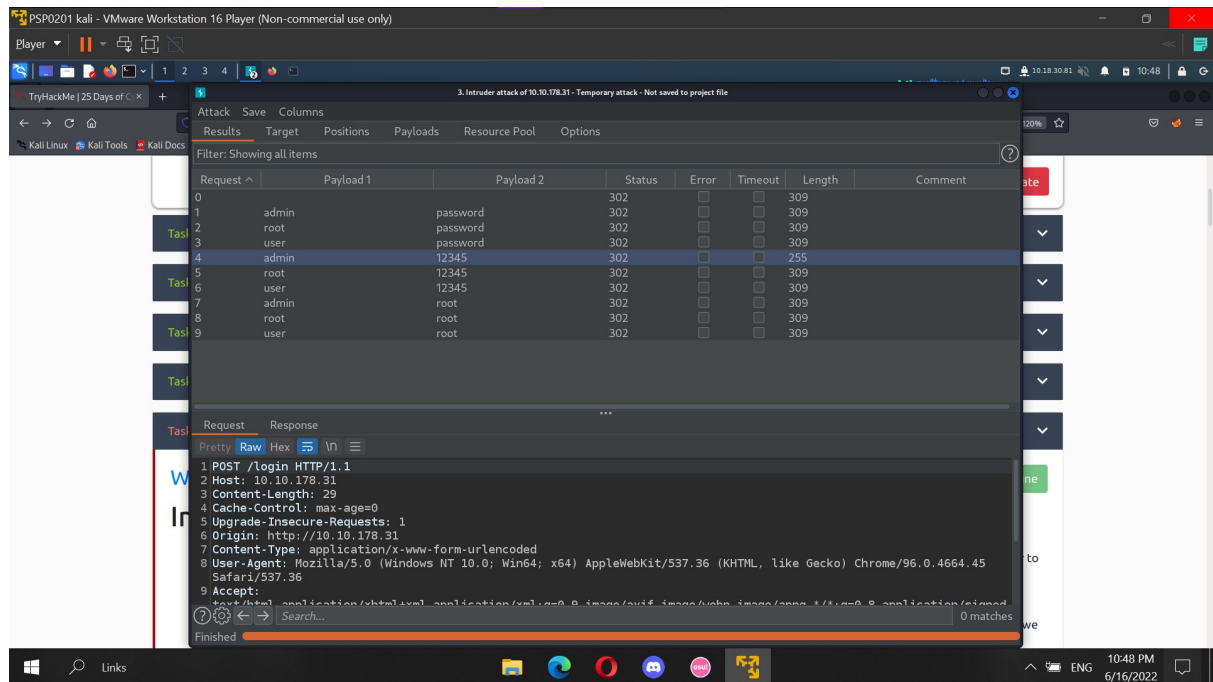
admin

12345

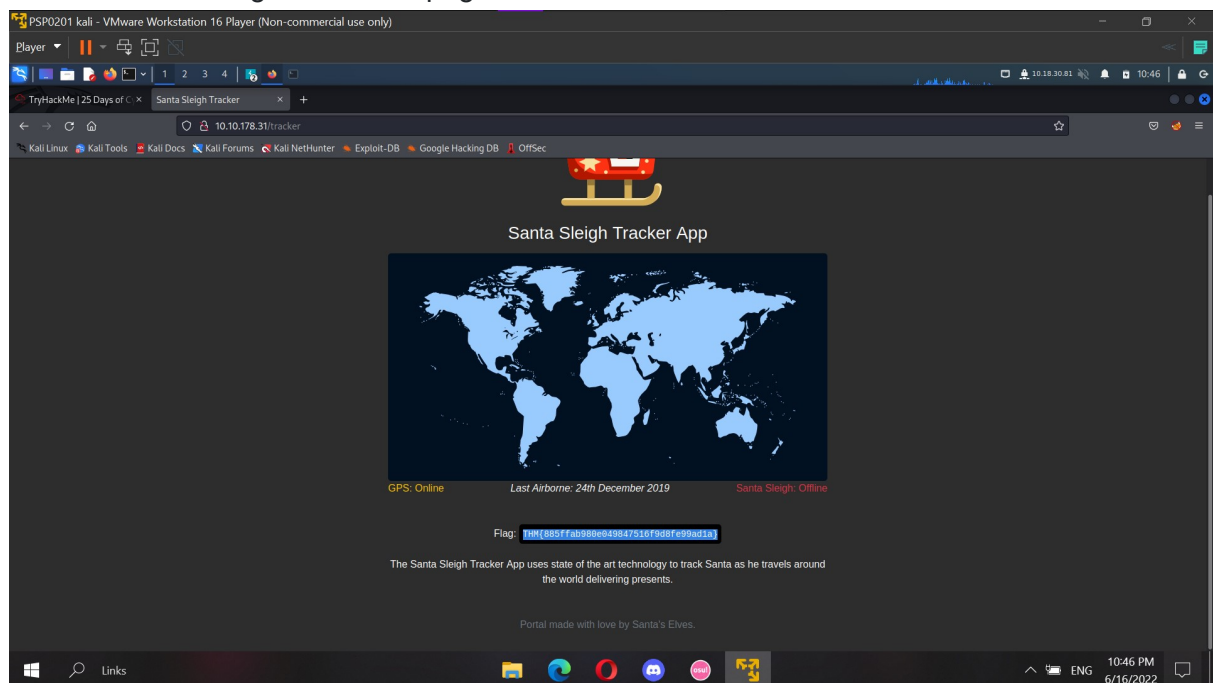
Add

Add from list ... [Pro version only]

Go to the payload and add a few common username entries in set 1 and common passwords in set 2.



Press the start attack. The result will then be shown and we can know there is a combination that is different from the others. We got to know which combination is right. Use the combination and sign in into the page.



After login successfully, the flag will show up. Capture the flag and paste it into the answer.