# Reconnaissance Fundamentals – Regular Exam

### Execution Summary

* You are hired to perform a digital investigation for the following target: **185.218.124.165**
* This is a template for **uploading your screenshots and data**.
* The exam objective is to utilize active and passive reconnaissance to identify stored online ssh private key.
* Finding exposed public ssh key does not complete the exam objective.
* You are free to report vulnerabilities if you find any along the way. Each vulnerability gives extra points.
* Not all vulnerabilities are giving the same number of points.
* The order of the vulnerabilities **DO NOT MATTER**, nor the tools used to get to them.
* You are free to upload multiple **screenshots** for each **vulnerability**, including your **path** and how did you **find** it.
* **No network breach or local privilege escalation is needed!**

**Do not overstress or overcomplicate it. The time is enough, you can do it.**

### Scope

Scope is open, meaning you can perform your own information gathering and you are free to enumerate the target for vulnerabilities from every angle.

### Appendix

This is the data section. Make sure to **detail each finding**. The overall vulnerability count is unknown, try to **find as much as possible** while following the **main objective**. It is a good practice to **explain your finding**.

When describing your finding, make sure to be as clear as possible by **answering** the following **questions**:

1. What is the vulnerability I found?
2. How did I find it?
3. What "bad" can happen, what risk does it carry?

After the description, make sure to **drop** your **screenshots** below.

### Vulnerability 1

| **Description:** |
| --- |
| **→ Open SSH (Secure Shell) port -22. Allowing inbound traffic from all external IP addresses to SSH port is vulnerable to banner grabbing and brute force attack. It is a best practice to restrict access from specific IP addresses to port 22.** |
| **Screenshots:** |
| **->** |

### Vulnerability 2

| **Description:** |
| --- |
| **→Cross-site Scripting Found. After checking open ports and found port 80 is open i entered the IP in the browser see pic 1. After that i try to add some information to see if the info is comming back, see picture 2 and 3.** |
| **Screenshots:** |
| **→1.**  **2.**  **3.** |

### Vulnerability 3

| **Description:** |
| --- |
| **→HTML injection attack also found. I we see the info which we are puting in the search filed is comming back for example mitko see pic 1. From the output after that you see the h # is showing up, see pic 2.** |
| **Screenshots:** |
| **→ 1.**  **2.** |

### Vulnerability 4

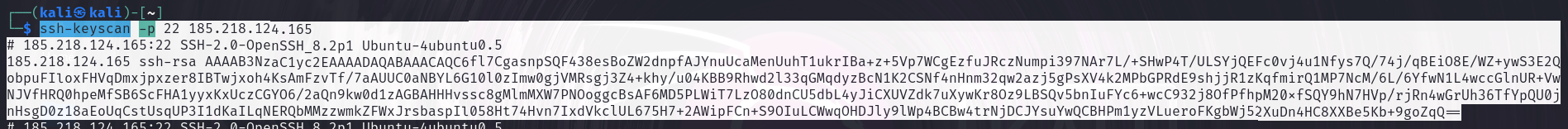
| **Description:** |
| --- |
| **→The HTTP code 200 OK success status response code indicate that the server has successfully processed the request. While this status code does not carry much information by itself, it signals to attackers that their attempt was successful. I have used DIRB to found this, please see picture.** |
| **Screenshots:** |
| **->** |

### Vulnerability 5

| **Description:** |
| --- |
| **→ Found an old PHP version after checking some additional information on the browser with the curl -I command. Please see the picture. PHP/7.4.33 end of life in 2022.** |
| **Screenshots:** |
|  |

Vulnerability 6

I also found the Public SSH Key for the open port 22. Please see the picture.



### Writeup

This is the write-up section. Here, you can explain your exam engagement in open format. Screenshots and outputs from tools are allowed. Good formatting and detailed explanations can increase your overall points, however, bad formatting and poor explanations can decrease your overall points.

# Digital Investigation Report

**Target IP:** 185.218.124.165  
**Assessment Type:** Active and Passive Reconnaissance  
**Objective:** Identify vulnerabilities and locate any exposed SSH private key.  
**Scope:** Open – unrestricted enumeration and information gathering allowed.

##  Vulnerability 1 – Open SSH Port (Port 22)

* **Description:** Port 22 (SSH) is openly accessible from any external IP address.
* **Discovery Method:** Identified during basic port scanning.
* **Risk Impact:** Exposes the SSH service to:
* Brute-force login attempts
* Banner grabbing
* Unauthorized access attempts
* **Recommendation:** Restrict SSH access to specific trusted IPs using firewall rules or access control lists (ACLs).

## 離 Vulnerability 2 – Cross-Site Scripting (XSS)

* **Description:** Reflected Cross-Site Scripting vulnerability exists on the web application served over port 80.
* **Discovery Method:** Injected test strings into input fields; the input was reflected unescaped in the response.
* **Risk Impact:**
* Theft of session cookies
* Execution of arbitrary scripts
* Client-side redirection and data manipulation
* **Recommendation:** Implement input sanitization and output encoding. Consider using security libraries or frameworks with built-in XSS protection.

## 隣 Vulnerability 3 – HTML Injection

* **Description:** HTML tags entered into a search field are rendered directly in the response.
* **Discovery Method:** Injected values like “mitko” and HTML elements (e.g., <h#>) into input fields; confirmed rendering in browser output.
* **Risk Impact:**
* Web page defacement
* Phishing via fake forms or buttons
* Gateway to more severe XSS vulnerabilities
* **Recommendation:** Sanitize all user inputs and apply context-aware output encoding to prevent interpretation as HTML.

##  Vulnerability 4 – Exposed Directories (Using DIRB)

* **Description:** Hidden or unintended directories are accessible via HTTP and return HTTP 200 OK.
* **Discovery Method:** Used the DIRB tool to perform directory brute-forcing.
* **Risk Impact:**
* Exposure of sensitive files or configuration
* Discovery of outdated or unlinked resources
* Increased attack surface
* **Recommendation:** Disable directory listing, secure access to sensitive directories, and remove unused or test files.

## 茶 Vulnerability 5 – Outdated PHP Version (7.4.33)

* **Description:** Server is running PHP version 7.4.33, which reached end-of-life (EOL) in 2022.
* **Discovery Method:** Used curl -I to inspect HTTP response headers.
* **Risk Impact:**
* Vulnerable to known exploits with no official security patches
* Potential code execution or denial-of-service risks
* **Recommendation:** Upgrade to a supported PHP version (e.g., PHP 8.2+) and ensure regular updates are applied.

##  Vulnerability 6 – Public SSH Key Exposure

* **Description:** A public SSH key associated with port 22 was discovered.
* **Discovery Method:** Not fully detailed; implied discovery via HTTP or file enumeration.
* **Risk Impact:**
* May aid attackers in identifying users or hosts
* Combined with other information, may assist in targeted attacks
* **Recommendation:** Ensure public keys are not exposed in unintended locations. If unnecessary, remove them from accessible directories.

# ✅ Conclusion

The engagement revealed multiple security concerns across the target system, including both web and network-level vulnerabilities. While the primary objective was to locate an exposed private SSH key (which is not confirmed to be found), the identified issues warrant attention.

Each vulnerability poses a specific risk and, if chained, could lead to deeper compromise or reconnaissance of the internal environment. Prompt remediation and implementation of secure configurations are strongly advised.