**Week 9**

**Penetration Testing Report**

**Introduction**

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 9 Labs**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

**1. Objective**

The objective of the assessment was to uncover vulnerabilities in the **Week 9 Labs** and provide a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

**2. Scope**

This section defines the scope and boundaries of the project.

| **Application Name** | **SQL Injection** |
| --- | --- |

**3. Summary**

Outlined is a Black Box Application Security assessment for the **Week 9 Labs**.

**Total number of Sub-labs: 12 Sub-labs**

| **High** | **Medium** | **Low** |
| --- | --- | --- |
| **4** | **4** | **4** |

**High - Number of Sub-labs with hard difficulty level**

**Medium - Number of Sub-labs with Medium difficulty level**

**Low - Number of Sub-labs with Easy difficulty level**

# 1. SQL Injection

# 1.1. Strings & Errors Part 1!

| **Reference** | **Risk Rating** |
| --- | --- |
| Strings & Errors Part 1! | **Low / Medium / High** |
| **Tools Used** | |
| Manual injection | |
| **Vulnerability Description** | |
| SQL Injection allows an attacker to view data that attackers are normally not able to retrieve.  Data can be information about users their credentials, personal details etc.  This is blindbased sqli. | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| <https://www.bugbountyhunter.org/internship_labs/HTML/sqli_lab/lab_1/lab_1.php> | |
| **Consequences of not Fixing the Issue** | |
| If poor SQL commands are used to check user names and passwords, it may be  possible to connect to a system as another user with no previous knowledge of the password. | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| <https://portswigger.net/web-security/sql-injection> | |

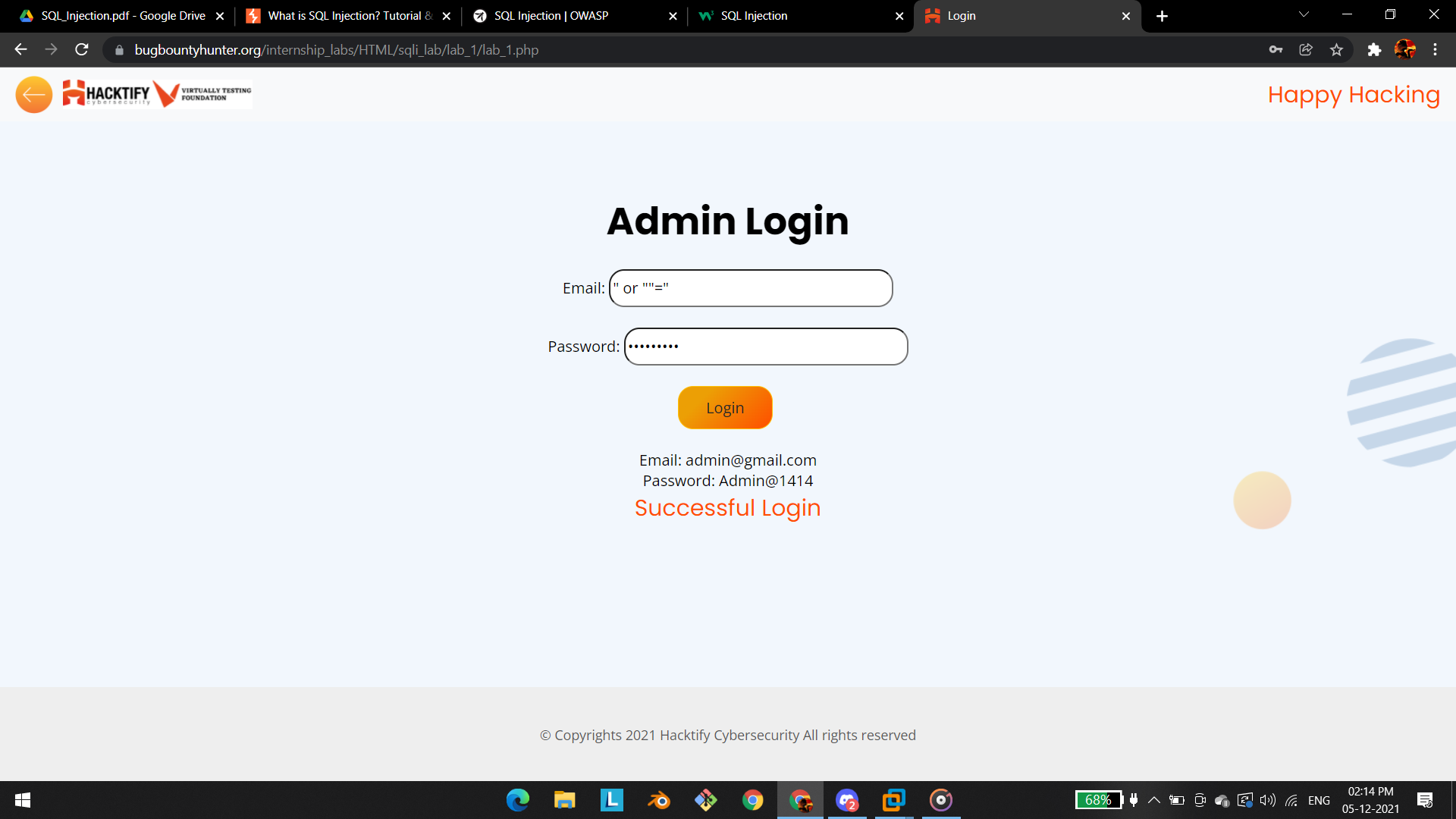
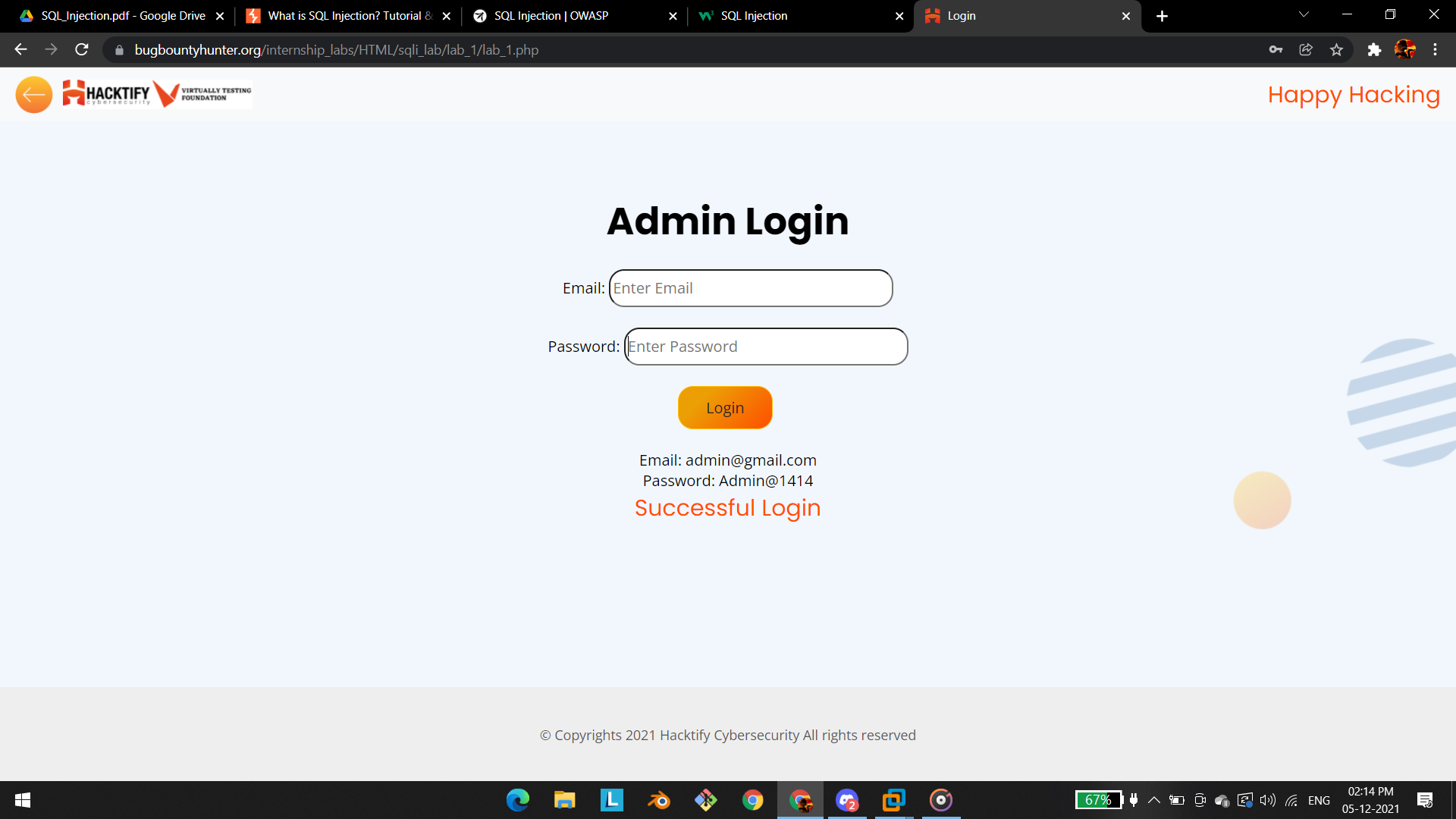
# 

# Proof of Concept

**Query:**

Email:" or ""="

Password=" or ""="



# 1.2. Strings & Errors Part 2!

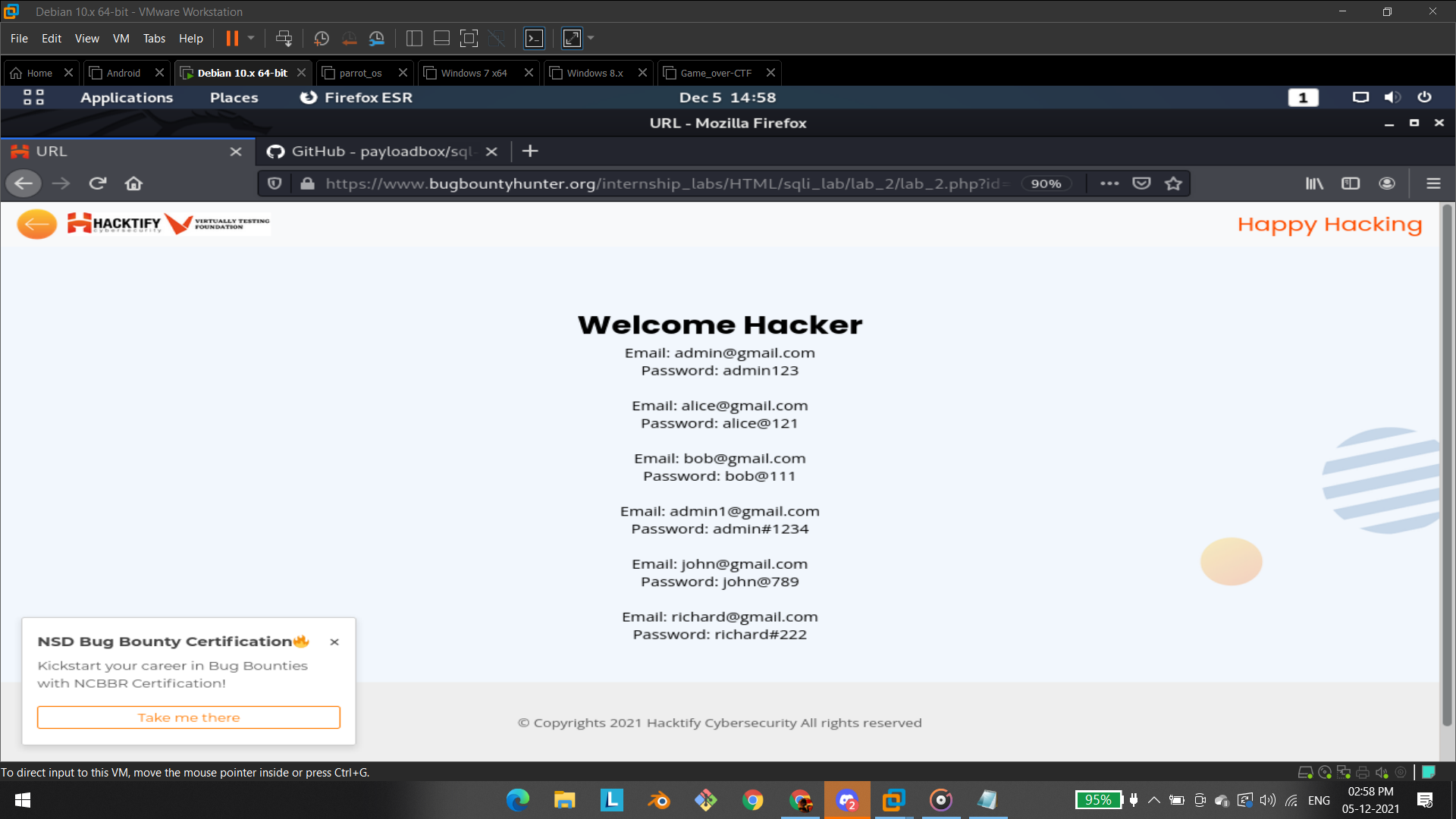
| **Reference** | **Risk Rating** |
| --- | --- |
| Strings & Errors Part 2! | **Low / Medium / High** |
| **Tools Used** | |
| Manual injection | |
| **Vulnerability Description** | |
| SQL Injection allows an attacker to view data that attackers are normally not able to retrieve.  Data can be information about users their credentials, personal details etc.  the malicious got executed in url field with the parameter called **id.** | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| <https://www.bugbountyhunter.org/internship_labs/HTML/sqli_lab/lab_2/lab_2.php> | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| <https://owasp.org/www-community/attacks/SQL_Injection> | |

# Proof of Concept

**Query:**

**query->' OR 'x'='x**

**link:**<https://www.bugbountyhunter.org/internship_labs/HTML/sqli_lab/lab_2/lab_2.php?id=%27%20OR%20%27x%27=%27x>



# 1.3. Strings & Errors Part 3!

| **Reference** | **Risk Rating** |
| --- | --- |
| Strings & Errors Part 3! | **Low / Medium / High** |
| **Tools Used** | |
| Manual injection | |
| **Vulnerability Description** | |
| SQL Injection allows an attacker to view data that attackers are normally not able to retrieve.  Data can be information about users their credentials, personal details etc.  the malicious got executed in url field with the parameter called **id** and the attacker can able to retrieve the username and passwords of all the username and password that are stored in the database | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| <https://www.bugbountyhunter.org/internship_labs/HTML/sqli_lab/lab_3/lab_3.php> | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| <https://portswigger.net/web-security/sql-injection> | |

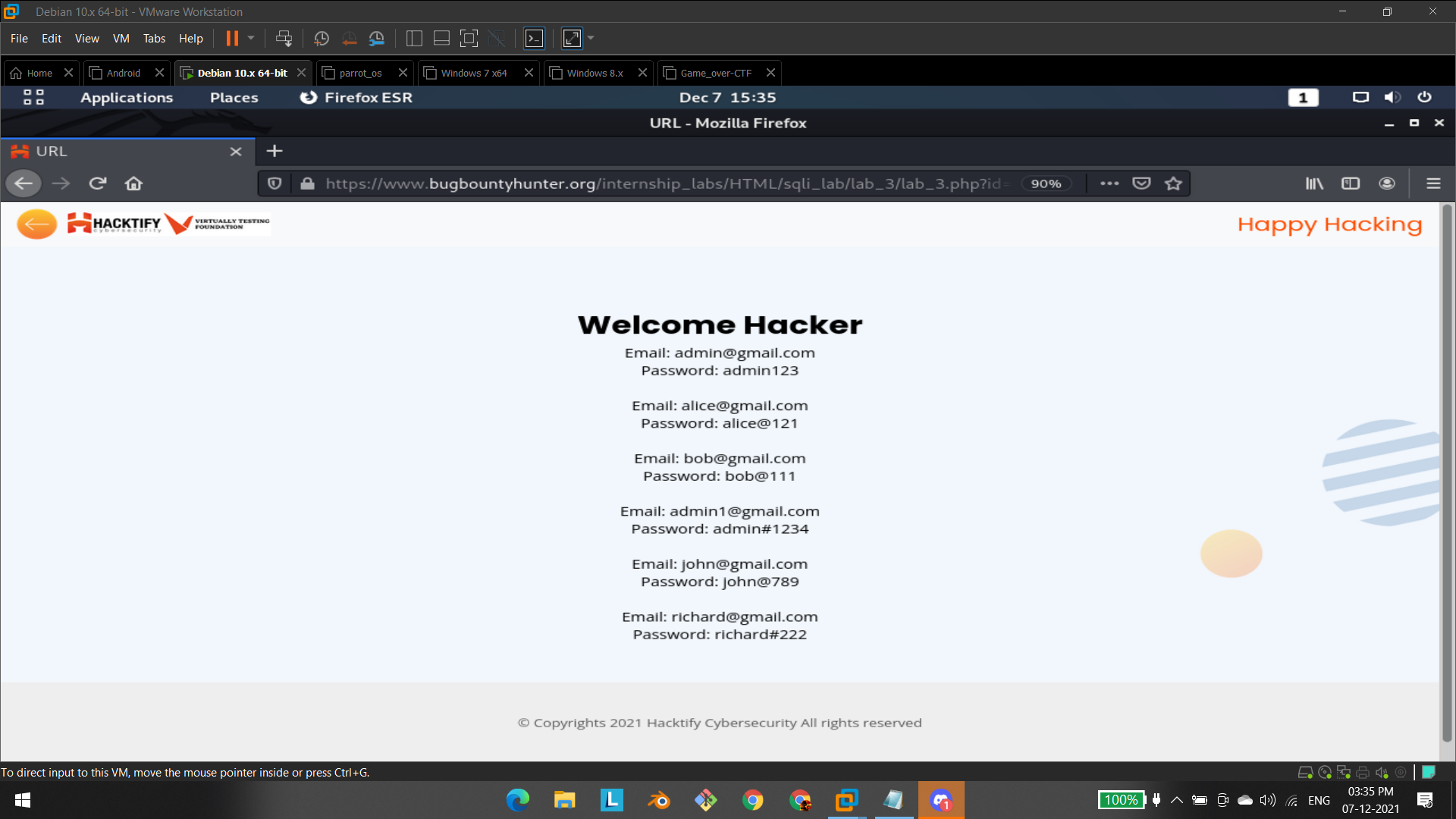
# 

# Proof of Concept

**Query:**

Query:" or ""="

**link:**[https://www.bugbountyhunter.org/internship\_labs/HTML/sqli\_lab/lab\_3/lab\_3.php?id=" or ""="](https://www.bugbountyhunter.org/internship_labs/HTML/sqli_lab/lab_3/lab_3.php?id=)

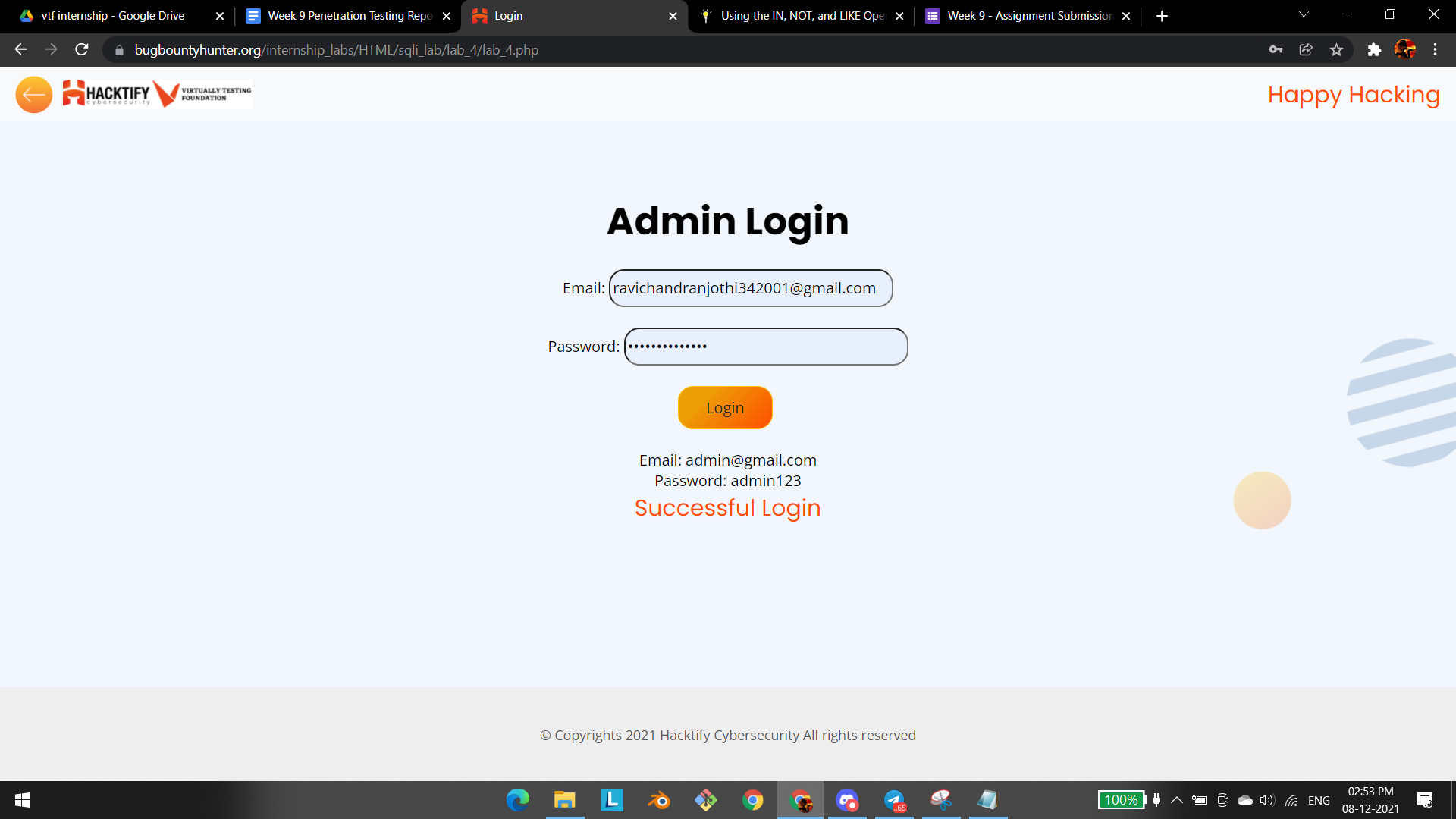


# 1.4. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept



# 

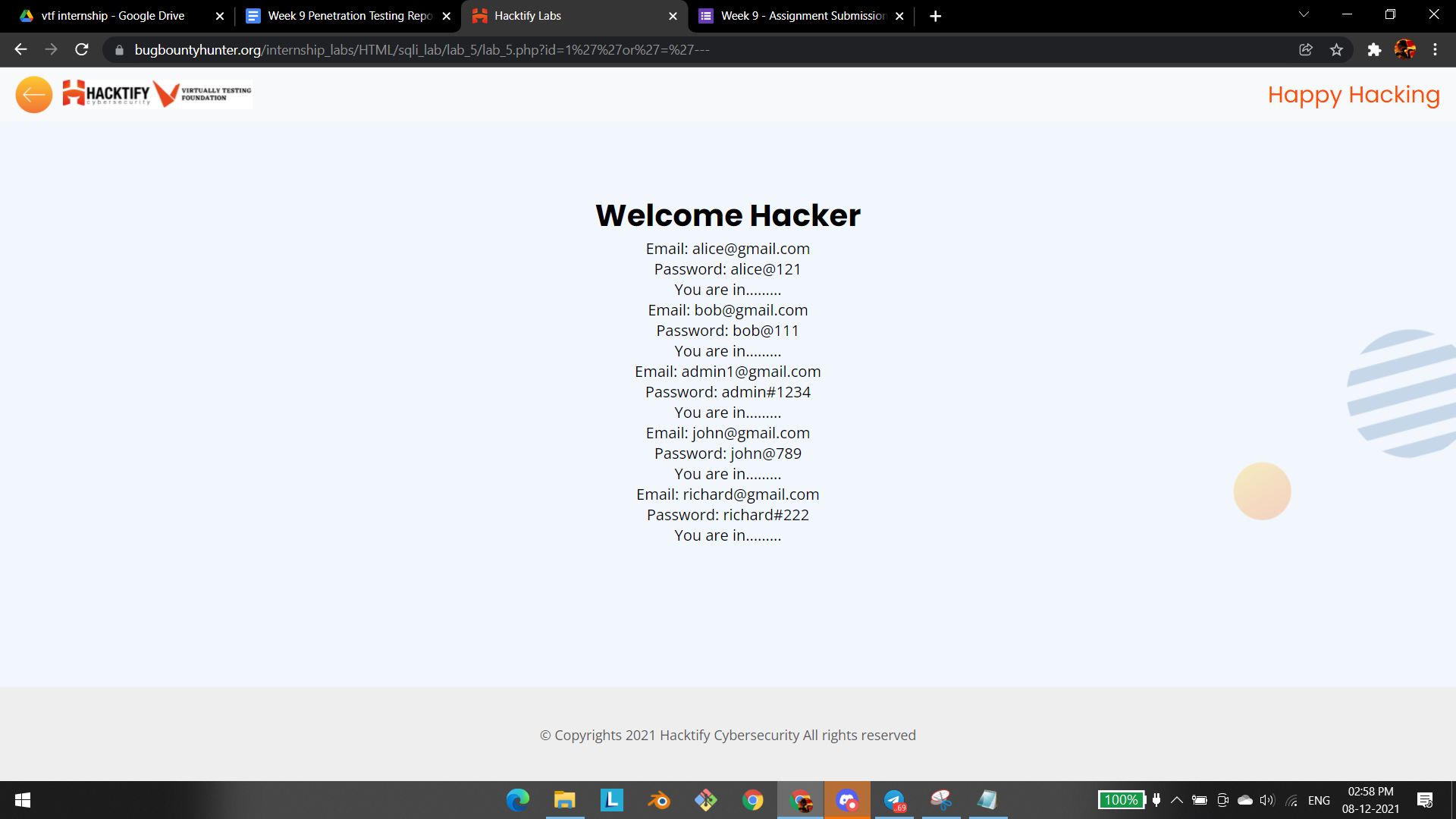
# 

# 1.5. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

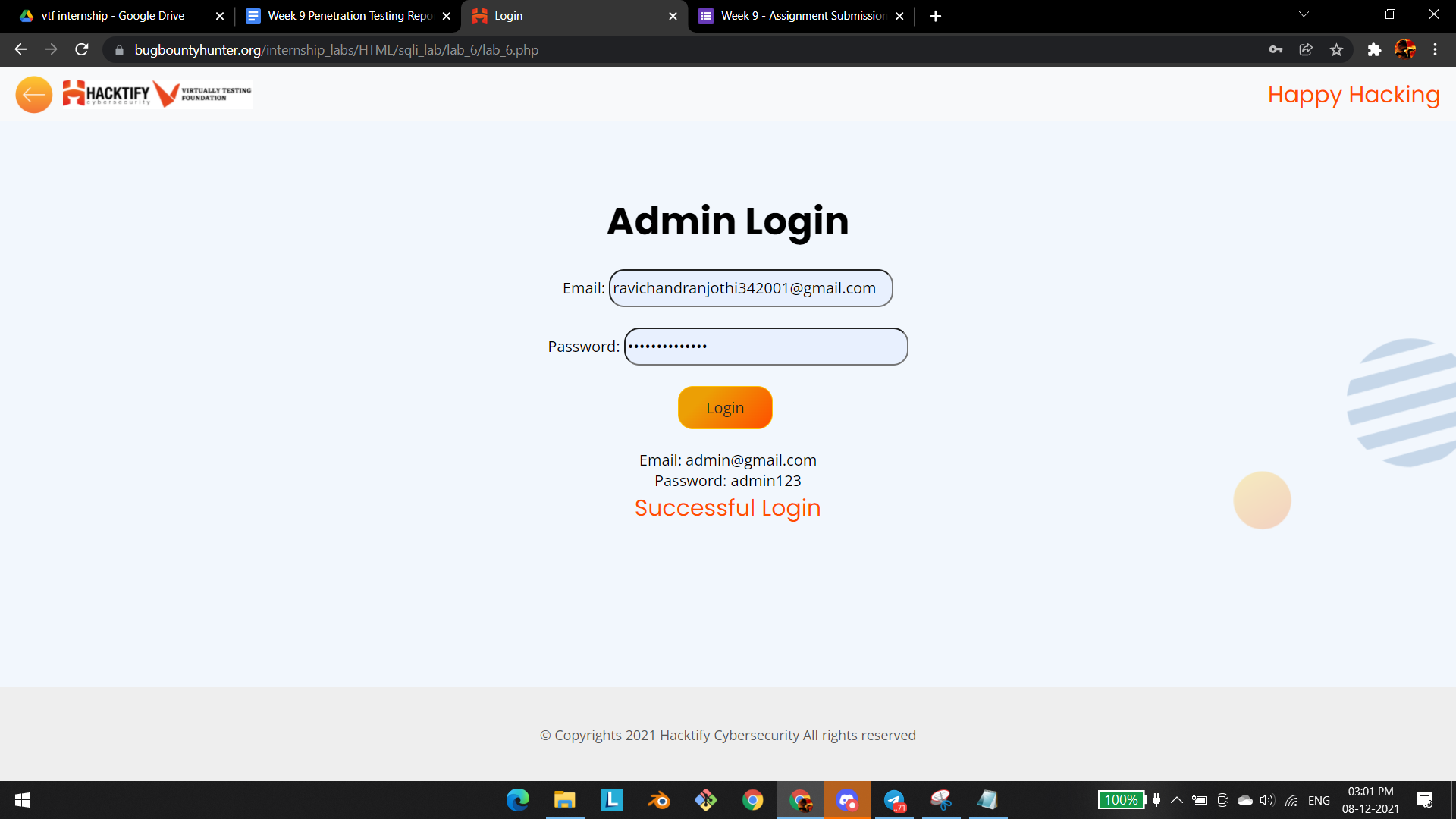


# 1.6. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

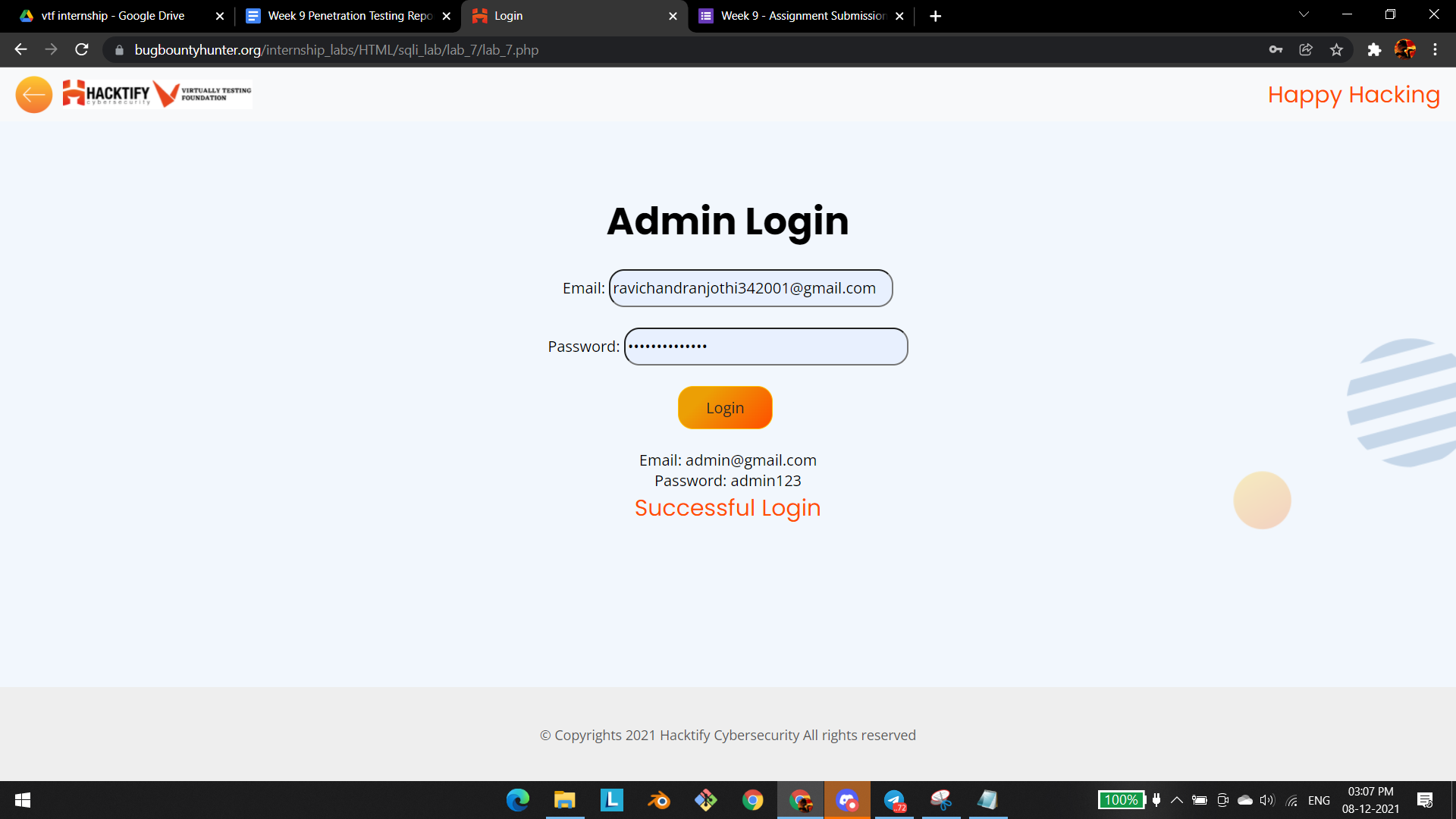


# 1.7. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept



# 

# 

# 1.8. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

# 1.9. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

# 1.10. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

# 1.11. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

# 1.12. {Sub-lab-2 Name}

| **Reference** | **Risk Rating** |
| --- | --- |
| {Sub-lab-2 Name} | **Low / Medium / High** |
| **Tools Used** | |
| Tools that you have used to find the vulnerability. | |
| **Vulnerability Description** | |
| About the vulnerability and its working | |
| **How It Was Discovered** | |
| Automated Tools / Manual Analysis | |
| **Vulnerable URLs** | |
| URLs of the vulnerable pages in the lab | |
| **Consequences of not Fixing the Issue** | |
| What will be the consequences if the vulnerability is not patched? | |
| **Suggested Countermeasures** | |
| Give some Suggestions to stand against this vulnerability | |
| **References** | |
| URLs to the sources used to know more about this vulnerability | |

# 

# Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

**NOTES:**

* **Everything mentioned inside {} has to be changed based on your week, labs and sub-labs.**
* **If you have 2 labs in same week you need to mention that, if not ignore those mentions for lab 2.**
* **Here it is given with 2 Sub-labs vulnerability, you need to add all the sub-labs based on your labs.**
* **Don’t forget to add the screenshot of the vulnerability in the proof of concept.**
* **Add only 1 screenshot in the Proof of Concept section.**
* **This NOTE session is only for your reference, don’t forget to delete this in the report you submit.**