**Week 07**

**Penetration Testing Report**

**Introduction**

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 07 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 07 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** | Lab 1-Server-Side Request Forgery(CSRF) |
| --- | --- |

**3. Summary**

Outlined is a Black Box Application Security assessment for the **Week 07 Labs**.

**Total number of Sub-labs: {count} Sub-labs**

| **High** | **Medium** | **Low** |
| --- | --- | --- |
| **2** | **2** | **2** |

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

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

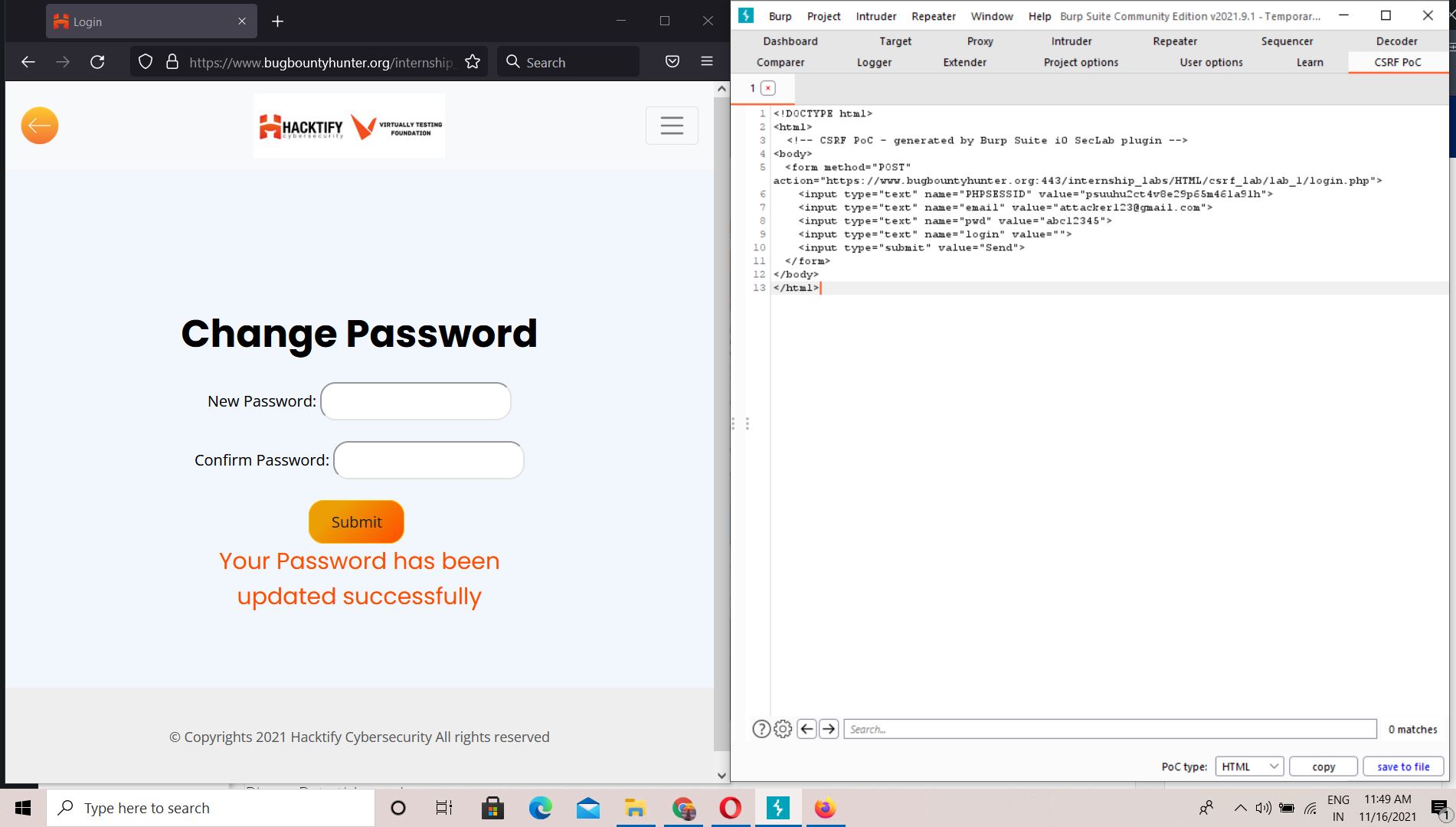
**Low - Number of Sub-labs with Easy difficulty level**

# 1. Server-Side Request Forgery

# 1.1. [Eassyy CSRF](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_1/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| Eassyy CSRF | **Low** |
| **Tools Used** | |
| Web Browser,Burp Suite | |
| **Vulnerability Description** | |
| In this lab ,the vulnerability is Cross-Site Request Forgery CSRF in which a victim load or executes malicious unwanted things on website. | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_1/login.php | |
| **Consequences of not Fixing the Issue** | |
| In this attack an attacker can take full control of the account by changing the password,username of victims account,and taking full access. | |
| **Suggested Countermeasures** | |
| By implementing CSRF Tokens | |
| **References** | |
| <https://portswigger.net/web-security/csrf>  https://owasp.org/www-community/attacks/csrf | |

# Proof of Concept



# 

# 

# 

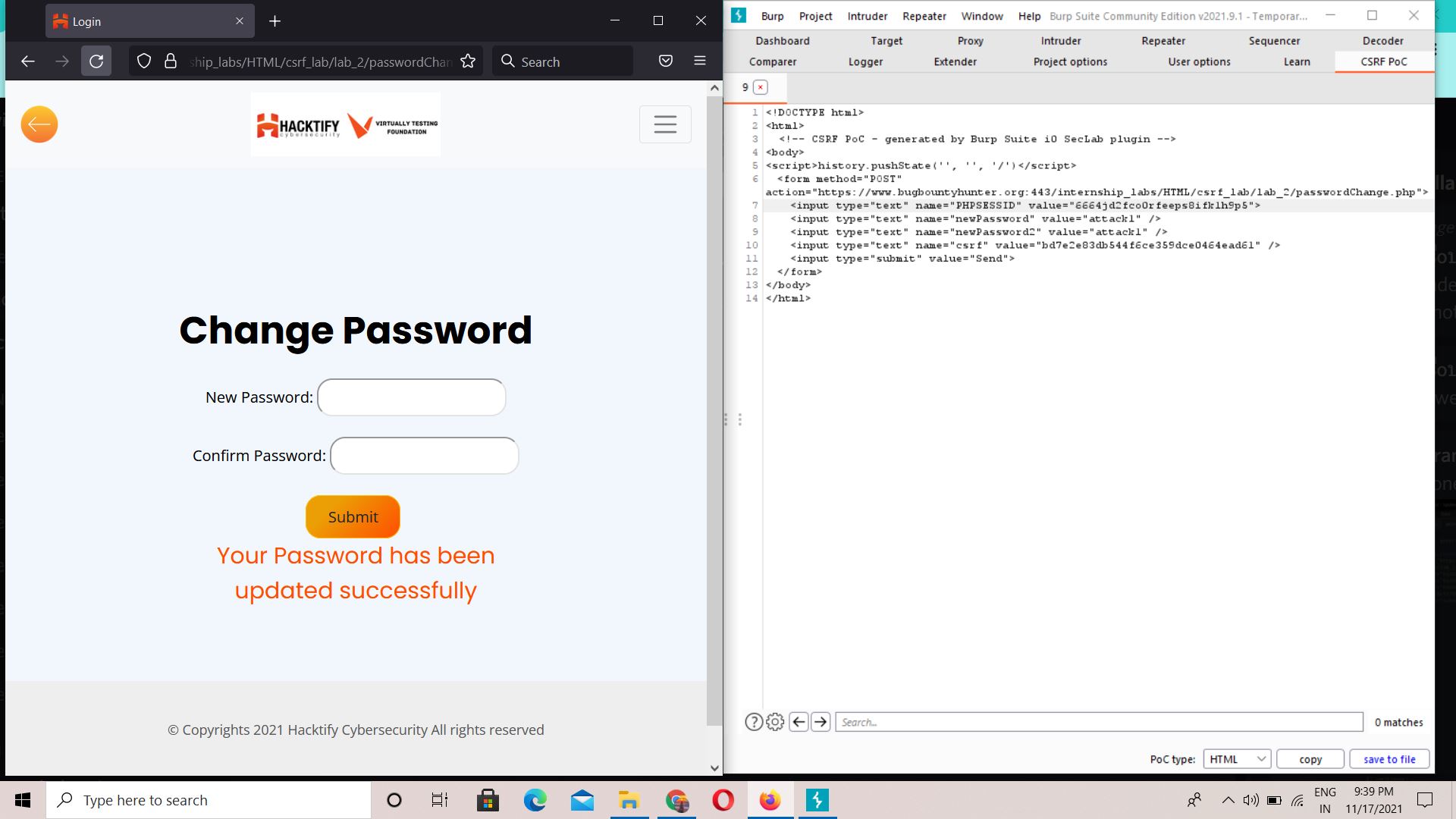
# 

# 

# 1.2. [Always Validate Tokens](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_2/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| Always Validate Tokens | **Medium** |
| **Tools Used** | |
| Web Browser,Burp Suite | |
| **Vulnerability Description** | |
| In this lab ,the vulnerability is Cross-Site Request Forgery CSRF in which a victim load or execute malicious things on website. | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_2/index.php | |
| **Consequences of not Fixing the Issue** | |
| In this attack an attacker can take full control of the account by changing password,username,clear tokens of victims account,and taking full access. | |
| **Suggested Countermeasures** | |
|  | |
| **References** | |
| https://owasp.org/www-community/attacks/csrf | |

# Proof of Concept



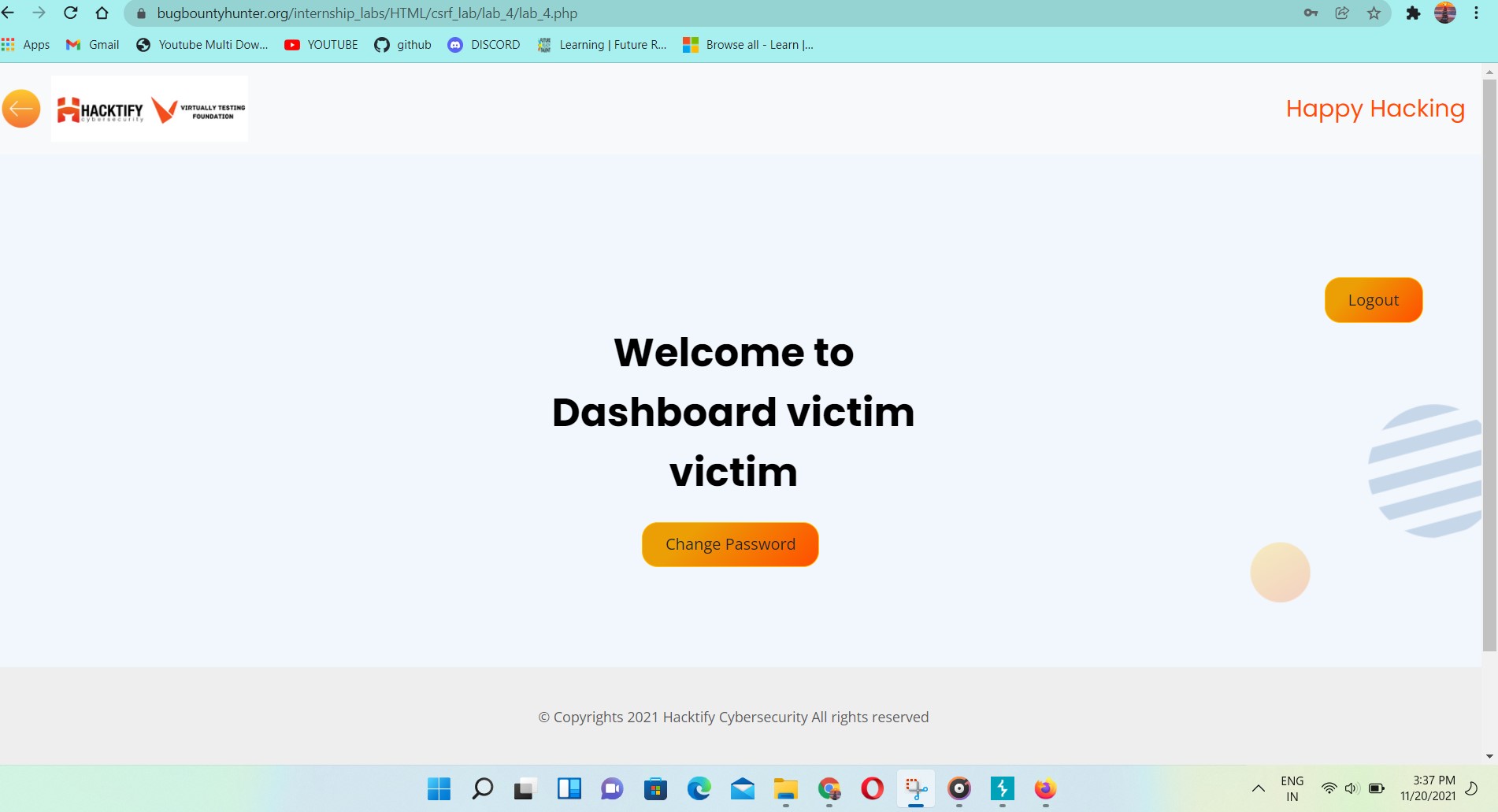
# 

# 

# 1.3. [I hate when someone uses my tokens!](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_4/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| I hate when someone uses my tokens! | **Medium** |
| **Tools Used** | |
| web browser,burp suite | |
| **Vulnerability Description** | |
| In this vulnerability an attacker can take full control on account by changing the values of tokens of users account. | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_4/index.php | |
| **Consequences of not Fixing the Issue** | |
| In this attack an attacker can change the tokens of users,possibility of taking full control over users account or system. | |
| **Suggested Countermeasures** | |
| usage of csrf tokens | |
| **References** | |
| https://owasp.org/www-community/attacks/csrf | |

# Proof of Concept

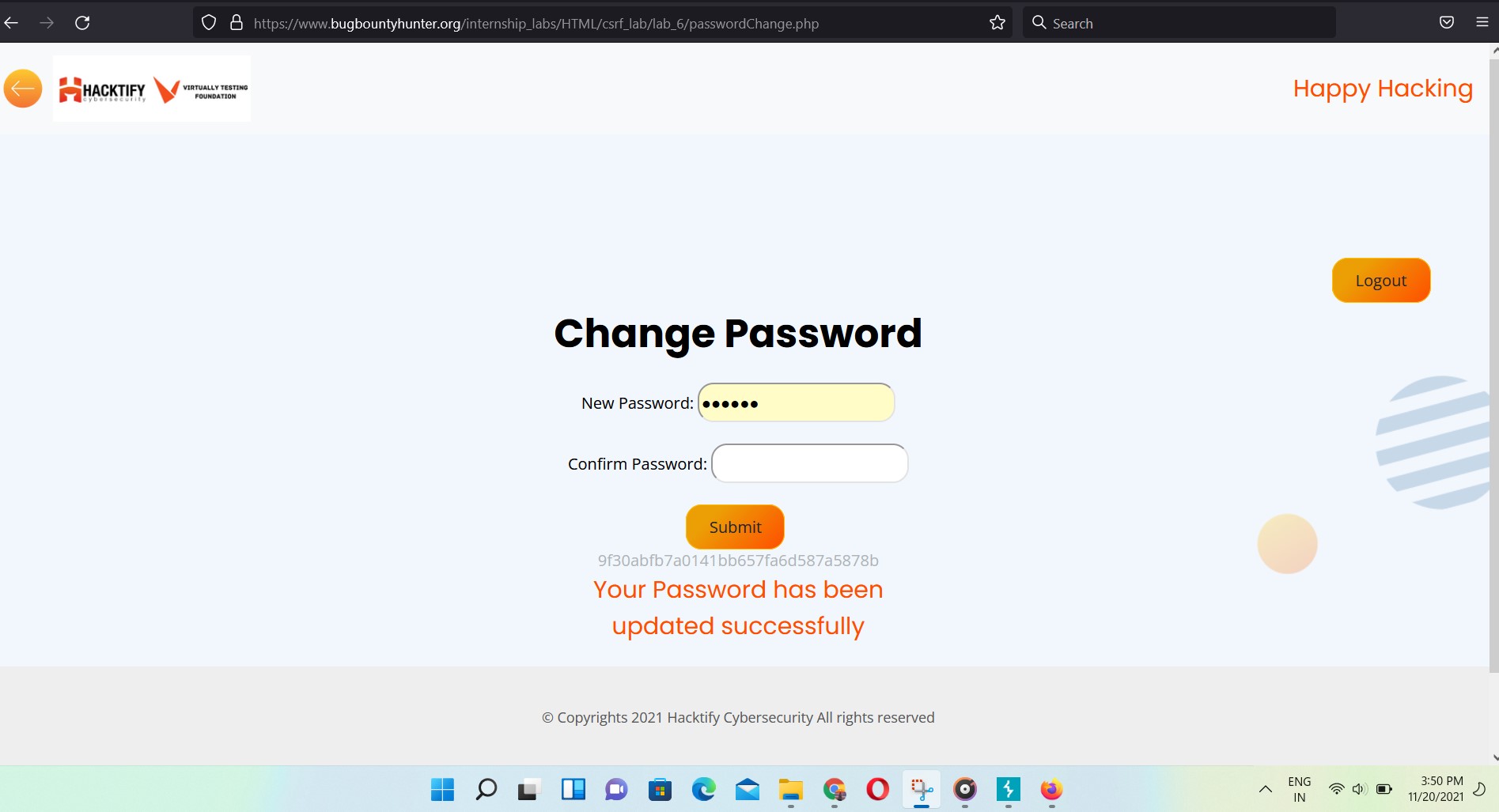


# 

# 1.4. [GET Me or POST ME](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_6/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| GET ME or POST ME | **Low** |
| **Tools Used** | |
| Web Browser ,Burp Suite | |
| **Vulnerability Description** | |
| In this lab,vulnerability is Cross-Site Request Forgery that makes victims load or execute malicious or unwanted things on web applications. | |
| **How It Was Discovered** | |
| Manual Analysis : changing the request method from POST to GET | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_6/index.php | |
| **Consequences of not Fixing the Issue** | |
| in this attack an attacker can change the tokens of users,possibility of taking full control over users account or system. | |
| **Suggested Countermeasures** | |
| usage of csrf tokens | |
| **References** | |
| https://owasp.org/www-community/attacks/csrf | |

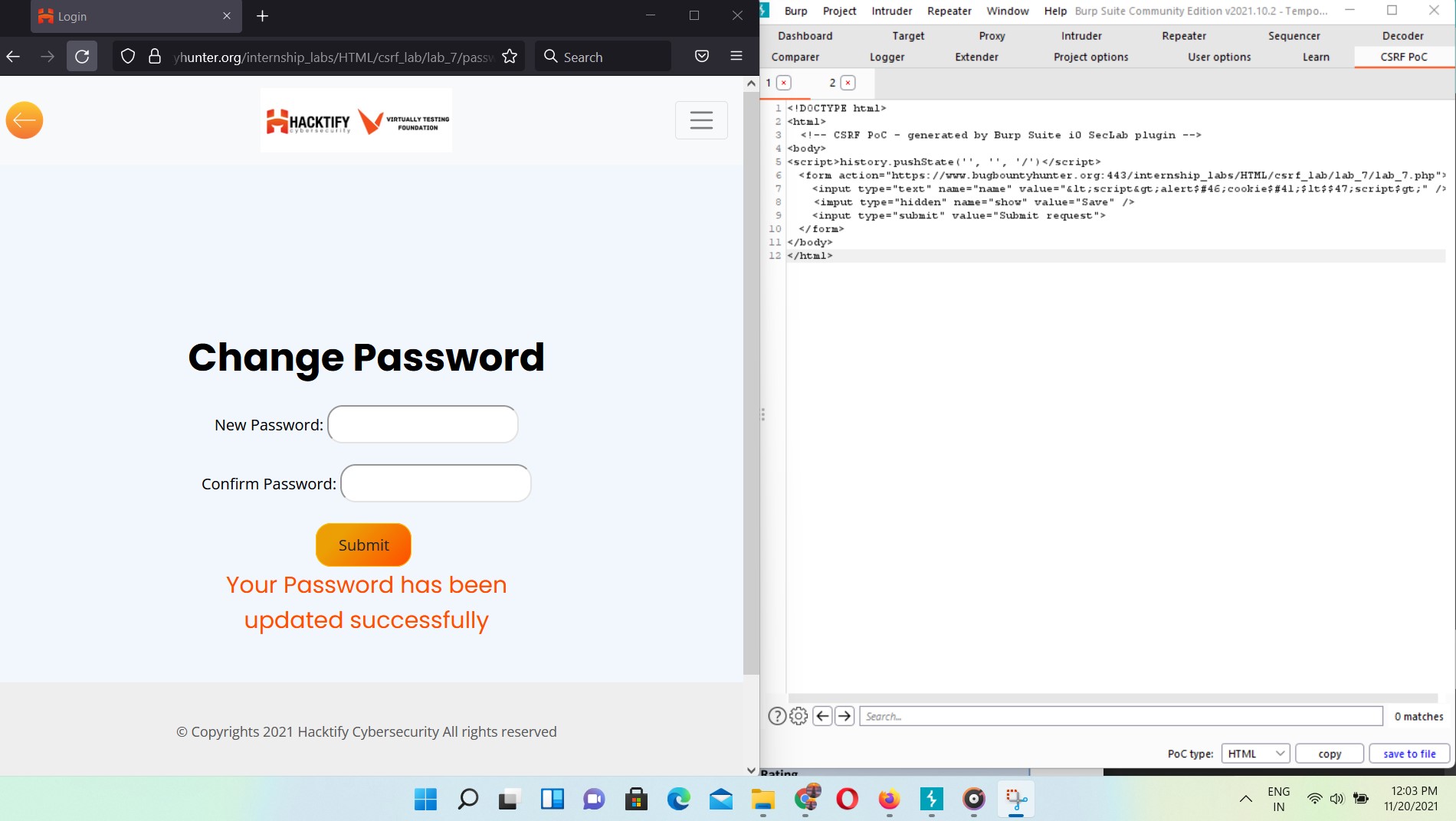
# Proof of Concept



# 1.5. [XSS the saviour](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_7/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| XSS the Saviour | **High** |
| **Tools Used** | |
| Web Browser,Burp Suite | |
| **Vulnerability Description** | |
| This vulnerability is Cross-Site Request Forgery that makes victims load or execute malicious or unwanted things on web applications. | |
| **How It Was Discovered** | |
| Manual Analysis Injection of XSS script on attacker,and implement into victims account after generating CSRF poc | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_7/index.php | |
| **Consequences of not Fixing the Issue** | |
| in this attack an attacker can change the tokens of users,possibility of taking full control over users account or system. | |
| **Suggested Countermeasures** | |
| It can mitigated by creating pre-sessions (sessions before a user is authenticated) and including tokens in login form | |
| **References** | |
| <https://owasp.org/www-community/attacks/csrf>  https://portswigger.net/web-security/csrf | |

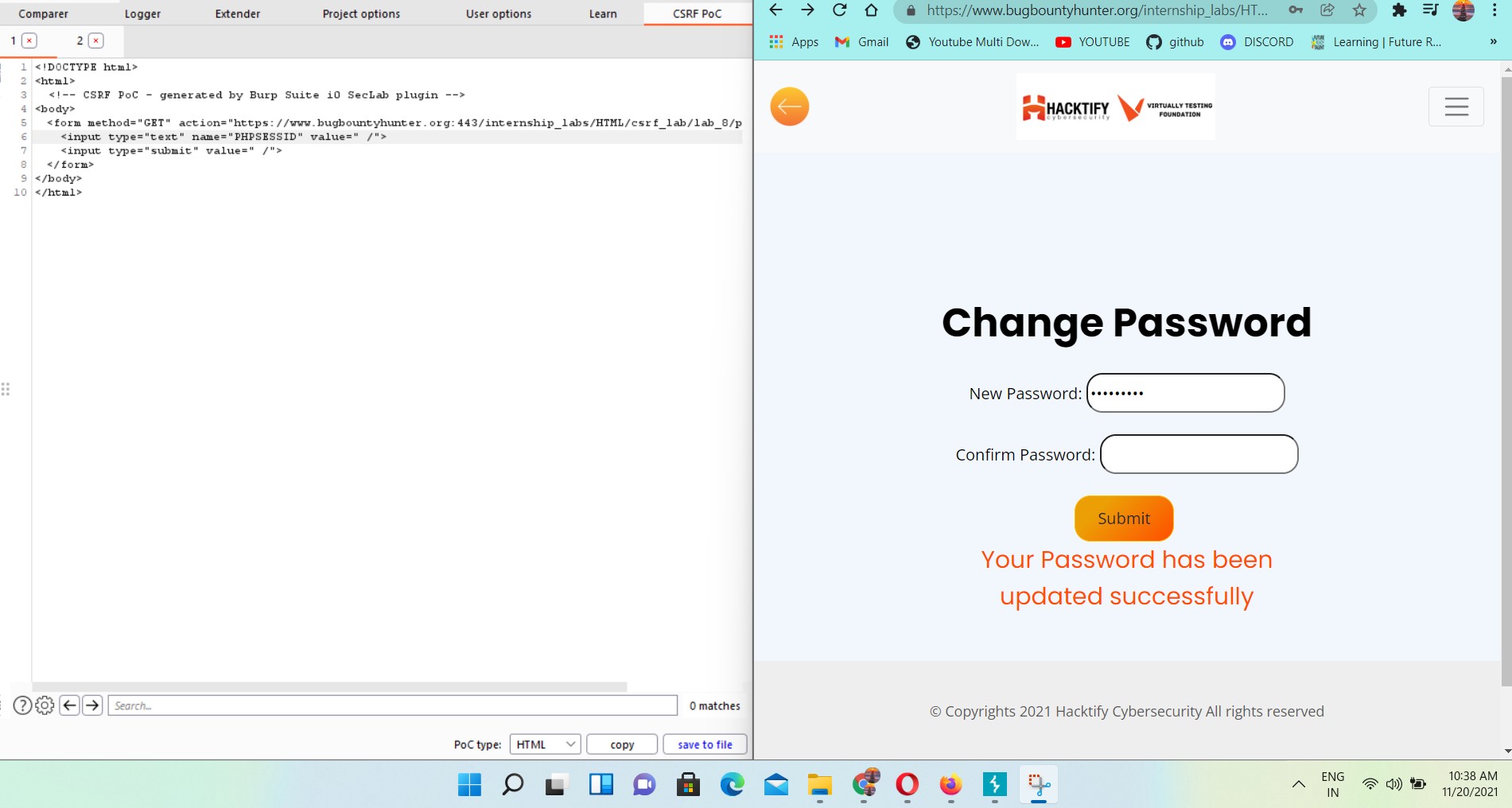
# Proof of Concept



**1.6** [**rm -rf token**](https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_8/index.php)

| **Reference** | **Risk Rating** |
| --- | --- |
| rm -rf token | **High** |
| **Tools Used** | |
| Web Browser,Burp Suite | |
| **Vulnerability Description** | |
| In this lab,vulnerability is Cross-Site Request Forgery that makes victims load or execute malicious or unwanted things on web applications. | |
| **How It Was Discovered** | |
| Manual Analysis ,by removing csrf token & sending request | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship\_labs/HTML/csrf\_lab/lab\_8/login.php | |
| **Consequences of not Fixing the Issue** | |
|  | |
| **Suggested Countermeasures** | |
| It can be mitigated by creating pre-sessions (sessions before a user is authenticated) and including tokens in login form. | |
| **References** | |
| https://owasp.org/www-community/attacks/csrf | |

# Proof of Concept



# 