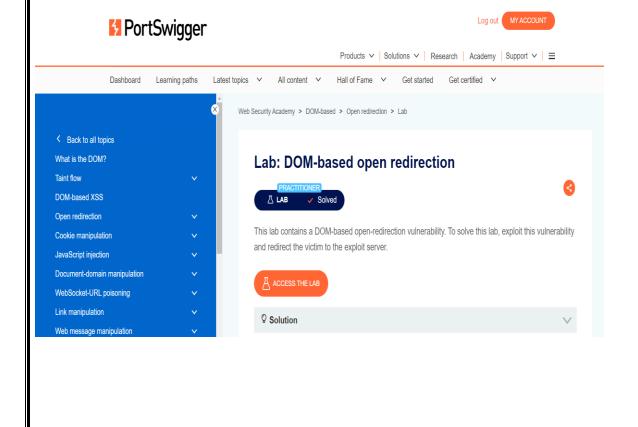
VULNERABILITY LABS

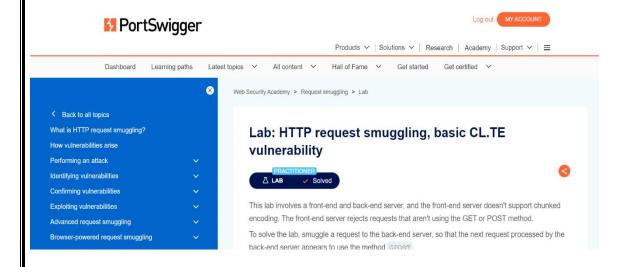
- 1.AUTHENTICATION
- 2. DOCUMENT OBJECT MODEL (DOM)
- 3. HTTP REQUEST SMUGGLING
- 4. CROSS ORIGIN RESOURCE SHARING (CORS)
- 5. SQL INJECTION
- 6. CROSS SITE SCRIPTING (XSS)
- 7. CROSS SITE REQUEST FORGERY
- 8. SERVER SIDE TEMPLATE INJECTION
- 9. COMMAND INJECTION
- 10. SERVER SIDE REQUEST FORGERY (SSRF)

AUTHENTICATION Log out MY ACCOUNT PortSwigger Products \checkmark | Solutions \checkmark | Research | Academy | Support \checkmark | \equiv × Web Security Academy > Authentication vulnerabilities > Password-based > Lab Sack to all topics Lab: Username enumeration via different responses How vulnerabilities arise ∆ LAB Vulnerabilities in password-based authentication This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists: Candidate usernames Vulnerabilities in OAuth authentication · Candidate passwords To solve the lab, enumerate a valid username, brute-force this user's password, then access their

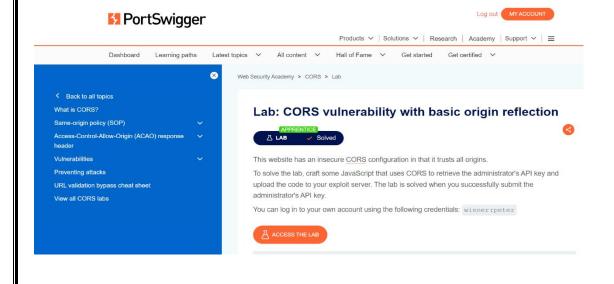
DOCUMENT OBJECT MODEL (DOM)



HTTP REQUEST SMUGGLING



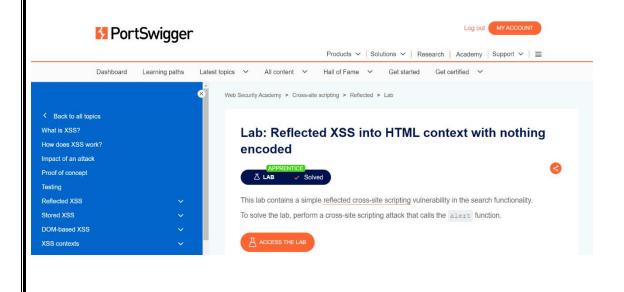
CROSS – ORIGIN RESOURCE SHARING (CORS)



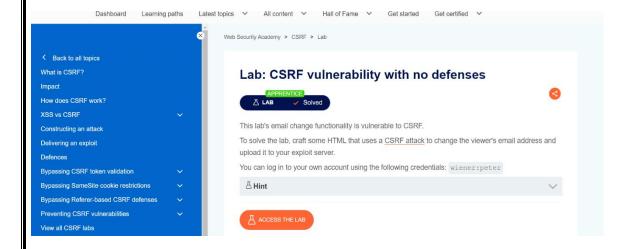
SQL INJECTION



<u>CROSS – SITE SCRIPTING (XSS)</u>



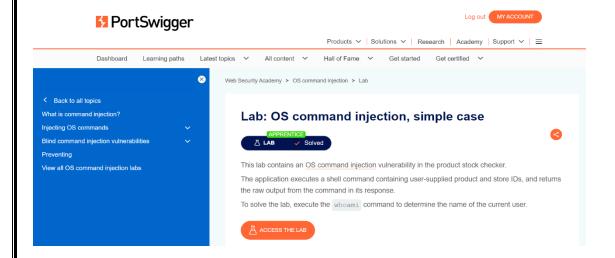
<u>CROSS – SITE REQUEST FORGERY</u>



SERVER - SIDE TEMPLATE INJECTION



COMMAND INJECTION



SERVER – SIDE REQUEST FORGERY (SSRF)

