Cybersecurity lab

2023-2024

Attack of a web application

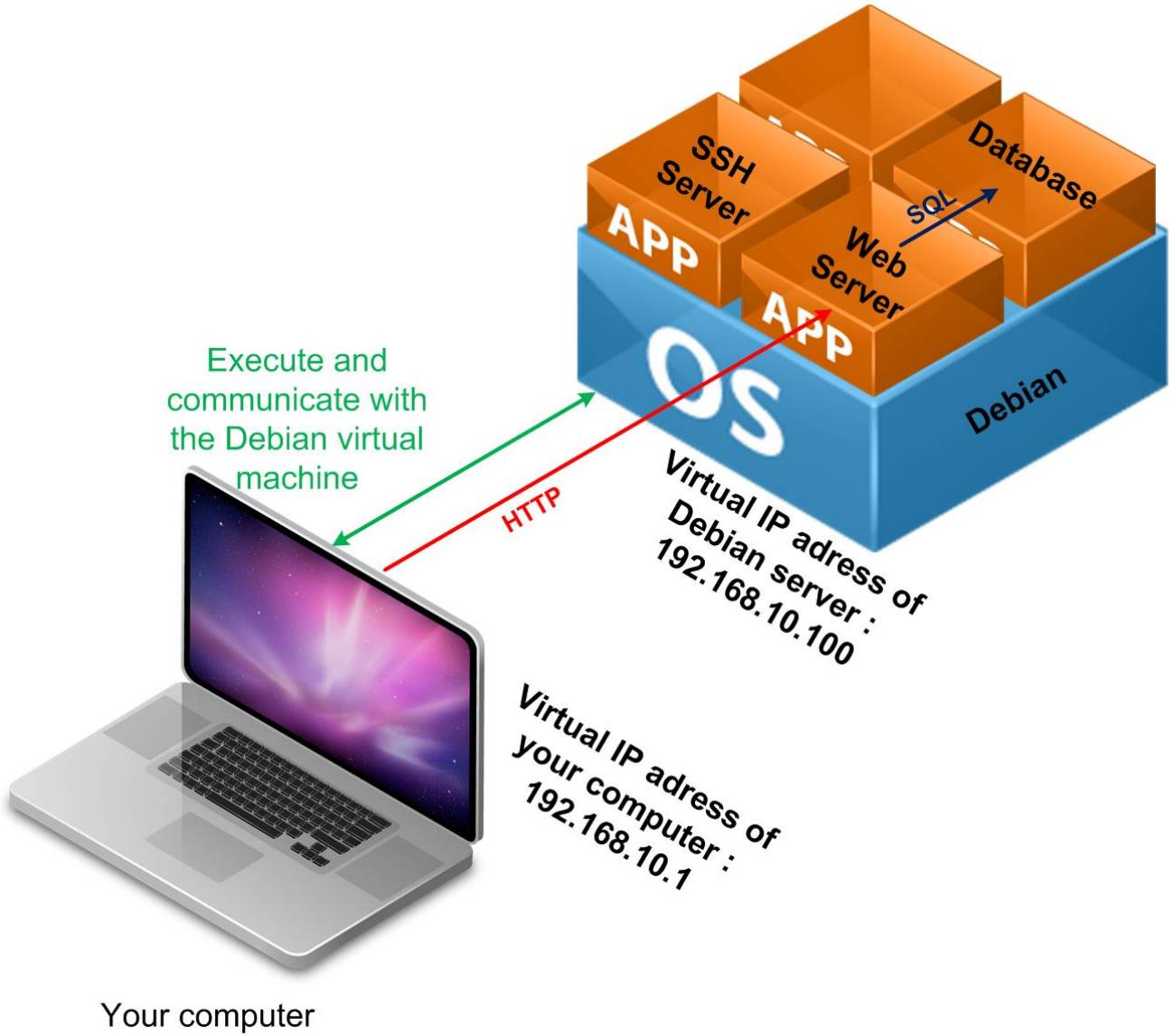
Summary

- Lab objective
- Login to the vulnerable website
- Attack
- Questions

Lab objective

- The purpose of this lab is to attack the vulnerable web application hosted on the virtual server
- At the end of this lab you will have to know how the SQLi, XSS and CSRF attacks work
- The virtual machine does not need to access the Internet in this lab

Architecture



Login to the vulnerable website

- Once the “VM Debian vulnerable" has been started, do not enter a login or password in command line interface
- From a web browser on your computer, go to the website: http://192.168.10.100
- The credentials for the web application are:
  - Login : admin
  - Password : isepsecurity
- Browse the 4 attacks presented in the menu:
  - CSRF
  - SQL injection
  - SQL injection (Blind)
  - XSS (Stored)
- Read the explanations of each attack with the URLs in the section "More information" of each page

Questions

- **CSRF**

1. Describe how the attack works
2. Does changing the method of submitting the form to POST fix the vulnerability? Justify
3. What solution do you propose to fix this vulnerability? Explain in detail how to do it

- **SQL injection**

4. Display a list of all application users by exploiting the SQL injection
5. Retrieve the hashed passwords of all users and retrieve their equivalent in clear
6. What is your recommendation to avoid SQL injection?

Questions

- **Blind SQL injection**

7. Describe the difference between blind SQL injection and previous SQL injection. Determine how to collect information
8. Determine the version number of the Mysql database. Explain your method

- **Cross Site Scripting (XSS)**

9. Explain what is the principle of this attack
10. Display the user's cookie to all visitors of this page
11. Is it better to use the "htmlspecialchars" escape function before inserting the data into the database or when the web application generates the page? Why?