What is Penetration Testing?

The phase where a hacker or a security expert exploits a vulnerability and tests how much damage he can cause using that vulnerability is called Penetration Testing phase.

Before we jump into the technicalities of the vulnerabilities listed in the OWASP Top 10 2013 list. Let's quickly try to understand how these vulnerabilities work.

Vulnerability	Explanation
Injection	It allows hacker to inject server side codes or commands. These are the flaws that allows a hacker to inject his own codes/commands into the web server that can provide illegal access to the data.
Broken Authentication and Session Management	These flaws generally arise when application functions related to security and session management are not implemented properly, which allows hackers to bypass authentication mechanisms. For eg. Logir

	mechanisms. For eg. Login
Cross Site Scripting (XSS)	This is one of the most common flaw in which hackers injects codes like HTML, JS directly into the web pages allowing them to deface websites and stealing data of the users who trust these websites.
Insecure Direct Object References (IDOR)	These are the flaws that may cause severe impact as with IDORs, the hackers get access to objects in the database that belong to other users, which allows them to steal or even edit critical data of other users on the website. They can either steal that information or even delete someone's account.
Security Misconfigurations	These are again one of the most common flaws as the developers/administrators forget to securely seal an application before making

Security Misconfigurations	These are again one of the most common flaws as the developers/administrators forget to securely seal an application before making it live. Common flaws under this vulnerability includes keeping default password, default pages etc.
Sensitive Data Exposure	These type of flaws occur when websites are unable to protect sensitive data like credit card information, passwords etc. which allows hackers to steal this information and may cause credit card fraud or identity theft.
Missing Function-Level Access Controls	These flaws occur when security implementation are not implemented properly in applications on both User interface and server i.e. front and back end respectively. This allows hackers to

Missing Function-Level Access Controls	These flaws occur when security implementation are not implemented properly in applications on both User interface and server i.e. front and back end respectively. This allows hackers to bypass security and gain restricted access.
Cross Site Request Forgery	This vulnerability allows a hacker to send forged requests on behalf of a trusted user, which allows the hacker to act on behalf of the user. For example, telling the bank server to transfer money from X to Y on the victim's behalf and the bank server accepting it.
Using Components with Known Vulnerabilities	There are certain applications or their components that are known to exhibit vulnerabilities. If anyone is using these applications, it becomes easy for hackers to exploit these vulnerabilities and steal

Using Components with Known Vulnerabilities	known to exhibit vulnerabilities. If anyone is using these applications, it becomes easy for hackers to exploit these vulnerabilities and steal user data for eg. using an older version of windows server can be exploited by using an exploit code which is available online.
Unvalidated Redirects and Forwards	This flaw redirects users from a trusted website to a malicious website, which allows hackers to steal sensitive user information. For eg. if a user visits website A which he trusts but is redirected to website X which has a malware. But as user trusts A, he ends up trusting X.

You can also check the list directly on the official OWASP website. Here's the link: https://www.owasp.org/index.php/Top_10_2013-Top_10

Don't worry if you don't understand all of these right now. We'll learn more about this

Q1/6

From where can the security experts and developers find the most common web system vulnerabilities?

A From OWASP Top 10 list.

Well done. Correct Answer.

Explanation:
OWASP has released Top 10 lists of 2010, 2013 and 2017, which helps security experts and developers to find the most common web based system vulnerabilities.

91% students get this answer correct at their first attempt

B By performing the vulnerability assessment of web based system.

C The lists can be accessed by

Q2/6

Which of the following statements correctly correspond to VAPT?

A VA helps in exploiting bugs, while PT caters with finding them.

B VA shows the impact of vulnerability, while PT only shows it exists.

C VA is dependent on PT.

D None of the above. ✓

Well done. Correct Answer.

Explanation:
VA helps in finding the vulnerabilities and shows that they exist, while PT helps in exploiting them and also tells the impact these vulnerabilities can cause. PT is dependent on VA.

Q3/6

OWASP distributes all the tools and documents for free to everyone.

A True

Well done. Correct Answer.

Explanation:
The Open Web Application Security Project (OWASP) is an Open-Source project, hence all tools, researches, documents, guidelines are made and distributed for free by the community.

65% students get this answer correct at their first attempt

B False

Q4/6

While performing penetration testing, a hacker finds that the website has injection flaws. What can be possibly done by the hacker?

A Hacker can steal all the passwords.

B Hacker can inject client side code to gain illegal access.

C Hacker can inject server side code or commands. ✓

Well done. Correct Answer.

Explanation:
Injection Vulnerabilities allow a hacker to inject and execute his own code like PHP code or commands like windows cmd commands on the server itself giving him complete control of the server.

D Hacker can't do anything as he does not have any login credentials.

Q5/6

Suppose a hacker is trying to attack a website by forcefully trying to login into the admin account. The hacker entered ‘admin’ as username and password as ‘password’ which gave him the access. Which kind of OWASP vulnerability is this?

A Injection

B IDOR

C Security misconfiguration ✓

Well done. Correct Answer.

Explanation:
This is a common vulnerability done by most developers/ admins as they keep the default password and username for convenience.

D Cross Site Request Forgery

Q6/6

Suppose your college's website data was stolen and all the student records were erased. It was found that the college's website was running on Windows server 2003 which has a public exploit. Which OWASP vulnerability is this?

A	Injection
B	IDOR
C	Security misconfiguration
D	Using components with known vulnerabilities ✓

Well done. Correct Answer.

Explanation:
These flaws occur when developers/server admins use 3rd party softwares/applications/code that already have known public vulnerabilities and anyone can search about about them and misuse it.

Now that we have come to the end of this topic, you should be able to:

1. Explain vulnerability assessment and penetration testing
2. Understand what OWASP is and what it does
3. Understand the role of OWASP, its top ten lists and the role these play in web VAPT

If you have doubts regarding any of the above mentioned points, please go through the video and text chapter again.