20 Web Security Questions

With answer key and explanation

Open Education Project at BCIT

1. In Web programming, when sending HTTP requests, is POST more secure than GET to send data over HTTP protocols ?

Answer:
The major difference is that when sending GET requests, the data is visible to everyone in the URL. In POST requests, the data is part of the header not part of the URL. However in both cases the data is not encrypted. Therefore, none of the POST or GET are secure.

2. What is a “phishing” attack ?

Answer:
Sending someone an email or hypertext message that contains a malicious link that is intended to look like a URL that the person knows.

For example, when this HTML script gets rendered in an email

https://td.com

The user only sees td.com in their email. They click on it, and it takes them to hackers.com. Hackers can fake something like td website in their domain hacker.com and ask user to enter their user/pass and then steal the user's credential

3. What is hashing in the context of security?

Answer:
A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

4. Why are hash functions used to store passwords in DB?

Answer:
Since hash is a one-way compression function, instead of storing the password itself, its hash value is stored. The user enters their password at the time of login. Then the hash value of the entered password will be compared with the stored hash value in DB and if both matched,then the user will be logged in.

5. What is MD5?

Answer:
MD5 is a hash function producing a 128-bit hash value.

6. For what purpose a proxy server is generally used by hackers?

Answer:
To hide their malicious activity on the network.

7. What is Man in the Middle attack?

Answer:
Man in the Middle or MitM attacks create a server with a relay address and when a data is sent between two pastries a hacker gets between and spy

8. What technology is used to hide information inside a picture ?

Answer:
Steganography is used to hide information in images,videos or even music.

9. What are the general practices to improve the security of a software product?

Answer:

- check entry points
- employing layered defenses
- least privilege
- Reduce Attack Surface Early
- Try to trap memory-related issues at run time, including heap-based buffer overruns

10. When is the best opportunity to influence the security design of a product

Answer:
The early in the product life cycle

11. What is fuzzing testing technique in improving security?

Answer:
Fuzzing testing technique is a very useful testing technique for finding security defects and means taking valid data and morphing it and feeding it back to the application

12. What is the difference between symmetric and asymmetric keys in data encryption ?

Answer:
Symmetric security (encryption) same key to open and to lock
Asymmetric security (encryption): two keys of public key and private key

13. How are public keys and private keys used?

Answer:
•Tom gives his public key to everyone
•However only Tom has access to his private key
•What Tom locks (signs) using his private key can only be opened by Tom's public key
•What Other people lock using Tom's public key can only be opened by Tom's private key

14. What is a two-step authentication?

Answer:
It is authentication in two step, 1) using something they already know (password) and a 2) second temporary code which will be sent to them (to email, cell phone etc)

15. Which of the following four passwords is the most secure?

A. rrr34567
B. G$4Th!5Z
C. kind*48
D. 123456

Answer:B
It contains a combination of numbers,letters and symbols; it contains both upper and lower case letters; and it does not include any sequence of numbers nor includes any words from the dictionary.

16. Is a private browser such as incognito mode in chrome more secure?

Answer:
Private browsing does not make browsing more secure; private proving simply prevents browsers from storing certain kinds of files on the user's device (cookies, caching js file). Otherwise the data are still to whoever spoofing the network

17. Can Turning off the GPS of our smartphone prevent any tracking of our phone’s location?

Answer:
No! Aside from GPS, smartphones can also be tracked using the cellular network towers or /and Wi-Fi networks that the phone is connected to. The difference is that without GPS the location of the smartphone is less accurate

18. What is the main difference between “https://” and "http://" at the beginning of a URL of a web page?

Answer:
Https is the encrypted version of http. That means the exchanged data over the net is encrypted

19. Is a public Wi-Fi network safe for online banking if it requires a password to access?

Answer:
If a WiFi key is accessible to everyone, that means anyone can connect and run network spoofing applications (such as wireshark) and eavesdrop the exchange of data. However,banking over a secure website, https, is fine on public WiFi as long as you are 100% sure you are entering your credentials at the right website, not a fake copy of your bank's website

20. How can using a Virtual Private Network (VPN) improve security?

Answer:
A Virtual Private Network creates an encrypted connection between a user's device and the internet

Aug 2020