19UCS181 - VAIBHAV

The LNM Institute of Information Technology, Jaipur

Department of Computer Science & Engineering

Web Security (WEBSEC)

End Term

2021-22 Odd Sem

Time: 180 Minutes **Date:** 14/12/2021 **Maximum Marks:** 40

Instructions:. *There are total 9 questions. All questions are compulsory.Answer without reasoning will not be considered.*

Q.1:	Suppose you have a website http://hello.com. The website uses a third-party java script code: <script src="http://sing/script.js"> <script>. The http://sing/script.js contains the following code: **console.log("sing");** **fetch("http://sing/api");** When you open http://hello.com, you get the following output in console: "Access to fetch at http://sing/api has been blocked by CORS policy." The third party script tried to load data from the third party api, but it failed to load despite third party api and third party script have the same origin. Explain the reason of failure with proper reasoning.	[5]
Q.2:	Can same origin policy of browser be bypassed by exploiting a bug in browser? Explain with proper reasoning and example. Suggest possible way of defending the exploit for the bug in browser.	[5]
Q.3:	Suppose an attacker inject a script in a website using a comment section. The script tag contains some malicious payload <script> alert(1);<script>. Can content security policy defend against the given stored XSS attack? Explain with proper reasoning.	[5]
Q.4:	Explain how privilege seperation and least privilege principal help in secure brwoser design with example attack.	[5]
Q.5:	Explain how CSRF attack can be stopped by CSRF token with a suitable example.	[5]
Q.6:	Explain how a non executable stack can stop code injection attack using buffer overflow and how return to libc can be launched despite of non executable stack.	[4]
Q.7:	Explain how clickjacking attack can be stopped by X frame option and content security policy with an example.	[4]
Q.8:	According to the best security practice defined for web application, session related data should be created for each new session and the session interval should be shorter for better security. Expalin the advantage and disadvantage of such practice with an example.	[3]
Q.9:	Suppose you are going to develop a web application for mess service and mess payment system in your campus. The web application will be used within the campus intranet. You decided to use threat modeling for the web application. Explain how and when threat modeling will be performed in the given scenario. Explain also the advantage of threat modeling in the given case.	[4]