1. **List out the techniques used to prevent web server attacks?**

- Patch Management
- Secure installation and configuration of the O.S
- Safe installation and configuration of the web server software
- Scanning system vulnerability
- Anti-virus and firewalls
- Remote administration disabling
- Removing of unused and default account
- Changing of default ports and settings to customs port and settings

2. **What is REST Security Design Principles?**

1. **Least Privilege:** An entity should only have the required set of permissions to perform the actions for which they are authorized, and no more. Permissions can be added as needed and should be revoked when no longer in use.

2. **Fail-Safe Defaults:** A user's default access level to any resource in the system should be "denied" unless they've been granted a "permit" explicitly.

3. **Economy of Mechanism:** The design should be as simple as possible. All the component interfaces and the interactions between them should be simple enough to understand.

4. **Complete Mediation:** A system should validate access rights to all its resources to ensure that they're allowed and should not rely on cached permission matrix. If the access level to a given resource is being revoked, but that isn't reflected in the permission matrix, it would violate the security.

5. **Open Design:** This principle highlights the importance of building a system in an open manner—with no secret, confidential algorithms.

6. **Separation of Privilege:** Granting permissions to an entity should not be purely based on a single condition; a combination of conditions based on the type of resource is a better idea.

7. **Least Common Mechanism:** It concerns the risk of sharing state among different components. If one can corrupt the shared state, it can then corrupt all the other components that depend on it.

8. **Psychological Acceptability:** It states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present. In short, security should not make worse the user experience.

3. **How can we improve cloud security?**

1) Implement Strong Authentication Protocol
2) User Access Management Solutions.
3) Monitor, Log, and Analyze User Activities.
4) Provide Employee Training.
5) Implement a Data Backup and Recovery Policy.
6) Take Advantage of Cloud Computing Without the Security Risks.
7) Deploy Two-Factor Authentication
8) Monitor, Log, and Analyze User Activities

4. What are the various ways to handle account brute forcing?

1) Password Length.
2) Password Complexity.
3) Limit Login Attempts.
4) Modifying htaccess file.
5) Using Captcha.
6) Two Factor Authentications.
7) Create rule of Web Application Firewall (WAF)

5. What is DLP (Data Loss Prevention)?

DLP (Data Loss Prevention) is an acronym for data loss prevention, or data leak prevention, and refers to network security tools that can identify confidential information, track its movement through an enterprise, and prevent unauthorized exposure or disclosure of sensitive data by enforcing leak prevention policies. Sensitive information is:

- Corporate data, including strategic planning documents, financial documents, due diligence research and employee information.
- Intellectual property such as product design documents, internal price lists, source code and process documentation.
- Customer information, including credit card numbers, medical records, financial statements and Social Security numbers.

If you want to read more interview questions and answers about application security, API security and Cloud security, click the link: **https://www.amazon.com/Application-Security-Information-Interview-Questions-ebook/dp/B07VJKWH37**