EXAMINATIONS – 2021

TRIMESTER 2

NWEN 304

Advanced Network Applications

Time Allowed: ONE HOUR

CLOSED BOOK

Permitted materials: Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this examination.
No electronic dictionaries are allowed.

Instructions: Attempt ALL TWENTY ONE (21) questions:

There are THREE (3) sections:

- Section A - True or False [10 marks]
- Section B - Multiple Choice [20 marks]
- Section C - short Answers [30 marks]

The examination consists of 60 marks in total.

SECTION A [10 marks] State True or False by circling the correct answer.

1. HTTP is a statetless protocol.

   a. True
   b. False

   True

2. When cache contents are set with a private directive, it means that the contents cannot be stored in browser's cache.

   a. True
   b. False

   False

3. In quorum consensus, strong consistency arises when the read sets do not overlap with the write sets.

   a. True
   b. False

   False

4. Relational databases support horizontal scaling while NoSQL databases support vertical scaling.

   a. True
   b. False

   False

5. I can get a cookie from a website I've never been to.

   a. True
   b. False

   True

SECTION B [20 marks] Multiple Choice Questions. Circle the correct answer(s).

6. How are the route parameters captured in a Node application?

   a. eq.data
   b. app.locals
   c. req.params
   d. res.params

   c

7. What will be the output of the following EJS code:?

```
{
  "name":"<strong>Smith</strong>"
}
 <p>Welcome, <%=user %>.</p>
```

   a. Smith
   b. Smith
   c. **Smith**
   d. Run time error

   b

8. Which of the following represents a record in NoSQL?

   a. Field
   b. Document
   c. Collection
   d. database

   b

9. Which one of the following flags should we use to ensure that our cookies are only sent over HTTPS?

   a. HTTPOnly
   b. Secure
   c. SameSite
   d. HTTPSOnly

   b

10. Which of the following is not an example of XSS attack? .

    a. Stored XSS
    b. DNS XSS
    c. Refelected XSS
    d. DOM based XSS

    b

11. Select **ALL** valid statements with respect to Authorization code grant workflow.

    a. Life time of a refresh token is more than the life time of an access token.
    b. Resource server does not need to contact the authorization server for user verification.
    c. A client secret is part of the access token request which is then used to verify the client application.
    d. Authorization code grant can be used as-it-is without amendments for applications that run entirely in browser.

    a,c

12. Which of the following depicts the structure of a JWT?

    a. Header.Payload.Signature
    b. Paylaod. Header.Signature
    c. Signature.Header.Payload
    d. None of the above

    a

13. Select **ALL** valid statements.

    a. In causal consistency causally related writes must be seen by all devices in the same order.
    b. Asynchronous leader-follower replication models compromise availability in favour of consistency.
    c. A semi-synchronous leader-follower replication model avoids the issue of writes being lost when a leader fails.
    d. An overlap between read and write sets in a Quorum consensus based replication model allows reads to be consistent with the updated writes in the write set.

    a,c,d

14. Consider an application that involves more writes than reads. In such a scenario, which of the following will be a suitable configuration for Quorum consensus replication such that there is a good balance between availability and consistency?

    a. N = 3, R = 3, W = 1
    b. N = 3, R = 2, W = 2
    c. N = 3, R = 1, W = 1
    d. N = 3, R = 1, W = 3

    b

15. Which of the following consistency model is suitable when a system needs to reflect a change immediately to all the replicas ?

    - Eventual consistency
    - Strong consistency
    - Casual consistency
    - None of the above

    b

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

SECTION C [30 marks] Short Answer Questions.

16. Explain the use of CACHE-CONTROL:NO-CACHE HTTP header. **(4 marks)**

Cache-control is an HTTP header used to specify browser caching policies in both client requests and server responses.

No-cache is one of the directives that can be used with the Cache-control header. It means that the response may be stored by any cache along the path from the origin server to the client machine, even if the response is normally non-cacheable. However, the stored response MUST always go through validation with the origin server first before using it.

17. Present the polynomial that serves as the shared secret in Shamir's polynomial algorithm for (3:5) secret sharing where the secret is 7685. Give reason for the choice of the polynomial. **(4 marks)**

$$C_2x^2 + c_1x^1 + 7685$$

Shamir's algorithm is based on the fact that a polynomial of degree m-1 can be uniquely identified by m points.

18. Bob runs his bog at bobblog.com. As his blog became popular he decides to make some money and signs up with a third-party ad network. The ad provider gives him the following HTML code snippet (Snippet A), and tells him to add it to his page where he wants ads to be shown:
`<script src="http://clcikads.com/ads.js?customer=bobblog"> </script>`
Describe one attack that is possible with snippet A that can be avoided by using the attribute http-only with cookies. Briefly explain your answer. **(4 marks)**

HttpOnly for cookies can help to prevent them being accessed by client side javascript. This can stop XSS (Cross site scripting) attacks which could come from the included javascript that has been included from the remote source in the script.

19. Explain the use of ACCESS-CONTROL-ALLOW-ORIGIN" HTTP header in the context of cross-origin resource sharing (CORS). **(5 marks)**

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading of resources.

For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. For example, XMLHttpRequest and the Fetch API follow the same-origin policy.

The Access-Control-Allow-Origin response header is a CORS directive that indicates whether the response can be shared with requesting code from the given origin. It specifies either a single origin, which tells browsers to allow that origin to access the resource; or else — for requests without credentials — the "*" wildcard, to tell browsers to allow any origin to access the resource.

E.g. Access-Control-Allow-Origin: https://mozilla.org

Access-Control-Allow-Origin: * (without credentails)

20. What is the CAP theorem and why is this theorem important for developing NoSQL databases? **(5 marks)**

CAP theorem states that we can only achieve at most two out of three guarantees for a database: Consistency, Availability and Partition Tolerance. Since in the case of a distributed systems, the partitioning of the network is must, the tradeoff is always between consistency and availability.

In a NoSQL type distributed database system, multipler nodes work together to give an impression of a single working database unit to the user (horizontal scalability). When a user wants to write to the database, the data is appropriately written to a node in the distributed database. The user may not be aware of where the data is written. This update is propagated to the other relevant nodes in the system. But if few nodes fail and we still want to provide users with access to the database (availability), we will have to compromise on consistency as the updates made at one node might not have been propogated to the other end of the partition. NoSQL databases when designed need to identity which of the properties must be guranteed and solutions that cater to these requirements are build into the system.

E.g.: MongoDB picks consistency and partition tolerance Cassandra picks availability and partition tolerance

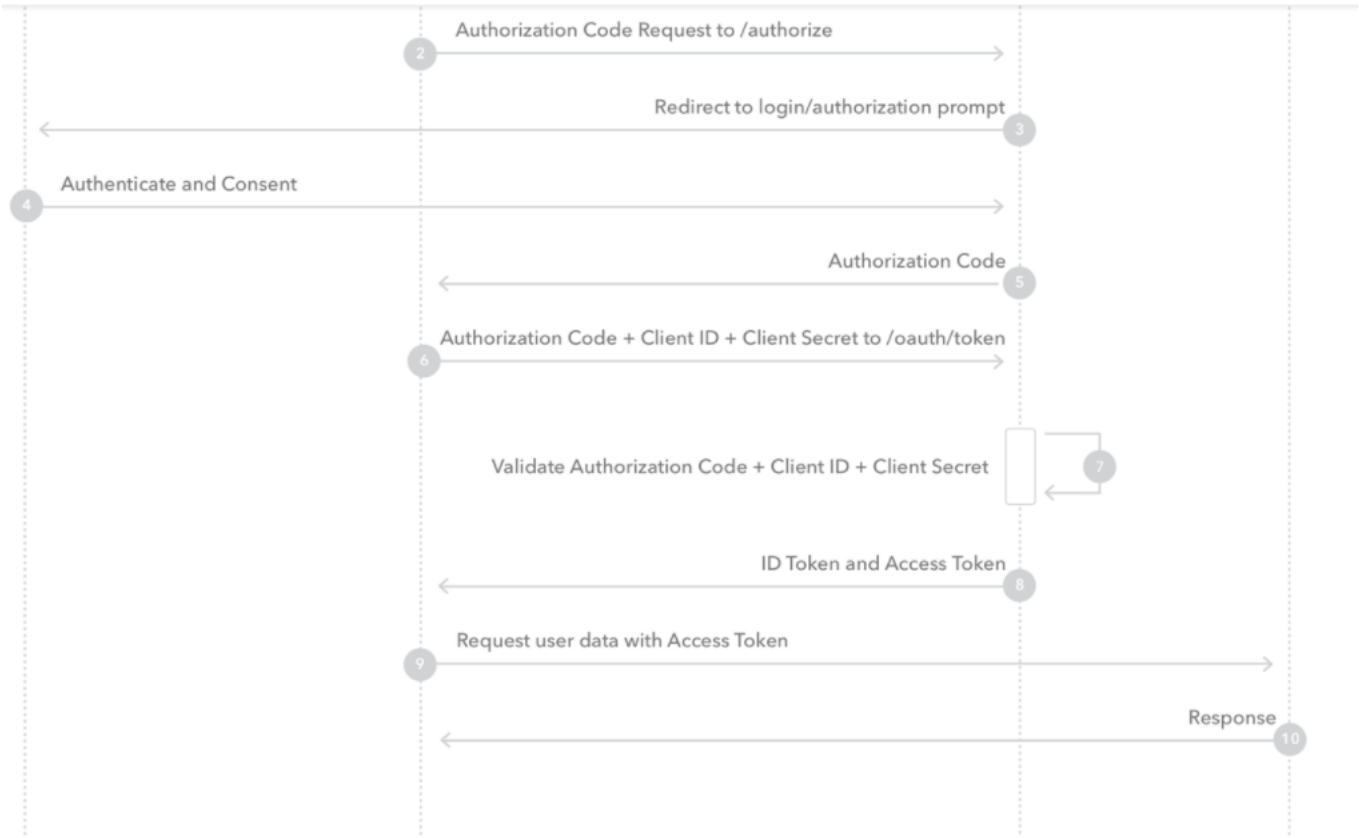
21. What is the authorization code grant type in `OAuth`? Briefly explain how this grant type enables delegated resource access in `OAuth`. **(8 marks)**

An authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.

The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token.

After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Steps involved : figure below:



* * * * * * * * * * * * * * * *

Student ID: .....

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.