1. Describe SQL injection attack and the threats it makes on web applications? (10 marks)
    1.1. Show one of the SQL injection preventing mechanisms using suitable programming language or a pseudo code. (10 marks)
    1.2. Discuss importance of frontend and backend input validations in web applications. (5 marks)

2. You are an IT security officer in XYZ Company. One day your boss asking your recommendation for enabling a feature in a web application as unregistered users can share an article with other users /friends using email service running on web server.
    2.1. What are the risk associates with this implementation? (5 Marks)
    2.2. If you are going to implement this, what are the boundary conditions that you can identify? (5 marks)
    2.3. Web developers in your organization make an argument with you as if the network perimeter security (Firewalls, Intrusion Detection System, Antivirus software, Anti spam gateways, etc) is adequate, no need to think about the application security attack vectors. Are you agree with this? Please elaborate. You can use suitable image to make your answer more clear. (10 marks)
    2.4. What is the objective of enhancing security through obscurity techniques? (2 marks)
    2.5. Does it really effective? (3 marks)

3. "Don't trust anyone until they can prove to you that they can be trusted". This is one of the popular phrases in information security and business world.
    3.1. How this statement is relevant to secure application development. Brief technical description required considering the risk factors. (5 marks)
    3.2. Write a program or pseudo code to validate address field using regular expression. Address field can contain alphanumeric characters, spaces, dots (.), minus (-), underscore (_) and slashes (/). The length must be minimum 3 characters and maximum 50 characters. (15 marks)
    3.3. What is the different between lazy and greedy modifiers in regular expression? (5 marks)

4. Please answer these direct questions.
    4.1. What is symmetric key crypto system? (2 marks)
    4.2. What is asymmetric key crypto system? (2 marks)
    4.3. What is Cipher and key ?(2 msarks)
    4.4. What is the major difference between MD5 algorithm and 3DES algorithm? (4 marks)
    4.5. What is mean by dictionary attack? (2 marks)
    4.6. What is the use of HASH algorithms in your applications to validate username and password? Suitable diagrams may useful. (6 marks)
    4.7. Write down three categories of authentication mechanisms and relevant examples. (6 marks)
    4.8. What is the use of CAPTCHA doce in web applications? (1 mark)

Answers

1. Describe SQL injection attack and the threats it makes on web applications? (10 marks)
   - Student can describe this by their own way. (using examples or wordings)
   - IT may contain following or more
     - One of injection attacks like Code injection, email injection, command injection, etc.
     - Attackers can exploit week vulnerability in input validation for execute arbitrary SQL codes against the application database.
     - This technique tricks the sql engine to run attacker queries pass through the application input field.
     - Ex : This is a great guestbook); drop table USERS; **Object manipulations** (Describe)
     - Ex : ' or '1'='1'; **Authentication bypass** (Describe)

   1.1. Show one of the SQL injection preventing mechanisms using suitable programming language or a pseudo code. (10 marks)

```
if( isset($_POST['comment']) && strlen($_POST['comment']) > 0)
      echo storeComment(htmlentities($_POST['comment']));
else
   error ($error_message);
```

   Or similar answers. Students can write examples using regular expressions.

   1.2. Discuss importance of frontend and backend input validations in web applications. (5 marks)

   Attackers can disable or by pass front end validations using various techniques. Using Backend input validation mechanisms application can validate inputs if attackers able to bypass the front end validations.

   Front end validations useful to quickly respond to users and reduce server calls.

2. You are an IT security officer in XYZ Company. One day your boss asking your recommendation for enabling a feature in a web application as unregistered users can share an article with other users /friends using email service running on web server.

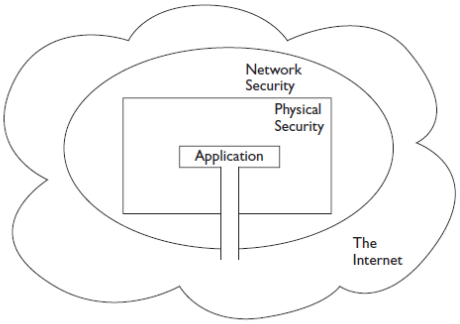
   2.1. What are the risk associates with this implementation? (Two correct answers - 5 Marks)
   - Attackers may try to send spam emails
   - Attackers can read unencrypted emails
   - Conflict of interest between sender and receiver
   - Mail server may blacklisted due to sending spam emails
   - Attacker may run automated scripts to send emails
   - Attackers may attached malicious attachments
   - Attackers may provide misleading instructions through emails
   - This service may down due to various reasons. (DOS attack, Technical fault, Email sevice subscription, etc)

- Etc,

2.2. If you are going to implement this, what are the boundary conditions that you can identify? (Two correct answers - 5 marks)

- Lengthy email addresses
- Blank/ fake recipient addresses
- Multiple email address at a time
- Negative user comments
- Malicious attachments
- Email injection
- Spam mails
- Cross site scripting
- Receivers may Acknowledgements and reply
- Etc,

2.3. Web developers in your organization make an argument with you as if the network perimeter security (Firewalls, Intrusion Detection System, Antivirus software, Anti spam gateways, etc) is adequate, no need to think about the application security attack vectors. Are you agree with this? Please elaborate. You can use suitable image to make your answer more clear. (10 marks)



If a web application has a weakness, attackers can bypass all security controls. So this argument is false.

(Students can obtain full marks for similar answers and diagrams)

2.4. What is the objective of enhancing security through obscurity techniques? (2 marks)

Confusing hackers

2.5. Does it really effective? (3 marks)

This is really doesn't work.

This strategy does make your code difficult to maintain and update, but that's about it.

3. “Don’t trust anyone until they can prove to you that they can be trusted”. This is one of the popular phrases in information security and business world.

3.1. How this statement is relevant to secure application development. Brief technical description required considering the risk factors. (5 marks)

Answer must describe use of a **User Authentication** mechanism in a web application. Similar answers can have full marks.

There are two primary goals for any user authentication scheme:

To ensure that users actually are who they say they are (or are actual humans rather than automated scripts)

To ensure that users have the ability to access the resources they are entitled to and are denied access to resources for which they do not have sufficient privileges

3.2. Write a program or pseudo code to validate address field using regular expression. Address field can contain alphanumeric characters, spaces, dots (.), minus (-), underscore (_) and slashes (/). The length must be minimum 3 characters and maximum 50 characters. (15 marks)

```
function check_comment($tainted_comment) {
  $pattern = '^[\w\s.-_/]$';
  if (preg_match($pattern, $tainted_comment) != 0) {
    return $tainted_comment;
  } else {
    return FALSE;
  }
}
```

Patterns = **'^[a-zA-Z0-9\s.-_/]$'**; , **'^[\w\s.-_/]$'**;

Full marks can be given for similar patterns and codes.

Name of the faction “**preg_match”** is not required but pattern marching mechanism should be specified in pseudo level.

10 marks can be given for correct pattern.

Students who try to wrote this pseudo code and if it has a checking condition can obtain 5 marks maximum.

3.3. What is the different between lazy and greedy modifiers in regular expression? (5 marks)

- Greedy modifiers continue to match the patterns up to end of the string “/n”. Then it will backtrack to the last point that matches found.

- Lazy modifies works exactly opposite was as greedy modifiers.
- They stop as soon as they reach a matching section of the string.

Students can earn marks for other correct comparisons end examples (Please see the information given bellow).

- *Greedy Modifiers*
    - if our pattern is <.+>
    - our test string is $string = "<abc>DEF</abc>def“
    - Expect to match : First substring with in the angle brackets (**<abc>**DEF</abc>def).
    - How this RegX engine works.
        - it will continue to try to match the rest of the string, until matching causes the entire string to fail. (/n)
        - where it can no longer match, it will backtrack to the last point in by removing character by character in the string that successfully matched. (>)
        - This is how the engine will process our example string.
        - What would be the matching string ? (**<abc>**DEF</abc>def)
        - The most common greedy modifiers are the plus (+), star (*), and curly brackets ({ }).

- *Lazy Modifiers*
    - Lazy modifiers work in exactly the opposite way as greedy ones.
    - They stop as soon as they reach a matching section of the string.
    - To make our example pattern lazy rather than greedy, we'll add a ?
        - Our pattern is <.+?>
        - Now .+ combination will attempt to match as few times as possible
        - Finally, the pattern reaches a character that matches > and the engine returns the match: <abc>DEF</abc>def

4. Please answer these direct questions. (Similar answers can obtain full marks)

4.1. What is symmetric key crypto system? (2 marks)

If a crypto system uses one key for encryption and decryption, this crypto system call symmetric key crypto system.

4.2. What is asymmetric key crypto system? (2 marks)

If a crypto system uses one key for encrypt and other key for decrypt, , this crypto system call asymmetric key crypto system.

4.3. What is Cipher and key ?(2 msarks)

Cipher – The Encrypted code of an input produced by the encryption algorithm.

Key - The special knowledge you must have to read the encrypted data.

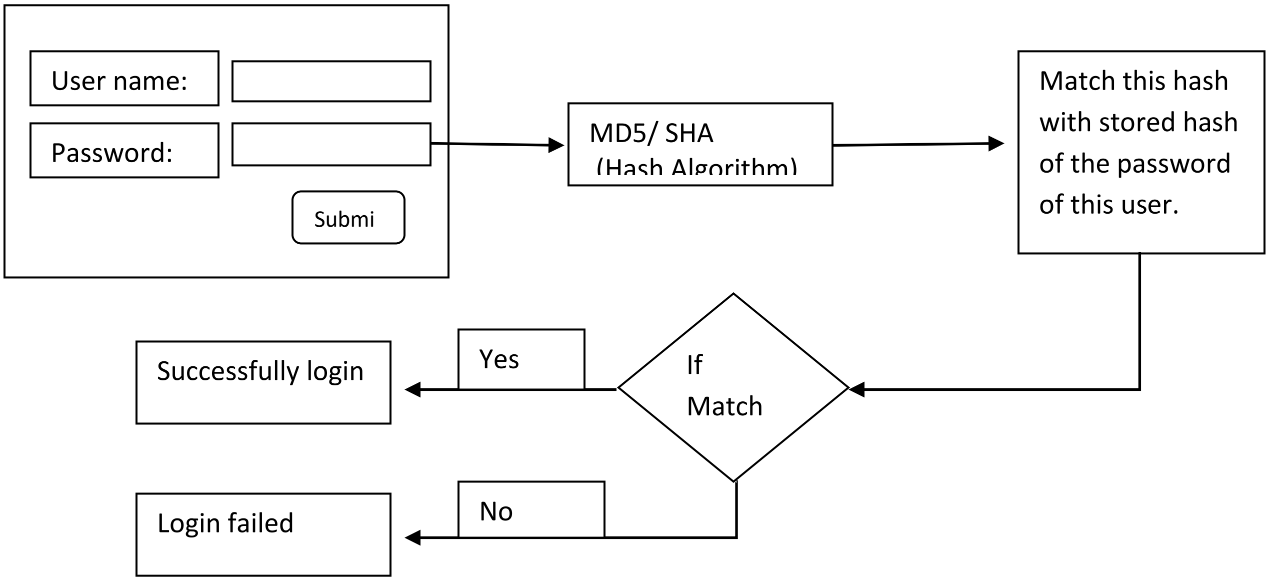
4.4. What is the major difference between MD5 algorithm and 3DES algorithm? (4 marks)

MD5 is one way encryption algorithm. Decryption of the MD5 cipher text is technically infeasible. 3DES algorithm can encrypt plaintext and decrypt cipher text using a key.

4.5. What is mean by dictionary attack? (2 marks)

This is a cipher or password defeating technique which is trying likely possibilities of words in dictionary.

4.6. What is the use of HASH algorithms in your applications to validate username and password? Suitable diagrams may useful. (6 marks)



4.7. Write down three categories of authentication mechanisms and relevant examples. (6 marks)

What you know: Username and password

What you have: security badges, swipe cards, and VPN tokens

What you are: biometric analysis – Figure print, Eye Retina

4.8. What is the use of CAPTCHA code in web applications? (1 mark)
Determine whether or not the user is human.