Birla Institute of Technology & Science, Pilani
Work Integrated Learning Programmes Division
First Semester 2021-2022

Assignment

Course No.	: **BITS SS ZG570**
Course Title	: **Cloud , IoT & Enterprise Security**
Nature	**: Open Book**
Weightage	: **20%**
Start Date	: **20th Oct, 2021**
End Date	: **30th Oct, 2021**

Note to Students:

1. Pl. upload your Assignment as Single PDF File and rename it with your BITS ID Number using TAXILA

Q.1 What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack? What steps should be taken when a DoS attack is detected? What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others? **[2 Marks]**

Q.2 Rajesh wants to send a message X (assumed to be an integer mod N) to Ramesh , he computes the value $E(x) \equiv XE$ (mod N) and sends this to Ramesh. At the reception side of the message, the value $y = E(x)$, Ramesh computes $D(y) \equiv yd$ (mod N); this will be equal to the original message x. where E and D are functions to encode and decode.

a) What type of Algorithm can be designed with the above conditions? Justify it

Let p and q be two large primes 512 bits each, and let $N = pq$. We will think of messages to Ramesh as numbers modulo N, excluding the trivial values 0 and 1. Also, let e be any number that is relatively prime to $(p-1)(q-1)$. Then if Ramesh public key is the pair of numbers (N, e) .

b) What is the private key of Ramesh?

c) Also what is the Algorithmic Complexity of the above considering the exponential computations of Rajesh and Ramesh.

[5 Marks]

Q.3. Define Attack Surface Analysis?. What are the entry and exit points for the below Scenario in an Enterprise like Amazon to map the Attack Surface with the following Conditions :

1. Different types of users with different roles and privileges can access the system
2. Complexity increases with the number and types of users.
3. Need to Check for unauthenticated, anonymous users and highly privileged admin users.
4. Group type of attack point into buckets based on risk purpose, implementation, design and technology.
5. Count the number of attack points of each type, then choose some cases for each type, and focus your review/assessment on those cases.
6. Understand every endpoint in order to understand the Attack Surface and the potential risk profile of a system.
7. Count the different general type of endpoints and the number of points of each type.
8. Budget what it will take to assess risk at scale, when the risk profile of an application has significantly changed.

[3 Marks]

3. Check the following code for SQLi ? Modify if necessary? What is the output this code? Explain with reasons.

[5 Marks]

****

```
    String query = "select * from employee where employee_name = ?";
  List<String> employees = new ArrayList<>();
  try (pStatement = con.pStatement(query)) {
    pStatement.setString(1, "rajesh");
    try (ResultSet rSet = pStatement.executeQuery()) {
      while (rSet.next()) {
        employees.add(rSet.getString(1));
      }
    }
  }
  Assert.assertEquals(1, employees.size());
  Assert.assertTrue(employees.contains("rajesh"));

  query = "insert into employee(employee_name, ramesh, madhav, vishnu) values(?, ?, ?, ?)";
  int insertedRecordCount;
  try (pStatement = con.pStatement(query)) {
    pStatement.setString(1, "ravi");
    pStatement.setInt(2, 239);
    pStatement.setInt(3, 125);
    pStatement.setInt(4, 11);
    insertedRecordCount = pStatement.executeUpdate();
  }
  Assert.assertEquals(1, insertedRecordCount);
```

```
    query = "update employee set blue = ? where employee_name = ?";
    int updatedRecordCount;
    try (pStatement = con.pStatement(query)) {
        pStatement.setInt(1, 10);
        pStatement.setString(2, "orange");
        updatedRecordCount = pStatement.executeUpdate();
    }
    Assert.assertEquals(1, updatedRecordCount);




    query = "delete from employee where employee_name = ?";
    int deletedRecordCount;
    try (pStatement = con.pStatement(query)) {
        pStatement.setString(1, "ravi");
        deletedRecordCount = pStatement.executeUpdate();
    }
    Assert.assertEquals(1, deletedRecordCount);

}
```

[3 Marks]

4. Check the following attack inputs w.r.t URL and SQL ? Modify if necessary? What is the output this code? Explain with reasons.

```
PreparedString div = new PreparedString( "<a href=\"http:\\\\example.com?id=?\"
onmouseover=\"alert('?')\">test</a>", new HTMLEntityCodec() );

div.setURL( 1, request.getParameter( "url" ), new PercentCodec() );
 div.set( 2, request.getParameter( "message" ), new JavaScriptCodec() );
            out.println( div.toString() );

 PreparedString query = new PreparedString(

"SELECT * FROM users WHERE name='?' AND password='?'", new OracleCodec() );
           query.set( 1, request.getParameter( "name" ) );
            query.set( 2, request.getParameter( "pass" ) );
           stmt.execute( query.toString() );
```

[2 Marks]

5. Explain the following Security Attacks with proper examples :

a) Worm
b) Virus
c) Bots
d) DDoS
e) XSS

[2 Marks]

6.

The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D(P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

```
Program CV :=
{. ..
        main-program :=
                {if D(CV) then goto next:
                else infect-executable;
                        }
                        next:
}
```

In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus**.** **[3 Marks]**

******************** ALL THE BEST *****************