***1 (A)***



Google hacking is the term used when a hacker tries to find  
vulnerable targets or sensitive data by using the Google search  
engine.

Operators are used to refining the results and maximize the search value. They are your tools as well as hackers’ weapons.

Google can search many different types of files, including PDF and Microsoft Office documents. In this example we will search for confidential files in web pages:

"not for distribution" confidential,

Finds Login Pages of CentOS,

inurl:/login/index.php intitle:CentOS

Microsoft Excel spreadsheets containing the words username, password, and email.:

filetype:xls username password email

Access SAP Crystal report, crystal reports help analyse data by creating richly formatted reports. These reports can be a major

Inurl: apspassword

***(B)***



**Authentic Process**

Fundamental building block and primary line of defence. The basis for access control and user accountability.  
Identification presents an identifier to the security system. Verification is the presenting or generating of authentication information that corroborates the binding between the entity and the identifier.

Authenticating user identity through 4 functions.

1. Something the individual knows: password, pin, prearranged questions.
2. Something the individual possesses (token): smartcard, physical key, electronic key card
3. Static Biometrics: fingerprint, retina, face

Dynamic biometrics: voice pattern, handwriting, typing rhythm

**Password Authentication:**

Widely used line of defence against intruders  
• User provides name/login and password  
• System compares password with the one stored for that specified login

The user ID:  
• Determines that the user is authorized to access the system  
• Determines the user’s privileges  
• Is used in discretionary access control

Offline dictionary attack

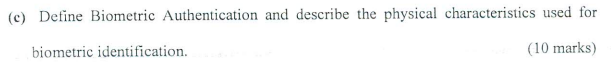
Popular password attack

Password guessing against single user

Workstation Hijacking

Exploiting user mistakes

***(C)***



***Biometric Authentication***

Attempts to authenticate an individual based on unique physical  
characteristics  
• Based on pattern recognition  
• Is technically complex and expensive when compared to passwords and  
tokens  
• Physical characteristics used include:  
o Facial characteristics  
o Fingerprints  
o Hand geometry  
o Retinal pattern  
o Iris  
o Signature  
o Voice

Diagram

Description automatically generated

Diagram

Description automatically generated

***2 (A)***

******

Text, application, email

Description automatically generated

Table

Description automatically generated

***(B)***



DAC

Discretionary access control (DAC)  
• Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

Table

Description automatically generated

Diagram

Description automatically generated

***(C)***



Prepared Statements: pre-compiled SQL commands created inside a program that can be used many times over the course of the application’s lifecycle. By default, PS input parameters are bound. Bound parameters are treated as plain text values, which prevents any command alteration during an SQL injection attack.

Least Privilege: A program requires user credentials to run SQL commands, such as insert, update, search, delete, and drop, to communicate with a database. he program user should only have the required database privileges. Additional privileges should be granted on an as-needed basis. With minimal database privileges, the potential damage of an SQL injection attack is reduced.

Input Validation: Suspicious inputs are filtered prior to submission or processing by the server when validated. An example of input validation is an email validator. Passing an SQL injection query would not work, since the input field only accepts a valid email address based on a regular expression

Diagram

Description automatically generated