Chapter-6

Date ______
Page ______

Software Security

6.5# SQL Injection

→ SQL Injection is a type of web application security vulnerasability in which an attacker is able to submit database ~~to~~ SQL command that is executed by web application, exposing the back-end database.

→ A SQL injection attack can ~~occur~~ occur when a web application utilizes the ~~input~~ user-supplied data without proper validation or encoding as part of the command or query.

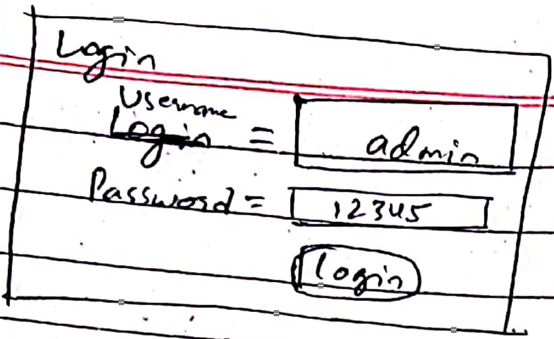
→ SQL injection allows an attacker to create, read, alter or modify or update and delete data stored in ~~back~~ back-end database.

→ SQL injection, attack can give access to sensitive information such as:- credit card number, social security number or other finincial ~~details~~ data.

→ How SQL injection works?

① In order to run malicious SQL queries against a DB server, the attacker must find the ~~input~~ input within a web application that is included inside of a SQL query.

② ~~To~~ An attacker can include payload that will be included as part of the SQL query and run against the DB server.



Login

~~Login~~ Username = admin

Password = 12345

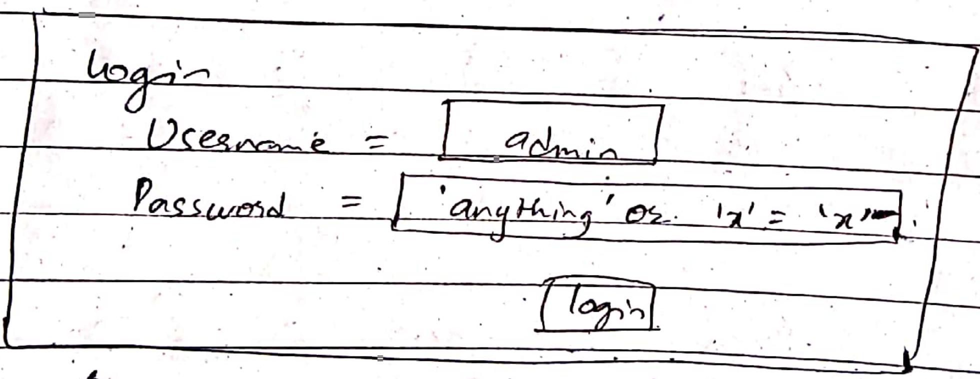
login

Query :

Select ~~all~~ * from login where
username = "admin", and
Password = "12345"

O/P →	Username	Password
	admin	12345

SQL injection :



login

Username = admin

Password = 'anything' or 'x' = 'x'

login

Query with ~~payload~~/ SQL injection :

Select * from login where
username = " admin" and
password = ~~"~~ 'anything' or 'x' = 'x'

O/P →	Username	Password
	admin	12345
	admin1	abc123
	admin123	a12131

→ Prevention of SQL injection :-

(a) Adopting an ~~validation~~ input validation technique in which user input is authenticated against a set of define rules for length, type, syntax etc.

(b) Ensuring that users with the permission to access the database have least prilviliges (rights).

(c) Removing all the stored procedure ~~stored~~ that are not in use.

(d) Use strongly typed parameterized query APIs with the placeholder ~~Sub~~ substitution makers.

(e) Show case ~~&~~ when using ~~the~~ stored procedures since they are generally safe from injection.

6.1 # Basic attacks :-

→

Software Security :-

→ Software security is an idea implemented to protect the software from ~~no~~ malicious attack and other hacker risks.

6.1# Basic attacks :-

→ Some common basic software attacks are as follows :-

1. Buffer overflow
2. Stack overflow
3. Command injection
4. SQL injection

① Buffer and Stack overflow:-

→ They overwites the contents of the ~~head~~ heap or stack respectively by writing extra bytes.

② Command injection:

→ Command injection can be found on software code when system commands are used mostly.

→ New system commands are append to the existing Commands by malicious attack.

6.2 # State-based attacks:-

→ State is the ability to remember information as a users travels from ~~pate~~ page to page within a site.

→ Web is stateless in a sense that it doesnot remember which ~~a~~ page a user viewing or in which orde a pages may be viewed.

→ A User is always free to ~~close~~ click the Back button or force reload the page.

→ So, web developers ~~are~~ must take code state information themselves So they can ~~to~~ ~~infor~~ enforces rules about page access and session management.

{ Pg - 97 ~~ead~~ EAPd_NOTE(1)-pdf }

64 # Cross-site scriptings :- (XSS)

→ ~~It~~ XSS allows attacker or hackers to inject malicious ~~Code~~ client-side scripts into web pages.

→ How XSS occurs? :-

→ An attacker can use XSS to send a malicious scripts to an unsuspecting user.

→ The end user's browser has no way of knowing that the script should not be trusted, and will be executed.

→ Because it thinks that the script came from a trusted source. and the malicious scripts can access all the cookies, session tokens, or other sensitive information.

→ These scripts can even rewrite the content of HTML page.

→ Prevention are :-

① Use Web Application Firewall (WAF).

② Configure or set the rules of WAF to prevent ~~XSS~~ XSS.

→ ~~&~~ There are two types of XSS attacks. They are:-

① Stored XSS Attack

② Reflected XSS Attack

① Stored XSS Attack :- (Type-I XSS or Presistent XSS)

→ Stored XSS attacks are those where the injected scripts are permanently stored in the ~~se~~ targeted server such as database, comments field, etc.

→ The victim retrives the malicious scripts from the server when it requests the stored information.

② Reflected XSS Attacks:

→ Reflected & attacks are ~~thoe~~ those where the infected script is reflected off the web server, Such as in the ~~form of~~ error message, search ~~result~~ result, etc.

→ Reflected attacks are delivered via another ~~Em~~ route such as email, or some other ~~sites~~ web site.

~~③~~