RAMA UNIVERSITY

www.ramauniversity.ac.in

MOBILE SECURITY

FACULTY OF EGINEERING & TECHNOLOGY

LECTURE -18

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

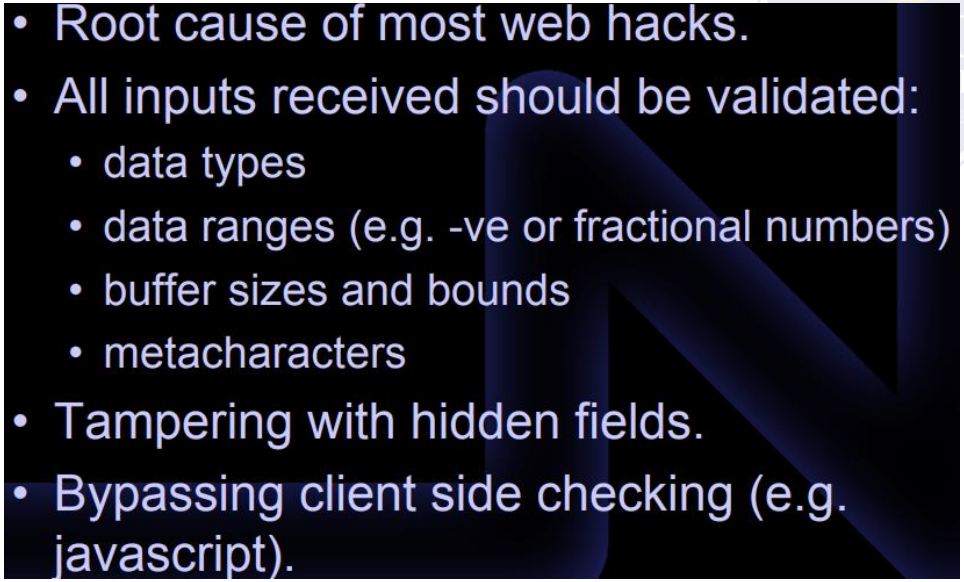
OUTLINE

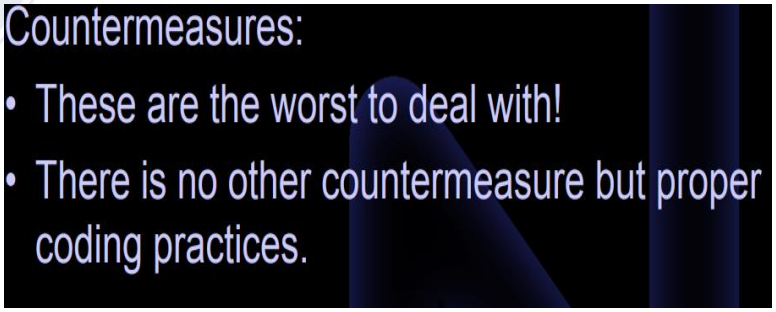
- Web Application Attack
- Input Validation attacks
- What is SQL injection (SQLi)?
- What is the impact of a successful SQL injection attack?
- MCQ
- References

INPUT VALIDATION ATTACK

Input Validation attacks

❑An input validation attack is any malicious action against a computer system that involves manually entering strange information into a normal user input field. Input validation attacks take place when an attacker purposefully enters information into a system or application with the intentions to break the system's functionality.





INPUT VALIDATION ATTACK

Types of input validation attacks

Buffer overflow-

❑This is a type of attack that sends too much information for a system to process, causing a computer or network to stop responding. A buffer overflow might also cause excess information to take up memory that was not intended for it, sometimes even overwriting memory.

Canonicalization attacks-

❑A canonicalization attack takes place when someone changes a file directory path that has digital permissions to access parts of a computer in order to allow access to malicious parties that use this unauthorized entry to steal sensitive information or make unapproved changes.

XSS attacks-

❑Also called cross-site scripting, these attacks involve placing a malicious link in an innocuous place, like a forum, which contains most of a valid URL with a dangerous script embedded. An unsuspecting visitor might trust the site they are on and not worry that a comment or entry on the site contains a virus

INPUT VALIDATION ATTACK

Types of input validation attacks

SQL injection attacks-

❑SQL injection attacks involve taking a public URL and adding SQL code to the end to try to gain access to sensitive information. An attacker might enter code into a field commanding a computer to do something like copy all of the contents of a database to the hacker, authenticate malicious information, reveal hidden entries in a database or delete information without consent.

WHAT IS SQL INJECTION (SQLI)?

What is SQL injection (SQLi)?

SQL injection attacks-

❑SQL injection attacks involve taking a public URL and adding SQL code to the end to try to gain access to sensitive information. An attacker might enter code into a field commanding a computer to do something like copy all of the contents of a database to the hacker, authenticate malicious information, reveal hidden entries in a database or delete information without consent.

- ❑ SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

❑In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

WHAT IS SQL INJECTION (SQLI)?

What is SQL injection (SQLi)?

Parameters from the URL or input fields get used in SQL queries.

An instance of Input Validation attacks.

Data can be altered to extend the SQL query.

- e.g. http://server/query.asp?item=3+OR+1=1

Execution of stored procedures.

May even lead to back-end database server compromise.

Countermeasures:

- Again, no easy fix.
- Thorough source code review.
- Following the principle of least privilege for the database application.
- Elimination of unnecessary database users and stored procedures.

WHAT IS SQL INJECTION (SQLI)?

What is the impact of a successful SQL injection attack?

SQL injection attacks-

❑A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

SQL injection examples

❑There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

- ❑Retrieving hidden data, where you can modify an SQL query to return additional results.
- ❑Subverting application logic, where you can change a query to interfere with the application's logic.
- ❑UNION attacks, where you can retrieve data from different database tables.
- ❑Examining the database, where you can extract information about the version and structure of the database.
- ❑Blind SQL injection, where the results of a query you control are not returned in the application's responses.

MCQ

11. ACL stands for _____

a) Access Condition List

b) Anti-Control List

c) Access Control Logs

d) Access Control List

12. When a packet does not fulfil the ACL criteria, the packet is _____

a) resend

b) dropped

c) destroyed

d) acknowledged as received

13. Network administrators can create their own ACL rules based on _____ _____ and _____

a) Address, Protocols and Packet attributes

b) Address, Protocols and security policies

c) Address, policies and Packet attributes

d) Network topology, Protocols and data packets

14. One advantage of Packet Filtering firewall is _____

a) more efficient

b) less complex

c) less costly

d) very fast

15. Packet filtering firewalls work effectively in _____ networks.

a) very simple

b) smaller

c) large

d) very large complex

REFERENCES

- https://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf
- https://whatis.techtarget.com/definition/input-validation-attack