CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

UNIVERSITY INSTITUTE OF COMPUTING

Bachelor of Computer Application

Subject Name: Web Security

Code : CAT-309

INJECTION ATTACKS

DISCOVER . LEARN . EMPOWER

Injection Attacks

Course Outcome

CO Number	Title	Level
CO1	Students will learn injection Attack.	Understand
CO2	Learn about security services.	Understand

- Sql Injection
- Sql Injection Impact
- Phising
- File Upload

Injection Attack

Injection attacks allude to a wide class of assault vectors. In an infusion assault, an assailant supplies unfrosted contribution to a program. This info gets handled by a mediator as a major aspect of an order or inquiry. Thus, this adjusts the execution of that program.

- SQL Injection Attack
- XSS Attack
- Email Attack

SQL Injection

- Each web application utilizes a database to store data
- SQL is utilized to mange data in the database
- Client provided information is consolidated into SQL explanation
- SQL infusion assault comprises of addition or "infusion" of a SQL question through the information from the customer to the application. This changes the execution conduct of the backend inquiry and enables an assailant to execute unapproved SQL directions.

SQL Injection Example

- Books index – enables a client to look for a book by writer name https://example.com/error.php?authorname=James
- The backend inquiry to recover the books subtleties is SELECT title, year FROM books WHERE writer = 'James'
- Result : Web webpage shows the rundown of books composed by James

SQL Injection Impact

- Adjust the database – Add new tables, erase existing tables, and so forth…
- Bargain client accounts by acquiring their passwords Collects delicate information like charge card numbers, SSN, and so forth…
- Can get to the records on the server
- Cause Denial of administration by ceasing the database

SQL Injection Remedy

Approve Input

- Info information contains just a specific rundown
- Perform server side approval

Parameterized questions (show tests)

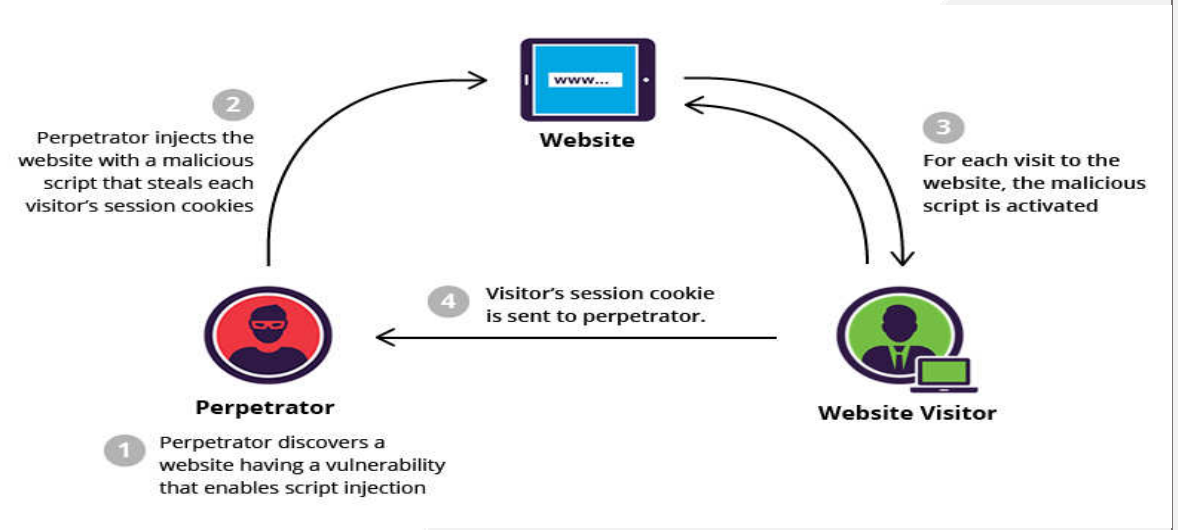
- Otherwise called arranged proclamations ,Define all the SQL explanations first and after that pass parameters
- Attacker can not change the purpose of the inquiry put away methodology additionally works

Store passwords in salted hash design

- Associate with the database with Low advantaged client

SQL Injection Remedy

Cross-Site scripting (XSS) is a kind of infusion security assault in which an assailant infuses information, for example, a vindictive content, into substance from generally confided in sites. Cross-webpage scripting assaults happen when an untreated source is permitted to infuse its very own code into a web application.


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Reference:
https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/csrf-cross-site-request-forgery.png

How cross-site scripting works

- Like all injection attacks, XSS takes advantage of the fact that browsers can't tell valid markup from attacker-controlled markup -- they just execute whatever markup text they receive.
- The Same Origin Policy requires that all content on a webpage come from the same source. When the Same Origin Policy isn't enforced, an attacker is able to inject a script and modify the webpage to suit their own purposes -- for example, to extract data that will allow the attacker to impersonate an authenticated user, or to input malicious code for the browser to execute.
- XSS can be used in a number of ways to cause serious problems. The traditional use of XSS enables an attacker to steal session cookies, allowing that attacker to pretend to be the user (victim). But it's not just stealing cookies; attackers can use XSS to spread malware, deface websites, create havoc on social networks, phish for credentials and in conjunction with social engineering techniques.

XSS IMPACTS

- Burglary of Accounts/Services
- Client Tracking/Statistics
- Program/User misuse
- Credentialed Misinformation

Finding and Exploiting XSS Vulnerabilities

- An essential way to deal with distinguishing XSS vulnerabilities is to utilize a standard verification of-idea assault string, for example, the accompanying:

  "><script>alert(document.cookie)</script>

- This string is submitted as each parameter to each page of the application, and reactions are checked for the presence of this equivalent string. In the event that cases are discovered where the assault string seems unmodified inside the reaction, at that point the application is more likely than not powerless against XSS.
- Model

  Assume that the returned page contains the accompanying:

  <input type="text" name="address1" value="myxsstestdmqlwp">

Email Injection

- Email infusion is a kind of infusion assault that hits the PHP worked in mail work.
- It enables the noxious assailant to infuse any of the mail header fields like, BCC , CC, Subject, and so forth., which enables the programmer to convey spam from their unfortunate casualties' mail server through their exploited people's contact structure.
- It can conceivably influence any application that sends email messages dependent on contribution from discretionary clients.
- The principle reason of this assault is inappropriate client input approval or that there is no approval and filtration by any stretch of the imagination.

Working of Email Injection

- **Inject Cc and Bcc after sender argument.**

From:sender@domain.com%0ACc:recipient@domain.co,%0ABcc:recipient1@domain.com

So now, the message will be sent to the recipient and recipient1 accounts.

- **Inject To argument**

From:sender@domain.com%0ATo:attacker@domain.com

Now the message will be sent to the original recipient and the attacker account.

- **Inject Subject argument**

From:sender@domain.com%0ASubject:This's%20Fake%20Subject

The fake subject will be added to the original subject and in some cases will replace it. It depends on the mail service behavior.

Working of Email Injection

- **Change the body of the message**

  Inject a two-line feed, then write your message to change the body of the message.

  From:sender@domain.com%0A%0AMy%20New%20%0Fake%20Message.

  The fake message will be added to the original message.

Assessment Pattern

• Element 1(Quiz)	12 marks
• Element 2 (Surprise Test)	09 Marks
• Element 3 (Assignments)	12 Marks
• Element 4 (Tutorial/Presentations)	09 Marks

Applications

- Online Banking
- Protect client database
- Protect Server database
- Online payments

References

Reference Books:

- Web Security by Oscar MeridaPublisher: php[architect]
- DafyddStuttard, “The Web Application Hacker’s Handbook”, Wiley India Pvt. Ltd.

Reference websites:

- https://www.geeksforgeeks.org/types-of-security-attacks-active-and-passive-attacks/
- https://en.wikipedia.org/wiki/ASP.NET
- http://theory.stanford.edu/people/jcm/papers/sameorigin.pdf
- https://searchsecurity.techtarget.com/definition/authentication
- https://skorks.com/2009/08/different-types-of-encoding-schemes-a-primer/

THANK YOU

For queries
Email: manpreetkaur.uic@cumail.in