Welcome to the CoGrammar

SQL Injections

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: **Questions**

Cyber Security Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: www.hyperiondev.com/support

- We would love your **feedback** on lectures: Feedback on Lectures

- Find all the lecture **content** in you Lecture Backpack on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Security Tip

"Enable login alerts for all your online accounts."

Why?
Login alerts notify you immediately if your account is accessed from an unrecognized device or location. This early warning system allows you to take quick action—such as changing your password or enabling multi-factor authentication (MFA)—to secure your account before further damage is done.

How to Enable:

- Check your account security settings for an option like "Login Alerts" or "Account Activity Notifications."
- Ensure the alerts are sent to a secure email or phone number that only you can access.

Stay proactive and keep hackers out by staying informed!

SKILLS FOR LIFE

SKILLS BOOTCAMPS

Department for Education

CoGrammar

SQL injections

December 2024

Learning Objectives & Outcomes

- Define SQL Injection and identify its characteristics and common areas of vulnerability.
- Explain how SQL Injection exploits weaknesses in input validation and query structure, leading to unauthorized database access.
- Demonstrate how to write secure SQL queries using parameterized queries or prepared statements to prevent injection attacks.
- Examine a given SQL query or application code snippet to identify potential vulnerabilities to SQL Injection attacks.
- Assess the effectiveness of various SQL Injection prevention techniques, such as input validation, stored procedures, and the use of ORMs (Object-Relational Mapping).

Polls

Please have a look at the poll notification and select an option.

How familiar are you with SQL Injection vulnerabilities?

- Not at all
- Slightly familiar
- Moderately familiar
- Very familiar
- Expert

Polls

Please have a look at the poll notification and select an option.

What do you think is the primary reason for SQL Injection vulnerabilities?

- Lack of input validation
- Weak database permissions
- Insecure coding practices
- I don't know

Introduction SQL Injection

- **Definition:** SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
- **Key Threat:** Exploiting input fields to execute arbitrary SQL code

How SQL injection works

- User input: Applications often accept user input (e.g, login forms, search bars).
- Malicious payload: Attackers inject malicious SQL instead of normal input.
- Execution: If the input is not properly validated or sanitized, the database executes the attacker’s SQL commands.

Types of SQL injection

- Classic SQL injection:
  - Direct manipulation of SQL queries
- Blind SQL injection:
  - No error messages; relies on observing application behaviour.
- Boolean-Based SQL:
  - Exploits true/false condition
- Time Based SQL:
  - Leverages database time delays to infer information
- Out of Band SQL:
  - Uses alternate channels (e.g DNS) for data exfiltration.

Common Vulnerability areas

- User Authentication Forms (e.g., login pages)
- Search Bars (e.g., product searches)
- URL Parameters (e.g., ID fields)
- Cookies (if passed as SQL parameters)
- Hidden Form Fields

SQL Injection impact

- Data leakage or theft
- Unauthorized access
- Data modification or deletion
- Potential full database compromise

Mitigation Strategies

- **Input Validation:** Reject unexpected inputs.
- **Stored Procedures:** Encapsulate SQL logic in the database.
- **Escaping User Inputs:** Use library functions to escape dangerous characters.
- **Use ORM Frameworks:** e.g., Hibernate, Entity Framework
- Implement Web Application Firewalls (WAF).

Practical Example

- We’re going to perform a SQL injection attack on a simple web server built with Python(Flask) and SQLite as our database.

Polls

Please have a look at the poll notification and select an option.

What is the most effective method to prevent SQL Injection attacks?

- Input validation
- Parameterized queries
- Encrypting the database
- Firewalls

CoGrammar

Polls

Please have a look at the poll notification and select an option.

Which aspect of this lecture did you find most helpful?

- Understanding the concept of SQL Injection
- Learning about common attack techniques
- Implementing secure coding practices
- Examples and demonstrations

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar