CM3106 - Code Injection Attacks

Part 1: Implementing Code Injection attacks and Defences

To complete this Lab, an instance of SQL Server and SSMS should be installed on your desktop. Unfortunately, due to the current outbreak of CONVID-19, you cannot access your VM in N523 as usual.

Code injection allows unauthorized changes to your SQL Server instance via back doors. Attackers can use EXECUTE AS statement to implement such attacks. Policy-based management can be used as a technical tool to prevent code injection attacks by not allowing the use of the EXECUTE AS clause in stored procedure. Under certain circumstances, the code signing can also be used as an alternative to the EXECUTE AS clause to launch similar attacks. In this exercise, we will implement some of these techniques in using the WideWorldImporters database.

1. Open the SQL Server Management Studio (SSMS) tool on your PC and enter the SQL Server connection details. Use the type "Windows authentication". You are now connected to SQL Server.

----

2. Creates a stored procedure, called ‘dbo.CodeInjDemo’ to return the security context of the current user.

3. Edit the above stored procedure to run it as a privileged user in your instance.

4. Run the below script and notice the different security contexts are returned.

```
SELECT USER_NAME(), SUSER_SNAME(), ORIGINAL_LOGIN() ;
EXEC dbo.CodeInjDemo ;
```

5. Now you can use EXECUTE AS to perform a code injection attack. To this end, an attacker can use the EXECUTE AS to run a parametrised stored procedure, which will create a privileged user account with following properties. If the value 1 is passed to the procedure, a login with administrator rights is created. If the value 0 is passed to the procedure, the login is deleted before it is noticed by the DBA.

6. Use the code obfuscation method to reduce the likelihood that a DBA will recognize what is happening above. Can you view the contents of the stored procedure?

7. Implement a simple policy-based management (PBM) check to protect your Database from the above attack. To this end. You may need to create a condition first and then a policy.

8. To avoid using Execute As in stored procedures, attacker can use the code signature technique. Implement above attack using code signing method. For this purpose you may have to sign the stored procedure with a certificate as described in the lecture.

Part 2: Database Security Best Practices

Due to the outbreak of Covid 19, practical and written exams that were planned before Covid 19 could be replaced by coursework that may require individual research for articles to perform some of the given tasks in the coursework. Therefore, this part of the Lab today will be an active learning session, in which you will work together as a small group (2-3 people) on Blackboard Collaborate to improve your understanding of reading articles. In today’s activity you will search articles on the topic “Database Security Best Practices”. Please note that in this work we’re interested in Database security best practices in general, and not limited to a specific vendor specific product like MS SQL Server.

Section 1 - Article search and identification of relevant articles on your topic, i.e. “Database security best practices”.

At the end of this section, you should be able to

1. Analyse elements of a search result (e.g. Google Scholar) to classify an article as research or review paper
2. Analyse the structure and content of an article to distinguish research articles from review articles
3. Understand what information is contained in sections of a typical research article in order to read more efficiently
4. Apply knowledge of reference tools to improve understanding of research articles

Section 2 - Read the Article

In this section of the exercise, you read the main text of an article on your choice of the above topic. Each group has 15 minutes to read their sections and take notes (see Annex 1). Once the time is up, you will need to discuss / share your results with other groups.

Note: When reading an article, it is recommended that you follow the following order and ask the following questions.

ADIR (M) - Abstract, Discussion, Introduction, Results, (Methods). (Bogucka & Wood 2009)

Abstract. Ask "Is this article relevant enough to continue with the full text, or should I move on to another article?"

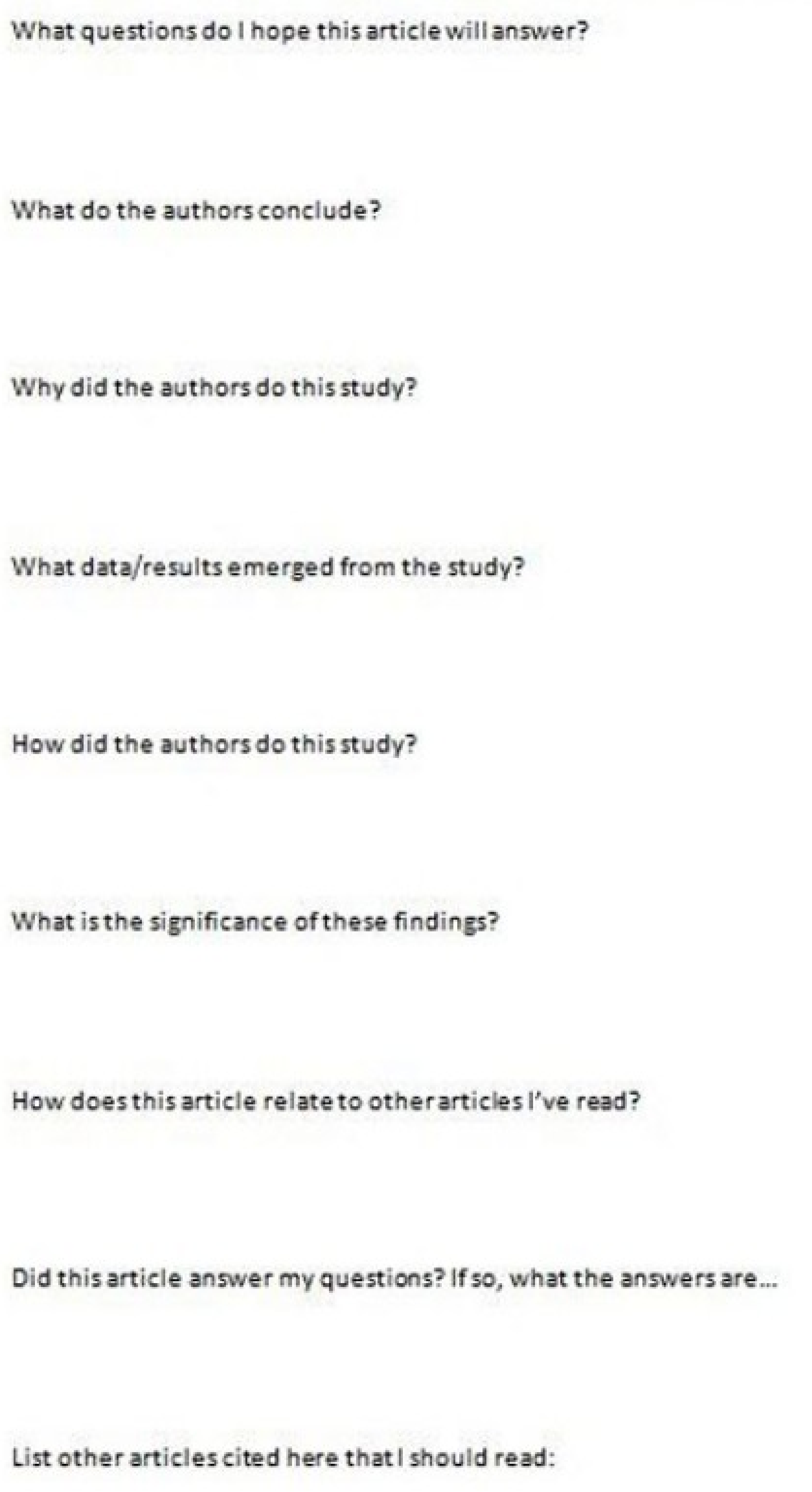
Discussion. Ask "What are the researchers' findings?"

Introduction. Ask "Why did the researchers do this study?" and "Does the research question match the conclusions?"

Results. Ask "Is the data collected suitable for answering the research question?" and "Does the data support the conclusions?"

Methods (optional). Ask "How can I repeat this study?" and "Are these methods suitable to gather the reported results?"

Annex 1: Increase your comprehension of scientific articles by taking notes.



What questions do I hope this article will answer?

What do the authors conclude?

Why did the authors do this study?

What data/results emerged from the study?

How did the authors do this study?

What is the significance of these findings?

How does this article relate to other articles I've read?

Did this article answer my questions? If so, what the answers are…

List other articles cited here that I should read:

Figure: Note-taking form (adapted from Bogucka & Wood 2009)

Bogucka, R., & Wood, E. (2009). How to read scientific research articles: a hands-on classroom exercise. *Issues in Science and Technology Librarianship*, *59*, 4-13.