# Cybersecurity

## Project 2.3.4 Find the Exploits

**TRAINING**

#7 Document the XSS stored exploit script: Use the View Source feature of the web page and create a screenshot of the few lines of code that could have prevented an XSS stored exploit had the programmer used them. (Show just the relevant lines of code, not the entire script.)

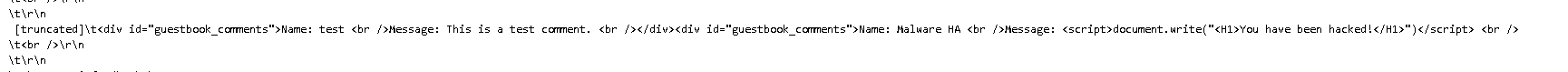
Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

#8 Save a screenshot of your entire Wireshark window with the Packet List showing the suspicious packet and the Packets Detail pane showing the exploited content.



#11 Save a screenshot of your entire Wireshark window with the suspicious packet in the Packet List and the exploited results in Packet Details.

Table

Description automatically generated

**REQUIREMENTS**

**Exploit 1:**

You suspect unauthorized hacker has hacked into one of your Bank of Virgil guestbook web

pages and used their script to show user cookie data.

1. Find the Suspicious Packet (Name the suspicious packet and provide a screenshot of the suspicious packet details.)

Packet #234

Graphical user interface, application, table

Description automatically generated with medium confidence

1. Identify the web page and the few lines of code that prevent this vulnerability.
2. Name the type of exploit.

XSS Stored Attack

1. Save a screenshot of the few lines of code that prevent this exploit (but not the entire script).

Text

Description automatically generated

1. Document your work. Describe how you found the exploit.

Went through each packet looking at the HTML data, skimming for any javascript code that may have been injected through a form

**Exploit 2:**

You suspect an attack on your Bank of Virgil database because unauthorized access has been

discovered.

1. Find the Suspicious Packet (Name the suspicious packet and provide a screenshot of the suspicious packet details.)

Packet #265

Graphical user interface, text, application, email

Description automatically generated

1. Identify the web page and the few lines of code that prevent this vulnerability.
2. Name the type of exploit.

SQL Injection

1. Save a screenshot of the few lines of code that prevent this exploit (but not the entire script).

A picture containing graphical user interface

Description automatically generated

1. Document your work. Describe how you found the exploit.

Clicked through each packet and watched where the user went by looking at the html. Then when I saw them go to the SQL Injection page I thought was a bit sus. Then the next packet had database information exposed!

**Exploit 3:**

You suspect a unauthrozied hacker is exploiting the Bank of Virgil Command Execute tool to

snoop on critical system data

1. Find the Suspicious Packet (Name the suspicious packet and provide a screenshot of the suspicious packet details.)

Graphical user interface, text, application, email

Description automatically generated

1. Identify the web page and the few lines of code that prevent this vulnerability.
2. Name the type of exploit.

Command Execution

1. Save a screenshot of the few lines of code that prevent this exploit (but not the entire script).

A picture containing text

Description automatically generated

1. Document your work. Describe how you found the exploit.

Clicked through the packets watching where the user went through the HTML. Saw they went to the command execution page and watched them execute a ping where they were able to snoop on critical system data