**TASK 1**

**QUESTION:**

YOU NEED TO FIND THE WEBSITES WITH THE FOLLOWING

VUNERABILITIES:

3 SQL INJECTION VULNERABILITIES (ERROR BASED)

3 TIME BASED SQL INJECTION VULNERABILITIES

3 BLIND SQL INJECTION VULNERABILITIES

**SUMMARY:**

Basically, there are 3 types of SQL injections:

1. Blind SQL Injection: In this type, the attacker's malicious input doesn't directly display the results of the injected query. Instead, they exploit the application's response to infer information by true/false responses or time delays.
2. Time-Based Blind SQL Injection: Attackers use this technique to induce delays in the application's response, making it possible to extract information through the time it takes for the server to respond.
3. Error-Based SQL Injection: By manipulating SQL queries to produce intentional errors, attackers can gather valuable information from the error messages generated by the database.

3 WEBSITES THAT ARE VULNERABLE TO ERROR BASED SQL INJECTION VULNERABILITIY:

1.<https://sinaha.ae/index.php?route=product/product&product_id=2436>

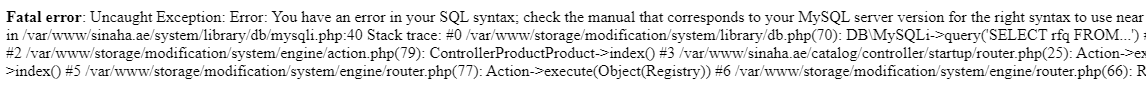
A picture containing text, screenshot, design

Description automatically generated

This is the basic webpage, and when we add the payload like ‘ , “ we get the following error

Vulnerable link:

<https://sinaha.ae/index.php?route=product/product&product_id=2436%27>



This indicates that the website is vulnerable to SQL Error Based Injection vulnerability.

2.<https://www.tufpak.com.pk/index.php?module=content&id=86>

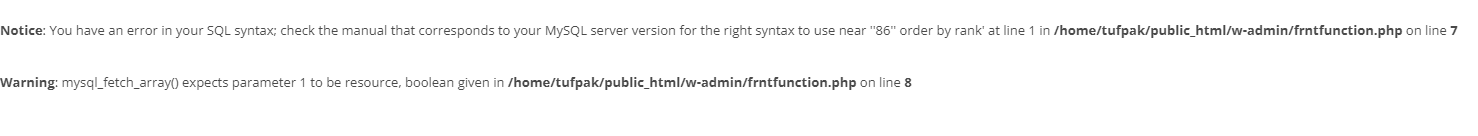
A screenshot of a website

Description automatically generated with medium confidence

This is the basic webpage, and when we add the payload like ‘ , “ we get the following error

Vulnerable link:

<https://www.tufpak.com.pk/index.php?module=content&id=86%27>



As we can see this website gives a SQL error along with the php database error that means this website is also vulnerable to the SQL Error based vulnerability.

3.<https://www.championsports.com.pk/products.php?ID=1>

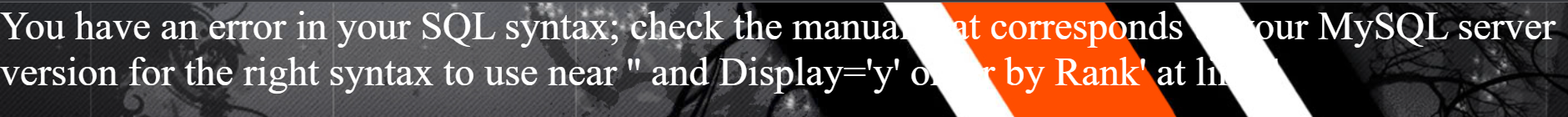
A screenshot of a website

Description automatically generated with low confidence

This is the basic webpage, and when we add the payload like ‘ , “ we get the following error

Vulnerable link:

<https://www.championsports.com.pk/products.php?ID=1%27>



Since the website is showing the above error, we can understand that the website is vulnerable to the SQL Error based Injection vulnerability.

3 WEBSITES THAT ARE VULNERABLE TO TIME BASED SQL INJECTION VULNERABILITIY:

1.<https://www.cdbl.com.bd/details.php?id=1>

A screenshot of a website

Description automatically generated with medium confidence

Payloads used:

AND ORDER BY SLEEP(5)

Vulnerable link:

<https://www.cdbl.com.bd/details.php?id=1%20AND%20ORDER%20BY%20SLEEP(5)>

When we add the payloads mentioned above, we can see that the website responds a little bit later than the usual response time i.e., the website responds after the time mentioned in the SLEEP command that in this case being 5 seconds.

This helps us to understand that the website is vulnerable to the SQL time-based vulnerability.

2.<https://www.biketowork.ch/de?id=1&L=1>

A person riding a bicycle

Description automatically generated with medium confidence

Payloads used:

AND ORDER BY SLEEP(5)

Vulnerable link: <https://www.biketowork.ch/de?id=1&L=1%20AND%20ORDER%20BY%20SLEEP(5)>

The website responds after the period specified in the SLEEP command, which in this case is 5 seconds when we add the payloads indicated above. This response time is later than the website's typical response time.

This clarifies the website's vulnerability to the SQL time-based vulnerability.

3.<http://www.pitschuch.at/cad.php?id=1>

A screenshot of a computer

Description automatically generated with medium confidence

Payloads used:

“ or sleep(5)#

Vulnerable link: [http://www.pitschuch.at/cad.php?id=1%22%20or%20sleep(5)#](http://www.pitschuch.at/cad.php?id=1%22%20or%20sleep(5))

This website is vulnerable to both SQL Error based vulnerability as well as the Time-based vulnerability as it responds in the time mentioned in the sleep query and displays an error SQL database error when the payload is given.

3 WEBSITES THAT ARE VULNERABLE TO BLIND SQL INJECTION VULNERABILITIY:

1.<https://pfi.gov.pk/detail.php?id=29>

Before giving the payload:

A screenshot of a computer

Description automatically generated with low confidence

After giving the payload:

A picture containing text, screenshot, design

Description automatically generated

Vulnerable link: <https://pfi.gov.pk/detail.php?id=29%27>

The data present on the website is completely misplaced when the single quote (‘) payload is given In the ID parameter of the URL.

This indicates that the Website is vulnerable to the SQL Blind injection vulnerability.

2.<https://www.kohyo.nl/detail.php?id=102>

Before giving the payload:

A screenshot of a computer

Description automatically generated with low confidence

After giving the payload:

A picture containing text, font, screenshot

Description automatically generated

Vulnerable link: <https://www.kohyo.nl/detail.php?id=102%27>

The data is completely misplaced and lost on the web page when the id parameter of the URL is given with payloads like single quote (‘) , this indicates that the website is vulnerable to the SQL Blind injection vulnerability.

3.<https://nwu.edu.bd/notice_details.php?id=35>

Before giving the payload:

A screenshot of a computer

Description automatically generated with low confidence

Vulnerable link:

<https://nwu.edu.bd/notice_details.php?id=35%27>

After giving the payload:

A close-up of a website

Description automatically generated with low confidence

As we can observe the contents in table and the entire table is missing in the Webpage when the payload is given to the id parameter of the URL.

This indicates that the webpage is vulnerable to SQL Blind Injection vulnerability.

Conclusion:

In conclusion, the security and integrity of databases are seriously threatened by time-based, blind, and error-based SQL injection vulnerabilities. These kinds of attacks make use of online applications' flaws, such include improper validation of user input.

Attackers may detect weaknesses and retrieve sensitive data by using time-based SQL injection attacks to create significant delays in query execution. On the other side, blind SQL injection attacks depend on time-based methods to extract data without immediately revealing the results, making them more challenging to identify. Attacks using error-based SQL injection take advantage of error messages produced by the database to obtain useful data about the layout and content of the database.

The impacts of these vulnerabilities can be severe, including unauthorized access of sensitive information, manipulation, or destruction of data. Organizations can suffer financial losses, damage to their reputation, and legal consequences because of these attacks.

Secure coding approaches and strong input validation methods must be used to reduce these vulnerabilities. To make sure that user input is adequately validated and does not generate SQL injection vulnerabilities, developers should utilize parameterized queries or prepared statements. Additionally, regular penetration tests and security audits may help find and fix any possible vulnerabilities in online applications.

Additionally, it's crucial to maintain databases and web application frameworks updated with the most recent security fixes.