



USER MANUAL

Vulnerability Test Flow

You will need the following information from your Network Administrator to do the **Advanced Vulnerability Test**.

1. VPN Details

- VPN username and VPN password
- VPN configuration files
- IP address range

2. Linux Network Details

- Network administrator username and password
- IP address list or range

3. Windows Network Details

- Network administrator username and password
- Network Domain name
- IP address list or range
- Remote access should be enabled for accessing windows systems.

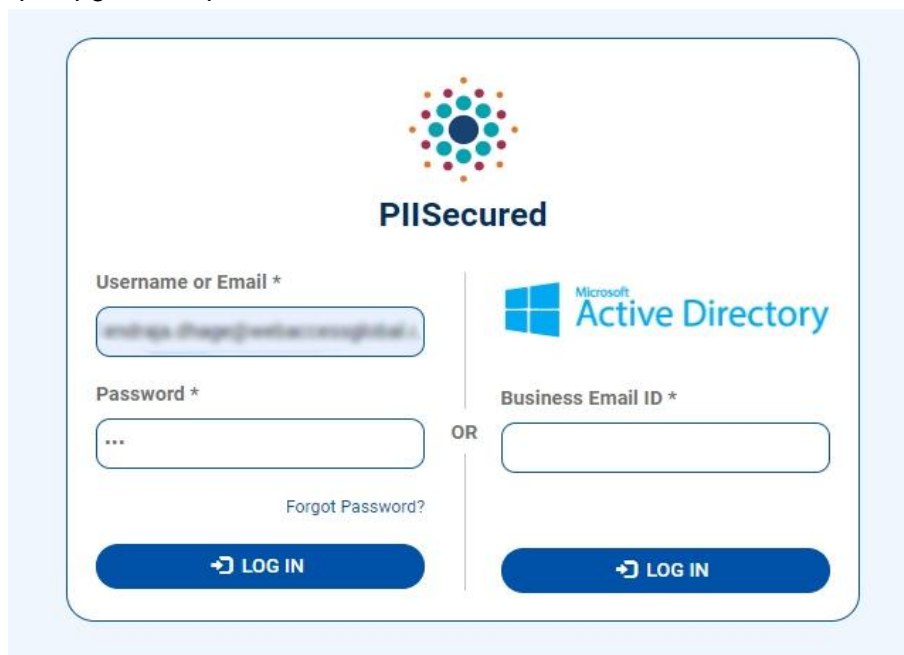
You will need the following information from your Network Administrator to do the **External Vulnerability Test**.

1. Domain Details

The steps for creating a vulnerability test in the OB360 application :

Step 1: Go to the PII Secured portal and use your partner user credentials to log in.

URL : <https://pg-ob360.piisecured.com/>



The login screen for PII Secured features a central logo at the top. Below it, there are two main login paths. The left path is for 'Username or Email' and 'Password', with a 'Forgot Password?' link. The right path is for 'Business Email ID' and includes the 'Microsoft Active Directory' logo. Both paths have a 'LOG IN' button. A vertical line separates the two paths, with the word 'OR' in the center.

Figure : Login Screen

Step 2 : After login, go to the side menu bar section. Click on the 'OB360 Login' button.

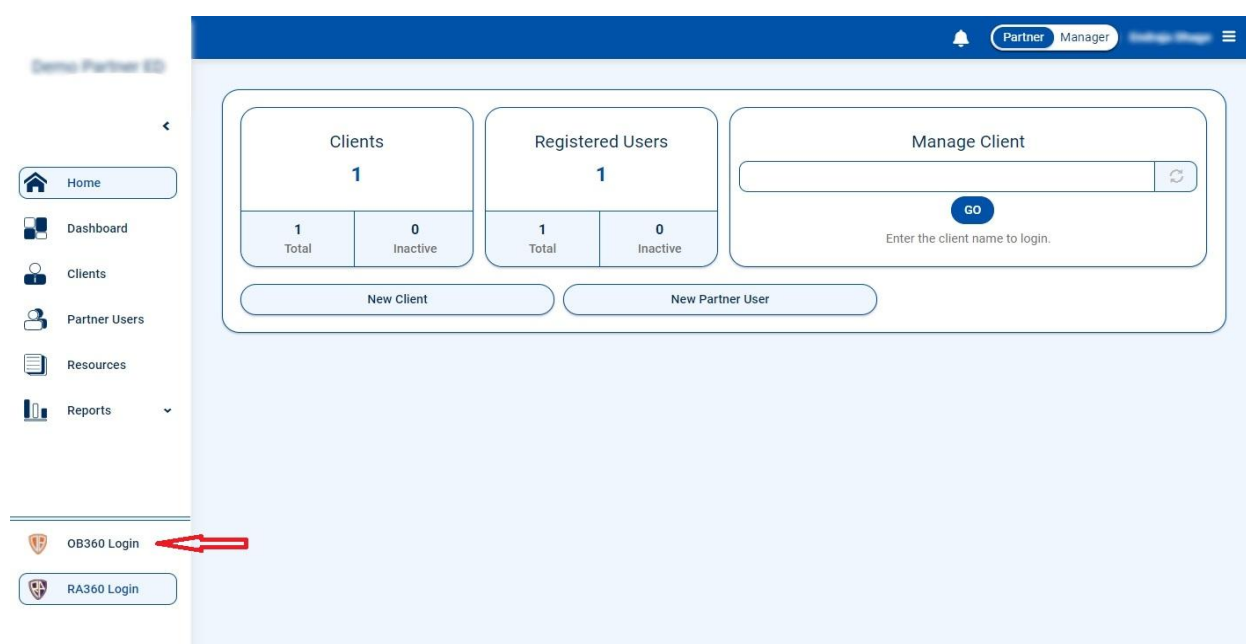
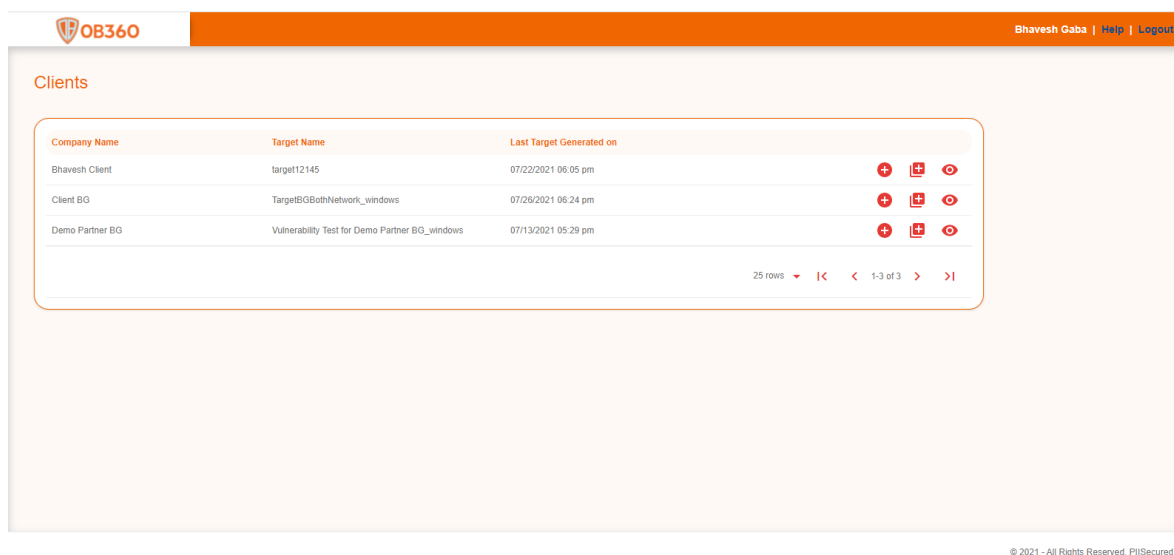


Figure : Home Screen

Step 3: You will be redirected to the OB360 application in a new tab.



Company Name	Target Name	Last Target Generated on	
Bhavesh Client	target12145	07/22/2021 06:05 pm	+ [icon] [icon]
Client BG	TargetBGBotNetwork_windows	07/26/2021 06:24 pm	+ [icon] [icon]
Demo Partner BG	Vulnerability Test for Demo Partner BG_windows	07/13/2021 05:29 pm	+ [icon] [icon]

25 rows |< < 1-3 of 3 > >|

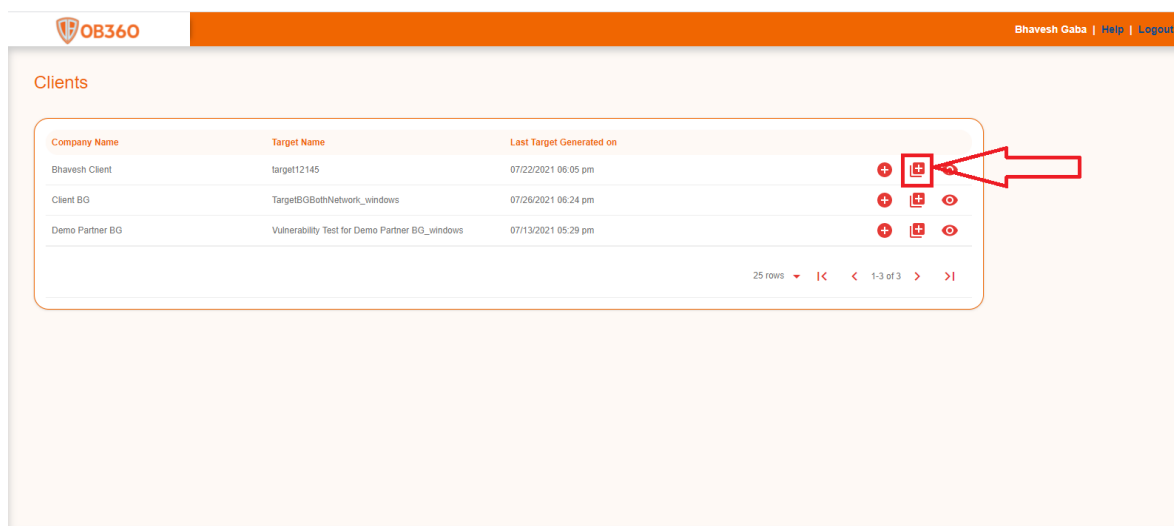
© 2021 - All Rights Reserved, PII Secured

Figure : Clients Screen 1

Here you will see a client list with its latest created target.
Through this page you will be able to do the following activities :

1. **Create External Vulnerability Test** - [Step 13](#)
2. **Create Advanced Vulnerability Test** - [Step 4](#)
3. **View Vulnerability Test** - [Step 12](#)

Step 4: Click on the "Advanced Vulnerability Test" icon for creating a new Advanced Vulnerability test.

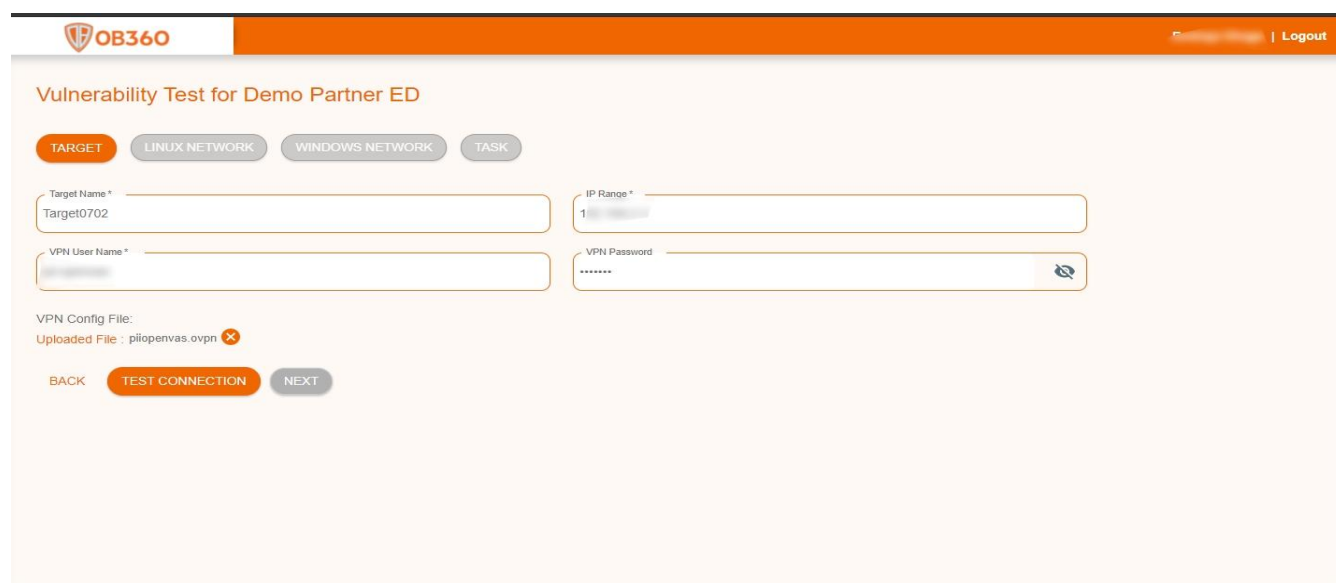


© 2021 - All Rights Reserved, PII Secured

Figure : Clients Screen 2

Step 5: Now you will redirect to the target page. Do the following steps to create a target.

- Enter the Target Name, IP Range, VPN Username and VPN Password.
- Upload VPN configuration file given by your network administrator.
- Click on the 'Test Connection' button.



Vulnerability Test for Demo Partner ED

TARGET LINUX NETWORK WINDOWS NETWORK TASK

Target Name* Target0702

IP Range* 1

VPN User Name*

VPN Password*

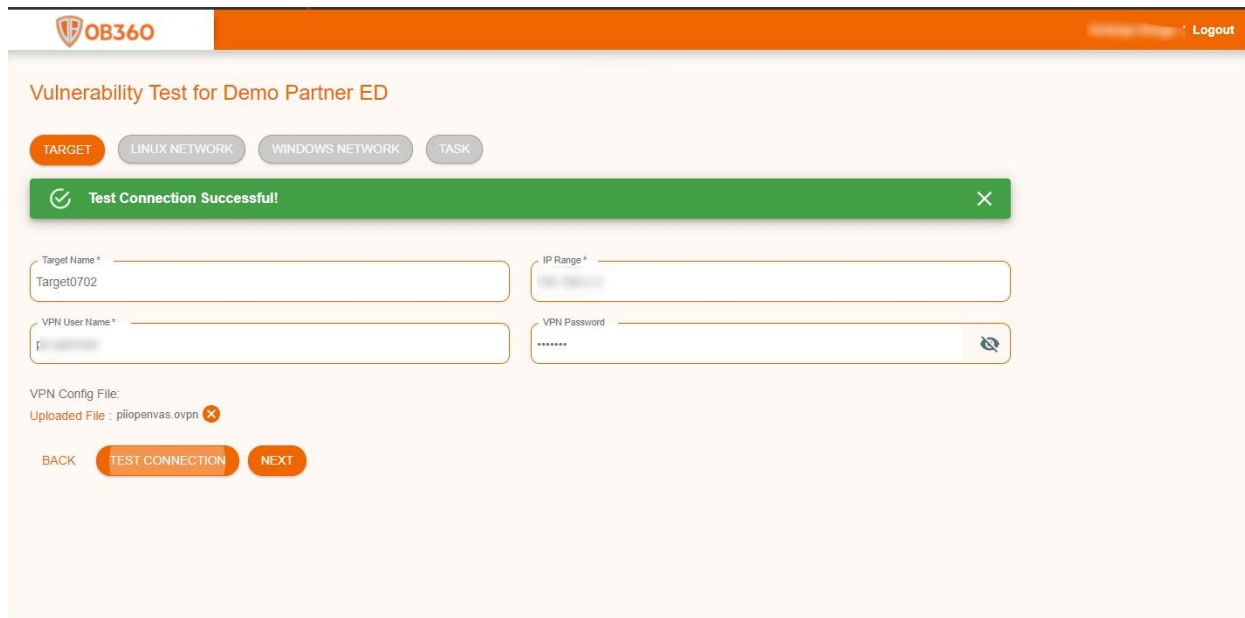
VPN Config File:
Uploaded File : pilopenvas.ovpn

BACK TEST CONNECTION NEXT

OB360 | © Copyright 2020

Figure : Target Screen

After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.



The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there's a navigation bar with the OB360 logo and a 'Logout' link. Below the navigation bar, there are four tabs: 'TARGET', 'LINUX NETWORK', 'WINDOWS NETWORK', and 'TASK'. The 'TARGET' tab is selected. A green success message banner at the top reads 'Test Connection Successful!'. Below this, there are four input fields: 'Target Name *' (containing 'Target0702'), 'IP Range *', 'VPN User Name *', and 'VPN Password'. Below the input fields, there's a section for 'VPN Config File:' with an 'Uploaded File : pilopenvas.ovpn' and a close icon. At the bottom, there are three buttons: 'BACK', 'TEST CONNECTION', and 'NEXT'. The 'NEXT' button is highlighted in orange, indicating it is enabled.

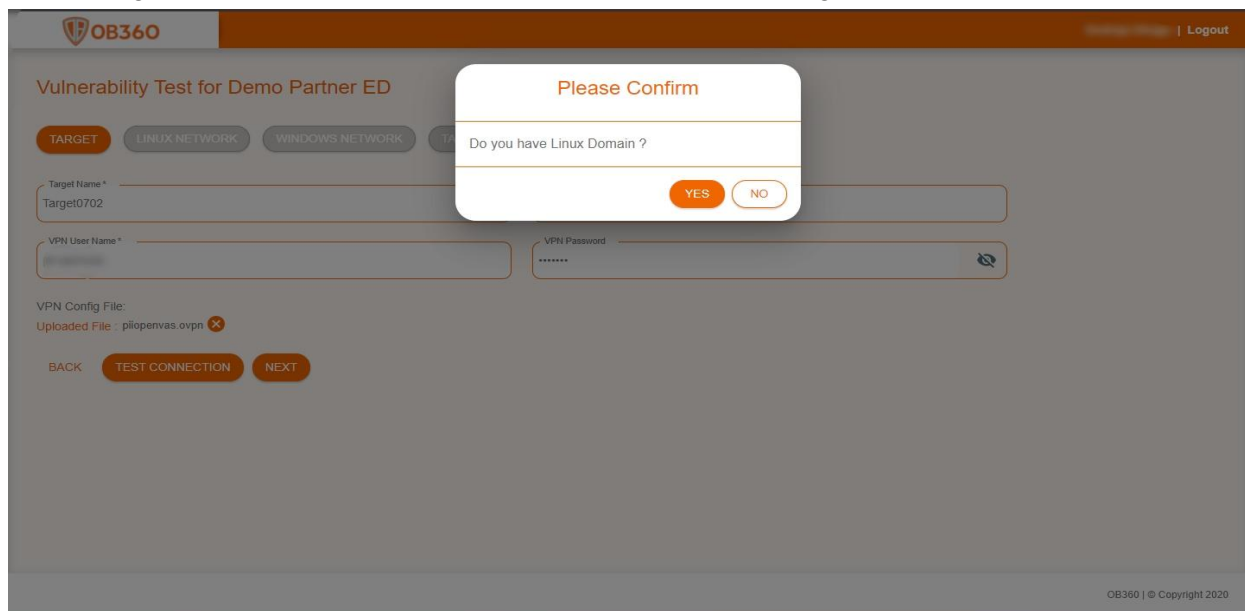
OB360 | © Copyright 2020

Figure : Target Success Screen

Note: If you get an error message 'Test Connection Failed' then enter correct credentials for target and try again till you get the success message.

Step 6: After the Next button is enabled click on it.

On clicking the next button a popup window will appear showing 'Do You have Linux Domain?'



The screenshot shows the same 'Vulnerability Test for Demo Partner ED' interface as before, but with a confirmation popup window in the center. The popup is titled 'Please Confirm' and contains the question 'Do you have Linux Domain?'. There are two buttons in the popup: 'YES' and 'NO'. The 'YES' button is highlighted in orange. The background of the main interface is dimmed.

OB360 | © Copyright 2020

Figure : Linux Confirmation Screen

Click on 'Yes' if you have linux network else click on 'No'

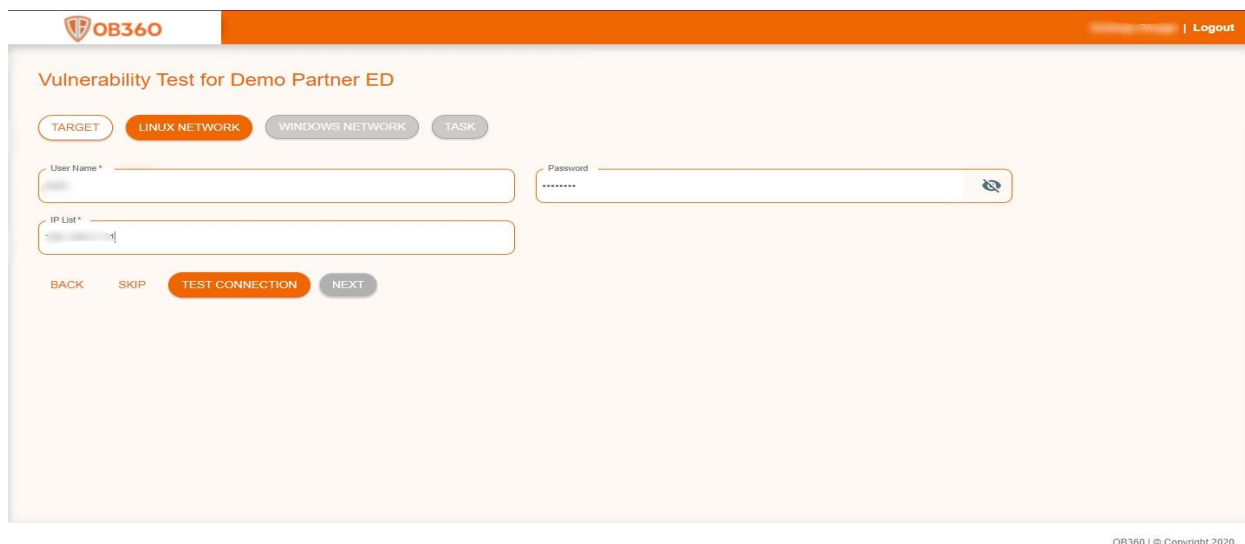
On click of 'Yes' you will redirect to [step 7](#).

On click of 'No' you will redirect to [step 9](#).

Step 7: Now you will redirect to the linux network page.

Do the following steps to create a target for the linux network.

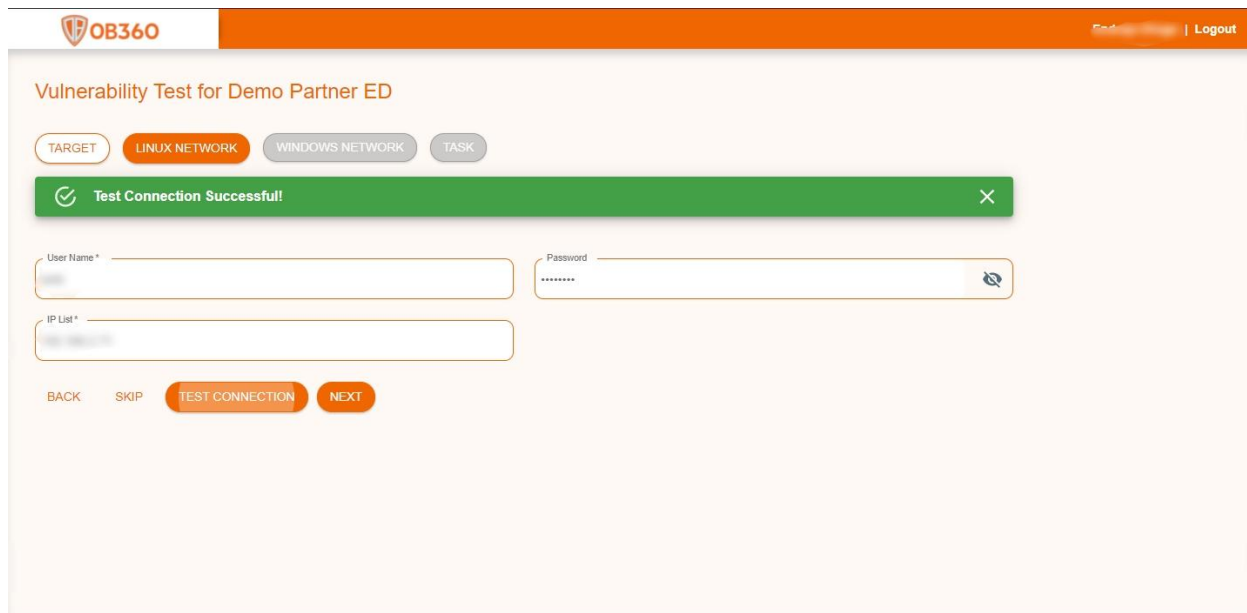
- Enter network administrator Username and Password
- Enter IP address list or IP range
- Click on the 'Test Connection' button.



The screenshot shows the 'Linux Network' configuration page within the OB360 application. The page has an orange header with the OB360 logo and a 'Logout' link. Below the header, the title 'Vulnerability Test for Demo Partner ED' is displayed. The main content area features four tabs: 'TARGET', 'LINUX NETWORK' (which is selected and highlighted in orange), 'WINDOWS NETWORK', and 'TASK'. Under the 'LINUX NETWORK' tab, there are three input fields: 'User Name *', 'Password' (with a toggle for visibility), and 'IP List *'. At the bottom of the form, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION' (highlighted in orange), and 'NEXT'. The footer of the page contains the text 'OB360 | © Copyright 2020'.

Figure : Linux Network Screen

After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.



The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there's a navigation bar with the OB360 logo and a 'Logout' link. Below the navigation bar, there are four tabs: 'TARGET', 'LINUX NETWORK' (which is active), 'WINDOWS NETWORK', and 'TASK'. A green success message banner at the top reads 'Test Connection Successful!'. Below this, there are input fields for 'User Name *', 'Password', and 'IP List *'. The 'Password' field has a toggle icon for visibility. At the bottom, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION', and 'NEXT'.

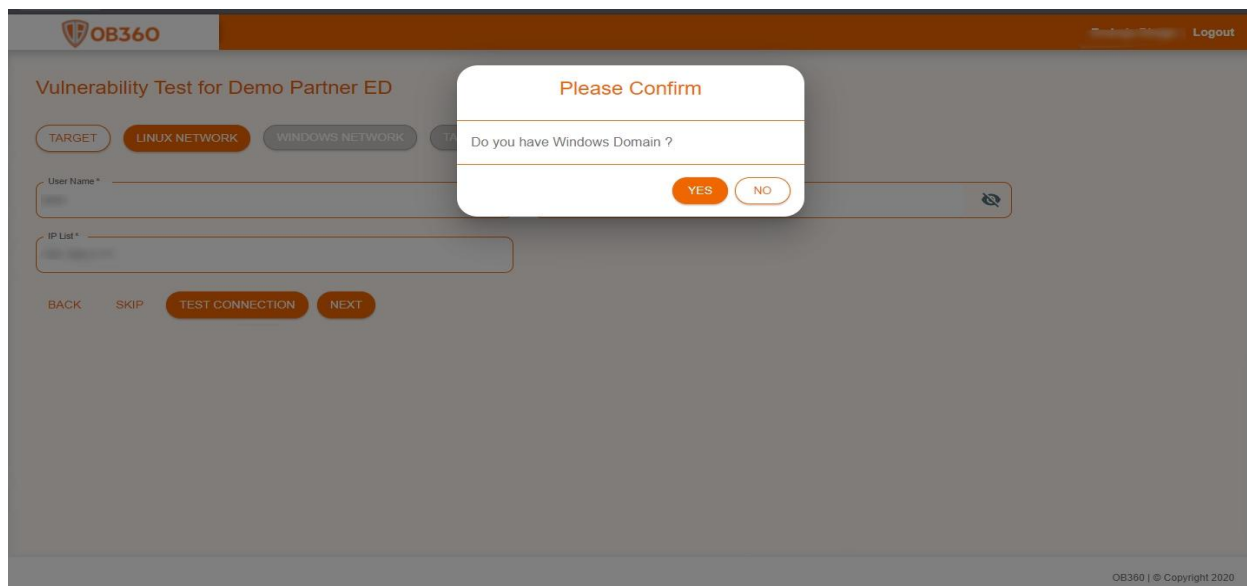
OB360 | © Copyright 2020

Figure : Linux Success Screen

Note: If you get an error message 'An Error Occurred' then enter correct credentials for linux network and try again till you get the success message.

Step 8: After the Next button is enabled click on it.

On clicking the next button a popup window will appear showing 'Do You have Windows Domain?'



The screenshot shows the same 'Vulnerability Test for Demo Partner ED' interface, but with a confirmation popup window. The popup is titled 'Please Confirm' and contains the question 'Do you have Windows Domain?'. It has two buttons: 'YES' and 'NO'. The background interface is dimmed, showing the same tabs and input fields as the previous screen.

OB360 | © Copyright 2020

Figure : Windows Confirmation Screen

Click on 'YES' if you have windows network else click on 'NO'

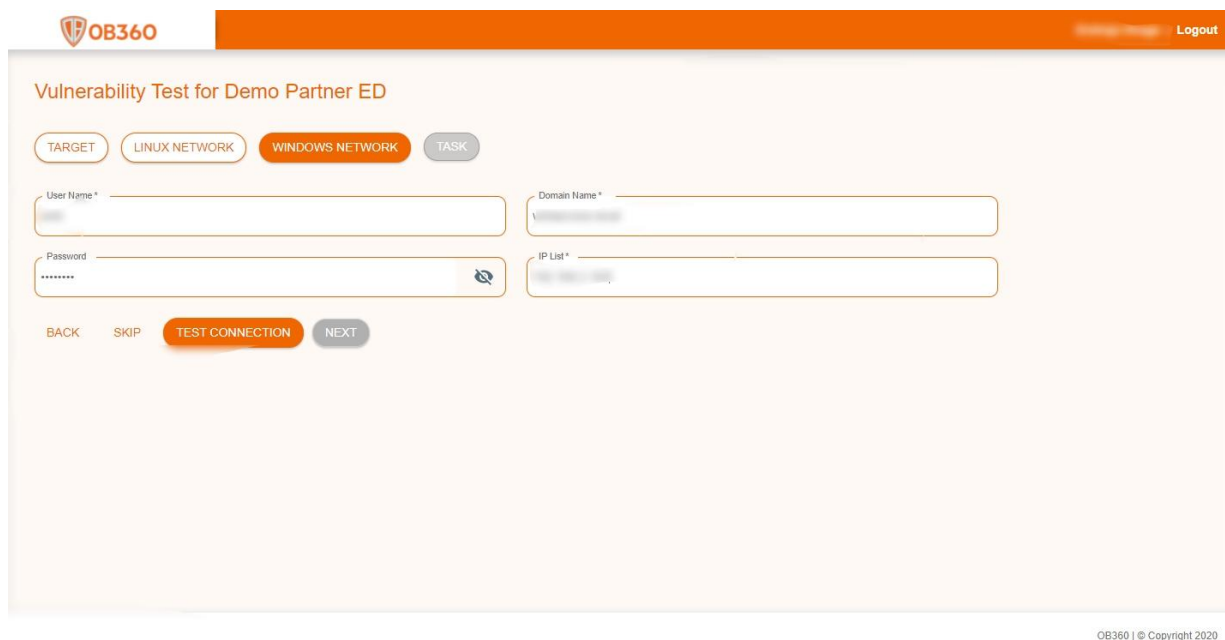
On click of 'Yes' you will redirect to [step 9](#).

On click of 'No' you will redirect to [step 10](#).

Step 9: Now you will redirect to the windows network page.

Do the following steps to create a target for windows network..

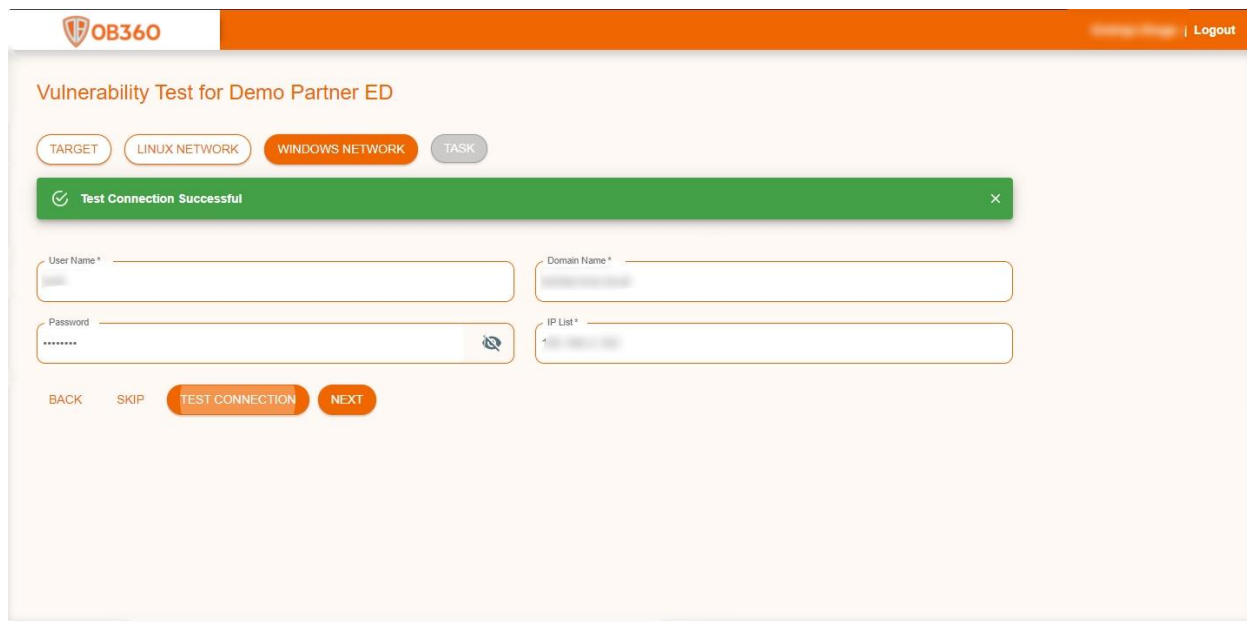
- Enter network administrator Username and Password, Domain Name
- Enter IP address list or IP range
- Click on the 'Test Connection' button.



The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there is an orange header with the OB360 logo and a 'Logout' link. Below the header, the title 'Vulnerability Test for Demo Partner ED' is displayed. Underneath, there are four tabs: 'TARGET', 'LINUX NETWORK', 'WINDOWS NETWORK' (which is selected and highlighted in orange), and 'TASK'. The main content area contains four input fields: 'User Name *', 'Domain Name *', 'Password' (with a masked password '*****' and a toggle icon), and 'IP List *'. At the bottom of the form, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION' (highlighted in orange), and 'NEXT'. In the bottom right corner of the page, there is a small text string: 'OB360 | © Copyright 2020'.

Figure : Windows Network Screen

After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.



OB360

Vulnerability Test for Demo Partner ED

TARGET LINUX NETWORK WINDOWS NETWORK TASK

Test Connection Successful

User Name *

Domain Name *

Password *

IP List *

BACK SKIP TEST CONNECTION NEXT

OB360 | © Copyright 2020

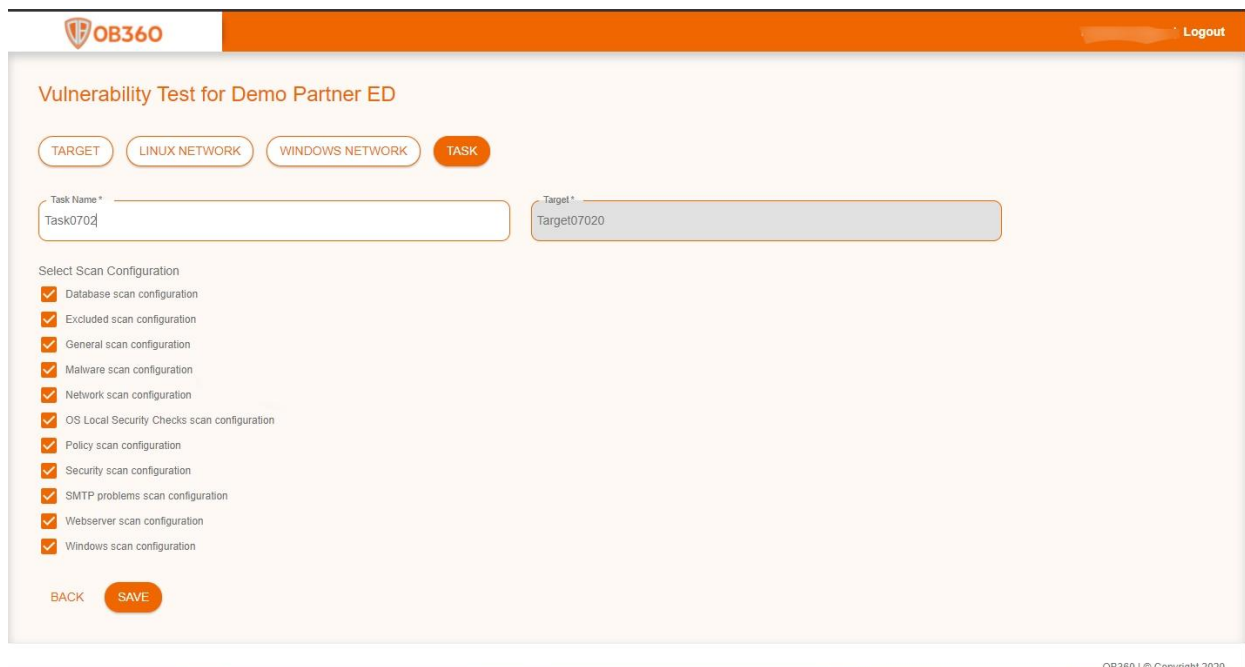
Figure : Windows Success Screen

Note: If you get an error message 'An Error Occurred' then enter correct credentials for windows network and try again till you get the success message.

Step 10: After the Next button is enabled click on it.

Now you will redirect to the task creation page.

Enter the task name and click on the save button after selecting at least one scan configuration from the list.



Vulnerability Test for Demo Partner ED

TARGET LINUX NETWORK WINDOWS NETWORK **TASK**

Task Name * Target *

Task0702 Target0702

Select Scan Configuration

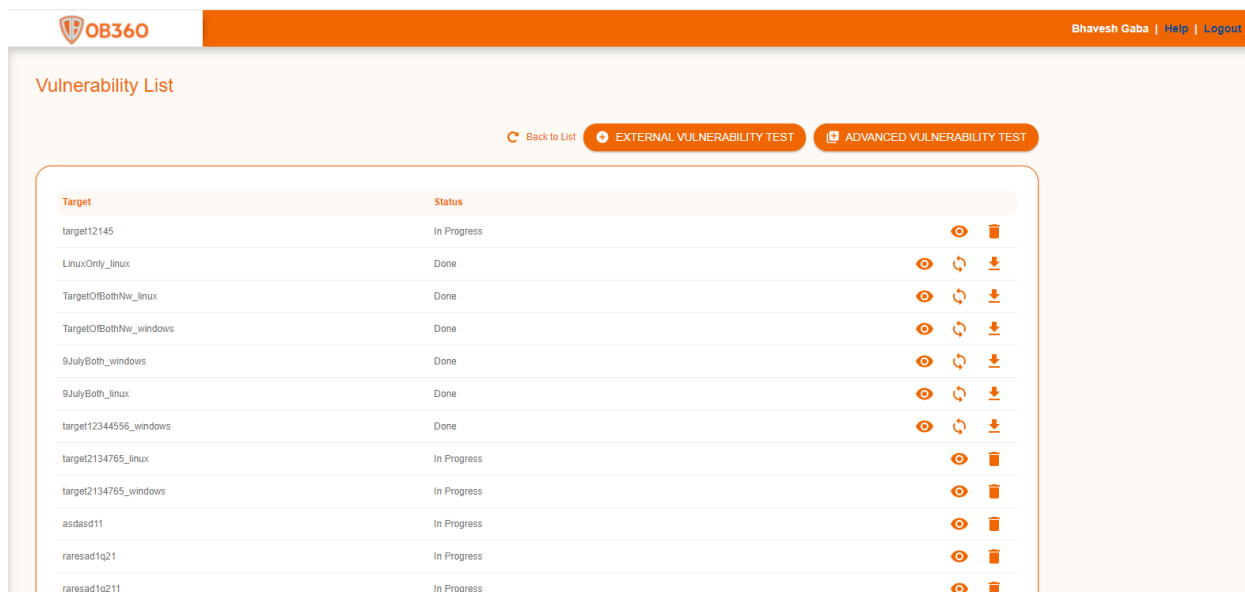
- ☒ Database scan configuration
- ☒ Excluded scan configuration
- ☒ General scan configuration
- ☒ Malware scan configuration
- ☒ Network scan configuration
- ☒ OS Local Security Checks scan configuration
- ☒ Policy scan configuration
- ☒ Security scan configuration
- ☒ SMTP problems scan configuration
- ☒ Webserver scan configuration
- ☒ Windows scan configuration

BACK SAVE

Figure : Task Screen

Step 11: After clicking the save button.

The page will redirect to the Report List page, where you will see the most recently generated vulnerabilities.



Vulnerability List

Back to List EXTERNAL VULNERABILITY TEST ADVANCED VULNERABILITY TEST

Target	Status	View	Refresh	Delete
target12145	In Progress			
LinuxOnly_linux	Done			
TargetOfBothNw_linux	Done			
TargetOfBothNw_windows	Done			
9JulyBoth_windows	Done			
9JulyBoth_linux	Done			
target12344556_windows	Done			
target2134765_linux	In Progress			
target2134765_windows	In Progress			
asdaad11	In Progress			
raresad1q21	In Progress			
raresad1q211	In Progress			

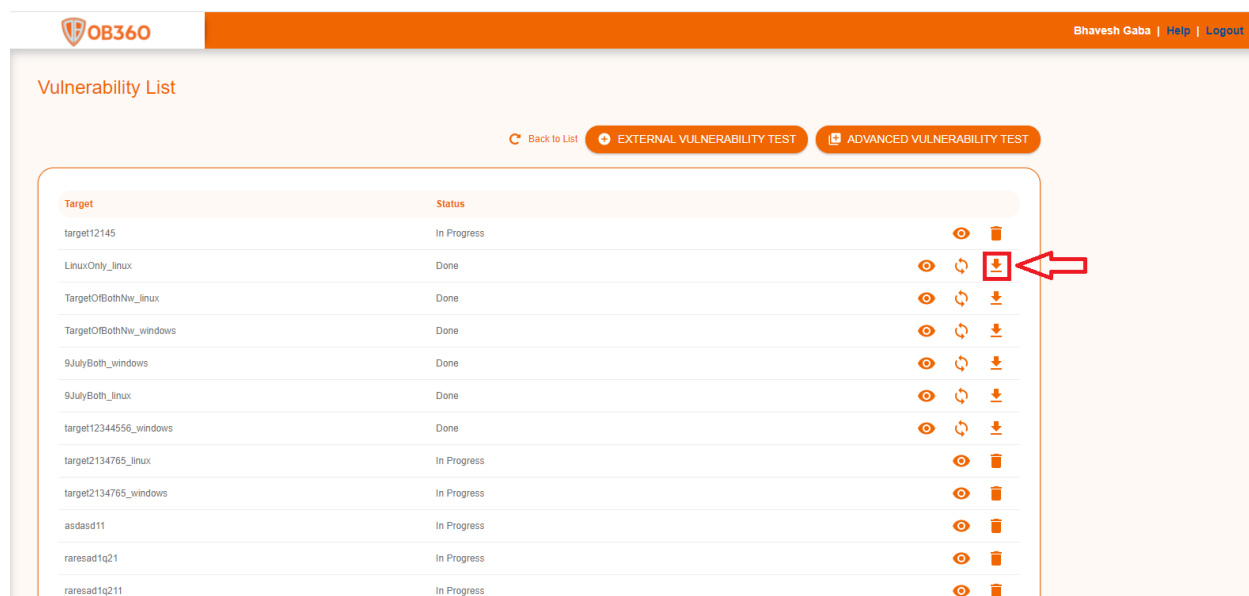
Figure : Latest Vulnerability List Screen

Status of the current Vulnerability test is 'In Progress'.

The selected task will be scanned. A report will be generated after all of the tasks have been scanned.

By clicking the view button, you can see the status of the created target.

When all the tasks have been completed, the status will be changed to "Done".



Target	Status	Actions
target12145	In Progress	View, Refresh, Download
LinuxOnly_linux	Done	View, Refresh, Download
TargetOfBothNw_linux	Done	View, Refresh, Download
TargetOfBothNw_windows	Done	View, Refresh, Download
9JulyBoth_windows	Done	View, Refresh, Download
9JulyBoth_linux	Done	View, Refresh, Download
target12344556_windows	Done	View, Refresh, Download
target2134765_linux	In Progress	View, Refresh, Download
target2134765_windows	In Progress	View, Refresh, Download
asdaad11	In Progress	View, Refresh, Download
raresad1q21	In Progress	View, Refresh, Download
raresad1q211	In Progress	View, Refresh, Download

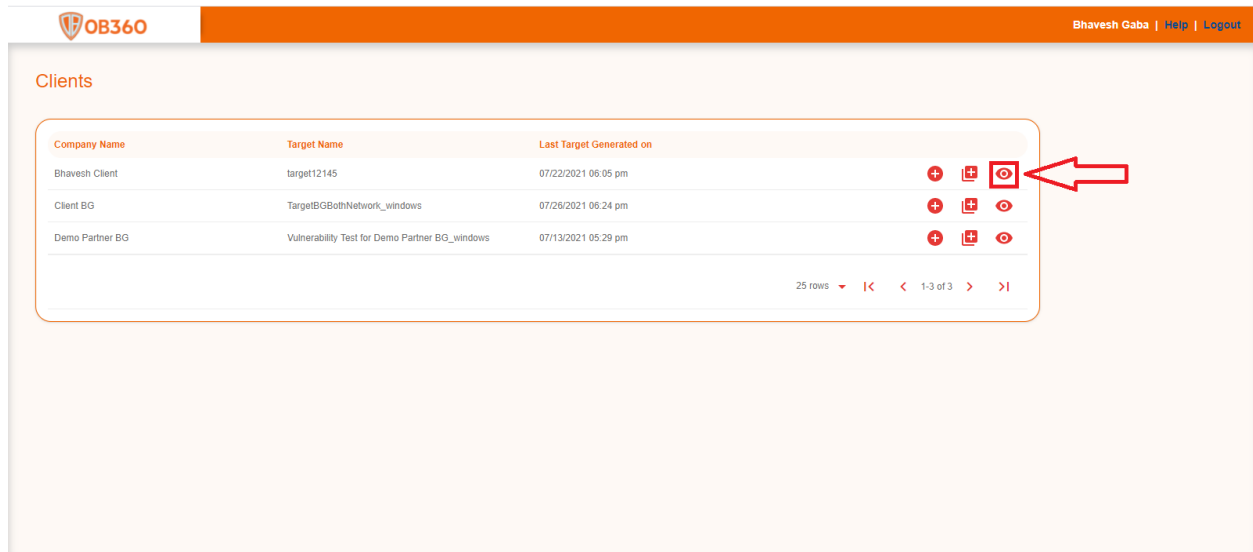
Figure : Vulnerability List Screen










Now you can download the report by clicking the 'Download' button . You will get the report in zip format.

Extract the zip and you will get all the reports generated for your task.

Step 12 :

Click on the "View Vulnerability Tests" icon for Viewing a Vulnerability test.

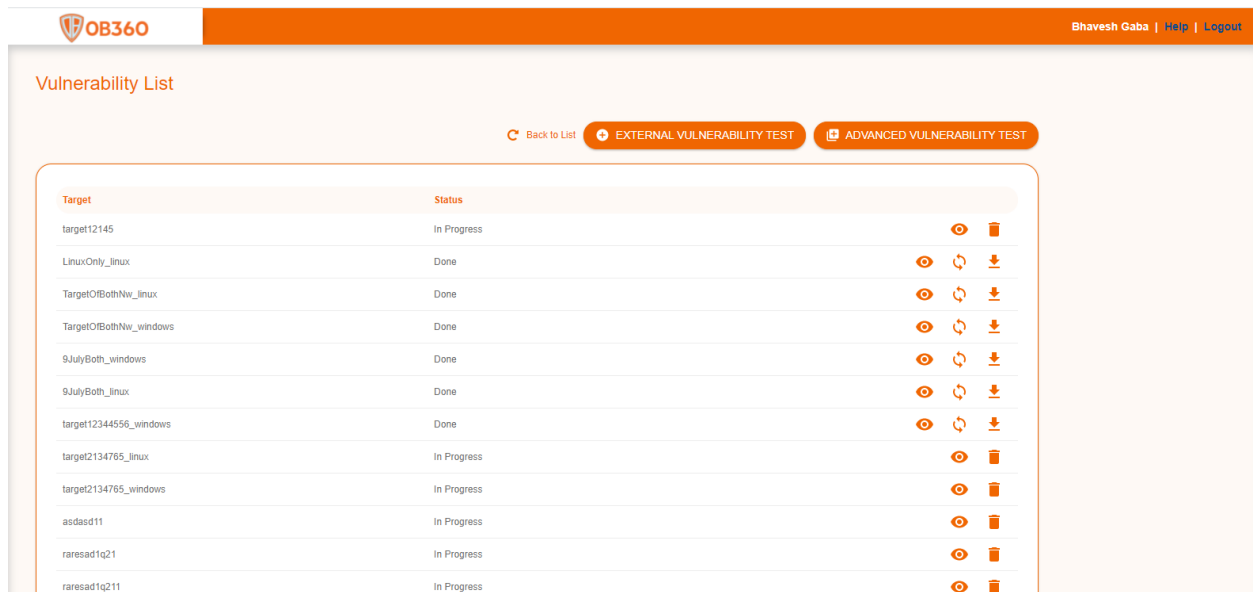


Company Name	Target Name	Last Target Generated on	
Bhavesh Client	target12145	07/22/2021 06:05 pm	  
Client BG	TargetBGBothNetwork_windows	07/26/2021 06:24 pm	  
Demo Partner BG	Vulnerability Test for Demo Partner BG_windows	07/13/2021 05:29 pm	  

© 2021 - All Rights Reserved, PII Secured

Figure :Client Screen

Here you will see a list of all Vulnerabilities along with their current status.

































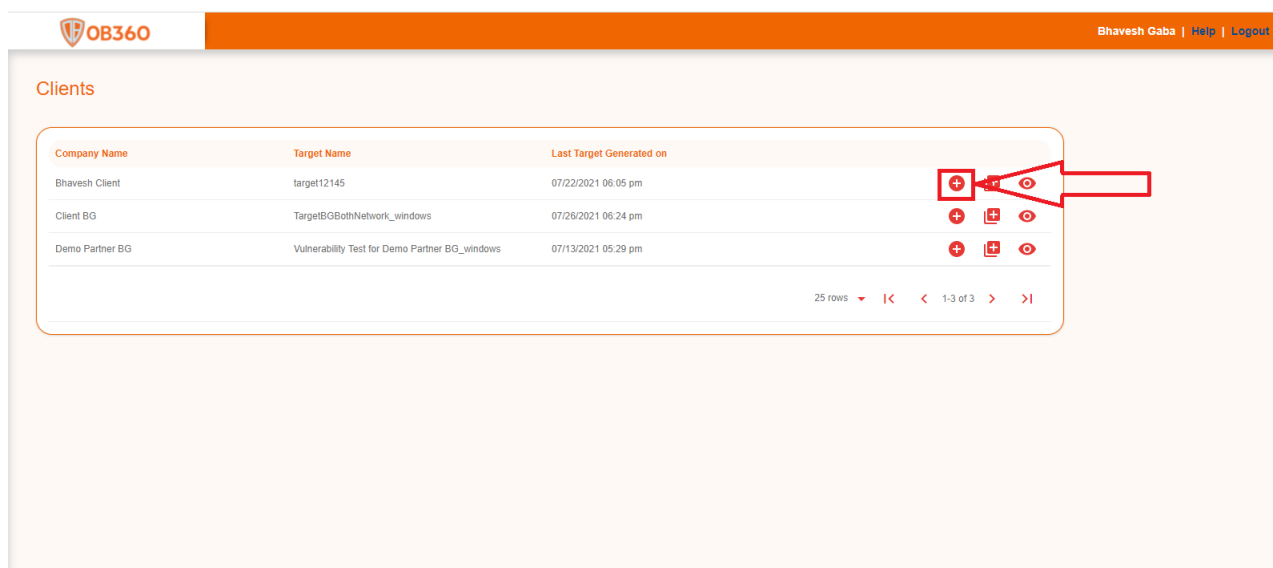
Target	Status	
target12145	In Progress	 
LinuxOnly_linux	Done	  
TargetOfBothNw_linux	Done	  
TargetOfBothNw_windows	Done	  
9JuryBoth_windows	Done	  
9JuryBoth_linux	Done	  
target12344556_windows	Done	  
target2134765_linux	In Progress	 
target2134765_windows	In Progress	 
asdaad11	In Progress	 
raresad1q21	In Progress	 
raresad1q211	In Progress	 

Figure : Vulnerability List Screen 1

Through this page you will be able to do the following activities :

1. Creating a new [External vulnerability test](#).
2. Creating a new [Advanced vulnerability test](#).
3. View status of created task.
4. Make a copy of the target.
5. Download the report.

Step 13 : To create a new External vulnerability test click on 'Create External vulnerability button.



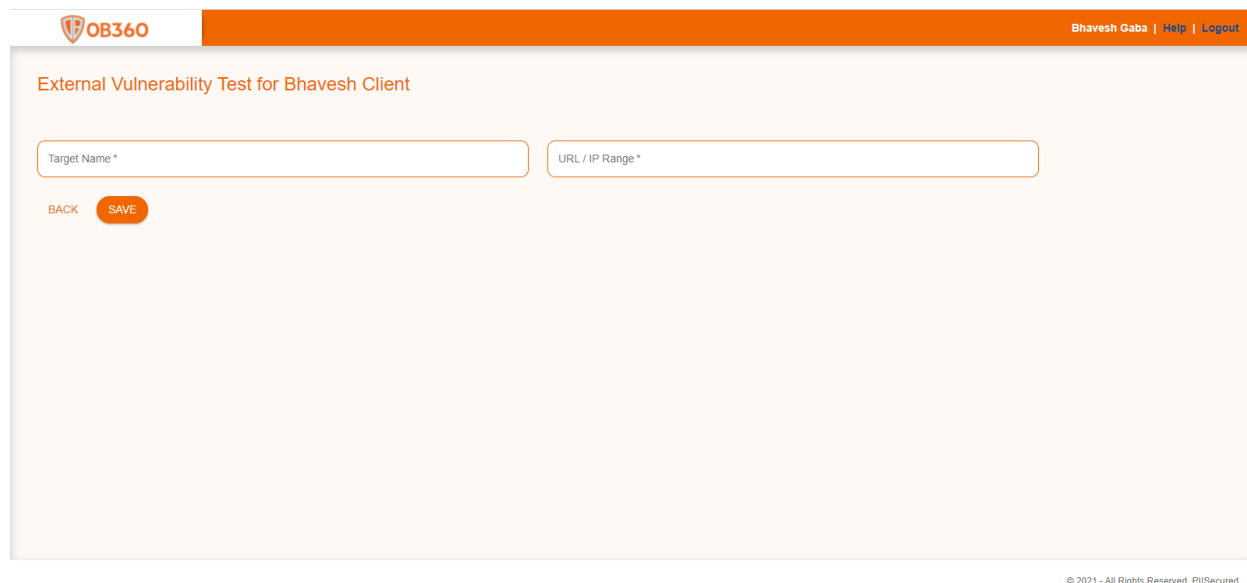
Company Name	Target Name	Last Target Generated on
Bhavesh Client	target12145	07/22/2021 06:05 pm
Client BG	TargetBGBothNetwork_windows	07/26/2021 06:24 pm
Demo Partner BG	Vulnerability Test for Demo Partner BG_windows	07/13/2021 05:29 pm

25 rows |< < 1-3 of 3 > >|

Figure : Client List Screen

Step 14 : Now you will redirect to the External target page. Do the following steps to create a target.

- Enter the Target Name, IP Range or Domain Name Eg: (example.com or 192.168.X.XX)

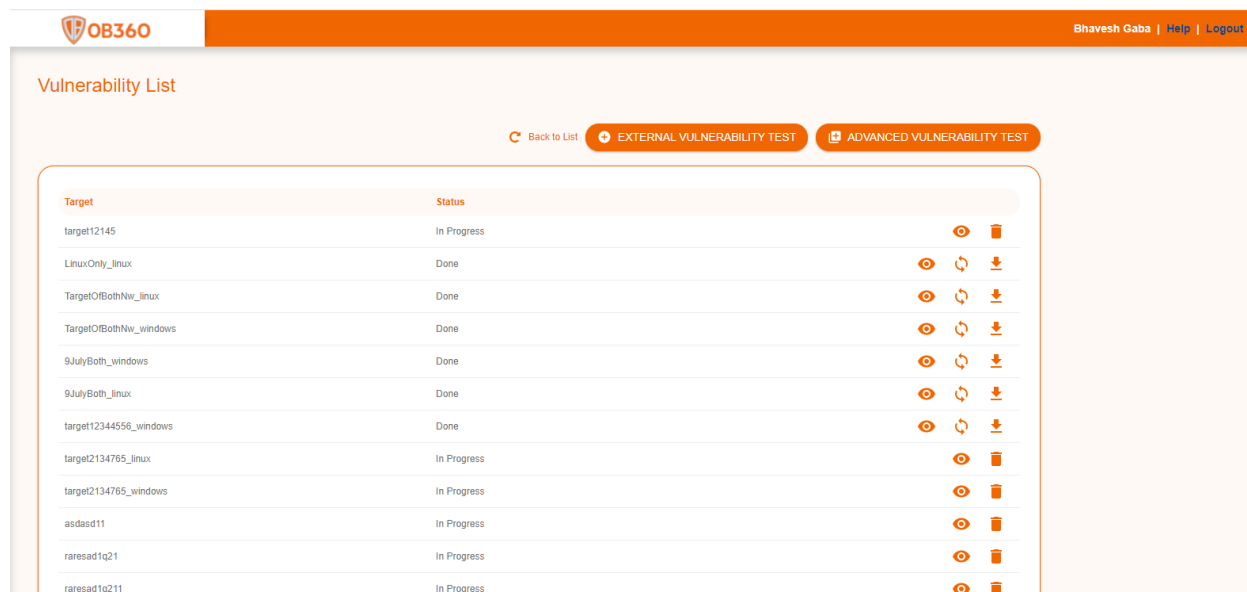


The screenshot shows the 'External Vulnerability Test for Bhavesh Client' page. It features two input fields: 'Target Name *' and 'URL / IP Range *'. Below these fields are two buttons: 'BACK' and 'SAVE'. The top navigation bar includes the OB360 logo and user information: 'Bhavesh Gaba | Help | Logout'. A copyright notice at the bottom right reads '© 2021 - All Rights Reserved, PII Secured'.

Figure : Advanced Target Screen 1

Step 15: After clicking the save button.

The page will redirect to the Report List page, where you will see the most recently generated vulnerabilities.



The screenshot shows the 'Vulnerability List' page. It features a table with columns 'Target' and 'Status'. The table lists various targets and their current status. To the right of the table are three buttons: 'Back to List', 'EXTERNAL VULNERABILITY TEST', and 'ADVANCED VULNERABILITY TEST'. The top navigation bar includes the OB360 logo and user information: 'Bhavesh Gaba | Help | Logout'.

Target	Status
target12145	In Progress
LinuxOnly_linux	Done
TargetOfBothNw_linux	Done
TargetOfBothNw_windows	Done
9JulyBoth_windows	Done
9JulyBoth_linux	Done
target12344556_windows	Done
target2134765_linux	In Progress
target2134765_windows	In Progress
asdasd11	In Progress
raresad1q21	In Progress
raresad1q211	In Progress

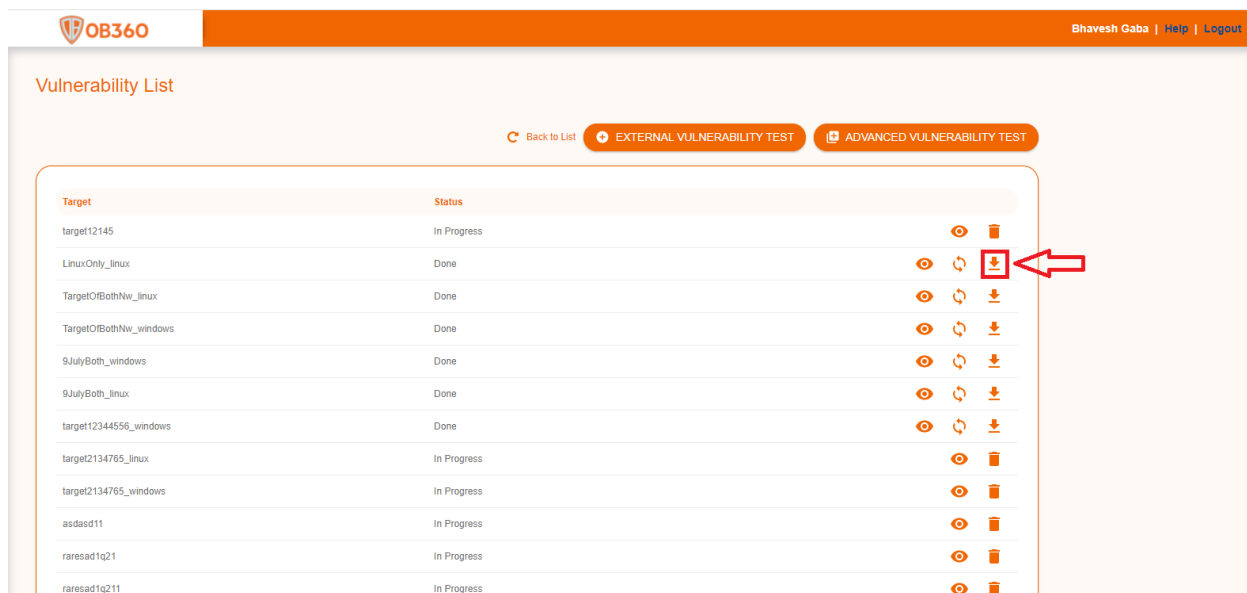
Figure : Latest Vulnerability List Screen

Status of the current Vulnerability test is 'In Progress'.

The selected task will be scanned. A report will be generated after all of the tasks have been scanned.

By clicking the view button, you can see the status of the created target.

When all the tasks have been completed, the status will be changed to “Done”.



















































Target	Status	Actions
target12145	In Progress	   
LinuxOnly_linux	Done	   
TargetOIBothNw_linux	Done	   
TargetOIBothNw_windows	Done	   
9JulyBoth_windows	Done	   
9JulyBoth_linux	Done	   
target12344556_windows	Done	   
target2134765_linux	In Progress	   
target2134765_windows	In Progress	   
asdasd11	In Progress	   
raresad1q21	In Progress	   
raresad1q211	In Progress	   

Figure : Vulnerability List Screen

Now you can download the report by clicking the ‘Download’ button . You will get the report in zip format.

Extract the zip and you will get all the reports generated for your task.

This completes the OB360 flow.