



OB360

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.

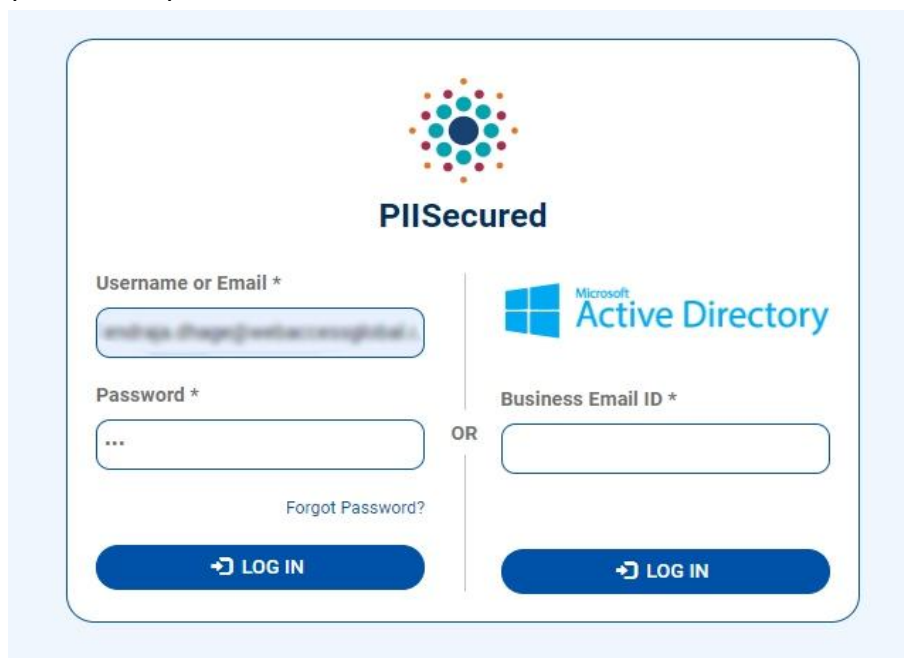
You will need the following information from your Network Administrator to do the **External Vulnerability Test**.

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://access.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 and a 'LOG IN' button. The right path is for 'Business Email ID *' and includes a 'Microsoft Active Directory' logo and a 'LOG IN' button. An 'OR' separator is placed between the two paths.

Figure 1: Login Screen

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

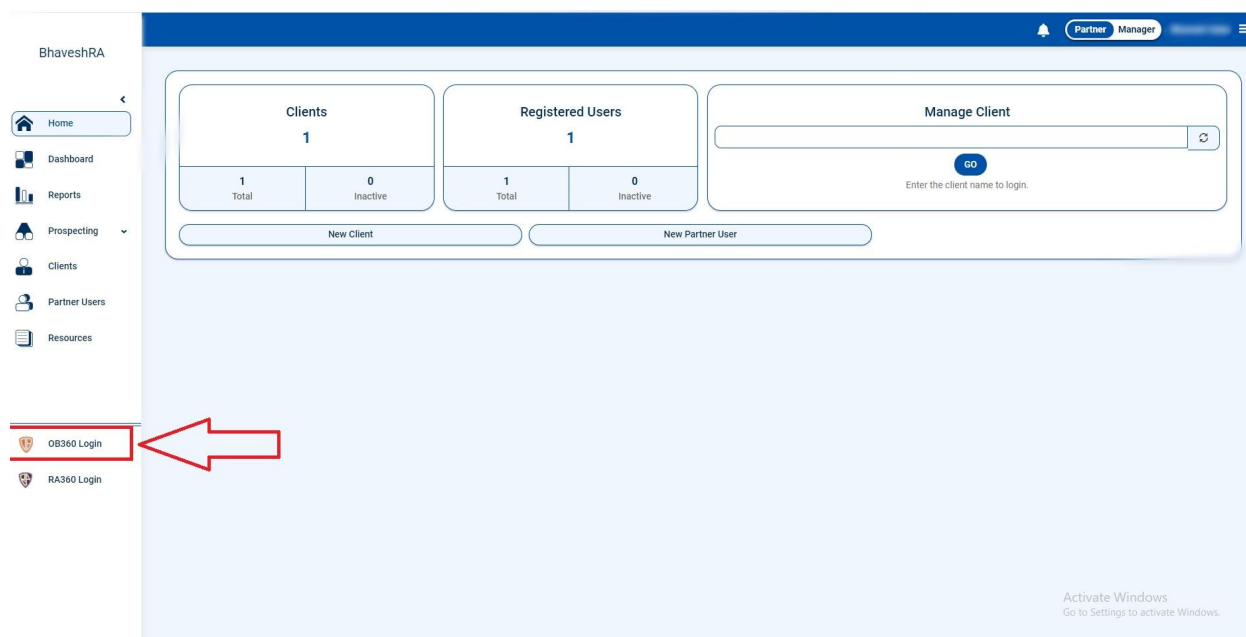


Figure 2: Home Screen

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

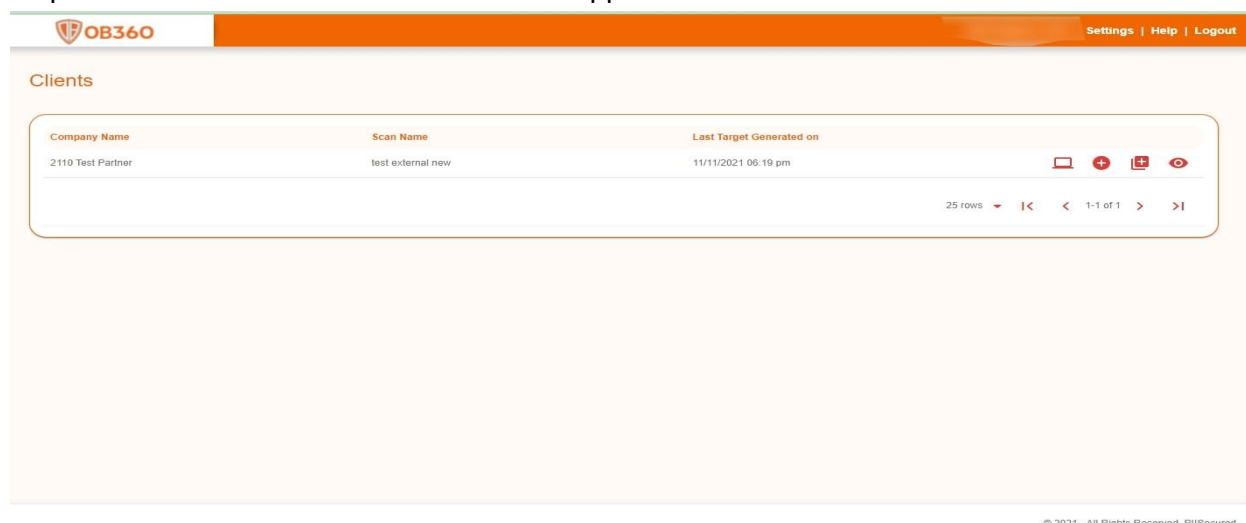


Figure 3: Clients Screen

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

1. **Schedule Test configuration from settings - [Step 4](#)**
2. **Create Penetration Testing [Step 8](#)**
3. **Create External Vulnerability Test - [Step 10](#)**
4. **Create Advanced Vulnerability Test - [Step 14](#)**
5. **View Test Details- [Step 22](#)**

There are seven different levels for the status. The following is a description of the target's status.

Scheduled	The task has been scheduled for scanning based on your times that have been set. Once it starts the status will be updated.
In Progress	The task is currently being scanned and assessed for recommendations
Scan Completed	The task has successfully run and generated data for the test. The report generation process should begin shortly.
Generating Report	Test reports are being generated based on the scanned data. Should be available for download over the next 24-48 hours.
Report Generated	Vulnerability Test Reports have been generated and are now available for download.
Failed	The task was unsuccessful due to an error. Please contact partner support.

Scheduling Configuration

Step 4: To create a Scheduler click on '**Settings**'

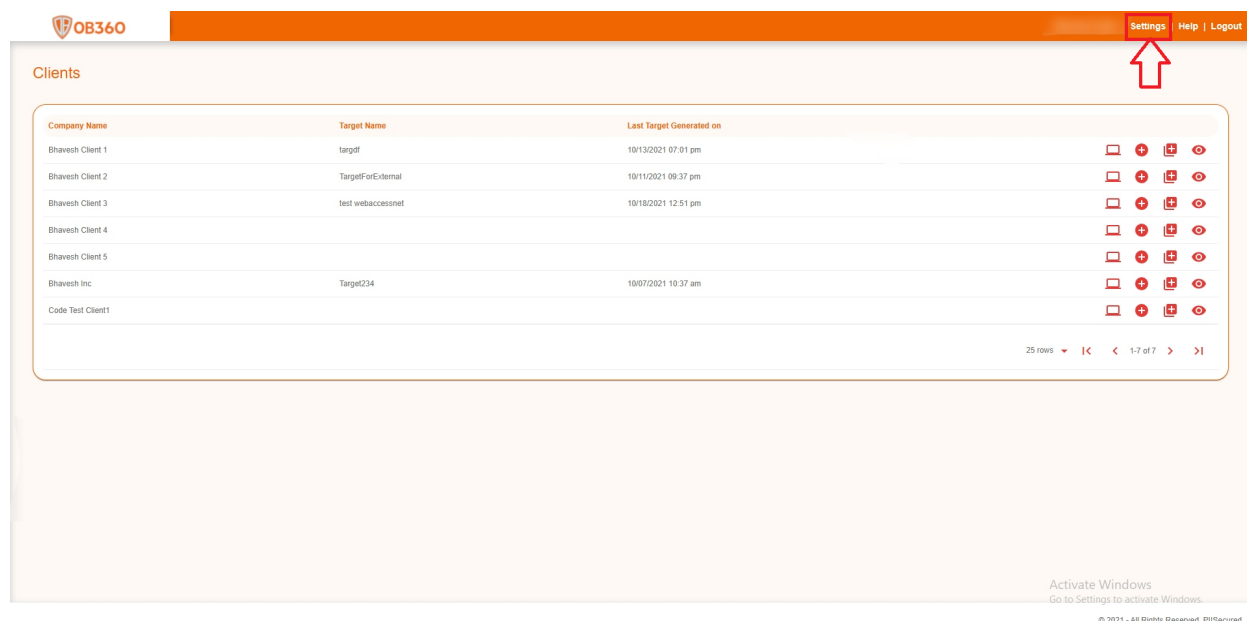


Figure 4: Client List Screen

Step 5: Now you will redirect to the Scheduling Configuration page here you will see the list of scheduled configurations to create a new one click on add **SCHEDULE**

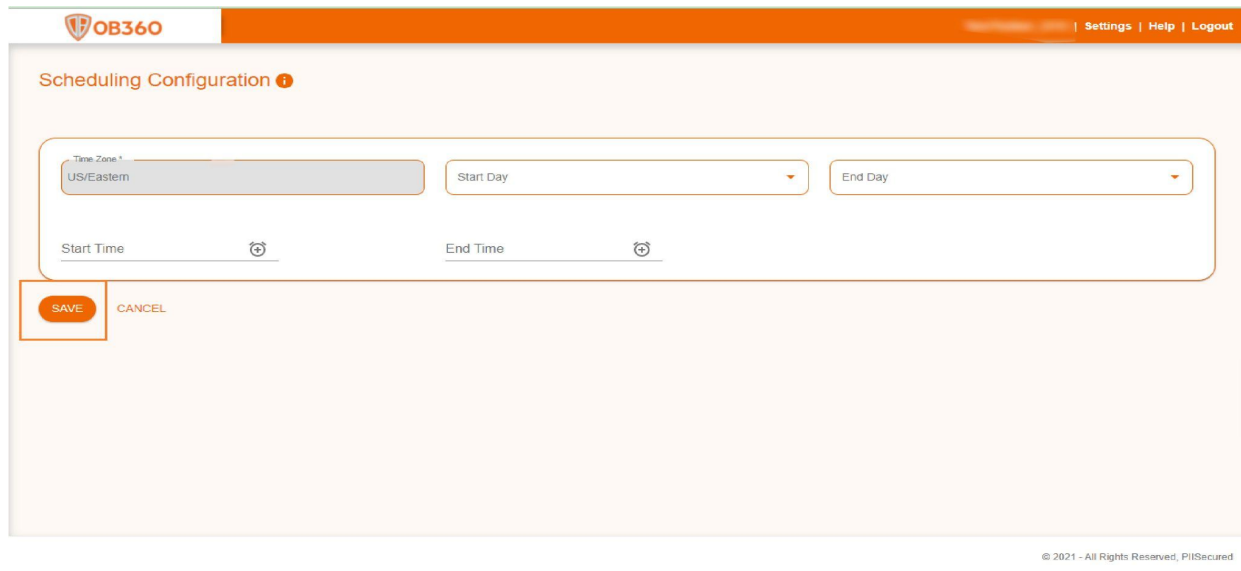


Figure 5: Scheduling List Screen

Step 6: Now you will redirect to the Add Scheduler Page. Do the following steps to create a scheduler.

- Enter the Start Date,
- Enter the End Date
- Enter the Start Time
- Enter the End Time

Then click **Save**

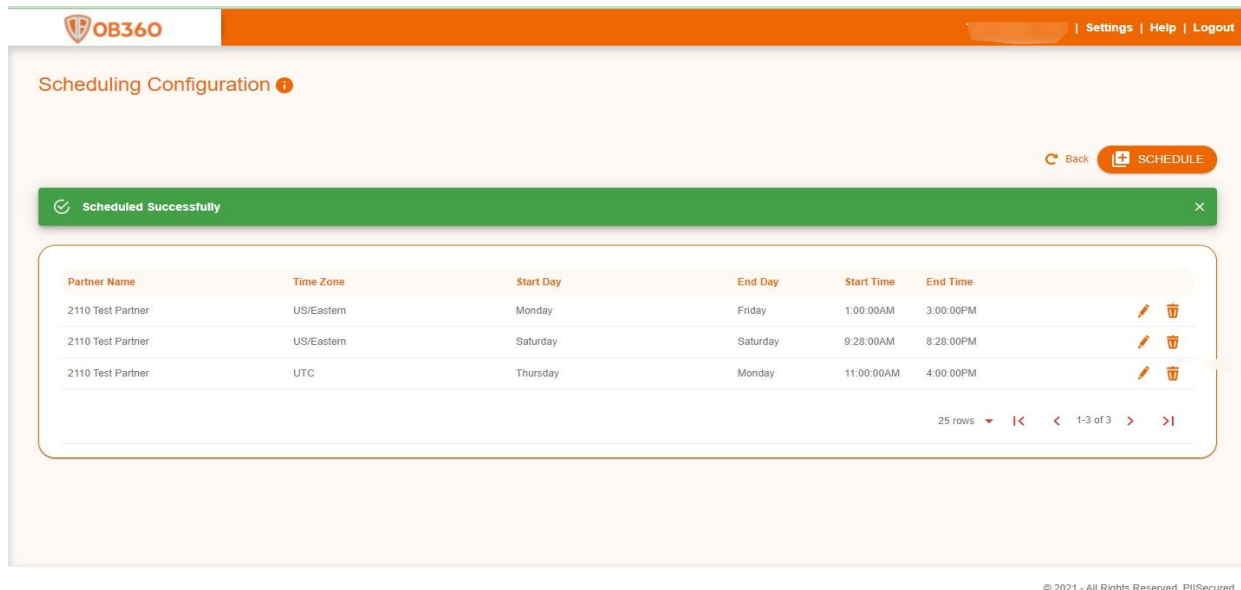


The screenshot shows the 'Scheduling Configuration' form in the OB360 interface. The form includes fields for 'Time Zone' (set to US/Eastern), 'Start Day' (dropdown), 'End Day' (dropdown), 'Start Time' (with a clock icon), and 'End Time' (with a clock icon). At the bottom left, there are 'SAVE' and 'CANCEL' buttons. The top navigation bar includes the OB360 logo and links for Settings, Help, and Logout. A footer note at the bottom right states '© 2021 - All Rights Reserved, PII Secured'.

Figure 6: Scheduling Form Screen

Step 7: After clicking the save button.

The page will redirect to the Scheduler List page, where you will see the most recently generated Scheduler. You can edit and delete the created scheduler from the same.



The screenshot shows the 'Scheduler List' screen in the OB360 interface. At the top, there is a green success message: 'Scheduled Successfully'. Below this is a table with columns: Partner Name, Time Zone, Start Day, End Day, Start Time, and End Time. The table contains three rows of data. At the bottom right of the table, there are pagination controls showing '25 rows' and '1-3 of 3'. The top navigation bar includes the OB360 logo and links for Settings, Help, and Logout. A footer note at the bottom right states '© 2021 - All Rights Reserved, PII Secured'.

Partner Name	Time Zone	Start Day	End Day	Start Time	End Time
2110 Test Partner	US/Eastern	Monday	Friday	1:00:00AM	3:00:00PM
2110 Test Partner	US/Eastern	Saturday	Saturday	9:28:00AM	8:28:00PM
2110 Test Partner	UTC	Thursday	Monday	11:00:00AM	4:00:00PM

Figure 7: Scheduling List Screen

Create Penetration Test

Step 8: To create a new Penetration test click on 'Create Pentest button.

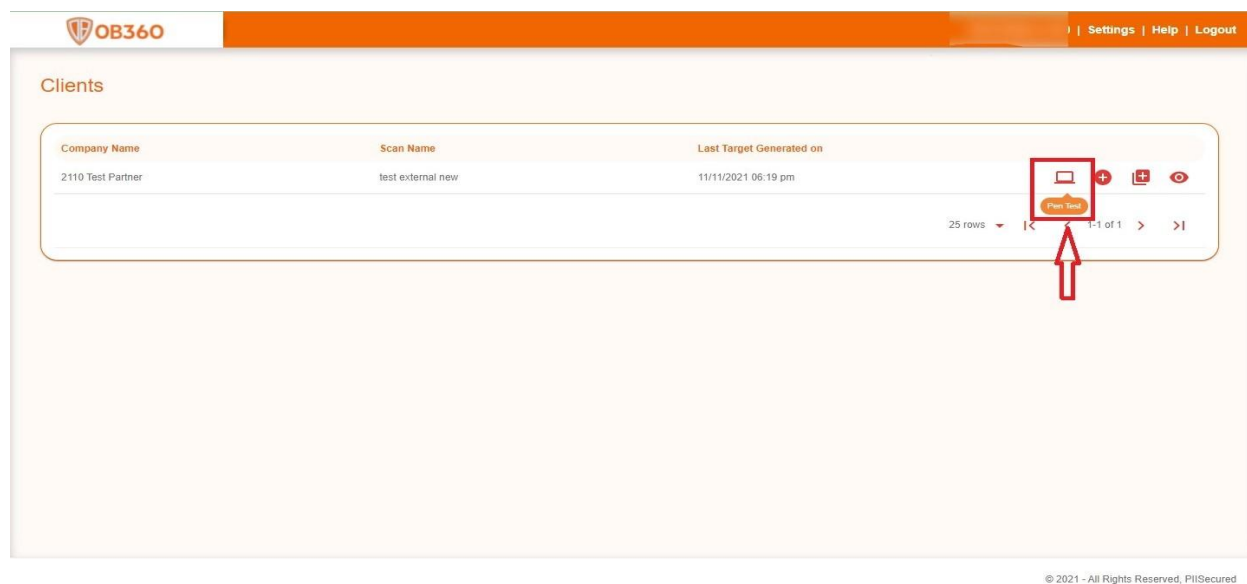


Figure 8: Client List Screen

Step 9: Now you will redirect to the Pentest page. Do the following steps to create a pentest.

- Enter the Company Name,
- URL / IP
- Select ScanType

Then click **Queue Scan**

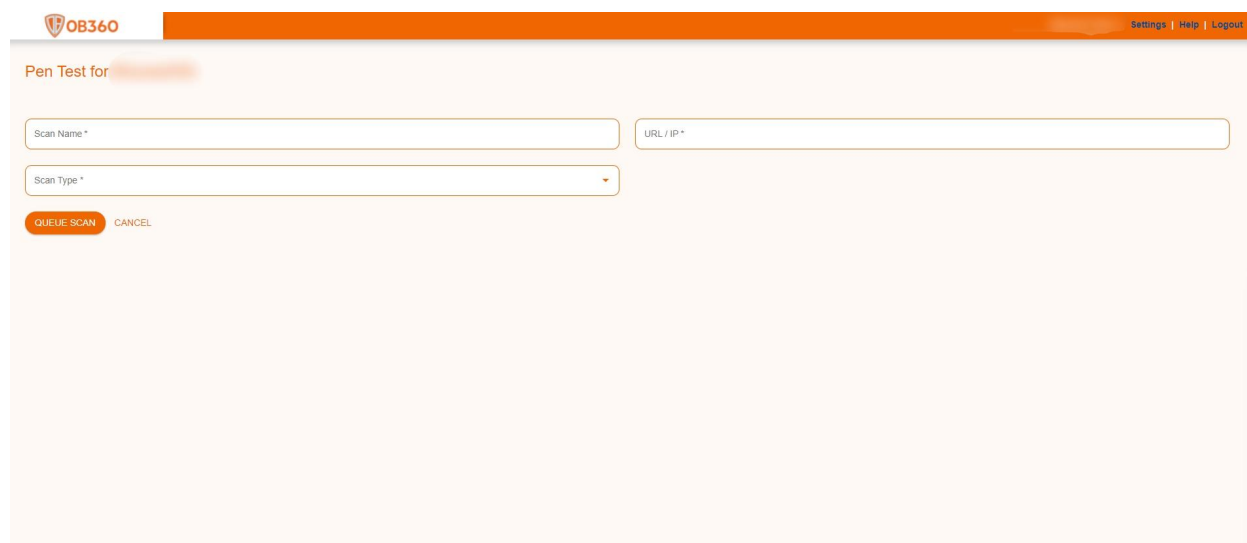


Figure 9: Add Pentest Screen

After clicking the **Queue Scan** button.

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

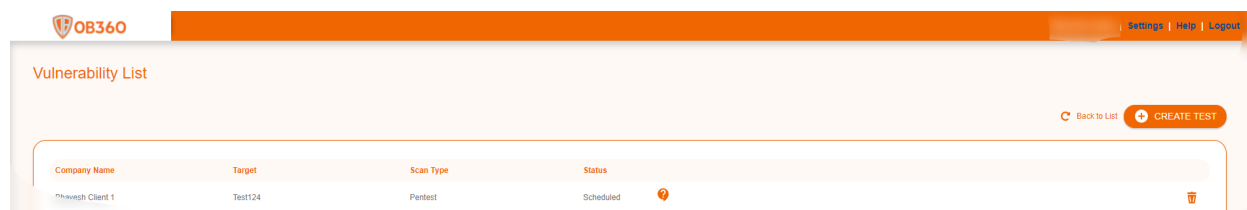


Figure 10: Vulnerability List Screen

Once the report is generated and ready to download, the respective partner will get the notification by email mentioned in [Email Notification](#).

External Vulnerability Test

Step 10: To create a new External vulnerability test click on 'Create External vulnerability button.

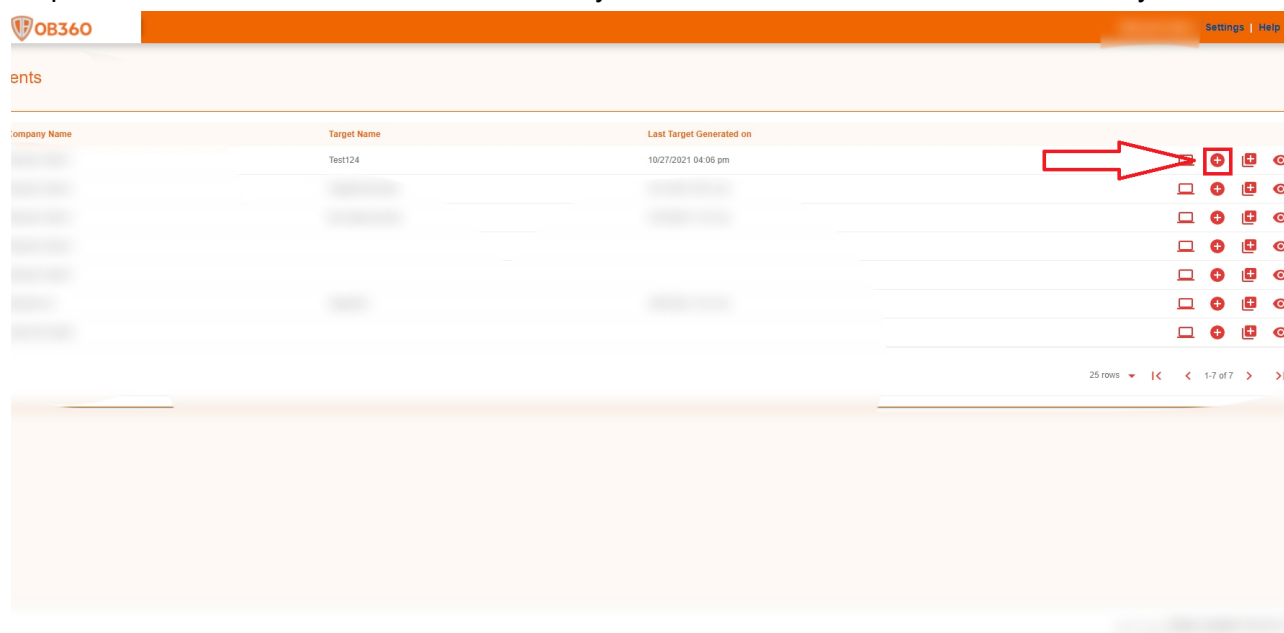


Figure 11: Client List Screen

Step 11: Now you will redirect to the External target page. Do the following steps to create a target.

- Enter the Target Name(Enter any appropriate name),
- IP Range or Domain Name
 - Single IP Address (e.g. 192.168.x.xx)
 - Multiple IP Address (e.g. 192.168.x.0-255 or 192.168.x.0, 192.168.x.2)
 - For Domain/URL (e.g. domainname.com]

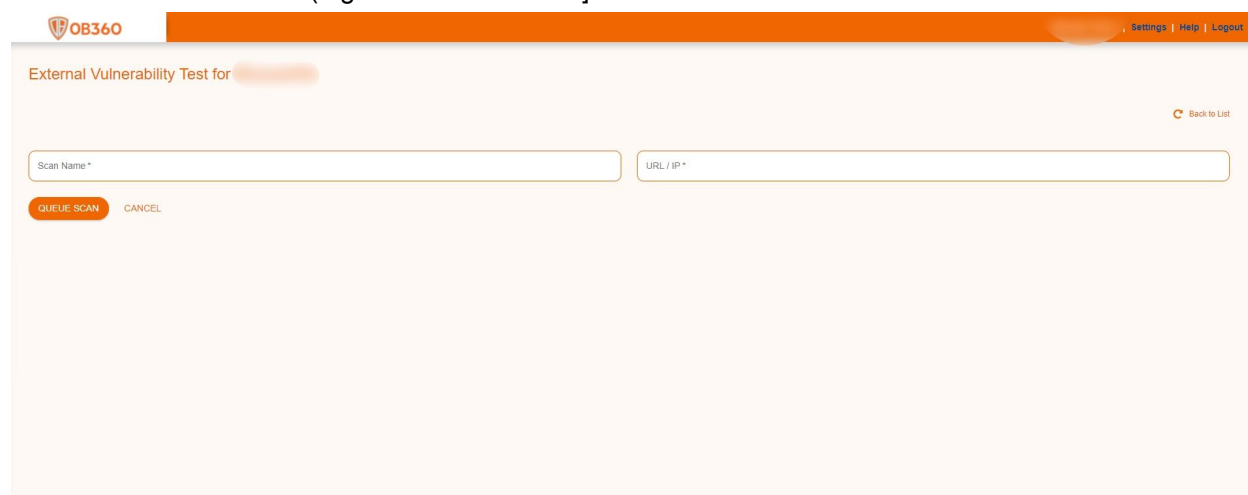
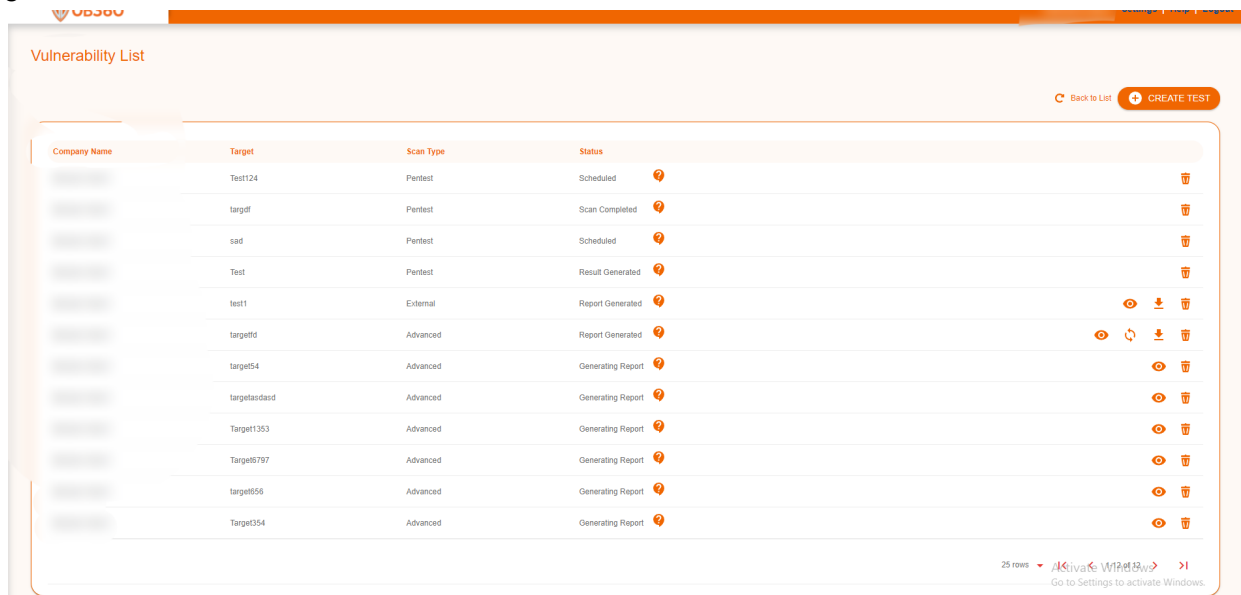


Figure 12 : External Target Screen

Step 12: After clicking the **Queue Scan** 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' interface. It features a table with columns: Company Name, Target, Scan Type, and Status. The table lists several scan tasks with their respective statuses. At the top right, there are buttons for 'Back to List' and 'CREATE TEST'. At the bottom right, there is a pagination bar showing '25 rows' and a Windows activation watermark.

Company Name	Target	Scan Type	Status
	Test124	Penetest	Scheduled
	targetf	Penetest	Scan Completed
	sad	Penetest	Scheduled
	Test	Penetest	Result Generated
	test1	External	Report Generated
	targettd	Advanced	Report Generated
	target54	Advanced	Generating Report
	targetasdaad	Advanced	Generating Report
	Target1353	Advanced	Generating Report
	Target8797	Advanced	Generating Report
	targetf56	Advanced	Generating Report
	Target354	Advanced	Generating Report

Figure 13: Latest Vulnerability List Screen

The status of the current Vulnerability test is '[Scheduled](#)'.

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 '[Report Generated](#)'.

Once the report is generated and ready to download, the respective partner will get the notification by email mentioned in [Email Notification](#).

Step 13: Now you can download the report by clicking the 'Download' button. You will get the report in zip format.

Vulnerability List

[Back to List](#) [+ CREATE TEST](#)


























Company Name	Target	Scan Type	Status	
Company 1	Test124	PenTest	In Progress	 
Company 1	target0	PenTest	Result Generated	 
Company 1	sad	PenTest	Scheduled	 
Company 1	Test	PenTest	Result Generated	 
Company 1	Target webaccess 2811	Advanced	Scheduled	  
Company 1	Target Html client test	Advanced	Generating Report	  
Company 1	test1	External	Report Generated	   
Company 1	target0d	Advanced	Report Generated	   
Company 1	target54	Advanced	Generating Report	  

Figure 14: Vulnerability List Screen

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

Advanced Vulnerability Test

Step 14: Click on the "Advanced Vulnerability Test" icon for creating a new Advanced Vulnerability Test.

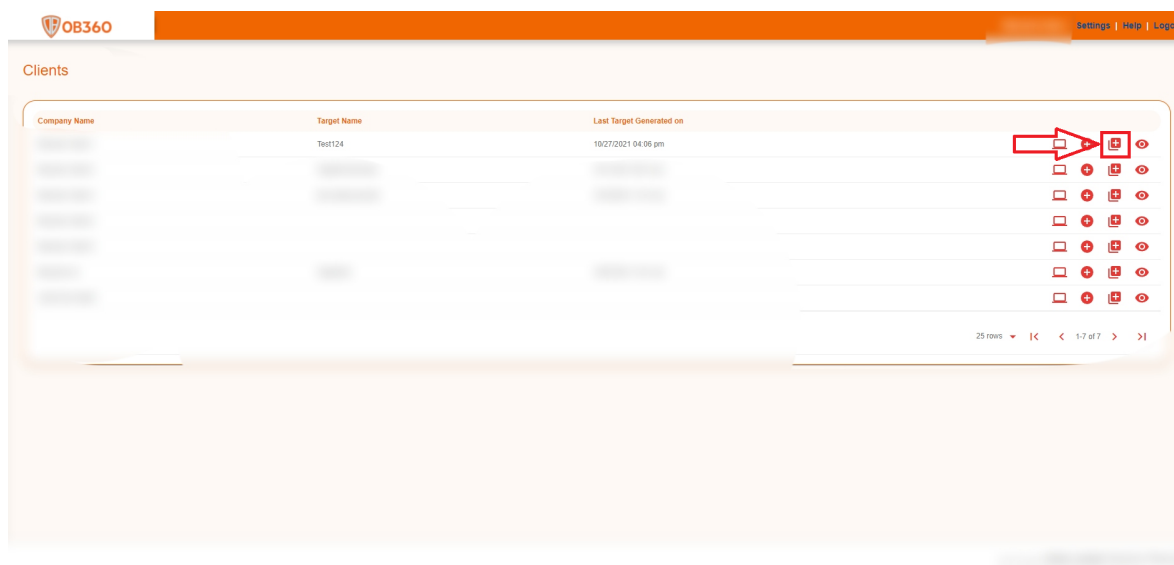
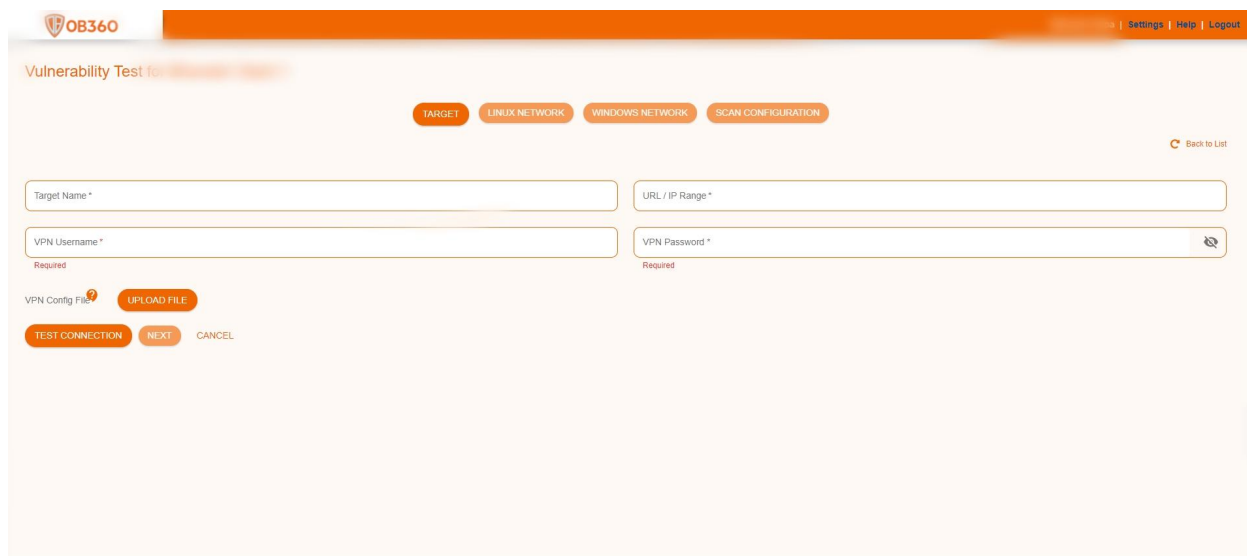


Figure 15: Clients Screen 2

Step 15: Now you will be redirected to the target page. Do the following steps to create a target.

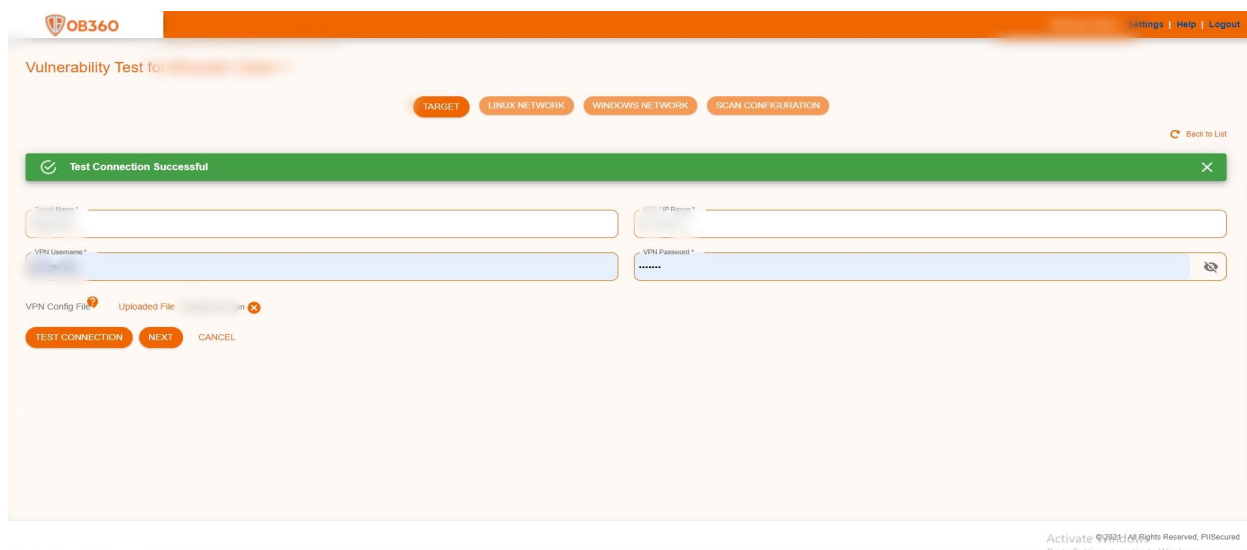
- Enter the Target Name, VPN Username, VPN Password and IP Range
 - Single IP Address (e.g. 192.168.x.xx)
 - Multiple IP Address (e.g. 192.168.x.0-255 or 192.168.x.0, 192.168.x.2)
 - For Domain/URL (e.g. domainname.com)
- Upload VPN configuration file is given by your network administrator (either .ovpn or .tgz format)
- Click on the 'Test Connection' button.



The screenshot shows the 'Vulnerability Test for [redacted]' interface. At the top, there are four tabs: 'TARGET', 'LINUX NETWORK', 'WINDOWS NETWORK', and 'SCAN CONFIGURATION'. Below the tabs, there are four input fields: 'Target Name *', 'URL / IP Range *', 'VPN Username *', and 'VPN Password *'. The 'VPN Username' and 'VPN Password' fields have a 'Required' label below them. There is an 'UPLOAD FILE' button next to the 'VPN Config File' label. At the bottom, there are three buttons: 'TEST CONNECTION', 'NEXT', and 'CANCEL'. A 'Back to List' link is in the top right corner.

Figure 16: Target Screen

After a 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 [redacted]' interface after a successful test connection. A green banner at the top says 'Test Connection Successful'. The input fields for 'Target Name', 'URL / IP Range', 'VPN Username', and 'VPN Password' are now highlighted in light blue. The 'VPN Config File' label now has an 'Uploaded File' status with a download icon. The 'TEST CONNECTION' button is disabled, and the 'NEXT' button is now enabled. The 'CANCEL' button remains disabled. The 'Back to List' link is still present in the top right corner.

Figure 17: 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 16: 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?'

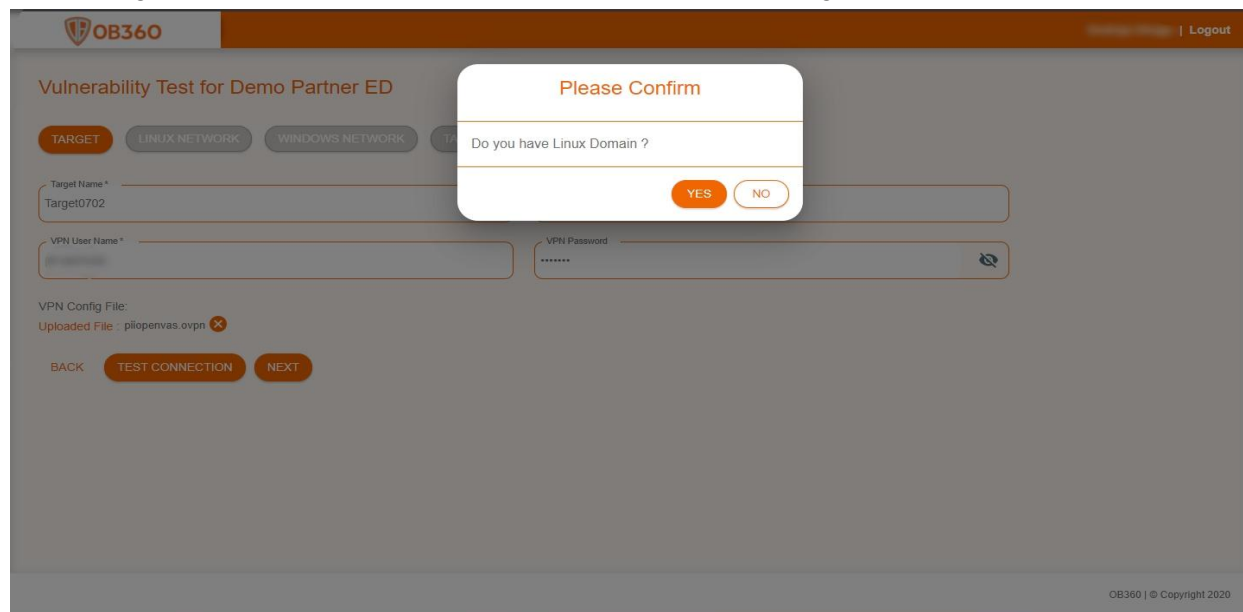


Figure 18: Linux Confirmation Screen

Click on 'Yes' if you have a Linux network else click on 'No'

On click of 'Yes' you will redirect to [step 17](#).

On click of 'No' you will redirect to [step 18](#)

Step 17: 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
Eg: Single IP Address (e.g. 192.168.x.xx)
Multiple IP Address (e.g. 192.168.x.0-255 or 192.168.x.0, 192.168.x.2)
- Click on the 'Test Connection' button.

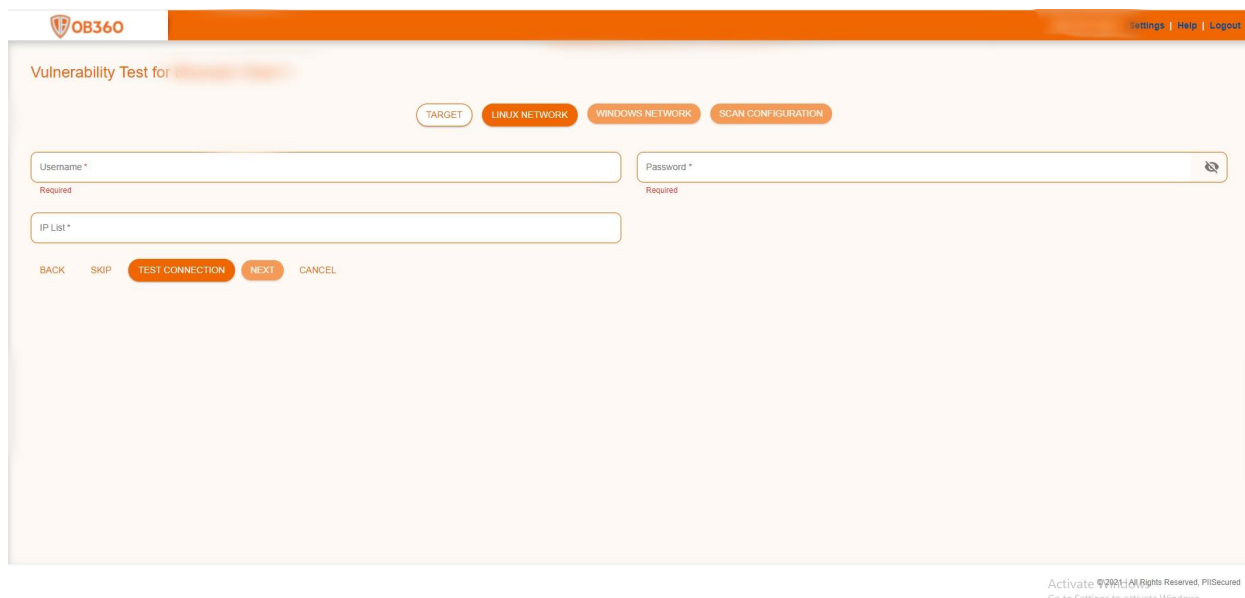


Figure 19: Linux Network Screen

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

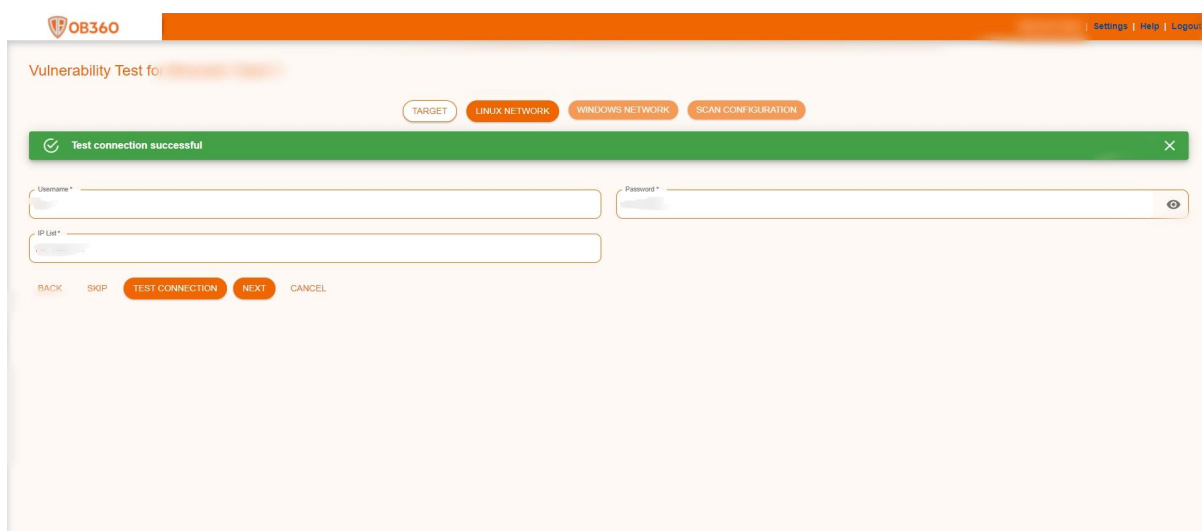


Figure 20: Linux Success Screen

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

Step 18: 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?'

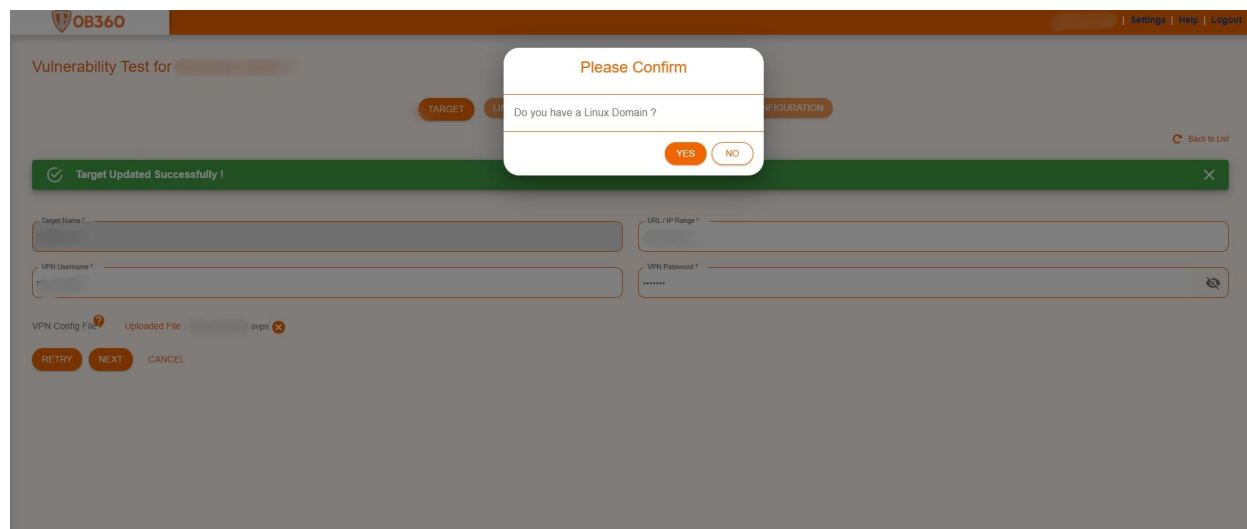


Figure 21: Windows Confirmation Screen

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

On click of 'Yes' you will redirect to [step 19](#).

On click of 'No' you will redirect to [step 20](#).

Step 19: Now you will redirect to the windows network page.

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

- Enter network administrator Username and Password, Domain Name
- Enter IP address list or IP range
Eg: Single IP Address (e.g. 192.168.x.xx)
Multiple IP Address (e.g. 192.168.x.0-255 or 192.168.x.0, 192.168.x.2)
- Click on the 'Test Connection' button.

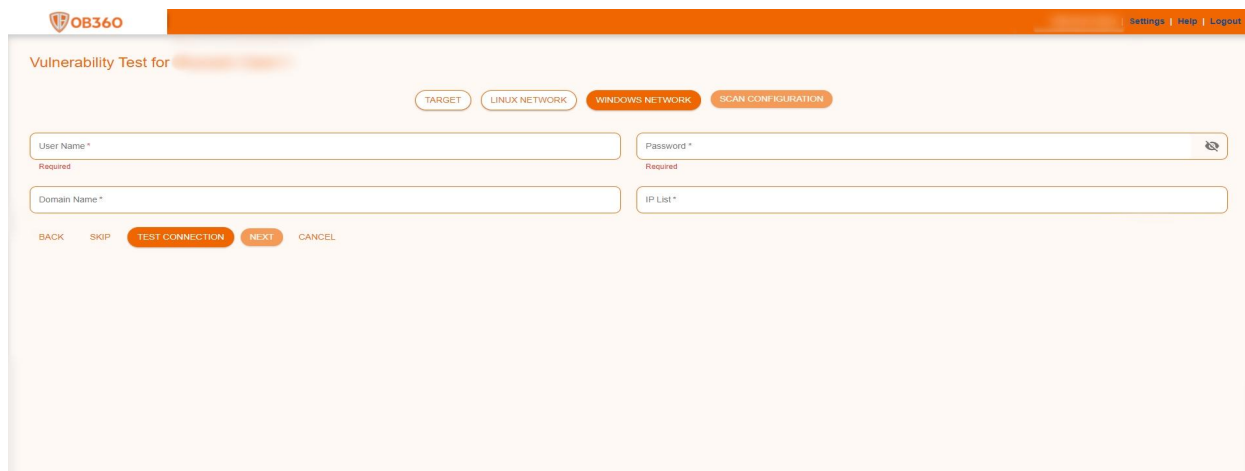


Figure 22: Windows Network Screen

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

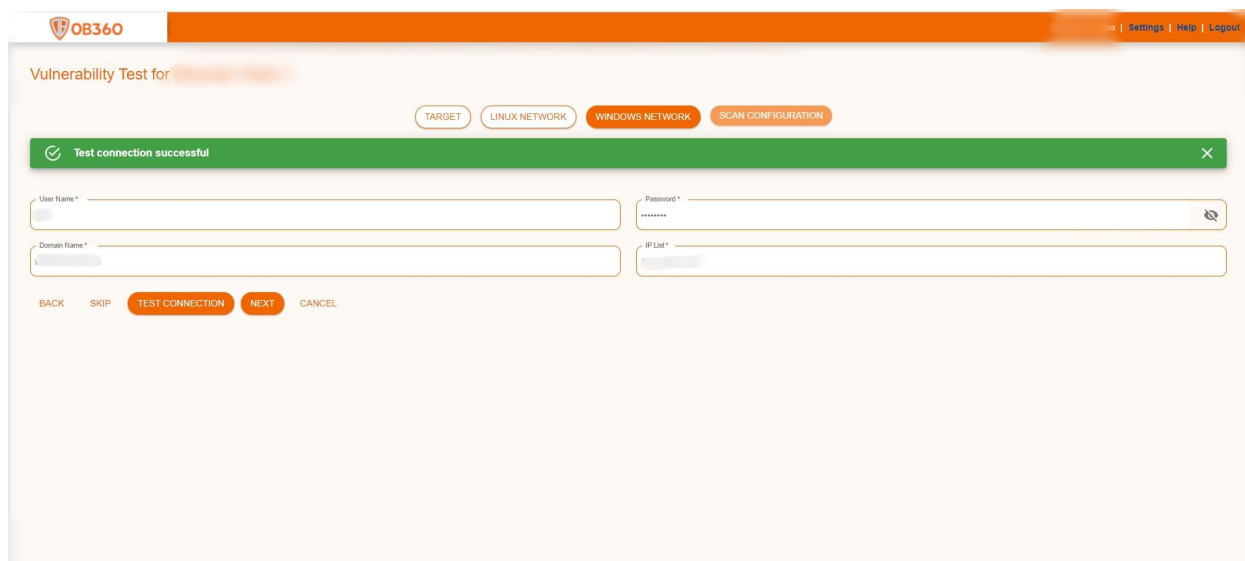


Figure 23: Windows Success Screen

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

Step 20: After the Next button is enabled click on it.

Now you will redirect to the Scan Configuration page.

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

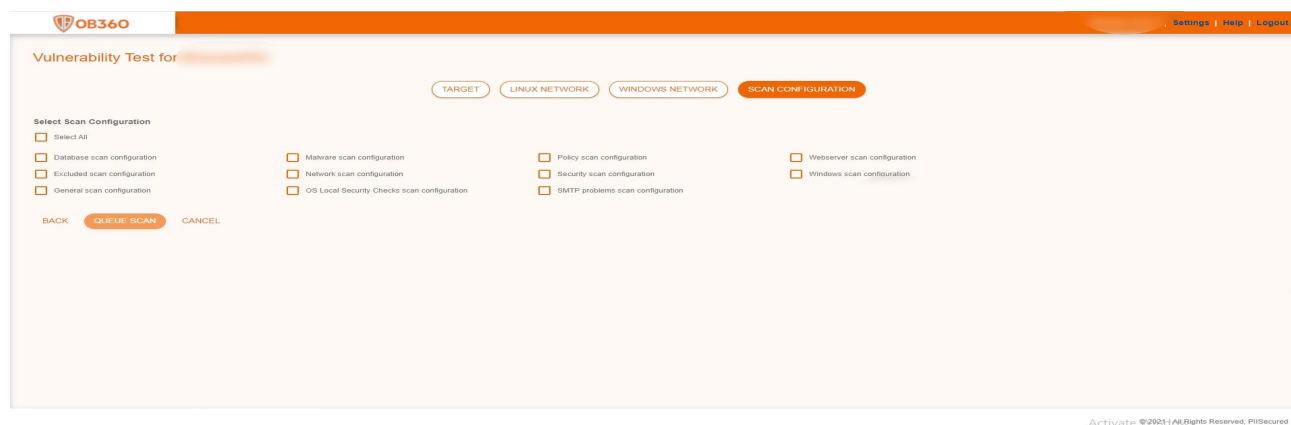


Figure 24: Scan Configuration Screen

Step 21: After clicking the **Queue scan** button.

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

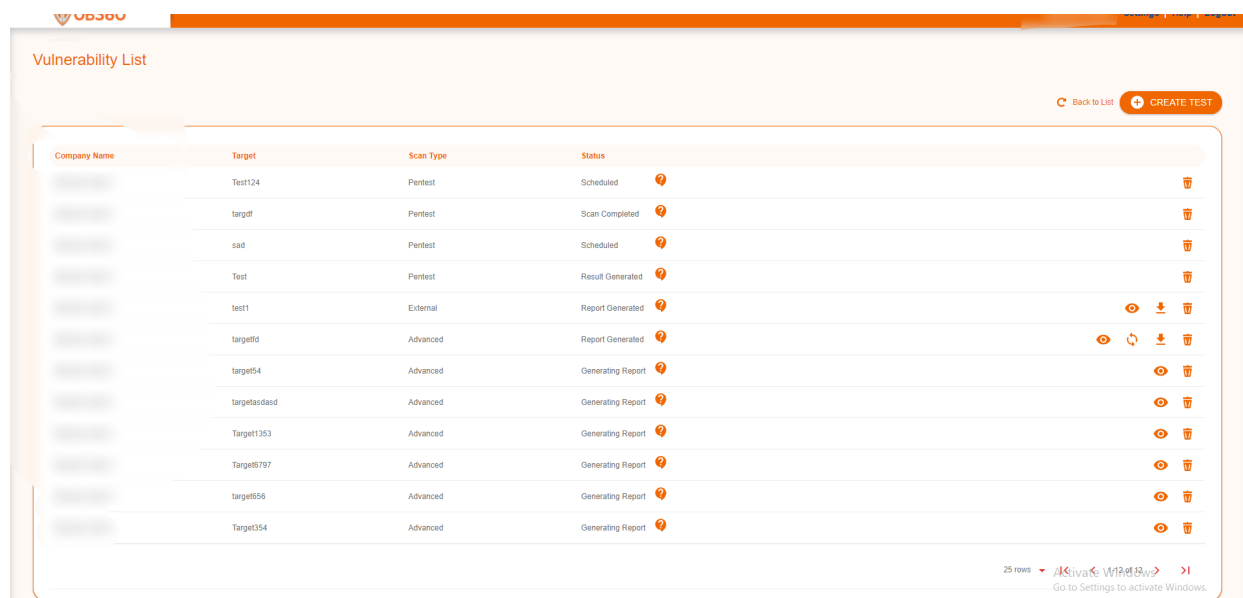


Figure 25: Vulnerability List Screen

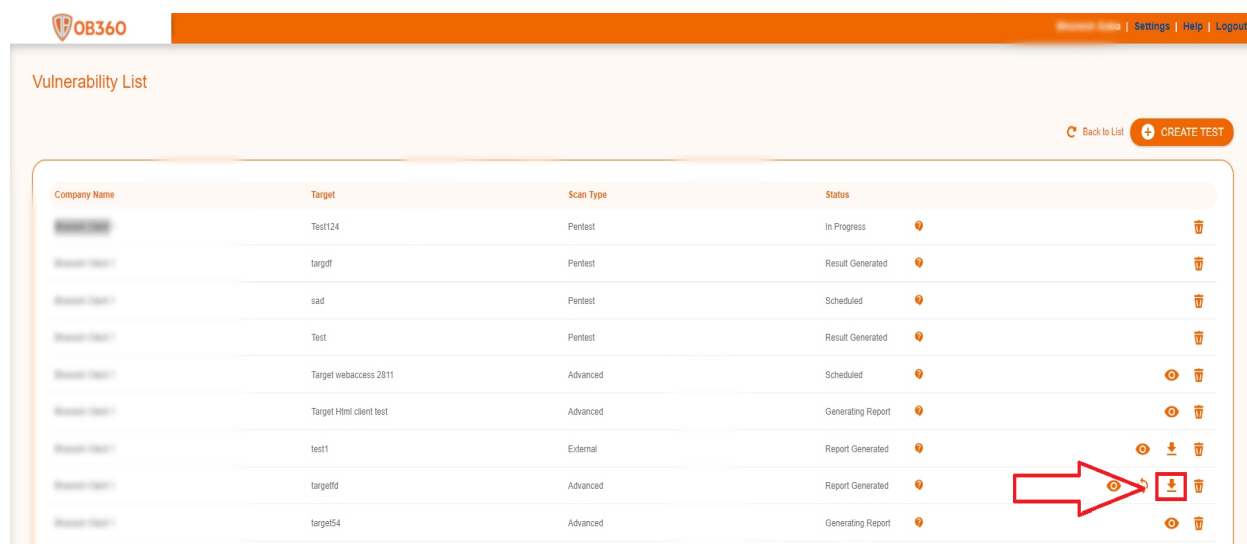
Status of the current Vulnerability test is '[Scheduled](#)'.

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 '[Report Generated](#)' .

Once the report is generated and ready to download, the respective partner will get the notification by email mentioned in [Email Notification](#).



Company Name	Target	Scan Type	Status	Action
[Redacted]	Test124	Pentest	In Progress	[View] [Delete]
[Redacted]	targetf	Pentest	Result Generated	[View] [Delete]
[Redacted]	sad	Pentest	Scheduled	[View] [Delete]
[Redacted]	Test	Pentest	Result Generated	[View] [Delete]
[Redacted]	Target webaccess 2811	Advanced	Scheduled	[View] [Delete]
[Redacted]	Target Html client test	Advanced	Generating Report	[View] [Delete]
[Redacted]	test1	External	Report Generated	[View] [Download] [Delete]
[Redacted]	targetf5d	Advanced	Report Generated	[View] [Download] [Delete]
[Redacted]	targetf54	Advanced	Generating Report	[View] [Delete]

Figure 26: 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.

View Vulnerability Test

Step 22: Click on the "View Vulnerability Tests" icon for Viewing a Vulnerability test.

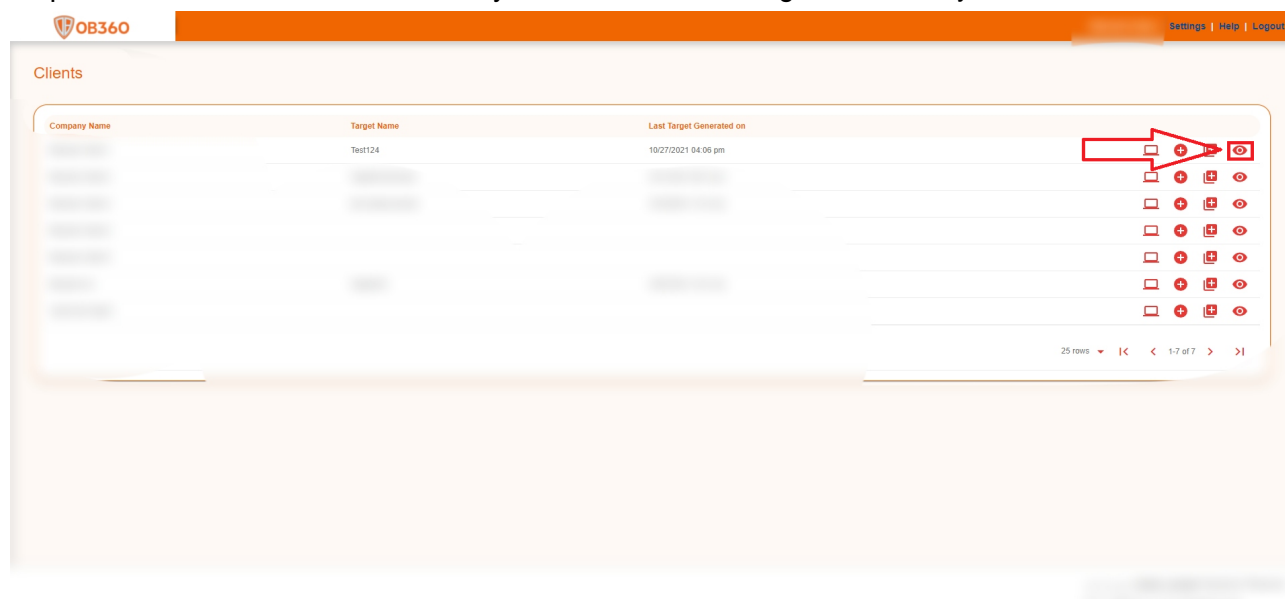


Figure 27: Client Screen

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

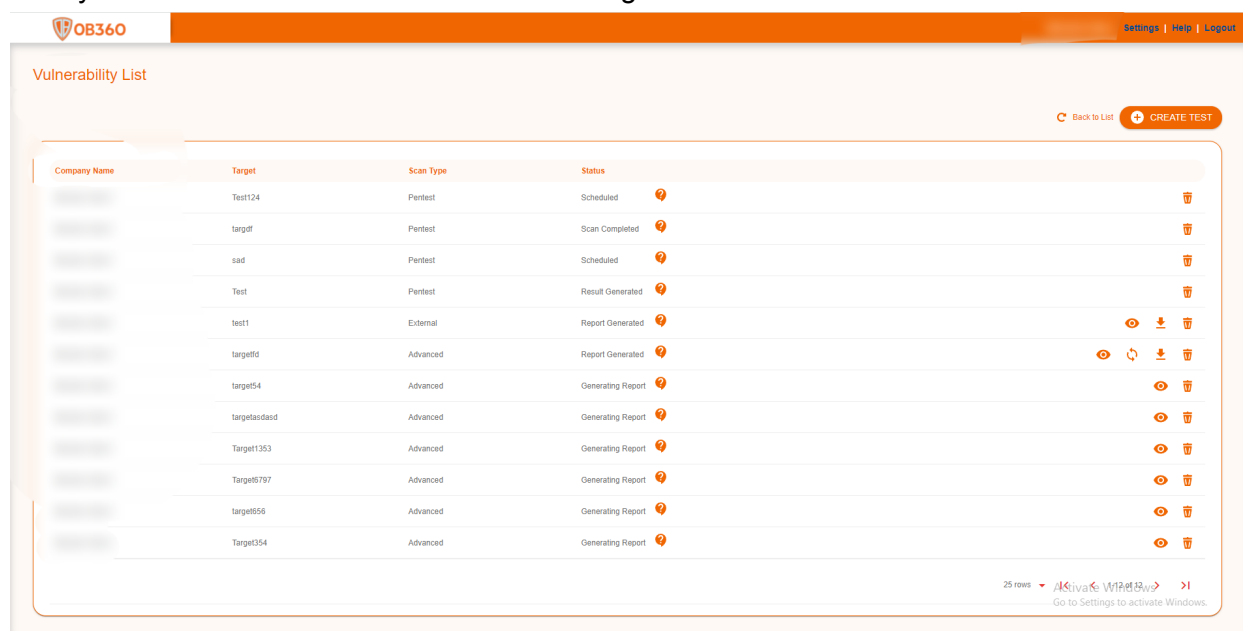
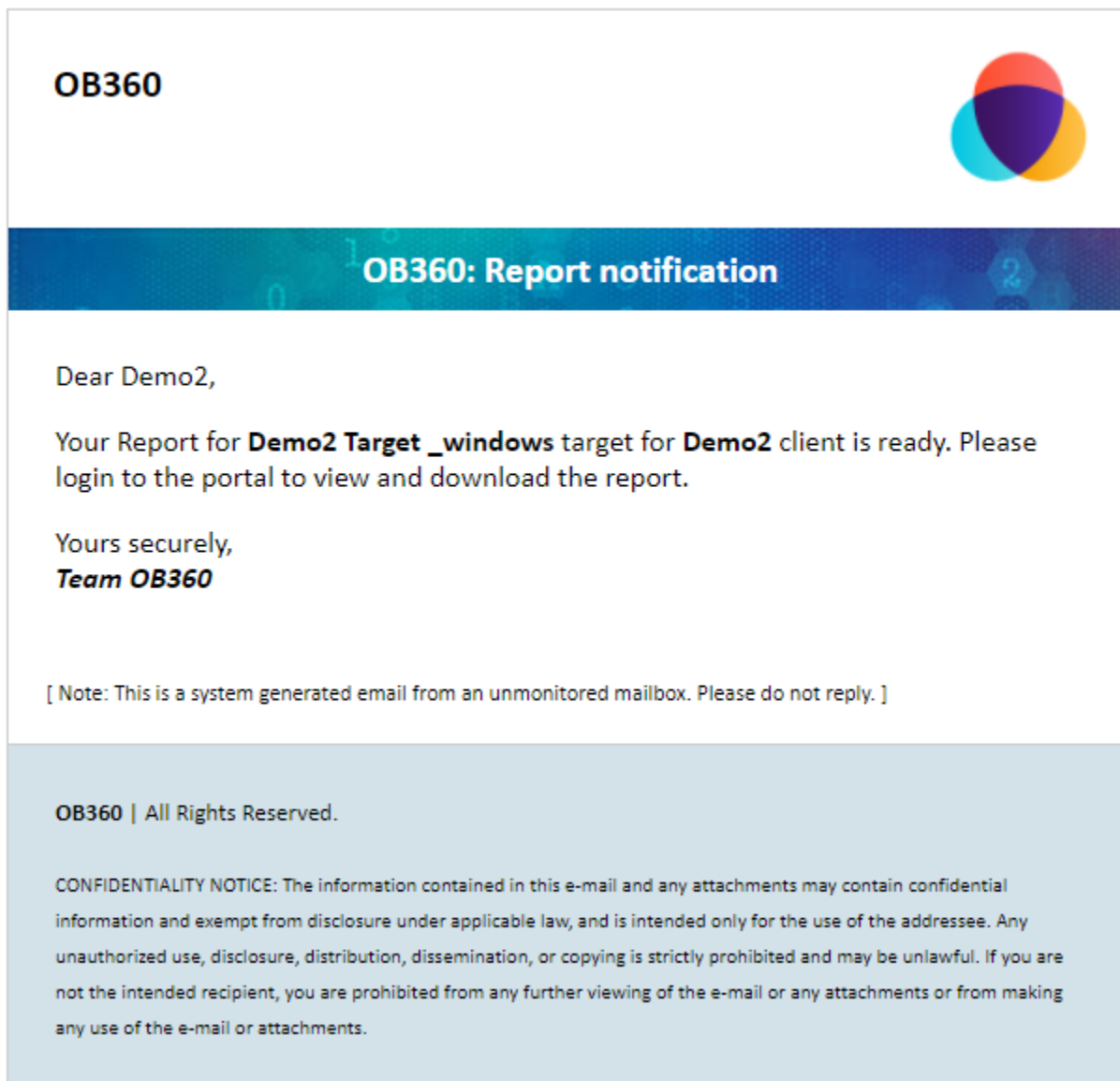


Figure 28: Vulnerability List Screen 1

Email Notification:

Once the report is generated and ready to download, the respective partner will get the notification by email as “**OB360: Report Notification**”.



You can now download the respective reports from the portal.