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 PIISecured portal and use your partner user credentials to log in.
URL: https://access.piisecured.com/

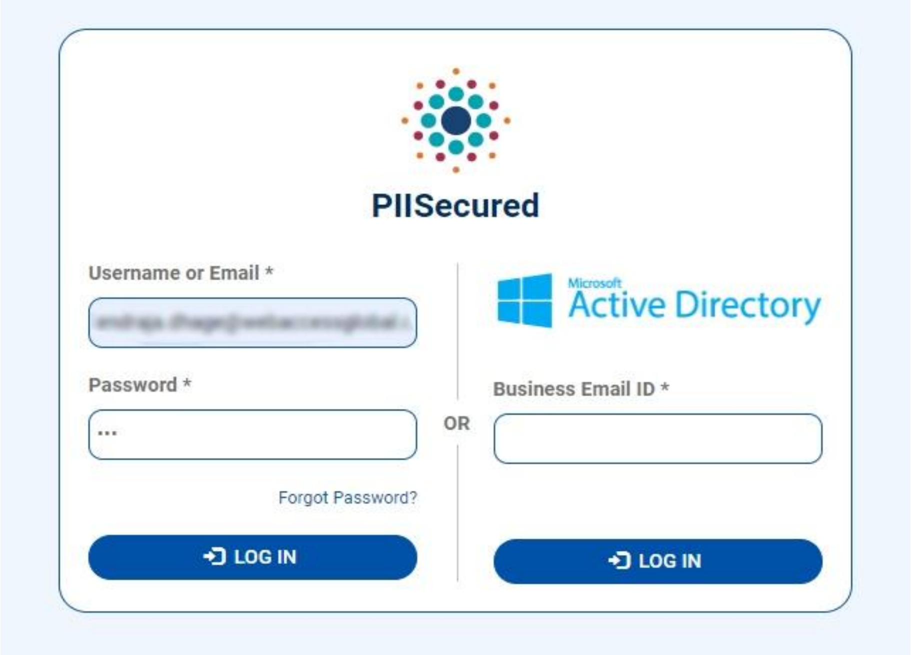


Figure 1: Login Screen

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

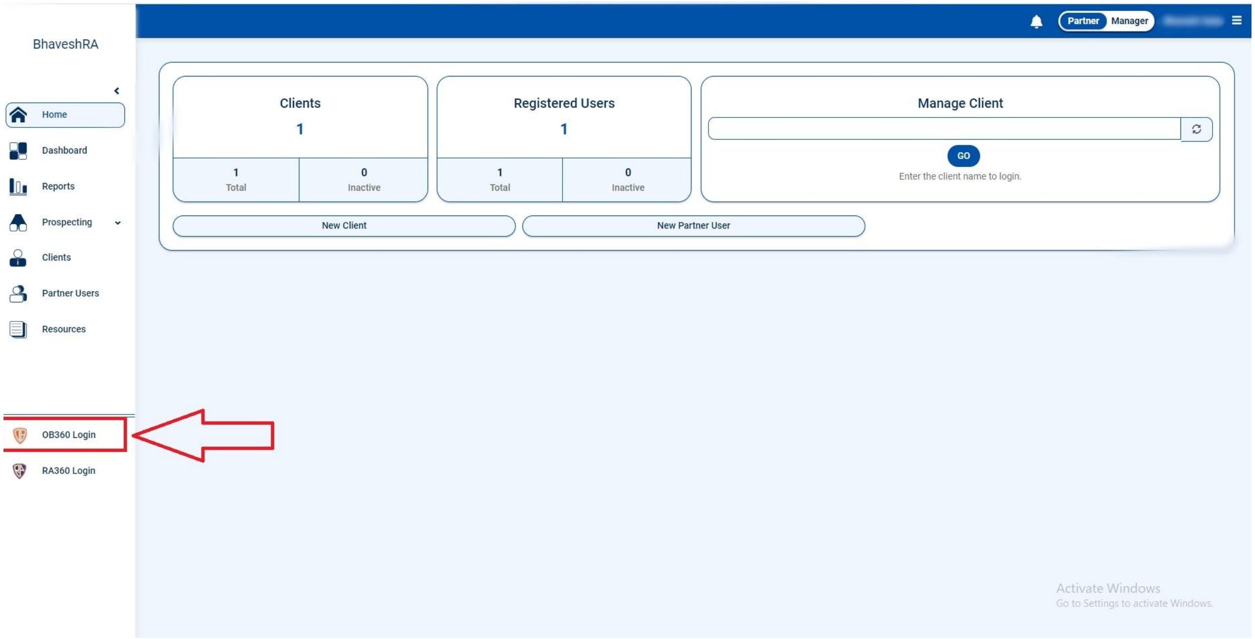
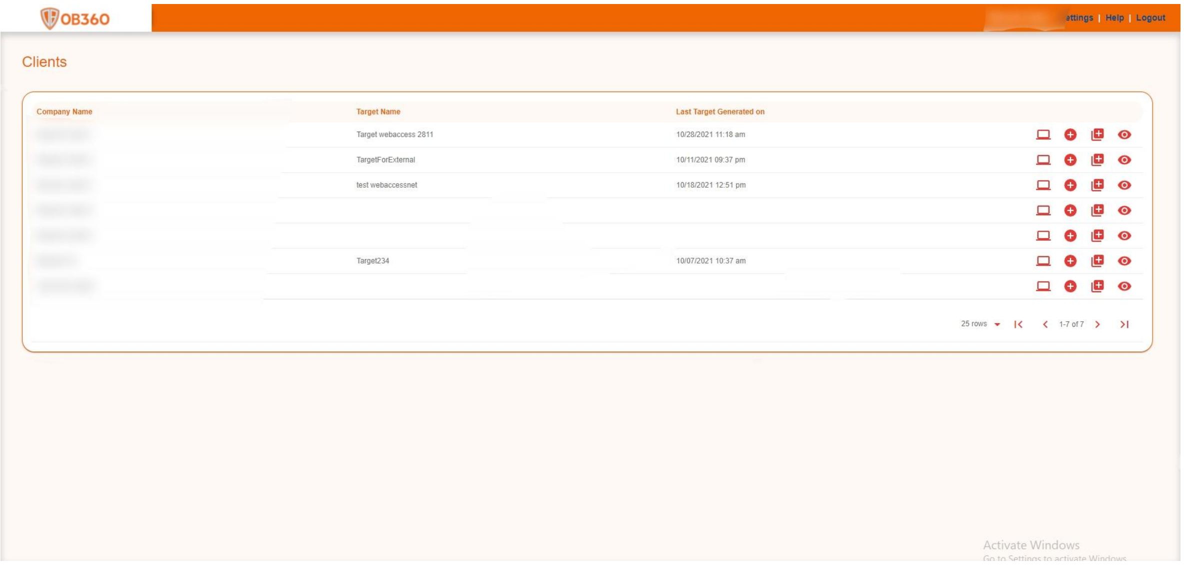


Figure 2: Home Screen

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



Clients

Company Name	Target Name	Last Target Generated on
[redacted]	Target webaccess 2811	10/28/2021 11:18 am
[redacted]	TargetForExternal	10/11/2021 09:37 pm
[redacted]	test webaccessnet	10/18/2021 12:51 pm
[redacted]		
[redacted]		
[redacted]	Target234	10/07/2021 10:37 am
[redacted]		

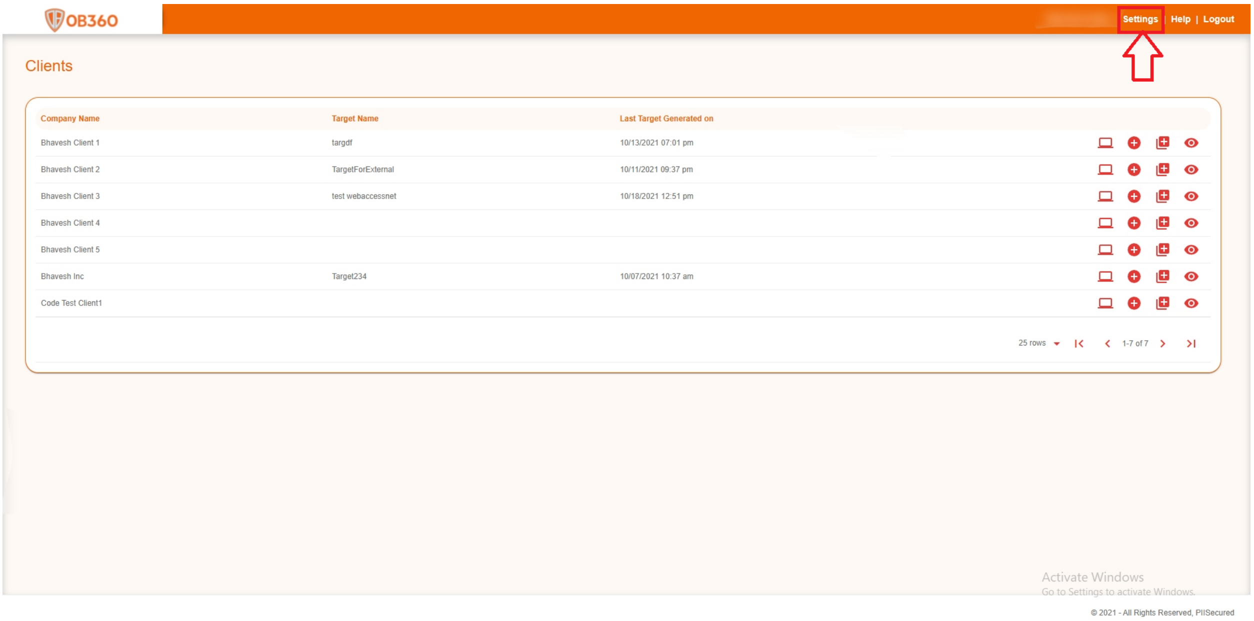
Figure 3: Clients Screen

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**

Scheduling Configuration

Step 4: To create a Scheduler click on ‘**Settings**’

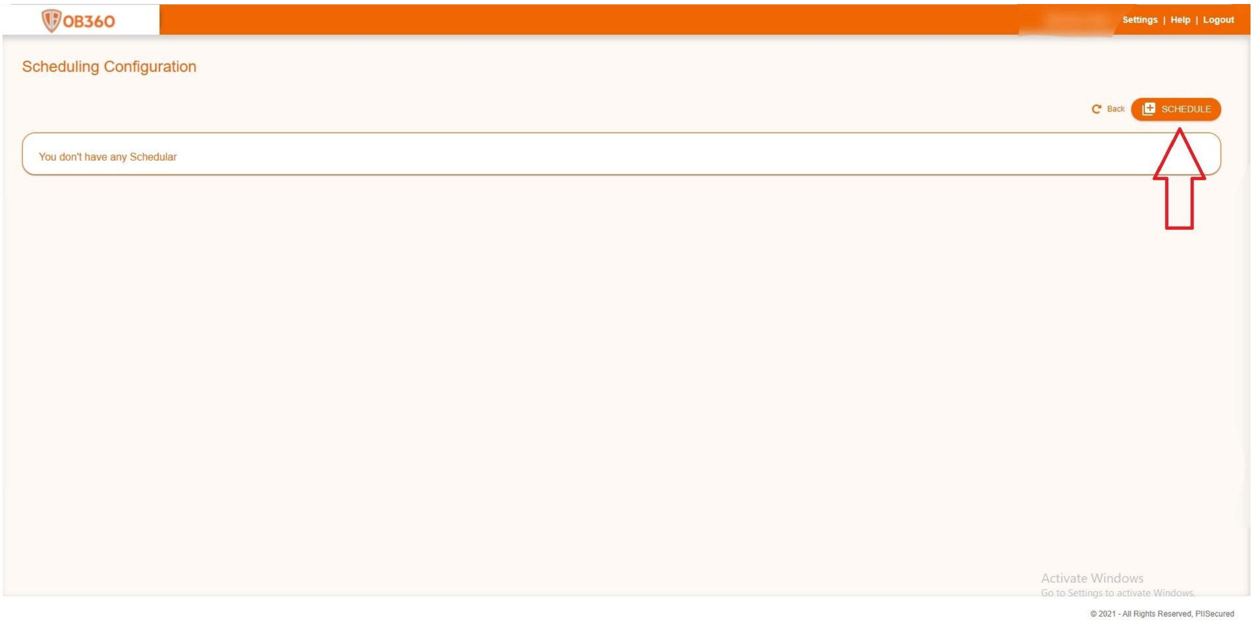


Clients

Company Name	Target Name	Last Target Generated on
Bhavesh Client 1	targdf	10/13/2021 07:01 pm
Bhavesh Client 2	TargetForExternal	10/11/2021 09:37 pm
Bhavesh Client 3	test webaccessnet	10/18/2021 12:51 pm
Bhavesh Client 4		
Bhavesh Client 5		
Bhavesh Inc	Target234	10/07/2021 10:37 am
Code Test Client1		

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**



Scheduling Configuration

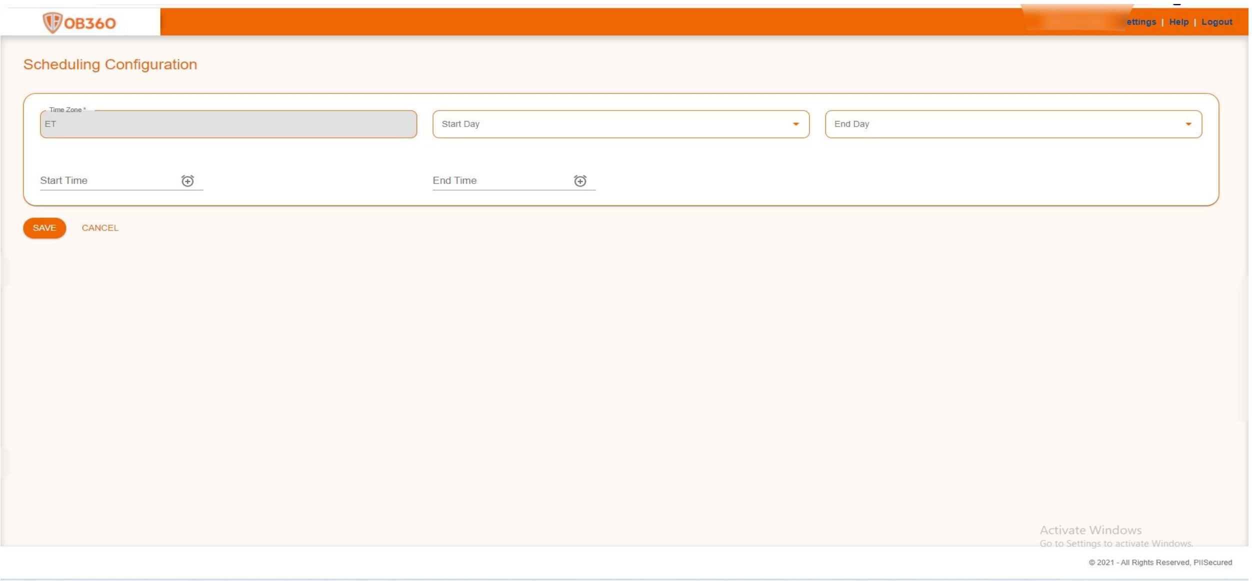
You don't have any Schedular

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**



Time Zone * ET

Start Day

End Day

Start Time

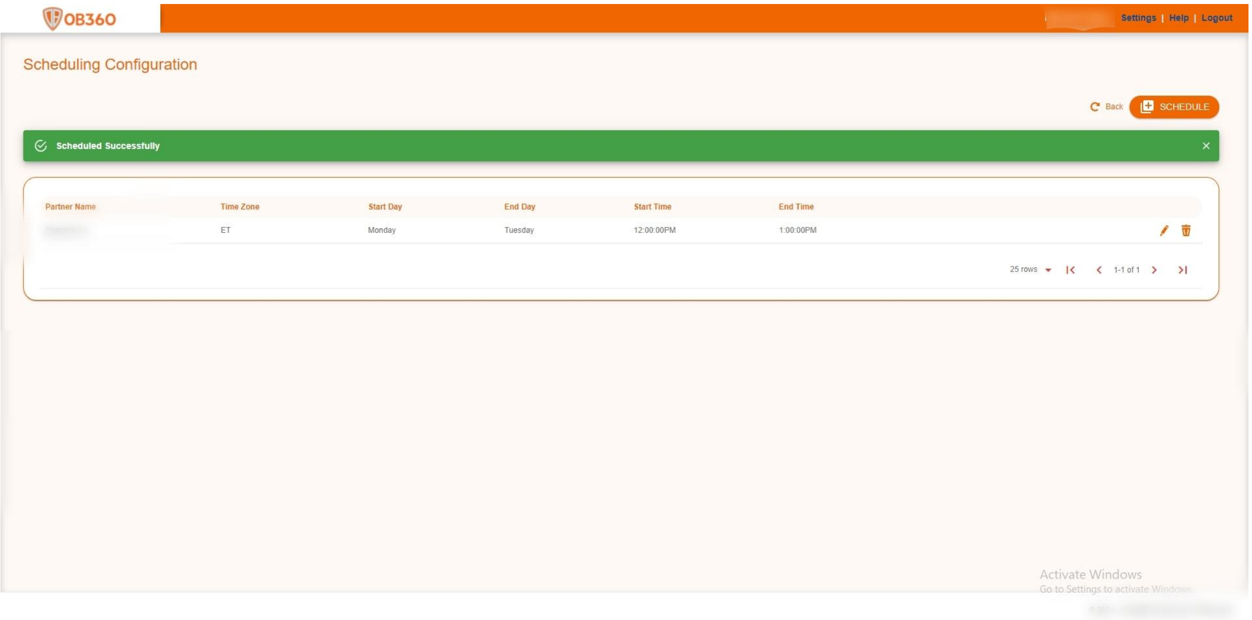
End Time

© 2021 - All Rights Reserved, PIISecured

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.



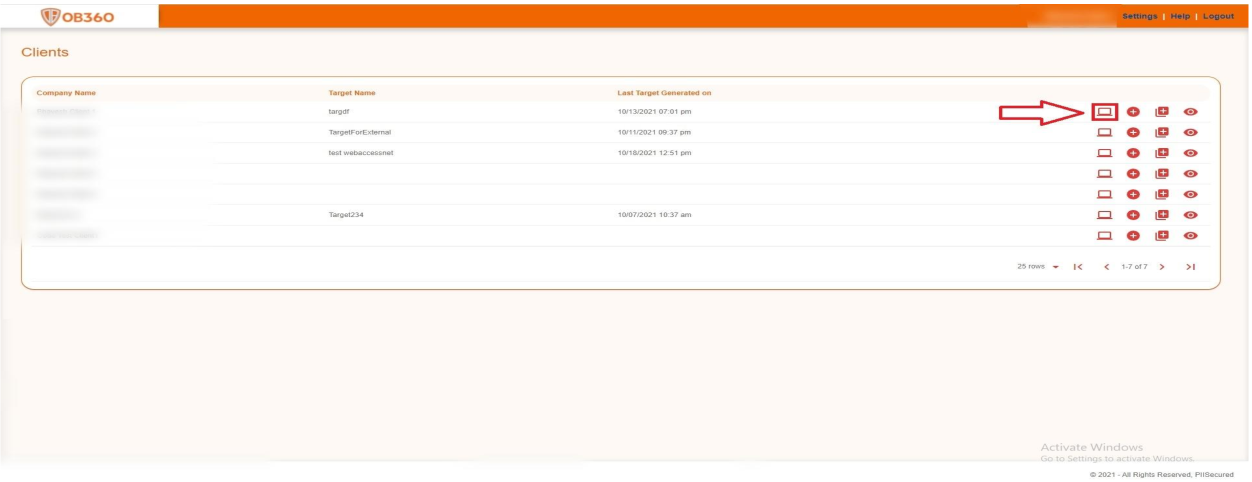
Scheduled Successfully

Partner Name	Time Zone	Start Day	End Day	Start Time	End Time
[redacted]	ET	Monday	Tuesday	12:00:00PM	1:00:00PM

Figure 7: Scheduling List Screen

Create Penetration Test

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



Clients

Company Name	Target Name	Last Target Generated on
[redacted]	targdf	10/13/2021 07:01 pm
[redacted]	TargetForExternal	10/11/2021 09:37 pm
[redacted]	test webaccessnet	10/18/2021 12:51 pm
[redacted]		
[redacted]		
[redacted]	Target234	10/07/2021 10:37 am
[redacted]		

25 rows 1-7 of 7

Activate Windows
Go to Settings to activate Windows.

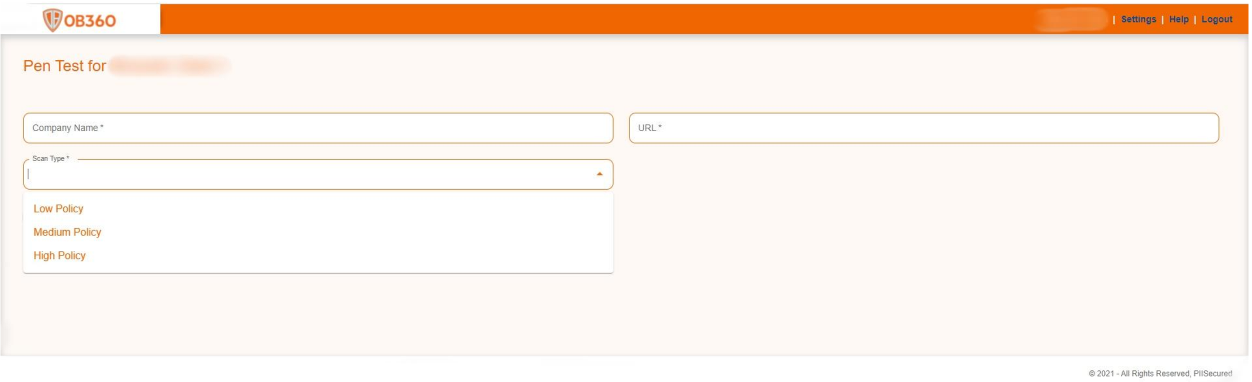
© 2021 - All Rights Reserved, PIISecured

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
- Select ScanType

Then click **Save**



Pen Test for [redacted]

Company Name *

URL *

Scan Type *

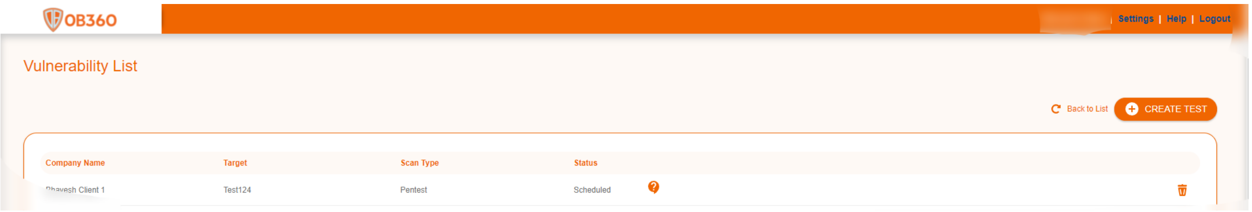
Low Policy
Medium Policy
High Policy

© 2021 - All Rights Reserved, PIISecured

Figure 9: Add Pentest Screen

After clicking the save button.

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

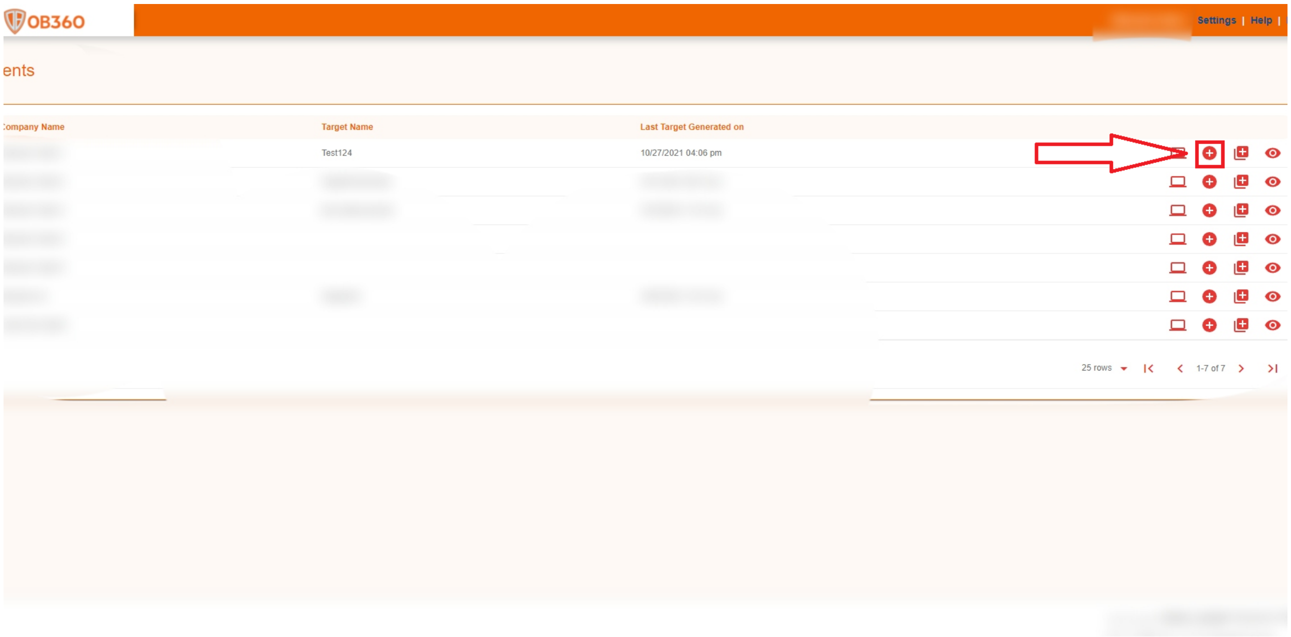


Company Name	Target	Scan Type	Status
Bhavesh Client 1	Test124	Pentest	Scheduled

Figure 10: Vulnerability List Screen

External Vulnerability Test

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

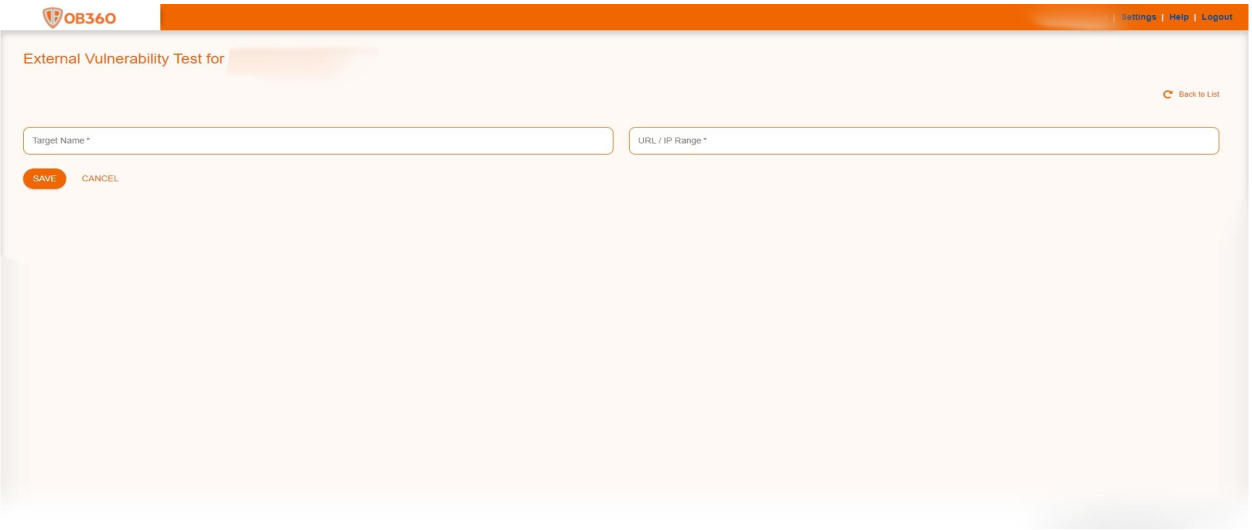


ompany Name	Target Name	Last Target Generated on
	Test124	10/27/2021 04:06 pm

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]



External Vulnerability Test for

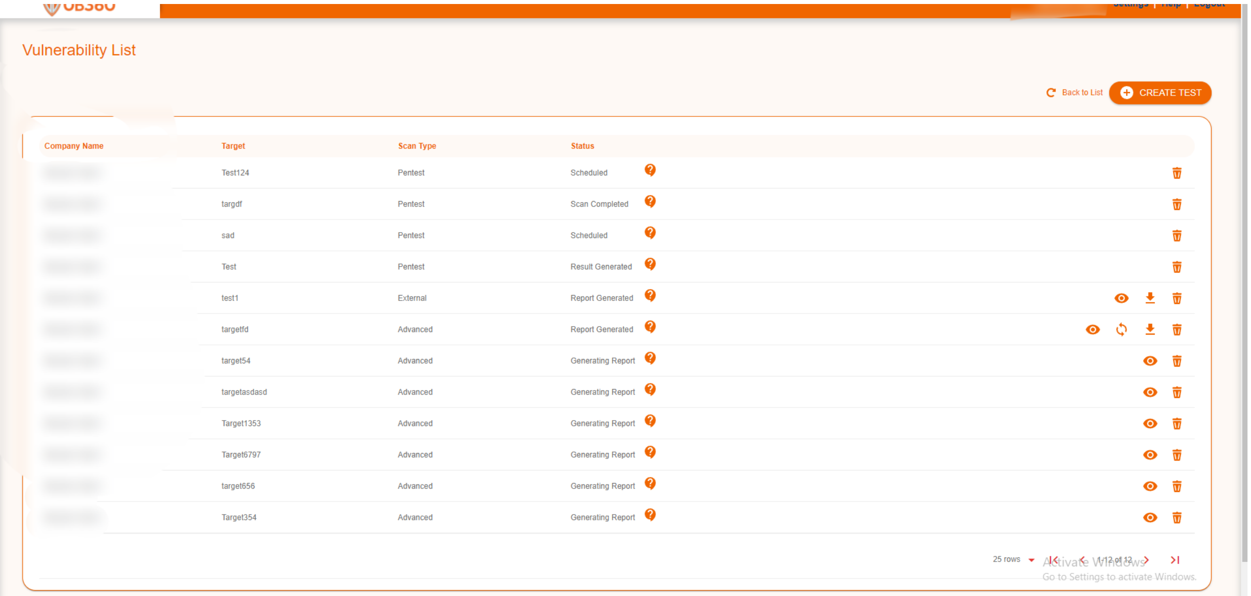
Target Name *

URL / IP Range *

Figure 12 : External Target Screen

Step 12: 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

Company Name	Target	Scan Type	Status		
[redacted]	Test124	Pentest	Scheduled	?	🗑
[redacted]	targdf	Pentest	Scan Completed	?	🗑
[redacted]	sad	Pentest	Scheduled	?	🗑
[redacted]	Test	Pentest	Result Generated	?	🗑
[redacted]	test1	External	Report Generated	?	👁 ⬇ 🗑
[redacted]	targetfd	Advanced	Report Generated	?	👁 ⟳ ⬇ 🗑
[redacted]	target54	Advanced	Generating Report	?	👁 🗑
[redacted]	targetasdasd	Advanced	Generating Report	?	👁 🗑
[redacted]	Target1353	Advanced	Generating Report	?	👁 🗑
[redacted]	Target6797	Advanced	Generating Report	?	👁 🗑
[redacted]	target656	Advanced	Generating Report	?	👁 🗑
[redacted]	Target354	Advanced	Generating Report	?	👁 🗑

Figure 13: Latest Vulnerability List Screen

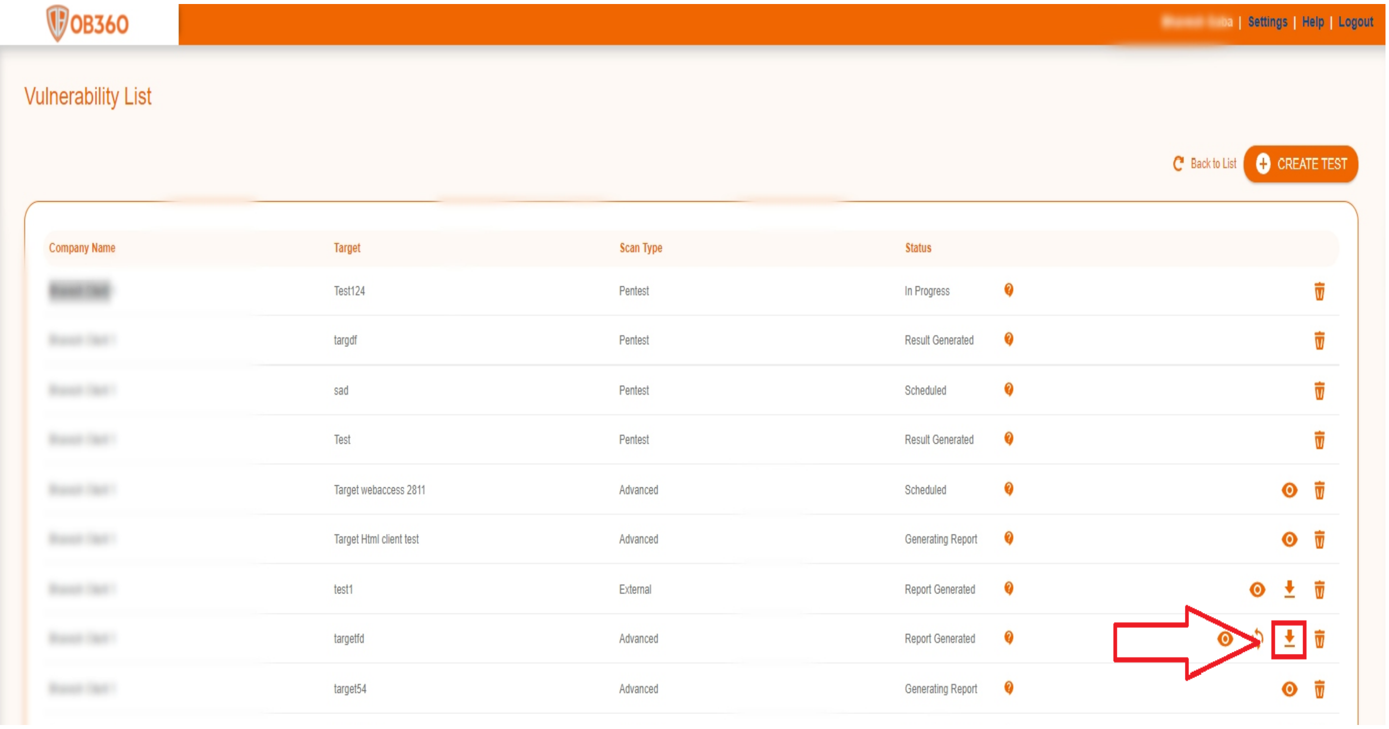
The status of the current Vulnerability test is ‘Scheduled’.

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”.

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



Vulnerability List

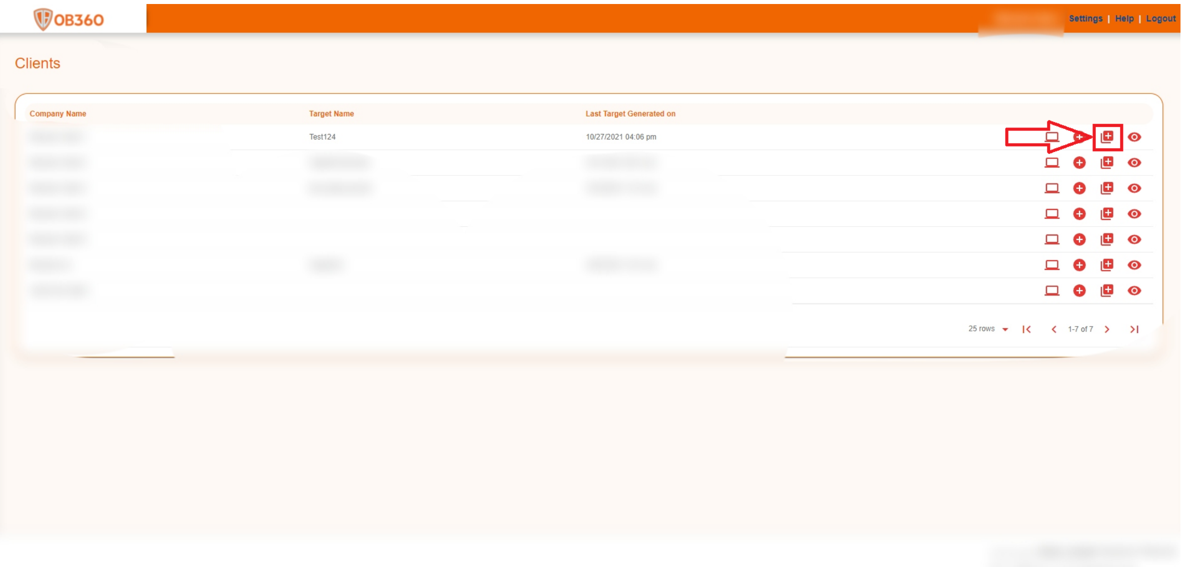
Company Name	Target	Scan Type	Status
[redacted]	Test124	Pentest	In Progress
[redacted]	targdf	Pentest	Result Generated
[redacted]	sad	Pentest	Scheduled
[redacted]	Test	Pentest	Result Generated
[redacted]	Target webaccess 2811	Advanced	Scheduled
[redacted]	Target Html client test	Advanced	Generating Report
[redacted]	test1	External	Report Generated
[redacted]	targetfd	Advanced	Report Generated
[redacted]	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.



Clients

Company Name	Target Name	Last Target Generated on
[redacted]	Test124	10/27/2021 04:06 pm
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		

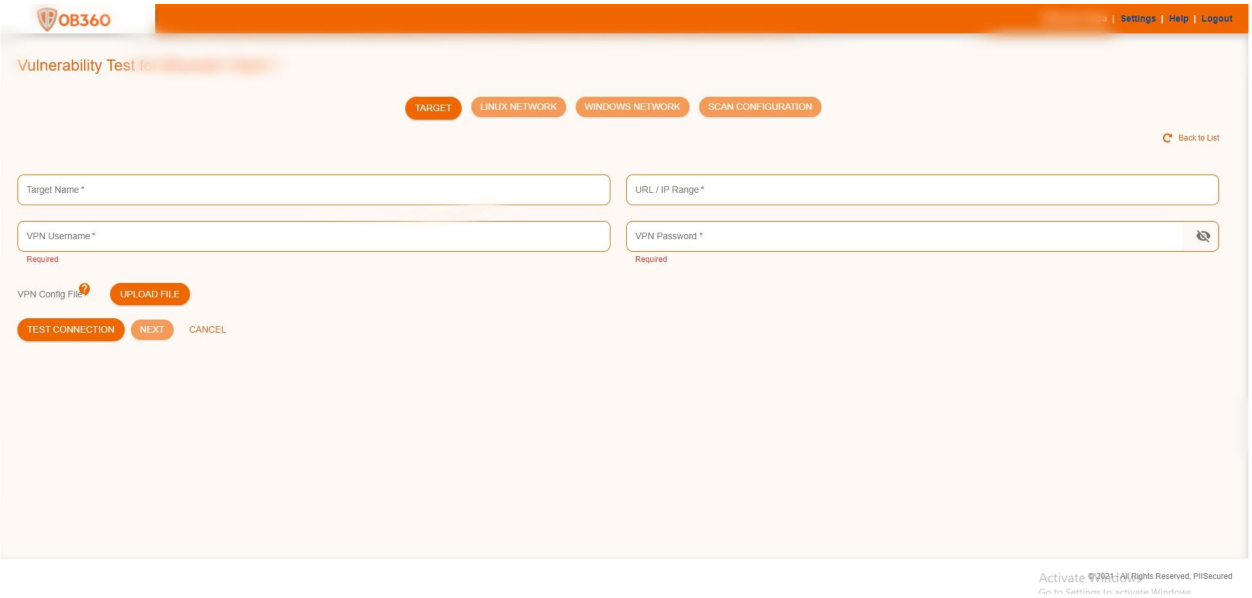
25 rows 1-7 of 7

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.



Vulnerability Test fo

Target Name *

URL / IP Range *

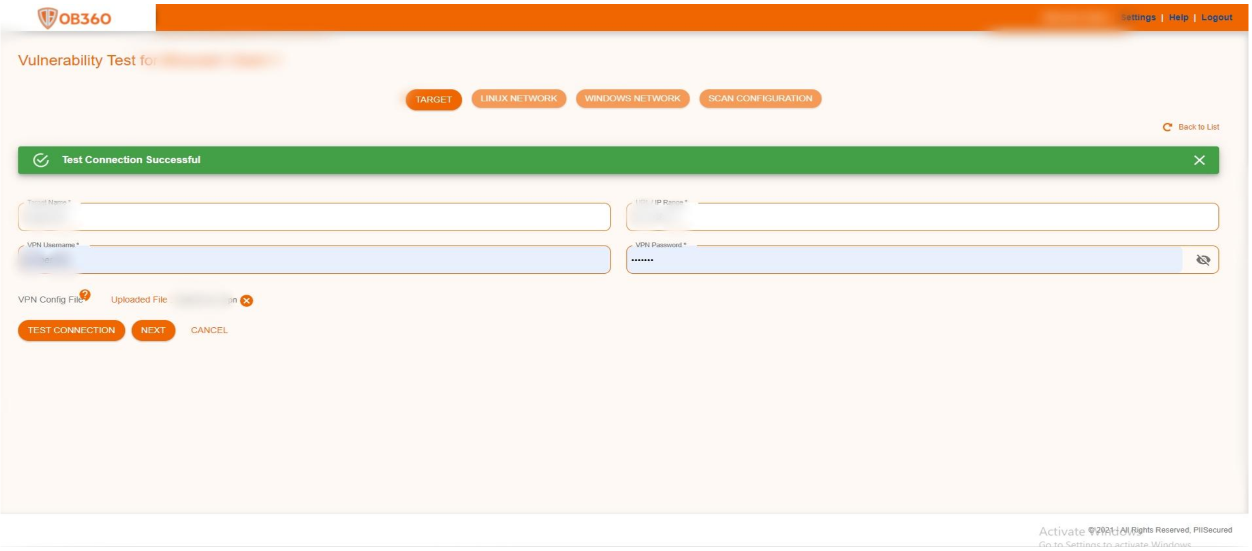
VPN Username *
Required

VPN Password *
Required

VPN Config File

Figure 16: Target Screen

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



Vulnerability Test fo

Test Connection Successful

Target Name *

URL / IP Range *

VPN Username *

VPN Password *
•••••••

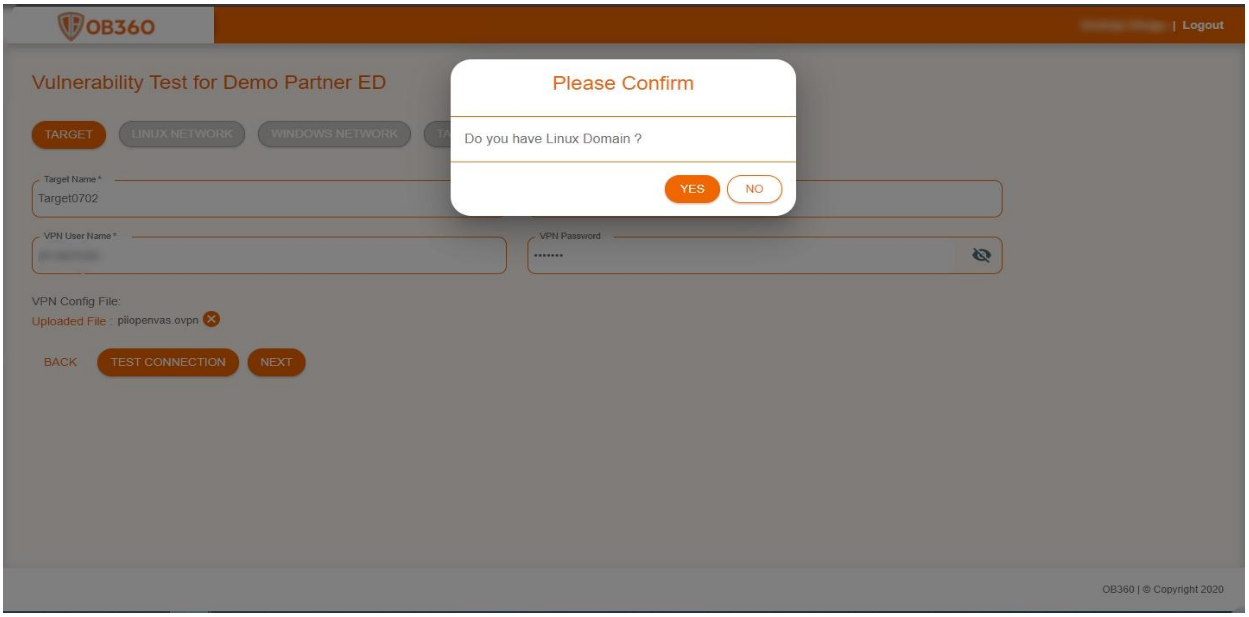
VPN Config File
Uploaded File

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?’



Vulnerability Test for Demo Partner ED

Please Confirm

Do you have Linux Domain ?

Target Name * Target0702

VPN User Name * [redacted]

VPN Password •••••••

VPN Config File:
Uploaded File : piiopenvas.ovpn

Figure 18: Linux Confirmation Screen

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

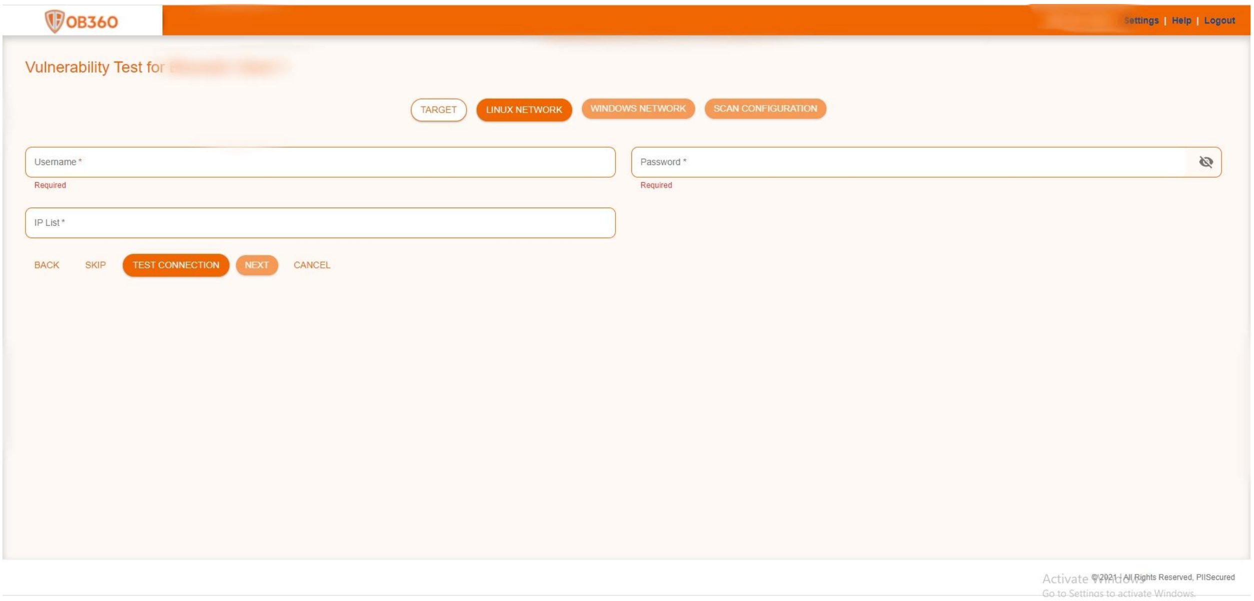
Onclick of ‘Yes’ you will redirect to step 17.

Onclick 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.



Vulnerability Test for [redacted]

Username *

Required

Password *

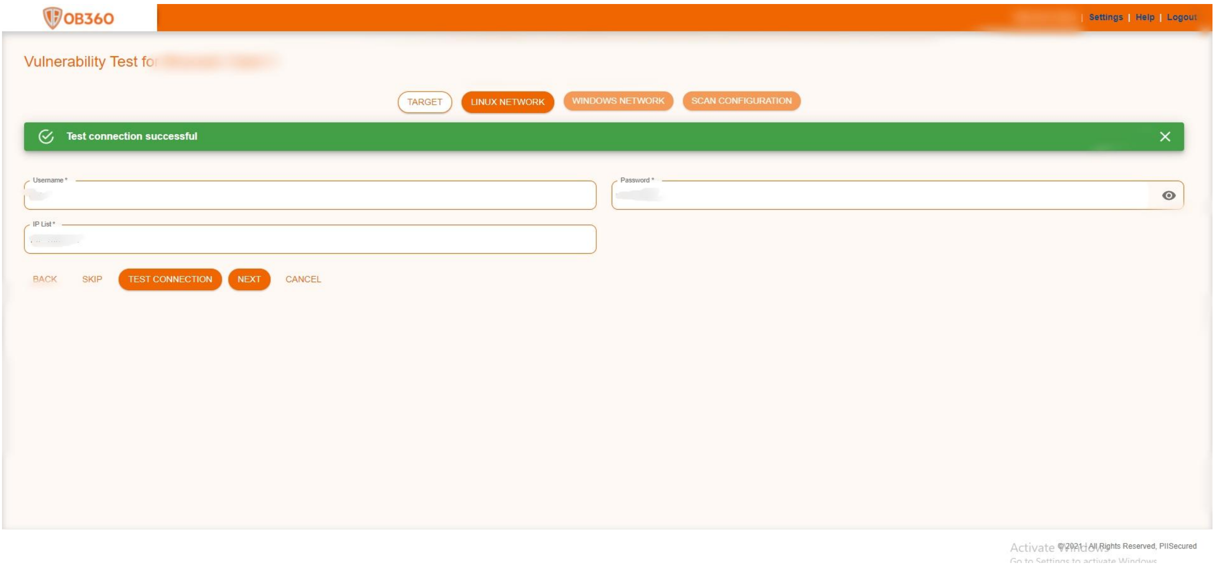
Required

IP List *

©2021 | All Rights Reserved, PIISecured

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.



Vulnerability Test fo [redacted]

Test connection successful

Username * [redacted]

Password * [redacted]

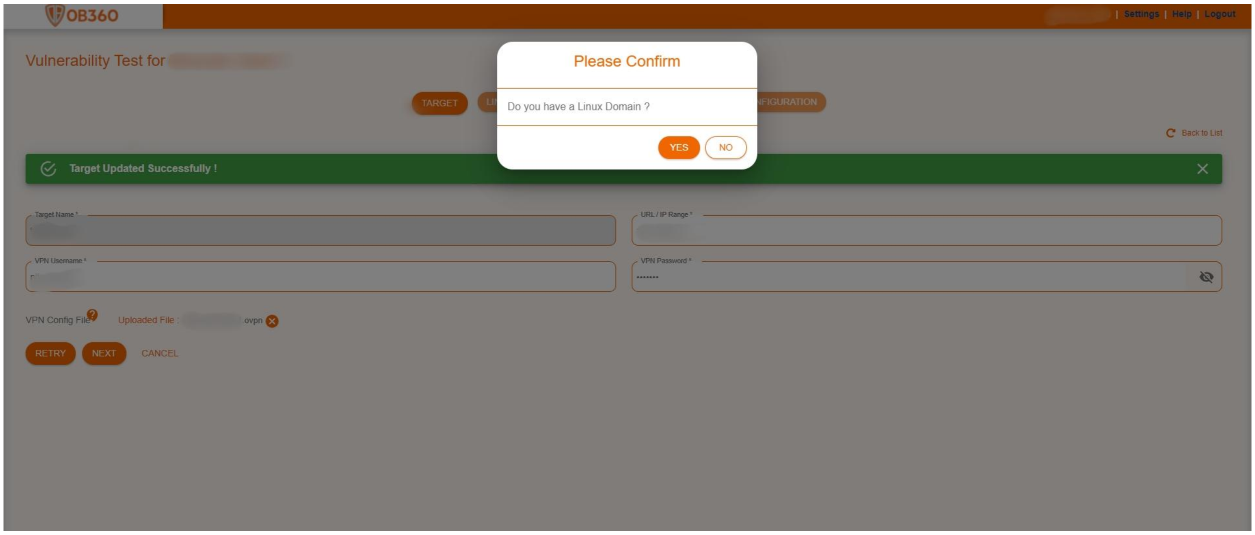
IP List * [redacted]

©2021 | All Rights Reserved, PIISecured

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?’



Vulnerability Test for [redacted]

Please Confirm

Do you have a Linux Domain ?

YES NO

Target Updated Successfully !

Target Name * [redacted]

URL / IP Range * [redacted]

VPN Username * [redacted]

VPN Password * •••••••

VPN Config File Uploaded File : [redacted] ovpn

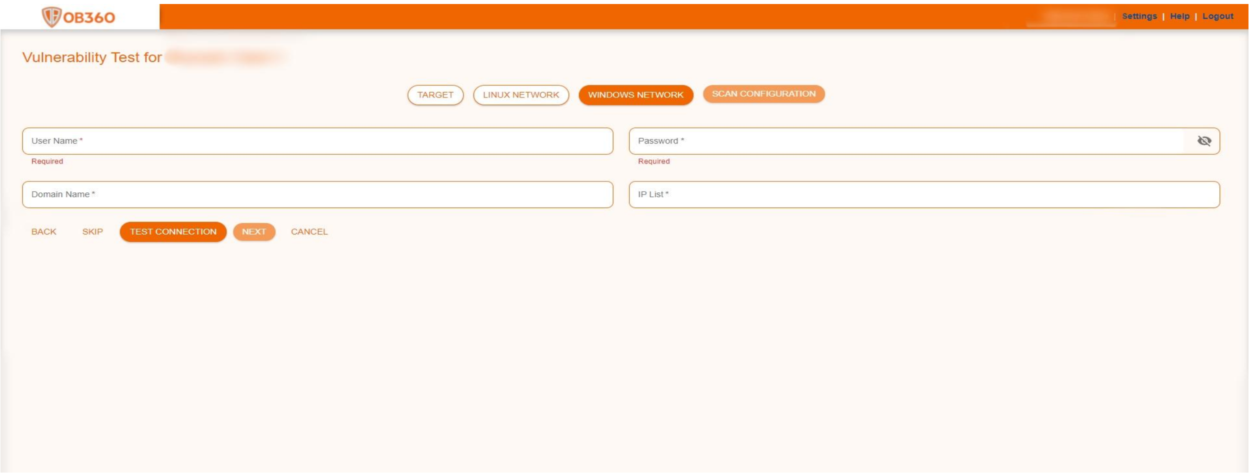
Figure 21: Windows Confirmation Screen

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

Onclick of ‘Yes’ you will redirect to step 19.
Onclick 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.

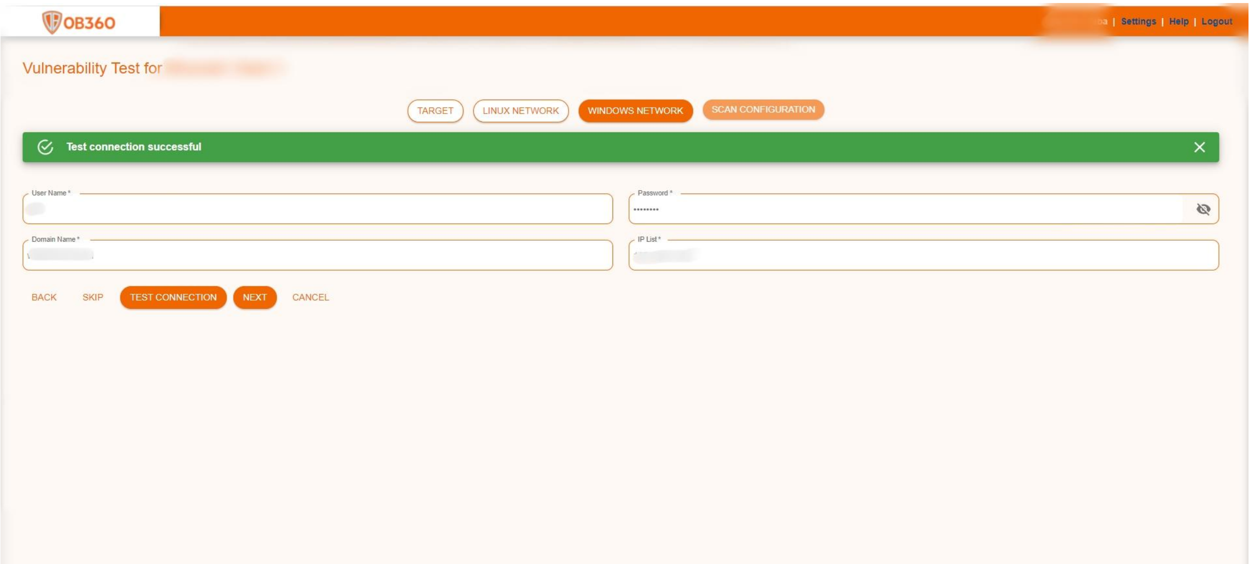
- Enter network administrator Username and Password, Domain Name
- Enter IP address list or IP range
  Eg: Single IP Address (e.g. 192.168.x.xx)
  Multiple IP Address (e.g. 192.168.x.0-255 or 192.168.x.0, 192.168.x.2)
- Click on the 'Test Connection' button.



Vulnerability Test for [redacted]

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.



Vulnerability Test for [redacted]

Test connection successful

User Name * [redacted]

Password * ••••••••

Domain Name * [redacted]

IP List * [redacted]

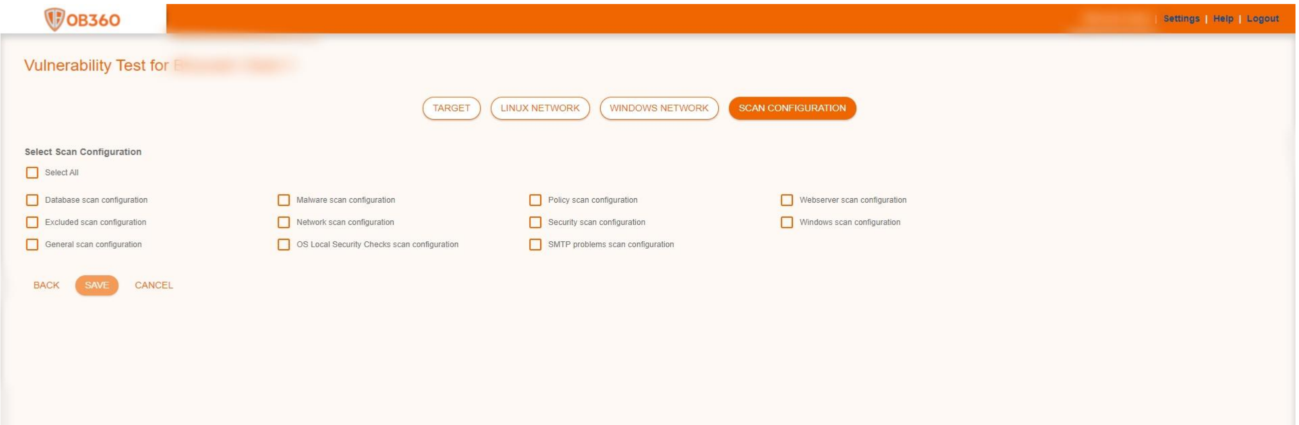
Figure 23: Windows Success Screen

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 Save button after selecting at least one scan configuration from the list.



Settings | Help | Logout

Vulnerability Test for [redacted]

TARGET | LINUX NETWORK | WINDOWS NETWORK | SCAN CONFIGURATION

Select Scan Configuration

□ Select All

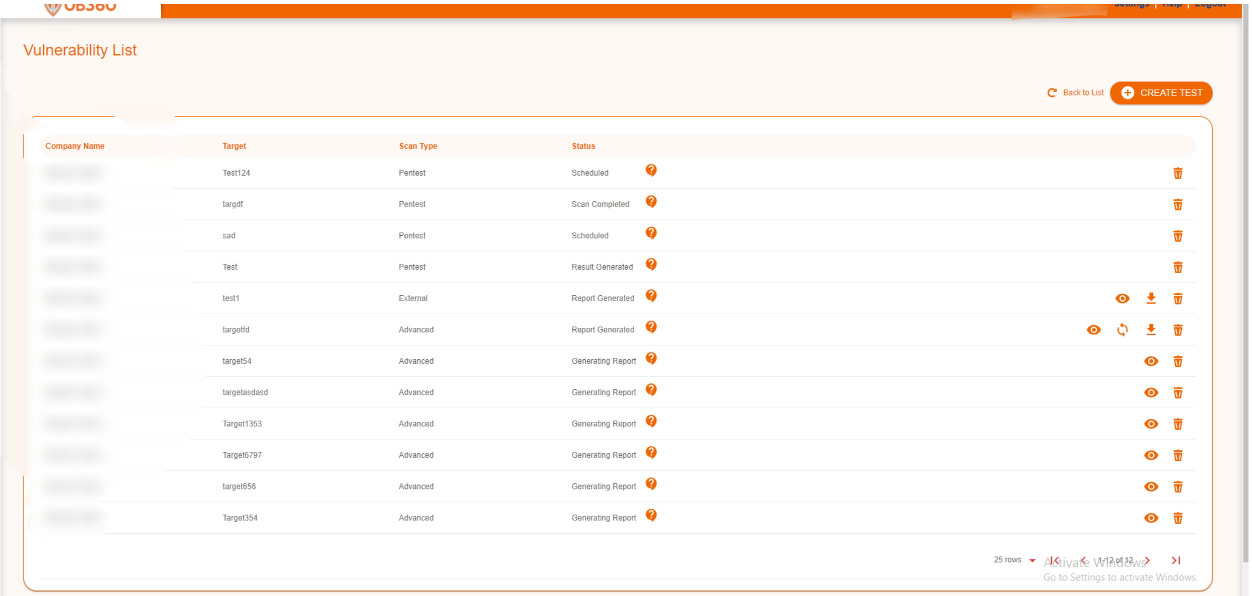
□ Database scan configuration
□ Excluded scan configuration
□ General scan configuration
□ Malware scan configuration
□ Network scan configuration
□ OS Local Security Checks scan configuration
□ Policy scan configuration
□ Security scan configuration
□ SMTP problems scan configuration
□ Webserver scan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

BACK | SAVE | CANCEL

Figure 24: Scan Configuration Screen

Step 21: 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 | CREATE TEST

Company Name	Target	Scan Type	Status
[redacted]	Test124	Pentest	Scheduled
[redacted]	targdf	Pentest	Scan Completed
[redacted]	sad	Pentest	Scheduled
[redacted]	Test	Pentest	Result Generated
[redacted]	test1	External	Report Generated
[redacted]	targetfd	Advanced	Report Generated
[redacted]	target54	Advanced	Generating Report
[redacted]	targetasdasd	Advanced	Generating Report
[redacted]	Target1353	Advanced	Generating Report
[redacted]	Target6797	Advanced	Generating Report
[redacted]	target656	Advanced	Generating Report
[redacted]	Target354	Advanced	Generating Report

25 rows | 1-12 of 12

Activate Windows
Go to Settings to activate Windows.

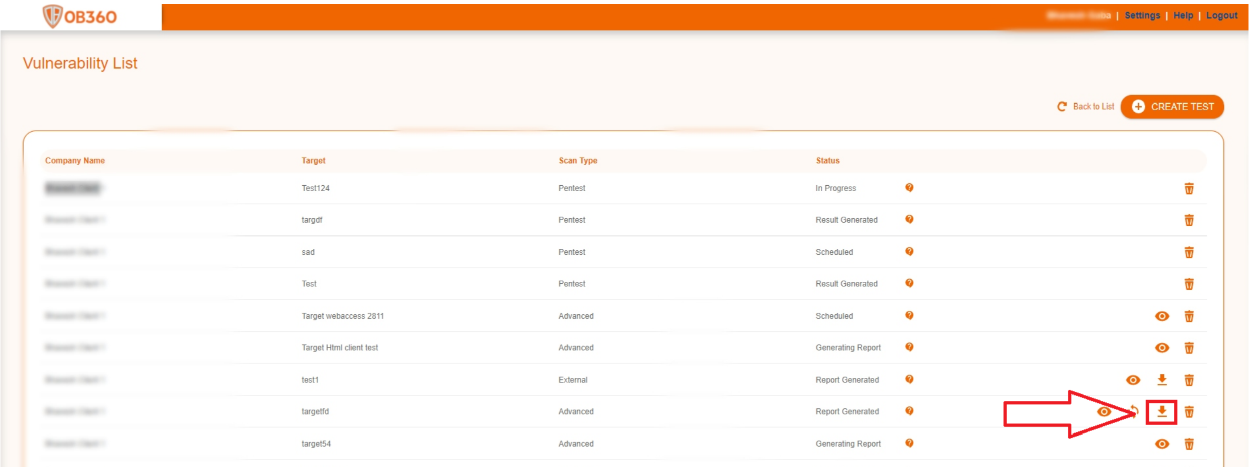
Figure 25: Vulnerability List Screen

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”.



Company Name	Target	Scan Type	Status
[redacted]	Test124	Pentest	In Progress
[redacted]	targdf	Pentest	Result Generated
[redacted]	sad	Pentest	Scheduled
[redacted]	Test	Pentest	Result Generated
[redacted]	Target webaccess 2811	Advanced	Scheduled
[redacted]	Target Html client test	Advanced	Generating Report
[redacted]	test1	External	Report Generated
[redacted]	targetfd	Advanced	Report Generated
[redacted]	target54	Advanced	Generating Report

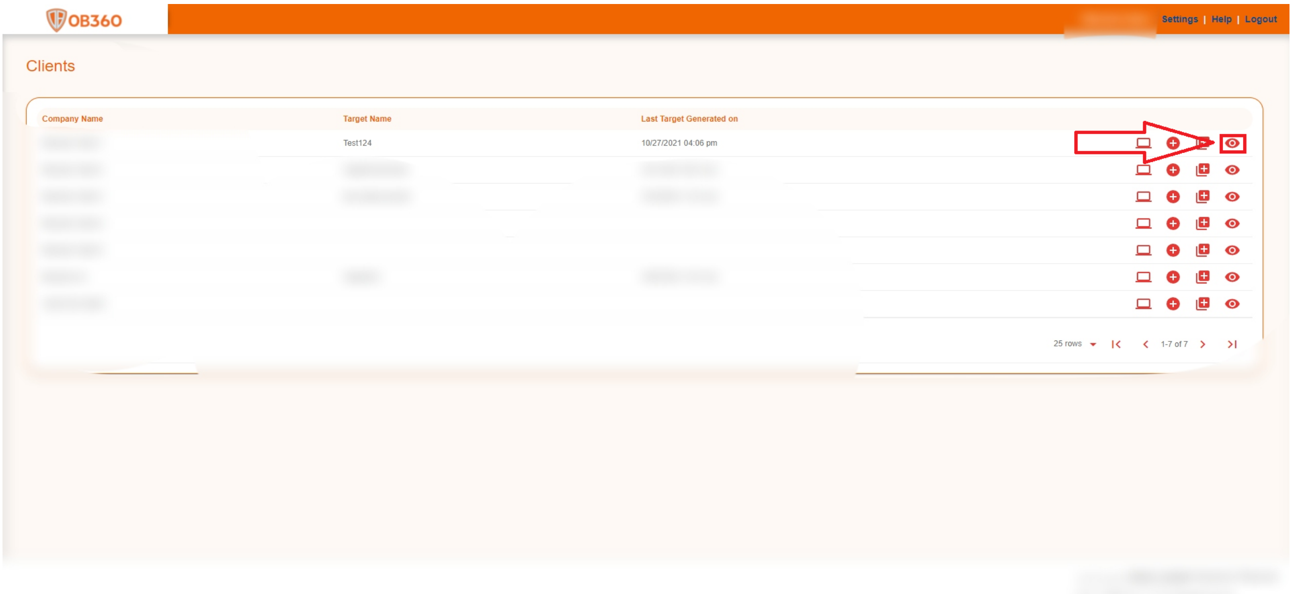
Figure 26: Vulnerability List Screen

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.

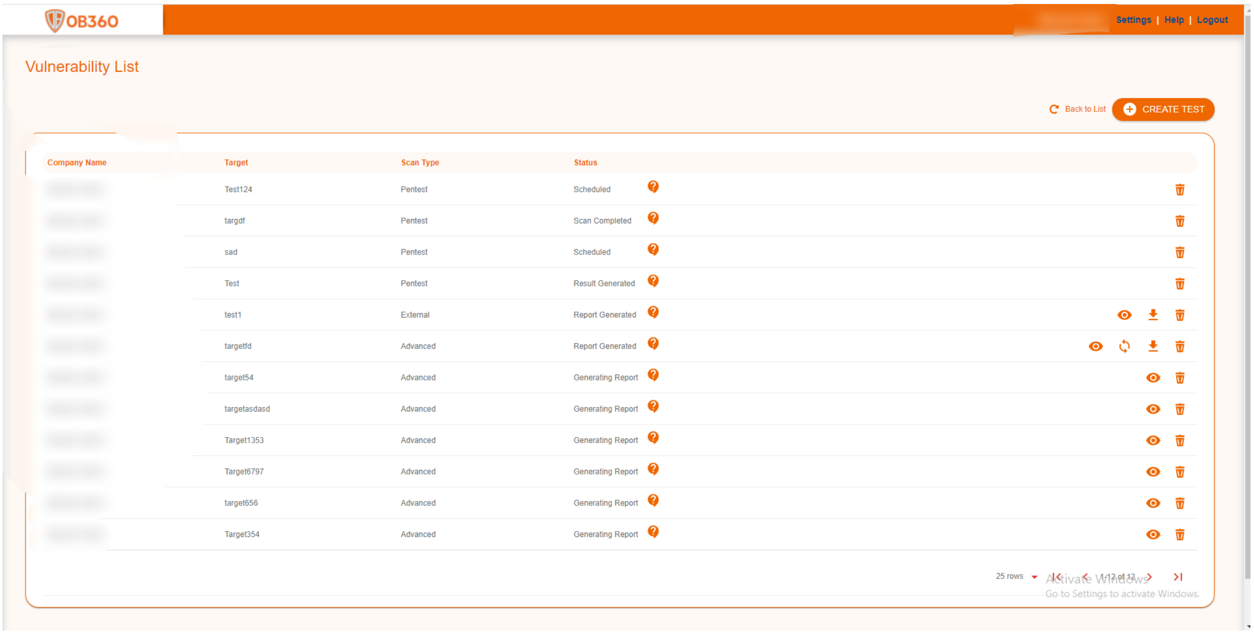


Clients

Company Name	Target Name	Last Target Generated on
[redacted]	Test124	10/27/2021 04:06 pm
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		

Figure 27: Client Screen

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



Vulnerability List

Company Name	Target	Scan Type	Status
[redacted]	Test124	Pentest	Scheduled
[redacted]	targdf	Pentest	Scan Completed
[redacted]	sad	Pentest	Scheduled
[redacted]	Test	Pentest	Result Generated
[redacted]	test1	External	Report Generated
[redacted]	targetfd	Advanced	Report Generated
[redacted]	target54	Advanced	Generating Report
[redacted]	targetasdasd	Advanced	Generating Report
[redacted]	Target1353	Advanced	Generating Report
[redacted]	Target6797	Advanced	Generating Report
[redacted]	target656	Advanced	Generating Report
[redacted]	Target354	Advanced	Generating Report

Figure 28: Vulnerability List Screen 1