**CYBAROGUE**

Index

1 . Cybarogue Framework

2. Create/Start new project

3. Dashboard

4. Testcases

5. Device Tool User Manual

5.1. Binwalk User Manual

(a)User Activities

(b)Reports

5.2. Firmwalker

(a)User Activities

(b)Reports

6. Android Tool User Manual

(a)User Activities

(b)Reports

7.Network Tool User Manual

7.1 Nmap User Manual

(a)User Activities

(b)Reports

7.2 Pcap Analyser User Manual

(a)User Activities

(b)Reports

7.3. Password Extractor User Manual

(a)User Activities

(b)Reports

8. Web Tool User Manual

8.1 SSLScan User Manual

(a)User Activities

(b)Reports

8.2 Wapiti User Manual

(a)User Activities

(b)Reports

8.3 Whatweb User Manual

(a)User Activities

(b)Reports

8.4 Nikto User Manual

(a)User Activities

(b)Reports

9.Thick Client Tool User Manual

9.1 Uncompyle6 User Manual

(a)User Activities

(b)Reports

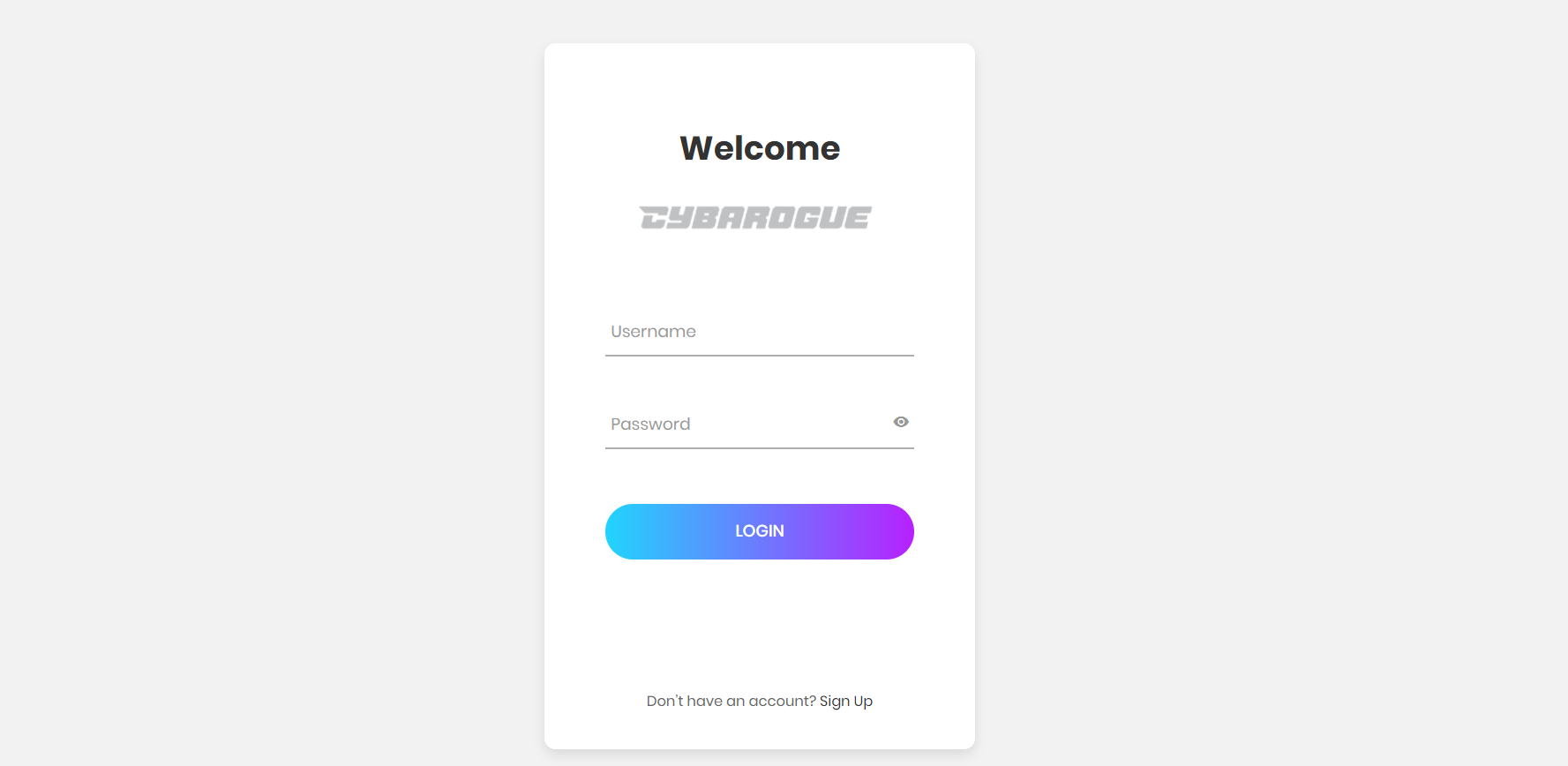
***Tools User Manuals***

In this let’s know about the Tools user manuals of each tool and how to use Cybarogue framework as well.

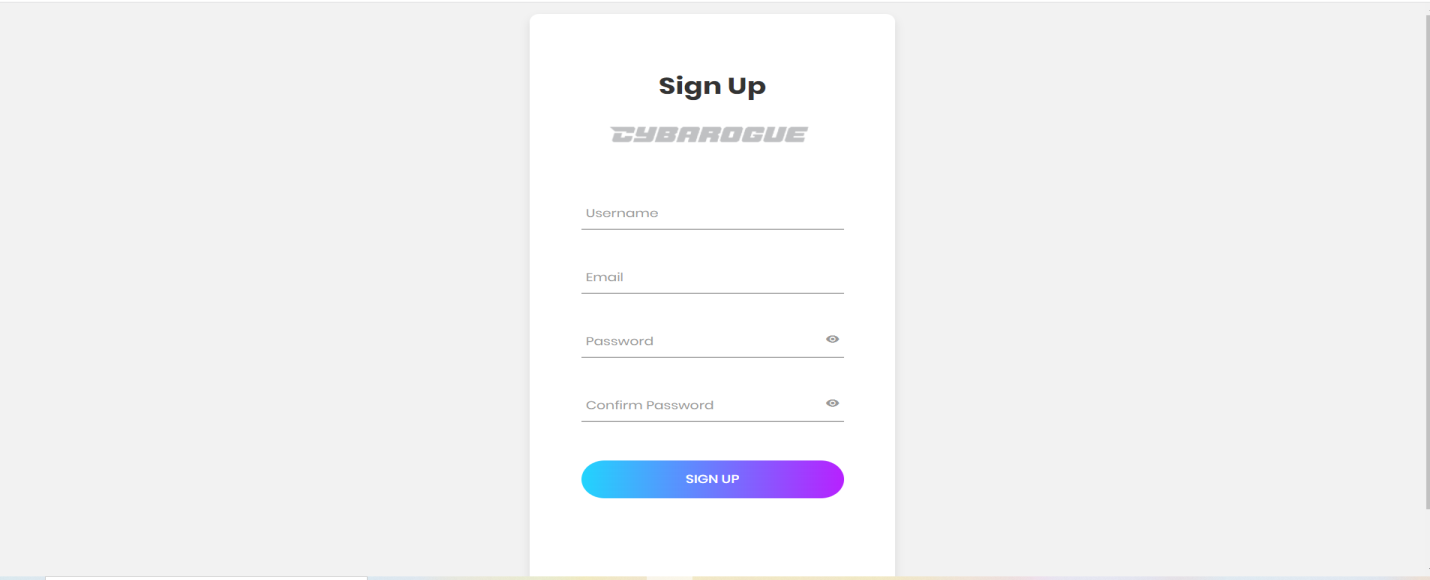
**1. Cybarogue Framework**:

First the Cybarogue needs signup or login if the user is new then needs signup and for existing user needs to login by using the respective credentials as shown below.

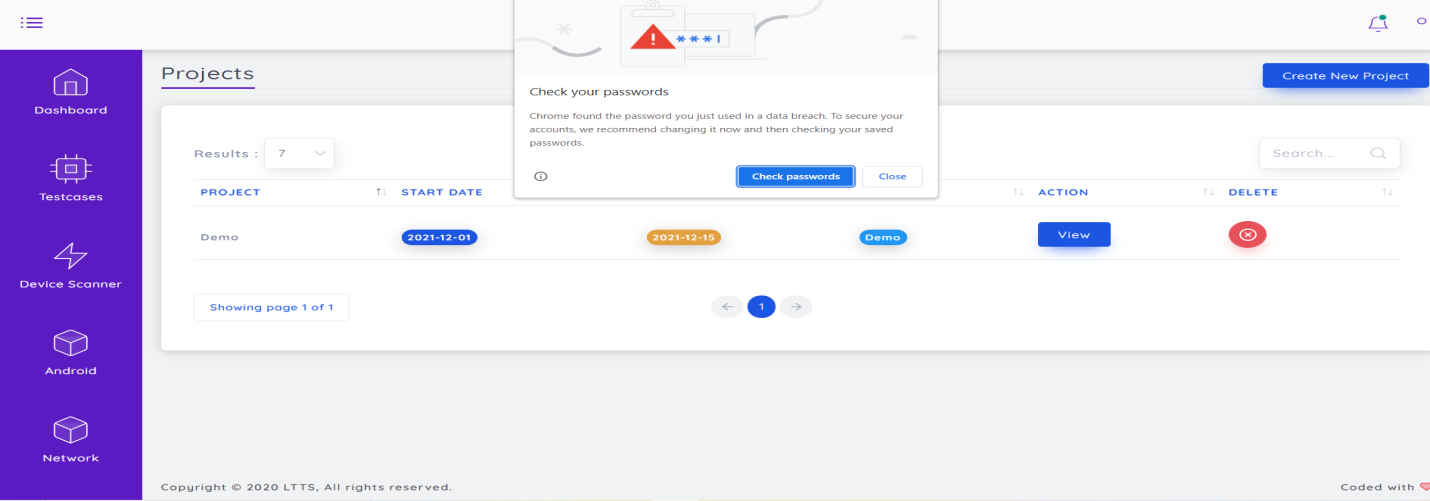
Step 1: Login page is as follows:



Step 2: For signup we need to fill the details and click signup.



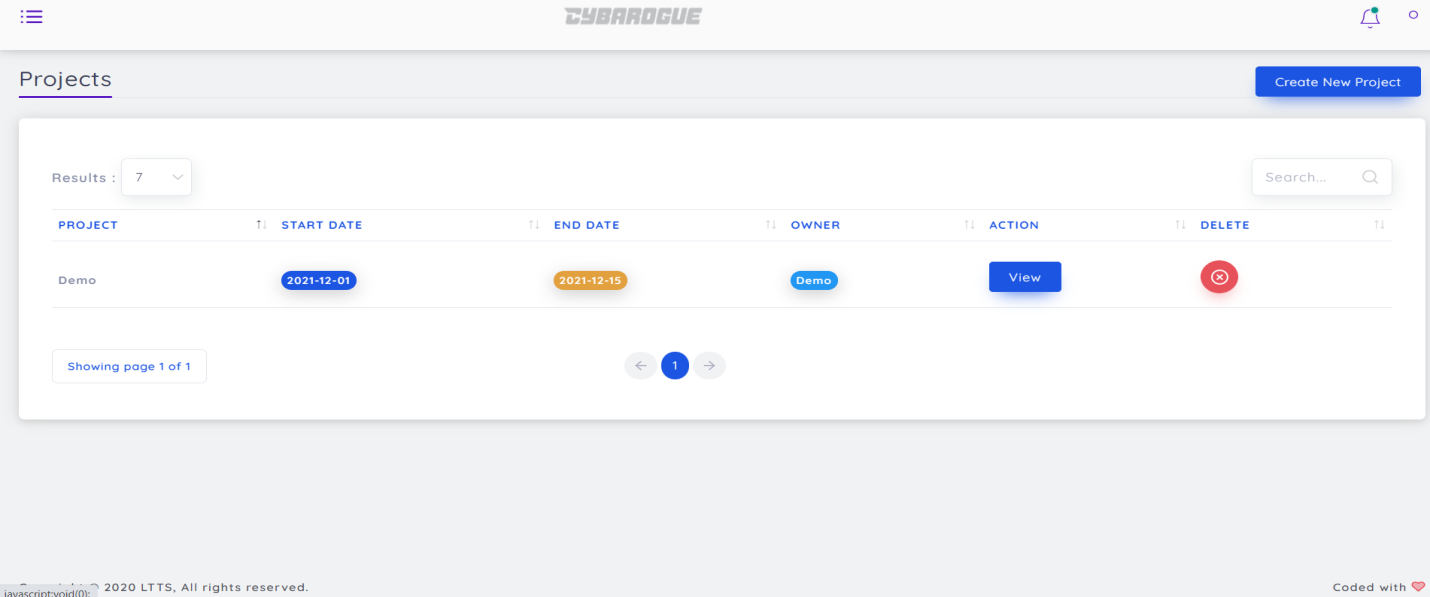
Step 3: After login first the home page seems as follows:



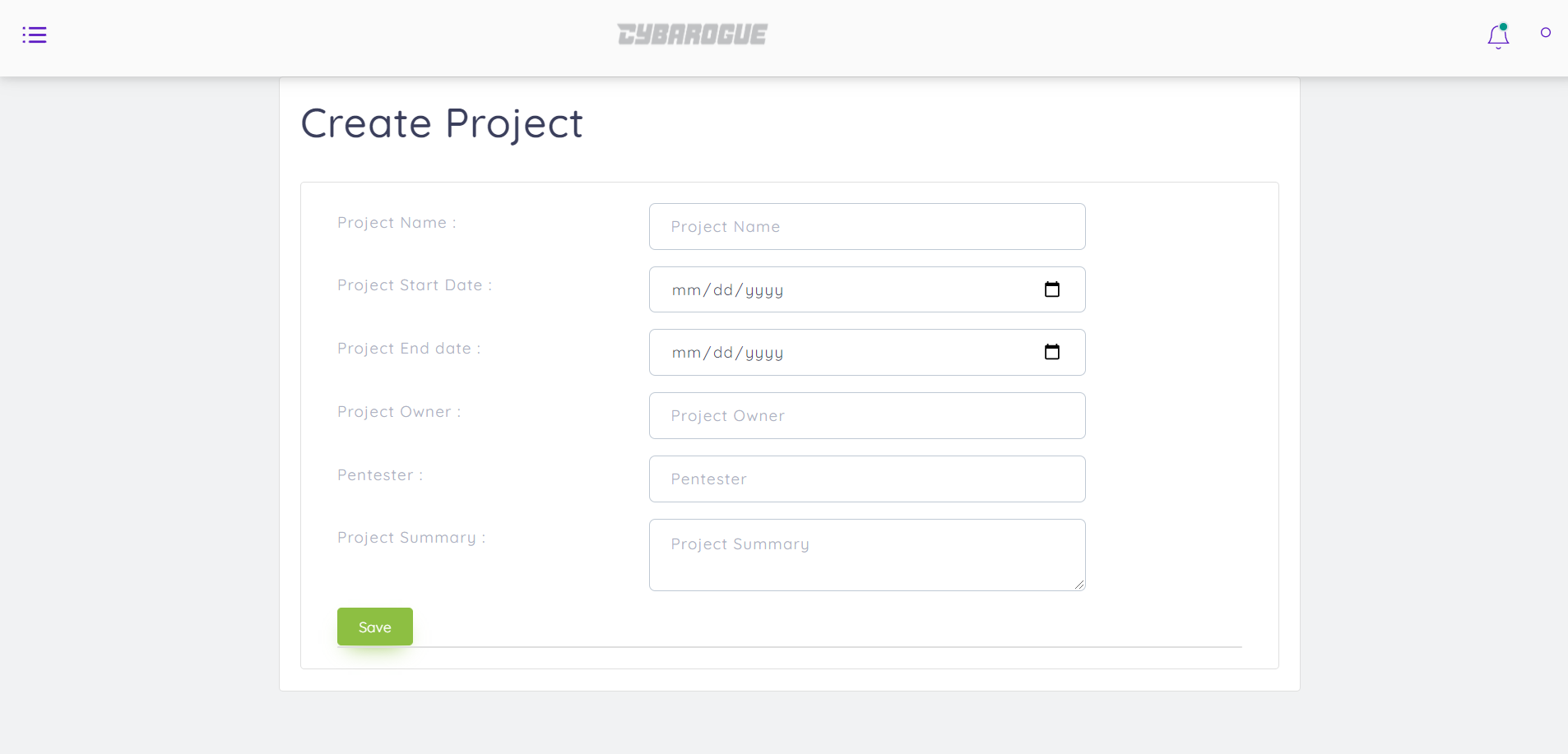
**2. Create/Start new project**

To create a new project first needs to login into the cybarogue and in the home page at the top right there is an option “New Project”. By clicking that we can see other page that regarding to create new project there you can fill all the details and click save then they automatically wents into project list there we can delete and view.

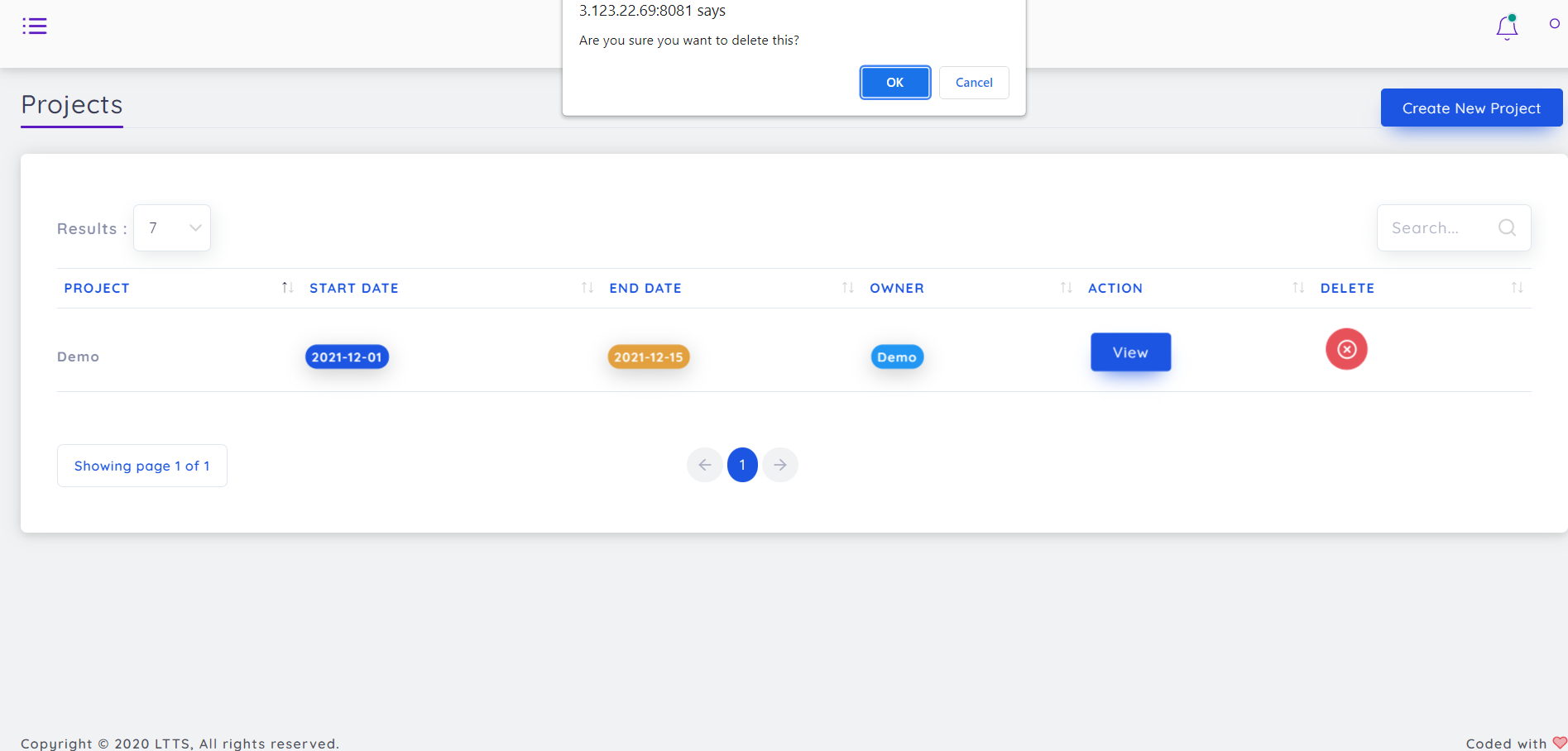
Step 1: To create new project



Step 2: After clicking Create new Project



Step 3: If we want to delete any project, we can able to see the popup notification for confirmation after clicking ok. The project is deleted.



Step 4:By clicking the option view.

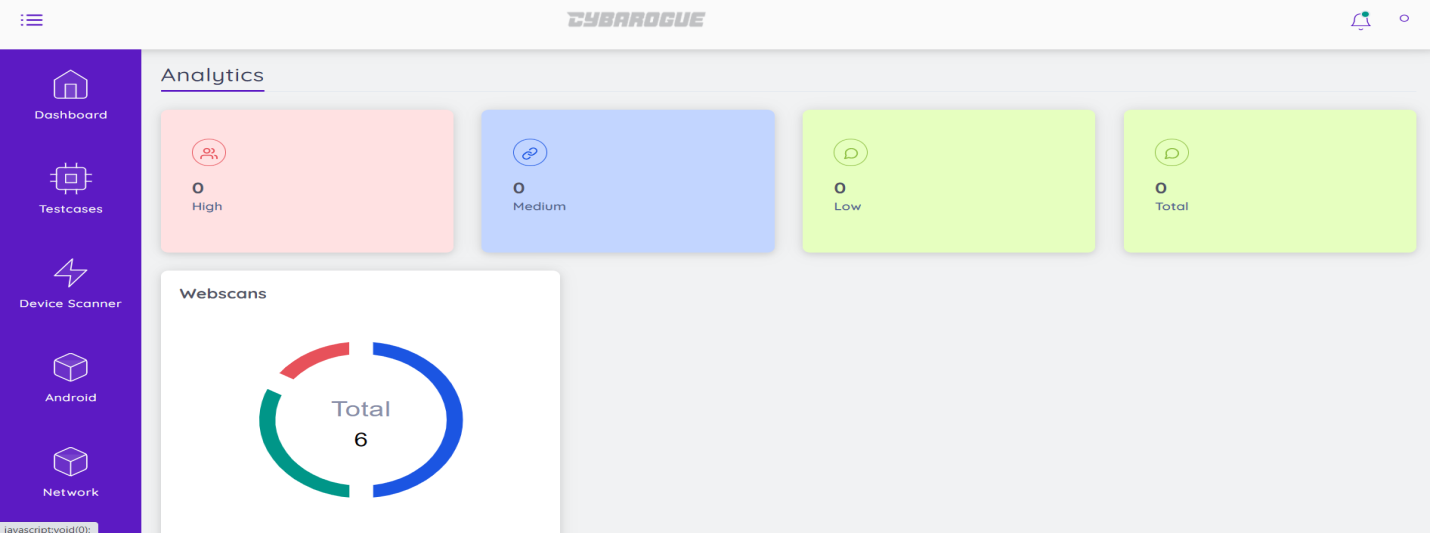


**3. Dashboard:**

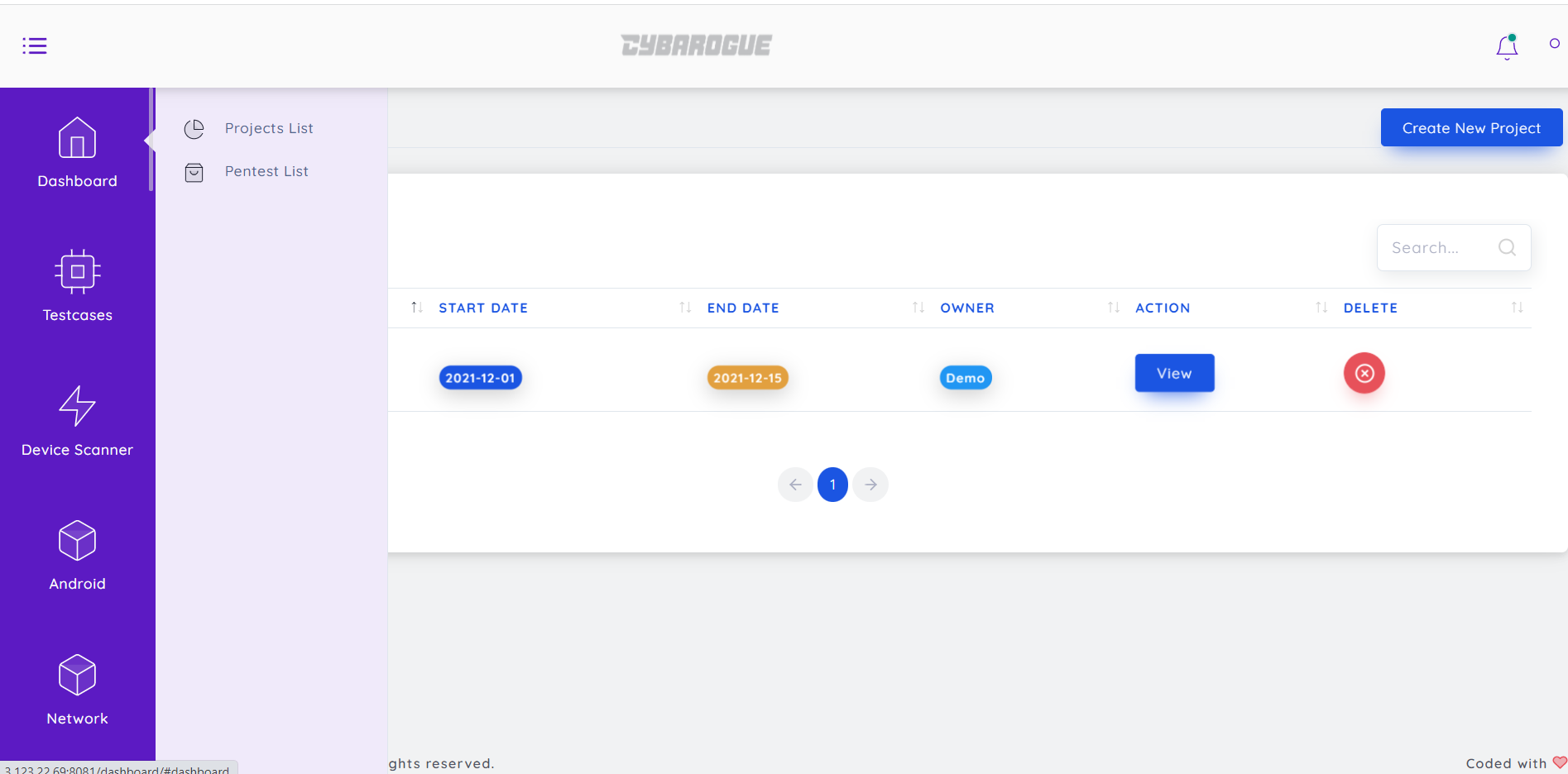
After clicking the three horizontal tiny lines at the top left corner we can able to see the dashboard and in the first option dashboard we can see project list and pentest list.

By clicking each we can see the list of according projects.

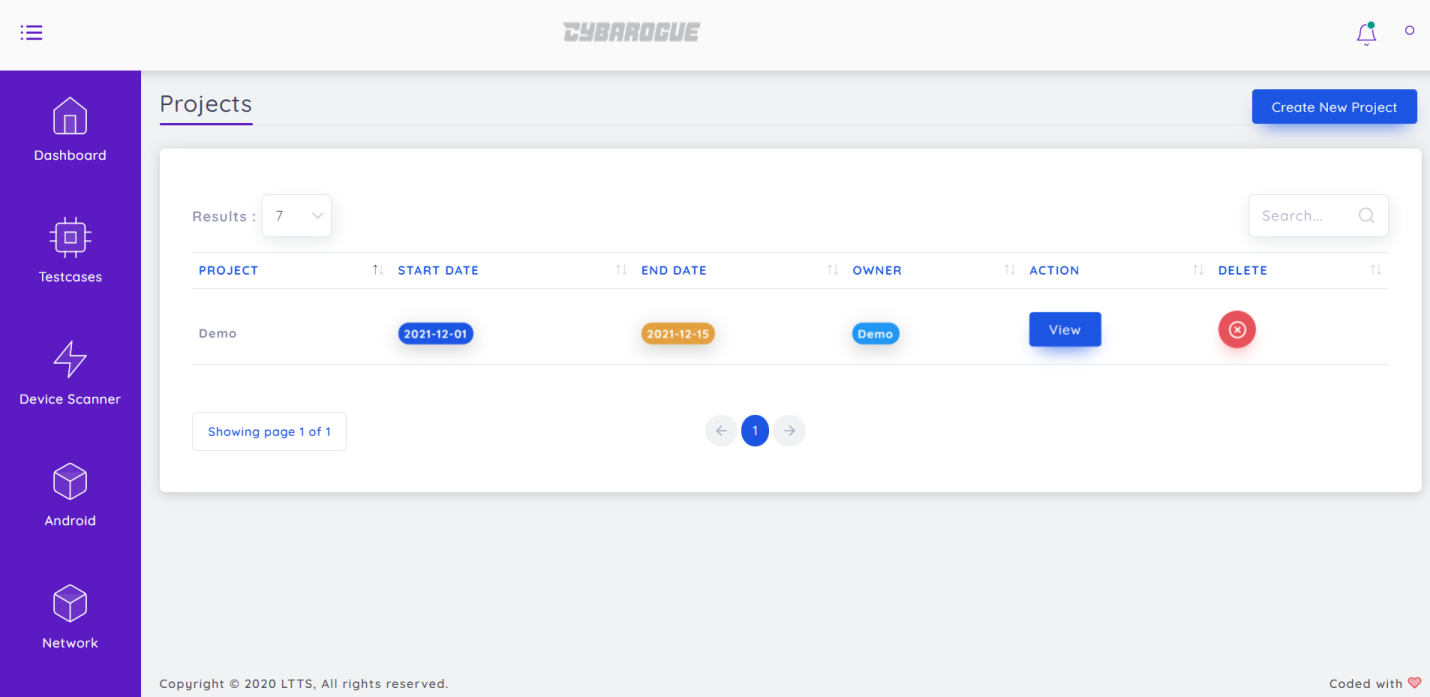
Step 1: By clicking the top right corner option we can see the dashboard following list as follows



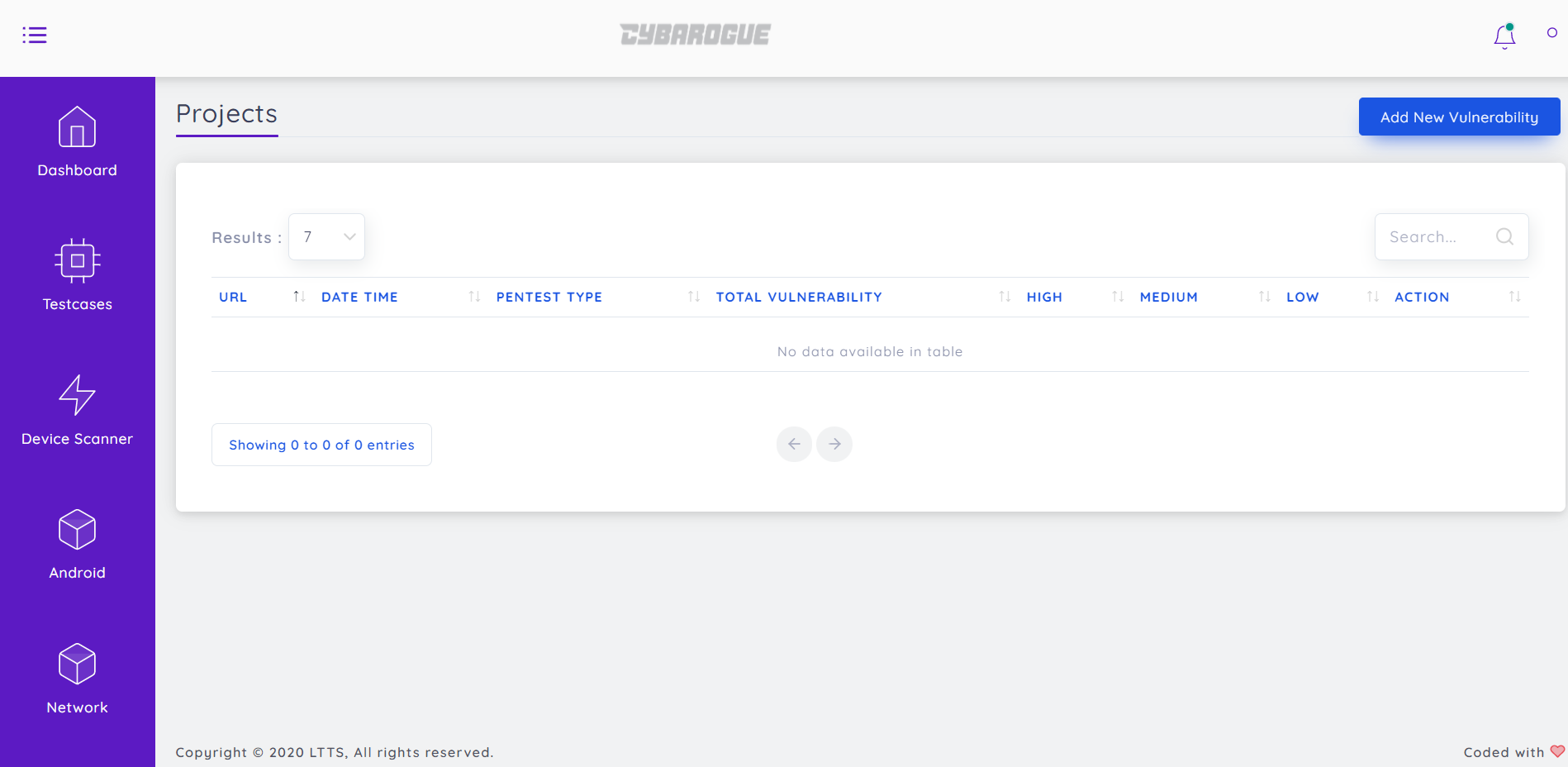
Step 2: By Selecting Dashboard option we can see the two sub options project list and pentest list as follows:



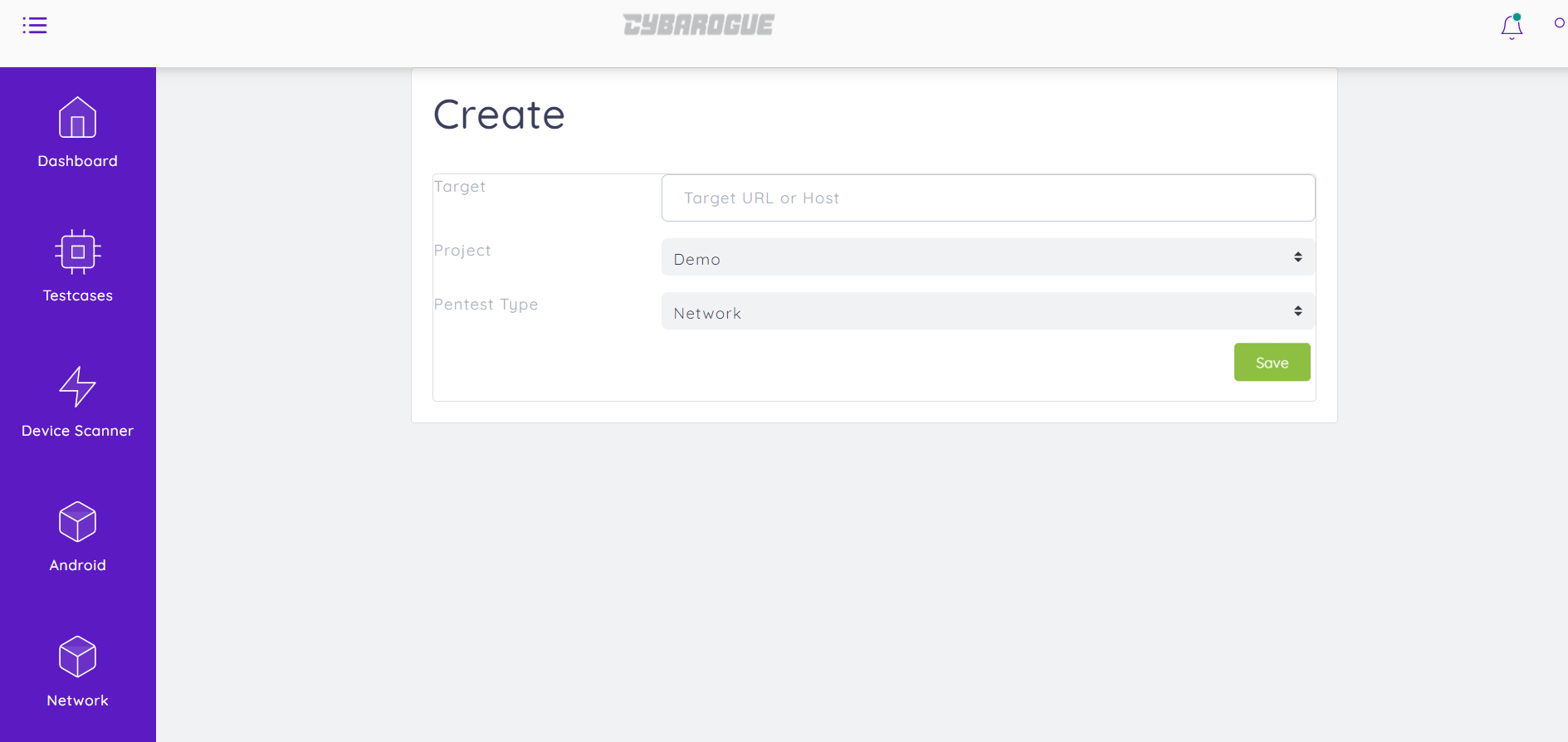
Step 3: By selecting Project list we can see as follows:



Step 4: By selecting Pentest list we can see the list we can see as follows:



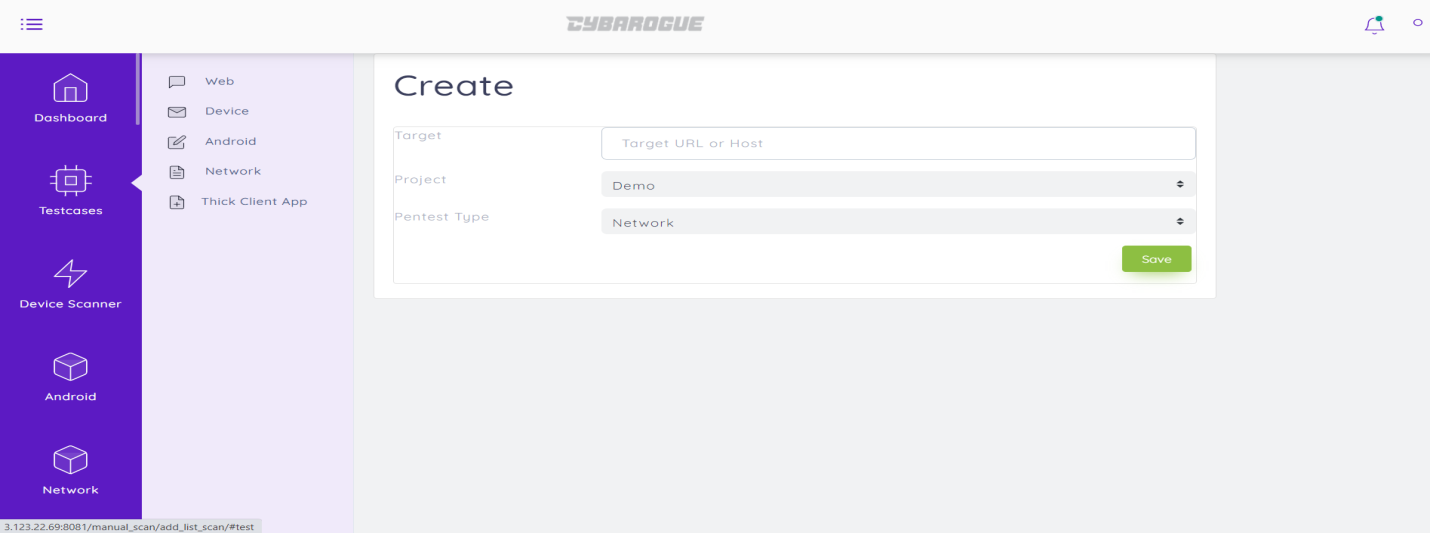
Step 5: By selecting “add new vulnerability” option we can add new pentest into cybarogue. Here we can do external of cybarogue pentests by our own. For that first we need to fill all the details to create new pentest and click save then the created pentest is automatically went into the list of pentest in the above step and for delete option it is same as project lists like it will ask the confirmation of deletion through popup notification.



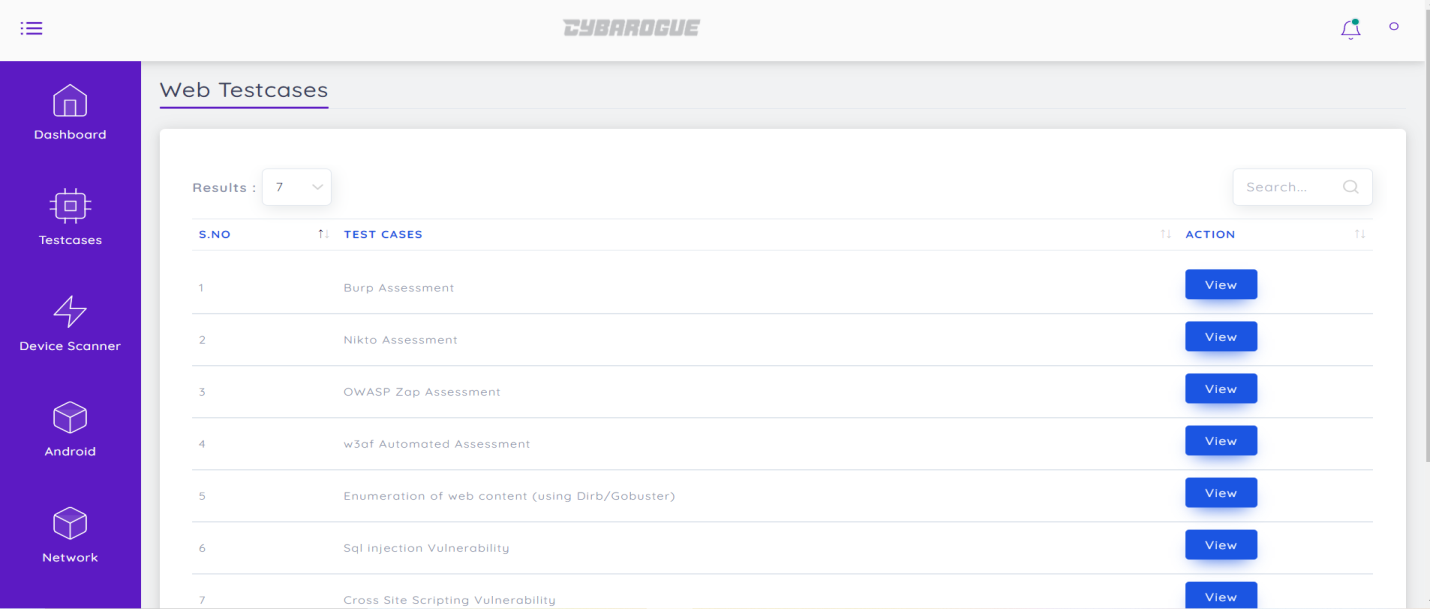
**4. Testcases**:

Below Dashboard option we can see the Testcases option in that there are all tool category. By clicking each we can see the list of each tools the target is just for reference means to get start the new scan we just need to know about each scan for that purpose these Testcases are helpful.

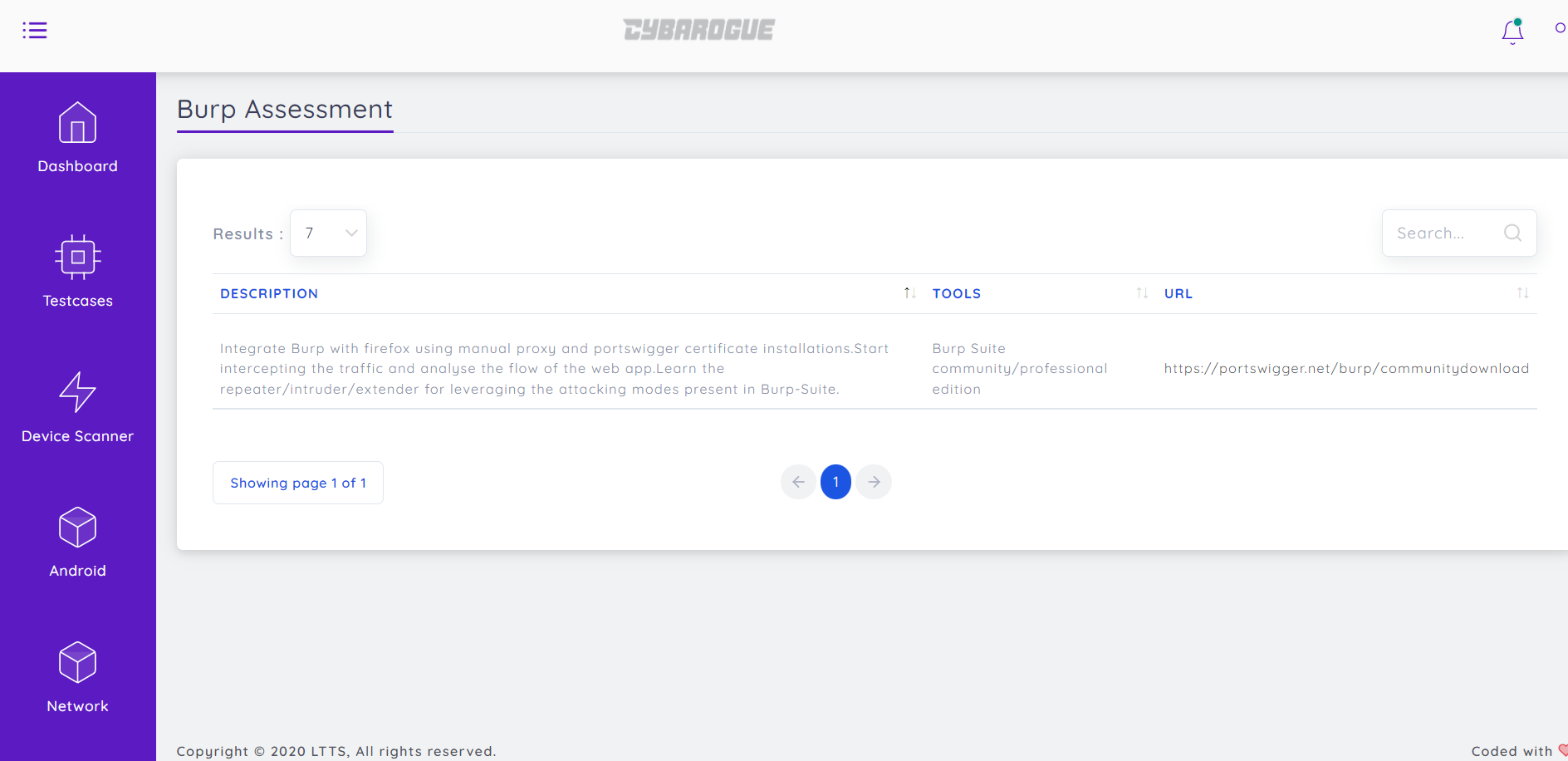
Step 1: By selecting Testcases option we can see the suboptions as follows:



Step 2: By Clicking each suboption for example if we select web we can see the list of testcases regarding to web as follows:



Step 3: By clicking view we can see the description(Definition) and also how to install and also reference link as well.



As same as Web we can get reference for all the tools in the Cybarogue by selecting each and get information about the tool like list of testscans and by clicking view we can get description, Tools and Url to download the regarding tool.

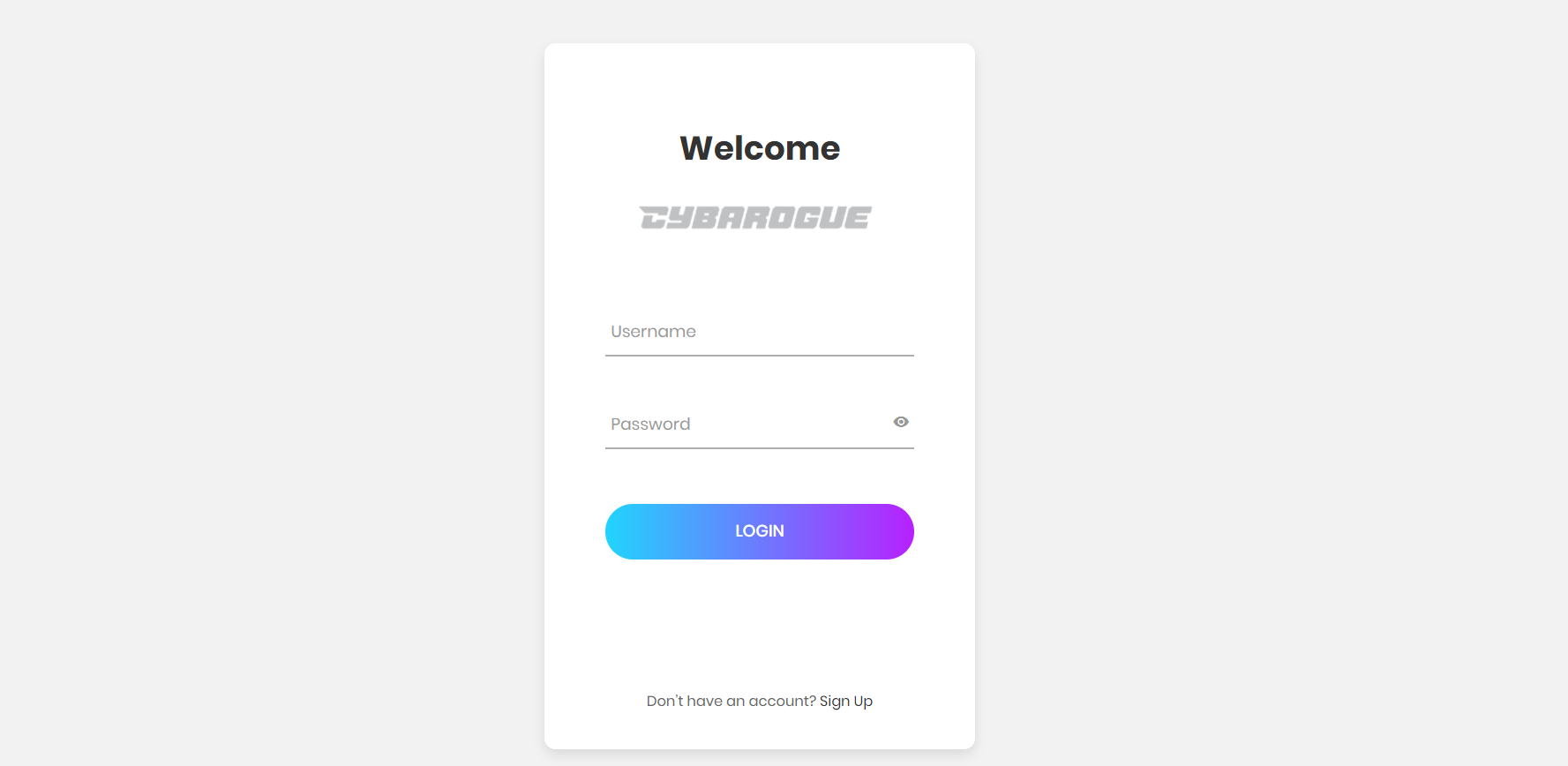
**5. Device Tool User Manual:**

5.1. Binwalk

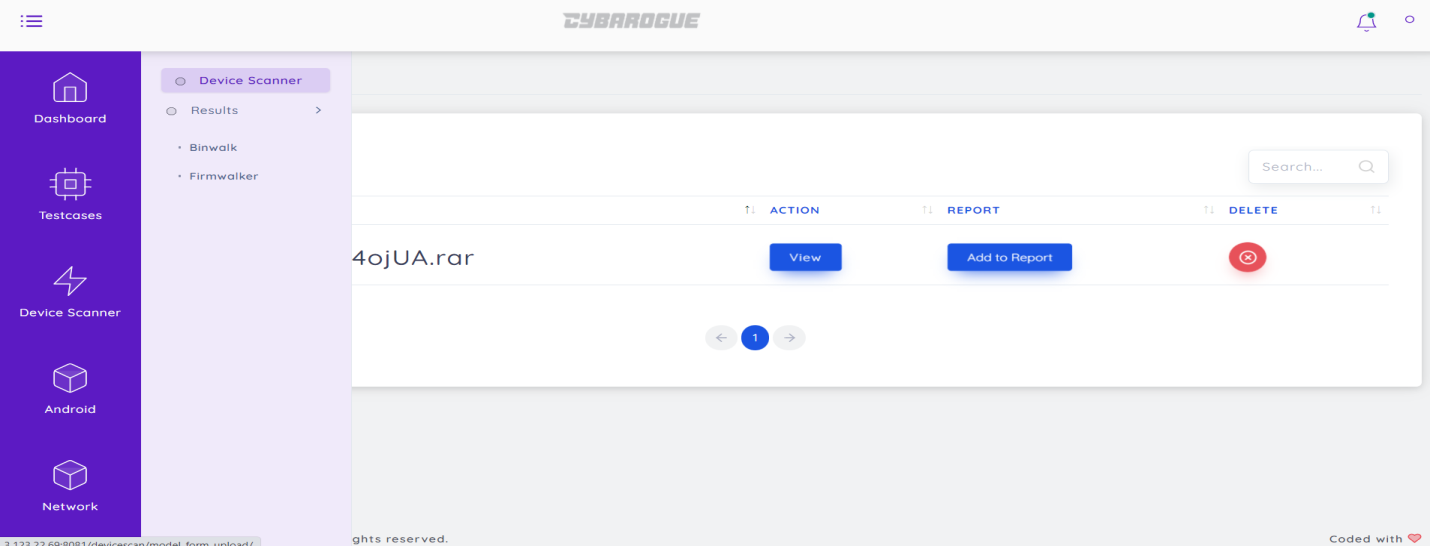
Binwalk is a fast and easy to use Python-based firmware security analysis tool that allows for firmware analysis, reverse engineering, and extraction of firmware images.

(a) User Activities:

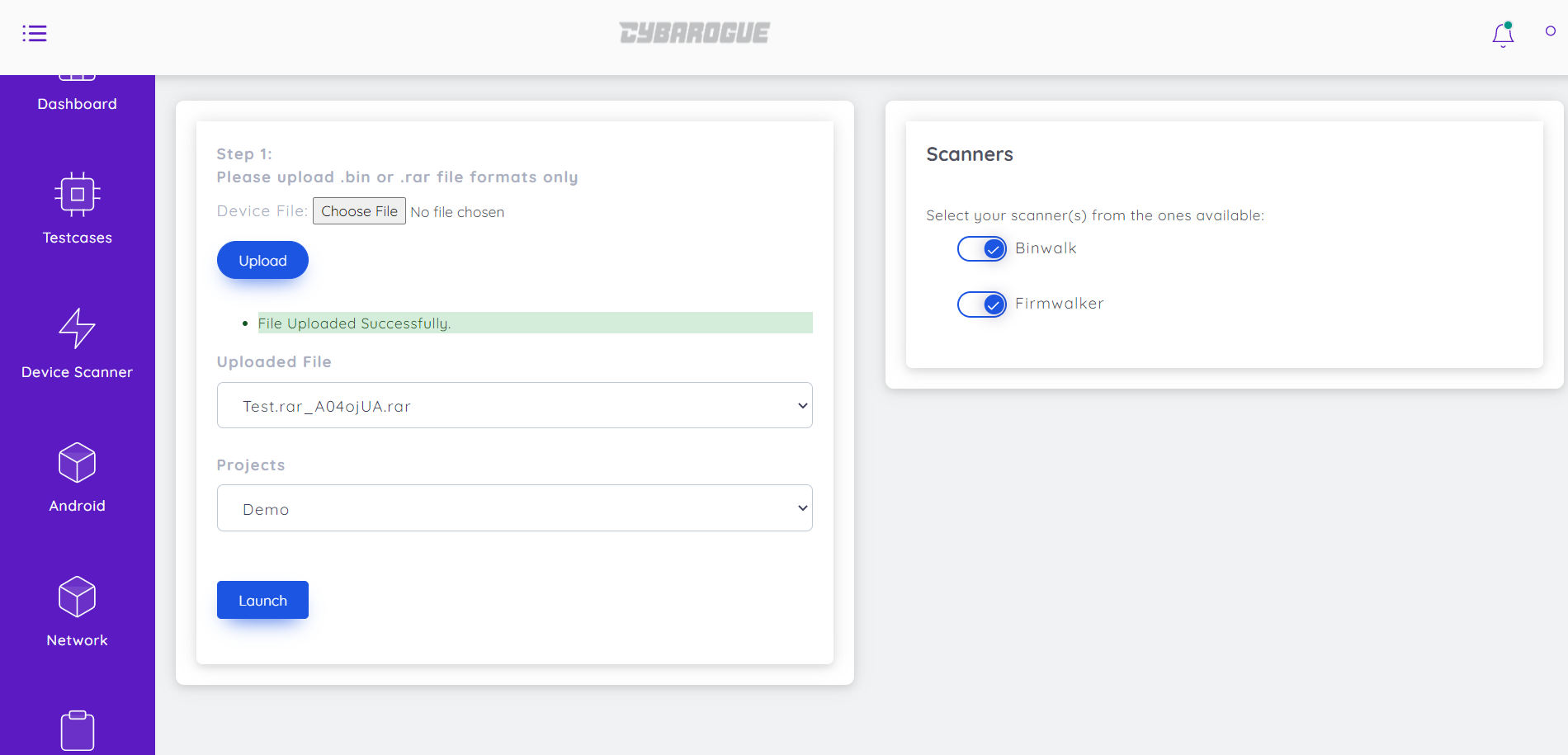
Step 1. User first make login with their respective credentials



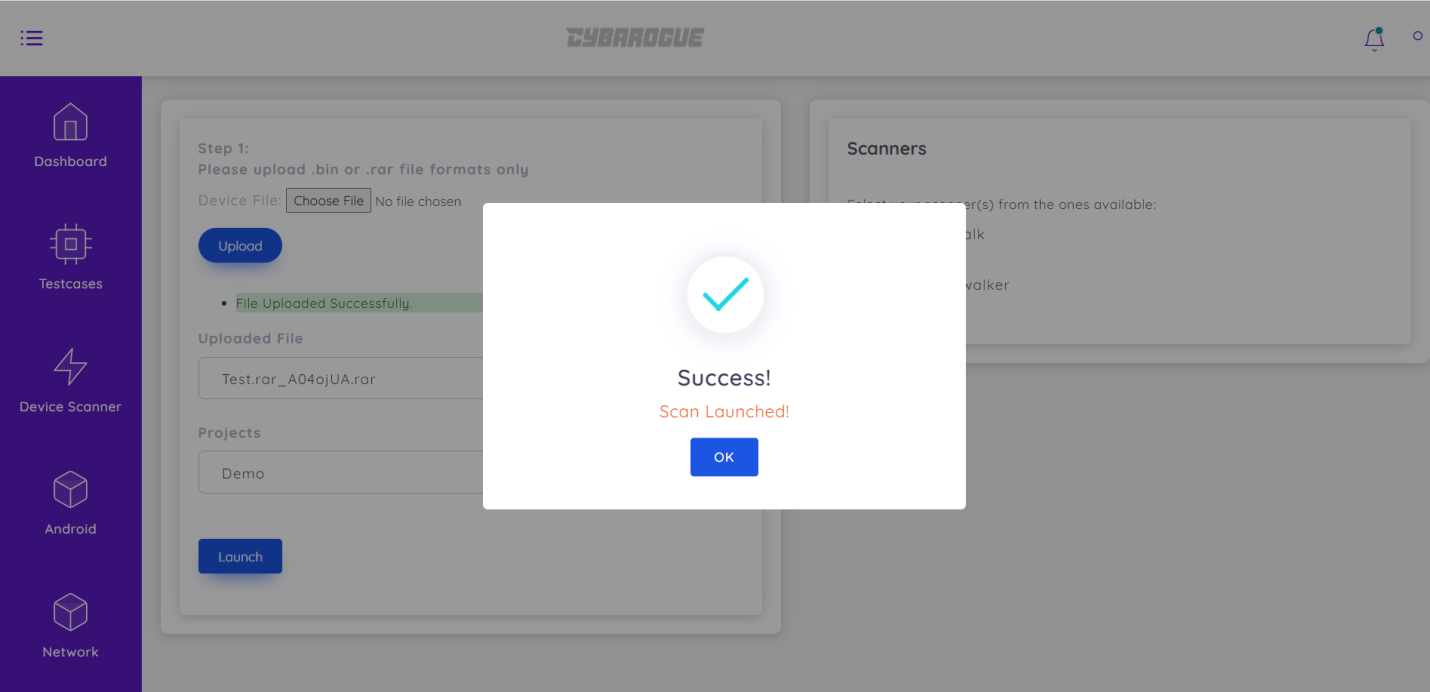
Step 2. Select device scanners which is at left side of the window it shows as follows:



Step 3. Click device scanners in that make sure that to enable Binwalk and upload file then click launch.



Step 4.After Clicking launch it gets scan launch success click ok as follows:



(d) Reports:

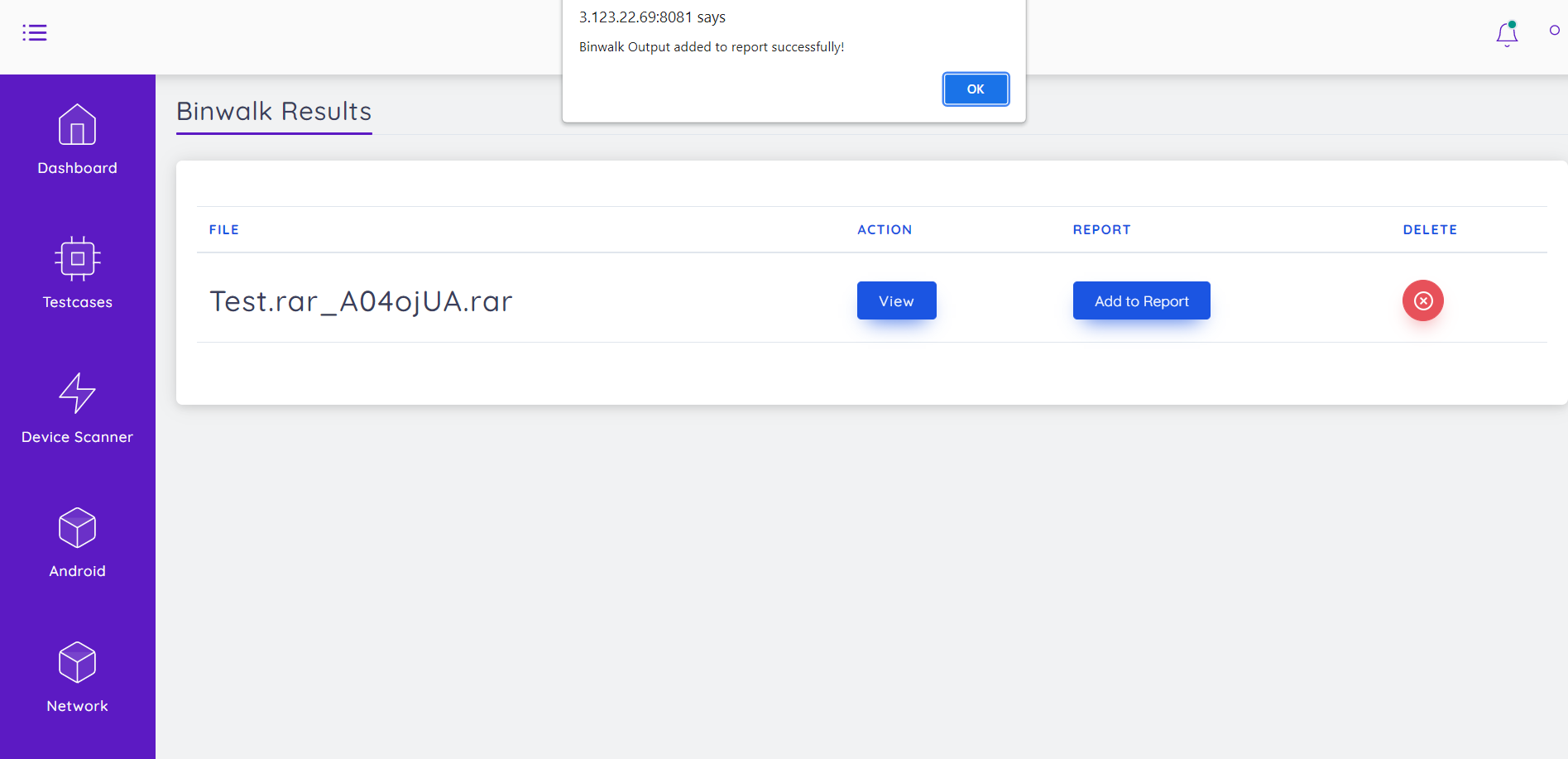
Go to Device Scanner portal🡪Results🡪 Binwalk

We can view the report by clicking view option and can use delete option if we want to delete any scan

After clicking view we can view the report as follows:



Click on add to report and then it shows an popup notification as follows by clicking ok it adds and by clicking generate report it gets download in the document format.



The binwalk generated report is as follows:



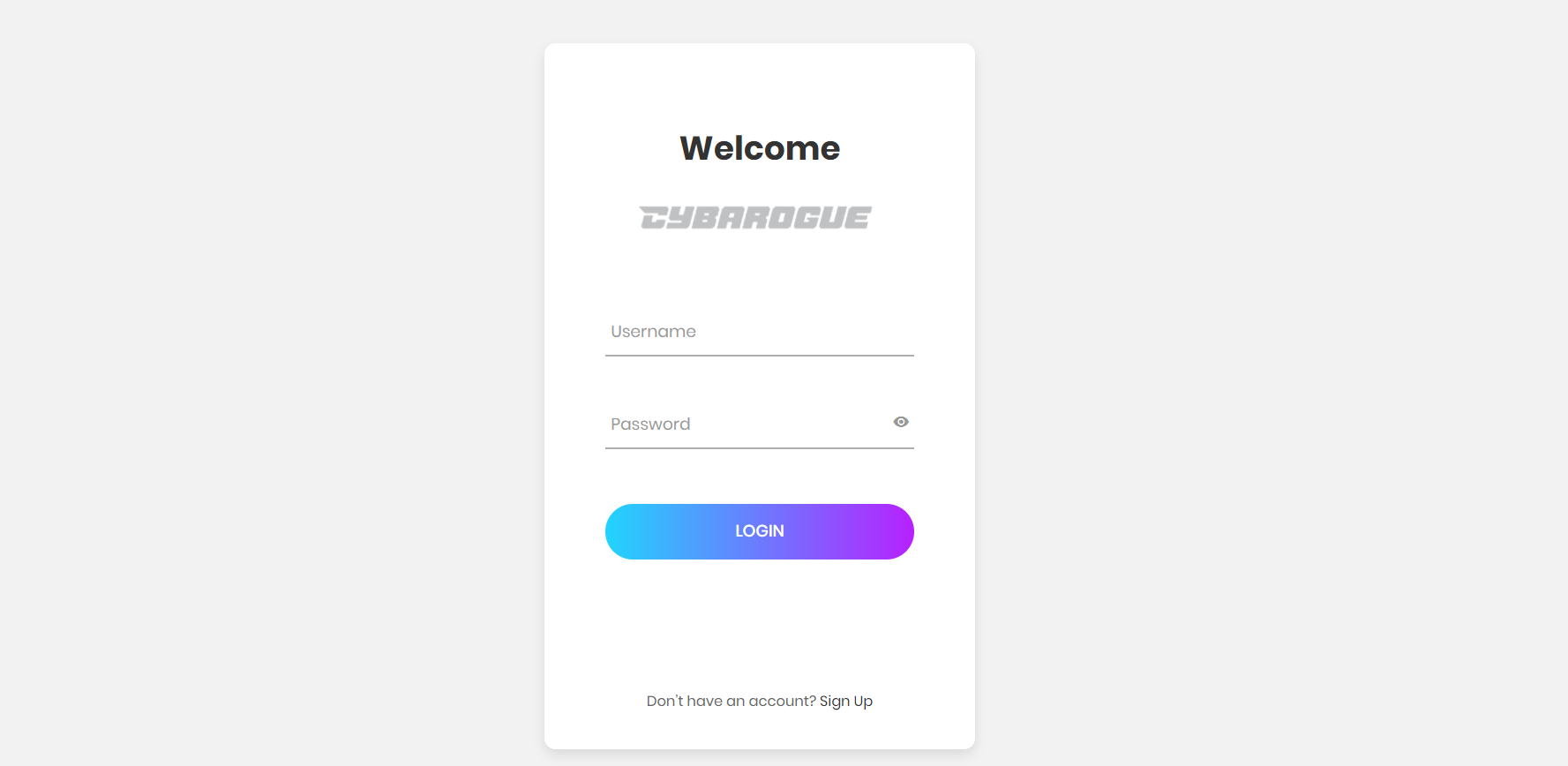
BINWALK:   
 Binwalk is an open source firmware extraction tool that extracts embedded file systems from firmware images. Binwalk is widely recognized as the leading tool for reverse engineering firmware images.  
 ***File Scanned: Test.rar\_A04ojUA.rar*** Scan ID: e378f1e8-1d64-4625-b487-51788aee0edd  
 ***Data Found:*** 0 0x0 RAR archive data  
 first volume type: MAIN\_HEAD  
  
 ***Generated By: Demo***

5.2. Firmwalker:

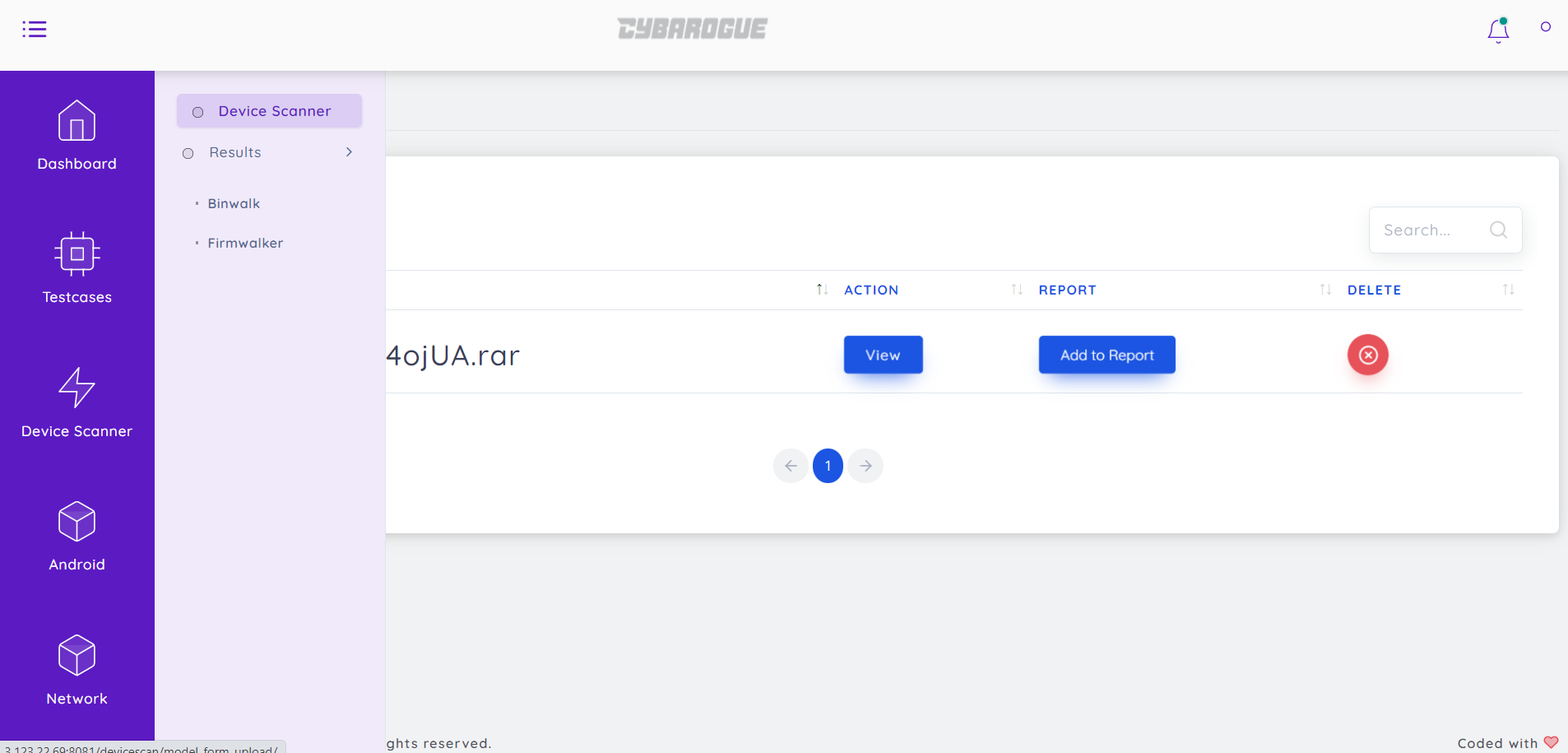
Firmwalker provides you quick initial results to initiate security assessment of firmware.

(a) User Activities:

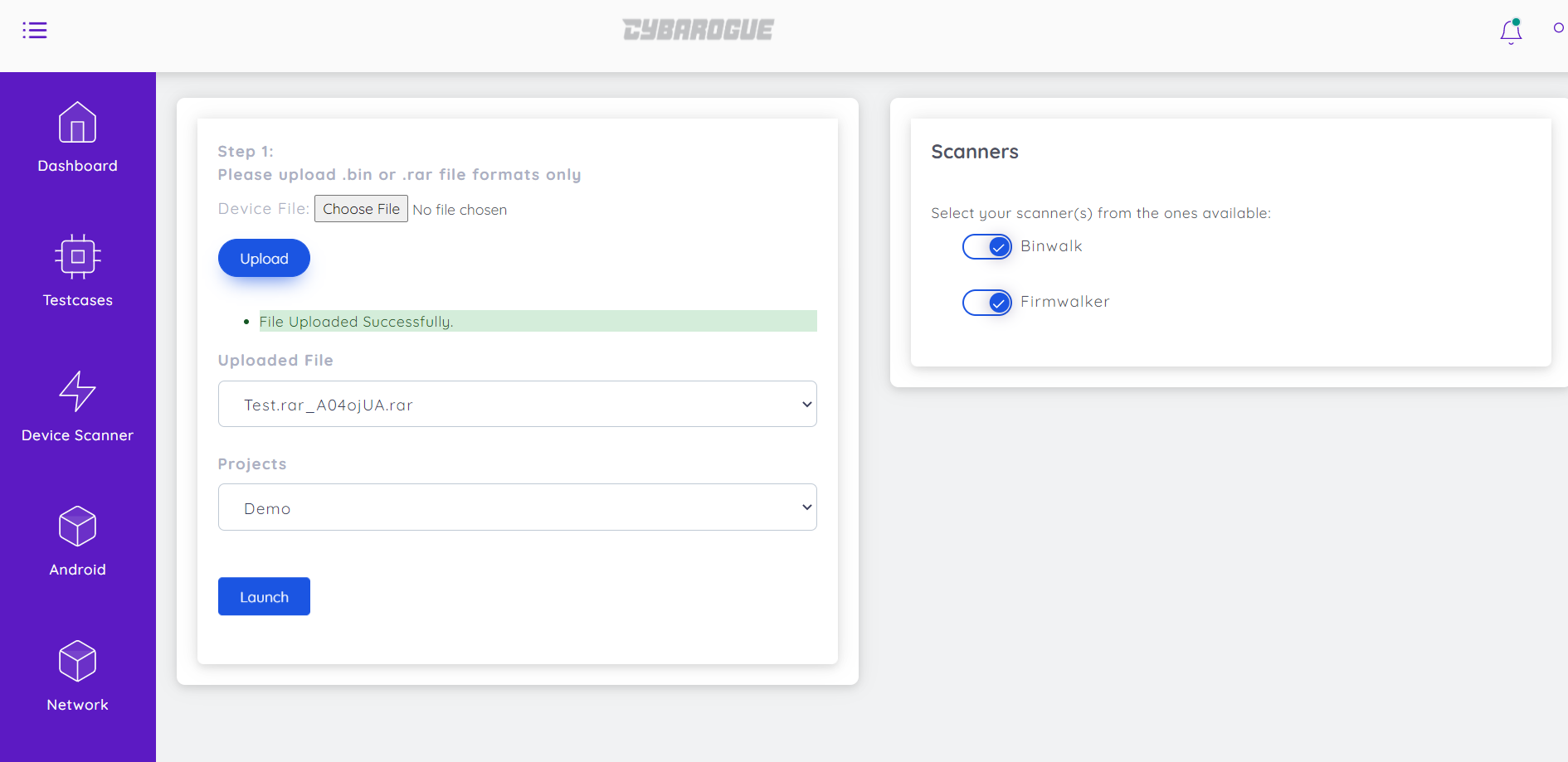
Step 1. User first login with their respective credentials



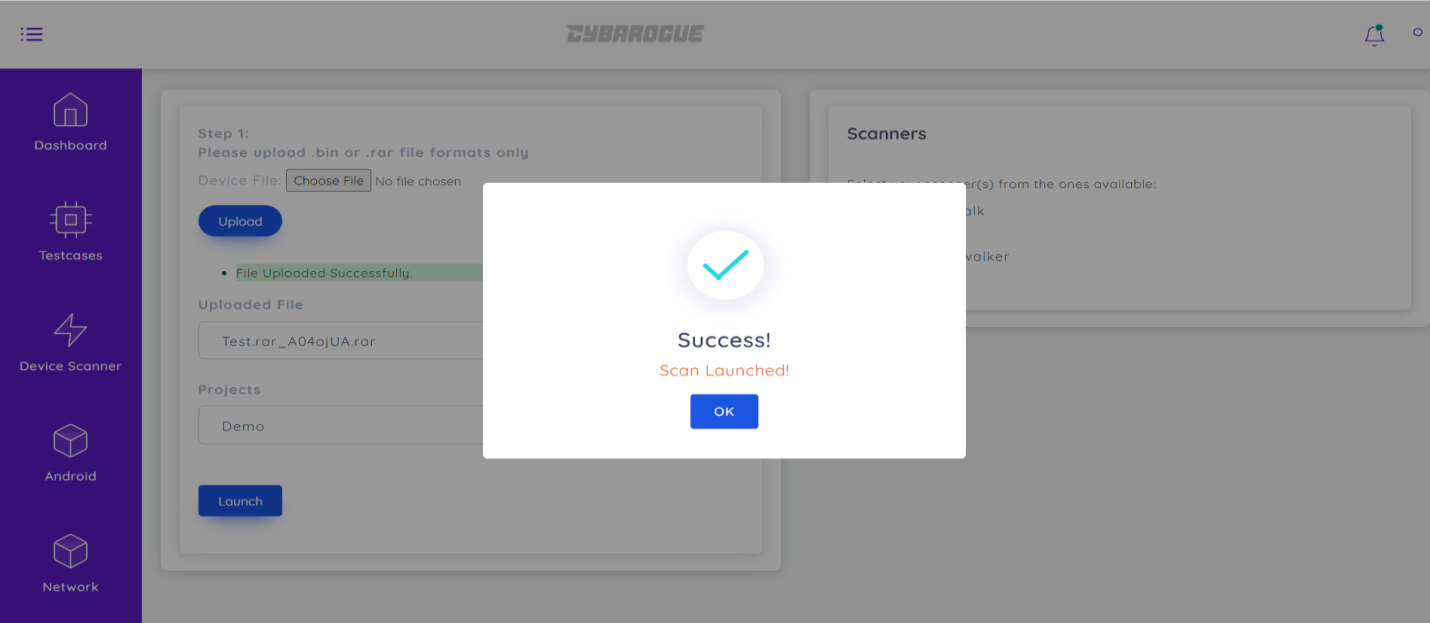
Step 2. Select device scanners which is at left side of the window it shows as follows



Step 3. Click device scanners make sure that to enable Firmwalker and upload file then click launch



Step 4.After Clicking launch it gets scan launch success click ok

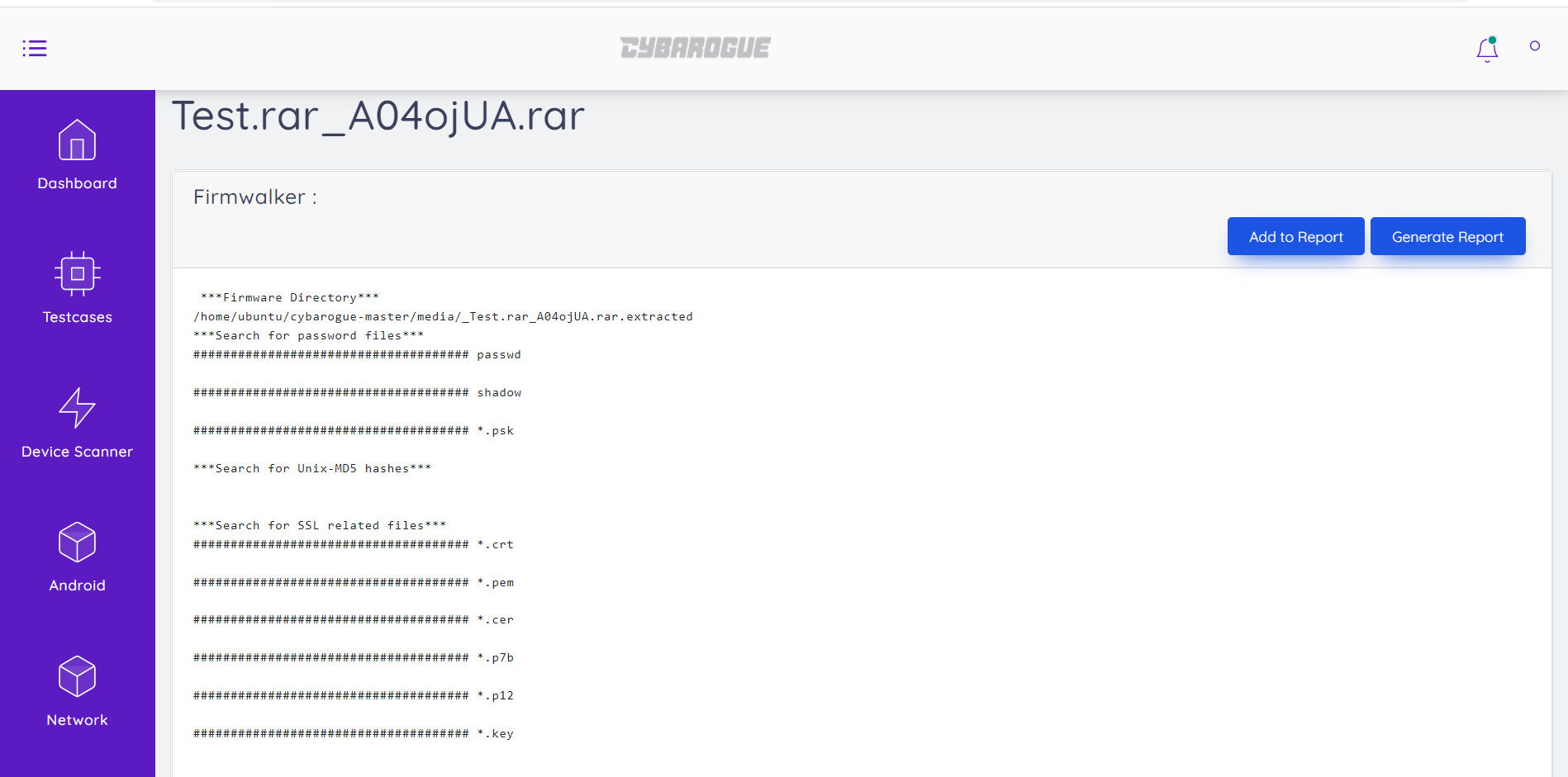


(d) Reports:

Go to Device Scanner portal🡪Results🡪 Firmwalker

We can view the report by clicking view option and can use delete option if we want to delete any scan

After clicking view we can view the report as follows:



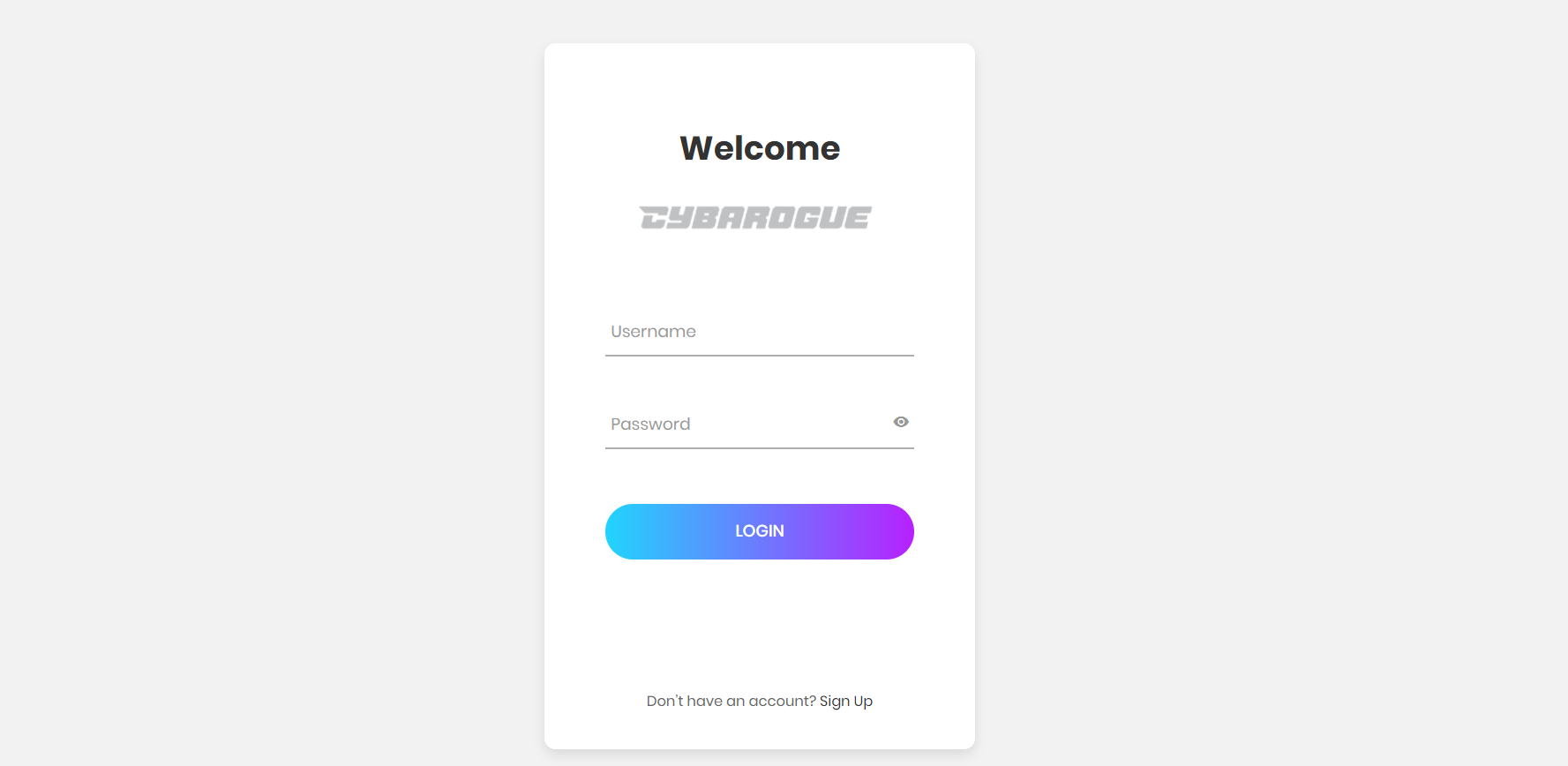
Click on add to report and then it shows an popup notification and by clicking ok it adds and by clicking generate report it gets download in the document format.

**6. Android Tool User Manual:**

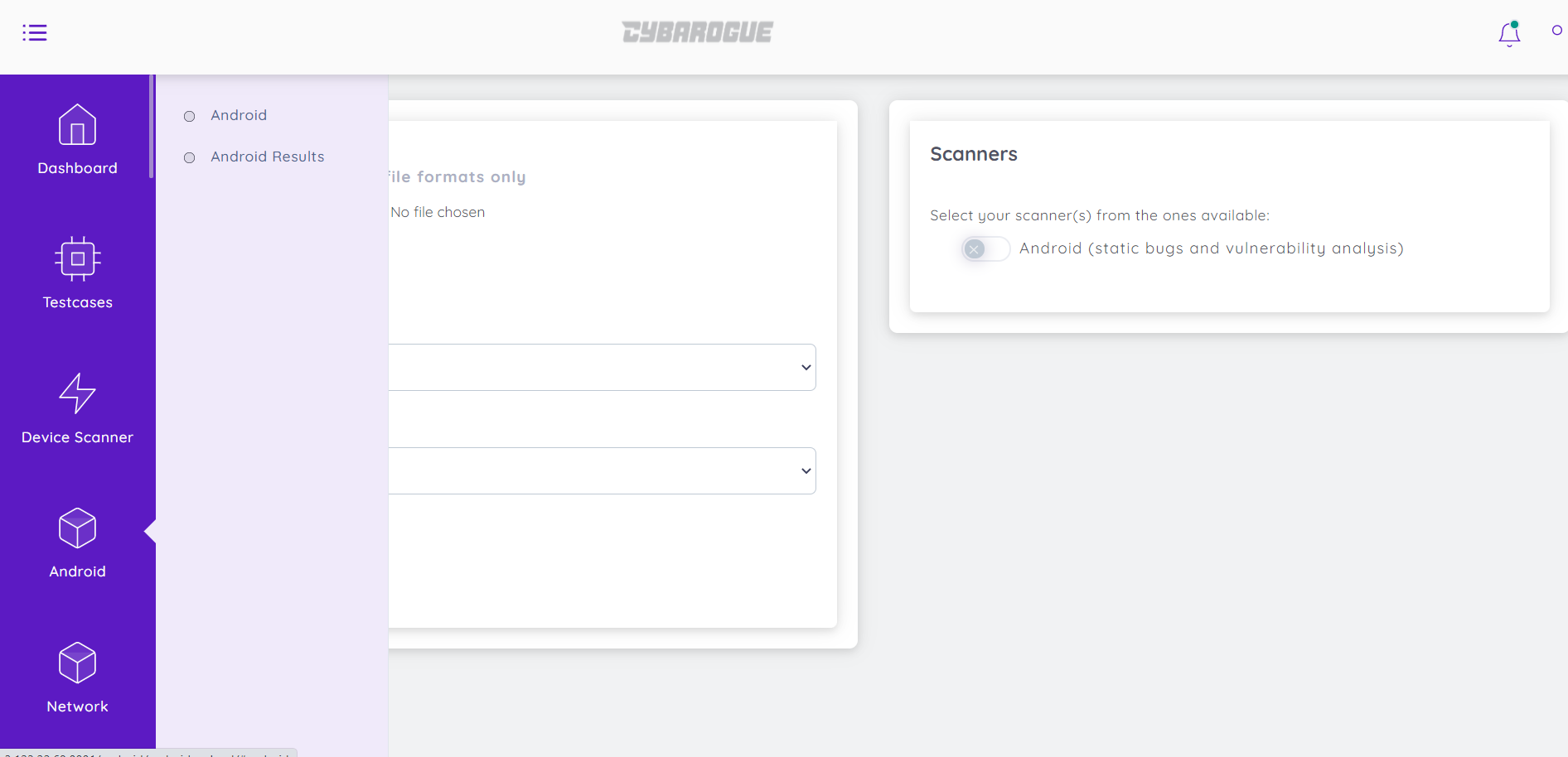
This class describes all device configuration information that can impact the resources the application retrieves. This includes both user-specified configuration options (locale list and scaling) as well as device configurations (such as input modes, screen size and screen orientation).

(a) User Activities:

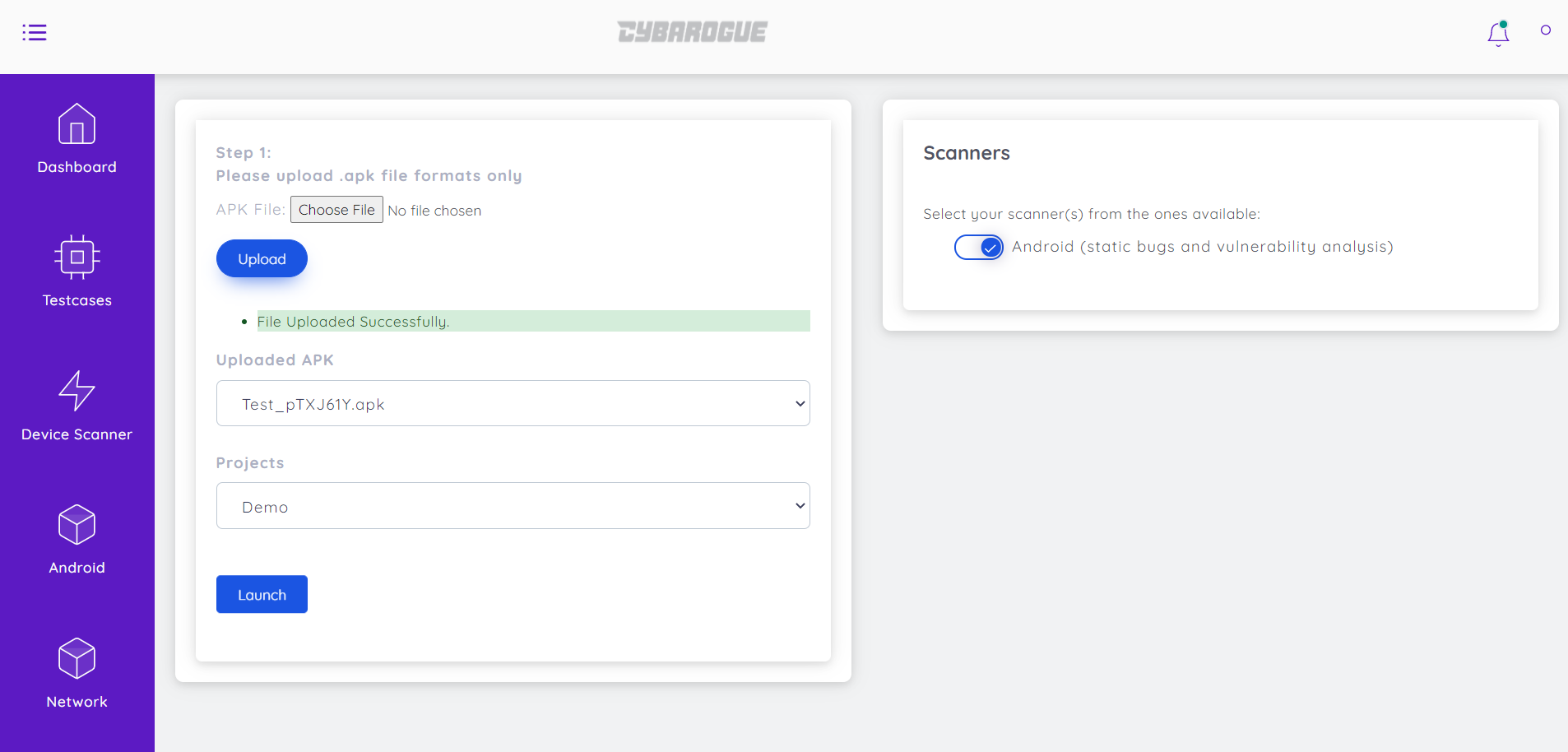
Step 1. User first make login with their respective credentials



Step 2. Select Android which is at left side of the window it shows as follows



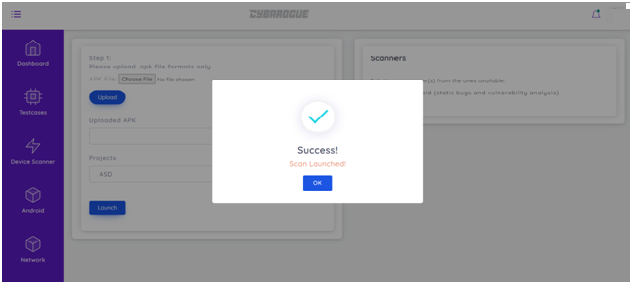
Step 3. Click on Android in that enable android upload any apk file and click upload then choose uploaded file,choose project type and click launch.



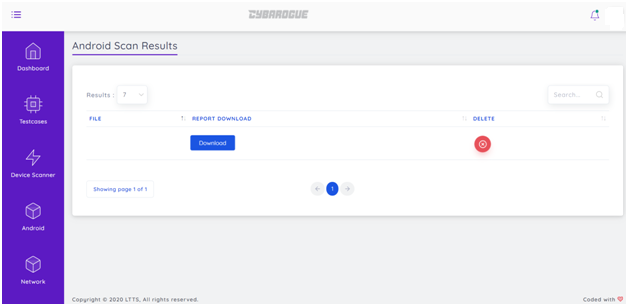
Step 4.After Clicking launch it gets scan launch success click ok

(d) Reports:

Go to Android portal🡪 Android Results



If we want to delete any scan click on delete option it deletes the scan and To download report click download and it downloads report in the form of zip file.



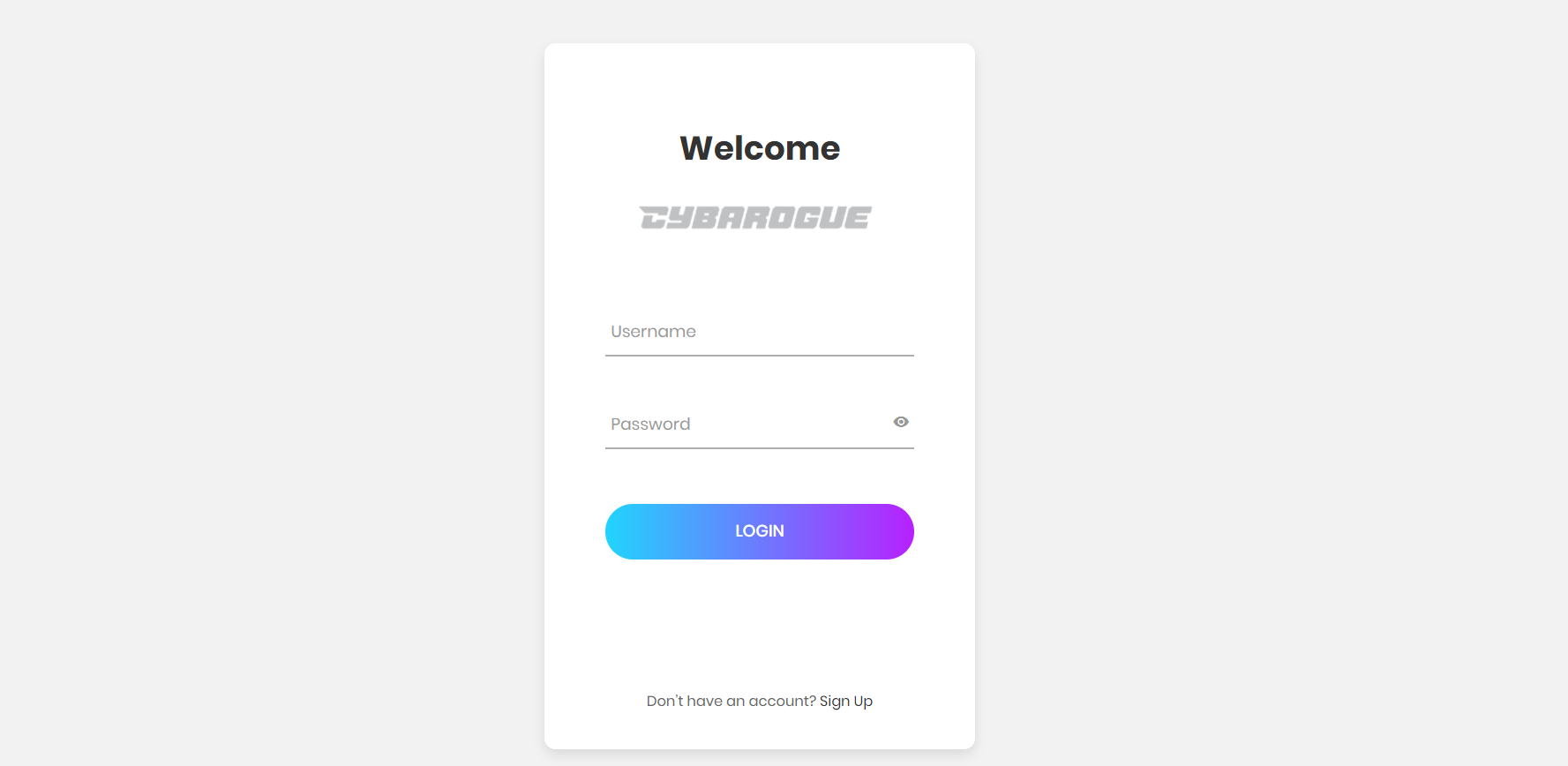
**7. Network Tool User Manual:**

In Network Application tools we use Nmap, NetCreds/Password Extractor and Pcap Analyser to design our framework.

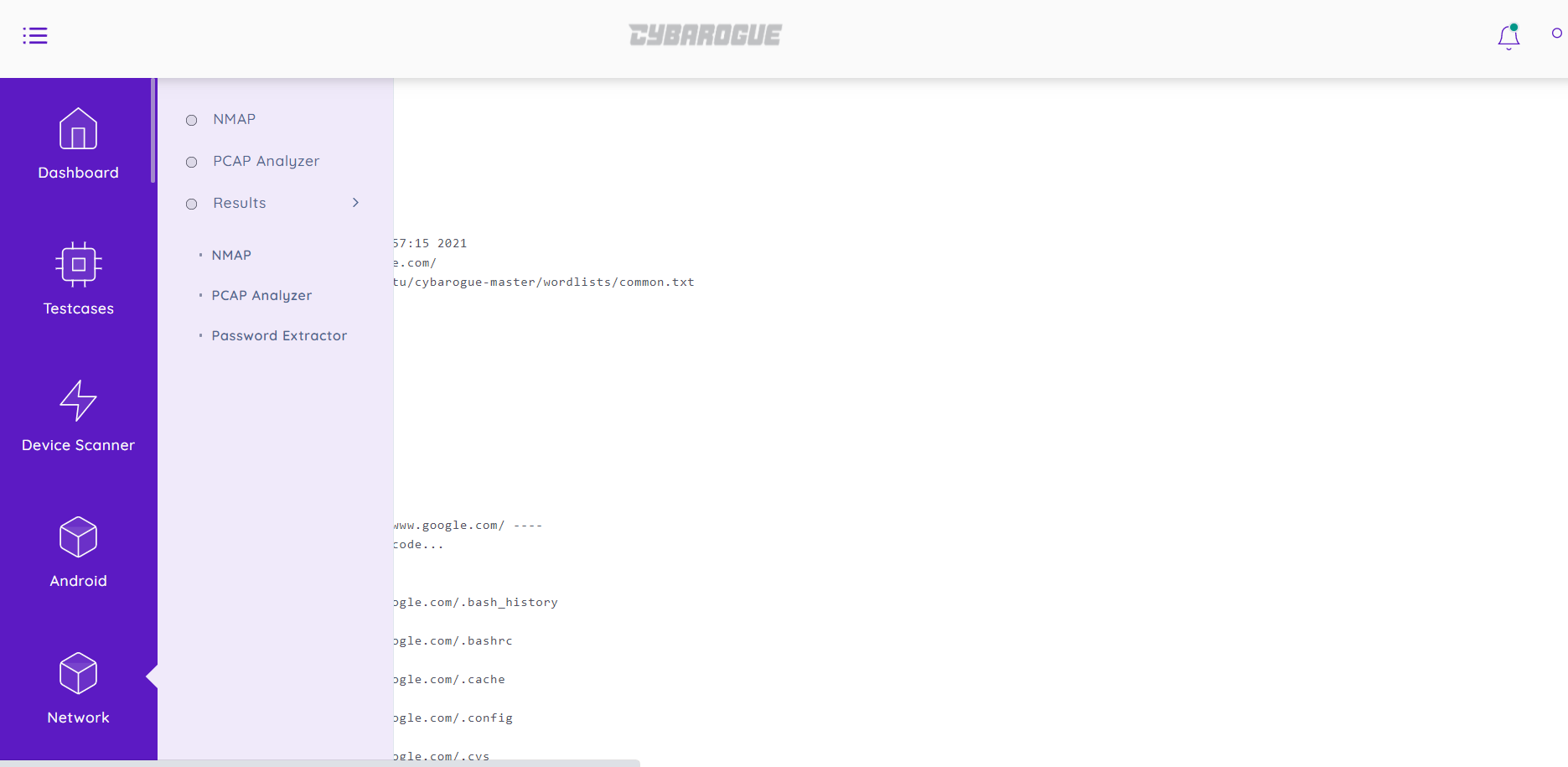
7.1. Nmap Tool User Manual:

(a) User Activities:

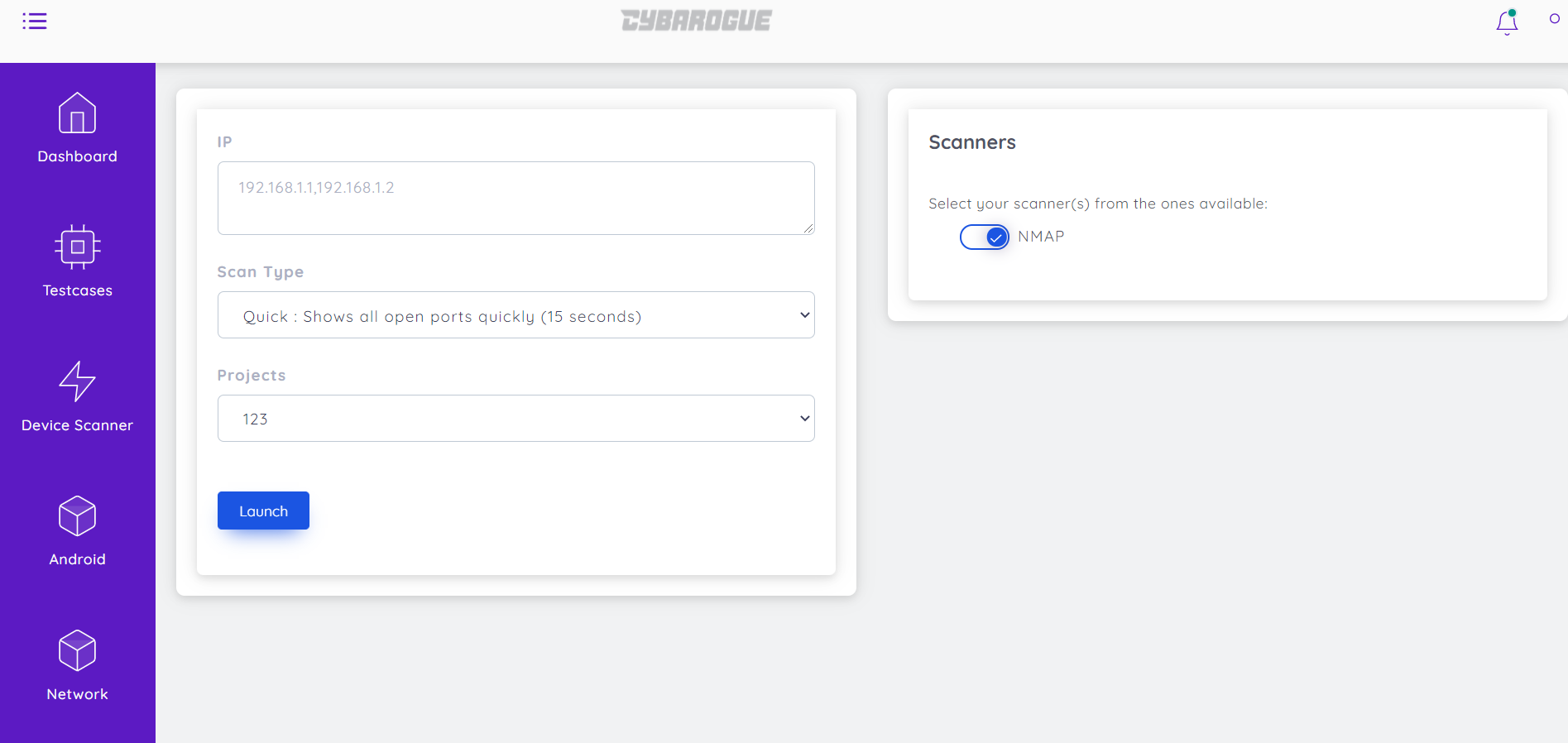
Step 1. User first login to Cybarogue with their respective credentials.



Step 2. Now, for usage of Nmap, User must click the Network which is at left side of the window

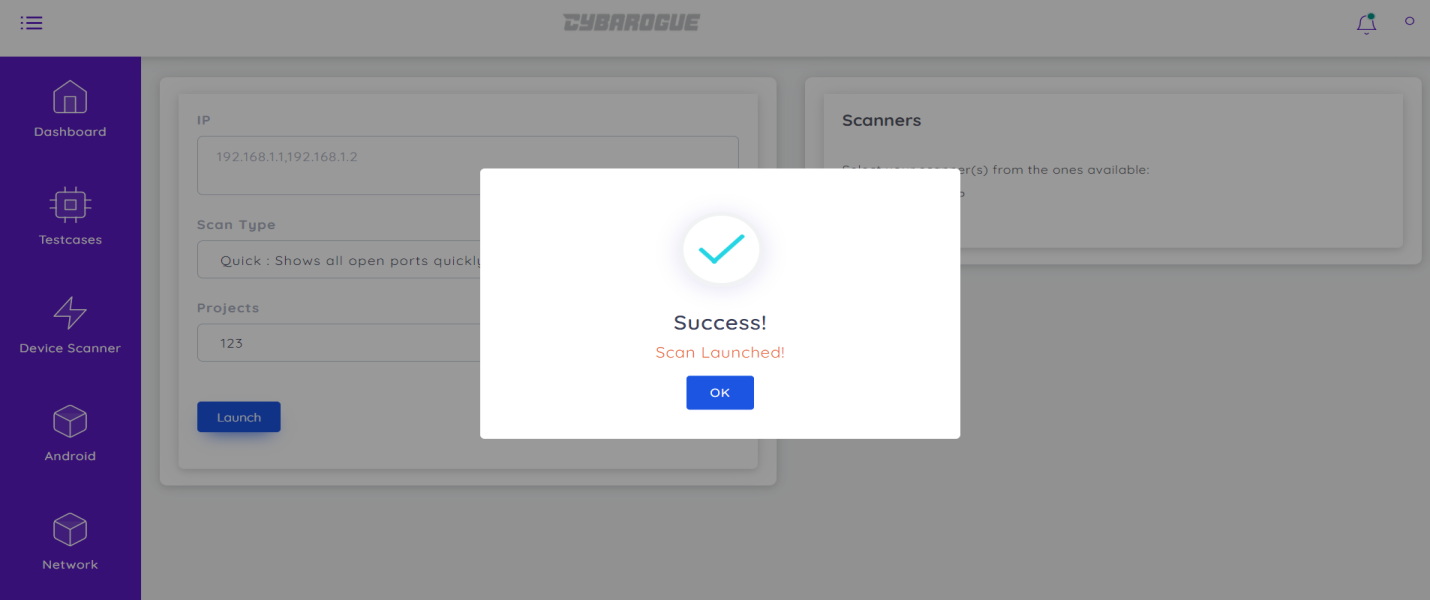


Step 3. In that give a click on NMAP, then it appears as following:



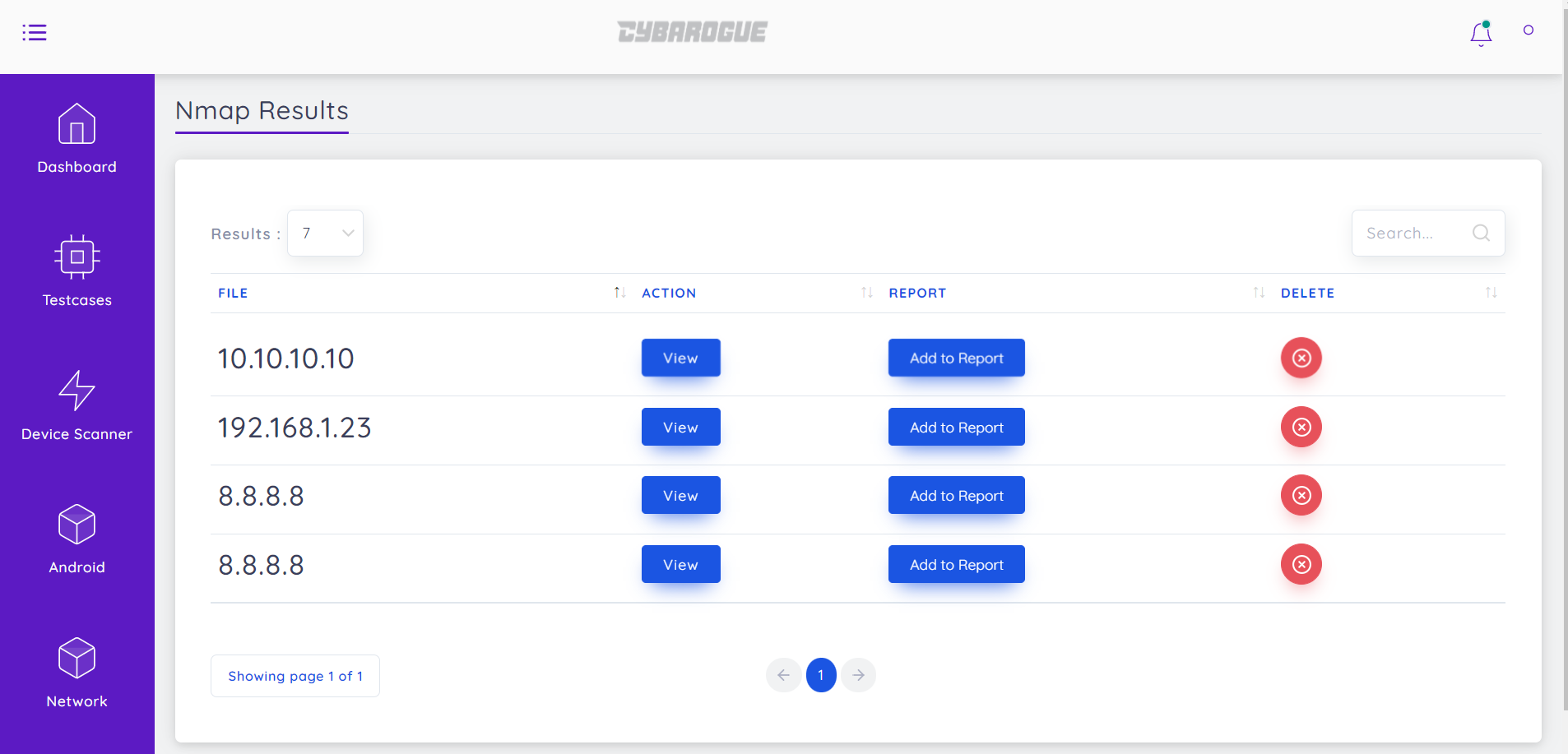
First give IP that which you need the ports and select scan type which you want and projects and enable nmap which is at right side finally give a click on launch

Step 4. After Clicking launch it displays, scan launched success then click ok.

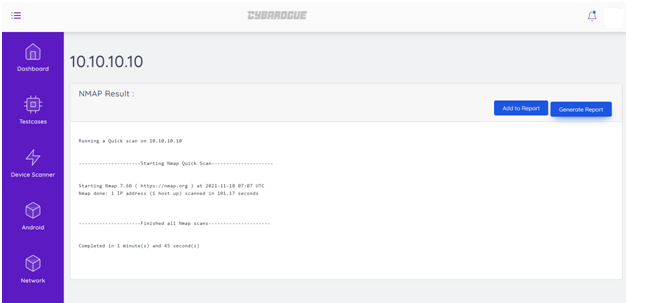


(d) Reports:

Click on Results->Nmap results then it displays as below:



After clicking view, it displays results then click on add to report



Finally clicking on Generate report then it automatically downloads the report as following in document format:



NMAP SCAN:   
 Nmap is a free and open source utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It is designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems.   
 ***URL Scanned: 10.10.10.10  
 Scan ID: 211e6e24-bfe4-4831-bbd6-9ea4f8a9f92f  
 Scan Type: Quick*** Result: Starting Nmap 7.60 ( https://nmap.org ) at 2021-11-18 07:07 UTC  
  
 ***Generated By: rs***

7.2. Pcap Analyser User Manual:

Packet capture analysis provides metrics for effective network performance monitoring, which makes it a versatile tool for IT specialists and network administrators. For instance, network packet analysis can indicate the location of network performance issues, show network configuration data, and ultimately understand the cause of slow network performance. Network troubleshooting isn’t the only use for packet analysis, though.

### Ensuring Security

Data packets can serve as an important component of network security monitoring. PCAP analysis tools help you to automate and visualize traffic patterns, so you can identify security threats as soon as they arise. For instance, packet capture analysis shows real-time network traffic data that can quickly show a spike in unauthorized activity.

**Finding Congestion**

Packet sniffing offers a real-time view of your data’s travel times, which can help you identify traffic congestion.

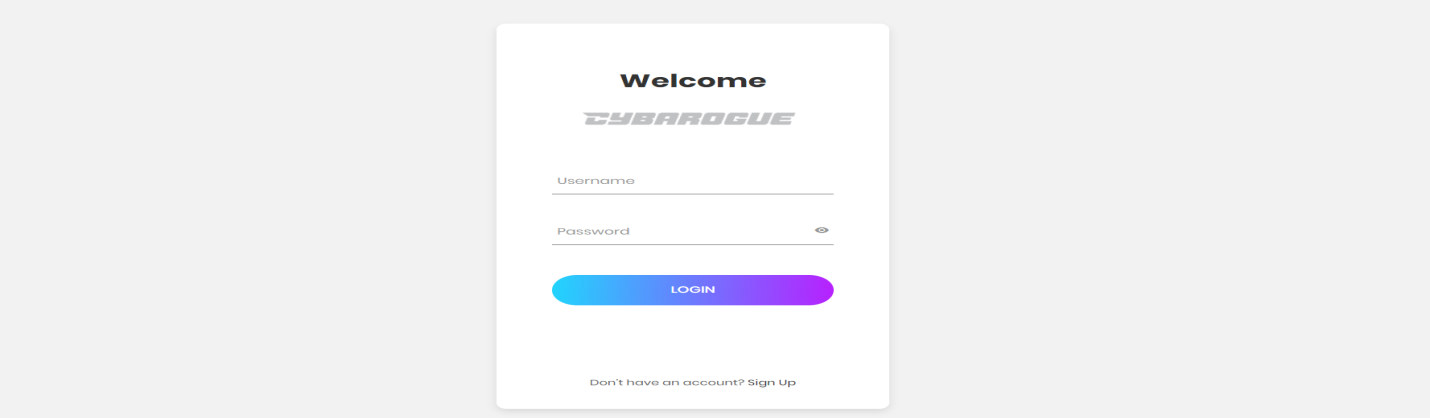
**Troubleshooting**

Once you have flagged a network problem with your PCAP analysis, you can dive into the granular dimensions of each packet to identify the source of the issue. Even if you only capture metadata, you can track down important details of unusual packets for effective troubleshooting.

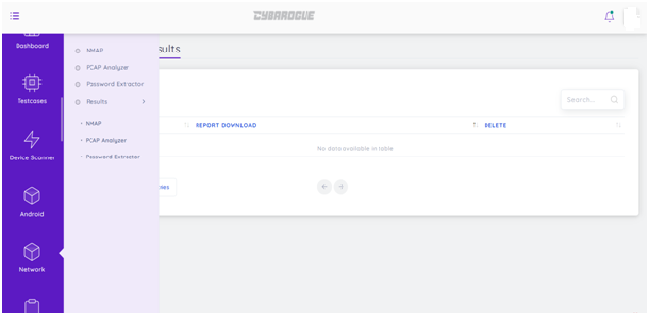
Because of its multipurpose use, packet analysis software is a crucial component of a comprehensive network performance management system. Packet analysis with PCAP API allows you to document the histories and transmission details of each data packet for a real-time understanding of your network performance.

(a) User Activities:

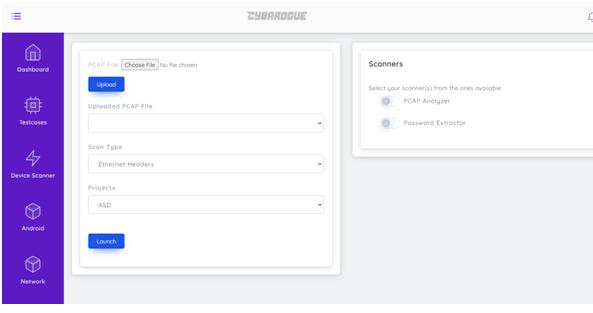
Step 1. User first login with their respective credentials.



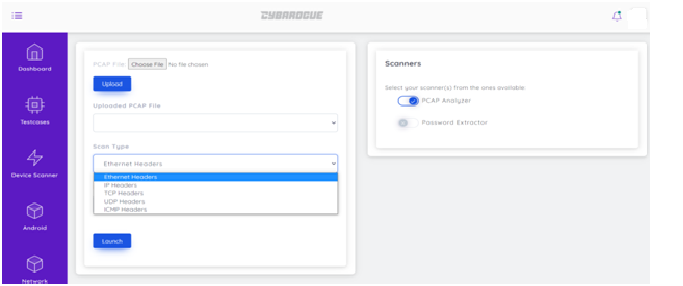
Step 2. Now, for usage of pcap analyser, User must click the Network which is at left side of the window same as Nmap and Pcap analyser is below the Nmap which is shown below:



Step 3. After Clicking Pcap Analyser it opens

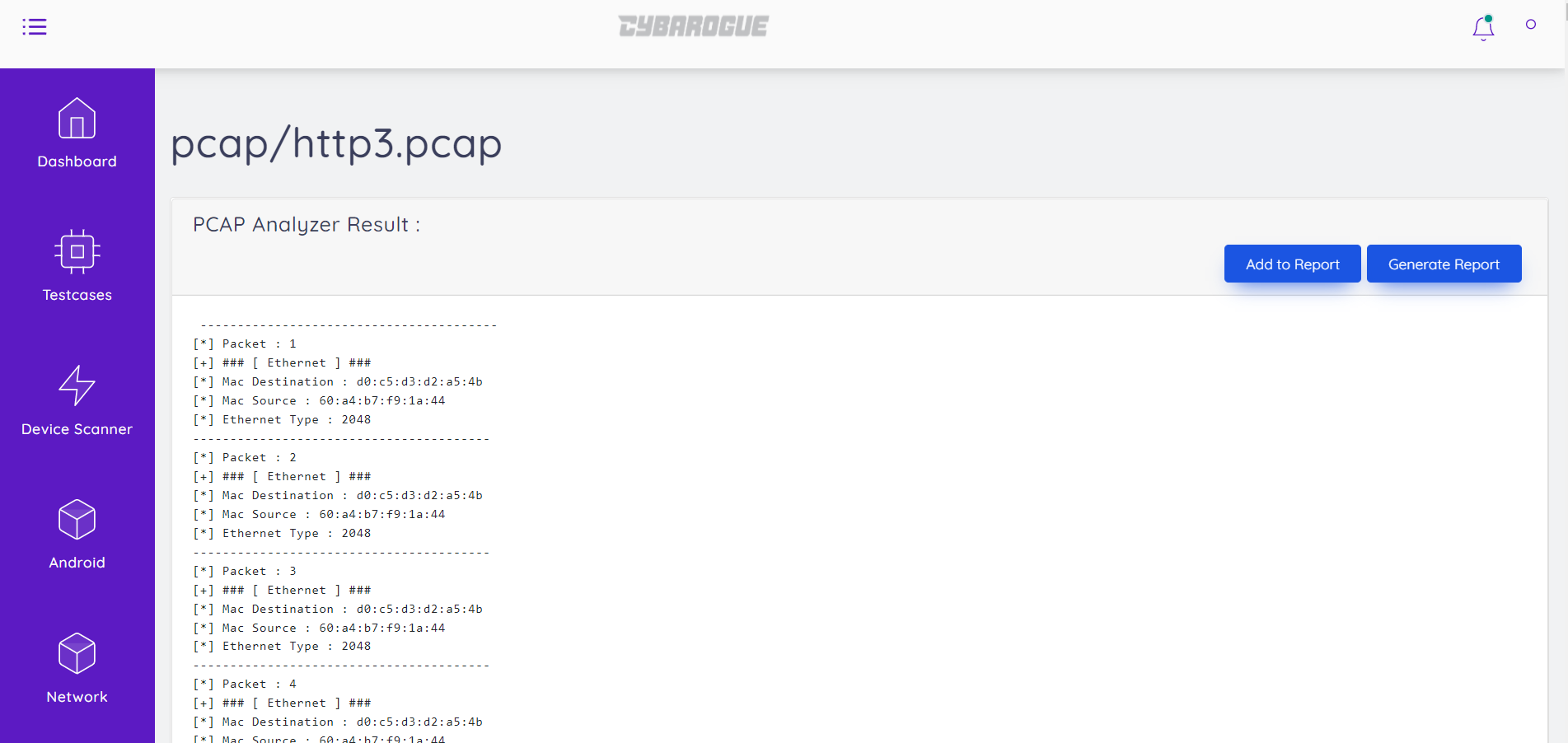


Step 4. First Choose any Pcap file that you want to capture packets then click on upload then it shows the uploaded file in uploaded pcap file then select scan type what you want then select projects and enable pcap analyser and finally give a click on launch.



(d) Reports:

Click on Results->Pcap Analyser results then Click on view then select add to report and then select generate report then it automatically downloads report as document format:



7.3. Password Extractor User Manual:

Same as Pcap Analyser, While enabling Password Extracter in the place of Pcap Analyser then it generates the report.

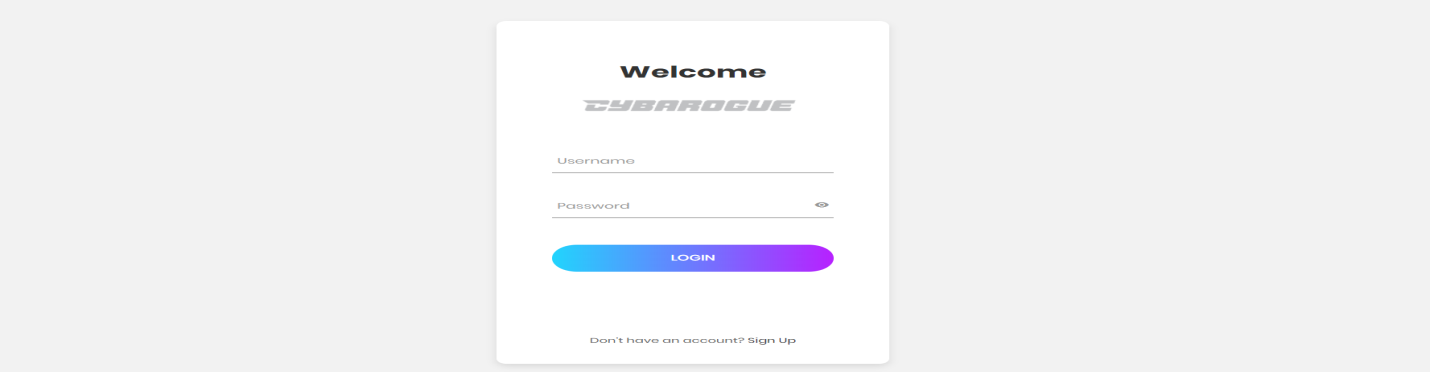
**8. Web Tools User Manual:**

In Cybarogue under Web Application tools we consider are SSLScan, Wapiti, Whatweb and Nikto to design our framework. Lets Know user manual of each Tool.

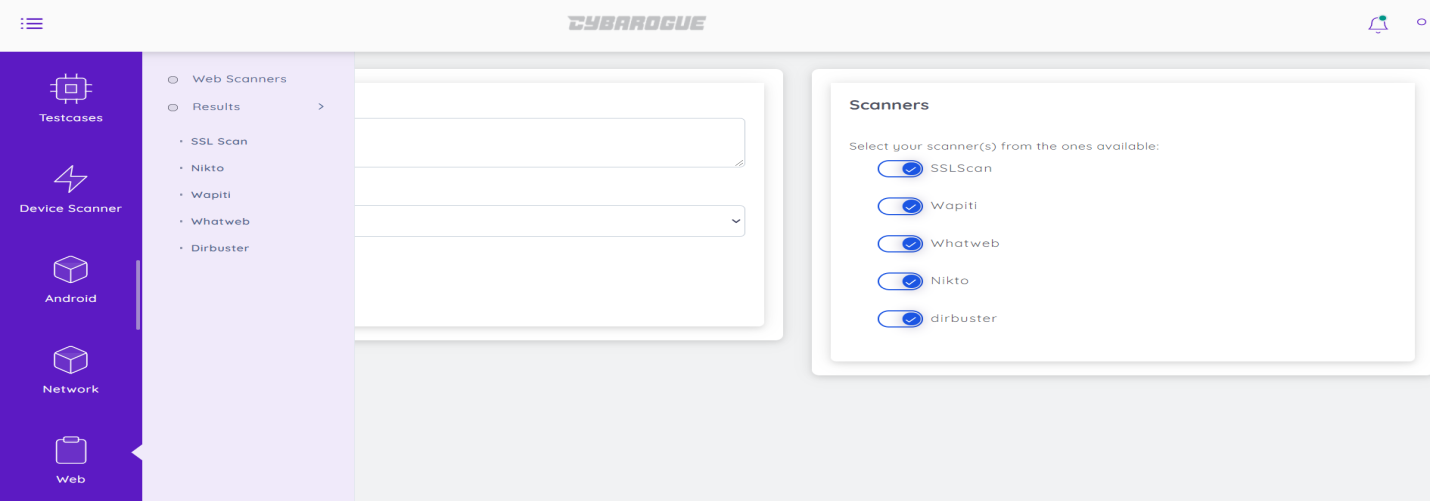
8.1. SSLScan User Manual:

(a). User Activities:

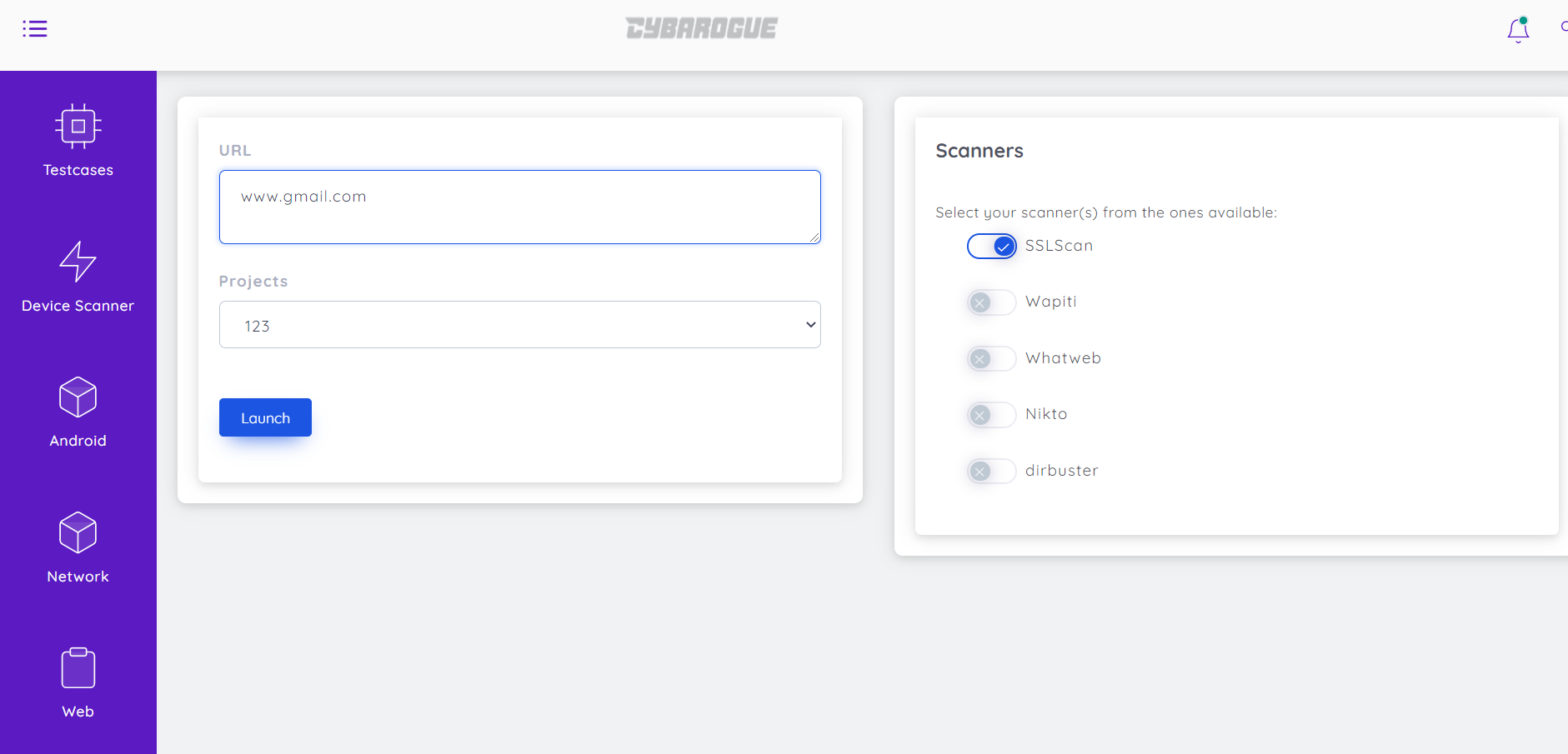
Step 1. User first make login with their respective credentials.



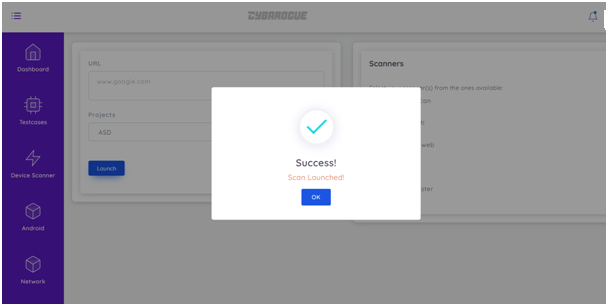
Step 2. Select Web portal which is at left side of the window it shows webscanners



Step 3. In Webscanners select SSLScan and give url to scan and select project, click launch

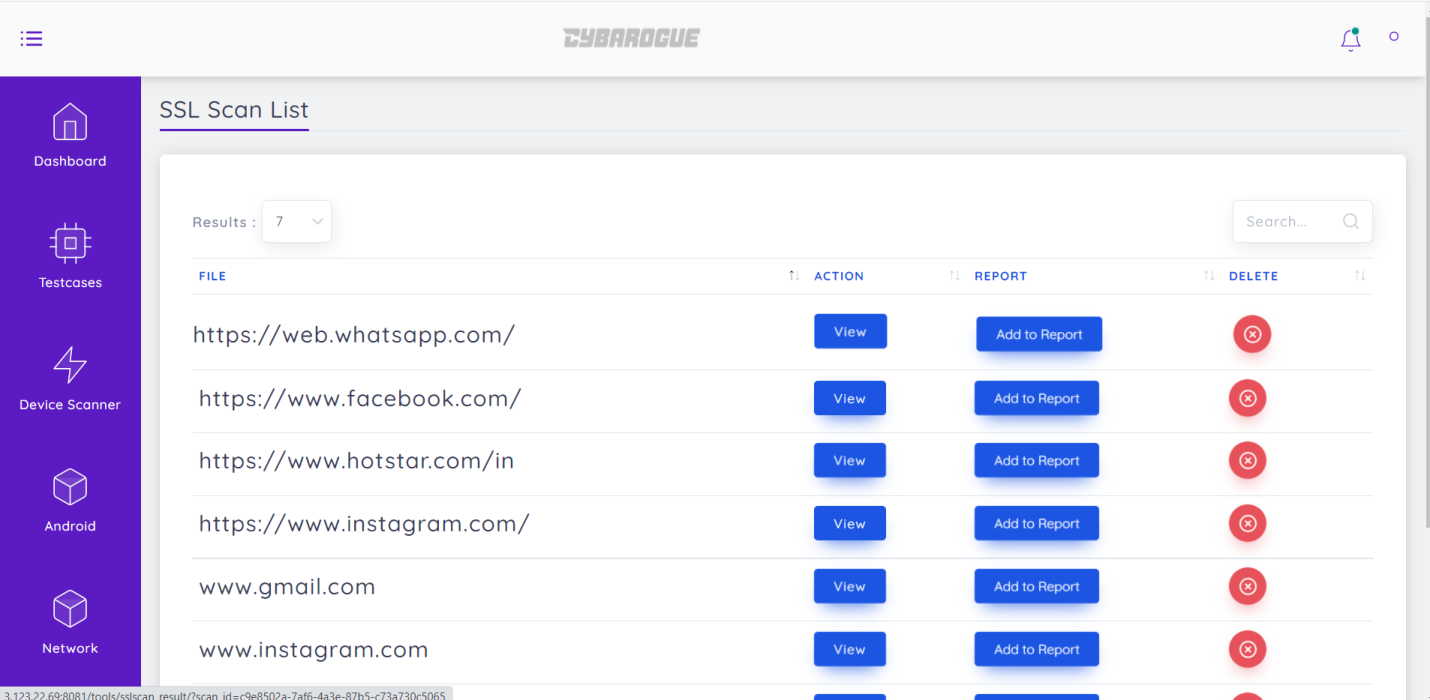


Step 4. After Clicking launch it displays, launch success then click ok.

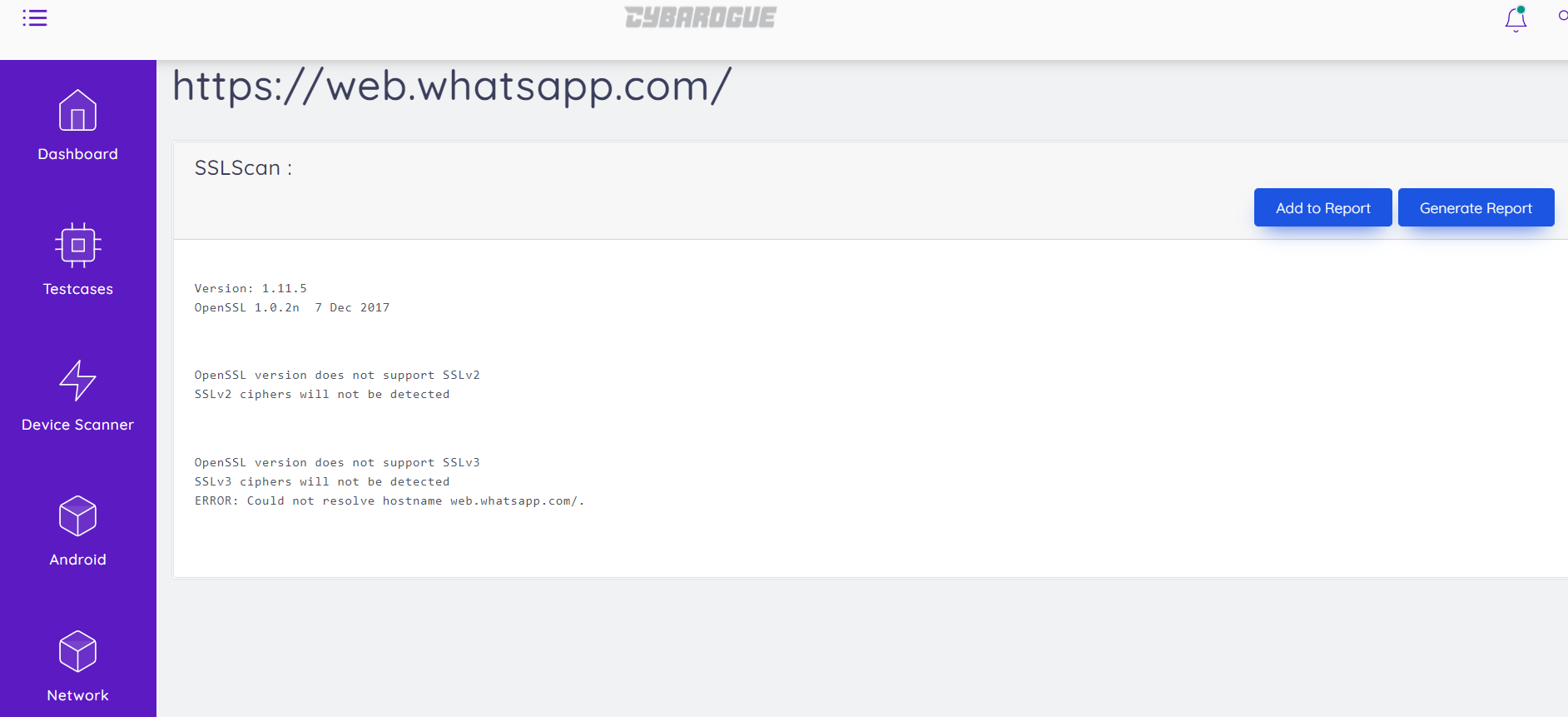


(d) Reports:

Go to Web portal🡪 Results-🡪SSLScan



Click on view and then select add to report and then select generate report then it automatically downloads report as document form at.

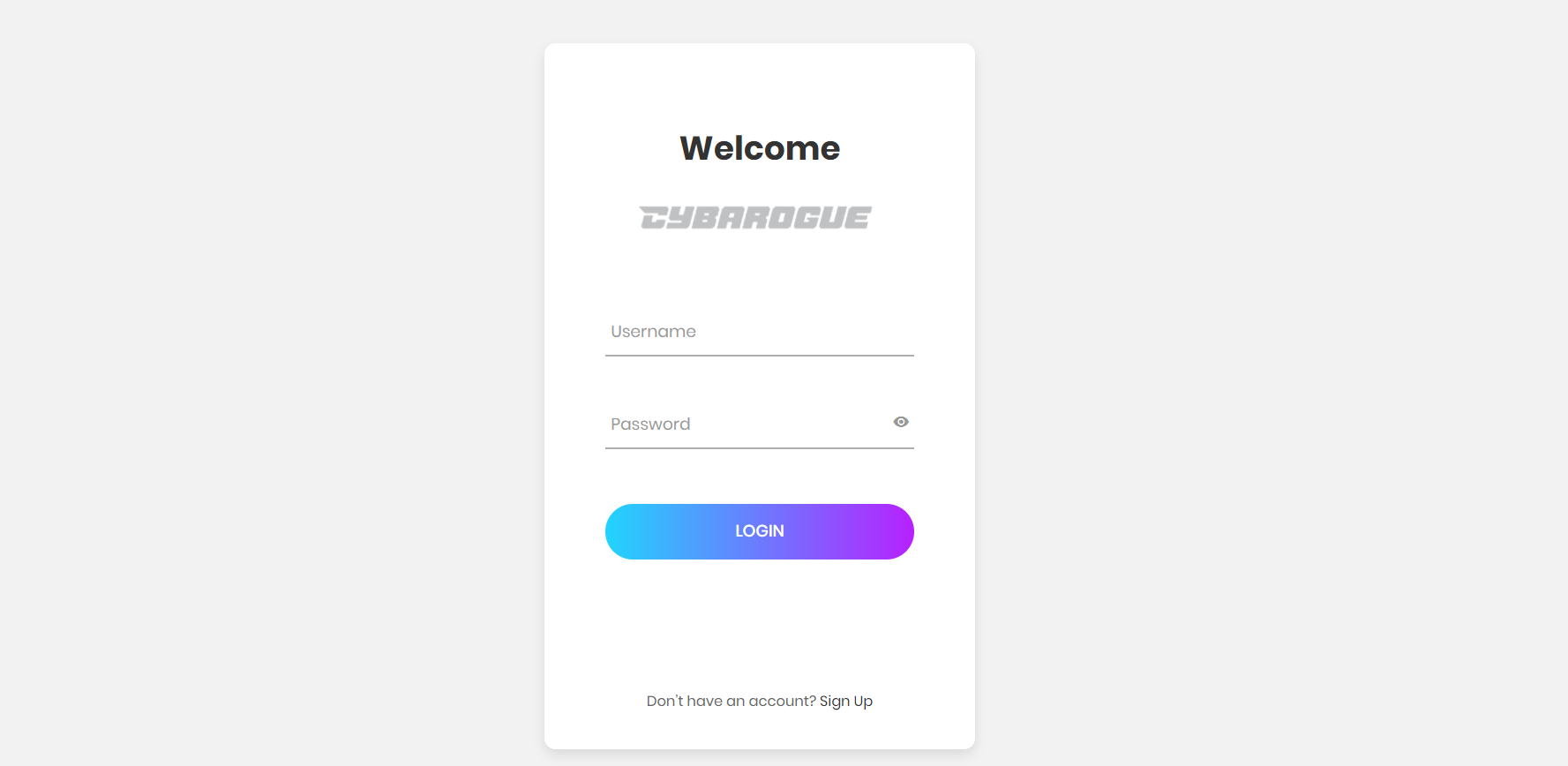


8.2. Wapiti User Manual:

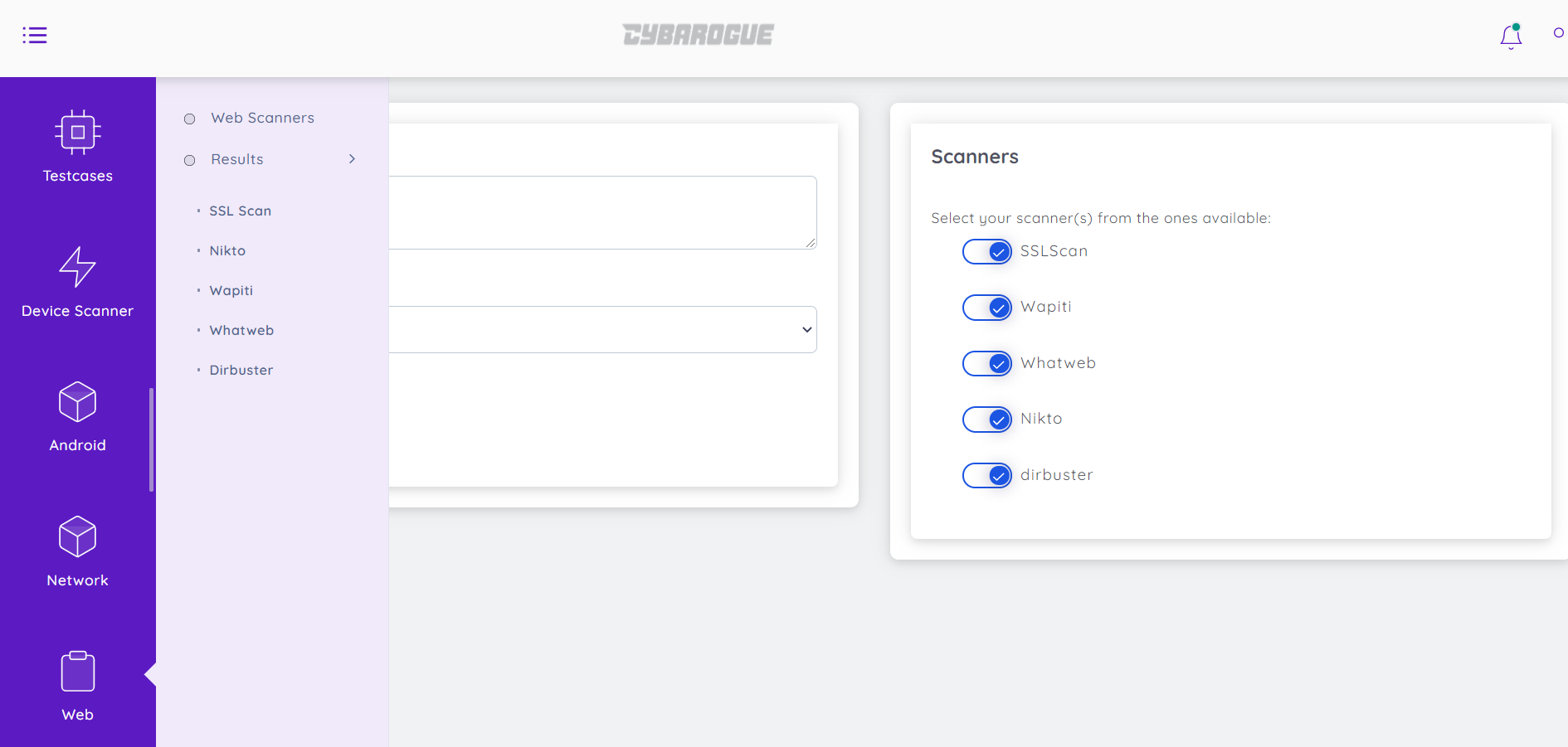
Wapiti allows you to audit the security of your websites or web applications.

(a) User Activities:

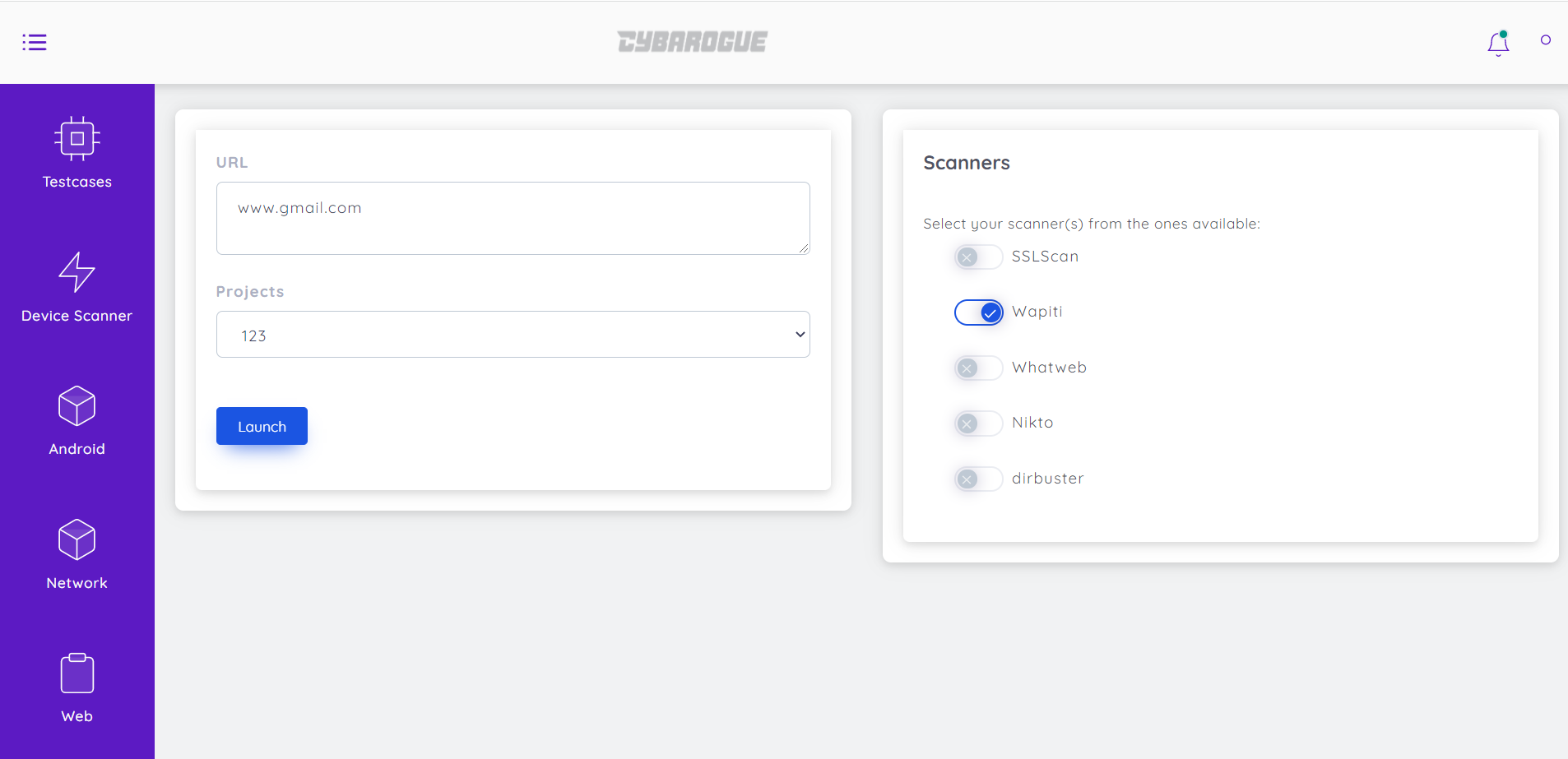
Step 1. User first make login with their respective credentials.

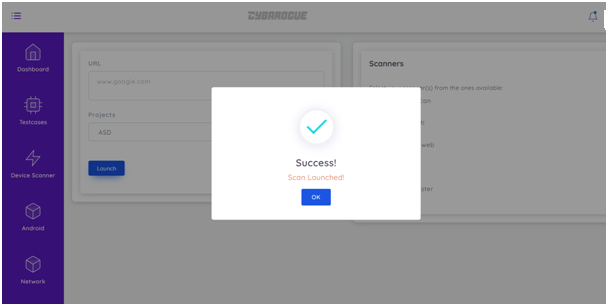


Step 2. Select Web portal which is at left side of the window it shows webscanners



Step 3. In Webscanners select Wapiti and give url to scan and select project, finally click launch

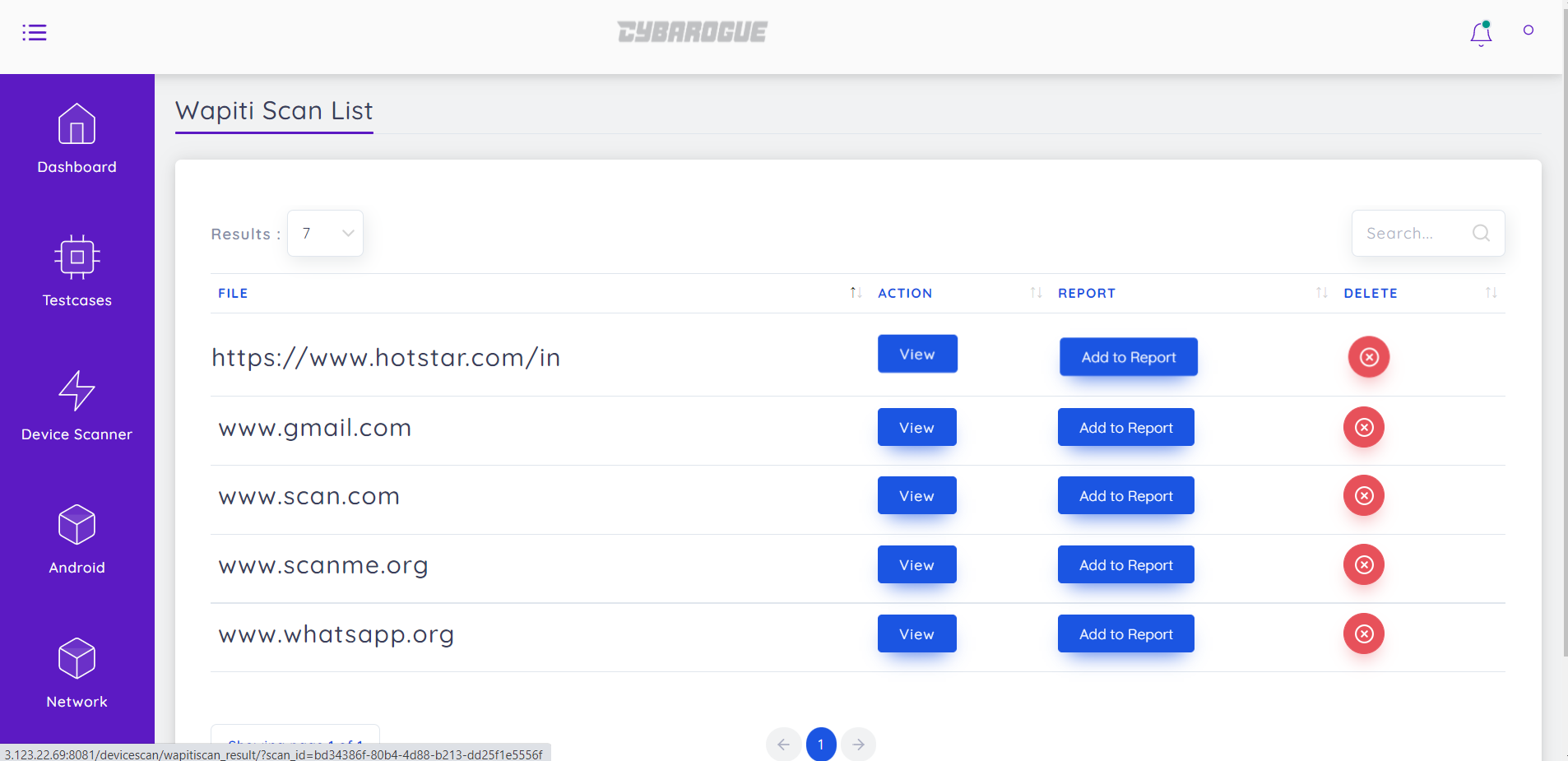


Step 4. Then it displays that launch success then click ok. 

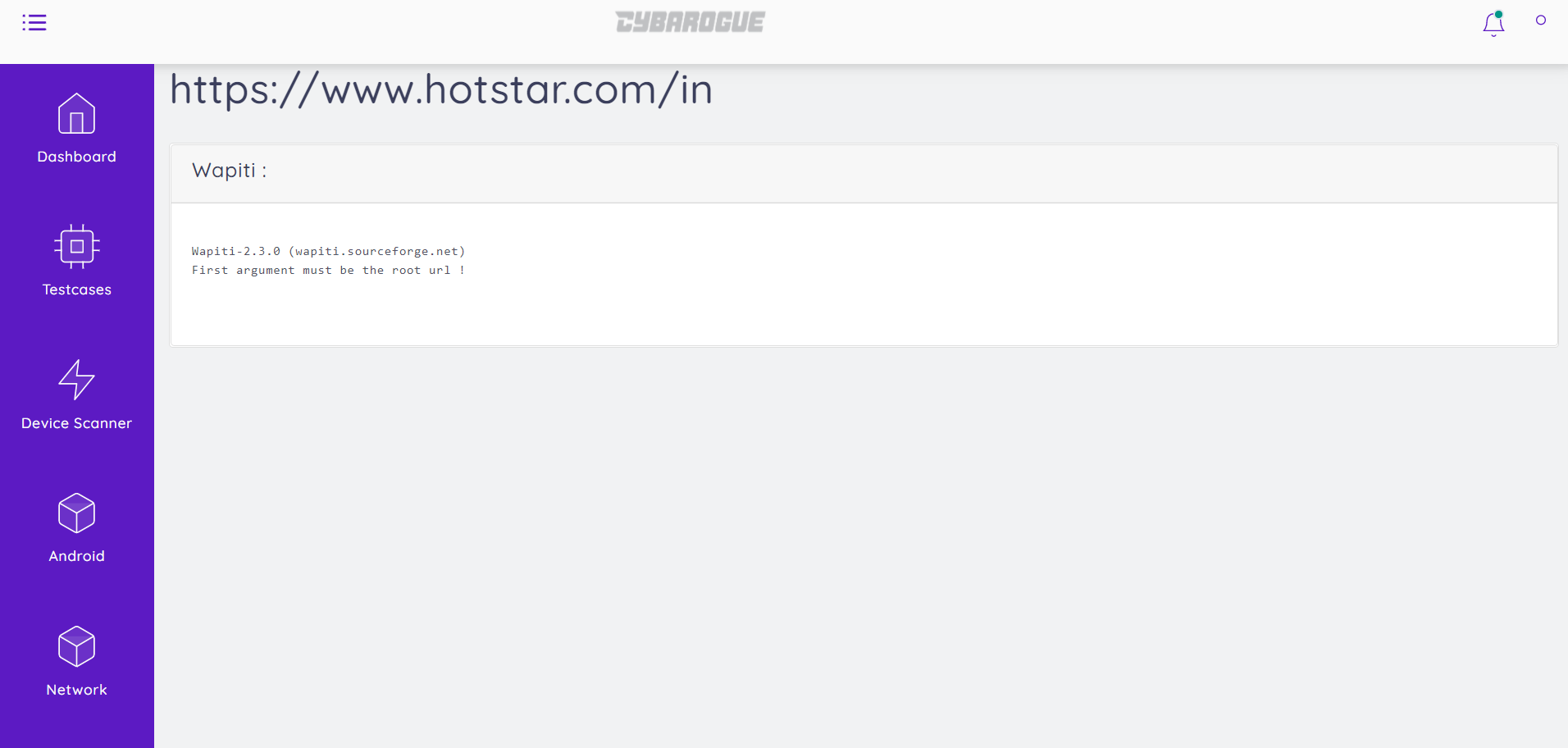
(d)Reports:

Wapiti will generate a report at the end of the attack process. Several formats of reports are available.

Go to Web portal🡪 results🡪Wapiti



Click on view and then select add to report and then select generate report then it automatically downloads report as document format

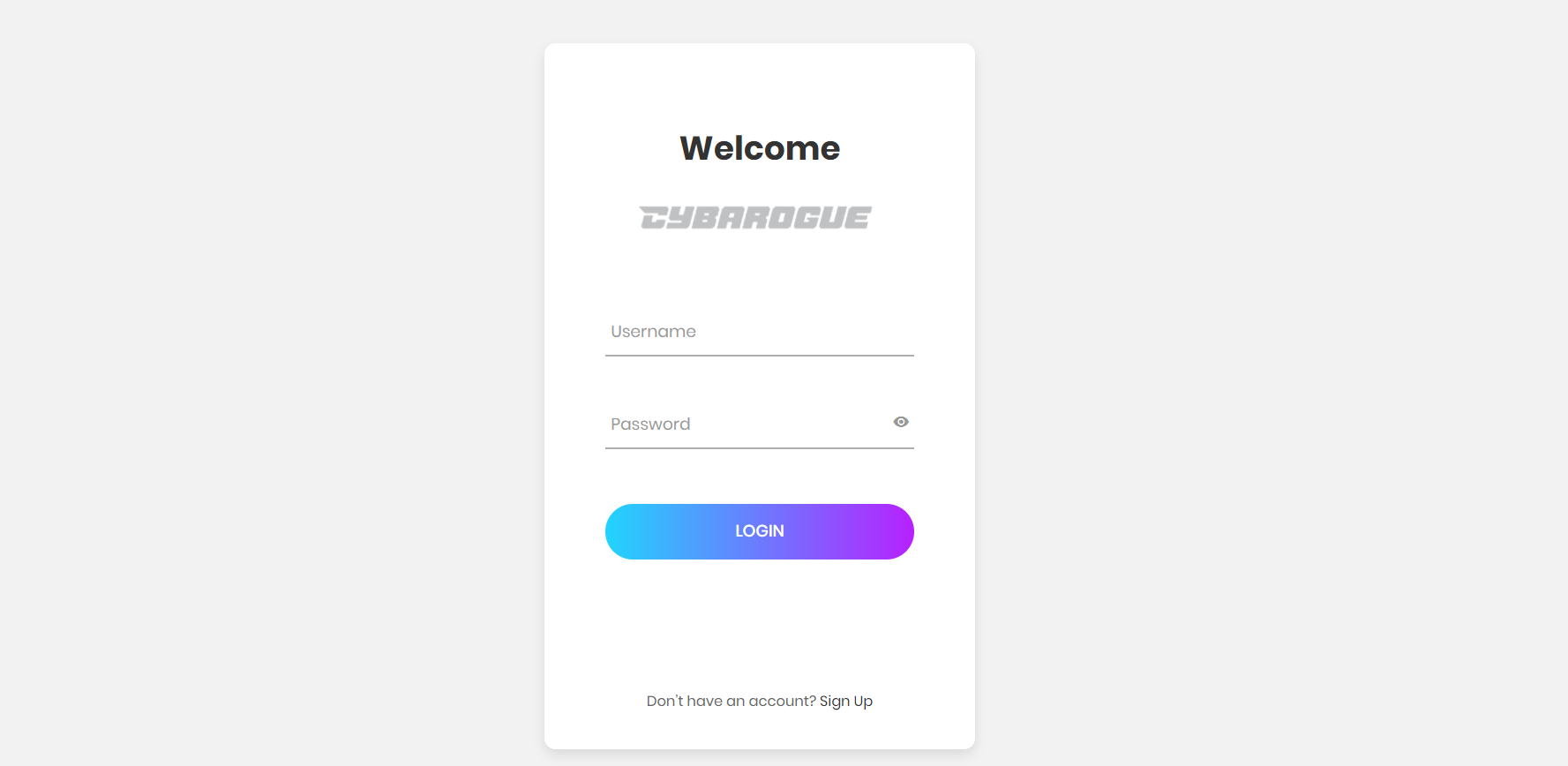


8.3. Whatweb User Manual:

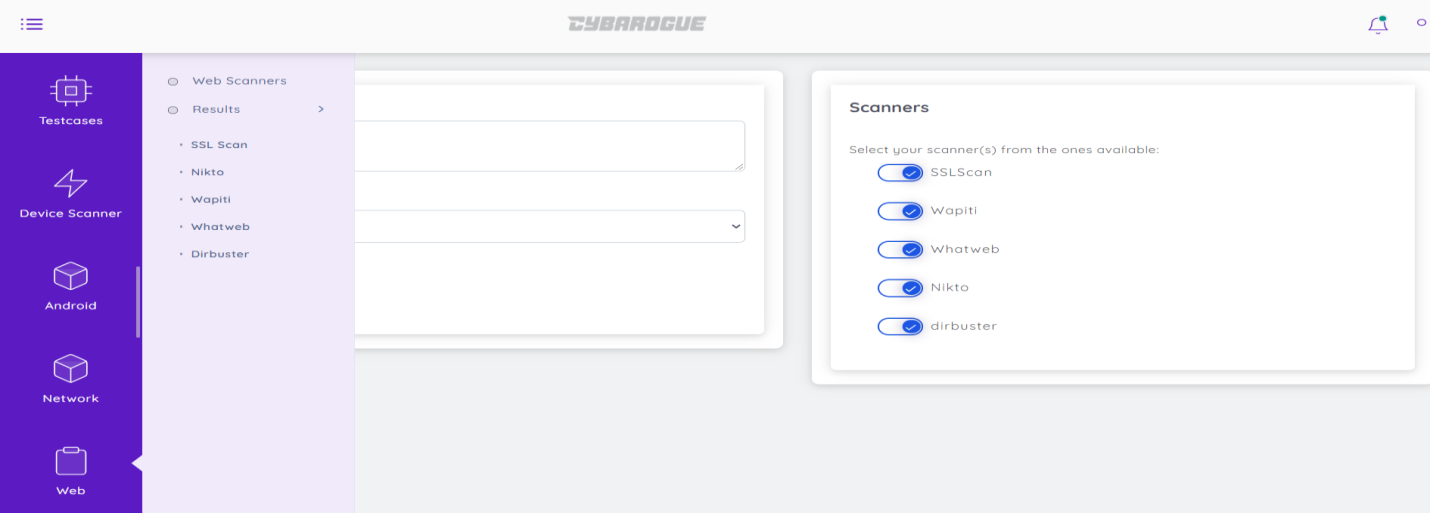
Remember whatweb can scan for ranges outside the LAN, on the WAN also. Find out google’s IP address, and  perform a scan on it’s range.

(a) User Activities:

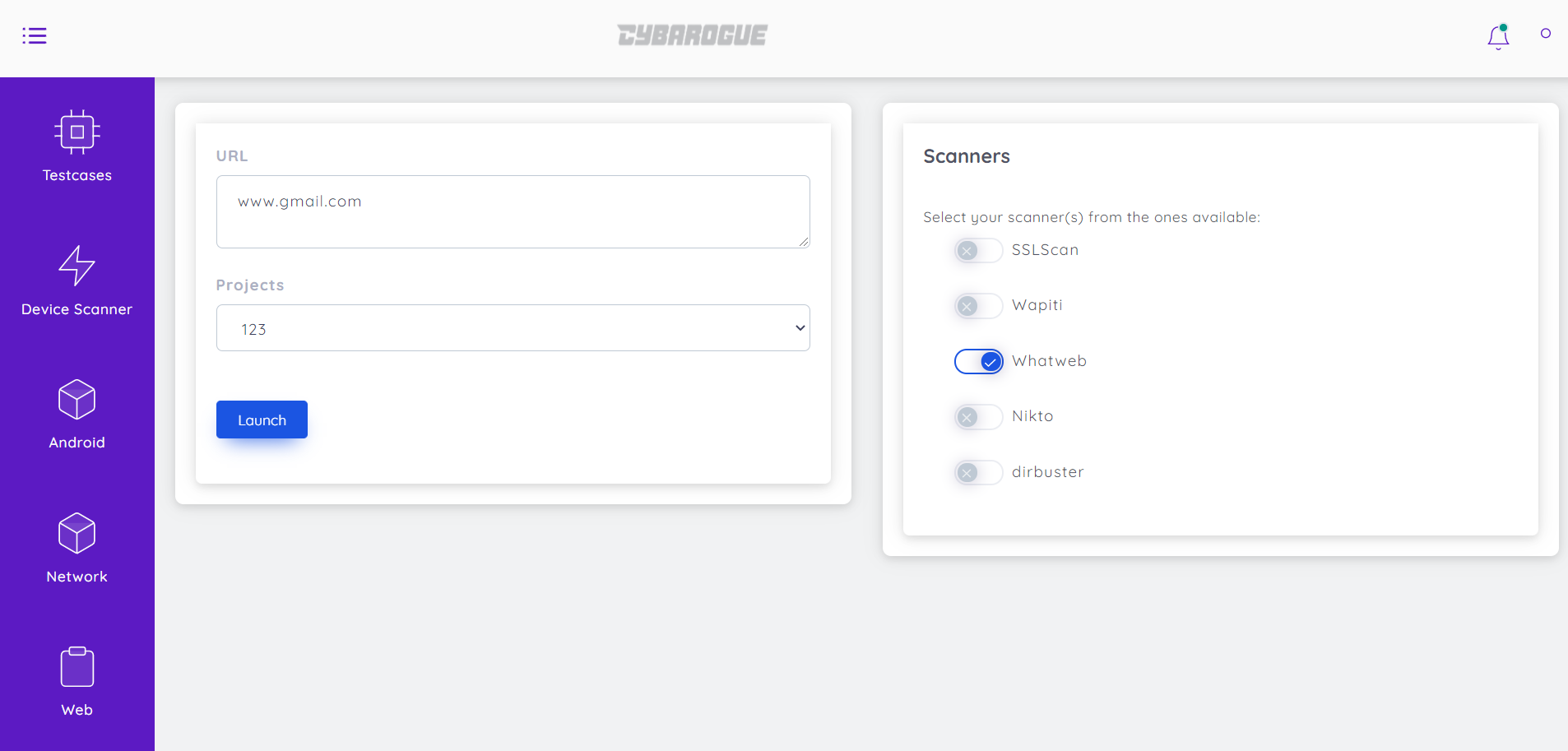
Step 1. User first make login with their respective credentials.



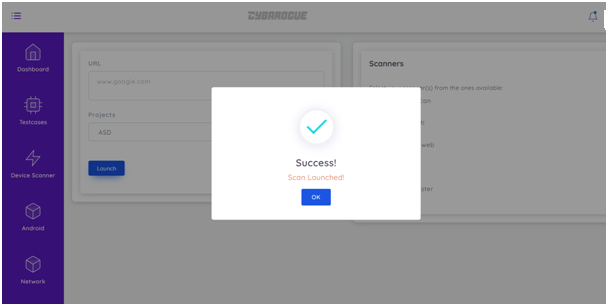
Step 2. Select Web portal which is at left side of the window it shows webscanners



Step 3. In Webscanners select Whatweb and give url to scan and select project, finally click launch

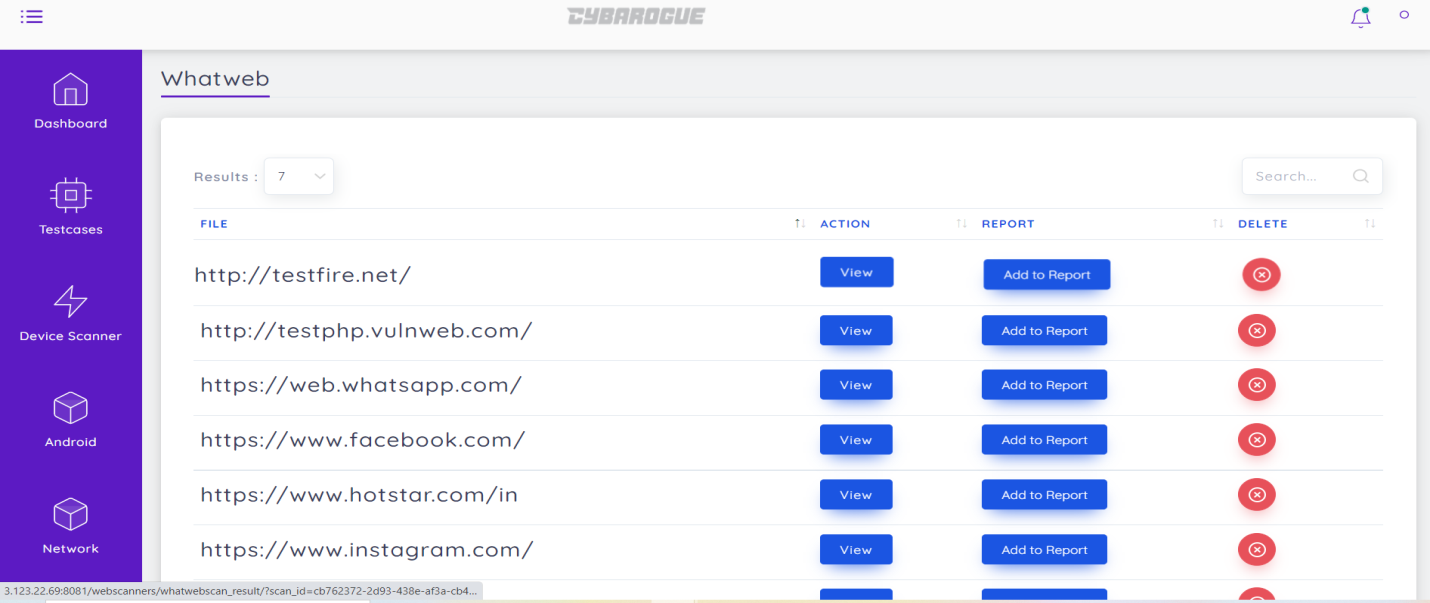


Step 4. Then it displays that launch success then click ok.

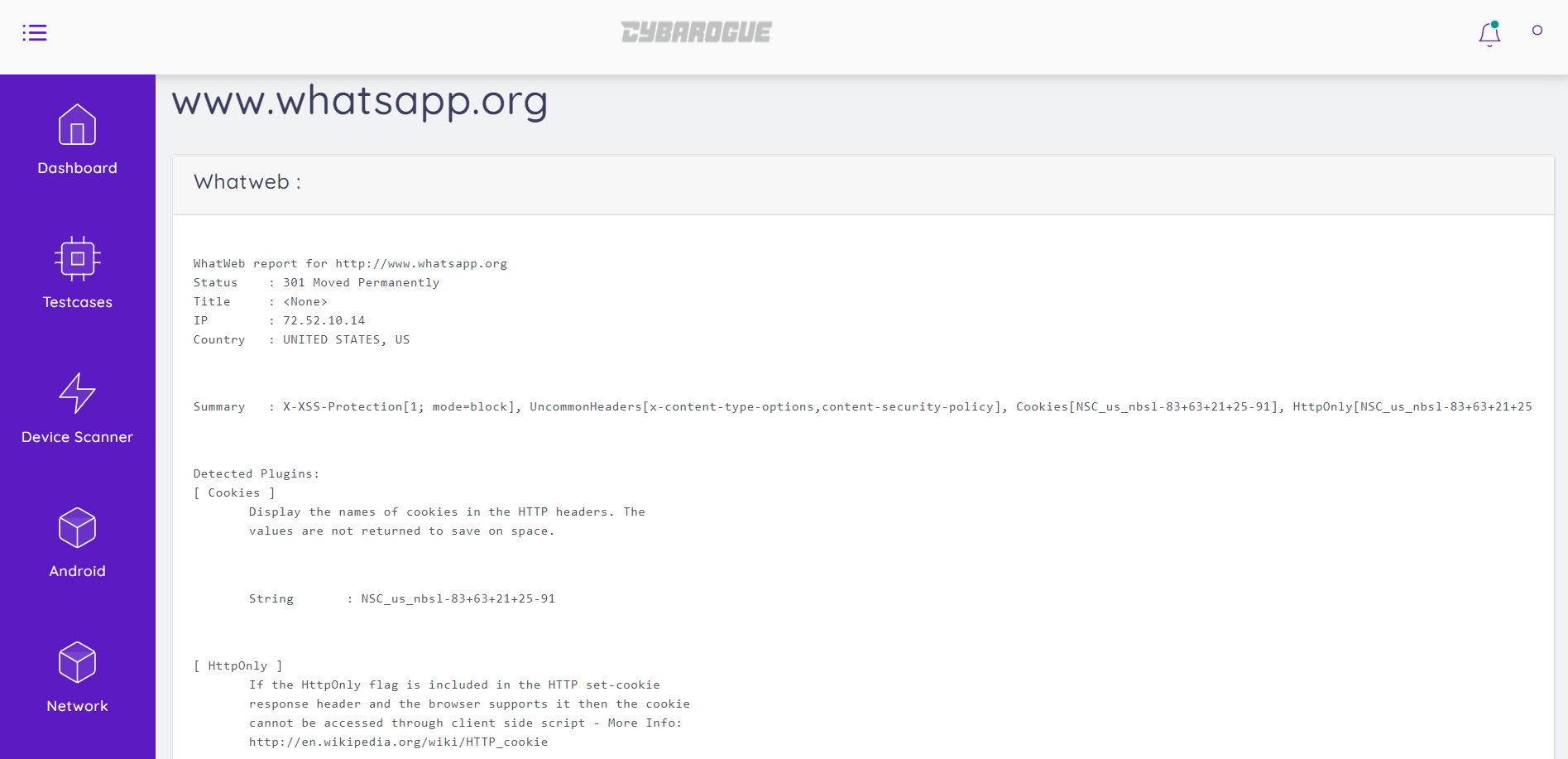


(b) Reports:

Go to Web portal🡪Results🡪 Whatweb



Click on view and select add to report and then select generate report then it automatically downloads report as document format



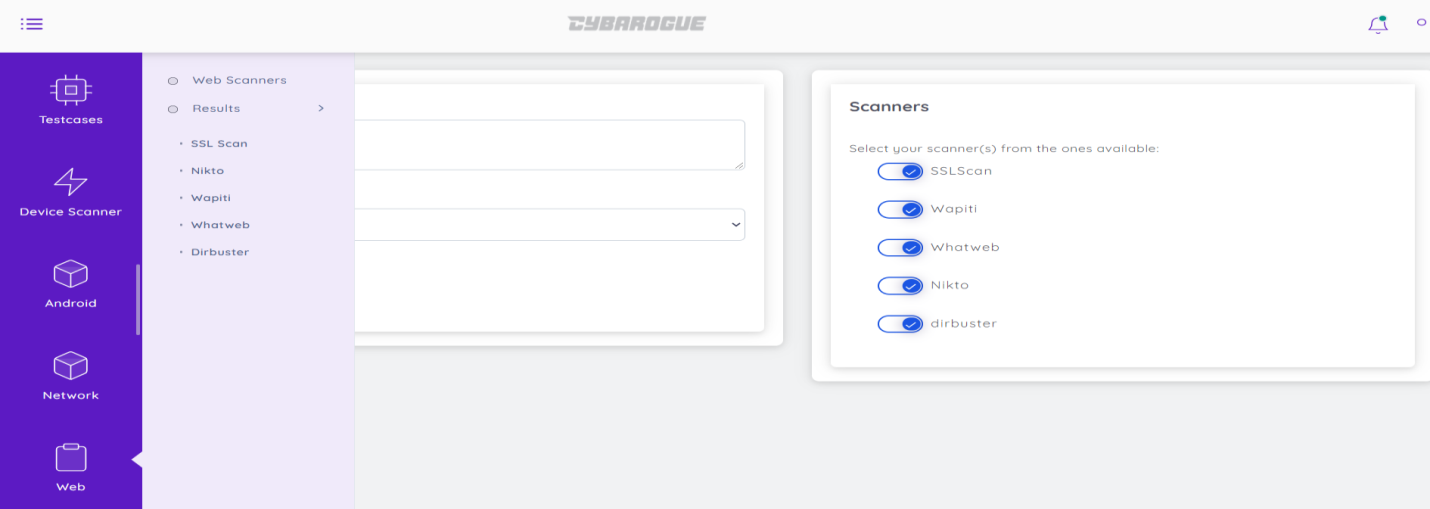
8.4. Nikto User Manual:

(a) User Activities:

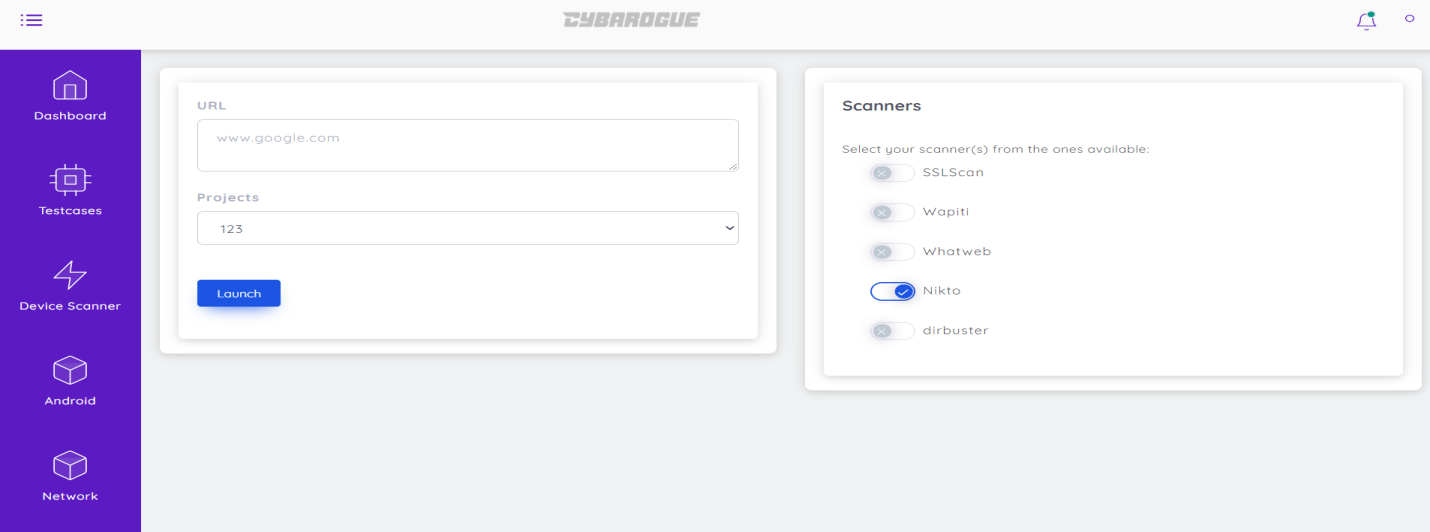
Step 1. User first make login with their respective credentials.



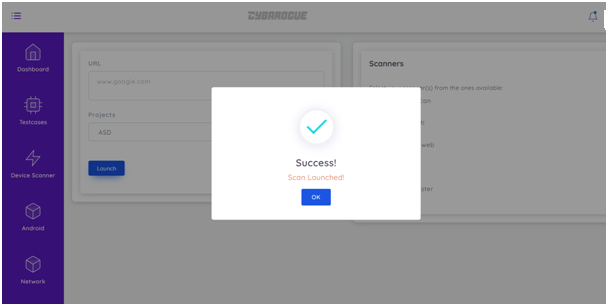
Step 2. Select Web portal which is at left side of the window it shows webscanners



Step 3. In Webscanners select Nikto and give url to scan and select project, finally click launch



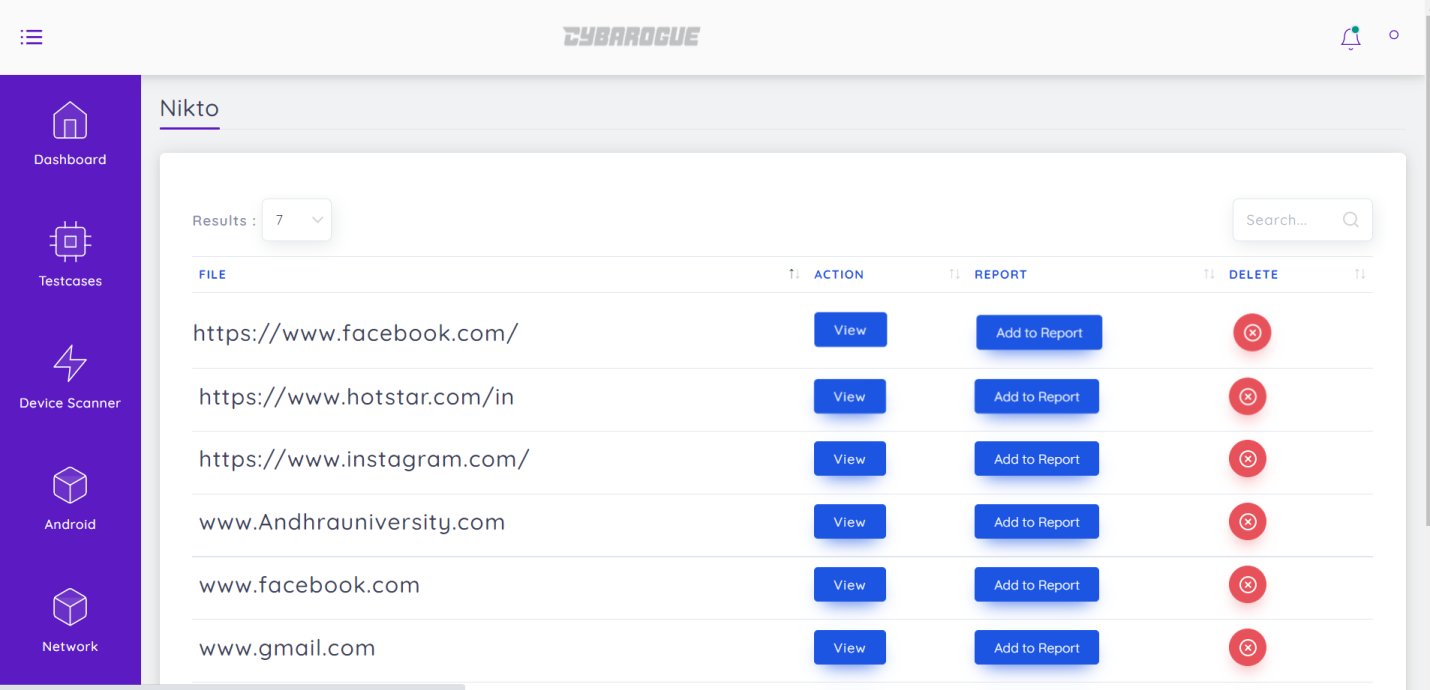
Step 4. Then it displays that launch success then click ok.



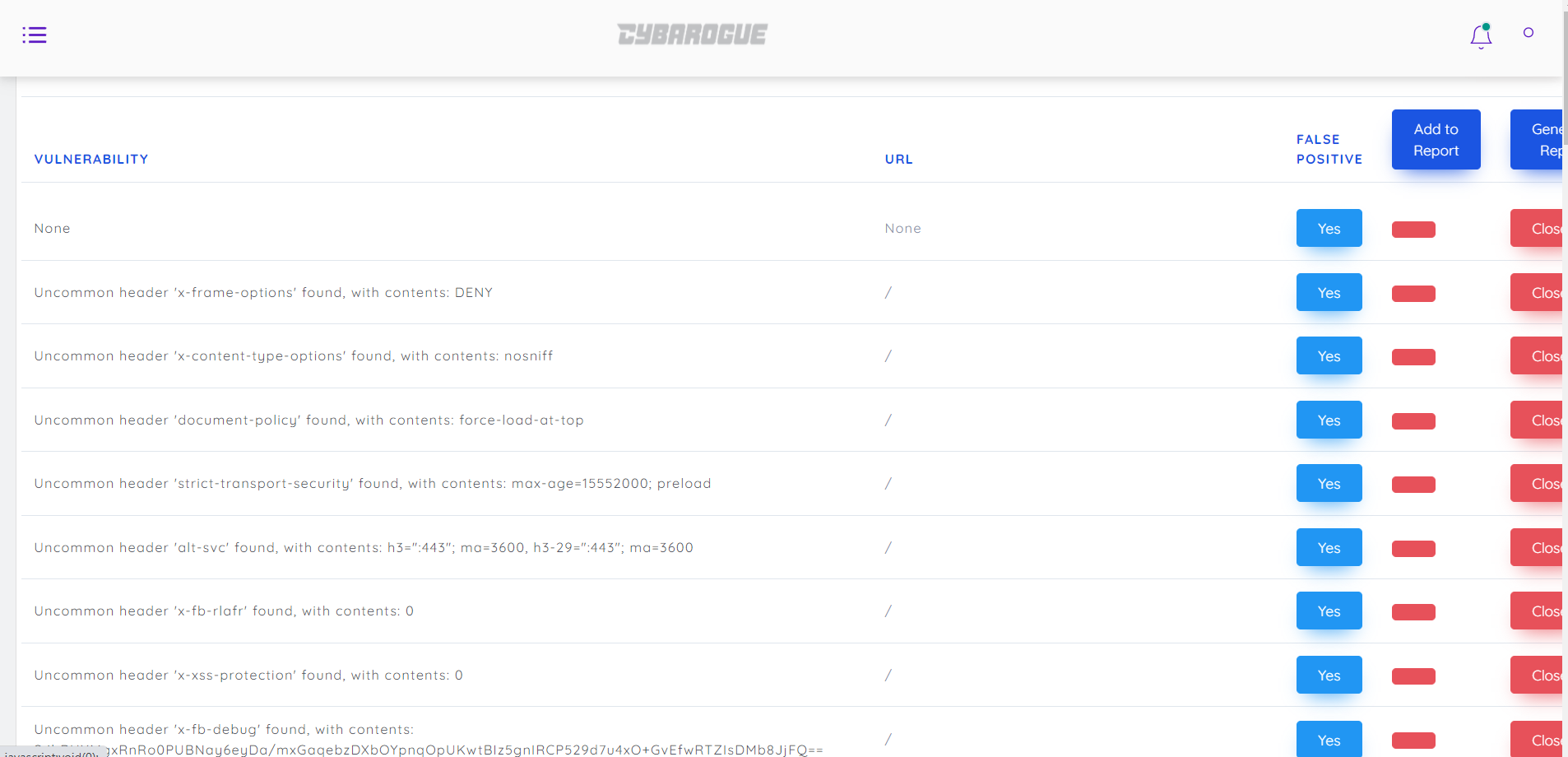
(b) Reports:

Go to Web portal🡪Results🡪 Nikto

Click on view and select add to report and then select generate report then it automatically downloads report as document format



Click on view then add to report



Then select generate report, it automatically downloads the report as below:



NIKTO SCAN:   
 Nikto is a web server assessment tool.  
 It is designed to find various default and insecure files, configurations and programs on any type of web server.  
 ***URL Scanned: www.google.com  
 Scan ID: d9c91848-ab7c-49a9-bd4b-a505b66f79c8  
 The following vulnerabilities are present:***Cookie NID created without the httponly flag  
 Uncommon header 'x-xss-protection' found, with contents: 0  
 Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN  
 Uncommon header 'referrer-policy' found, with contents: no-referrer  
 Uncommon header 'cross-origin-opener-policy-report-only' found, with contents: same-origin; report-to="static-on-bigtable"  
 Uncommon header 'x-content-type-options' found, with contents: nosniff  
 Uncommon header 'report-to' found, with contents: {"group":"static-on-bigtable","max\_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/static-on-bigtable"}]}  
 Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin  
 File/dir '/search/about/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/search/howsearchworks/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/groups/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/index.html?' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 Uncommon header 'link' found, with contents: </?hl=/>;rel="canonical"  
 File/dir '/?hl=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?hl=\*&/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?hl=\*&gws\_rd=ssl$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?hl=\*&\*&gws\_rd=ssl/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?gws\_rd=ssl$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/?pt1=true$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/m?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/wml?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/wml/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/xhtml?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/xhtml/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/imode?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/pda?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/pda/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin  
 Uncommon header 'content-security-policy' found, with contents: require-trusted-types-for 'script'

File/dir '/local?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/products?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/books/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/bkshp?\*q=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*q=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*output=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*pg=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*jtp=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*jscmd=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*buy=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*zoom=\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*q=related:\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*q=editions:\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*q=subject:\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books/about/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*zoom=1\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/books?\*zoom=5\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/ebooks/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/patents?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/patents/download/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/patents/pdf/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/patents/related/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/scholar/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 Uncommon header 'timing-allow-origin' found, with contents: https://www.google.com  
 File/dir '/maps?\*output=classic\*/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/maps?\*file=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/maps/d/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/maps?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/maphp?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 Uncommon header 'server-timing' found, with contents: gfet4t7; dur=7  
 Uncommon header 'content-security-policy-report-only' found, with contents: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile  
 Uncommon header 'service-worker-allowed' found, with contents: /maps  
 File/dir '/maps/\_/sw/manifest.json' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/maps/preview/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/maps/place/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/help/maps/streetview/partners/welcome/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/lochp?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/ie?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)

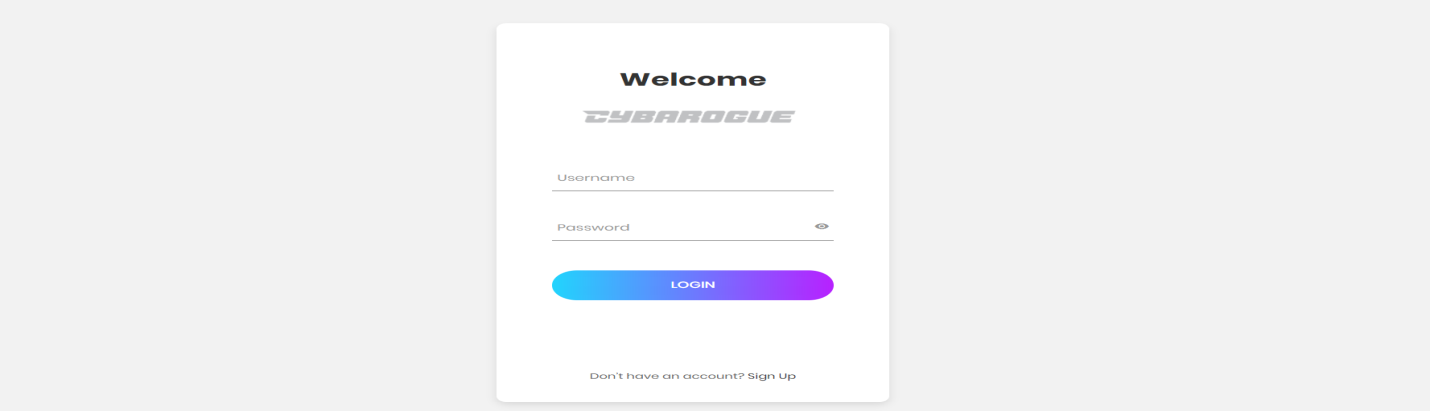
File/dir '/blogsearch/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/transit?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir ' /calendar/about/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/calendar/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/cl2/feeds/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/cl2/ical/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/coop/directory/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/coop/manage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/music?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/hottrends?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/viz?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/embed.js?' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/fetchComponent?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/beta/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/trends/topics/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/musicsearch/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/movies?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/safebrowsing/report\_badware/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/safebrowsing/report\_error/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/safebrowsing/report\_phish/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/reviews/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/profiles/me/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/cse?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/cse/home/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/cse/panel/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/cse/manage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/accounts/ClientLogin/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/accounts/ClientAuth/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/accounts/o8/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/accounts/o8/id/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/compressiontest/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/analytics/feeds/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/analytics/partners/comments/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/analytics/portal/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 Uncommon header 'x-guploader-uploadid' found, with contents: ADPycduwMY7anuwW7xWuUI3z54LstqwdcNRnfQKTA60X9X2FiAJAWXOM9EJVEvGsDXqUd9K2psPv4ebr\_TP7xYhYSqplaVXfKw  
 File/dir '/alerts/' in robots.txt returned a non-forbidden or redirect HTTP code (301)

File/dir '/ads/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/ads/plan/action\_plan?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/ads/plan/api/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/ads/hotels/partners/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/phone/compare/?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/hotelfinder/rpc/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/hotels/rpc/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/compare/\*/apply\*/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/edu/cs4hs/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/trustedstores/s/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/trustedstores/tm2/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/trustedstores/verify/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/adwords/proposal/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/shopping?\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/shopping/product/' in robots.txt returned a non-forbidden or redirect HTTP code (302)  
 File/dir '/about/careers/applications/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/landing/signout.html' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
 File/dir '/landing/now/ontap/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/searchhistory/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/maps/reserve/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/about/views/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/localservices/\*/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/finance/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 File/dir '/nonprofits/account/' in robots.txt returned a non-forbidden or redirect HTTP code (301)  
 "robots.txt" contains 281 entries which should be manually viewed.  
 /crossdomain.xml contains 0 line which should be manually viewed for improper domains or wildcards.  
 Allowed HTTP Methods: GET, HEAD   
  
 ***Generated By: rs***

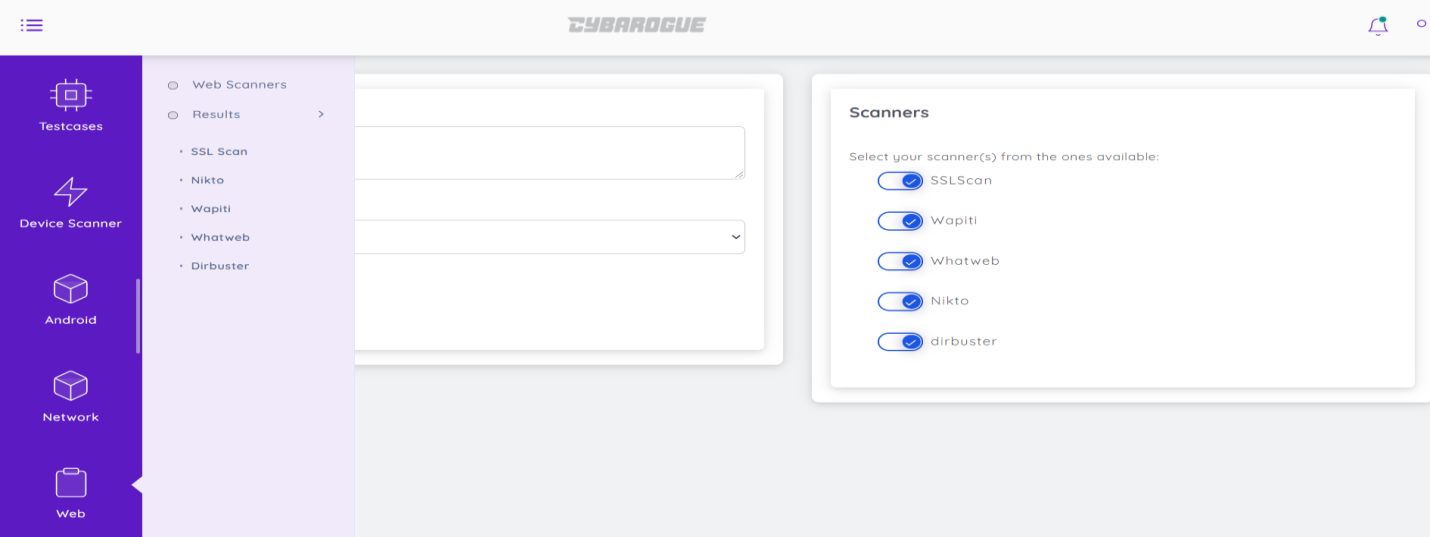
8.5. Dirbuster:

(a)User Activities

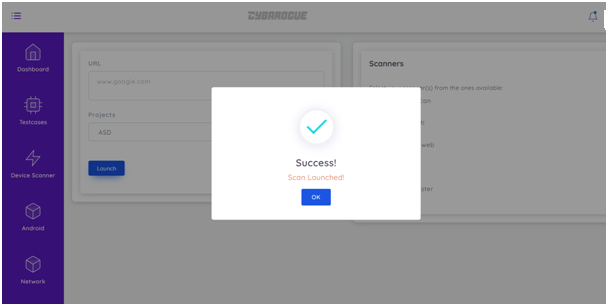
Step 1. User first make login with their respective credentials



Step 2. Select Web portal which is at left side of the window it shows webscanners.



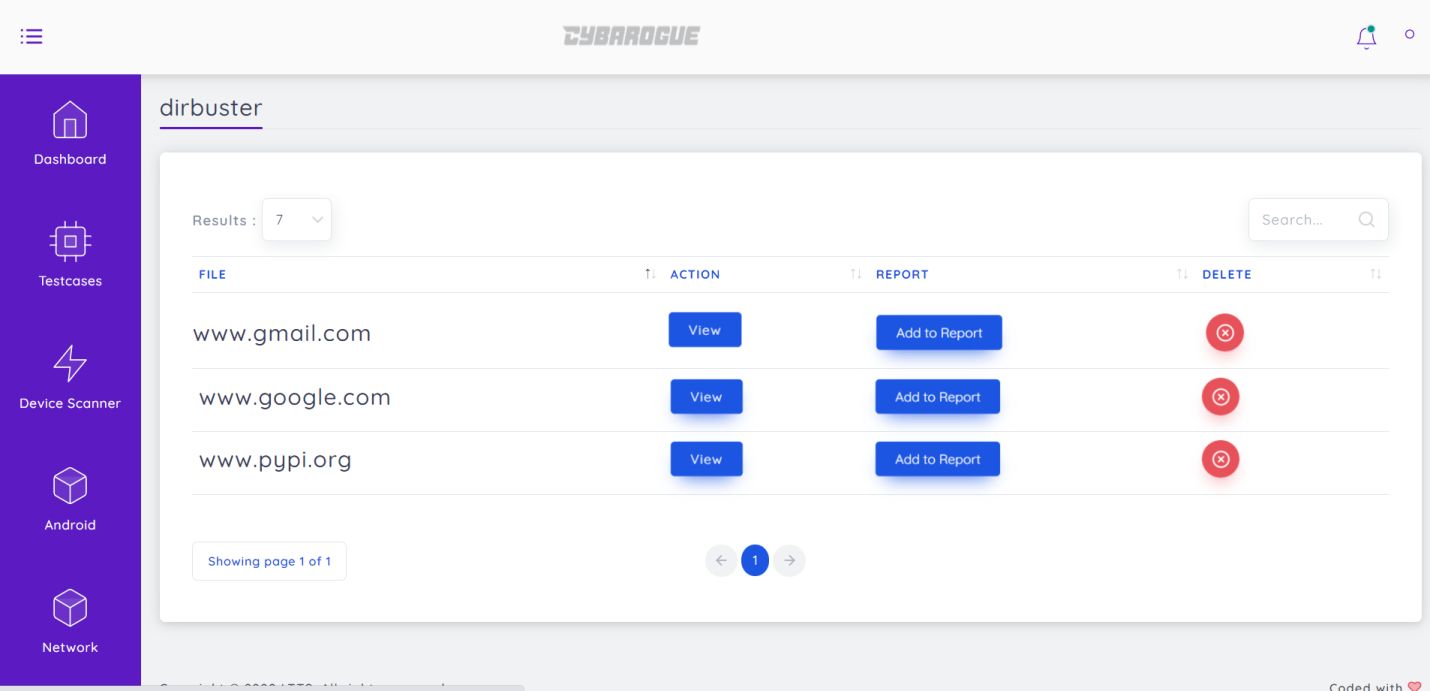
Step 3. In Webscanners select Dirbuster and give url to scan and select project, finally click launch then it displays that launch success then click ok.



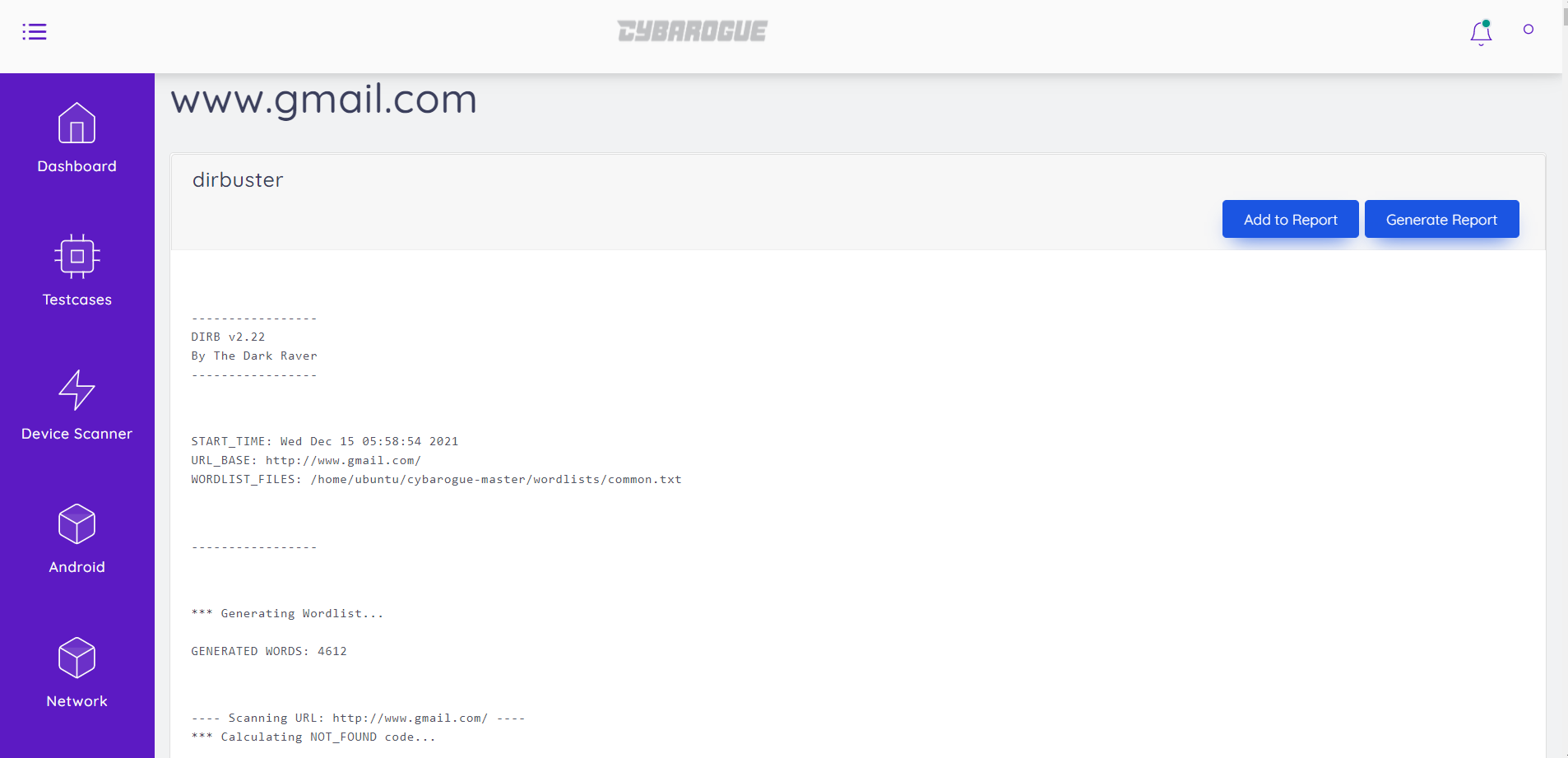
(b)Reports

Go to Web portal🡪Results🡪 Dirbuster

Click on view and select add to report and then select generate report then it automatically downloads report as document format.



By clicking view we can see as follows

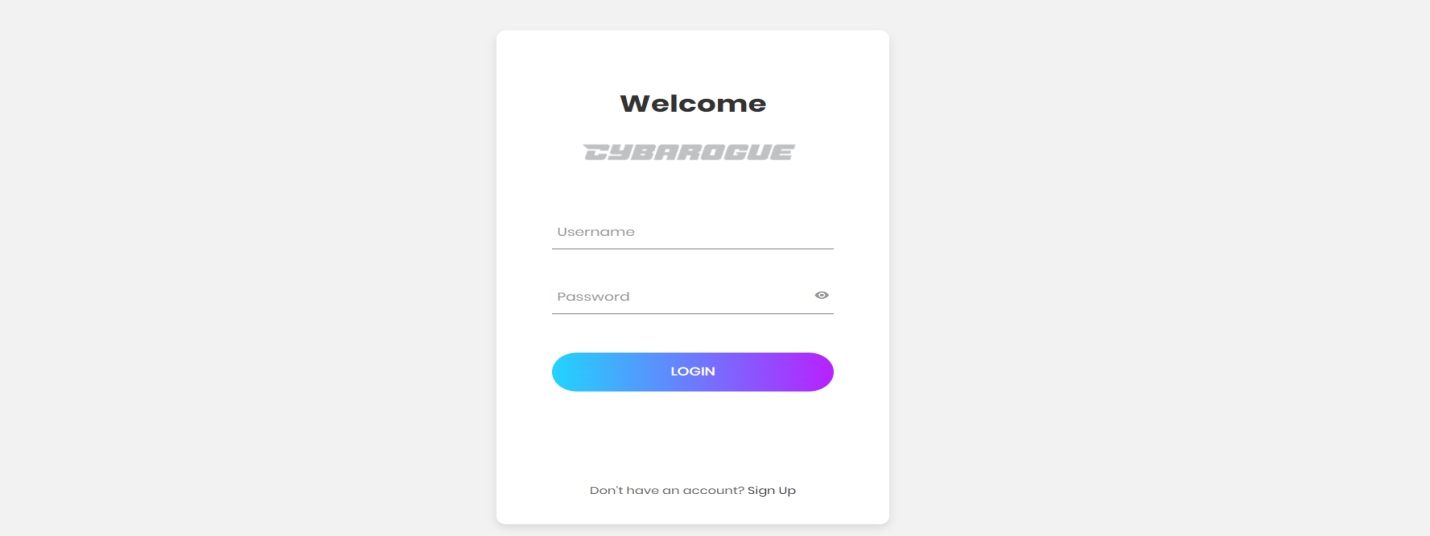


**9. Thick client User Manual:**

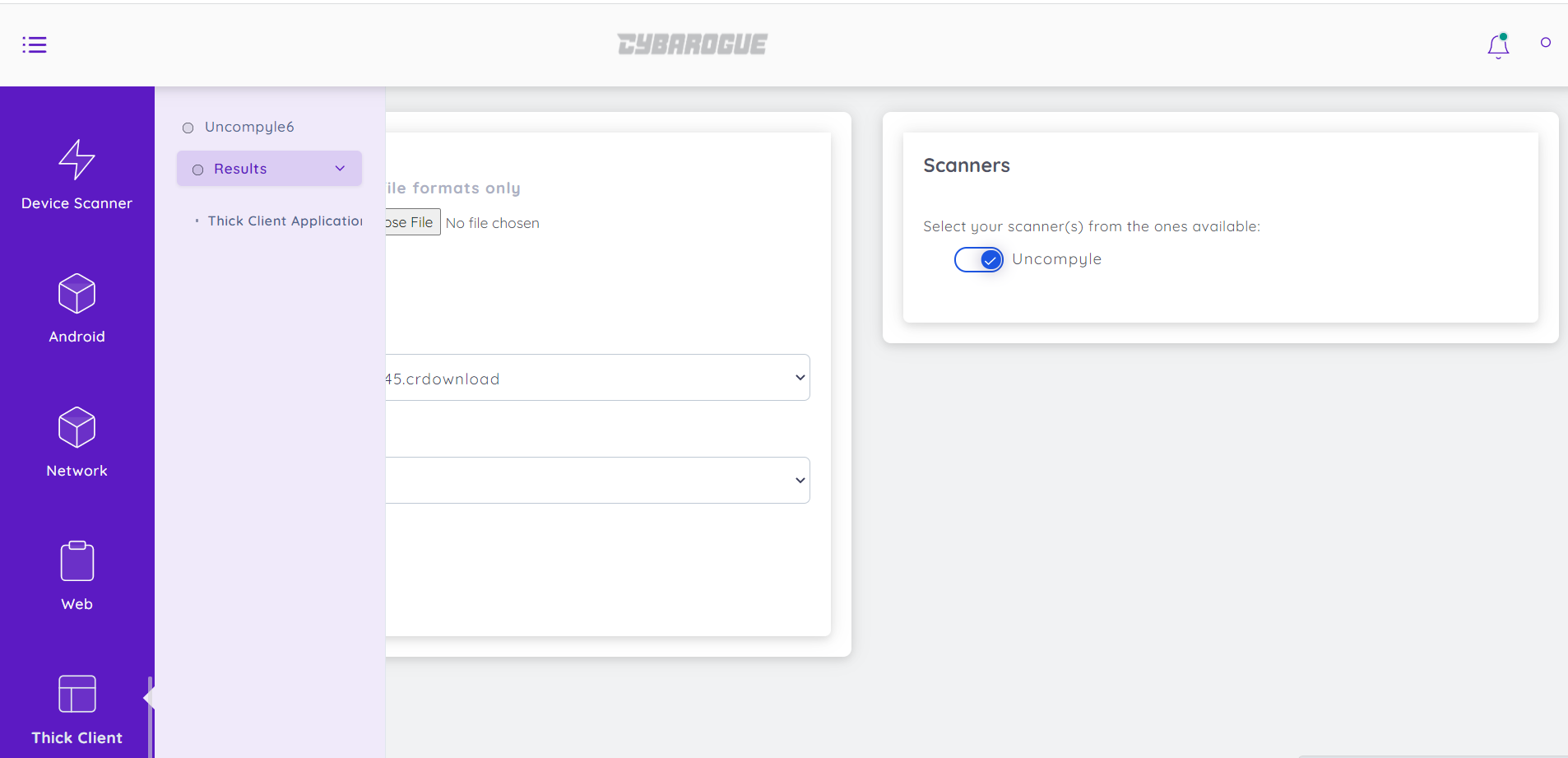
9.1. Uncompyle6 Tool User Manual:

(a) User Activities:

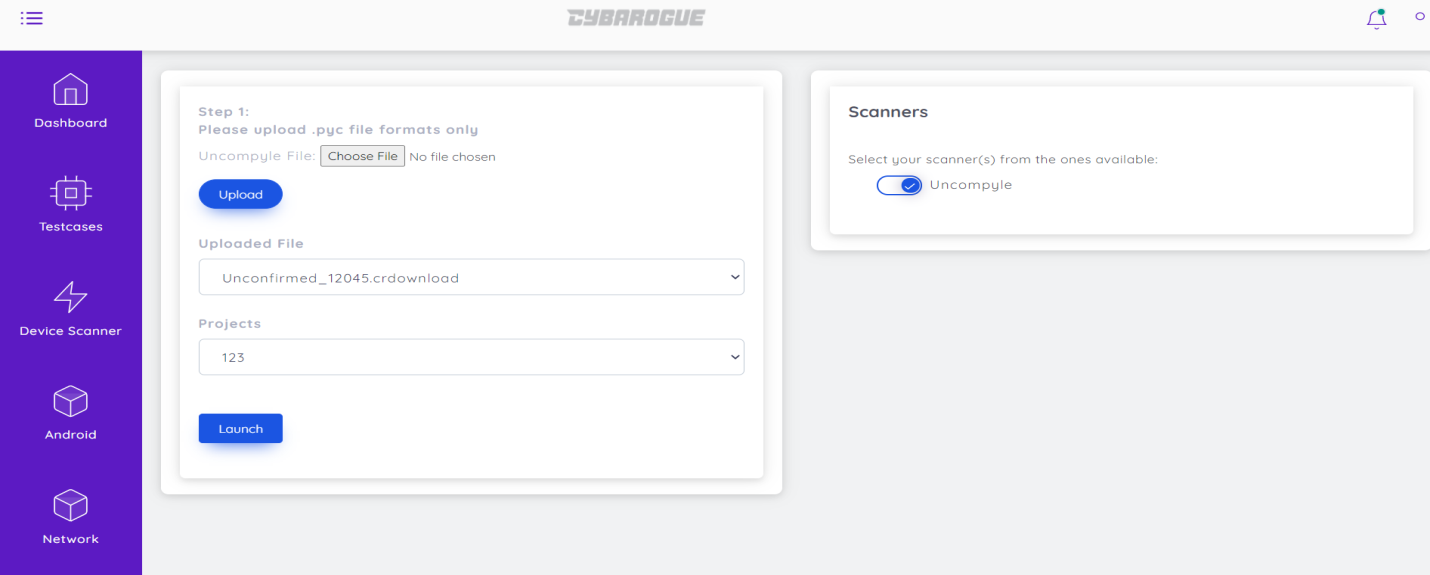
Step 1. User first make login with their respective credentials



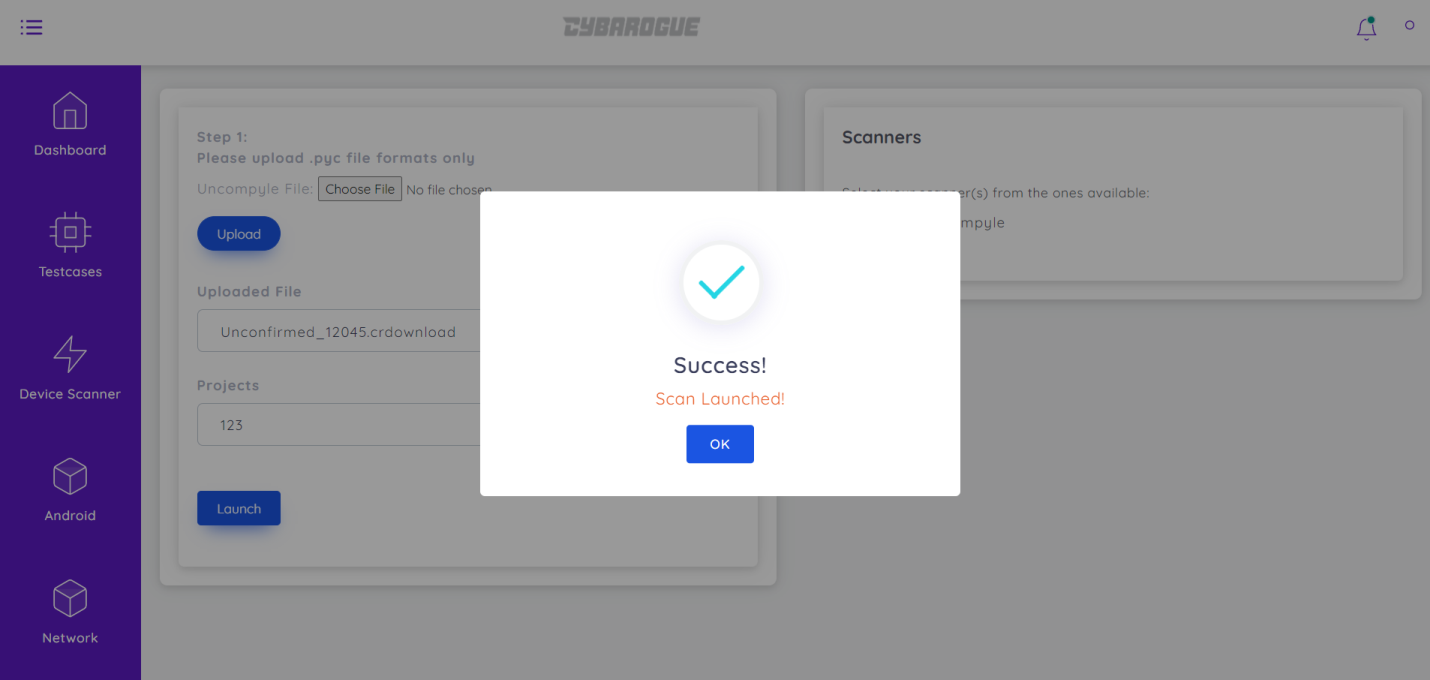
Step 2. Select ThickClient which is at left side of the window it shows as follows



Step 3. Click on Thickclient in that enable Uncompyle6 choose pyc file and projects then click upload finally click launch.



Step 4.After Clicking launch it gets scan launch success click ok



(b) Reports:

Go to Thickclient portal🡪 Results🡪Thickclient Applications

Click on view and add to report and then select generate report then it downloads report as document format.

