RAPID7

By

N Nithish

RAPID7

Introduction:

Rapid7 is a web-based application tool used to find vulnerabilities in a website coding part and monitor the devices by implanting insight IDR which can perform SEIM and XDR(Extended Detection and Response) but for XDR the end device needs to allow access to that feature. But when compared to EDR (End-point-Detection and Response) for login security we will use insights Ops and vulnerabilities management can be done by insight Vm for Security detection and Automation can be done by insight Connect
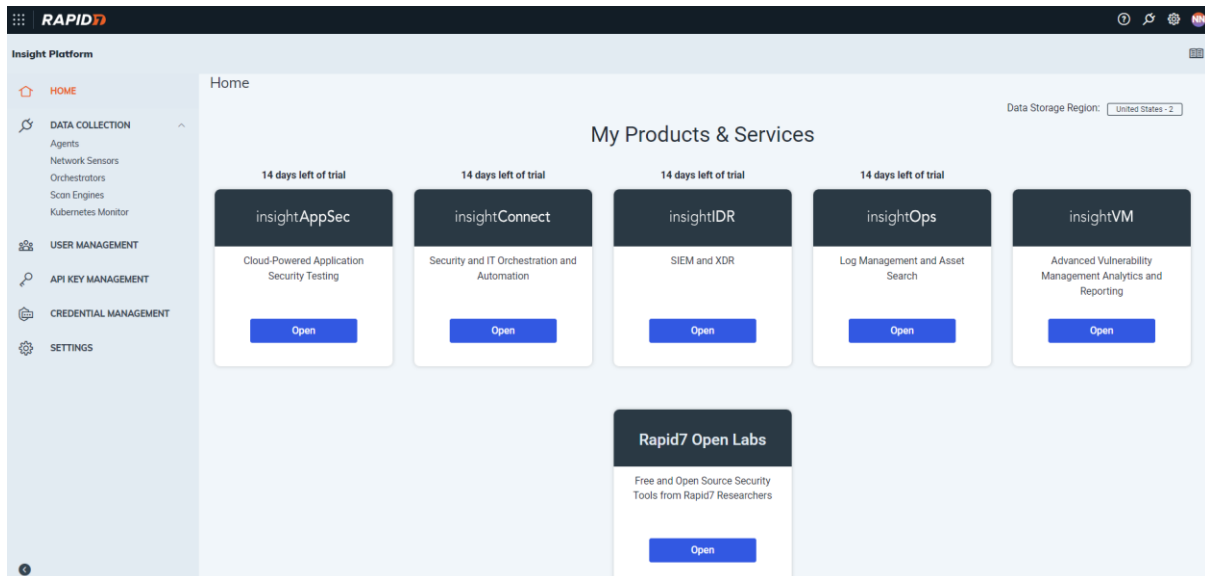

Figure 1 Home Page of Rapid7

As we can see the interface of Rapid7 Home where we will see services provided by Raipd7 On the left, we can see the option for Data collection with Agents, Network Sensors, orchestrators, Scan Engines, and Kubernetes Monitor. User Management, API (Application Interface) Management, Credential Management, and Settings.

In the AppSec we are going to perform the website security by finding out the vulnerabilities of that particular website so that we can figure out where the website is lacking security so that the developers of the organization will have a clear picture to patch the website in a secure way to use the website for their clients and consumers.

Remember the AppSec is meant to ensure the security of websites by providing the vulnerabilities to ensure the best security to that particular website It's not meant to perform illegal attacks on that particular organization.

It's a friendly beginner tool where they can generate reports on a demo website so that everyone will know how the tools. As we see below I will explain how the demo website and Domain-based website with clear and proper instructions.
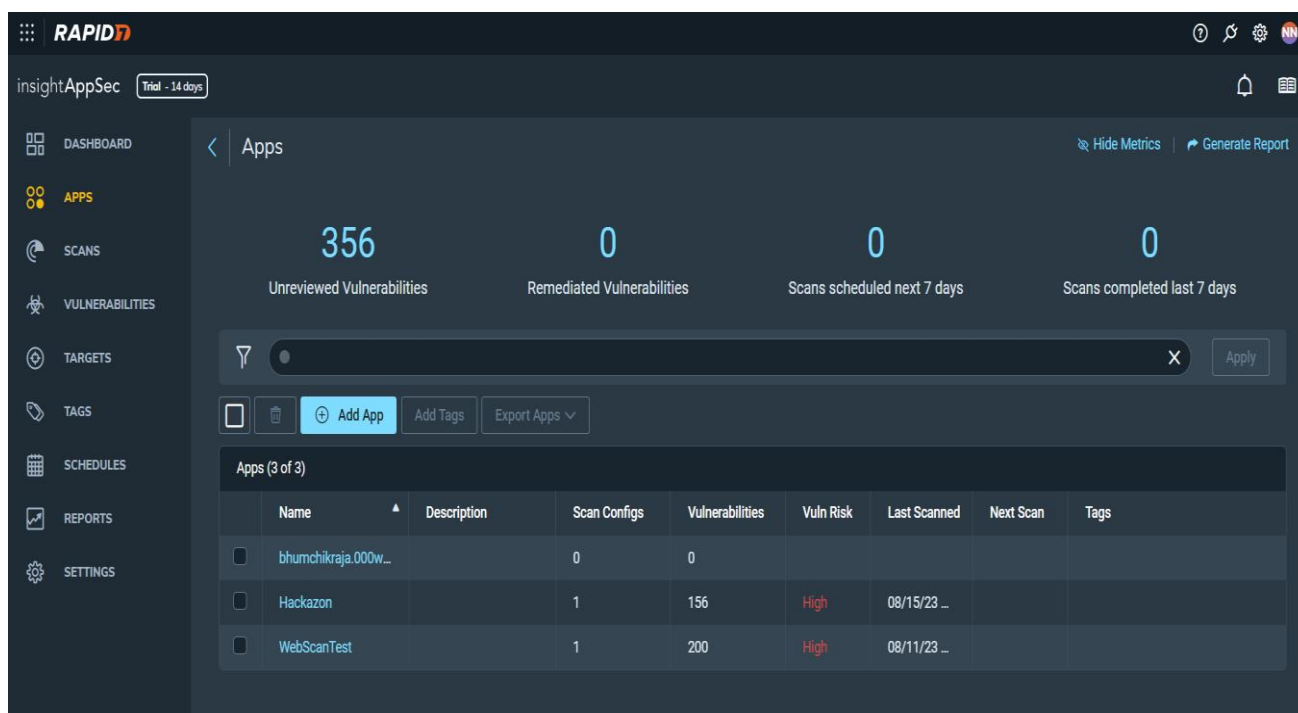
Insight AppSec

Figure 2 AppSec Home Page

As we can see on the home page of the app sec we have an option to Add App. If we click that particular option we will get an option as shown in Figure 3 where we can add our website URL or we can make a demo scan so that we can see how the scan works.

If we go with the option of scanning my Domain we can see a little bit of description of how that works but for that, we need a verified domain to perform the scan so that will be more authentic. If we select that option in Figure 4 we can see three steps to initiate the scan of the website of its domain For that we need to give the URL of the website and the second step is most importantly adding a meta tag to that source code of the website at the front end of HTML code in the pace of head tag so that Rapid7 has Access to make scan on that website and final step is to verify the website whether the meta tag is attached perfectly or not. If it's attached it will start the scan as shown in Figure 6.

If we select Demo scan As we can see from Figure 5 it will give two options basic scan and advanced scan In the basic scan we will have general vulnerabilities of the website which can be found within 10 minutes or more It generally consists of common vulnerabilities of post and get method vulnerability with basic login security so that it will be vulnerable to brute force attack and in the advanced scan we will see crucial vulnerabilities of a website like MFA will be present but the problem it can be bypassed by Cross X Scripting Attacks and Removing SSL certificates by using SSL Striping used in the burp Suit. It will take a long time of 20 minutes but it can be broken by a predefined attack generated by the Rapid7.
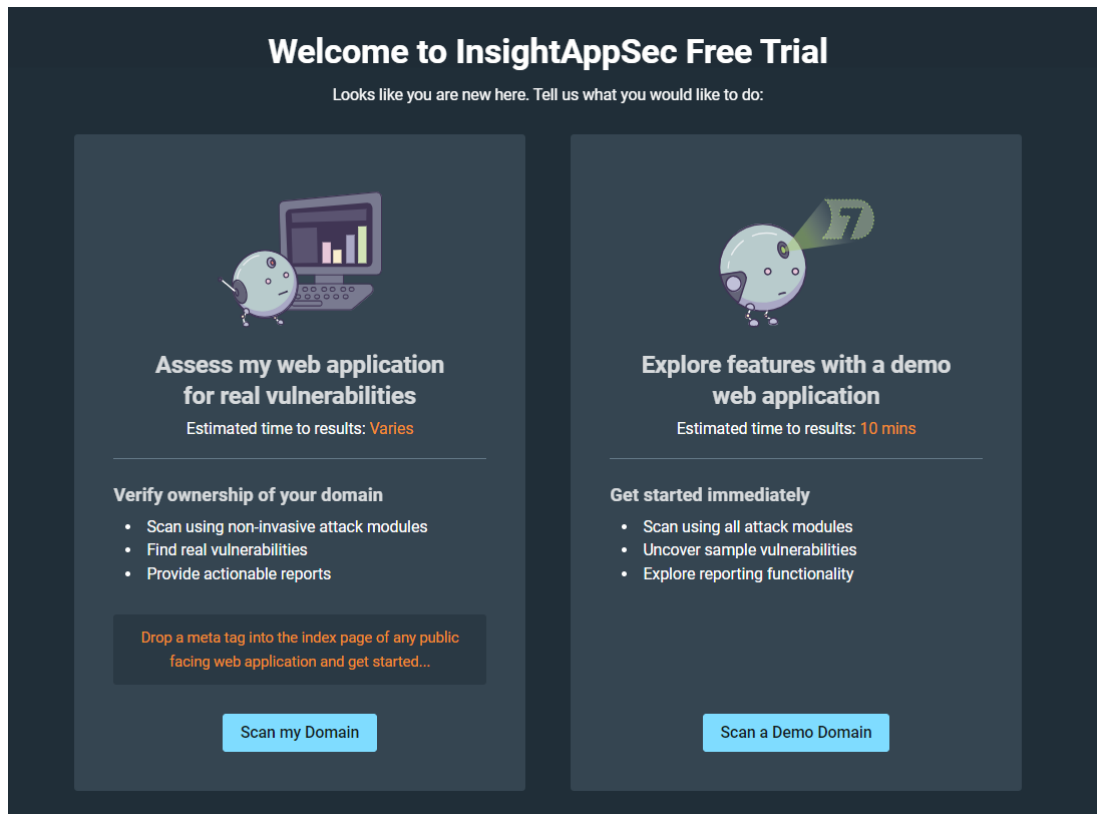
Figure 3 Add App Options

Choose the option to perform the scan for the website but be careful while attaching the meta tag to the code If we add it to other websites apart from the organization it may lead to a cyber-attack on that organization
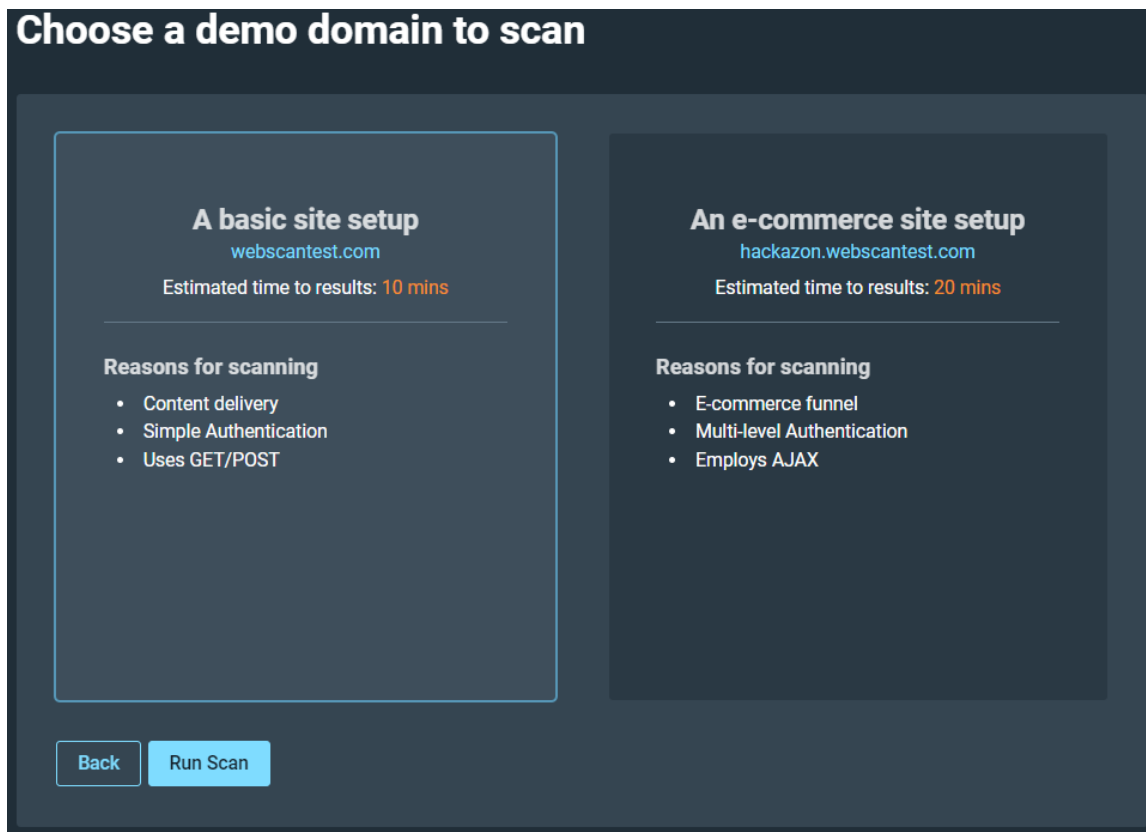

Figure 4 Scan My Domain Options

Figure 5 Performing Demo Scan Options

We need to choose an option to perform this scan of the website but a demo scan will give the exact vulnerabilities and risk mitigation of those vulnerabilities and a beginner will have a great experience of how this tool works on the AppSec.
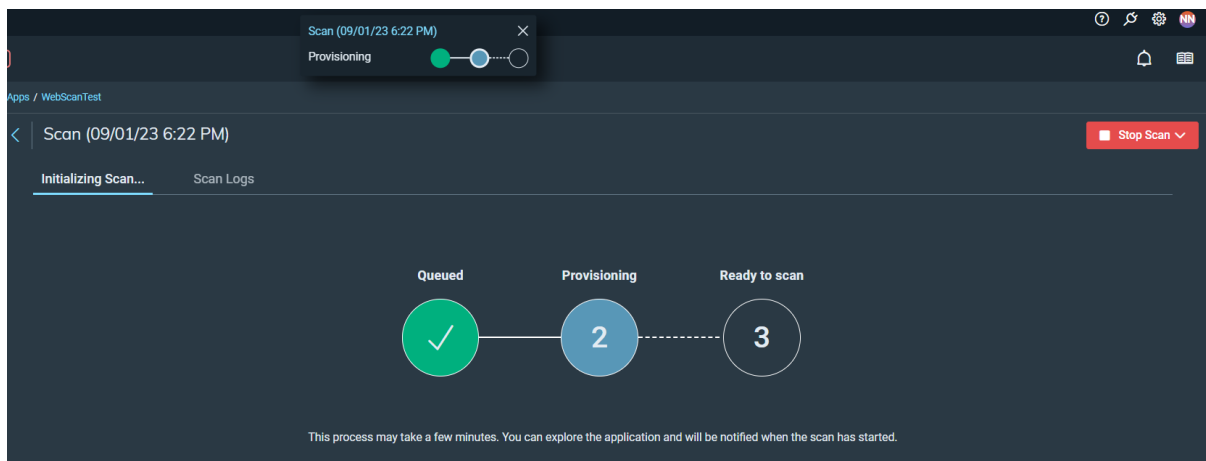
Figure 6 Initiate the Scan of the website

After selecting Demo Scan or Domain Scan in the AppSec we can see this tab where it needs three steps to start the process

Step 1: Everything related to the website will be queued

Step 2: Provisioning of the scan will take place

Step 3: It will be ready to scan the website
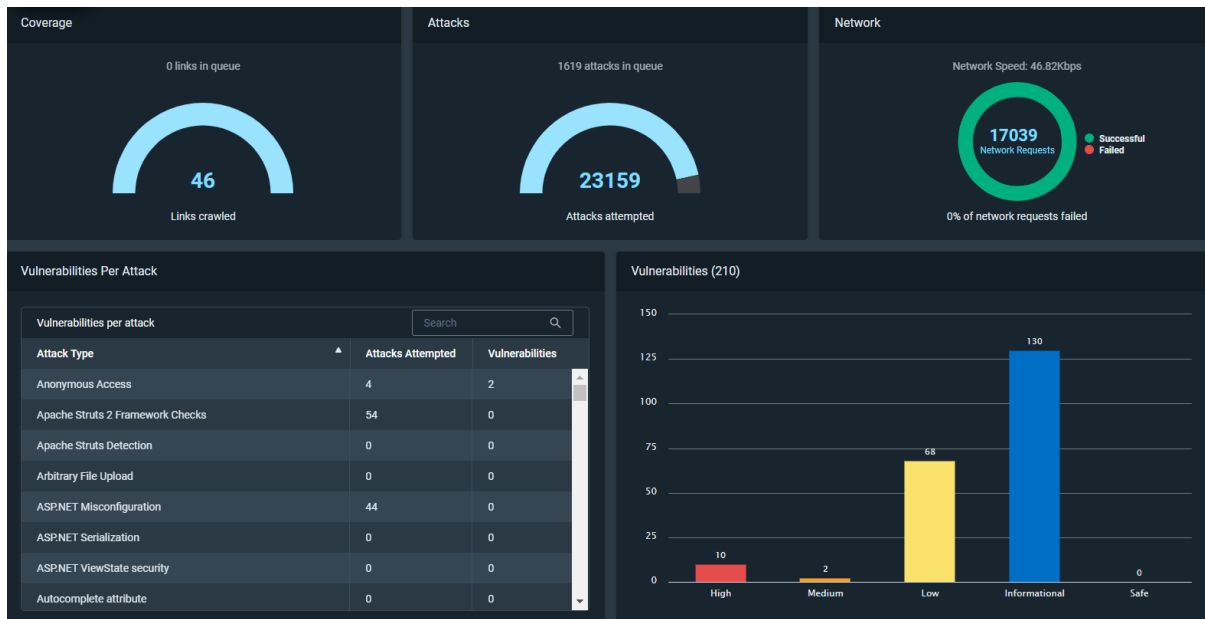
Figure 7 Scan Results of the website

As we can see the scan result of the website, we can see how many links have been crawled and the attacks performed by Rapid7 is 23159 The networking case is safe but if we start to see Vulnerabilities per attack we can see a lot of vulnerabilities with the main headings of attack and we can see how many possible way it can be attacked by Rapid7. The vulnerabilities graph says that there are 210 vulnerabilities in that website with levels of vulnerabilities This is the content of the overview now we will see vulnerabilities in detail of code.

Figure 8 shows a detailed explanation of the vulnerabilities

According to levels of vulnerability, it will start the showcase the list If we click each vulnerability, it will tell us the exact part of the code that is the reason for this vulnerability.

Figure 9 After clicking the first option in the Vulnerability list

As we can see that is exactly clear that it is JSON injection which means we will be injecting malicious code on the server side so it's also called a server-side injection attack. We can also see the status where we can keep it as a false positive which is also called a fake alarm alert but if we neglect that risk it will lead to the biggest vulnerability in the code of the website to mitigate that risk we need to modify the code at the point of as shown in figure 12.

Request and Response have happened between client and server through the Application interface where the response side will give details to hackers and the request side where the malware will be injected to force full execution of malware. In the Root cause as we can see the code is written using the post method so in the URL if we see it shows the server file named **search_by_name.php** As we know if we use PHP it has a lot of vulnerabilities and CVSS (Common Vulnerability Scoring System) score is very high that means we need to consider it as the high level of vulnerability.

For Replay Attack we will get the Chrome plugin which is an extension in the browser that will show the flow of requests and responses of the website.

Figure 10 shows the original traffic and attack traffic from 1st Attack.

Figure 11 Response from Original traffic-1

Figure 12 Attack traffic-1 response

As the above image tells us it gives details of the admin on the response side so the hacker will know the details after that particular attack and here is the place where the modification needs to be done as soon as possible to stop this attack.

Figure 13

As we can see above Figure 13 shows that any updates are done regarding the coding part to make sure it mitigates the vulnerability and comments on the code so that the developer or security experts will understand the flaw of the code through the conservation.
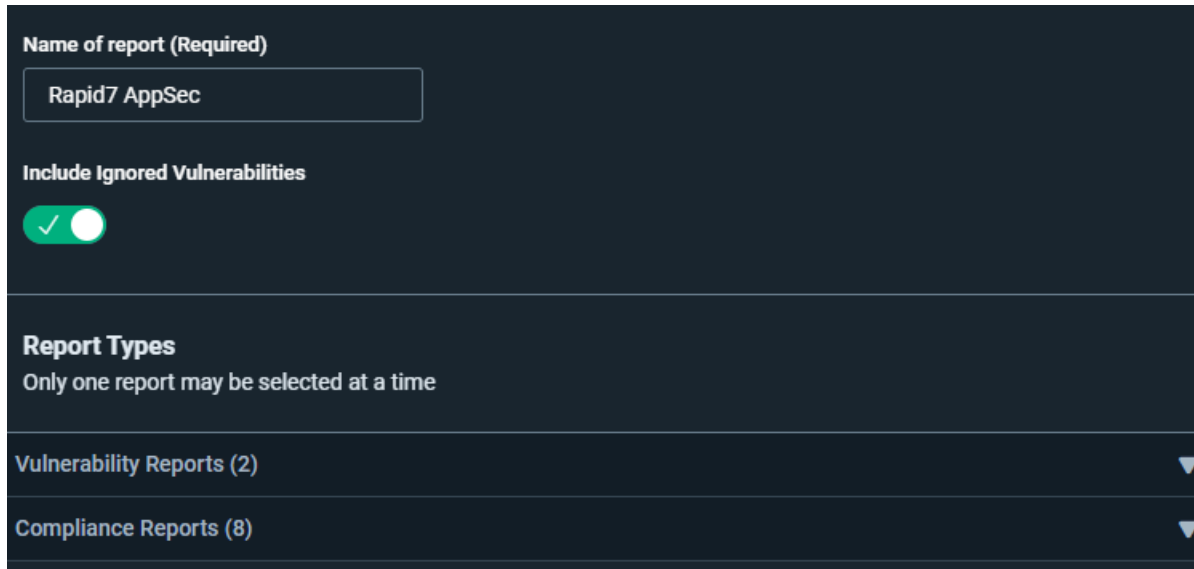
Downloading the Report of the Website

After scanning we can download the report but before downloading the report we need to validate the report to ensure that is genuine report after that we can generate the report as shown below

Figure 14 Report Validation and Generation
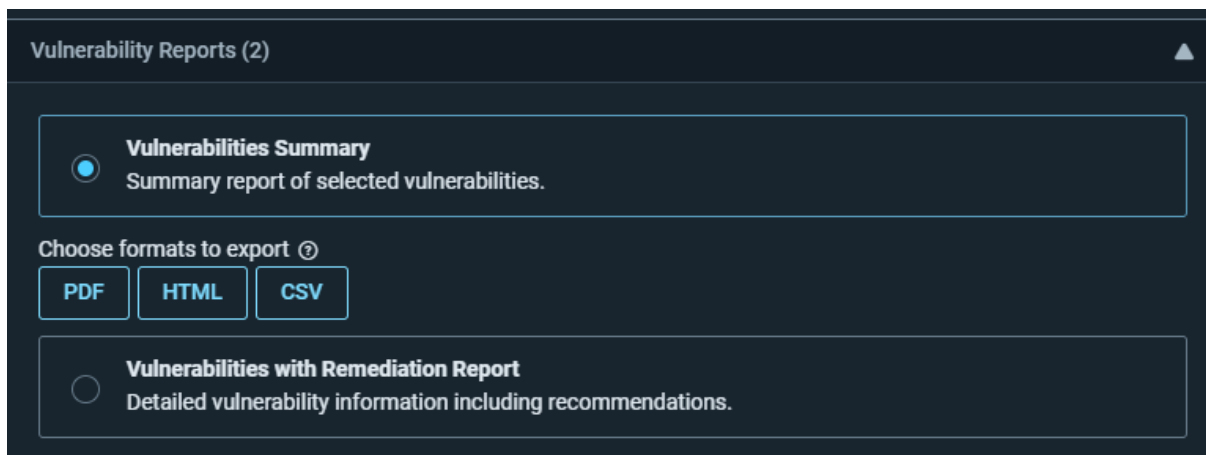
File Format of Report

As we can see the basic thing is which type of file we want to generate and submit to higher officials to see the security things in the code as shown below in Figure 15

Figure 16

As we can see in Figure 16 it also asks to include ignored vulnerabilities it is optional but if we include that we will have some more accuracy in the report that will help us solve the security issues and we can also say that up to now how many attacked are performed till on that so that everyone will have a scope of security on it.
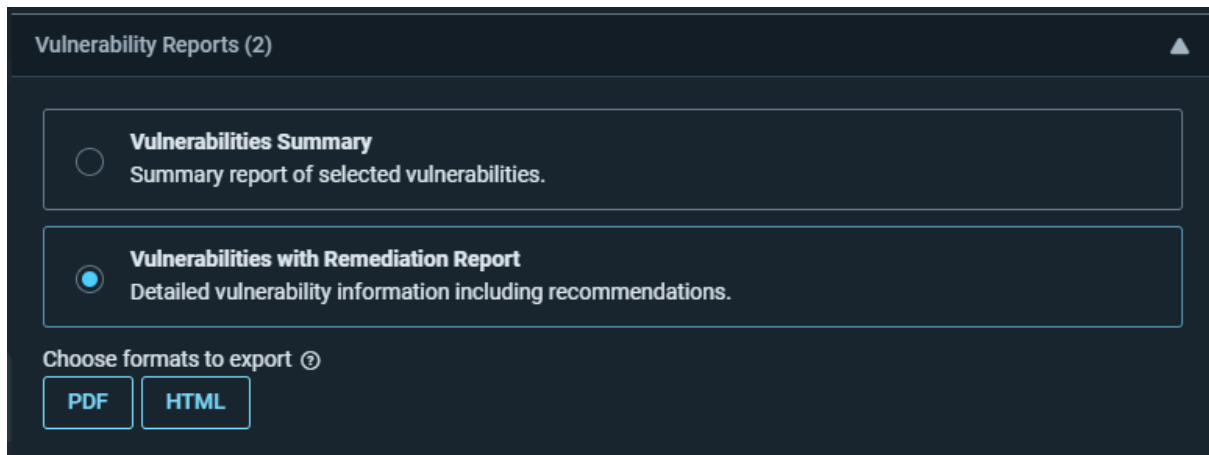
Figure 17&18 Vulnerability report

In the vulnerability report as we can see the basic report and advanced report with mitigation of the risk

When it comes to basic reports, a description of the attack will be known, and where the attack has been raised at a particular part of the code.

But when it comes to advanced reports it will perform all the basic operations of the report in that where the vulnerability has been raised it will give a solution for that particular and comments and code changes to mitigate the attack. It can be downloaded in PDF format or HTML format of the file.

It will make a report according to levels of vulnerability raised in that attack. The important point is the advanced report will have more accuracy and scope in the way the attack can happen and can be exposed with details and where it will start to mitigate and it will give a clear picture to make risk treatment
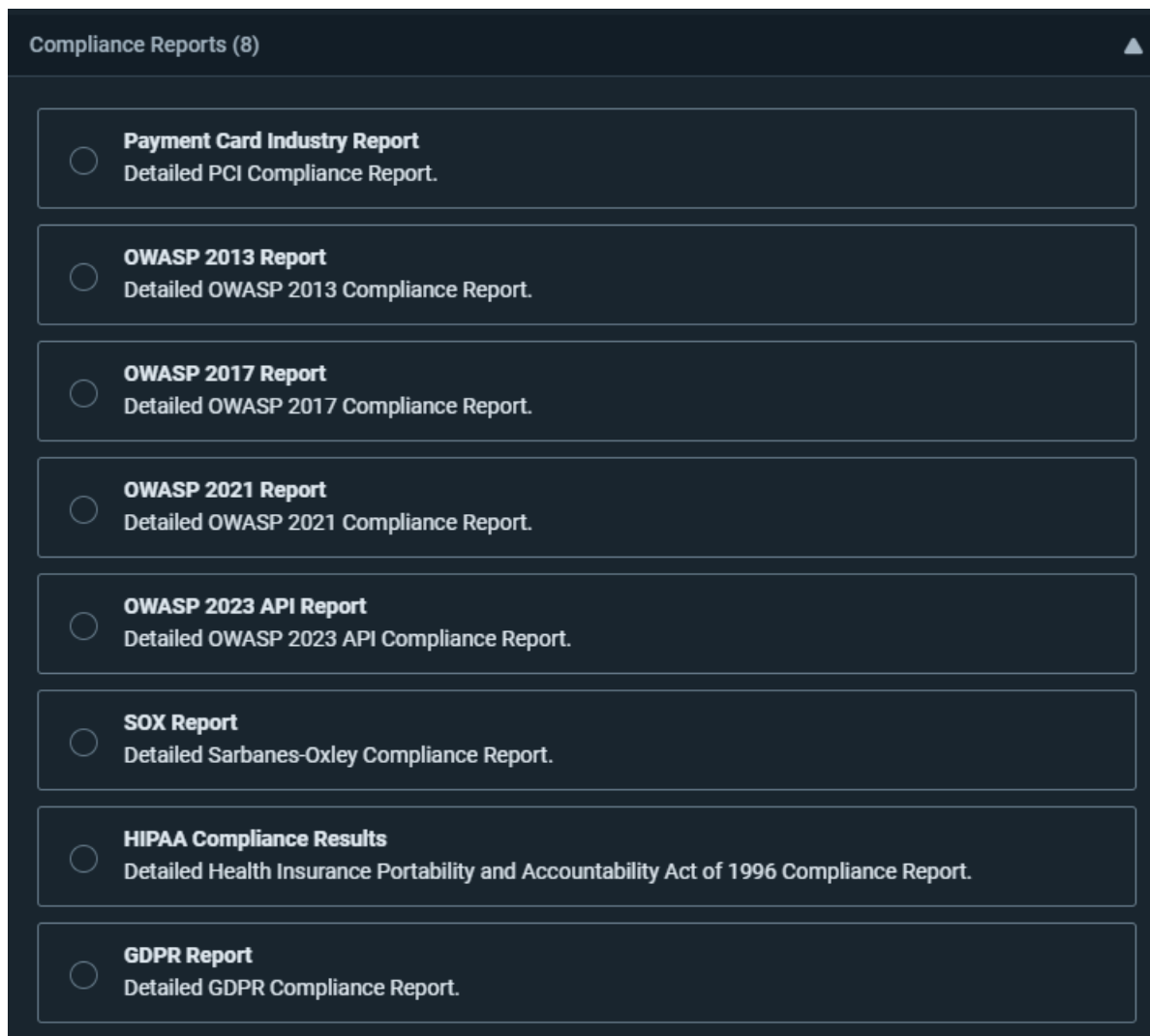
Figure 19 Compliance in report

As of now, we have seen the vulnerability scope in the report but we need to check whether it follows as per Figure 18 we can see how many policies have been included now in Rapid7 to ensure its security.

Payment card industry data security system (PCI DSS) is an industry that will ensure the security of credit card and debit cards.

OWASP will tell us all the top vulnerabilities that should be top list to be mitigated in the code to prevent cyberattacks.

SOX compliance is an annual obligation derived from the Sarbanes-Oxley Act (SOX) that requires publicly traded companies doing business in the U.S. to establish financial reporting standards, including safeguarding data, tracking attempted breaches, logging electronic records for auditing, and proving compliance.

HIPPA is an American policy that is meant to secure the details of the insurance holder of US citizens

GDPR is a European act that is meant to protect the data of the common people's user data

Final Report for Rapid7 AppSec

RAPID7 Vulnerabilities Summary
WebScanTest

App Name: WebScanTest   Scan Config: recommended-webscantest   Scan Date: 25/08/23 6:28 PM   Report Generated: 25/08/23 7:06 PM

19m 32s	46	210
Duration of Scan	Crawled Links	Vulnerabilities Discovered
Scan Completed - 25/08/23 6:48 PM	Logged Out	23159 - Attacks Performed

Vulnerabilities by Type

Vulnerability Type	Amount	Vulnerability Type	Amount
Anonymous Access	1	Predictable Resource Location	1
Autocomplete attribute	1	Privacy Policy Check	2
Blind SQL	2	Reflected Cross-site scripting (XSS)	1
Brute Force (HTTP Auth)	1	Reflection	2
Collecting Sensitive Personal Information	1	SQL Information Leakage	1
Content Security Policy Header	38	SQL Injection	2
Cookie attributes	8	Sensitive Data Exposure	1
Credentials over an insecure channel	1	Sensitive data over an insecure channel	4
Directory Indexing	3	Server Configuration	1
HTTP Authentication over insecure channel	1	Session Fixation	1
HTTP Headers	37	Session Strength	2
HTTPS Everywhere	45	Subresource Integrity	2
JSON Injection	4	X-Content-Type-Options	20
JavaScript Memory Leaks	1	X-Powered-By	25
		XPath Injection	1

Figure 20 Final report

It's the first page of the report generated by rapid7 where it will give all the basic details of the entire attack with a list and time of scan and URL which we performed to attack.

It will also list the vulnerabilities as per the report till now 210.

As we go next pages of the report it will give details of all website attacks that have happened on that website It depends on the option which we choose upto like basic or Advanced vulnerability report.

IDR

Introduction

The rapid7 will also provide IDR (Incident Detection and Response) is basically performs both SIEM and XDR. In order to maintain the integrity of data in an organization based on monitoring of all activities to provide real-time security to all devices in the organization. As we can see below figure 21 is the home interface of rapid7 IDR as of now we have not installed any collectors to collect the data.
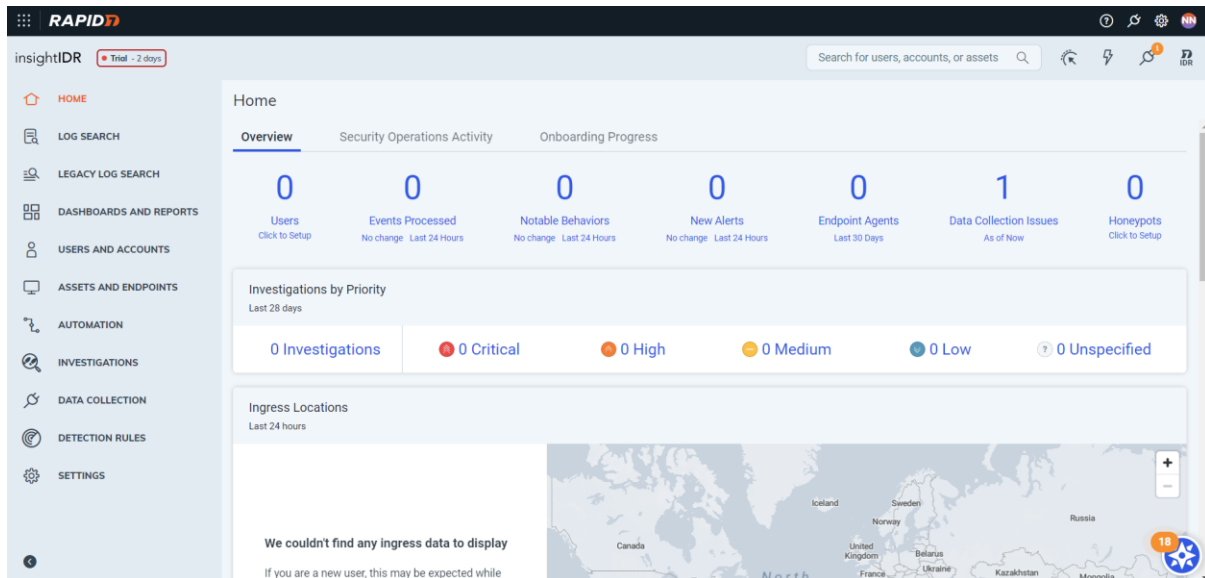

Figure 21 Rapid7 IDR home page

Steps to deploy the IDR collector:

1. We will be downloading the package for the Windows OS from the rapid7
2. After that we will deploy the package in the client computer. After that, it will start to install on the client computer
3. After completing all the steps, we need to copy the token number from the client's computer.
4. We need to activate the collector in the Legacy Log search in that we will have an option called Activate collector
5. We need to client name and we need to paste the token on the below and Activate the collector.
6. After this step the collector is successfully deployed on the client's computer
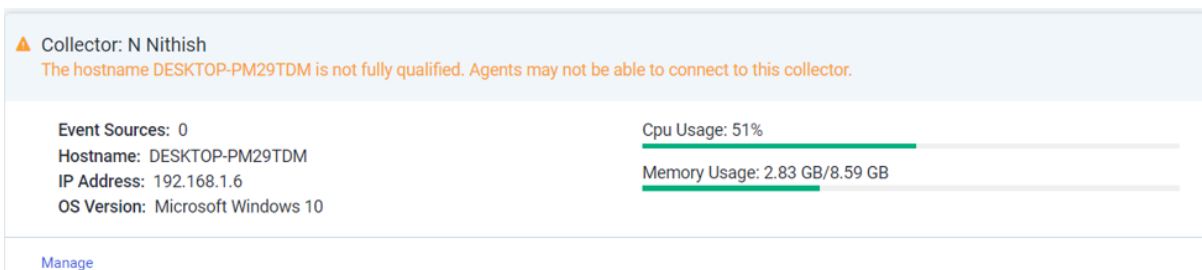
Insight Agent

The insight agent is a log collector and log analyzer It helps to collect logs from the client's computer to make sure to prevent any malicious activity in the client's computer it is a lightweight application and supported by all versions of Windows, Mac, and Linux OS.

Steps to deploy the agent in the client's computer:

1. We need to select the OS and version to download the package.
2. We also need to generate a token for the package and we will get the token based on the bit version like 32bit or 64bit
3. After generating the token, we need to download the package in the client system. We need to run the command that we generated in the token generation.
4. After successfully running the command the package, which conducts testing will show as shown below
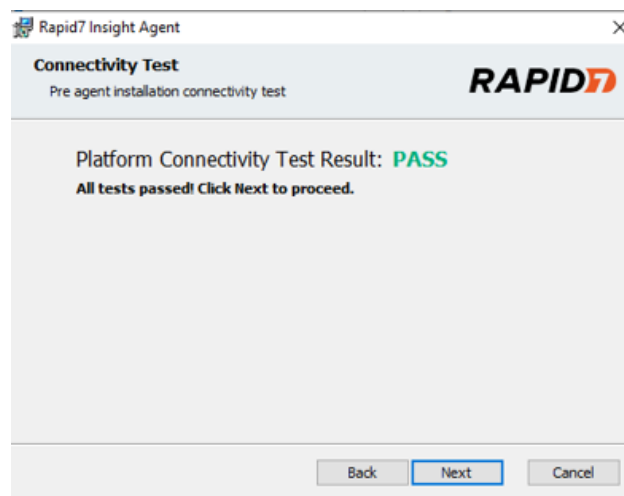
5. We need to click the next button to complete the process of installation of the package in the client system.
6. In the insight menu we can see that the desktop has been connected successfully.
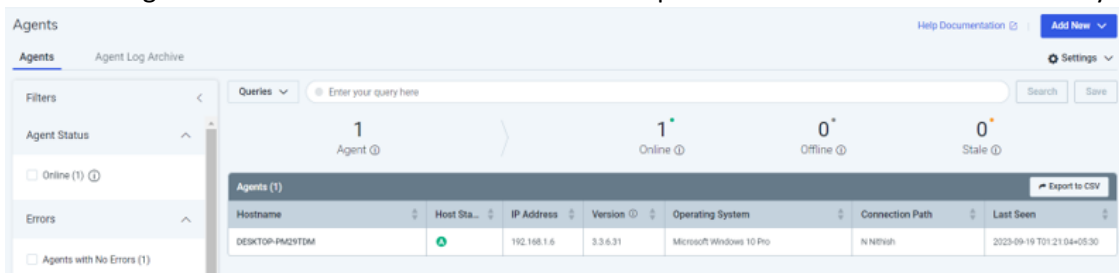
7. If we right-click on the Desktop we will get an option called Collect logs
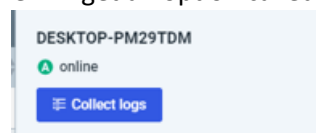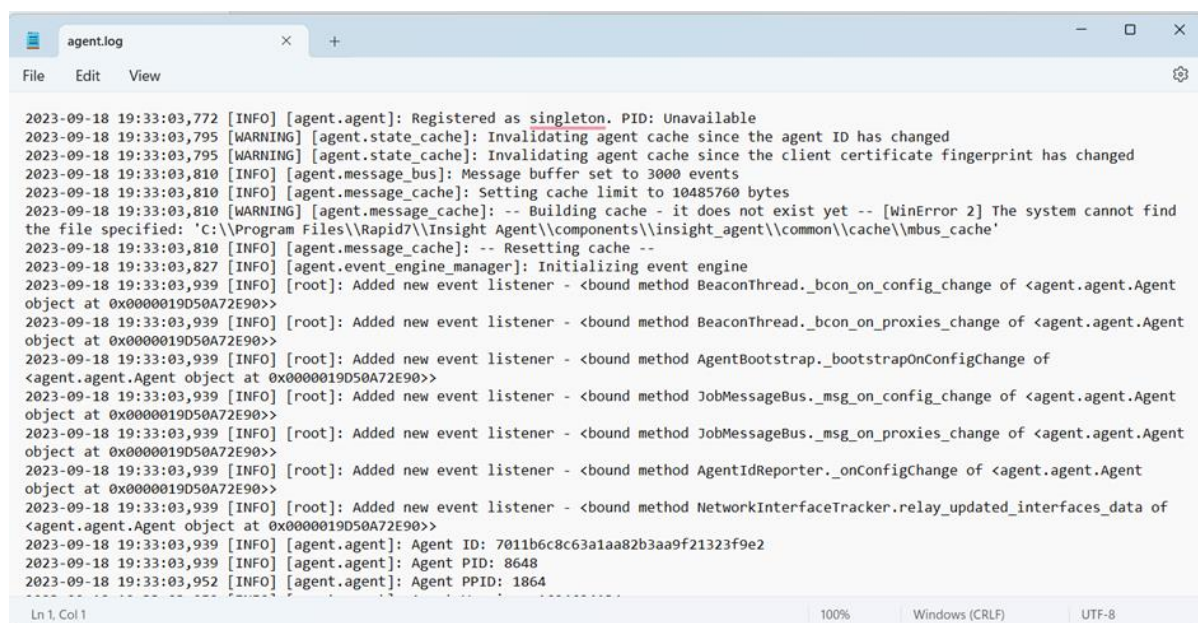
8. After collecting logs, we will get Complected in the status button

9. We need to download the file and the file will be downloaded in the form of zip file. We need to extract the file to see the content the below image shows the content in the zip file

10. The agent.log file contains the log files that are collected in the client system

Now we successfully collected the log files from the client system