

# ***RAPID***

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

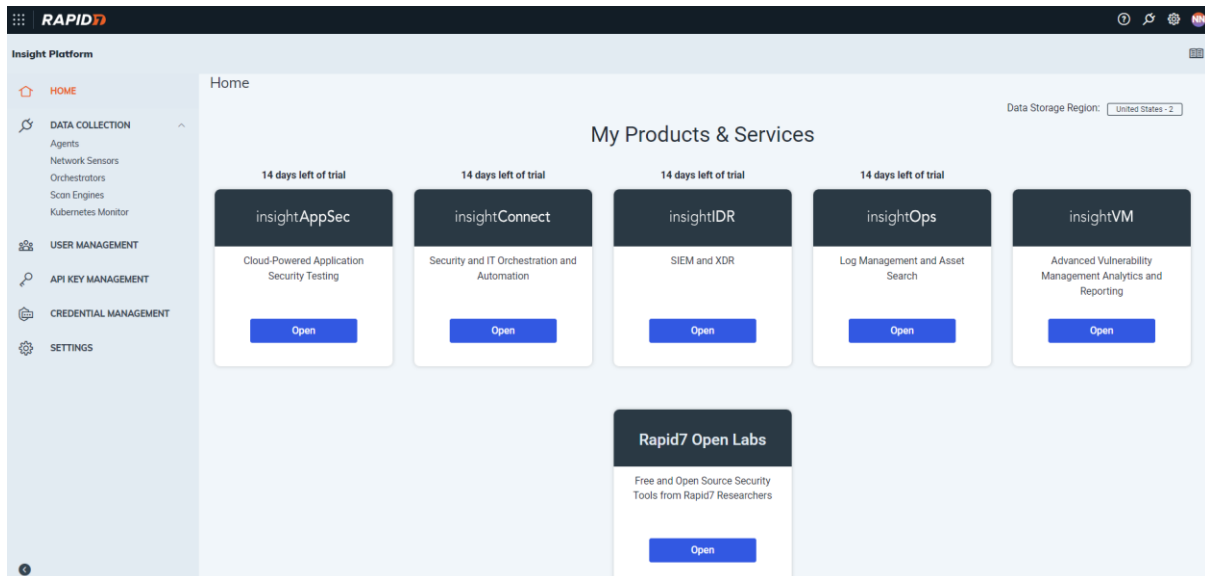


Figure 1 Home Page of Rapid7

As we can see the interface of Rapid7 Home where we will see services provided by Rapid7. 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 work. As we see below I will explain how the demo website and Domain-based website with clear and proper instructions.

# Insight AppSec

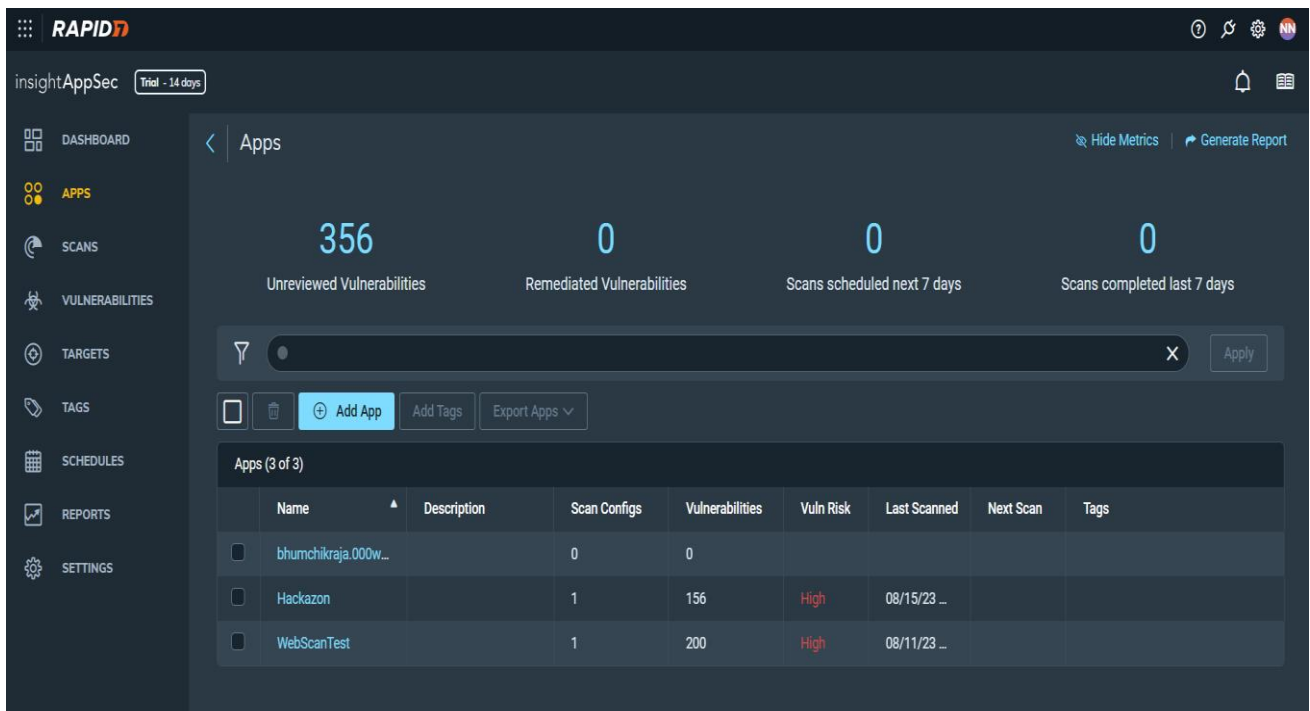


Figure 2 AppSec Home Page

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.

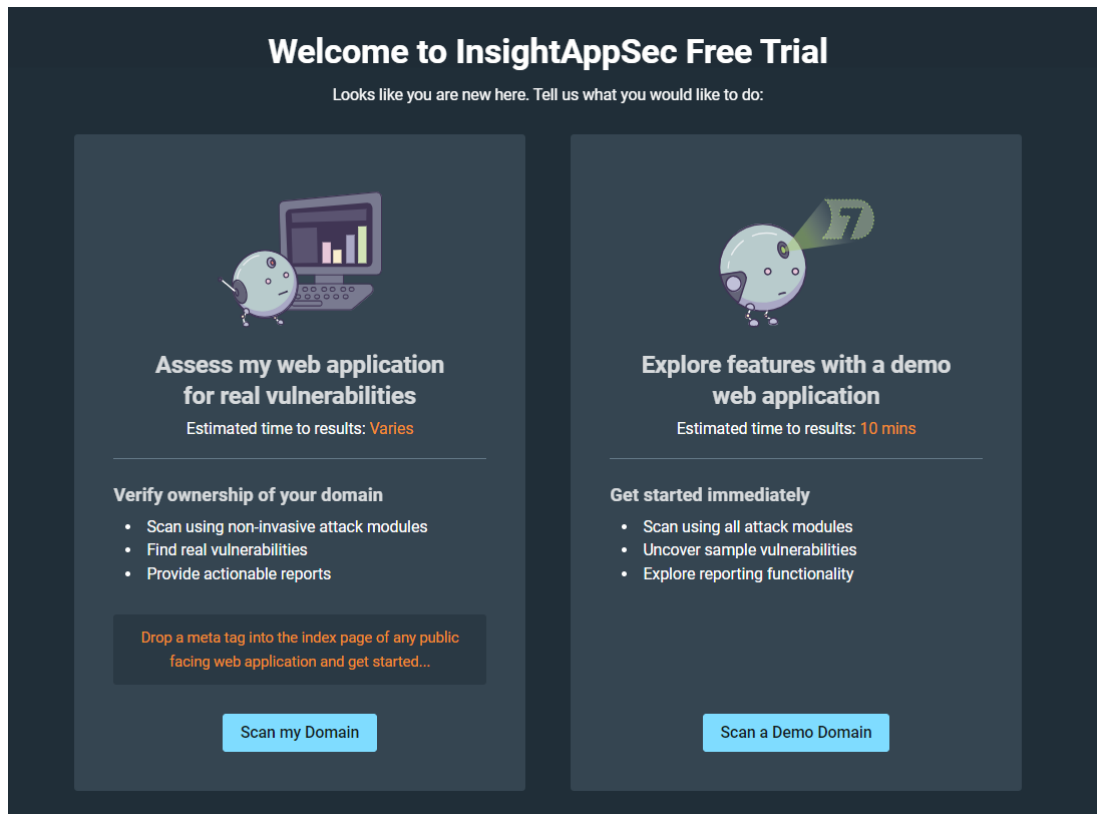


Figure 3 Add App Options

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

The image shows a form titled 'Scan My Domain Options' with a dark background. On the left, there is a vertical list of three steps: '1 Target domain', '2 Add meta tag to target domain', and '3 Verify domain'. Step 1 is currently active. Below step 1, there is a text input field with a dropdown menu showing 'http://' and a placeholder text 'e.g www.mydomain.com'. Below the input field, there is a note: 'Choose the most appropriate protocol for your target domain, as your choice of protocol affects the scan results.' At the bottom of the form, there are two buttons: 'Back' and 'Run Scan'.

Figure 4 Scan My Domain Options

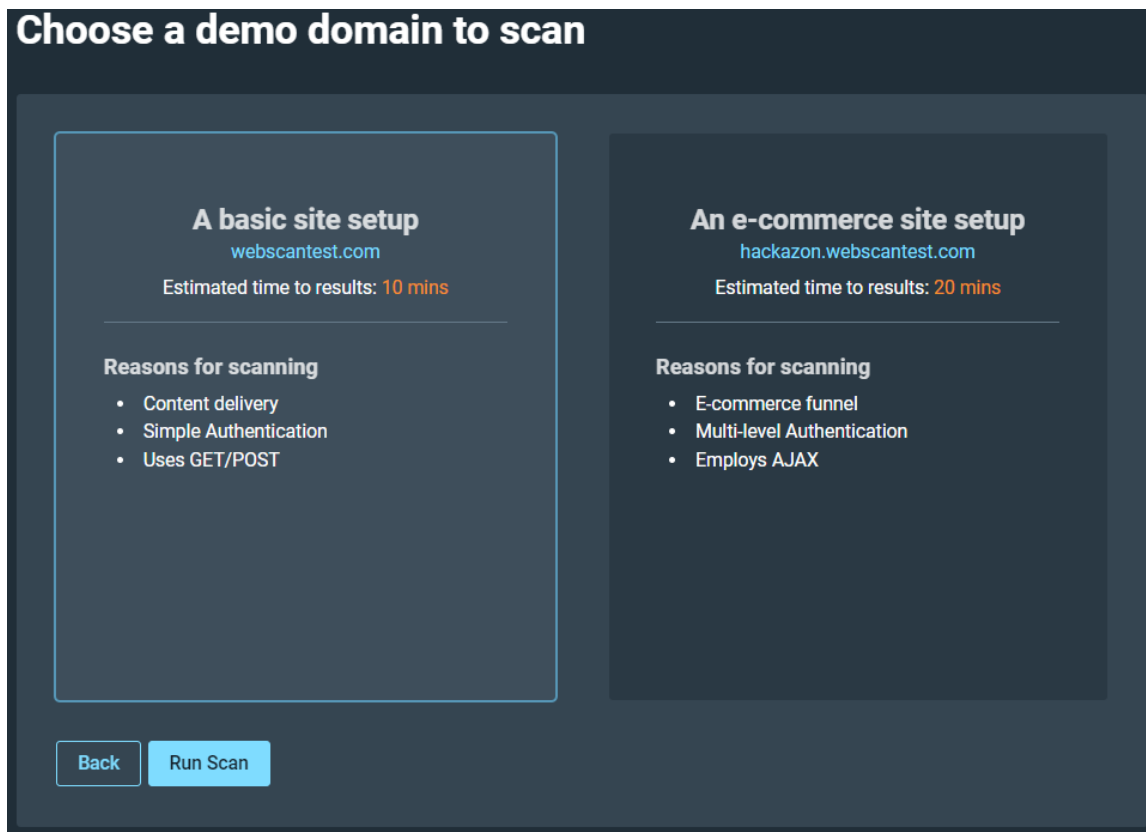


Figure 5 Performing Demo Scan Options

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.

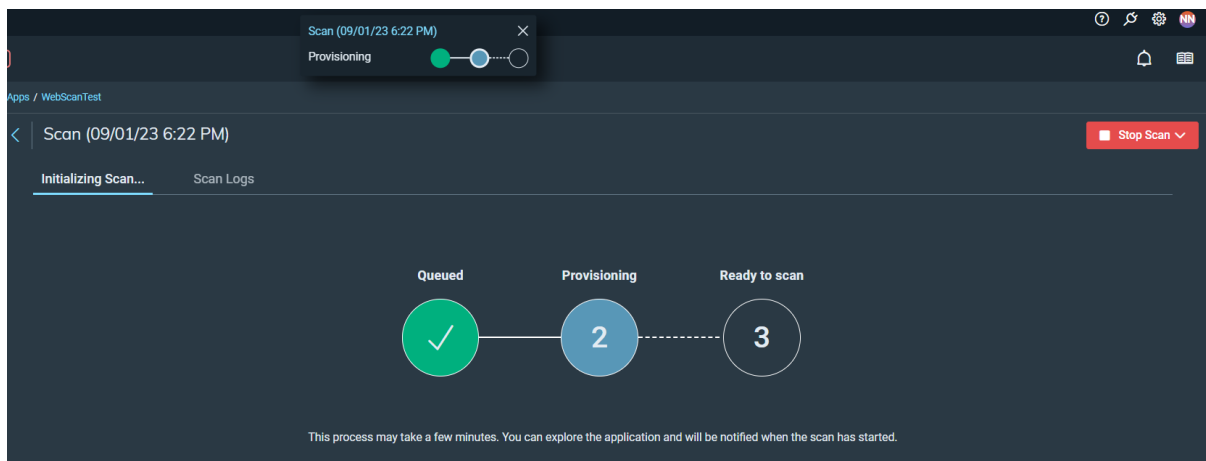


Figure 6 Initiate the Scan of the website

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

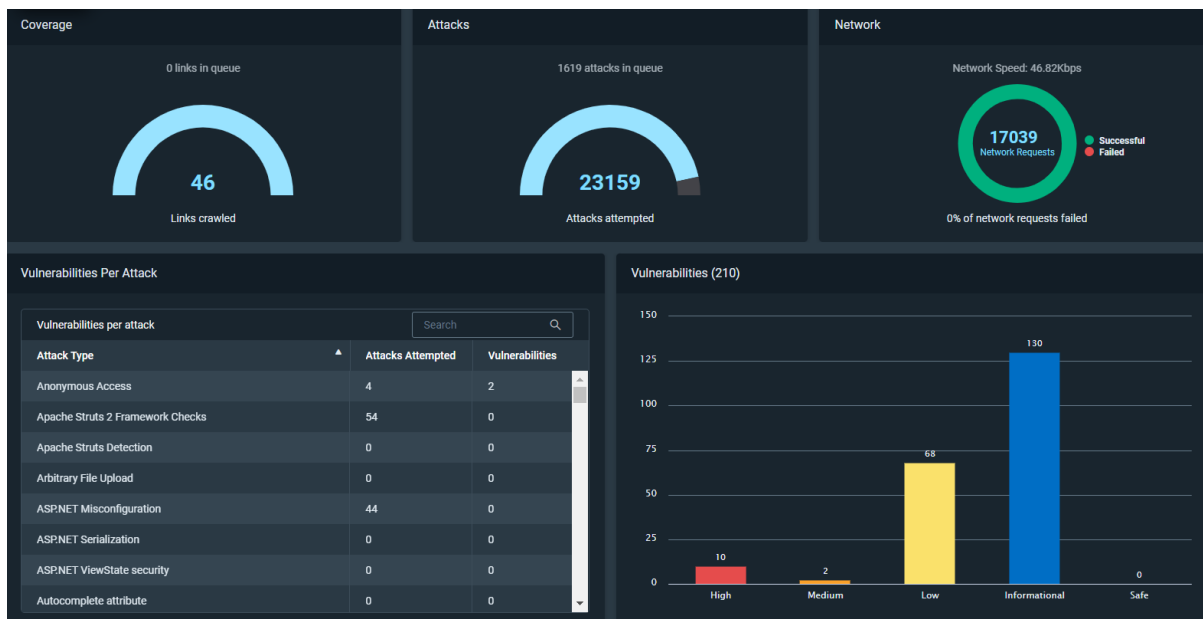


Figure 7 Scan Results of the website

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 ways 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.

Overview **Vulnerabilities** Crawl Map Scan Logs

Select Saved Filter [X] Apply Save

210 Vulnerabilities 207 Unreviewed 0 Ignored 0 False Positive 0 Verified 3 Remediated 0 Duplicate 0 New

Change Severity Change Status Export Vulnerability

Vulnerabilities for WebScanTest (200 of 210) Manage Columns

| URL   | Parameter    | Module Type            | Attack Type    | CVSS | Severity | First Discovered | Last Discovered  | Status     |
|---|--------------|------------------------|----------------|------|----------|------------------|------------------|------------|
| ...p://webscantest.com/infodb/search_by_name.php  | fname        | JSON Injection         | JSONInjection  | 9.8  | High     | 09/01/23 6:34 PM | 09/01/23 6:59 PM | Unreviewed |
| http://webscantest.com/react/16/                  | Directory[1] | JSON Injection         | JSONInjection  | 9.8  | High     | 09/01/23 6:37 PM | 09/01/23 6:59 PM | Unreviewed |
| ...webscantest.com/datastore/search_get_by_id.php | id           | SQL Injection          | SQLInjection   | 9.8  | High     | 09/01/23 6:47 PM | 09/01/23 6:59 PM | Unreviewed |
| ...webscantest.com/datastore/search_get_by_id.php | id           | Blind SQL              | BSQLInjection  | 7.8  | High     | 09/01/23 6:38 PM | 09/01/23 6:59 PM | Unreviewed |
| ...webscantest.com/rest/demo/index.php/products   | index        | JSON Injection         | JSONInjection  | 9.8  | High     | 09/01/23 6:47 PM | 09/01/23 6:59 PM | Unreviewed |
| http://webscantest.com/basic_auth/basic_auth.php  |              | Brute Force (HTTP A... | HTTPBruteForce | 6.3  | High     | 09/01/23 6:33 PM | 09/01/23 6:59 PM | Unreviewed |
| http://webscantest.com/react/15/                  | Directory[1] | JSON Injection         | JSONInjection  | 9.8  | High     | 09/01/23 6:35 PM | 09/01/23 6:59 PM | Unreviewed |
| ...scantest.com/datastore/search_get_by_name.php  | name         | SQL Injection          | SQLInjection   | 9.8  | High     | 09/01/23 6:38 PM | 09/01/23 6:59 PM | Unreviewed |
| ...scantest.com/datastore/search_get_by_name.php  | name         | Blind SQL              | BSQLInjection  | 7.8  | High     | 09/01/23 6:36 PM | 09/01/23 6:59 PM | Unreviewed |
| ...p://webscantest.com/infodb/search_by_name.php  | fname        | XPath Injection        | XPathInjection | 9.4  | High     | 09/01/23 6:35 PM | 09/01/23 6:59 PM | Unreviewed |

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.

Module Type: JSON Injection
Generate Report
Copy Vulnerability Link

High
Unreviewed

0 days ago
0 days ago
3

Severity
Status
First Detected
Last Detected
Times Discovered

Vulnerability Information

General

Attack TypeJSONInjection
AppWebScanTest
IDae843232-690e-40d8-b9b7-e585e5ac0339
JIRAX Not Exported
CVSS Score9.8 (Critical)
Vector StringAV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Root Cause

URLhttp://webscantest.com/infodb/search\_by\_name.php
Parameterfname
MethodPOST

Attack Variances - based on last scan 'Val: Scan (09/01/23 6:52 PM)'

Attack 1
Attack 2
Attack 3

Original ValueJohn
Attack ValueJohn%22,%22Account%22:%22administrator%22
Attack DescriptionServer Side Injection

Proof"Account"."administrator"
Proof Description

Show References & Recommendations
Replay Attack

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.

Module Type: JSON Injection Generate Report Copy Vulnerability Link

Original Traffic #1 Wrap Text

Request Response Copy

```

1 POST /infodb/search_by_name.php HTTP/1.1
2 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
3 Accept-Encoding: gzip, deflate
4 Accept-Language: en-US
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36
6 X-RTC-AUTH: R7_IAS
7 X-RTC-SCANID: 333137ae-87ad-4bde-a279-c93456d95b1e
8 Host: webscantest.com

```

Attack Traffic #1 Copy

```

1 POST /infodb/search_by_name.php HTTP/1.1
2 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
3 Accept-Encoding: gzip, deflate
4 Accept-Language: en-US
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36
6 X-RTC-AUTH: R7_IAS
7 X-RTC-SCANID: 333137ae-87ad-4bde-a279-c93456d95b1e
8 Host: webscantest.com

```

Discovery History - Discovered 3 Times

Scans containing vulnerability (3) Search

| Name                         | App         | Config               | Completed          | Duration |
|------------------------------|-------------|----------------------|--------------------|----------|
| Val: Scan (09/01/23 6:52 PM) | WebScanTest | recommended-websc... | 09/01/23 7:00 P... | 7m 35s   |

Figure 10 shows the original traffic and attack traffic from 1<sup>st</sup> Attack.

Original Traffic #1 Wrap Text

Request Response Copy

```

1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
3 Connection: close
4 Date: Fri, 01 Sep 2023 18:54:48 GMT
5 Pragma: no-cache
6 Content-Length: 628
7 Content-Type: text/html
8 Content-Encoding: gzip
9 Expires: Thu, 19 Nov 1981 08:52:00 GMT
10 Server: Apache/2.4.7 (Ubuntu)
11 Vary: Accept-Encoding
12 x-powered-by: PHP/5.5.9-1ubuntu4.29
13
14
15 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
16 <html>
17   <head>
18     <link type="text/css" rel="stylesheet" href="/css/style.css" />
19     <title>Search by name</title>
20
21   </head>
22   <body topmargin="0" leftmargin="0" marginheight="0" marginwidth="0" bgcolor="#000000">
23     <table cellspacing="0" cellpadding="0" border="4" align="center" width="810">

```

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.

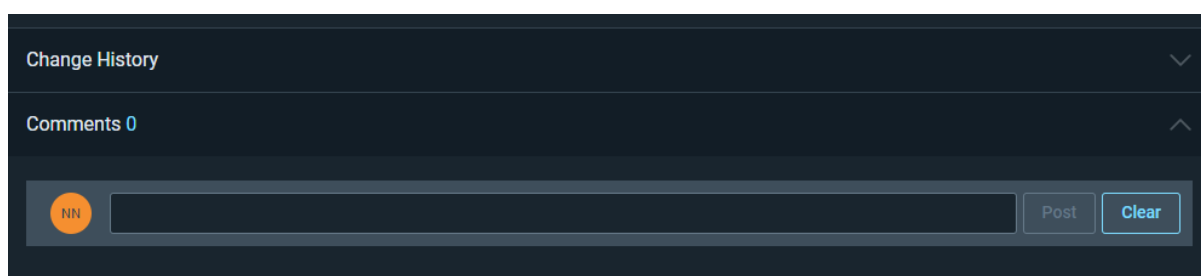


Figure 13

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

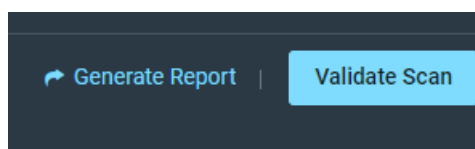
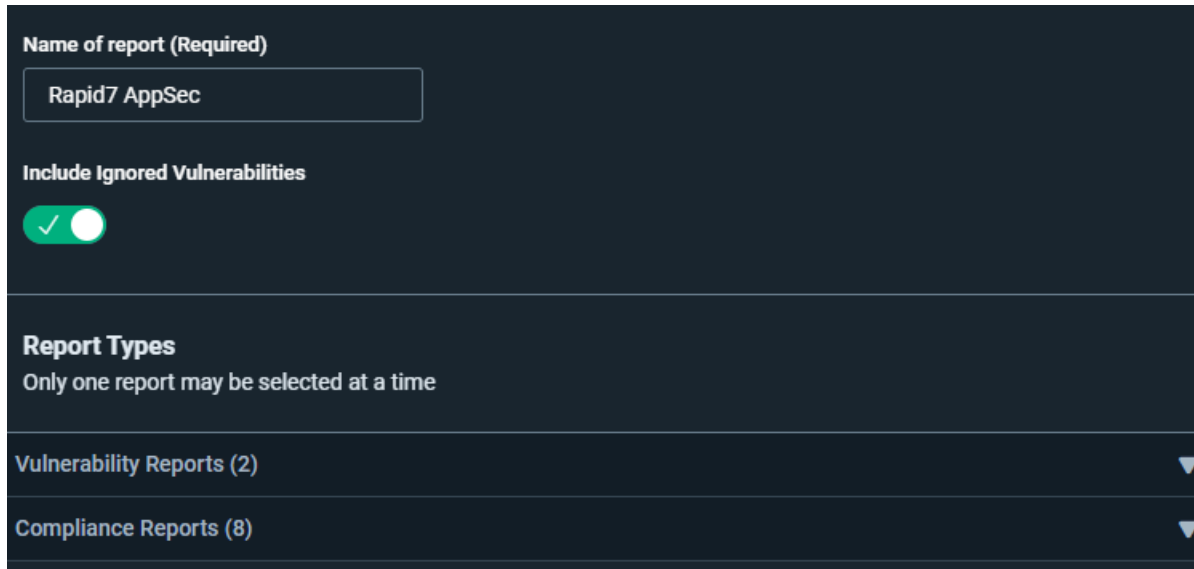


Figure 14 Report Validation and Generation

## File Format of Report

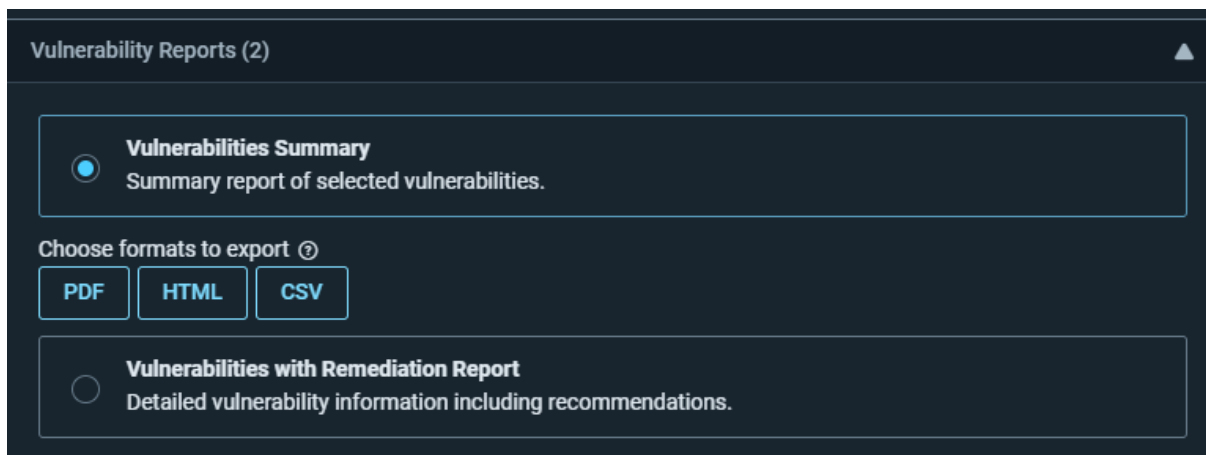
As we can see the basic thing is which type of file we want to generate and submit to higher officials to see the security things in the code as shown below in Figure 15



The screenshot shows a dark-themed configuration interface for generating a report. At the top, there is a section titled "Name of report (Required)" with a text input field containing "Rapid7 AppSec". Below this is a toggle switch for "Include Ignored Vulnerabilities", which is currently turned on, indicated by a green checkmark. The next section is titled "Report Types" with the instruction "Only one report may be selected at a time". Under this section, there are two expandable categories: "Vulnerability Reports (2)" and "Compliance Reports (8)", each with a downward-pointing arrow.

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.



This screenshot provides a detailed view of the "Vulnerability Reports (2)" section. It features two radio button options for selecting a report type. The first option, "Vulnerabilities Summary", is selected and described as a "Summary report of selected vulnerabilities." The second option, "Vulnerabilities with Remediation Report", is unselected and described as "Detailed vulnerability information including recommendations." Below these options, there is a section titled "Choose formats to export" with a help icon. It contains three buttons: "PDF", "HTML", and "CSV".

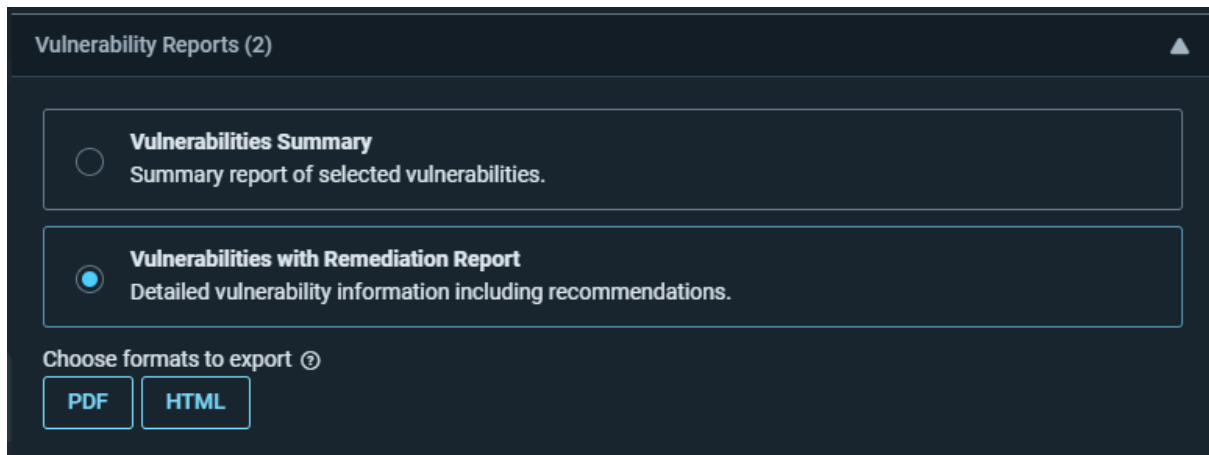


Figure 17&18 Vulnerability report

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

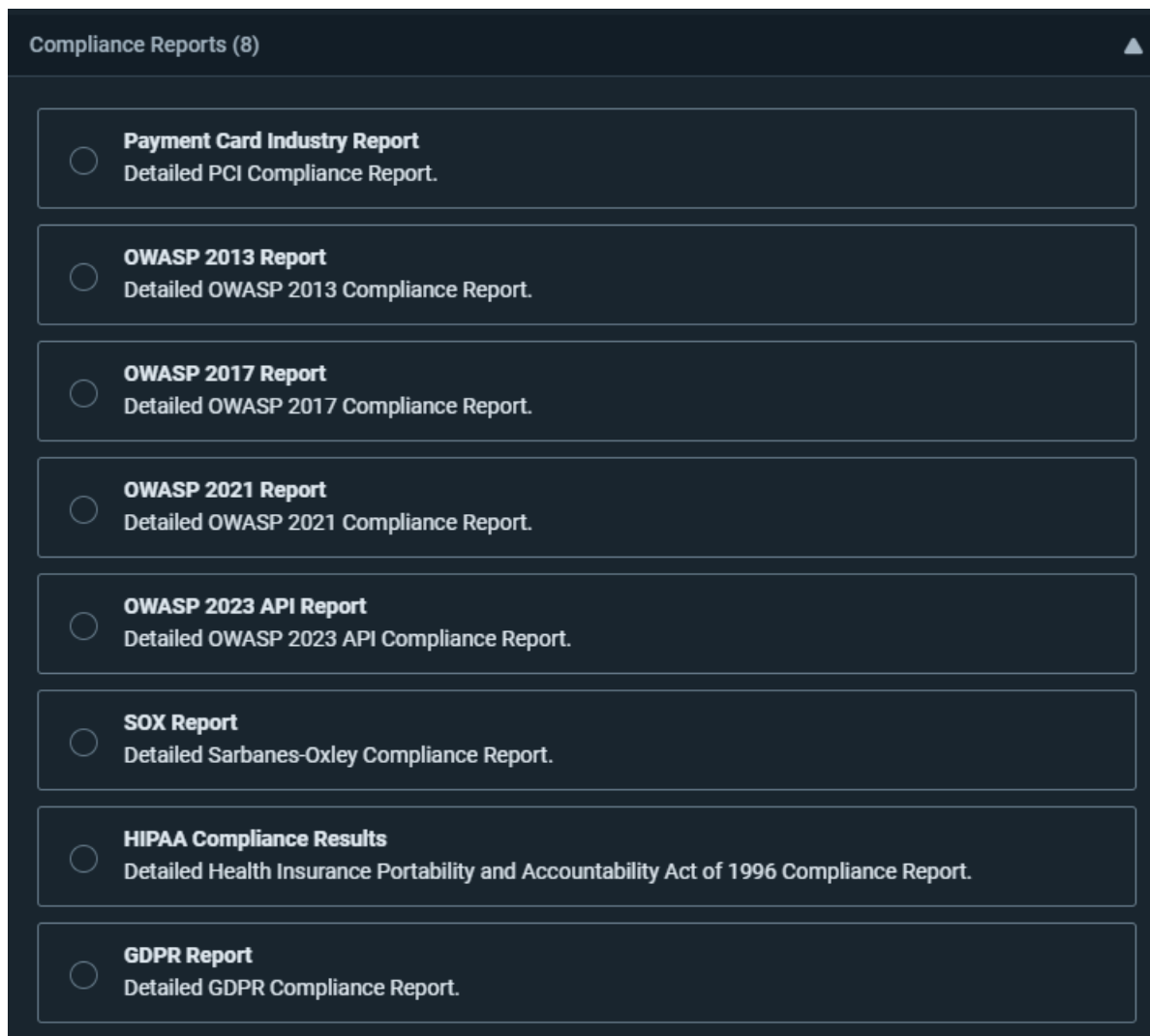


Figure 19 Compliance in report

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

|   |  |   |
|---|--|---|
| <b>19m 32s</b><br>Duration of Scan<br>Scan Completed - 25/08/23 6:48 PM | <b>46</b><br>Crawled Links<br>Logged Out | <b>210</b><br>Vulnerabilities Discovered<br>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.

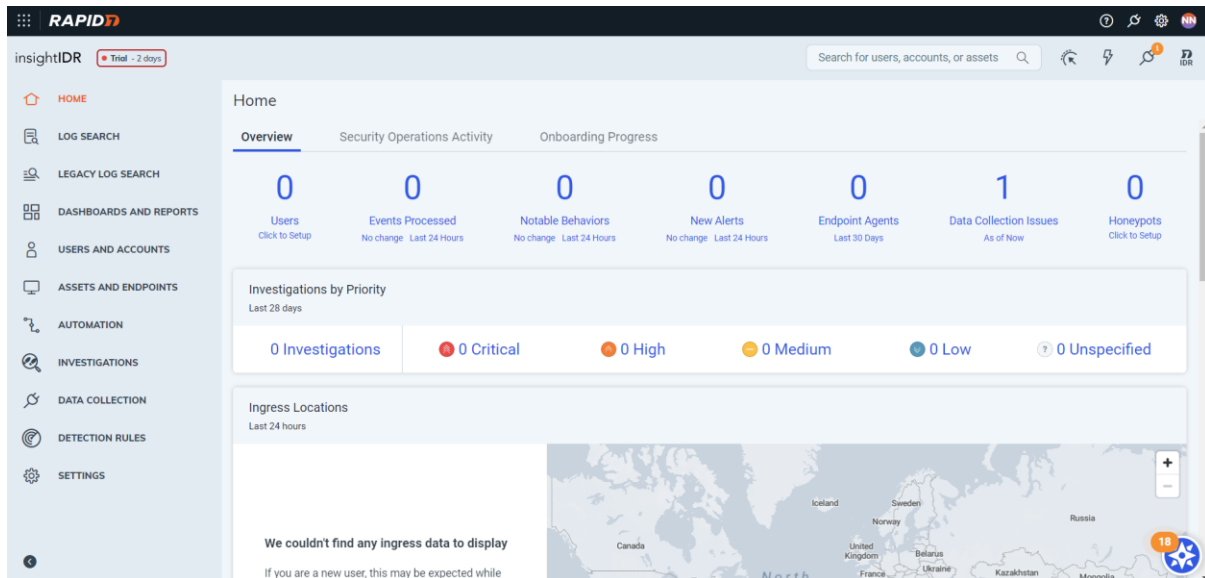
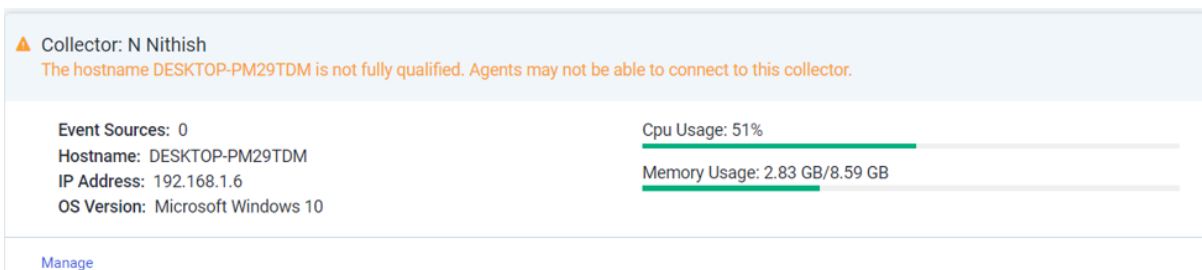


Figure 21 Rapid7 IDR home page

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

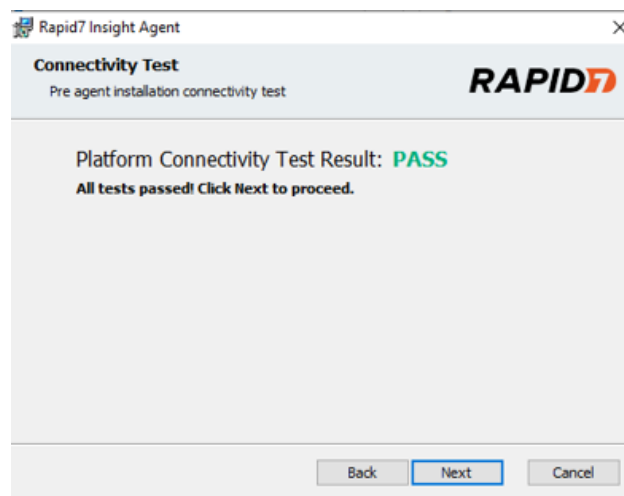


# Insight Agent

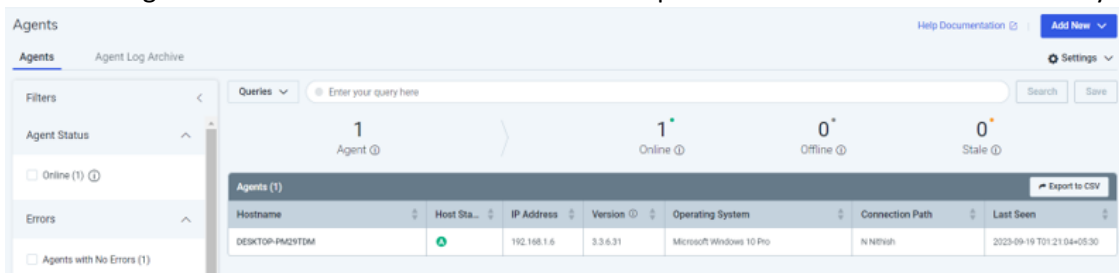
The insight agent is a log collector and log analyzer. It helps to collect logs from the client's computer to make sure to prevent any malicious activity in the client's computer. It is a lightweight application and is supported by all versions of Windows, Mac, and Linux OS.

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

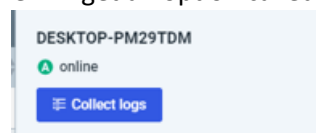
1. We need to select the OS and version to download the package.
2. We also need to generate a token for the package and we will get the token based on the bit version like 32bit or 64bit
3. After generating the token, we need to download the package in the client system. We need to run the command that 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



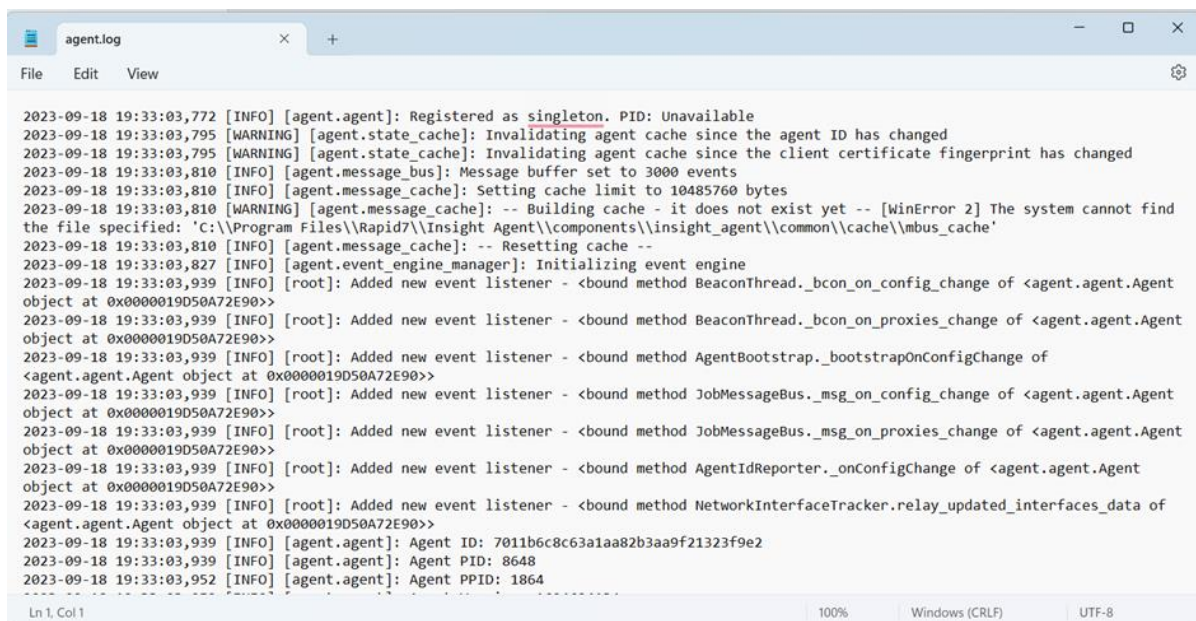
8. After collecting logs, we will get Completed in the status button

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

Downloads > tmpcvjtyq9r.zip

| Name                 | Type                      | Compressed size | Password p... | Size     | Ratio |
|----------------------|---------------------------|-----------------|---------------|----------|-------|
| agent.log            | Text Document             | 82 KB           | No            | 1,433 KB | 95%   |
| bootstrap.cfg        | Configuration Source File | 1 KB            | No            | 1 KB     | 6%    |
| bootstrap.log        | Text Document             | 7 KB            | No            | 21 KB    | 69%   |
| insight_agent.stderr | STDERR File               | 1 KB            | No            | 0 KB     | 0%    |
| insight_agent.stdout | STDOUT File               | 1 KB            | No            | 1 KB     | 42%   |
| SmartSocket.json     | JSON Source File          | 1 KB            | No            | 1 KB     | 62%   |

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



```
2023-09-18 19:33:03,772 [INFO] [agent.agent]: Registered as singleton. PID: Unavailable
2023-09-18 19:33:03,795 [WARNING] [agent.state_cache]: Invalidating agent cache since the agent ID has changed
2023-09-18 19:33:03,795 [WARNING] [agent.state_cache]: Invalidating agent cache since the client certificate fingerprint has changed
2023-09-18 19:33:03,810 [INFO] [agent.message_bus]: Message buffer set to 3000 events
2023-09-18 19:33:03,810 [INFO] [agent.message_cache]: Setting cache limit to 10485760 bytes
2023-09-18 19:33:03,810 [WARNING] [agent.message_cache]: -- Building cache - it does not exist yet -- [WinError 2] The system cannot find the file specified: 'C:\Program Files\Rapid7\Insight Agent\components\insight_agent\common\cache\mbus_cache'
2023-09-18 19:33:03,810 [INFO] [agent.message_cache]: -- Resetting cache --
2023-09-18 19:33:03,827 [INFO] [agent.event_engine_manager]: Initializing event engine
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method BeaconThread._bcon_on_config_change of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method BeaconThread._bcon_on_proxies_change of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method AgentBootstrap._bootstrapOnConfigChange of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method JobMessageBus._msg_on_config_change of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method JobMessageBus._msg_on_proxies_change of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method AgentIdReporter._onConfigChange of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [root]: Added new event listener - <bound method NetworkInterfaceTracker.relay_updated_interfaces_data of <agent.agent.Agent object at 0x0000019D50A72E90>>
2023-09-18 19:33:03,939 [INFO] [agent.agent]: Agent ID: 7011b6c8c63a1aa82b3aa9f21323f9e2
2023-09-18 19:33:03,939 [INFO] [agent.agent]: Agent PID: 8648
2023-09-18 19:33:03,952 [INFO] [agent.agent]: Agent PPID: 1864
```

Now we successfully the log files from the client system