

# **BURP SUITE FOR penTESTER**

**SOFTWARE VULNERABILITY  
Scanner & RETIRE.JS**



## Contents

<b>Introduction.....</b>	<b>3</b>
<b>Exploring the Burp Plugins .....</b>	<b>3</b>
<b>Software Vulnerability Scanner .....</b>	<b>3</b>
Configuring the Extension .....	4
Fingerprinting the installed software .....	8
<b>Retire.js .....</b>	<b>12</b>
Setting up the Plugin .....	12
Dumping the Outdated JavaScript Libraries .....	14

## Introduction

Not only the fronted we see or the backend we don't, are responsible to make an application vulnerable. A dynamic web application carries a lot within itself, whether it's about JavaScript libraries, third-party features, functional plugins, or many more. But what, if the installed features or the plugins themselves are vulnerable?

So, we won't be focusing on any specific vulnerability, rather we'll follow up with some nice burp extensions that will help us to **identify the vulnerable versions of the software or the libraries installed** within an application.

## Exploring the Burp Plugins

Over in all of our previous articles whatever scanner or the plugin we've used, they all dump almost the same results i.e., they identify and guide us about the **existing vulnerabilities** majorly based on the OWASP top 10. But, what about the software or the add-ons library versions that were embedded within the application's frameworks, how we could identify whether they are vulnerable or not.

Thereby to dig the web application at its maximum depth, the burp suite offers some amazing plugins that **scan the embedded software and the add-on libraries** and then further drop out the ones that have the **outdated version** or their **versions are vulnerable** to some specific exploits.

So, let's explore the two most popular extensions, one that checks the version from its exploits database and the other simply checks for the outdated JavaScript libraries.

## Software Vulnerability Scanner

Have you ever surfed [vulners.com](https://vulners.com) to identify the vulnerabilities found by the different security researchers?

Not yet, then over with this extension, you'll get a better understanding of the **vulners.com exploit's a database** or its scanning **API keys** and the other features that the web application carries within.

So, let's initiate by exploring, **what this burp extension is?**

The Software Vulnerability Scanner is one of the most popular burp extensions that scans the application to determine vulnerabilities in the software versions using the vulners.com API.

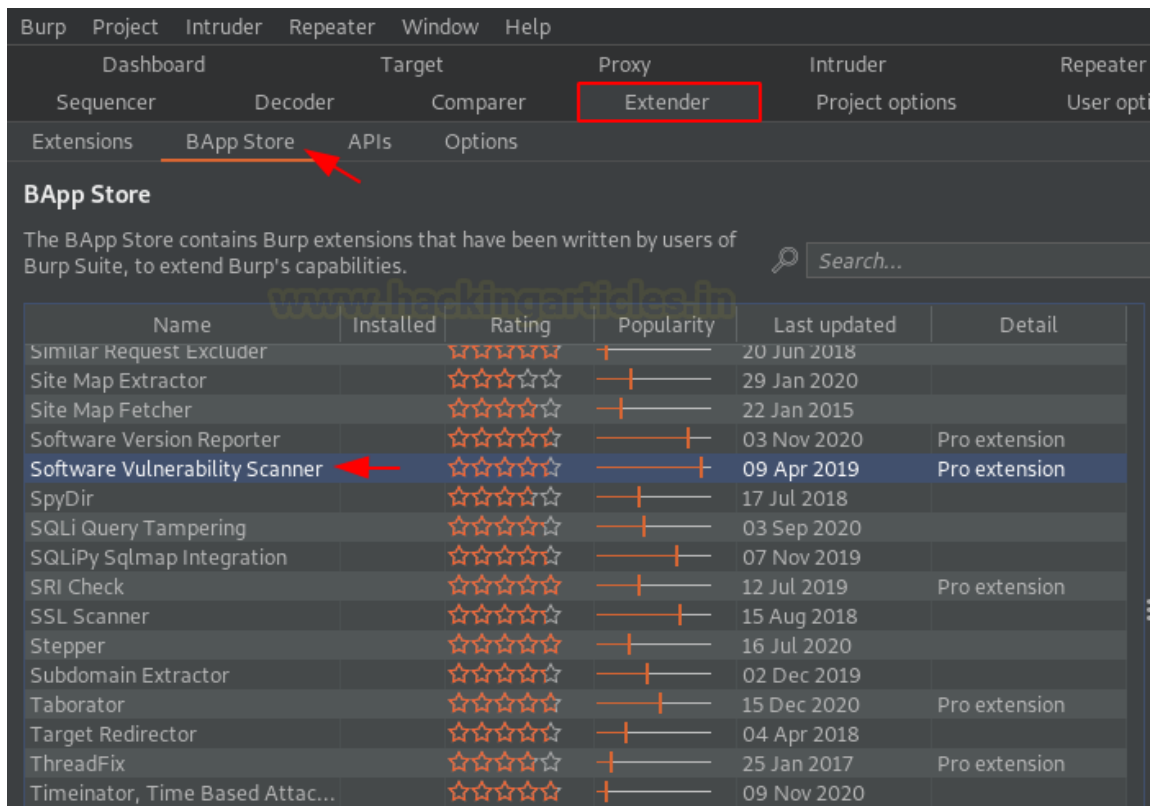
But ***how this plugin detects vulnerable software versions?***

To do so, this plugin follows either of the two –

1. It identifies the vulnerable software with the fingerprints or the CPE (Common Platform Enumeration).
2. It checks the vulnerable paths with the database and identifies whether any exploit can be used against that path or not.

## Configuring the Extension

Let's install the plugin by navigating to the **BApp Store** at the **Extender tab** and there we'll try to find **Software Vulnerability Scanner**.

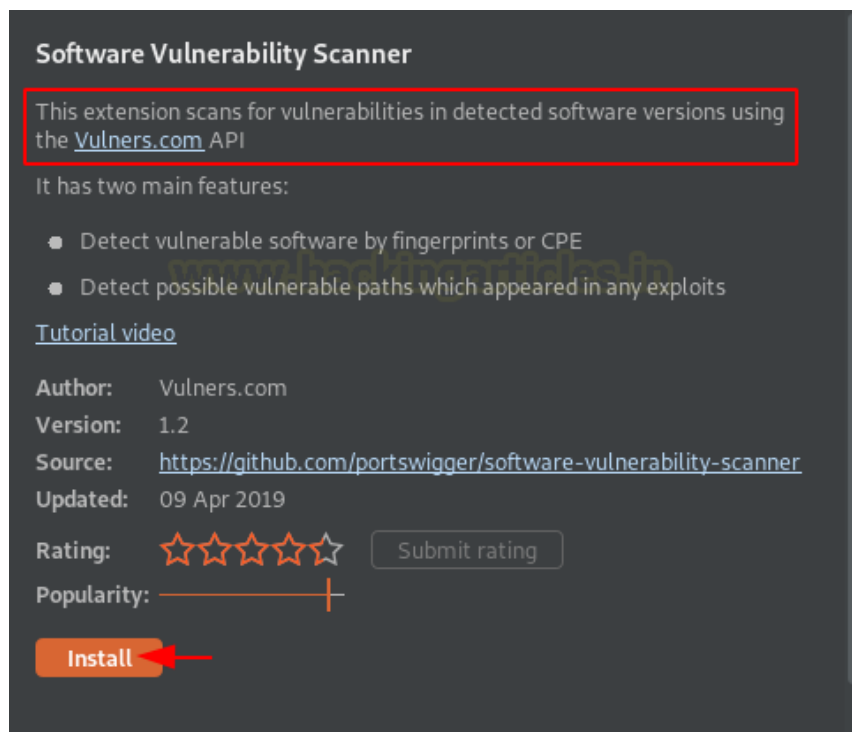


The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

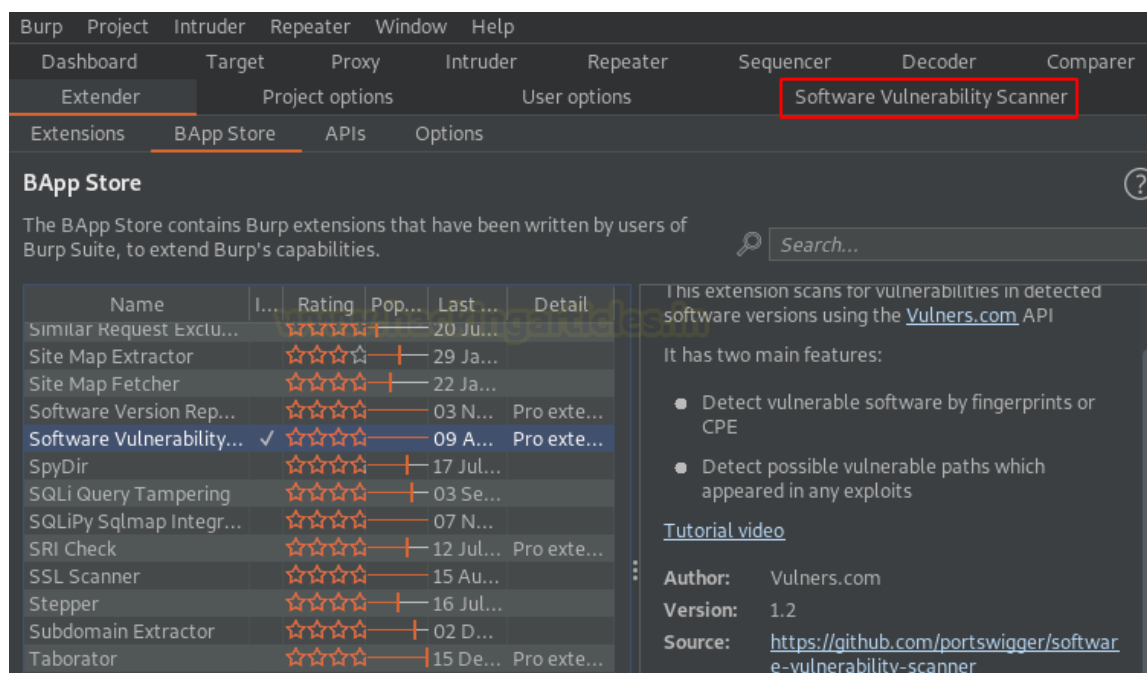
Search...

Name	Installed	Rating	Popularity	Last updated	Detail
Similar Request Excluder		☆☆☆☆☆	+	20 Jun 2018	
Site Map Extractor		☆☆☆☆☆	+	29 Jan 2020	
Site Map Fetcher		☆☆☆☆☆	+	22 Jan 2015	
Software Version Reporter		☆☆☆☆☆	+	03 Nov 2020	Pro extension
<b>Software Vulnerability Scanner</b>		☆☆☆☆☆	+	09 Apr 2019	Pro extension
SpyDir		☆☆☆☆☆	+	17 Jul 2018	
SQLi Query Tampering		☆☆☆☆☆	+	03 Sep 2020	
SQLiPy Sqlmap Integration		☆☆☆☆☆	+	07 Nov 2019	
SRI Check		☆☆☆☆☆	+	12 Jul 2019	Pro extension
SSL Scanner		☆☆☆☆☆	+	15 Aug 2018	
Stepper		☆☆☆☆☆	+	16 Jul 2020	
Subdomain Extractor		☆☆☆☆☆	+	02 Dec 2019	
Taborator		☆☆☆☆☆	+	15 Dec 2020	Pro extension
Target Redirector		☆☆☆☆☆	+	04 Apr 2018	
ThreadFix		☆☆☆☆☆	+	25 Jan 2017	Pro extension
Timeinator, Time Based Attac...		☆☆☆☆☆	+	09 Nov 2020	

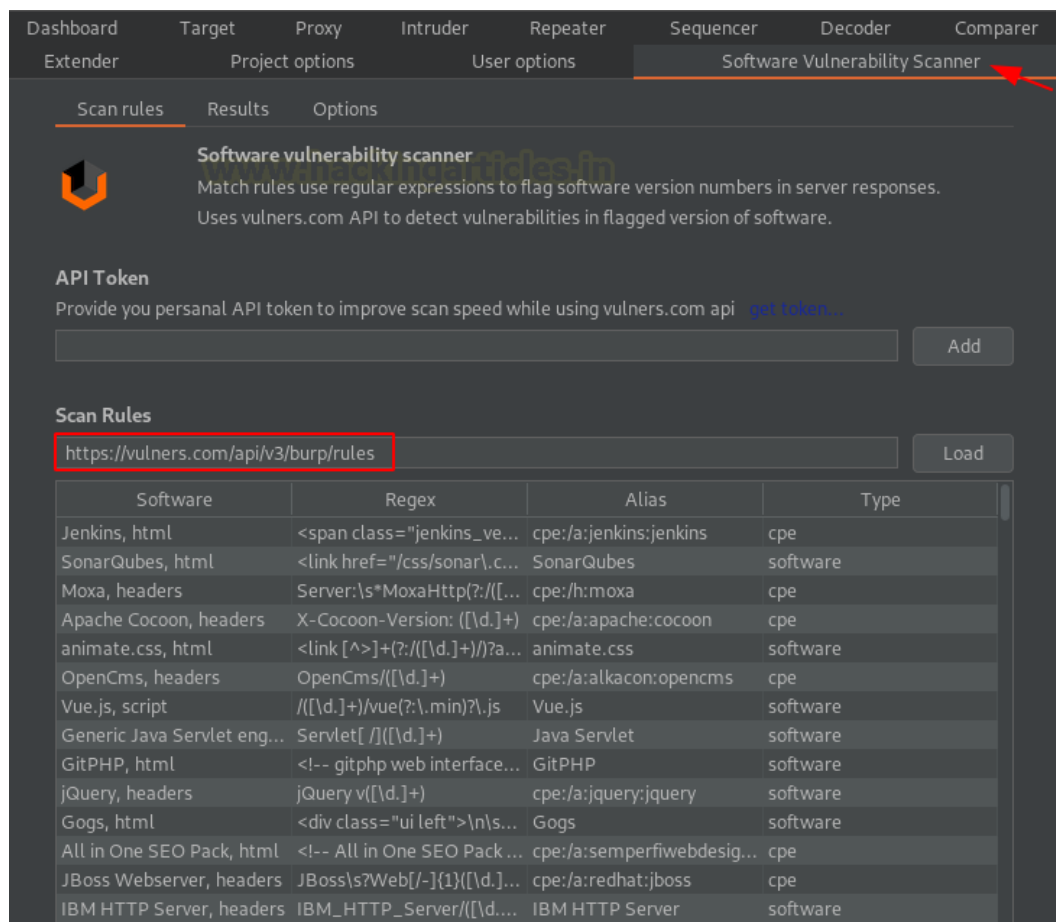
As soon as we find that, we'll tune over to the right section and will hit the **Install button** to make it a part of the Burp Scanner.



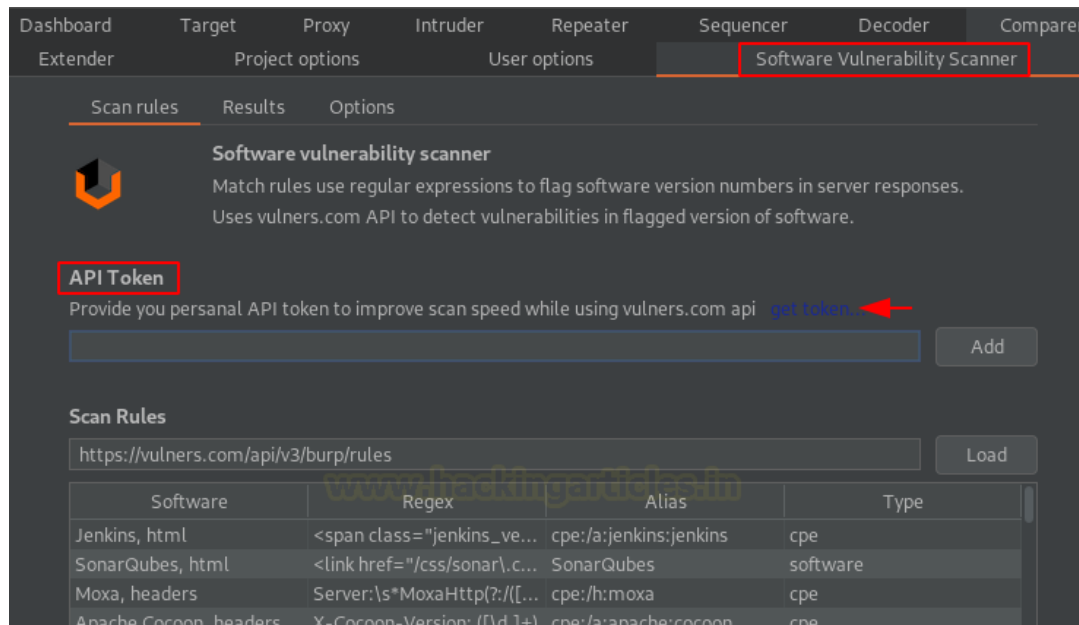
And within a few minutes, we'll get its tab positioned into the top panel as **"Software Vulnerability Scanner"**, let's explore it first.



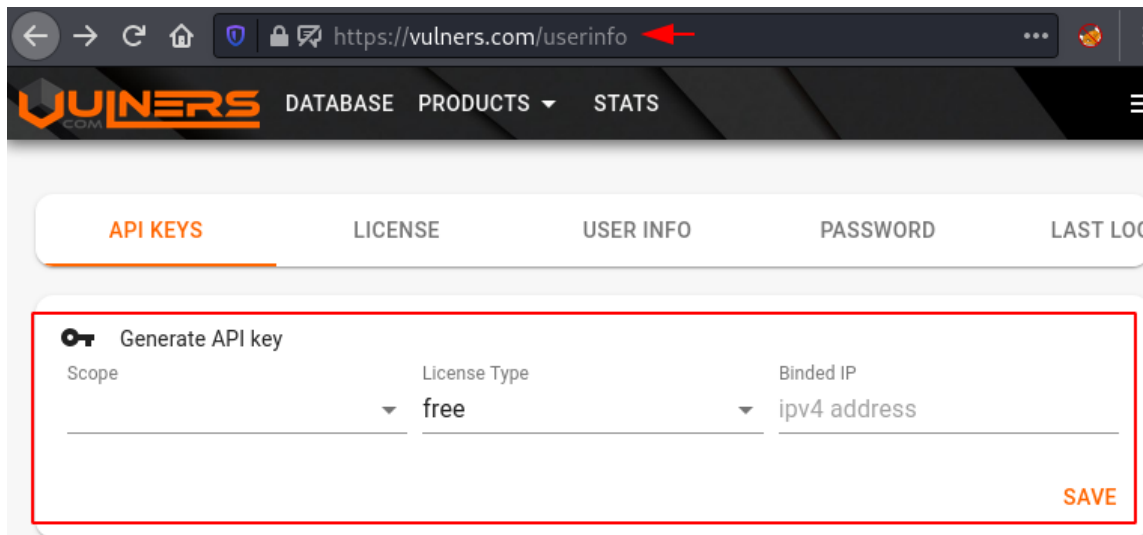
Navigating to the plugin's window, over at the **Scan Rules** tab, we're having two segregated sections one for the **API** and the other for the **Scan Rules**. However, the rule book for the scanning part had been loaded by default, thereby we just need to set the API key.



Although this plugin is good to go without the API key value, there it will simply try to match the vulnerable path with the database. But if you want to embed your key, you can hit the **get token..** section and **register for an API key** for free.

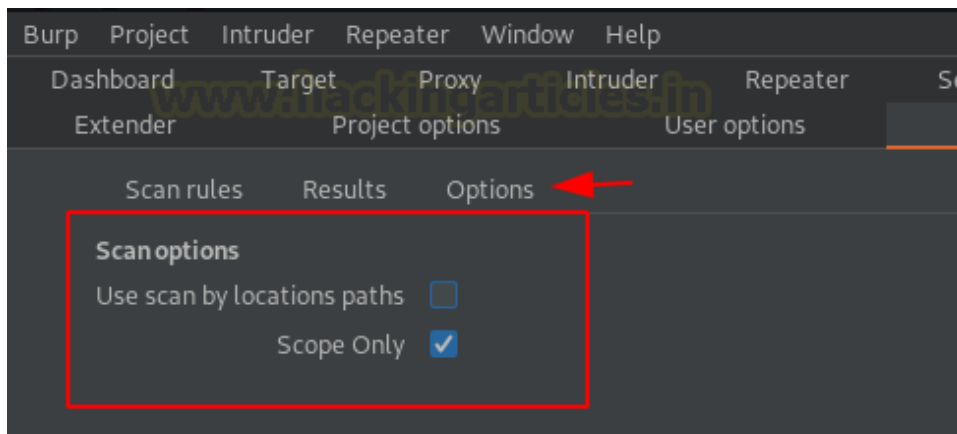


As soon as we hit the button, we got redirected to the vulners.com user info page. Login and fill the input fields to generate the API key.



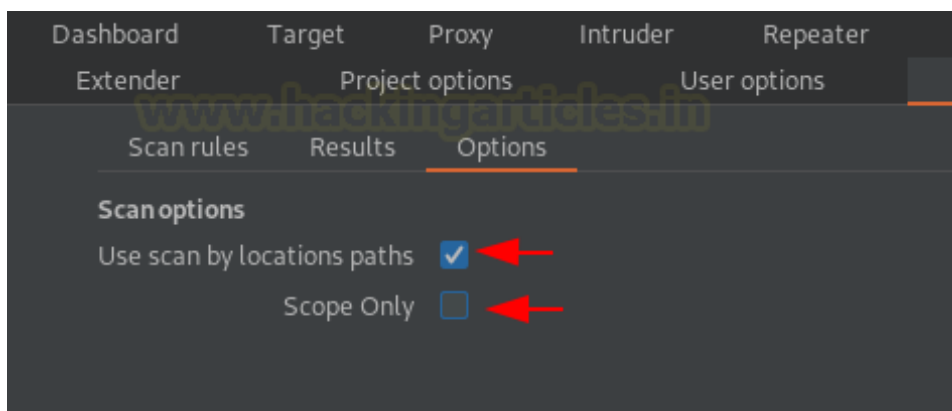
The screenshot shows the vulners.com user info page. The browser address bar displays <https://vulners.com/userinfo>. The page has a navigation bar with links for DATABASE, PRODUCTS, and STATS. Below this is a tabbed interface with tabs for API KEYS, LICENSE, USER INFO, PASSWORD, and LAST LOG. The API KEYS tab is selected. The form contains a 'Generate API key' section with a 'Scope' dropdown menu, a 'License Type' dropdown menu set to 'free', and a 'Binded IP' dropdown menu set to 'ipv4 address'. A red box highlights the entire form area, and a red arrow points to the 'Generate API key' button. A 'SAVE' button is located at the bottom right of the form.

However, for this section, we'll be working without the API key. But we'll enhance its scanning capabilities by **customizing it** over into the **options tab**.



The screenshot shows the Burp Suite Options tab. The 'Options' tab is selected, and a red arrow points to it. The 'Scan options' section is highlighted with a red box. It contains two checkboxes: 'Use scan by locations paths' (unchecked) and 'Scope Only' (checked).

Let's unflag the checkbox of **Scope Only** and hit the **Use scan by location paths** option. Although flagging this feature might give us some **false positives** as it will take keywords from the vulnerable application and then match them with the keywords present at the vulners.com's database.



The screenshot shows the Burp Suite Options tab with the 'Options' tab selected. The 'Scan options' section is highlighted with a red box. The 'Use scan by locations paths' checkbox is now checked, and the 'Scope Only' checkbox is now unchecked. Red arrows point to both checkboxes.

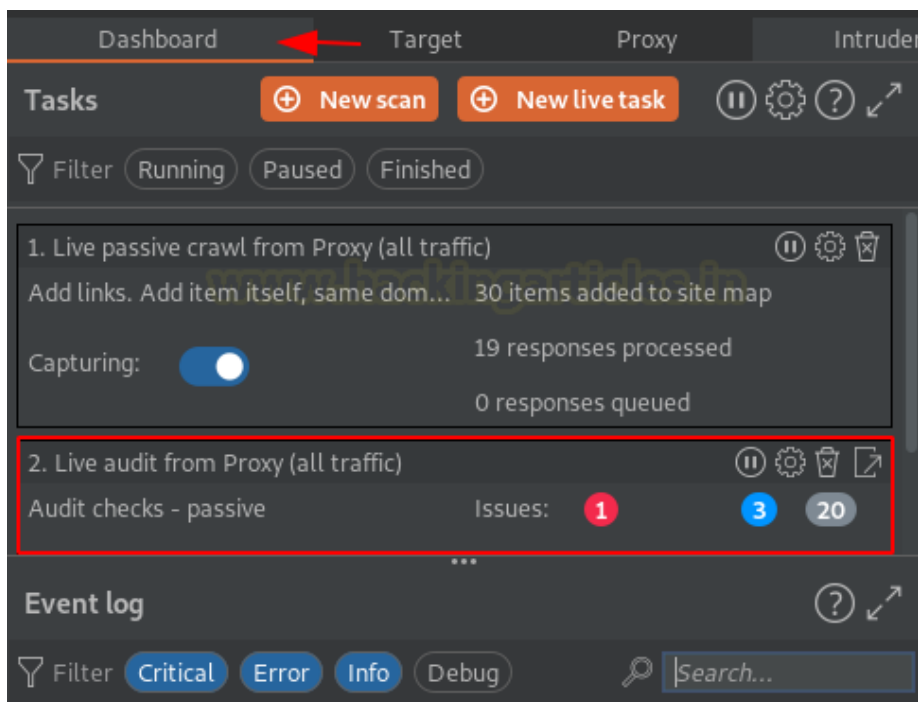


## Fingerprinting the installed software

Once done with the configuration, we'll thus **turn our browser's proxy** and will surf **testphp.vulnweb.com**. As soon as the web page boots up, we'll roam around to generate some traffic.

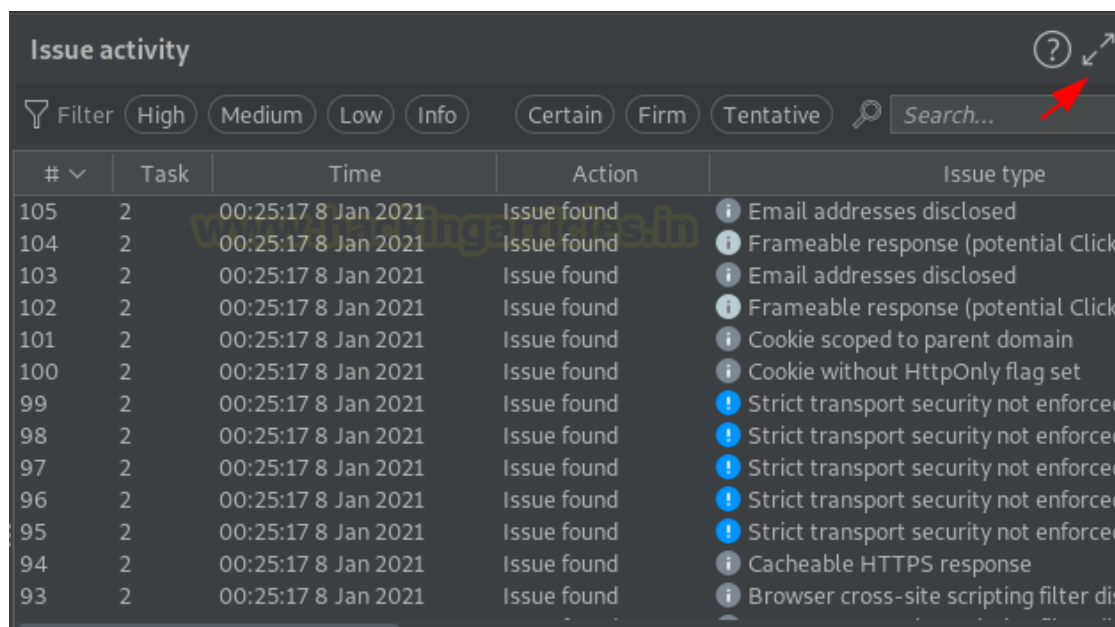


Enough roaming!! Let's get back to our burp suite monitor and will switch to the **dashboard** tab there. From the below image, we can see that the burp scanner was on **Live Audit**, i.e. whatever we did or surfed, it got captured and was shared with the burp scanner.



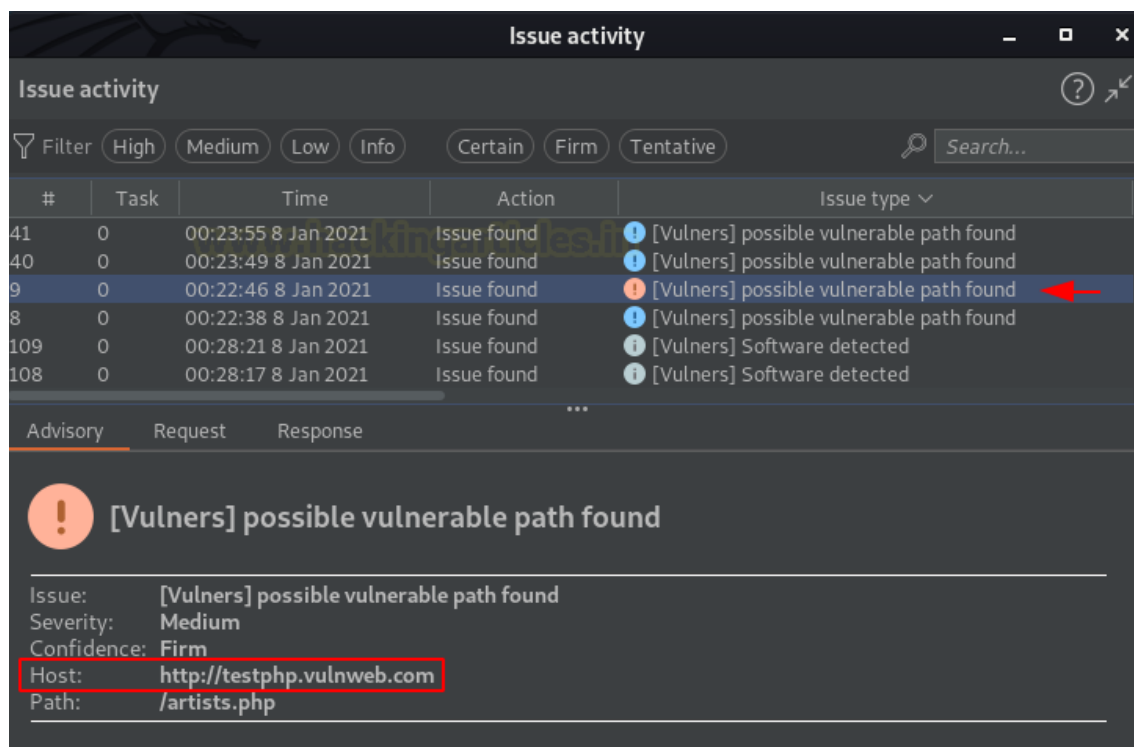


But what about the **Issue Activities**, let's explore it and check what it is having for us.



#	Task	Time	Action	Issue type
105	2	00:25:17 8 Jan 2021	Issue found	Email addresses disclosed
104	2	00:25:17 8 Jan 2021	Issue found	Frameable response (potential Click
103	2	00:25:17 8 Jan 2021	Issue found	Email addresses disclosed
102	2	00:25:17 8 Jan 2021	Issue found	Frameable response (potential Click
101	2	00:25:17 8 Jan 2021	Issue found	Cookie scoped to parent domain
100	2	00:25:17 8 Jan 2021	Issue found	Cookie without HttpOnly flag set
99	2	00:25:17 8 Jan 2021	Issue found	Strict transport security not enforce
98	2	00:25:17 8 Jan 2021	Issue found	Strict transport security not enforce
97	2	00:25:17 8 Jan 2021	Issue found	Strict transport security not enforce
96	2	00:25:17 8 Jan 2021	Issue found	Strict transport security not enforce
95	2	00:25:17 8 Jan 2021	Issue found	Strict transport security not enforce
94	2	00:25:17 8 Jan 2021	Issue found	Cacheable HTTPS response
93	2	00:25:17 8 Jan 2021	Issue found	Browser cross-site scripting filter di

As soon as the extend window opens, we'll sort its contents with the **Issue type**. From the below image we can see that the scanner found something stating "[vulners] possible vulnerable path found". Seems like our configuration is working perfectly.



#	Task	Time	Action	Issue type
41	0	00:23:55 8 Jan 2021	Issue found	[Vulners] possible vulnerable path found
40	0	00:23:49 8 Jan 2021	Issue found	[Vulners] possible vulnerable path found
9	0	00:22:46 8 Jan 2021	Issue found	[Vulners] possible vulnerable path found
8	0	00:22:38 8 Jan 2021	Issue found	[Vulners] possible vulnerable path found
109	0	00:28:21 8 Jan 2021	Issue found	[Vulners] Software detected
108	0	00:28:17 8 Jan 2021	Issue found	[Vulners] Software detected

**[Vulners] possible vulnerable path found**

Issue: [Vulners] possible vulnerable path found

Severity: Medium

Confidence: Firm

Host: http://testphp.vulnweb.com

Path: /artists.php

Let's explore this issue a bit deeper, carrying up from the **Issue details**, it dumps about a number of **exploits that use the same path** and are into the vulners database.

Issue: [Vulners] possible vulnerable path found  
Severity: Medium  
Confidence: Firm  
Host: http://testphp.vulnweb.com  
Path: /artists.php

**Note:** This issue was generated by a Burp extension.

#### Issue detail

! All found vulnerabilities have to be checked The following vulnerabilities for path **/artists.php** found:

- [EDB-ID:14948](#) - 4.3 **Exploit** - festos CMS 2.3b - Multiple Vulnerabilities  
MOAUB #9 - FestOS CMS 2.3b Multiple Remote Vulnerabilities. CVE-2010-4893. Webapps exploit for php platform
- [EXPLOITPACK:3374B8292767931C7AA675C7B5823E83](#) - **Exploit** - festos CMS 2.3b - Multiple Vulnerabilities  
festos CMS 2.3b - Multiple Vulnerabilities
- [1337DAY-ID-14043](#) - **Exploit** - FestOS CMS 2.3b Multiple Remote Vulnerabilities  
Exploit for php platform in category web applications
- [SSV:69806](#) - **Exploit** - festos cms 2.3b Multiple Vulnerabilities  
No description provided by source.
- [PACKETSTORM:151064](#) - **Exploit** - Ampache 3.8.6 Cross Site Scripting
- [1337DAY-ID-31907](#) - **Exploit** - Ampache 3.8.6 Cross Site Scripting Vulnerability  
Exploit for php platform in category web applications
- [PACKETSTORM:93713](#) - **Exploit** - Month Of Aabysssec Undisclosed Bugs - FestOS CMS 2.3b

Let's check the **PacketStorm** by hitting the "**Exploit**" button aligned with that. And as soon as we do so, we got redirected to the **vulners.com** website with the exploit data over it.

← → ↻ 🏠 🔒 https://vulners.com/packetstorm/PACKETSTORM:151064

**VULNERS** DATABASE PRODUCTS ▾ PRICING STATS TEAM BLOG

**packet storm** Ampache 3.8.6 Cross Site Scripting  
2019-01-09 00:00:00

**ID** PACKETSTORM:151064  
**Type** packetstorm  
**Reporter** Zekvan Arslan  
**Modified** 2019-01-09 00:00:00

**Description**

Multiple Reflected Cross-site Scripting Vulnerabilities in Ampache 3.8.6

As we tried to search **artistsits.php**, we got the path value similar to the one we had over at testphp.vulnweb.com.

## Description

```
`Multiple Reflected Cross-site Scripting Vulnerabilities in Ampache 3.8.6  COPY  DOWN

Information
-----

Advisory by Netsparker
Name: Multiple Reflected Cross-site Scripting in Ampache 3.8.6
Affected Software: Ampache
Affected Versions: 3.8.6
Homepage: http://ampache.org
Vulnerability: Reflected Cross-site Scripting
Severity: Medium
Status: Not Fixed
CVSS Score (3.0): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
Netsparker Advisory Reference: NS-18-046

Technical Details
-----

URL: http://{DOMAIN}/{PATH-OF-AMPACHE}/arts.php?action=find_art&object_type=live_stream&object_id=
Parameter Type: GET
Parameter Name: mbid
Attack Pattern: '"--></style></scRipt><scRipt>alert(0x031B4B)</scRipt>'

URL: http://{DOMAIN}/{PATH-OF-AMPACHE}/artists.php?action=show_missing&mbid='+alert(0x003D85)+'
Parameter Type: GET
Parameter Name: mbid
```

However, you can analyze the other listed exploits too much to have a better understanding of how vulnerable the software version could be.

Once done, we'll further move back to the **Software Vulnerability Scanner** tab at our burpsuite and will switch to the **Results** section there, which contains the **vulnerable software versions aligned with their names and hosts** and the **Possible vulnerable software uses specific paths**.

**Software Vulnerability Scanner**

Scan rules **Results** Options

**Vulnerable Software**

☐ Show only vulnerable software

Domain	Name	Version	CVSS Score	Vulnerabilit...
x.clearbitjs.com	jQuery, script			
www.googletagmanager.com	jQuery, headers	1.9.1		
www.acunetix.com	jQuery, headers	3.4.1		
www.acunetix.com	jQuery, script			
www.acunetix.com	Yeast SEO, html	15.5		
vulners.com	Django, html			
vulners.com	jQuery, script			
vulners.com	Linux, headers	vulnerability		
vulners.com	Linux, headers	servers		
vulners.com	Firebase, script	3.6.6		

Clear

**Possible vulnerable software uses specific paths**

Domain	path	CVSS Score	Vulnerabilities
testphp.vulnweb.com	/AJAX/styles.css	0.0	[PACKETSTORM:150886]
testphp.vulnweb.com	/artists.php	4.3	[EDB-ID:14948, EXPLOI...]
www.googletagmanager...	/gtm.js	0.0	[VULNERLAB:1969]

## Retire.js

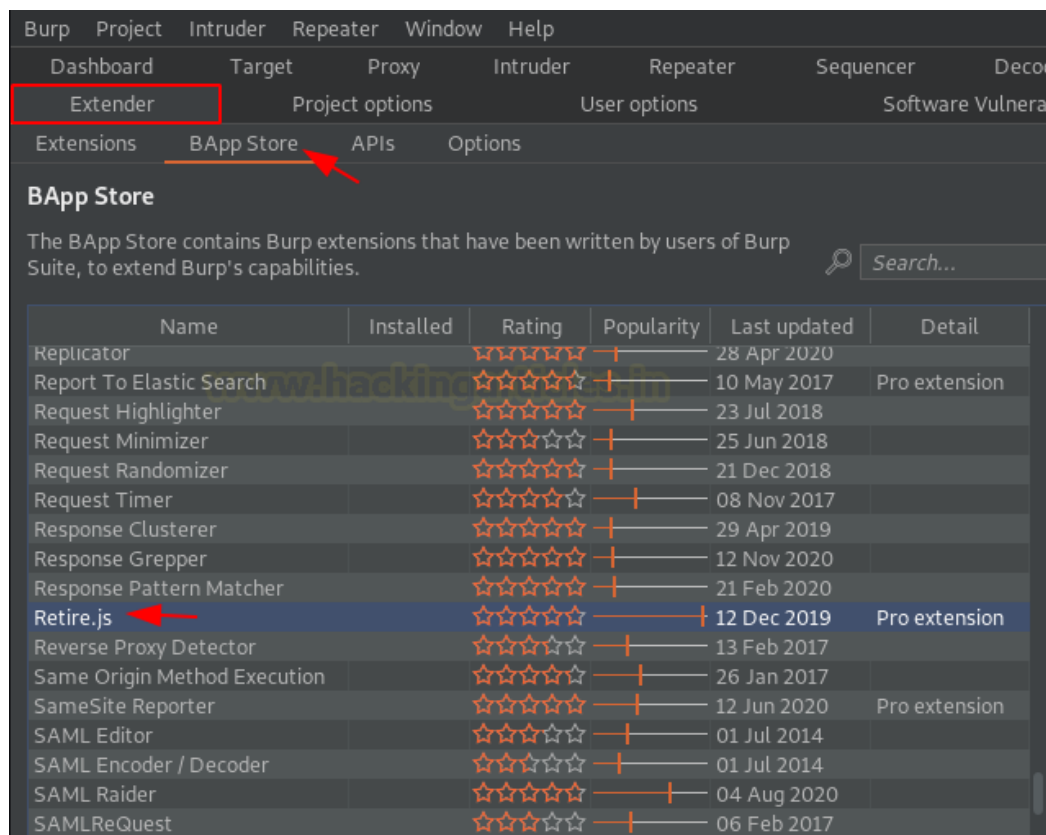
Dynamic web application carries several libraries within themselves whether it's React, Angular, or JQuery, but what about their analysis part like how we could identify whether the application we're testing is having an outdated version of the JavaScript packages or not.

Thereby for the analysis part, we're having one more amazing burp plugin i.e. **Retire.js**, its name itself reveals its work as **"Retire JavaScript"** i.e. it identifies the retired or the outdated versions (vulnerable) of javascript libraries that the application is using.

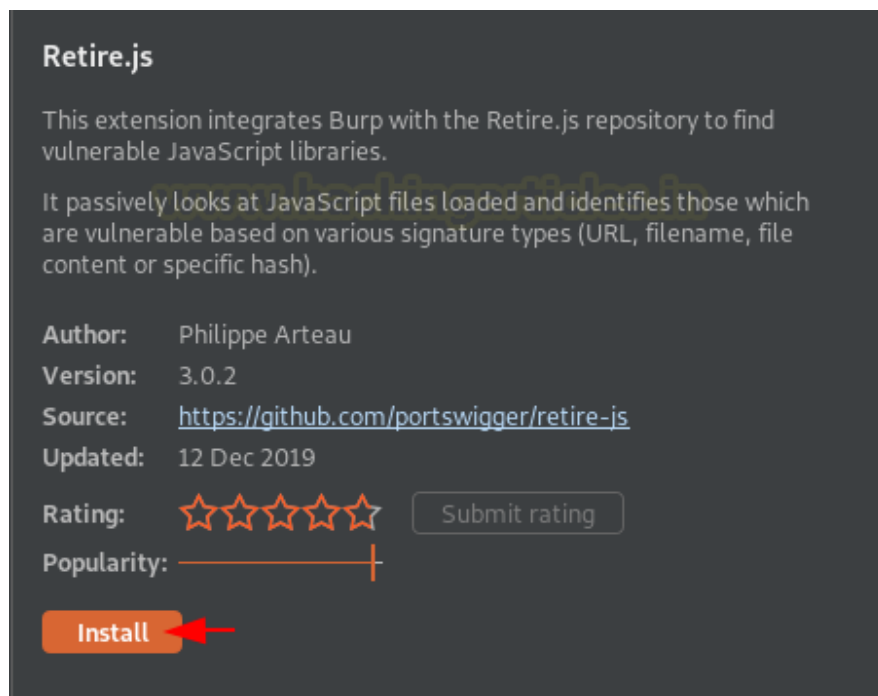
Before involving more in the theory section, let's jump directly to its installation. However, you can learn more about it from [here](#)

## Setting up the Plugin

Back into the bApp store and we'll search for the keyword **"R"**, and there the one with the highest popularity bar is our plugin.

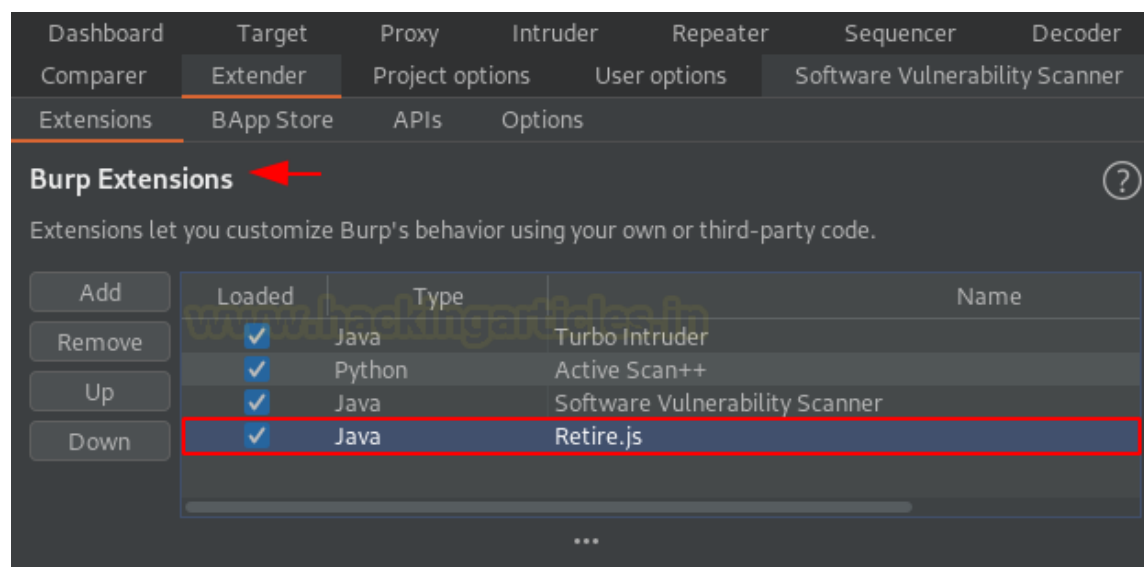


However, due to its popularity and its reviews Burp Suite had made it available only for the **Professional Edition** users. So, let's hit the **Install** button on the right-side and initiate the installation.



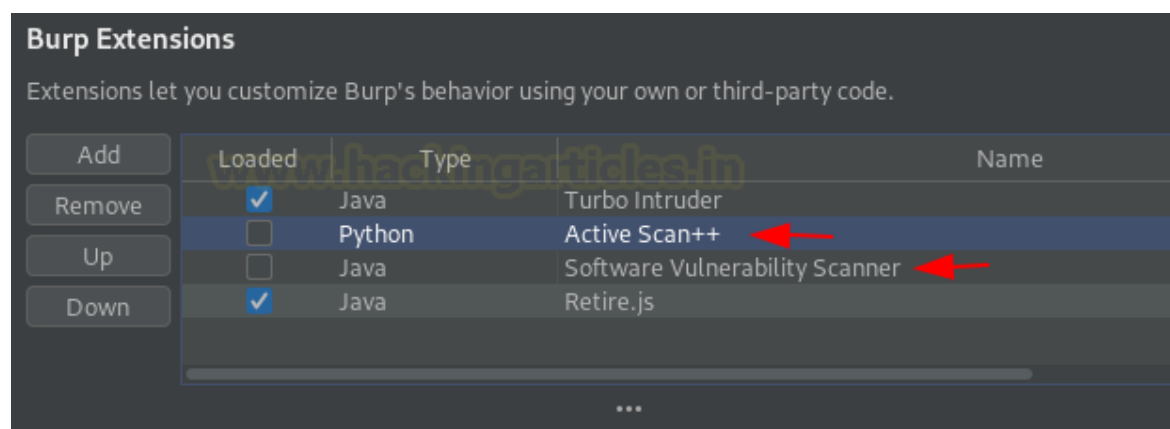
Once done with the installation part, let's check it over in the top panel. But wait!! Where it is?

Similar to Active scan++, as soon as the plugin got downloaded, it got embedded up with the Burp Scanner, but we can check its existence by switching to the **Extensions section** at the **Extender tab**.

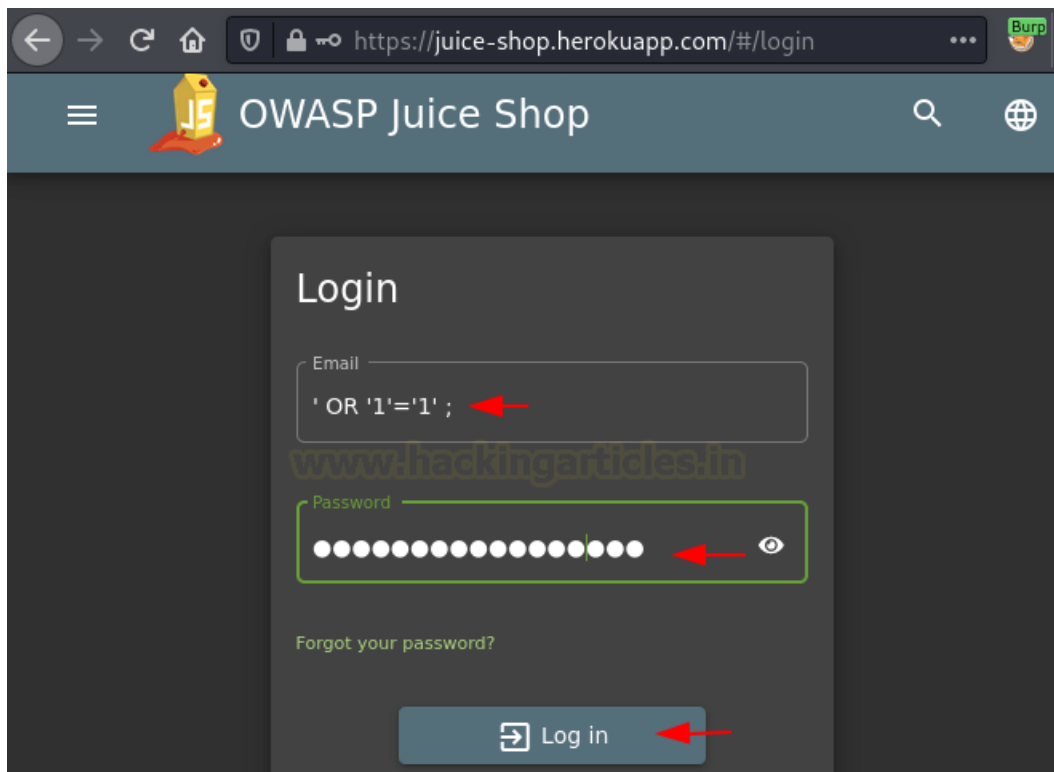


## Dumping the Outdated JavaScript Libraries

Once the plugin got configured, we just need to initiate the scanner and within a few minutes, we'll get the output. But to capture a clearer result, let's disable the other scanner plugins and we'll only flag **Retire.js**



Time to surf a vulnerable application. So, for time being, let's make it the **OWASP Juice Shop** and we'll bypass the application's login with '**OR '1'='1'**' ;

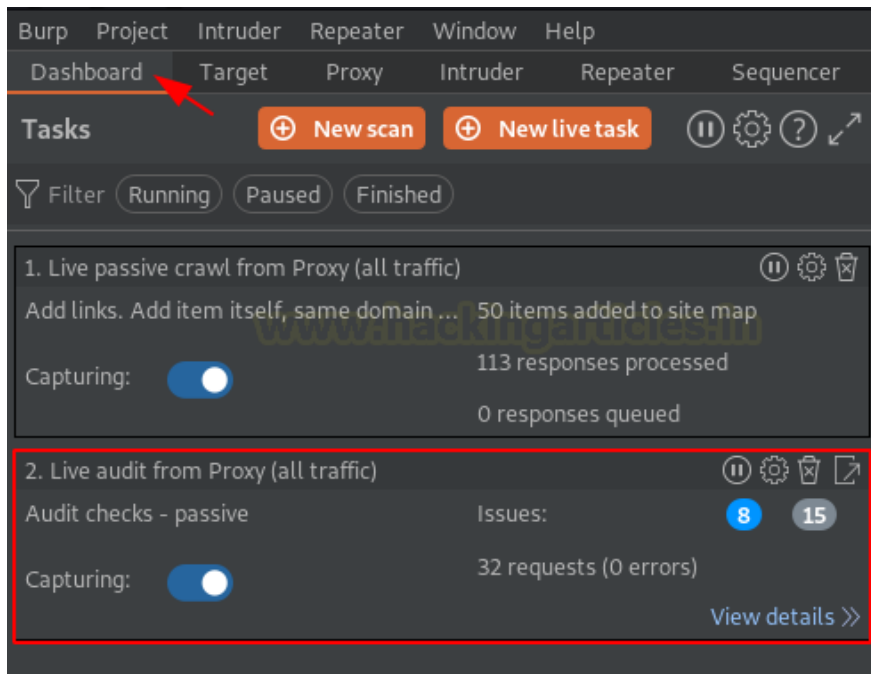


As we did at the testphp.vulnweb.com, we'll do the same here. Yes, **surf the website** with the **browser proxy ON** to generate traffic.

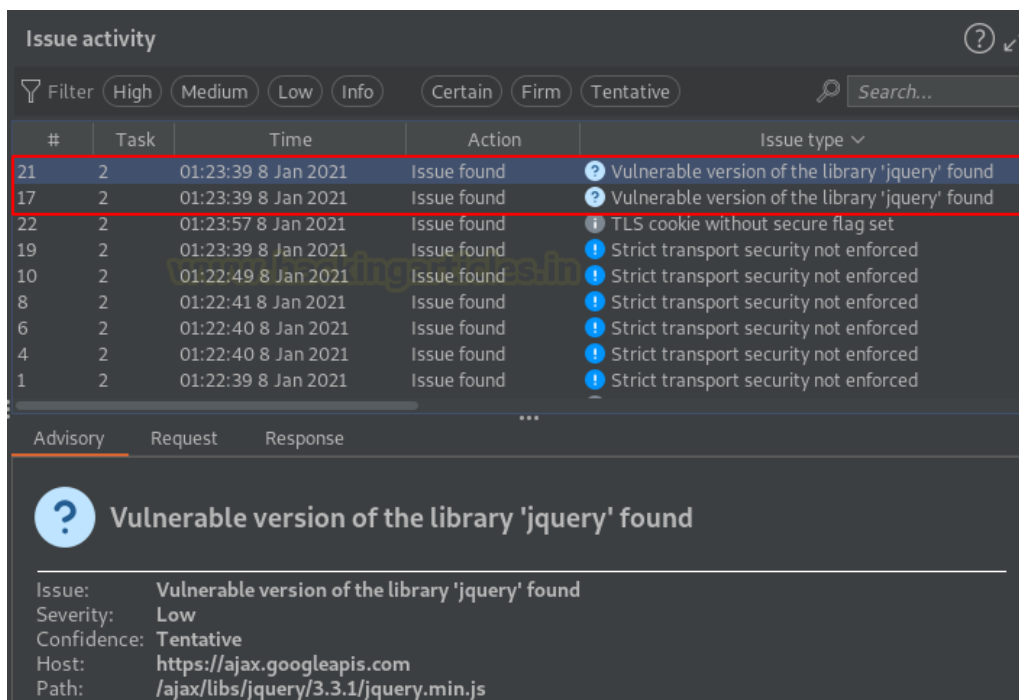


After a few page visits, let's move back to the burp suite dashboard and will check the **Tasks tab** there. From the below image, you can see that we got about **32 Requests** in the **Live Proxy Audit**.





Let's check them out in the **Issue Activity** tab. Sorting the contents as per the **Issue Type** we for the jquery vulnerabilities lined up there.



Turning to the **Advisory** section, we can see that Retire.js has **dumped a vulnerable jquery library** that was used over the profile web page of the application. However, we can search the exploitation of this jquery library on **google**, and then we're good to go.

Advisory Request Response

## Vulnerable version of the library 'jquery' found

Issue: Vulnerable version of the library 'jquery' found  
Severity: Low  
Confidence: Tentative  
Host: <https://juice-shop.herokuapp.com>  
Path: /profile

**Note:** This issue was generated by the Burp extension: Retire.js.

**Issue detail**

The library **jquery** version **3.3.1** has known security issues.  
For more information, visit those websites:

- <https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
- <https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b>

**Affected versions**

The vulnerability is affecting all versions prior **3.4.0** (between \* and **3.4.0**)

At last, let's check the **Response** tab to analyze how the plugin detected the vulnerable jquery version. So, from the below image, you can see that as soon as we hit the **right-arrow** button, we got the vulnerable version highlighted there, as the developer didn't notice that the jquery version is passing over with the HTML code.

Advisory Request Response

Pretty Raw Render \n Actions

```
OWASP Juice Shop
</title>
<meta charset="utf-8">
<meta name="description" content="">
<meta name="keywords" content="">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel="icon" type="image/x-icon" href="./assets/public/favicon.js.ico">
<link rel="stylesheet" href="https://code.getmdl.io/1.3.0/material.min.css">
<link rel="stylesheet" href="https://fonts.googleapis.com/icon?family=Material+Icons">
<link rel="stylesheet" href="./assets/public/css/userProfile.css" type="text/css">
<link rel="stylesheet" href="http://fonts.googleapis.com/css?family=Roboto:300,400,500,700,900">
<script src="//ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">
</script>
<script src="https://code.getmdl.io/1.3.0/material.min.js">
</script>
<style>
.mdl-textfield__input{
  border-bottom:1pxsolid#FFFFFF!important;
  font-size:13px!important;
}
</style></head><bodystyle="background:#303030;color:#FFFFFF;"><divclass="mdl-w-back"></div><a href="#"></a></div></body></html>
```

17  
18  
19

1 highlight

# JOIN OUR TRAINING PROGRAMS

