

# **Sri Lanka Institute of Information Technology**



## **Assignment – Web Audit**

<b>Student ID</b>	<b>Name</b>
IT19300788	C.V Wanigathunga

Module  
**Web Security – IE2062**


**23/10/2020**

## **Methodology**

- Adobe domain I selected from hacker one site for my web audit. Adobe inc. is an international American technology corporation for computers. Based in Delaware and located in San Jose , California, it has traditionally focused on the development of software products for entertainment and innovation, with a more recent foray into applications for digital marketing.
- In our search to provide a safe and secure environment for Adobe 's customers, Adobe recognizes that the security community is a force multiplier. To that end, security researchers contribute and aspire to have the best possible experience of vulnerability disclosure.

## **Eligible Vulnerabilities**

We encourage the coordinated disclosure of the following eligible web application vulnerabilities:

- Cross-site scripting
- Cross-site request forgery in a privileged context
- Server-side code execution
- Authentication or authorization flaws
- Injection Vulnerabilities
- Directory Traversal
- Information Disclosure
- Significant Security Misconfiguration (please follow [best practice](#)  when reporting subdomain takeovers)

To receive credit, you must be the first reporter of a vulnerability. When submitting a vulnerability, please provide concise steps to reproduce that are easily understood.

## **Program Exclusions**

While we encourage any submission affecting the security of an Adobe web property, unless evidence is provided demonstrating exploitability, the following examples are excluded from this program:

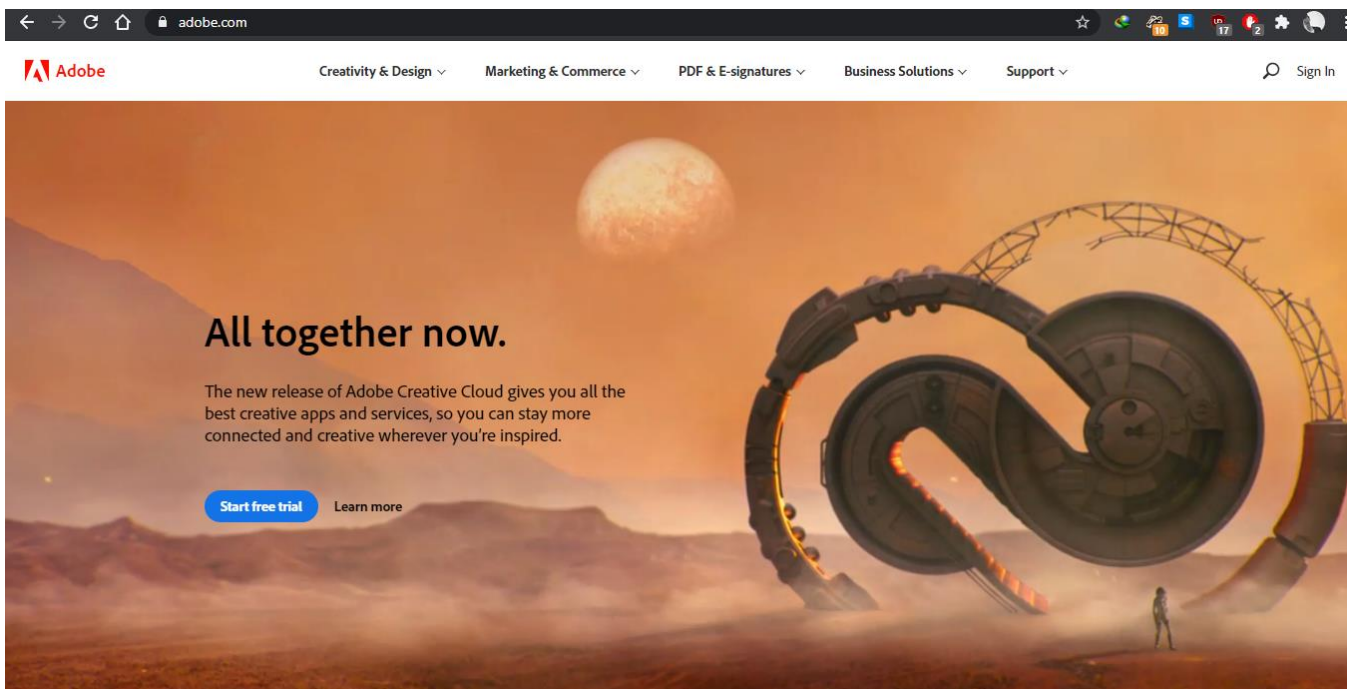
- Content spoofing / text injection
- Self-XSS [to be valid, cross-site scripting issues must be exploitable via reflected, stored or DOM-based attacks]
- Logout and other instances of low-severity Cross-Site Request Forgery
- Cross-site tracing (XST)
- Open redirects with low security impact (exceptions are those cases where the impact is higher such as stealing OAuth tokens)
- Missing HTTP security headers
- Missing cookie flags on non-sensitive cookies
- Password and account recovery policies, such as reset link expiration or password complexity
- Invalid or missing SPF (Sender Policy Framework) records (Incomplete or missing SPF/DKIM)
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
- SSL/TLS best practices
- Clickjacking/UI redressing with no practical security impact
- Software version disclosure
- Username / email enumeration via Login Page or Forgot Password Page error messages
- Methods to extend product trial periods.

## In Scope Domains

- \*.acrobat.com
- \*.adobe.io
- \*.adobecloud.com
- \*.adobecqms.net
- \*.bizible.com
- \*.marketo.com
- \*.mixamo.com
- \*.omniture.com
- \*.phonegap.com
- \*.tubemogul.com
- \*.typekit.com
- account.adobe.com
- accounts.adobe.com
- acrobat.adobe.com
- acrobatoauth.adobe.com
- adminconsole.adobe.com
- adobeid.services.adobe.com
- adobelogin.com
- adobestock.com
- assets.adobe.com
- auth.services.adobe.com
- behance.net
- campaign.adobe.com
- captivateprime.adobe.com
- cbconnection.adobe.com
- cloud.acrobat.com
- coldfusion.adobe.com
- commerce.adobe.com
- community.adobe.com
- create.adobe.com
- creative.adobe.com
- creativecloud.adobe.com
- documentcloud.adobe.com
- documents.adobe.com
- edex.adobe.com
- exchange.adobe.com
- experience.adobe.com
- experiencecloud.adobe.com
- fonts.adobe.com
- gps.echosign.com
- helpx.adobe.com
- licenses.adobe.com
- licensing.adobe.com
- lightroom.adobe.com
- marketing-assets.adobe.com
- marketing.adobe.com
- mobilemarketing.adobe.com
- partners.adobe.com
- photoshop.com
- platform.adobe.com
- portfolio.adobe.com
- secure.echosign.com
- shop.adobe.com

- spark.adobe.com
- status.adobe.com
- stock.adobe.com
- substance3d.com
- theblog.adobe.com
- xd.adobe.com
- \*.adobe.com
- \*.scene7.com
- \*.tt.omtrdc.net
- \*.adobeconnect.com

## Auditing



## Sublist3r

As a beginning process I want to enumerate subdomains of adobe.com. For enumerate that subdomains I have used “Sublist3r” tool. Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

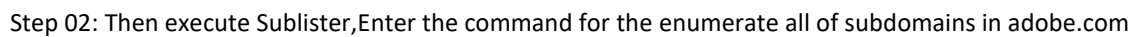
```

Adobe - Vulnerability Disclosure Program | HackerOne - Mozilla Firefox
Parrot Terminal
File Edit View Search Terminal Help
Sorry, try again.
[sudo] password for teddy:
root@parrot:~/home/teddy# apt install sublist3r
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpython-all-dev python-all python-all-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sublist3r
0 upgraded, 1 newly installed, 0 to remove and 1008 not upgraded.
Need to get 617 kB of archives.
After this operation, 1,933 kB of additional disk space will be used.
Get:1 https://indian-apac-mirror.parrot.sh/mirrors/parrot rolling/main amd64 sub
list3r all 1.0+git20200105-0kali1 [617 kB]
9% [1 sublist3r 299 B]

```

Step 01: I'm using Debian based kernel OS. So, I used

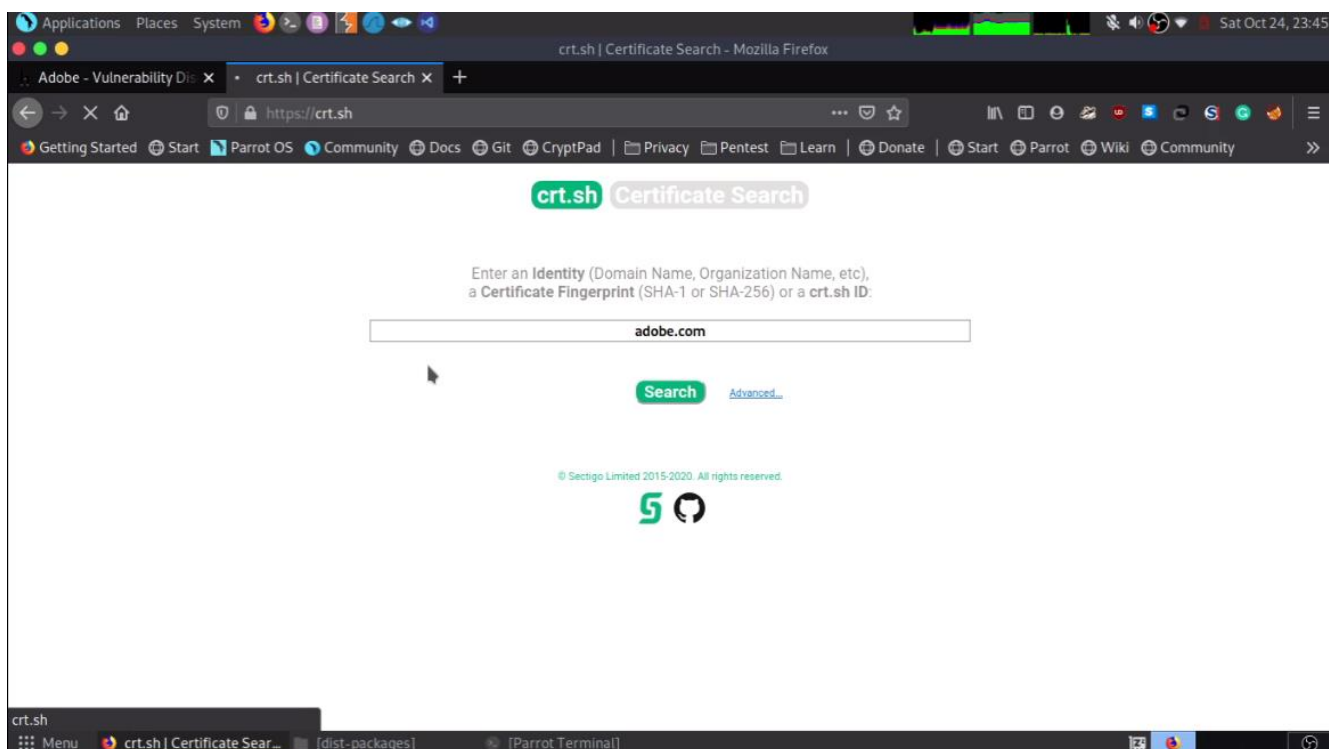
Command to install the Sublist3r tool in my computer. There After I located the Sublist3r.py & execute it in my terminal.



Step 03 : In here I have scanned bunch of sub domains relevant to "adobe.com".So there are 3202 sub domains I've got as result.

Crt.sh (

crt.sh is a web interface to a distributed database called the certificate transparency logs. It shows all of web site certifications and relevant information with that. Crt.sh is certificate fingerprinting tool & easy to use.



I have scan my target domain "adobe.com". I have got domain certifications informations. Certificate ID, Log in time, Defined Date, Common certification Name & issuer's Name.

Applications Places System

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

cr

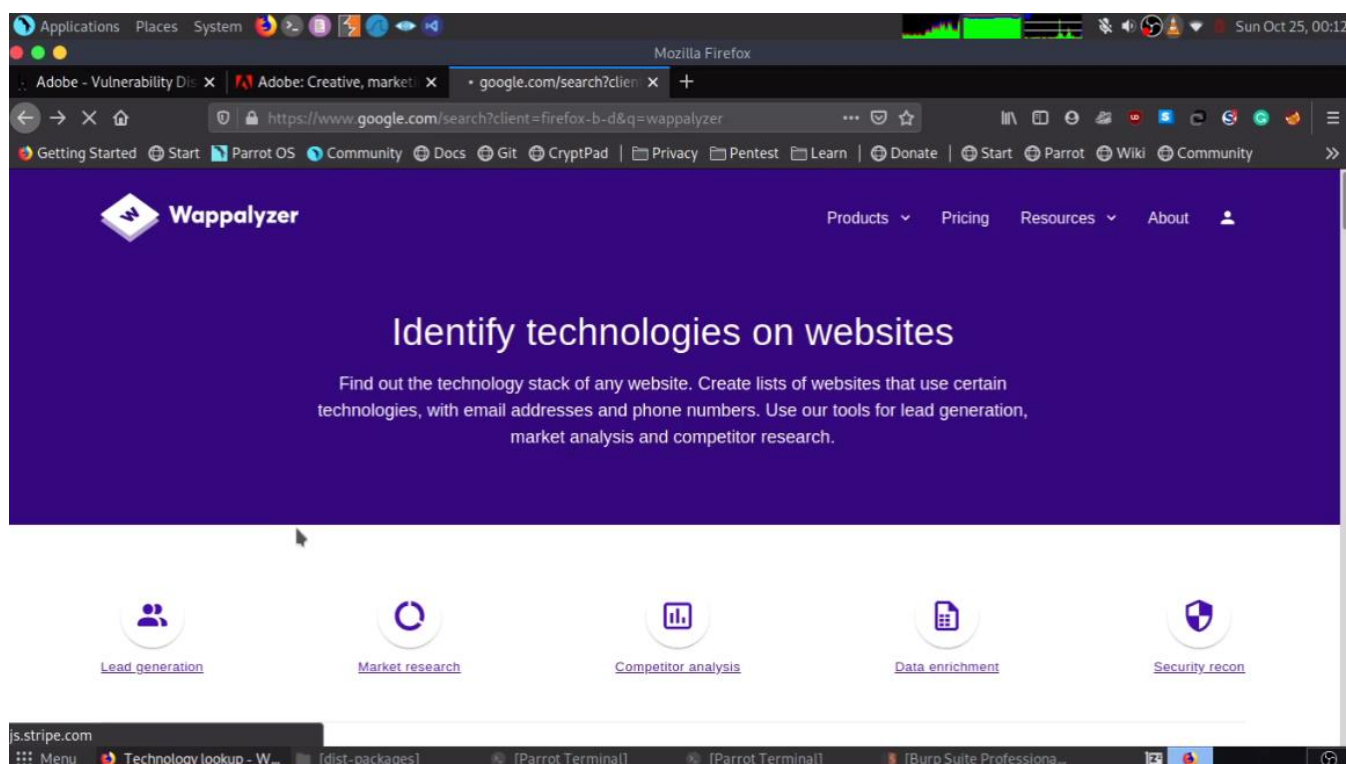
cr

cr

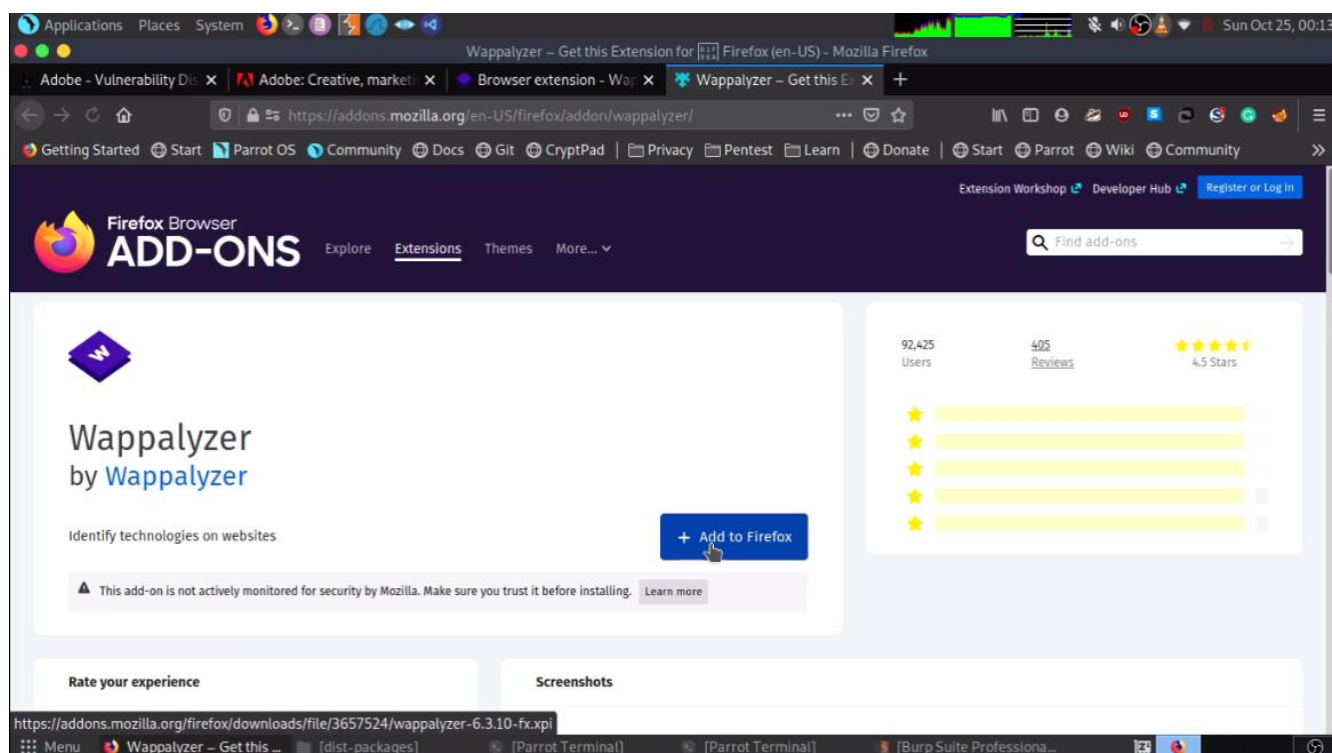
<



Programmatic access to technographic data. The Wappalyzer APIs provide instant access to website technology stacks, contact details and social media profiles. Wappalyzer is a technology profiler that shows you what websites are built with. Find out what CMS a website is using, as well as any framework, ecommerce platform, JavaScript libraries and many more.

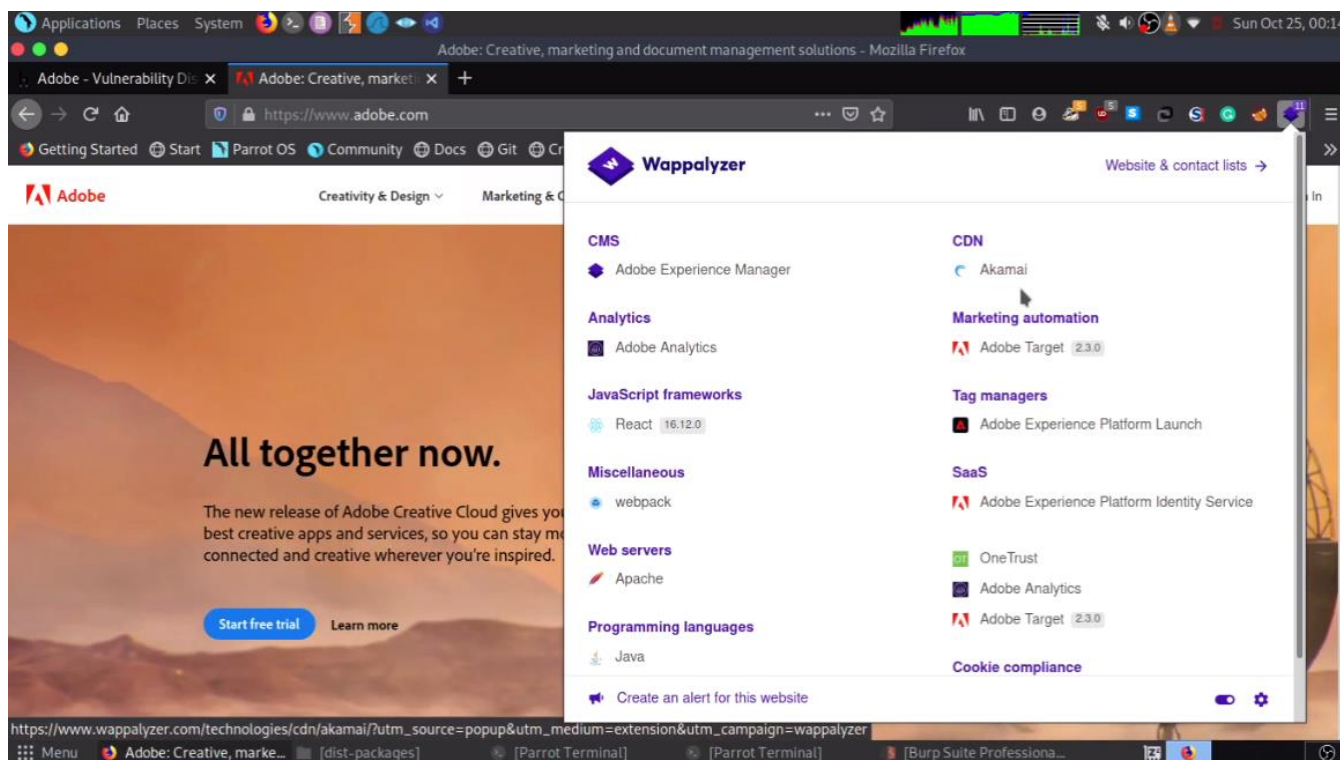


Step 01 : In here I'm using Firefox browser, It's chromium family browser. Wappalyzer extension easily working with chromium family browsers. In here I have install that add on in my web browser (Firefox).



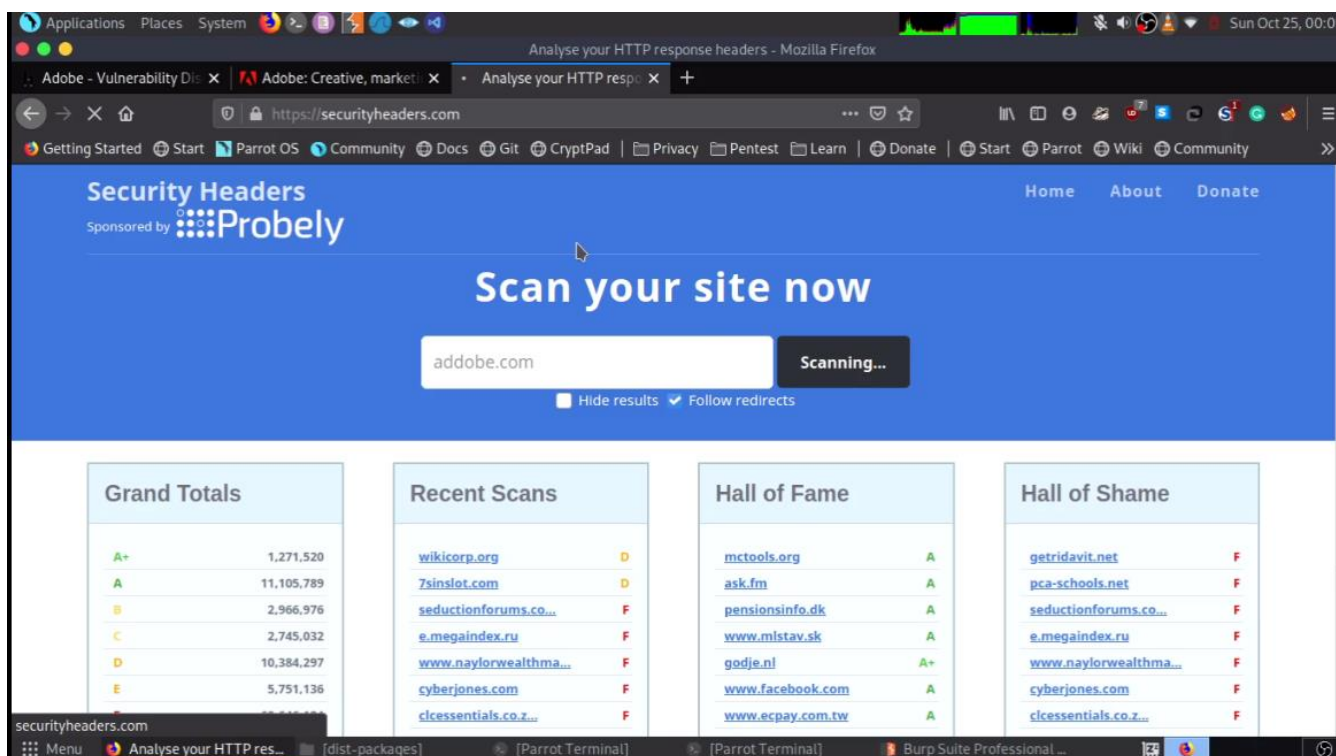


Step 02 : Wappalyzer is easy to use tool. With that I could analyze some point of information relevant to my target domain. Web server information, Designed frameworks, Tag managers, Analytics information & Framework information etc. such information can grab through this Wappalyzer tool.



## Securityheaders.com

Before I enter the website scanning process I want to enumerate security headers using their, So here with securityheaders.com its easy to find & It's doesn't take much time. This is very reliable tool.



There are services out there that will analyze the HTTP response headers of other sites, but I also wanted to add a rating system to the results. The HTTP response headers that this site analyses provide huge levels of protection and it is important that sites deploy them. Hopefully, by providing an easy mechanism to assess them, and further information on how to deploy missing headers, we can drive up the usage of security-based headers across the web.

In here I had got some HTTP header information overall mark adobe.com got "F" for their http headers points. So, that's really interesting point. it will help to figure out there are something wrong with adobe HTTP headers.

Applications Places System

Scan results for adobe.com - Mozilla Firefox

Adobe - Vulnerability Dis: x Adobe: Creative, market: x Scan results for adobe.x +

https://securityheaders.com/?q=adobe.com&followRedirects=on

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donate Start Parrot Wiki Community

adobe.com Scan

Hide results Follow redirects

### Security Report Summary

**F**

Site: <http://www25.adobe.com/?subid1=20201025-0535-17b9-9497-13fd1152fddc> - (Scan again over https)

IP Address: 199.59.242.153

Report Time: 24 Oct 2020 18:35:18 UTC

Headers: **Content-Security-Policy** **X-Frame-Options** **X-Content-Type-Options** **Referrer-Policy** **Permissions-Policy**

Warning: Grade capped at A, please see warnings below.

### Supported By

Probably

Ouch, you should work on your security posture immediately:

Start Now

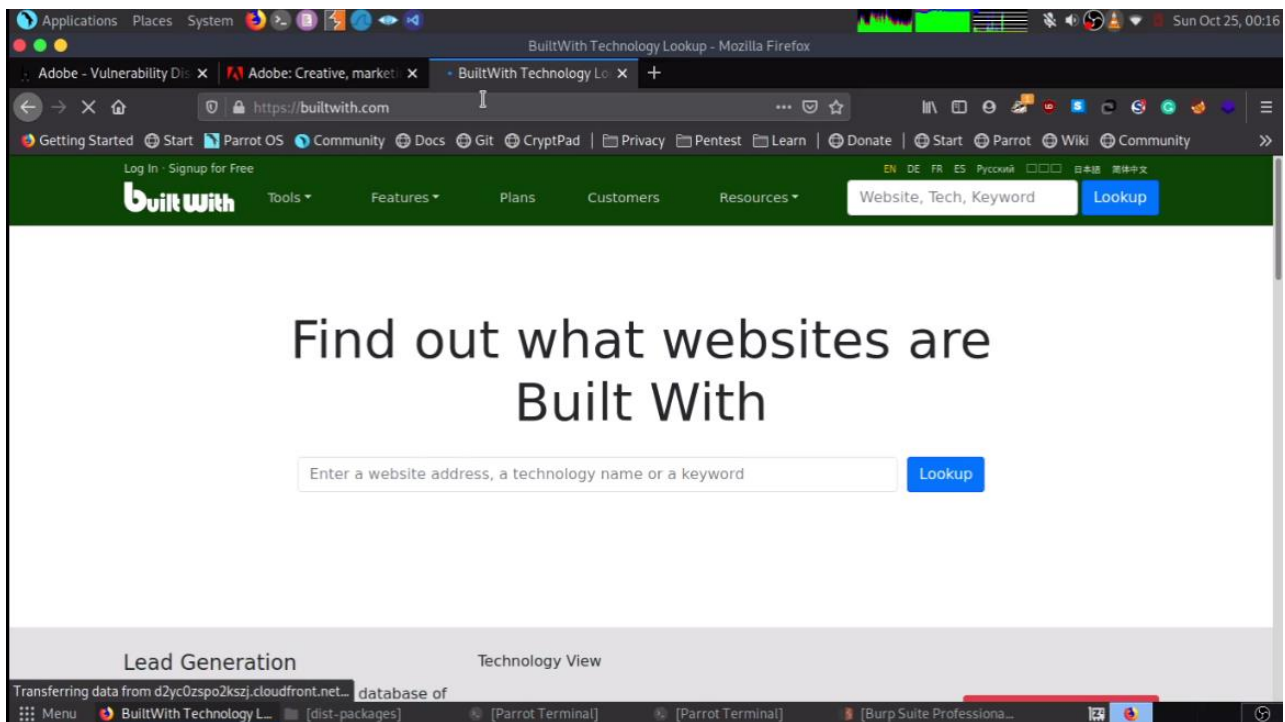
Menu Scan results for adobe... [dist-packages] [Parrot Terminal] [Parrot Terminal] Burp Suite Professional

In here I have gathered some informations relevant to adobe.com HTTP header files. I got some missing header informations. So that's very helpful thing for gaining access part.

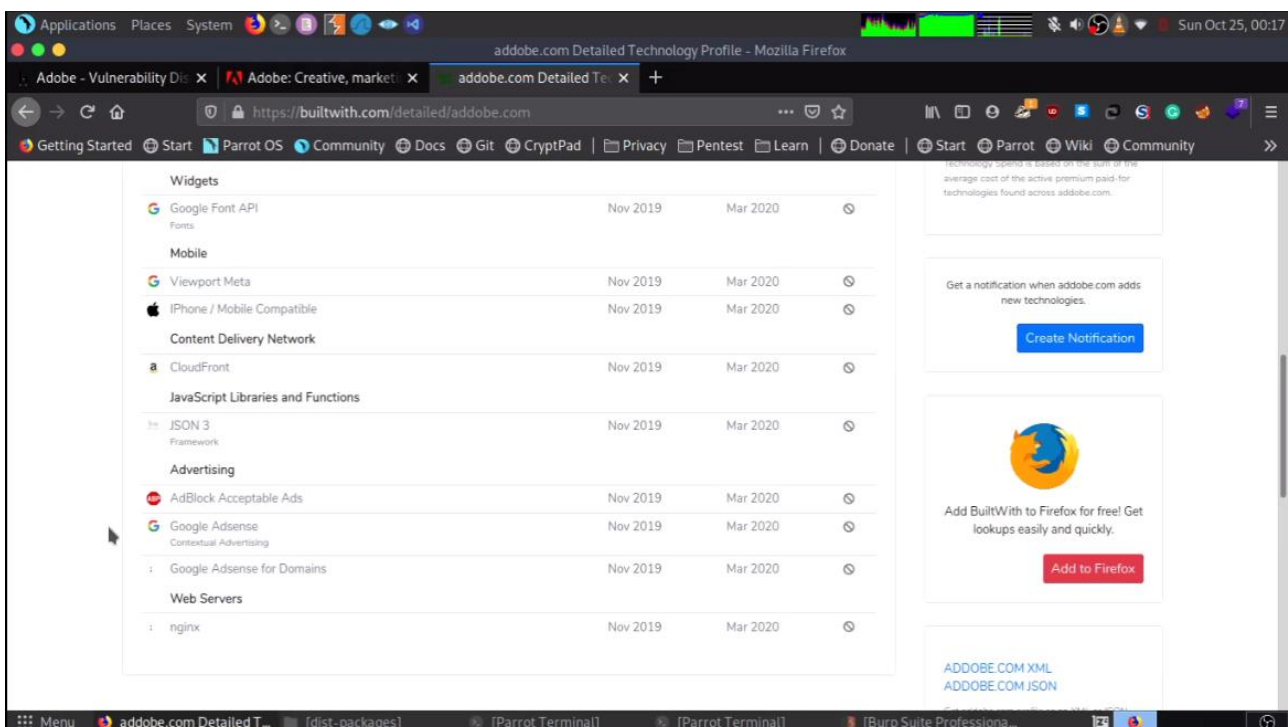
Missing Headers	
<b>Content-Security-Policy</b>	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<b>X-Frame-Options</b>	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
<b>X-Content-Type-Options</b>	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
<b>Referrer-Policy</b>	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<b>Permissions-Policy</b>	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.

## Builtwith.com

“built with” is web technology information profiler tool. Find out what a website is built with. It helps for web domain enumeration part and crawling their information.



In here, I have gathered some sort of information here. Widgets, Meta data, java scripts functions & their web servers etc.

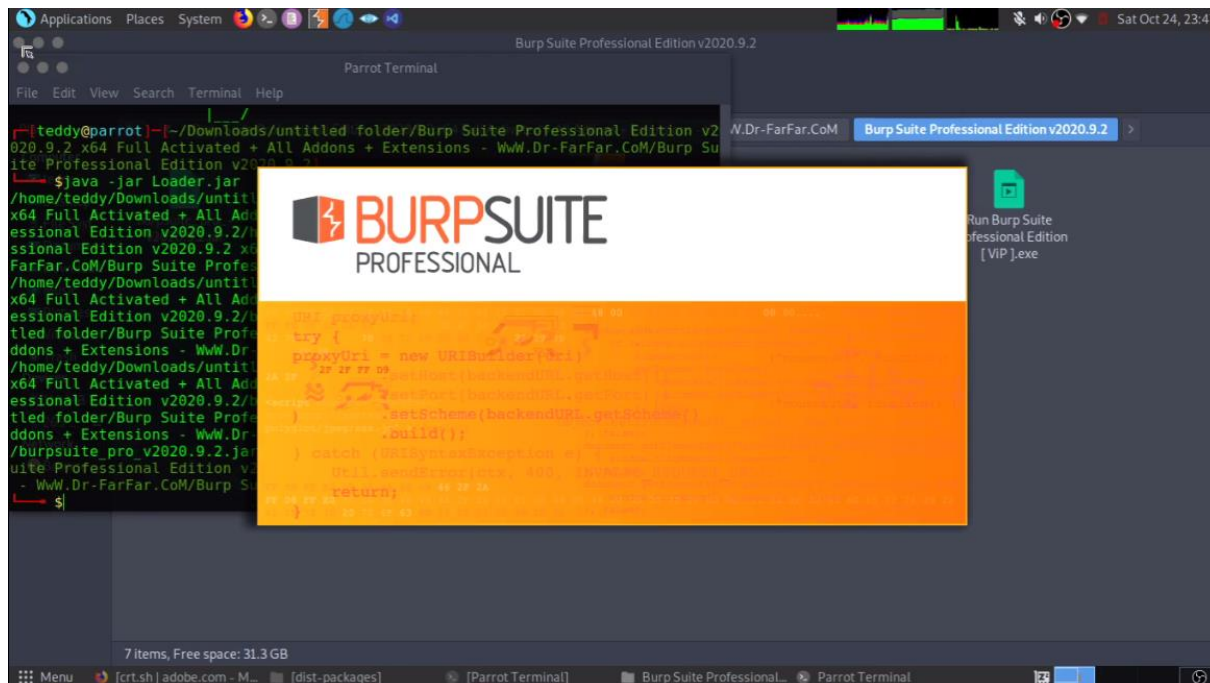


## Burp suit

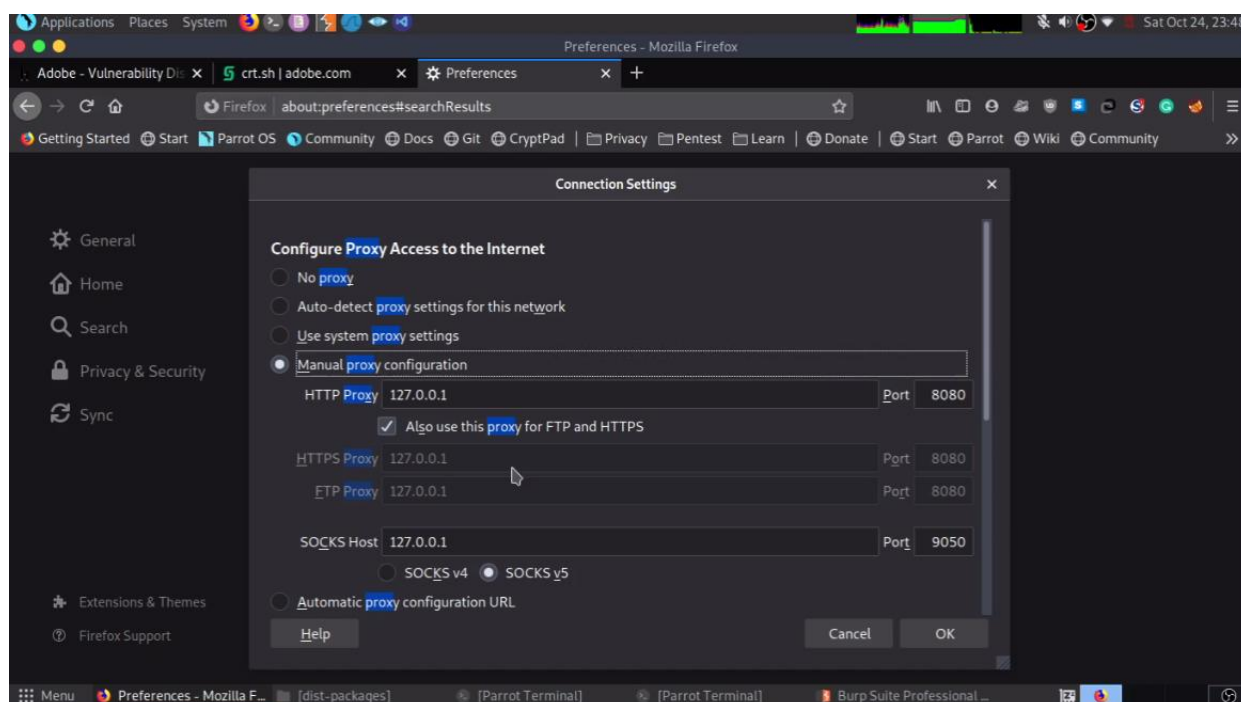
Burp Suite is a Java based Web Penetration Testing framework. It has become an industry standard suite of tools used by information security professionals. Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications. There are mainly two versions available burp suite Community Edition & Professional Edition. In here I have used professional edition.

Step 01 : In here need to extract loader java file of Burp Suite

#Java -jar Loader.jar

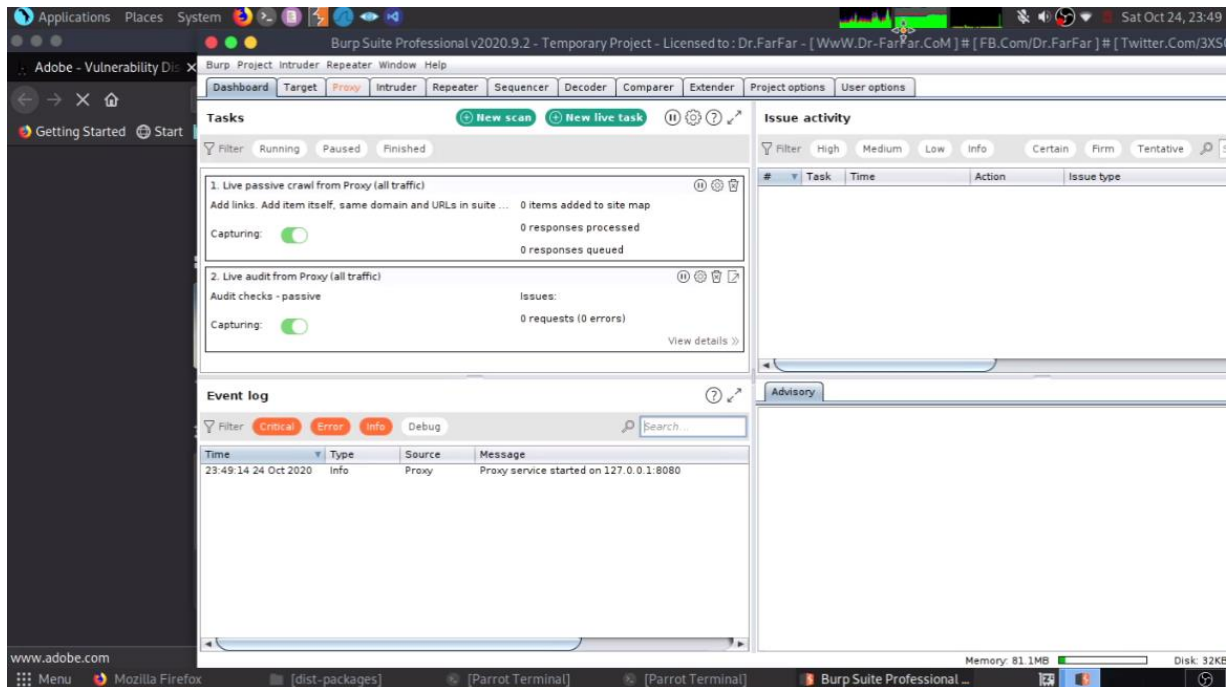


Step 02 : If we want to do penetration testing with burp suite we need to configure our browser proxy settings to "127.0.0.1" "port : 8080".use portswigger port for our scan,intercept,targets etc. Enable for FTP & HTTPs

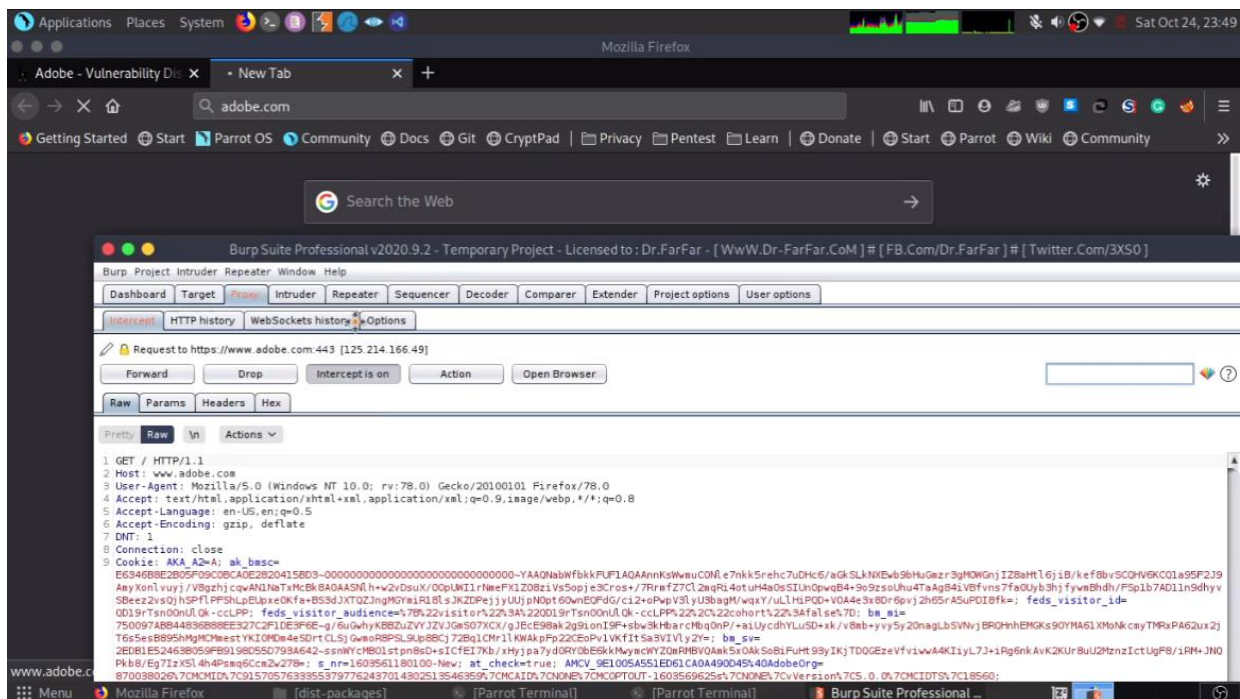




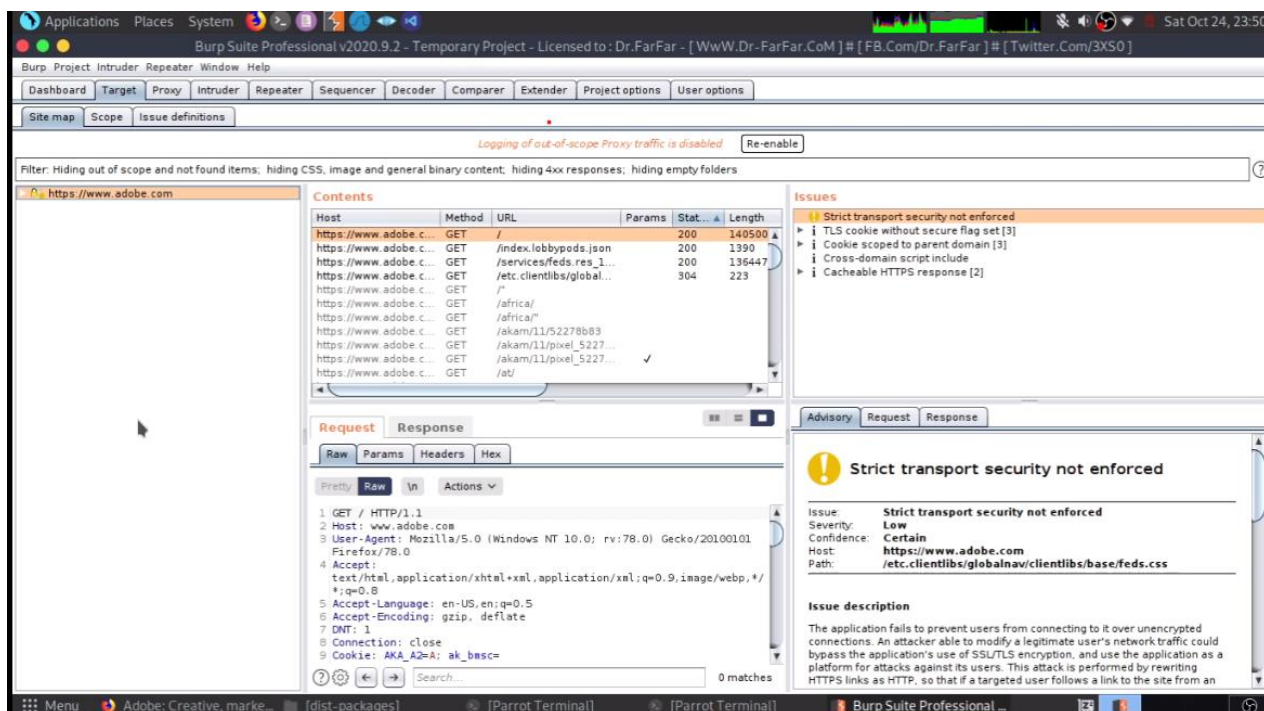
Step 03 : There after start burp suite & click on “start burp”, Then directly navigate to the burp suit UI.



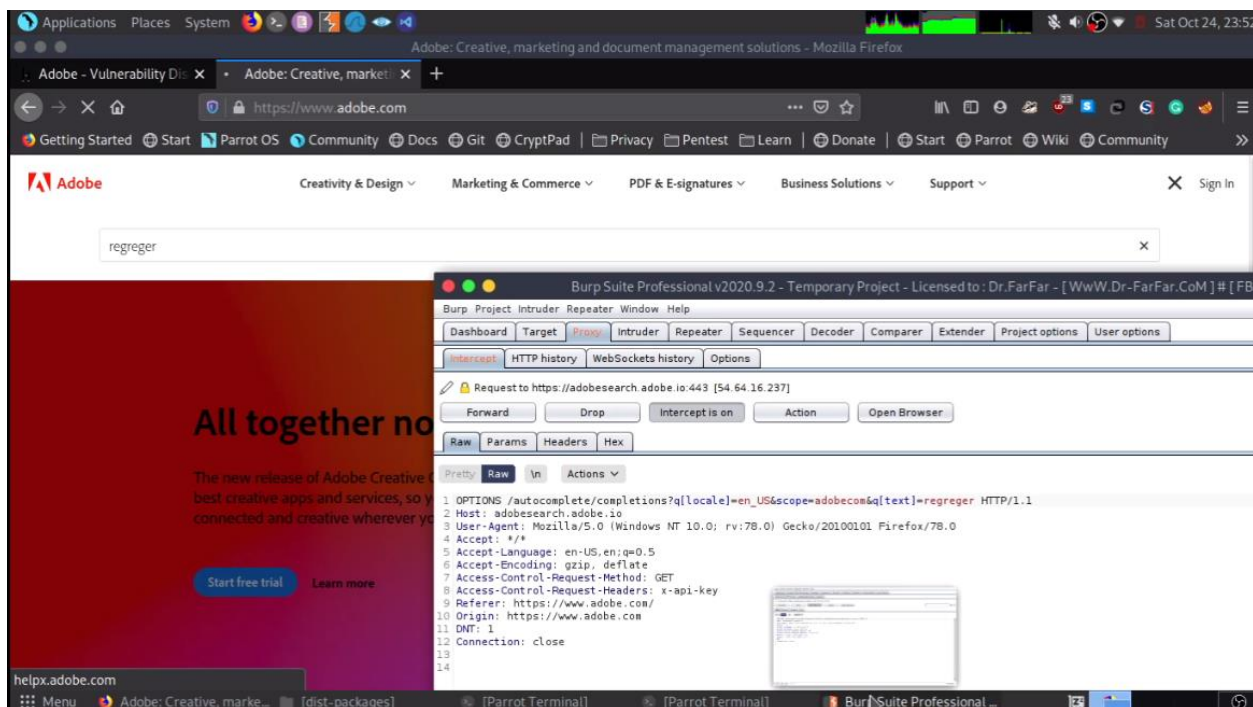
Step 04 : when we are once entered through the target domain we can use intercept mode is on. Intercepting operates as a web proxy server between your browser and target applications, and lets you intercept, inspect, and modify the raw traffic passing in both directions.



There after I have switched a target tab and and, I can see bunch of web domain contents, Http request, responses & issues. In here we can filter scope only sites with filter. Once we add one domain for target list there after we can add another domains to scope.

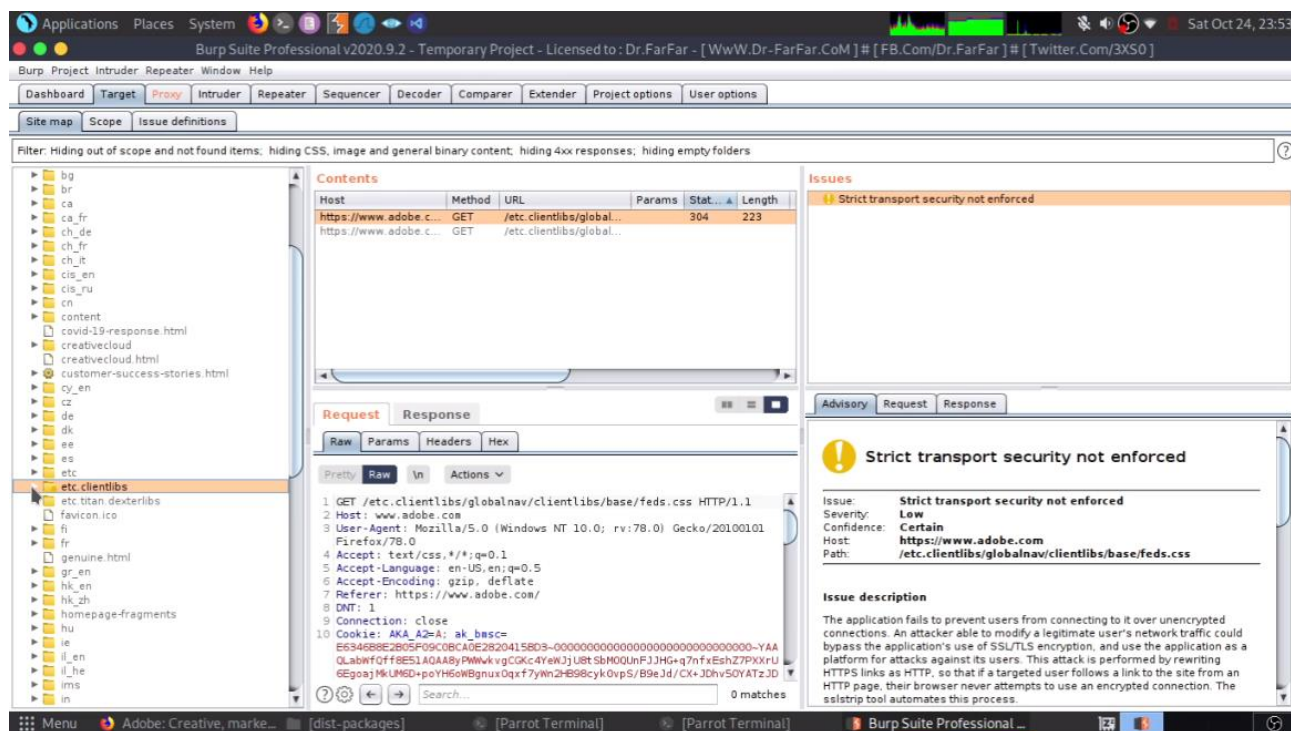


There after I have intercepted adobe.com, With doing input fields checking,

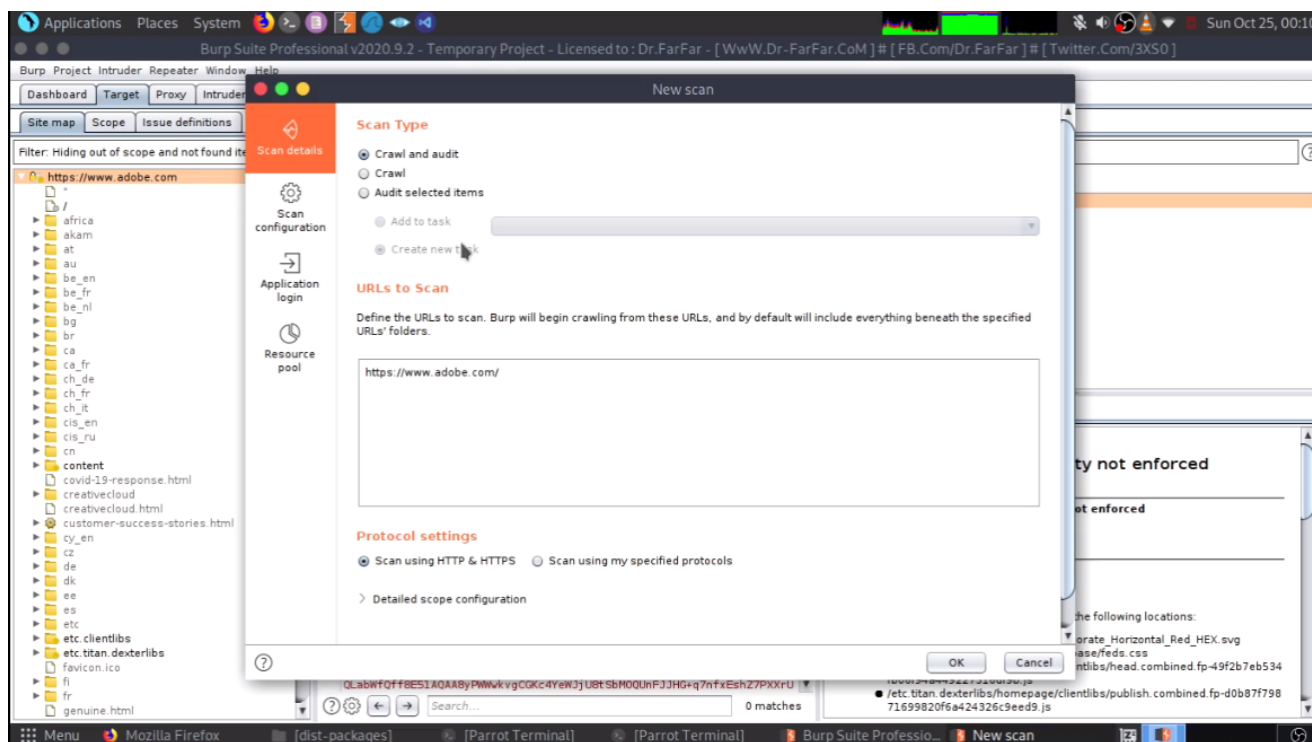




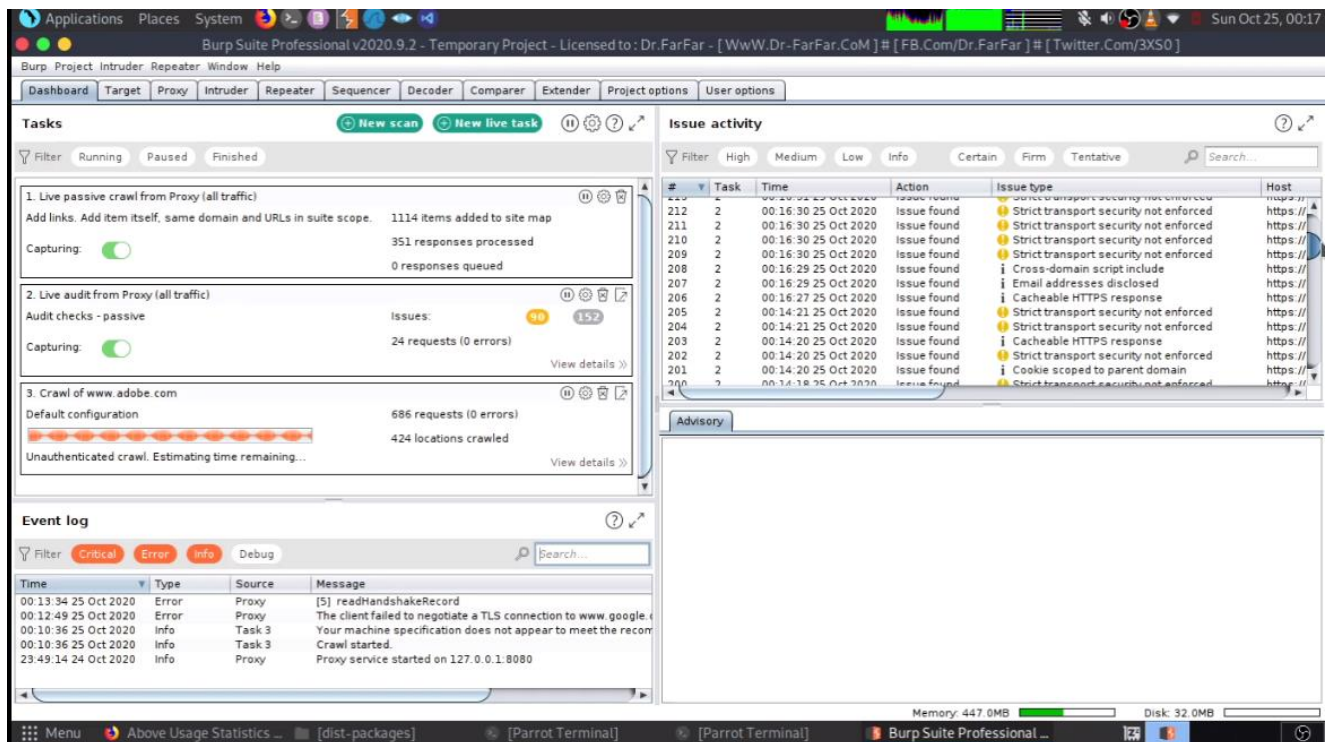
So, there after I have captured some issues without scanning. In enumeration process this is really helps to get idea what we want to going through .So in here I have captured transport security issue with burp suite



Then I have done burp scan with crawling all there relevant domain contents. there are 3 options available for professional users, but community edition only have 2 options. Audit & crawling for Professional users.in here I have done web crawling method, because I wanted to scan entire domain contents to capture some sensitive information



Process of Crawling, When crawling started can see analyzing bunch of content files of target lists. So, we can see bunch of security issues capturing with crawling process.



PS : When I try to crawl every time my target domains I had to face OS freeze problem or Crash situations because my system requirements doesn't enough for to do that process.(You can see that warning message In event log) ☹️.Finally I decided to avoid to burp in my PC.

## Nikto Scanner

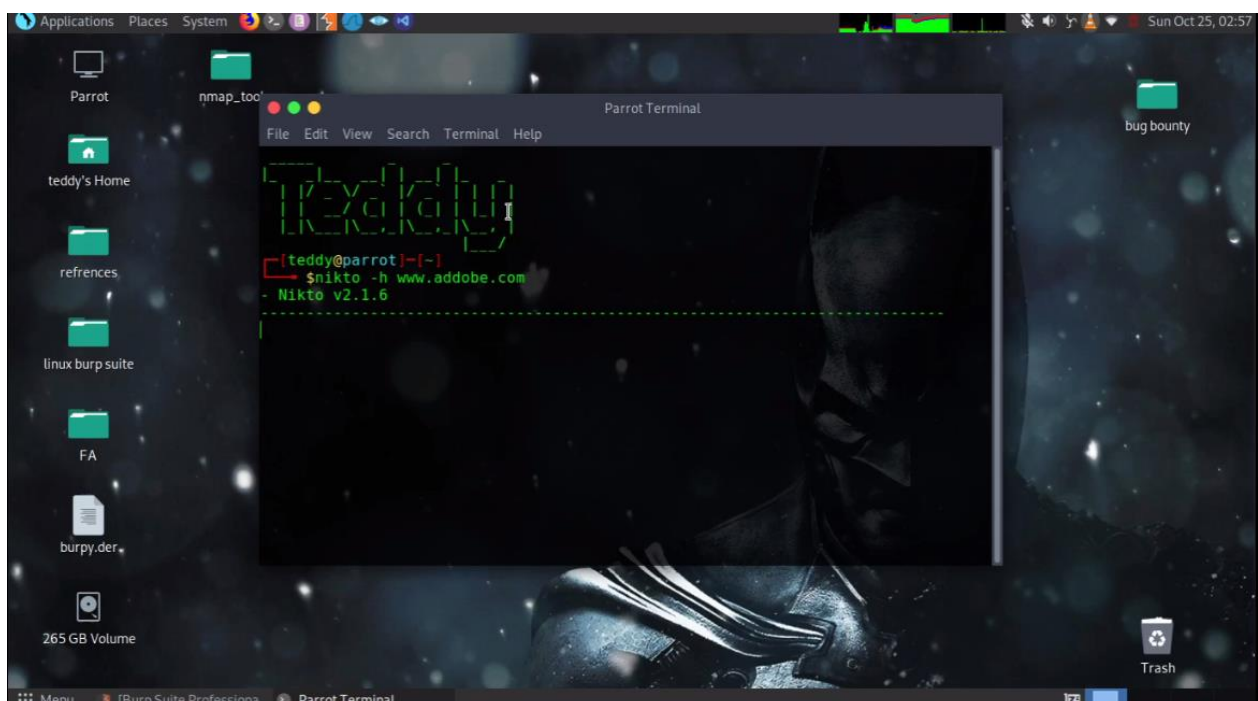
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

Not every check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

In here I'm used Nikto 2.1 version. Nikto can scan web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. So I have used target domain to get sensitive information.

#Nikto -h [www.adobe.com](http://www.adobe.com)

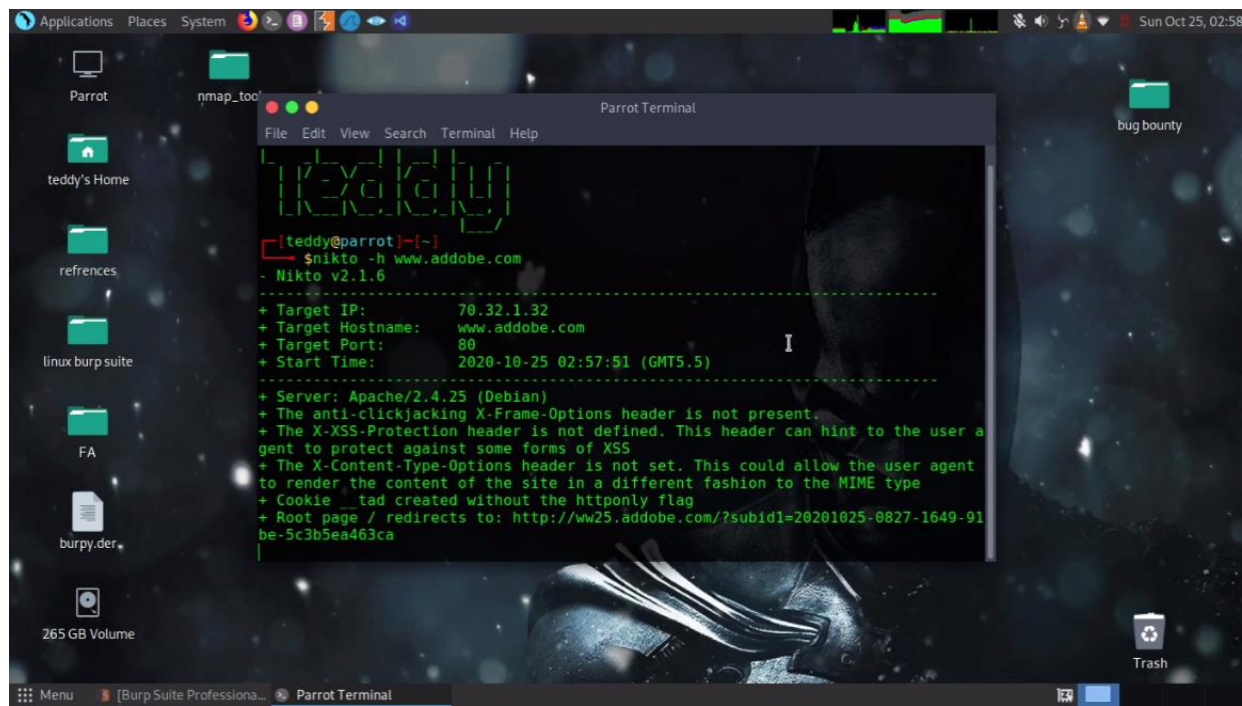


After that command execution, I got adobe's IP address & With several vulnerable points. In here

#XSS protection header is don't defined-So this is vulnerable for XSS attacks.

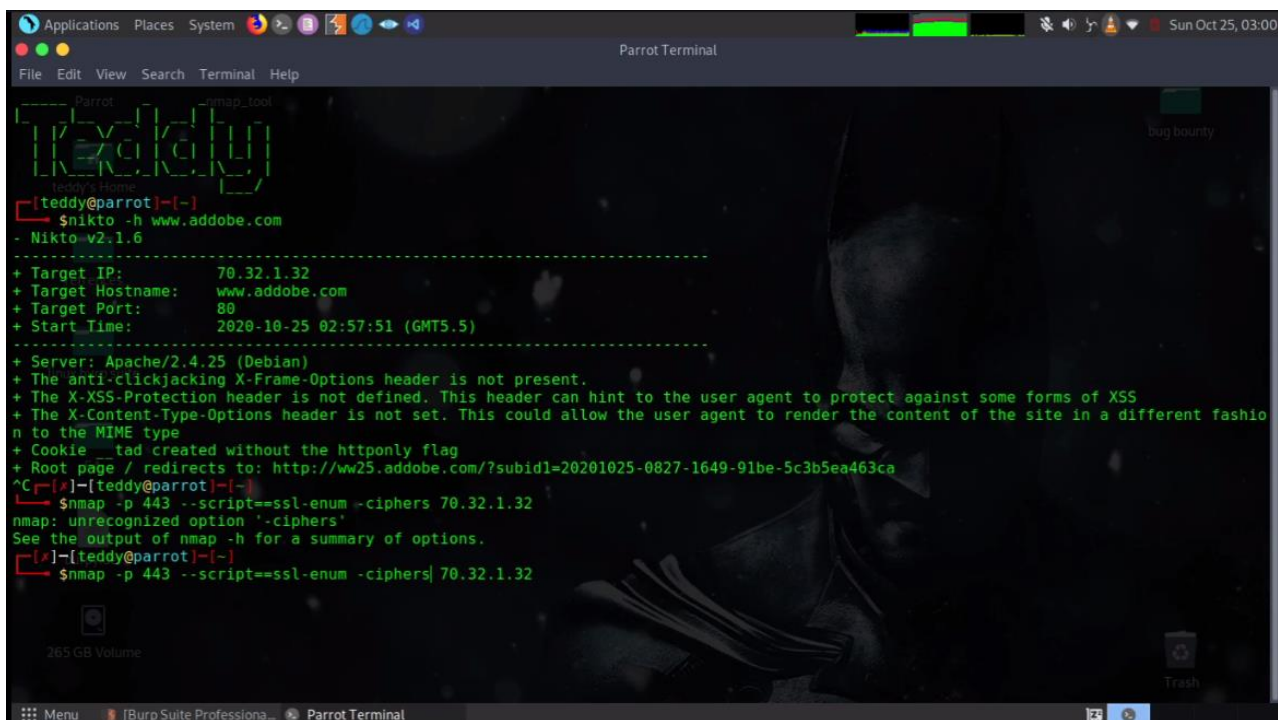
#Content-type headers are not defined

#Also we can see their web server information here



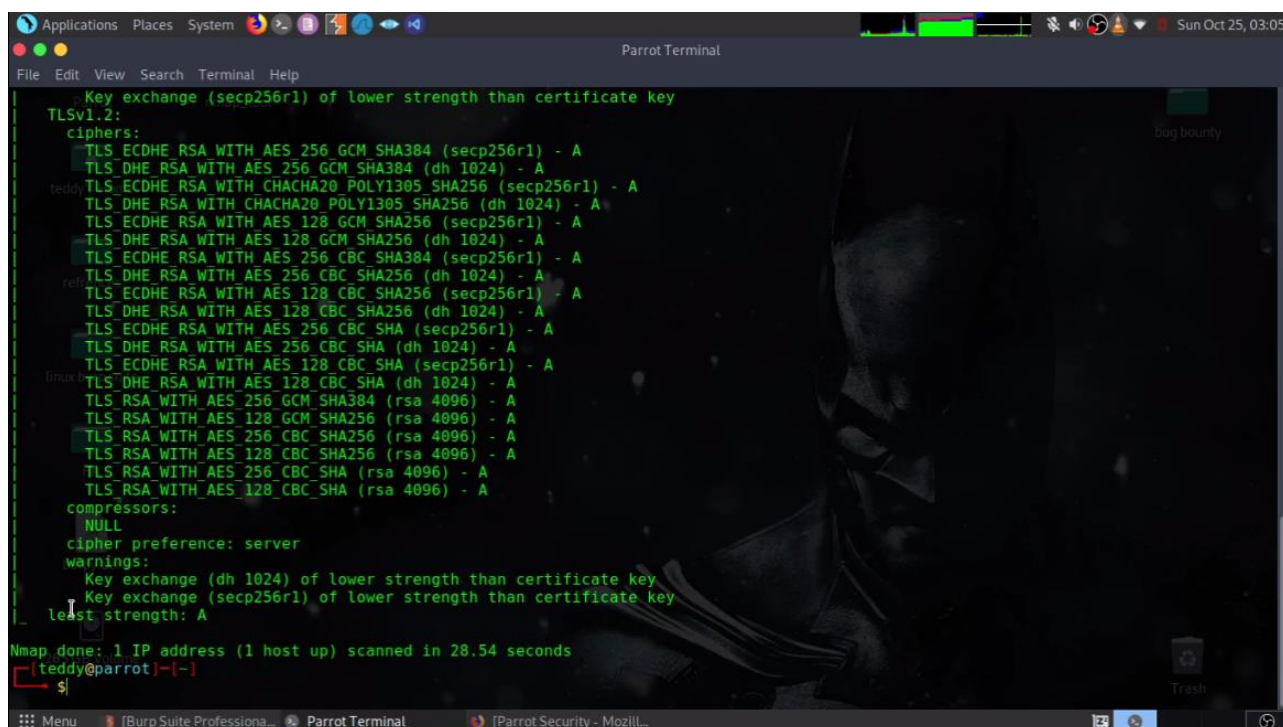
There after I had to check their ciphers weak or not, For that I have used Nmap scanner to enumerate their ciphers.

#nmap -p 443 --script=ssl-enum-ciphers (domain IP address here)





As a result of that my nmap scan, They have strength ciphers in their server.



```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help

Key exchange (secp256r1) of lower strength than certificate key
TLSv1.2:
ciphers:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
  teddy TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
  TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (dh 1024) - A
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A
  ref TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 1024) - A
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024) - A
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 4096) - A
  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 4096) - A
  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 4096) - A
  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 4096) - A
  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 4096) - A
  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 4096) - A
compressors:
  NULL
cipher preference: server
warnings:
  Key exchange (dh 1024) of lower strength than certificate key
  Key exchange (secp256r1) of lower strength than certificate key
least strength: A

Nmap done: 1 IP address (1 host up) scanned in 28.54 seconds
teddy@parrot:~$
```

## Netsparker

Netsparker is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications and web services, and identify security flaws. Netsparker can scan all types of web applications, regardless of the platform or the language with which they are built.

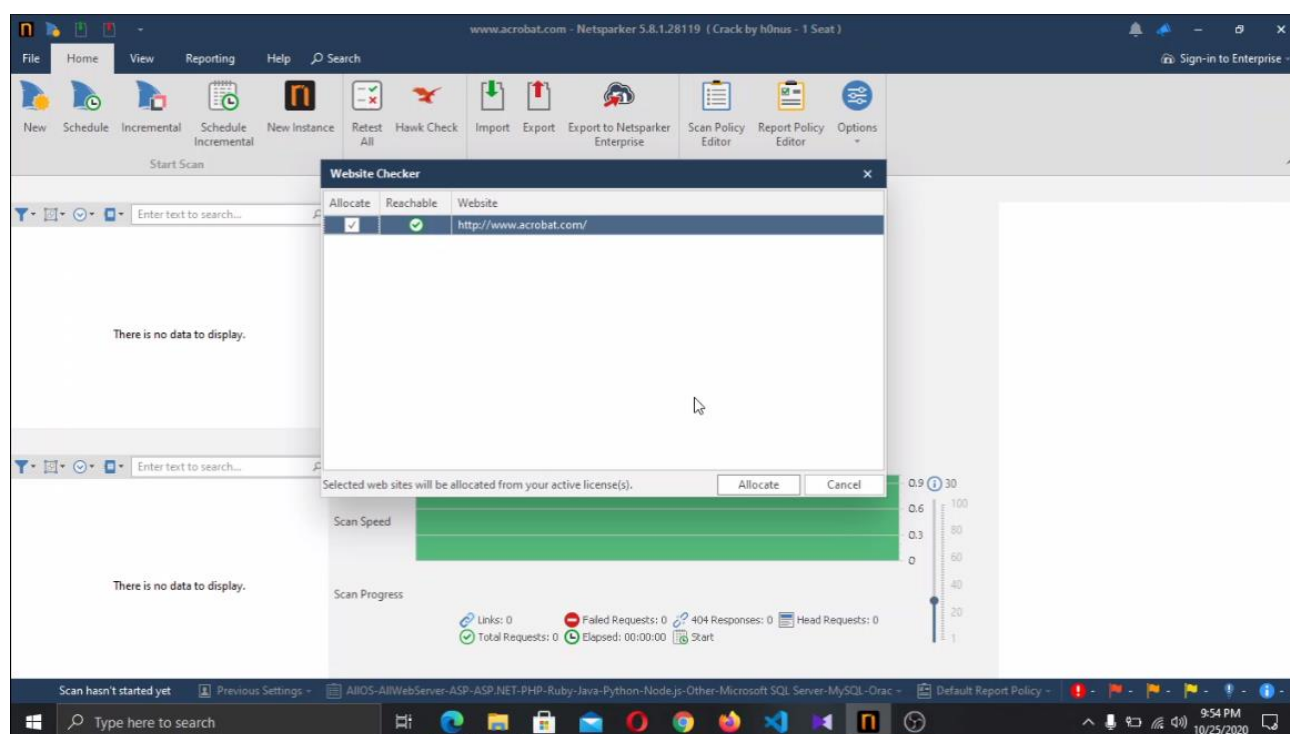
Netsparker is the only online web application security scanner that automatically exploits identified vulnerabilities in a read-only and safe way, in order to confirm identified issues. It also presents proof of the vulnerability so that you do not need to waste time manually verifying it. For example, in the case of a detected SQL injection vulnerability, it will show the database name as the proof of exploit.

Our scanning technology is designed to help you secure web applications easily without any fuss, so you can focus on fixing the reported vulnerabilities. If Netsparker cannot automatically confirm a vulnerability, it will inform you about it by prefixing it with '[Possible]', and assigning a Certainty value, so you know what should be fixed immediately.

Netsparker scanners can generate a proof when they identify the following vulnerability types:

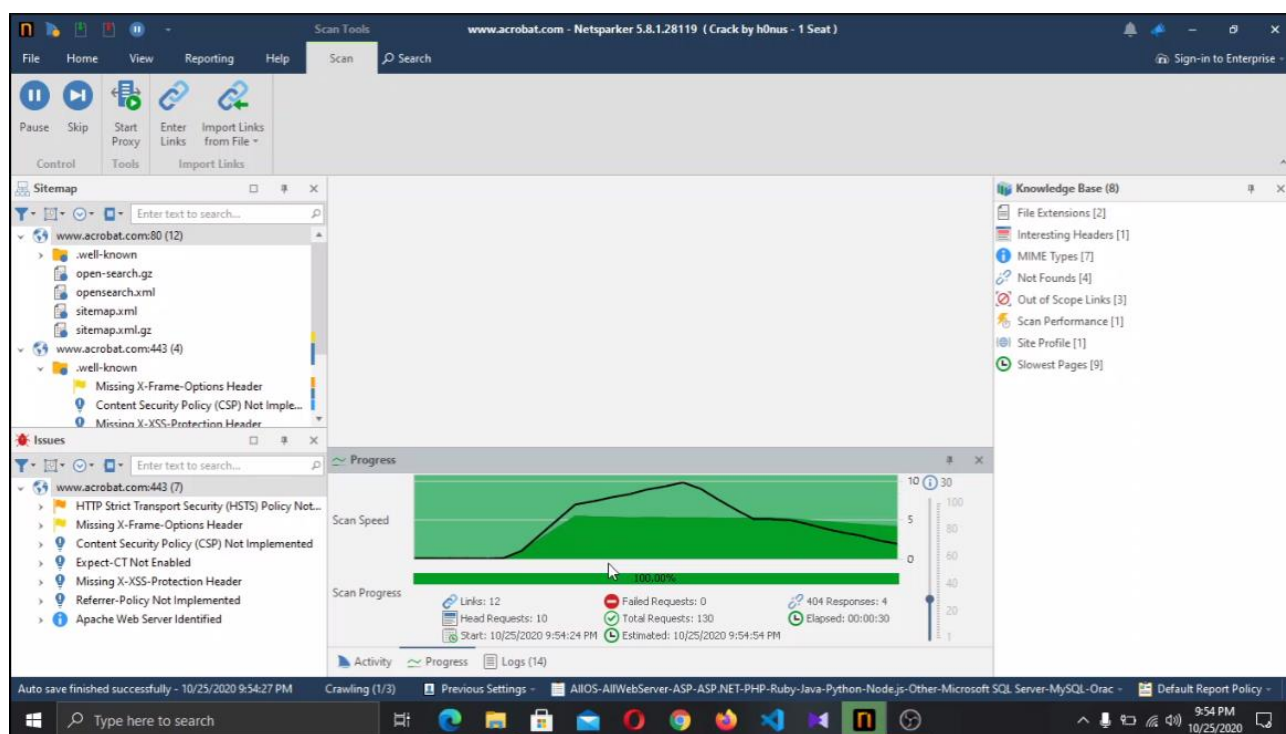
- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion (RFI)
- Command Injection
- Blind Command Injection
- XML External Entity (XXE) Injection
- Remote Code Evaluation
- Local File Inclusion (LFI)
- Server-side Template Injection
- Remote Code Execution
- Injection via Local File Inclusion

In here have used Netsparker for gather some information. First, I had to validate my target site is reachable or not by their “website checker”.

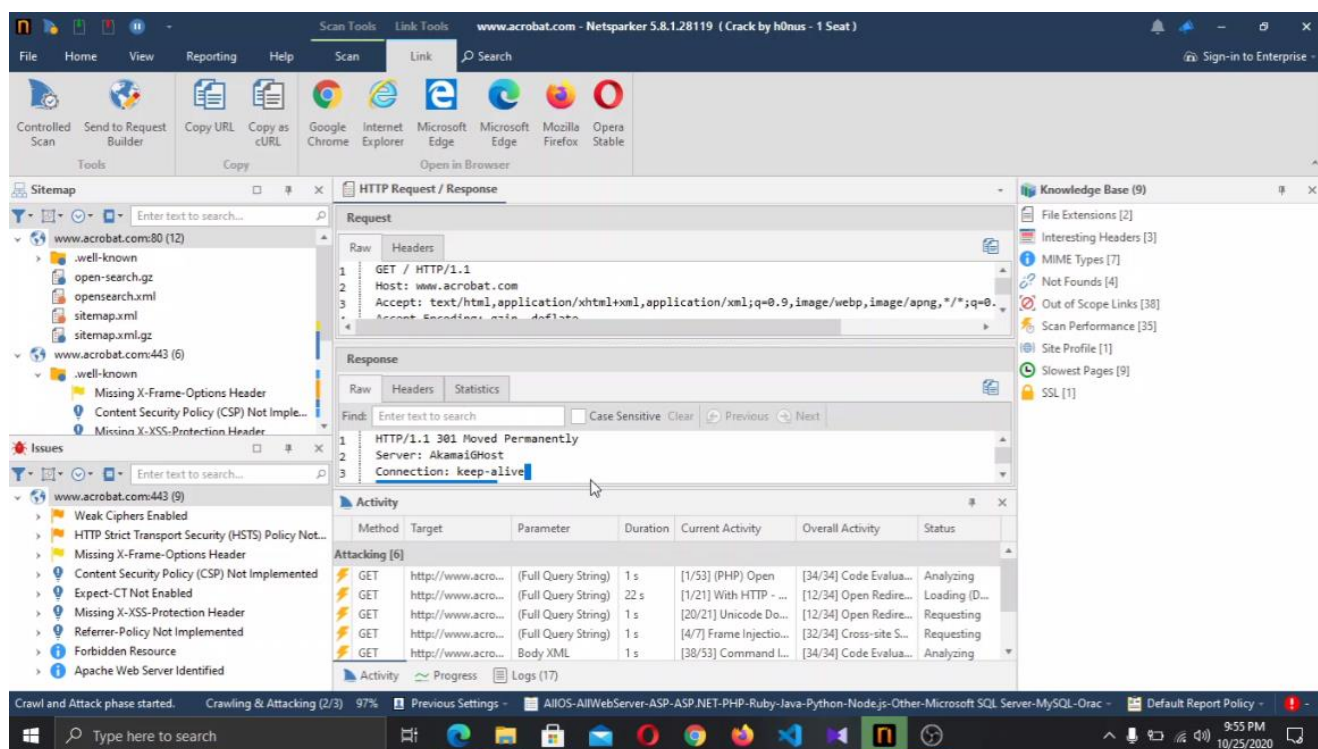




In this netstat window can see, detailed panel sitemap,issues,progress etc. So we can set how much requests grants to our target domain It can be do with progress panel. In here I have got several high level threats.



End report prompt of “acrobat.com”.In here I have got some issues.



## Vulnerabilities & Mitigations

### 1. Missing X-Frame-Options Header

- detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.
- Path: <http://www.adobe.com/opensearch.xml>
- Countermeasures : Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.

X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.

X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

---

### 2. Active Mixed Content over HTTPS

- A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.
- Path : <https://www.adobe.com/creativecloud.html>
- Countermeasures :

There are two technologies to defense against the mixed content issues:

HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)

Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with.

---

### 3. HTTP Strict Transport Security (HSTS) Errors and Warnings

- The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.
- Path : <https://www.adobe.com/>
- Countermeasures : Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

#### 4. Using Out-of-date Version (jQuery)

- Since this is an old version of the software, it may be vulnerable to attacks.
  - Path : <https://www.adobe.com/creativecloud/catalog/desktop.html>
  - Identified Version : 2.0.3
  - Latest Version : 2.2.4 (in this branch)
  - Countermeasures : upgrade your installation of jQuery to the latest stable version.
- 

#### 5. Session Cookie Not Marked as Secure (\*Very Critical)

- identified a session cookie not marked as secure, and transmitted over HTTPS. This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack. It is important to note that Netsparker inferred from the its name that the cookie in question is session related.
  - Path : <https://www.adobe.com/creativecloud/business/teams.html?mv=other&promoid=NYTLR3CX>
  - Identified Cookie: TID
  - Cookie Source: HTTP Header
  - Countermeasure : Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure).
- 

#### 6. Possible Cross-site Request Forgery

- Identified a possible Cross-Site Request Forgery. CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.
  - Path : <https://www.adobe.com/unsubscribe.html>
  - Countermeasures : Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
  - If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
- 

#### 7. Missing X-XSS-Protection Header

- detected a missing X-XSS-Protection header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.
- Path : <https://www.adobe.com/marketingtech/main.no-promise.min.js>
- Countermeasures : Add the X-XSS-Protection header with a value of "1; mode= block".