Sri Lanka Institute of Information Technology

Assignment – Web Audit

www.unity.com

WEB SECURITY – IE2062

Student ID	Name
IT20228880	K.K.K.P.Kumara

Acknowledgement

I would like to offer my heartfelt gratitude to Dr. Lakmal Rupasinghe, the lecturer in charge of the Web security module, for his excellent assistance and advice, which was instrumental in the beginning of this web audit.

I'd also want to express my gratitude to Ms. Chethna Lyanapathirana, Ms. Lanisha Rugghahakotuwa, and Ms. Chathu Udagedra for the assistance and advice they have provided us during the course of this Web audit.

Purpose

In a web application, a web audit is performed to identify and evaluate vulnerabilities that may result in security breaches, as well as inconsistencies that may exist on the site that may result in Google penalties.

Our batch asked to perform a web audit on any domain of our choosing. This report shows how to conduct a primary web audit touching on information gathering topic.

Abstract

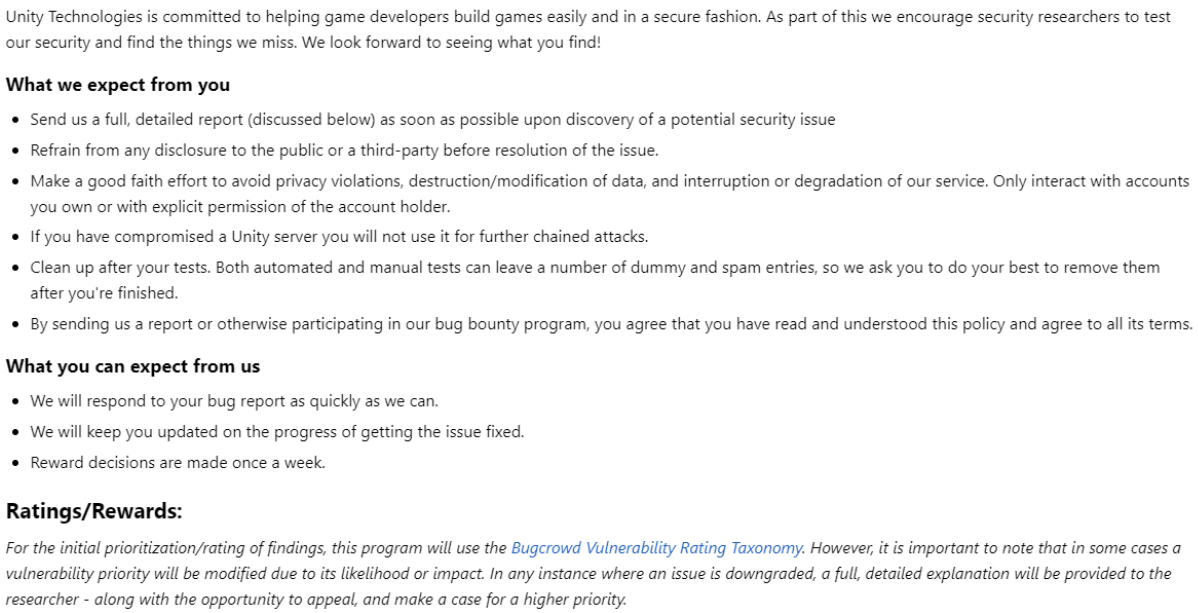
First step I gathered information about the targeted domain did the enumeration for domain and subdomains after that scanned for vulnerabilities by some tools such as burp suite,nikto,nmap netspaker etc. finally I could identified vulnerabilities of the domain which I chose and I got suggestions for mitigate identified vulnerabilities.

Contents

Introduction

I have selected the unity technology domain from bugcrowd.com for my web audit. A video game software development firm established in the United States, Unity Technologies is a leader in the industry. The gaming industry benefits from it since it allows artists and developers to render 3D worlds in real time. Unity is used to develop games and other interactive experiences on a variety of platforms, including desktop computers, mobile devices, and gaming consoles, among others. It is also possible to deploy Unity games over the web.

These web audits provide a safe and secure environment for Unity 's customers as well as developers .Unity can solve their vulnerabilities and fix them soon before a big trouble because of these audits.



Unity Technologies is committed to helping game developers build games easily and in a secure fashion. As part of this we encourage security researchers to test our security and find the things we miss. We look forward to seeing what you find!

What we expect from you

- Send us a full, detailed report (discussed below) as soon as possible upon discovery of a potential security issue
- Refrain from any disclosure to the public or a third-party before resolution of the issue.
- Make a good faith effort to avoid privacy violations, destruction/modification of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
- If you have compromised a Unity server you will not use it for further chained attacks.
- Clean up after your tests. Both automated and manual tests can leave a number of dummy and spam entries, so we ask you to do your best to remove them after you're finished.
- By sending us a report or otherwise participating in our bug bounty program, you agree that you have read and understood this policy and agree to all its terms.

What you can expect from us

- We will respond to your bug report as quickly as we can.
- We will keep you updated on the progress of getting the issue fixed.
- Reward decisions are made once a week.

Ratings/Rewards:

For the initial prioritization/rating of findings, this program will use the Bugcrowd Vulnerability Rating Taxonomy. However, it is important to note that in some cases a vulnerability priority will be modified due to its likelihood or impact. In any instance where an issue is downgraded, a full, detailed explanation will be provided to the researcher - along with the opportunity to appeal, and make a case for a higher priority.

Fig1 Bugcrowd rules about audits

In scope Domains

- www.unity.com
- id.unity.com
- dashboard.unity3d.com
- store.unity.com
- pay.unity.com
- analytics.cloud.unity3d.com

Enumeration

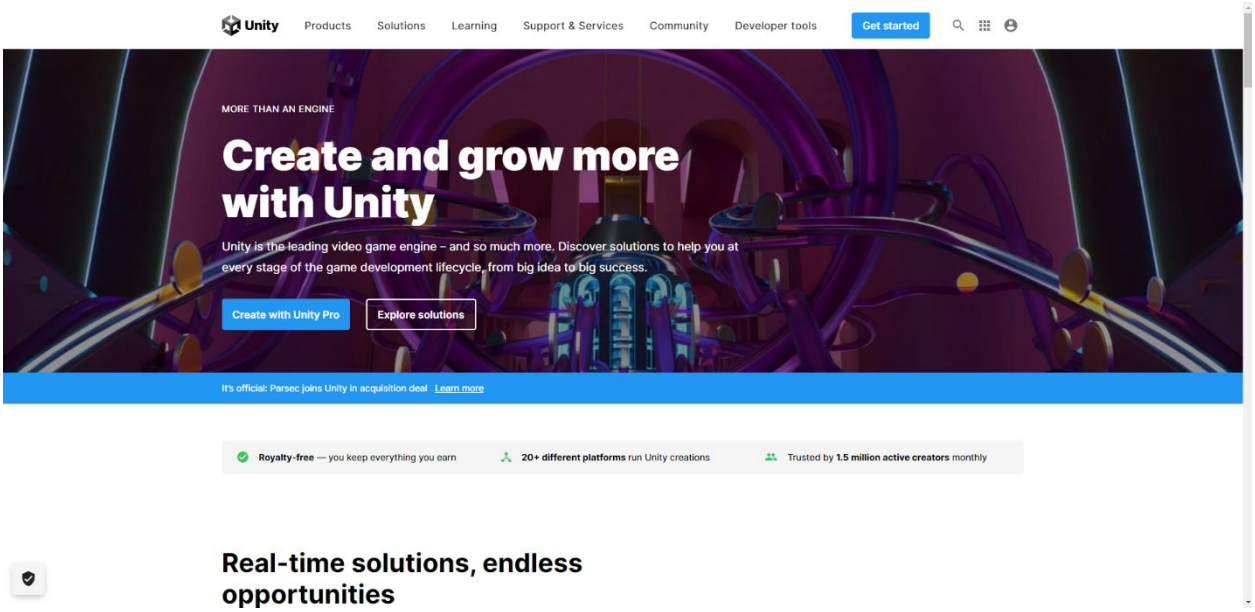


Figure 2 Unity.com website

I used some tools for audit my website which I selected .

Sublist3r

In beginning of the audit, my first step is enumerate subdomains of unity.com .For that process I used a tool named “Subslist3r”.This tool was designed to enumerate the subdomains of websites OSINT. This tool is a python based tool. Most bug bounty hunters and penetration testers are using this tool for identifying subdomains of the domain which they are targeting. Many search engines are using by this Sublist3r for enumerate the subdomains such as Yahoo,bing ,Google etc as well as Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS are using for enumerate process by this tool.

Step 01 : I used for that Parrot OS for this task.. So first I got the Sublist3r from GitHub and cloned by using following command.

Git clone https://github.com/aboul3la/Sublist3r

And we should install the tool.by using

#sudo apt install Subslist3r

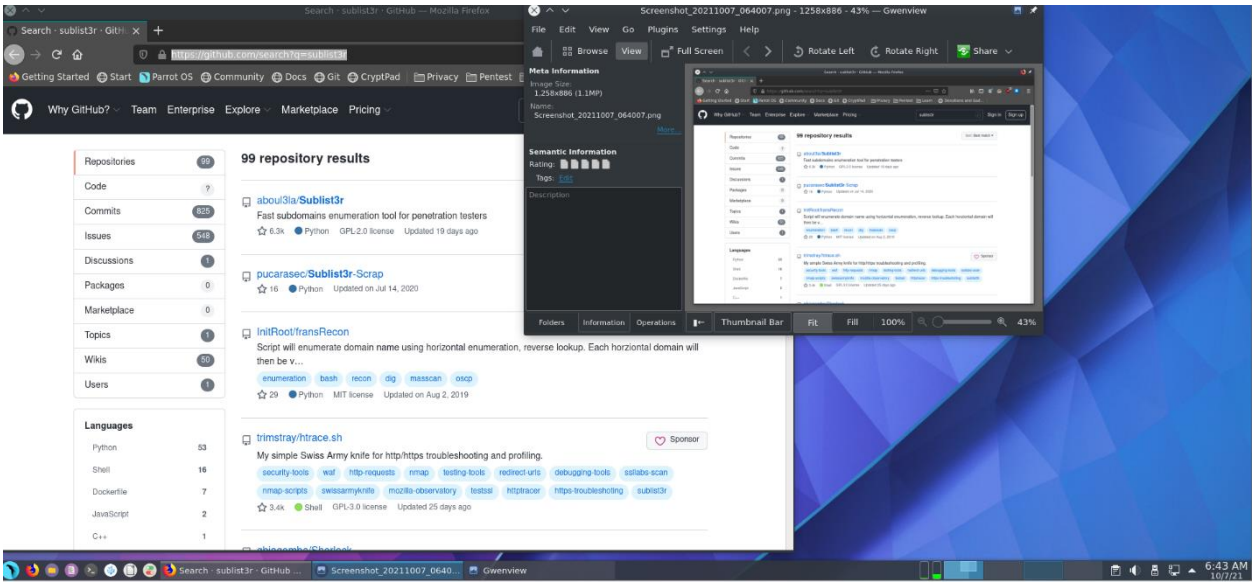


Figure 3 sublist3r in github

Step 02 : then execute the subslist3r.py and get help by typing -h

#python subslist3r.py -h

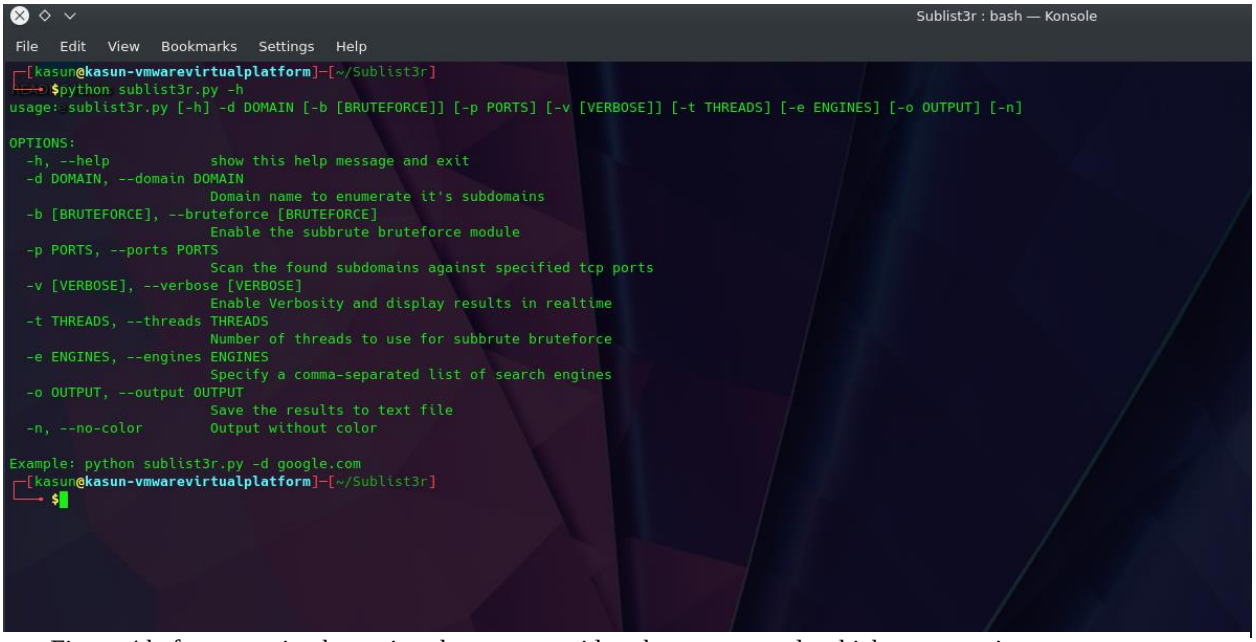


Figure 4 before scanning by typing -h we can get idea about commands which we are going to use

We can get idea about command which should we use by typing -h .After that execute the subslist3r for enumerate all sub domains in unity.com

#Python subslist3r.py -d unity.com

I found 177 sub domains relevant to “unity.com” by this Subslis3r tool.

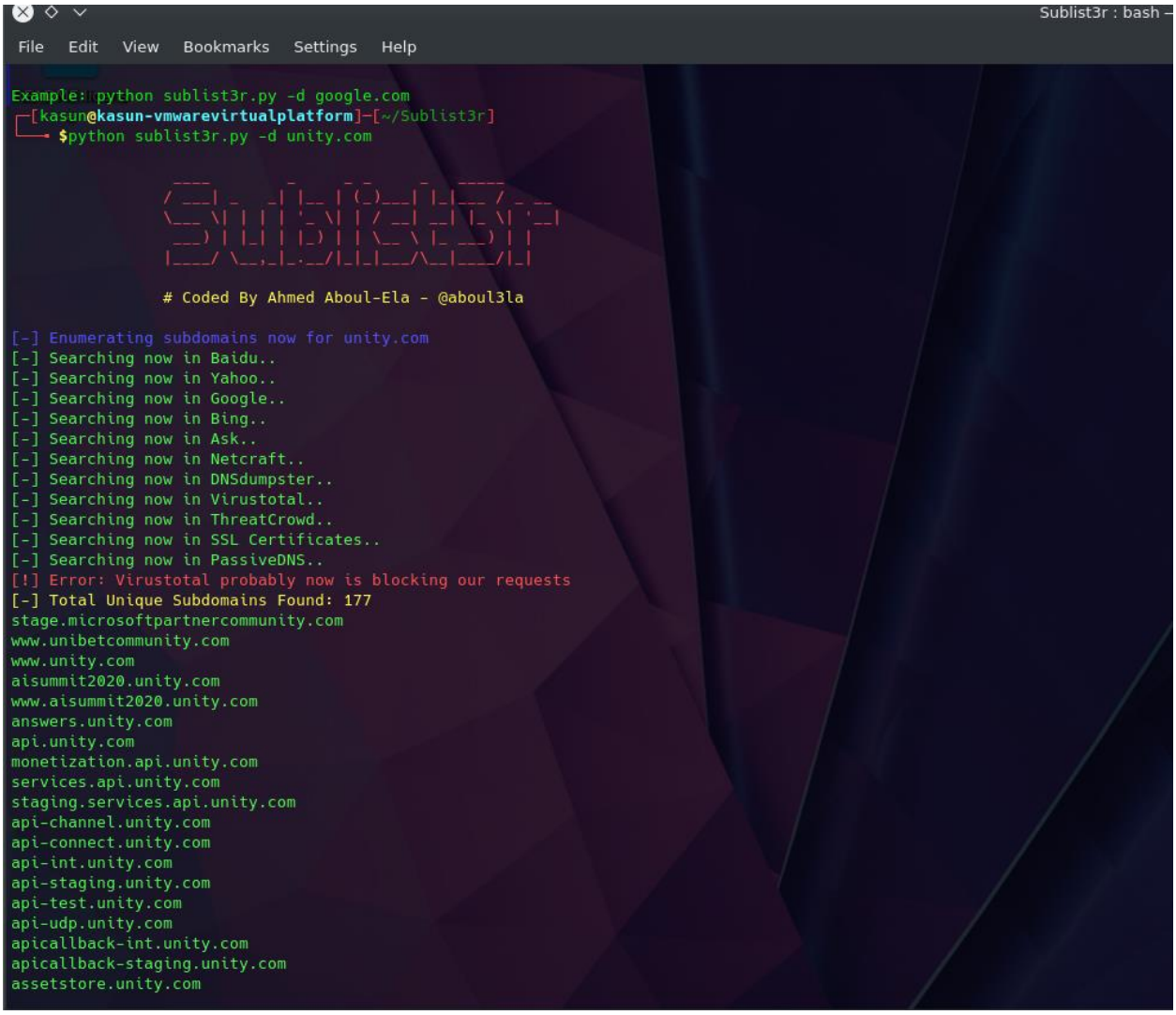


Figure 5 After scanning we can get list of subdomains of targeted domain

[Click here to view all Sub domains]

Recon-ng

This tool also same like sublist3r.we can find information about subdomains and get a knowledge about the subdomains.

I used parrot OS recon-ng is already installed into the OS .first we need to setup our source which we target to scope.I found 17 subdomains of unity.com by this tool.

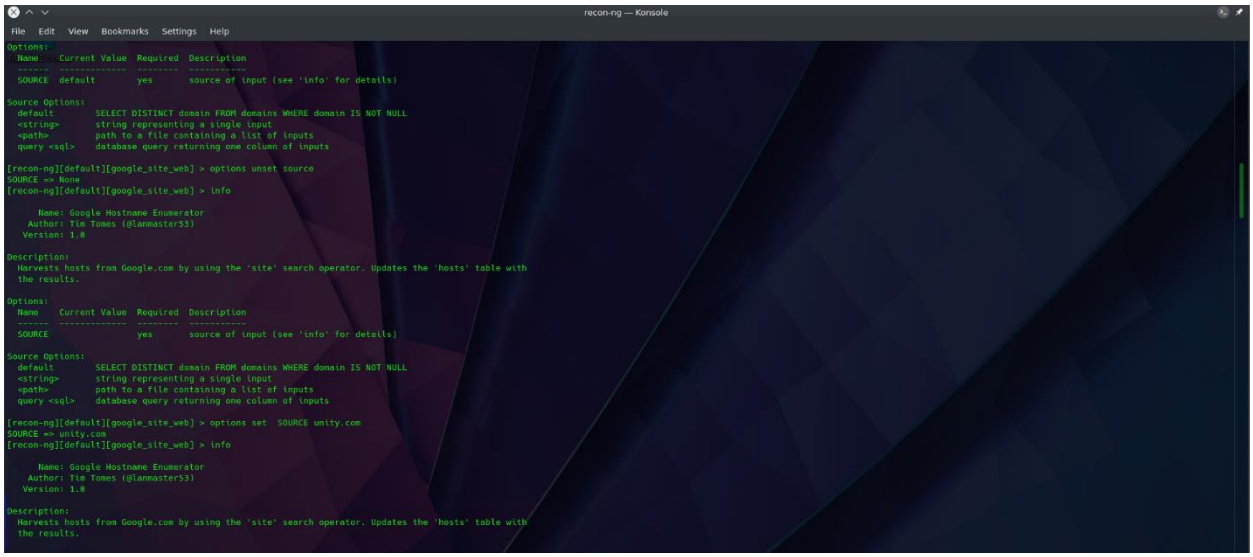


Figure 6 add a source to recon-ng tool

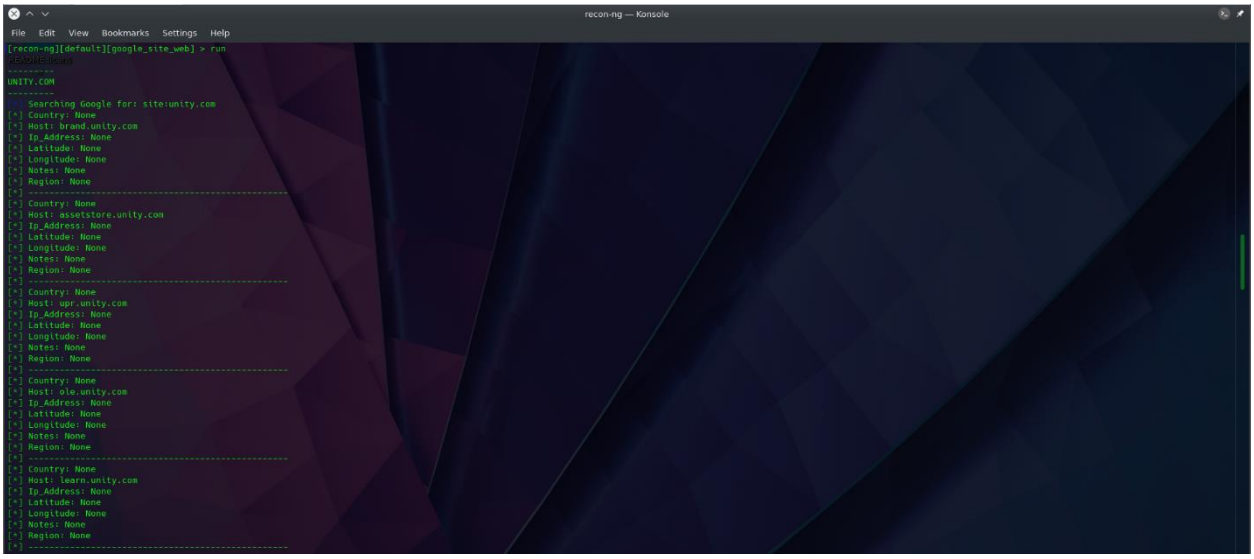


Figure 7 output of recon-ng after scanning

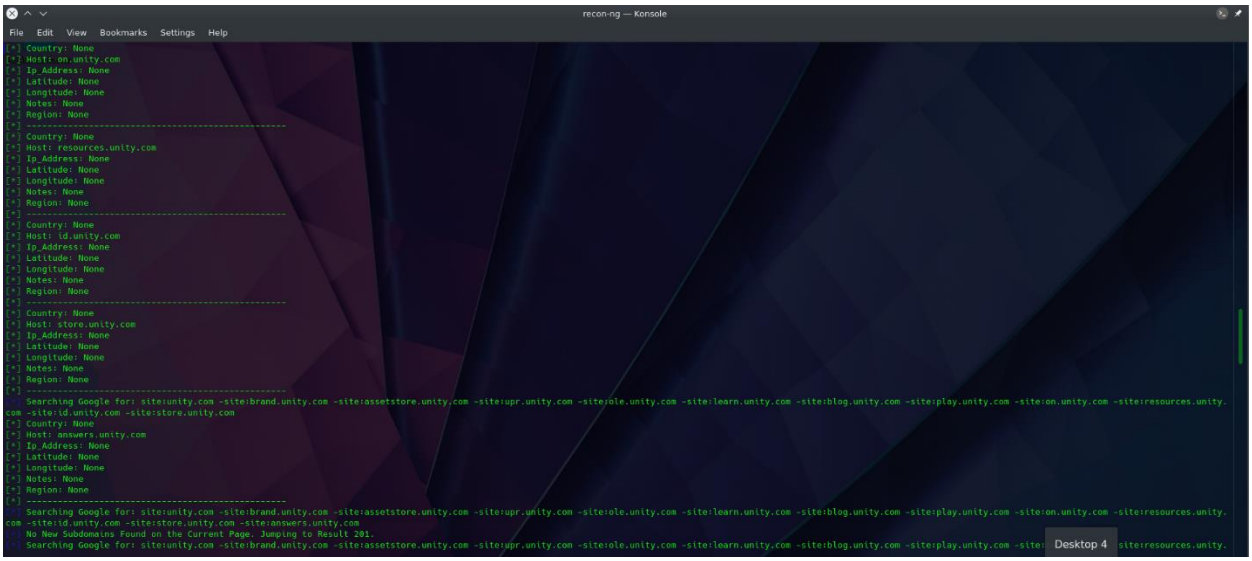


Figure 8 output of recon-ng after scanning

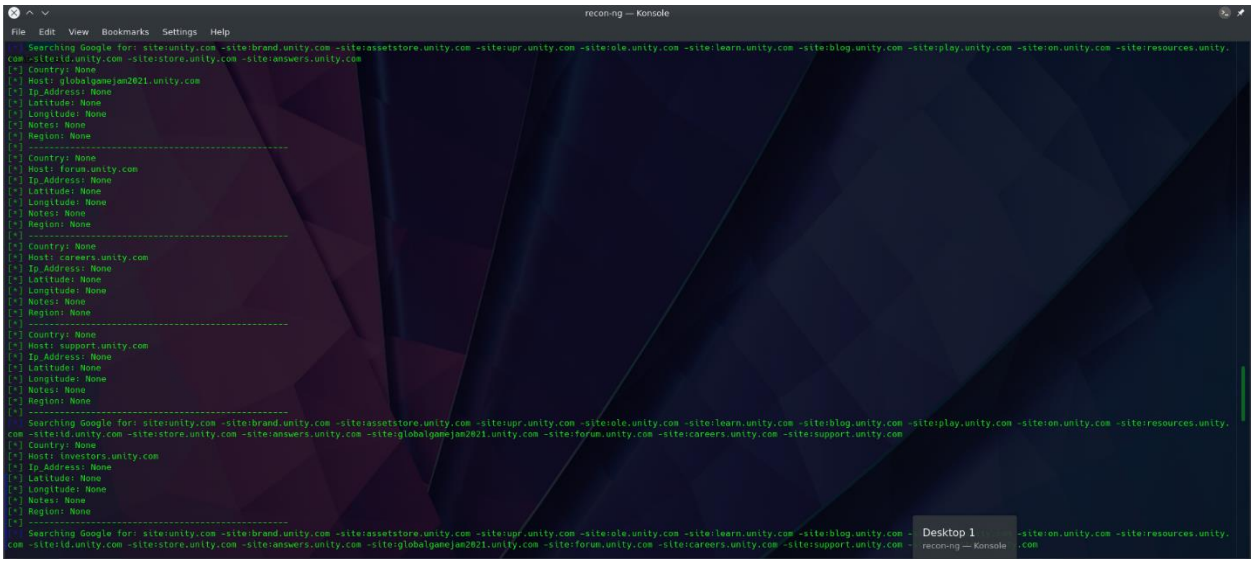


Figure 9 output of recon-ng after scanning

Crt.sh

After that process I used crt.sh for audit certifications and relevant information regarding “unity.com” .This has a web interface which has a distributed database with containing certificate transparency logs. This website provides relevant information and certifications of relevant domain.Crt.sh is very easy to use and it is a certificate fingerprinting tool.

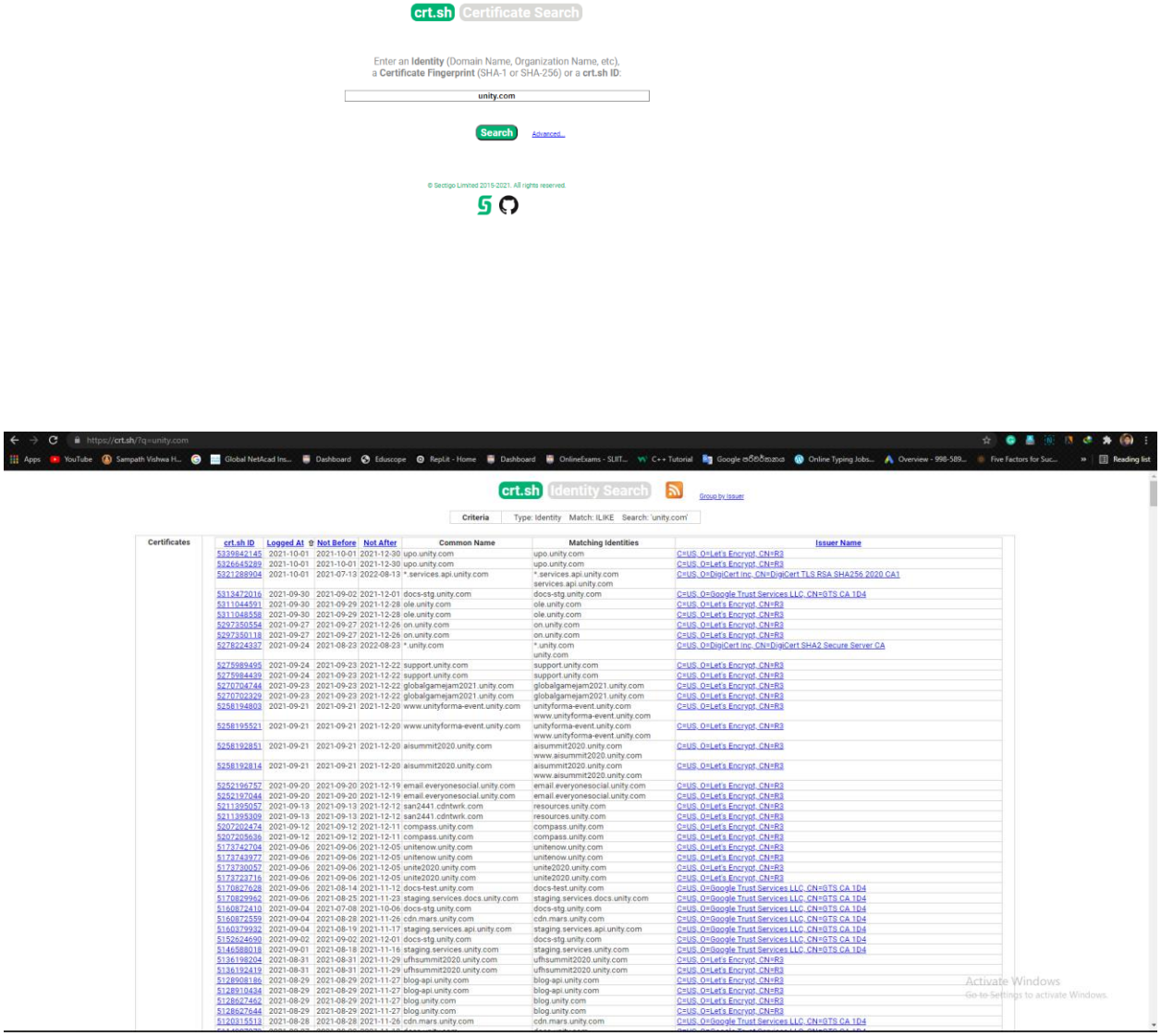
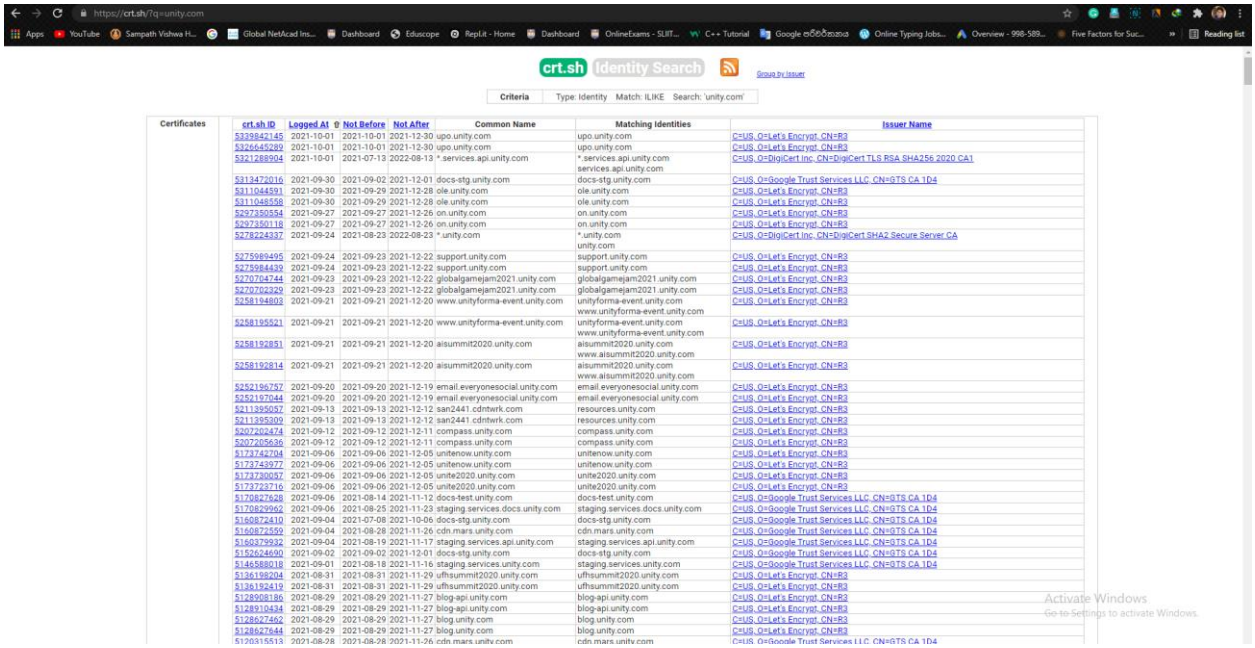


Figure 10 crt.sh shows the certificates that related to targeted domain



Wappalyzer

Wapplayzer provides information about CMS, frameworks, what are the e commerce platforms, JavaScript libraries of relevant website. This is useful for know what technologies used for build the relevant website which we are targeting. This can be considered as information profiler.

In chromium browser there is an extension called wappalyzer and it should be added to browser for get the information.

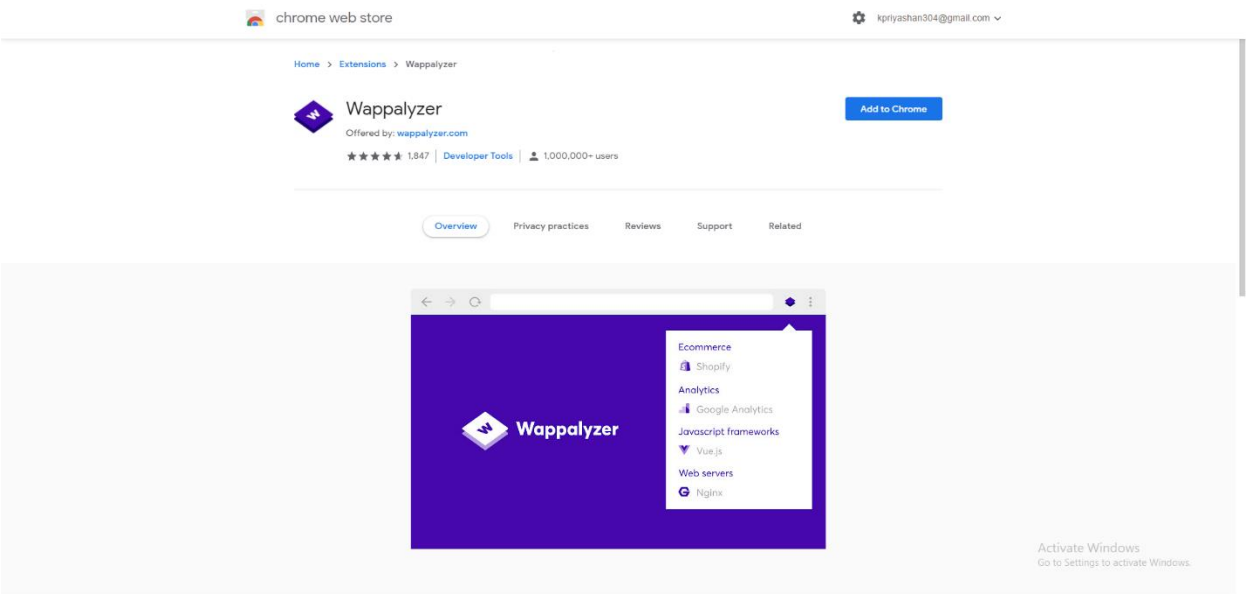


Figure 11 how to add extension to browser

After that go the unity.com and enable extension and we can see the details relevant site.

We can get details about

- CMS
- Tag managers
- Java script libraries
- Programming languages
- Java script frameworks

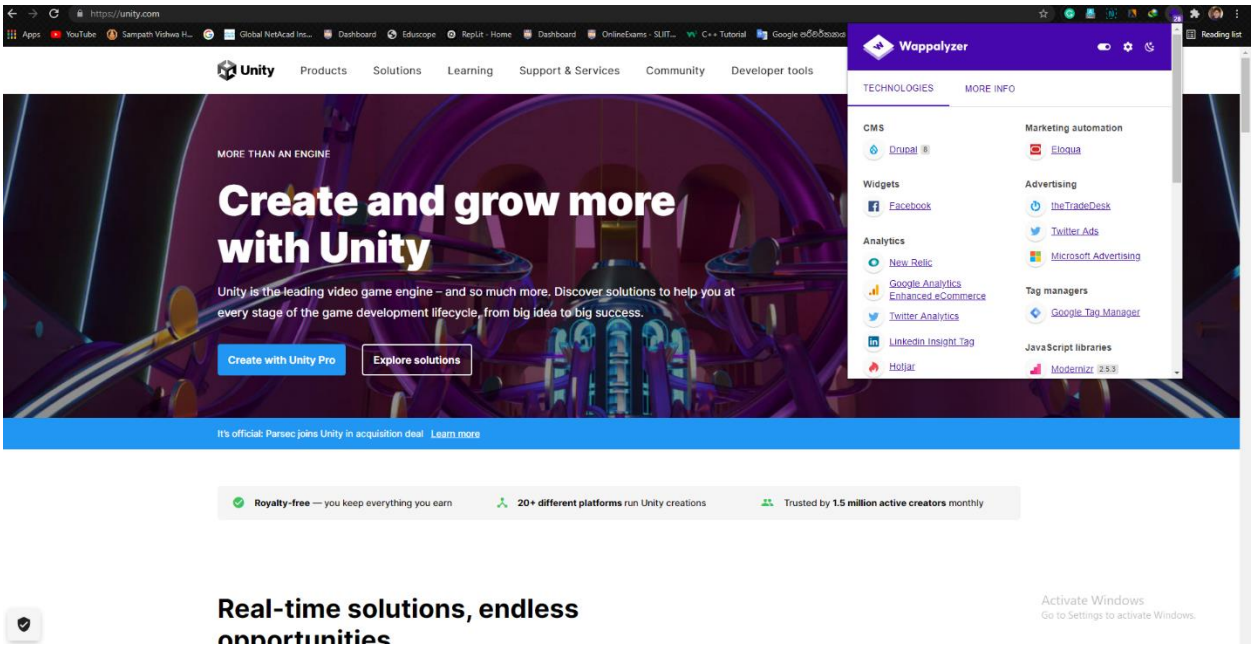


Figure 12 output of wappalyzer we can get information about technologies which site built

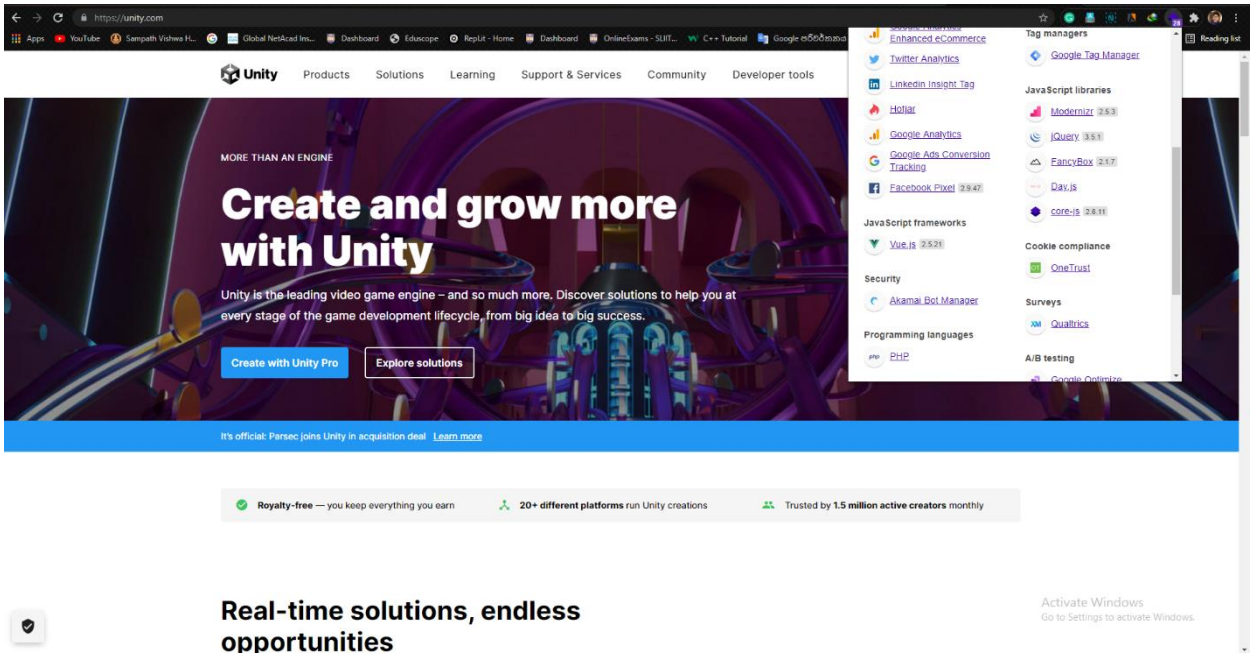


Figure 13 output of wappalyzer we can get information about technologies which site built

Securityheaders.com

This tool is very easy to use and more reliable .By this tool testers can enumerate the security headers .go to the www.securityheaders.com and enter the domain after that we can get all the details about security headers of the domain which we going to find.

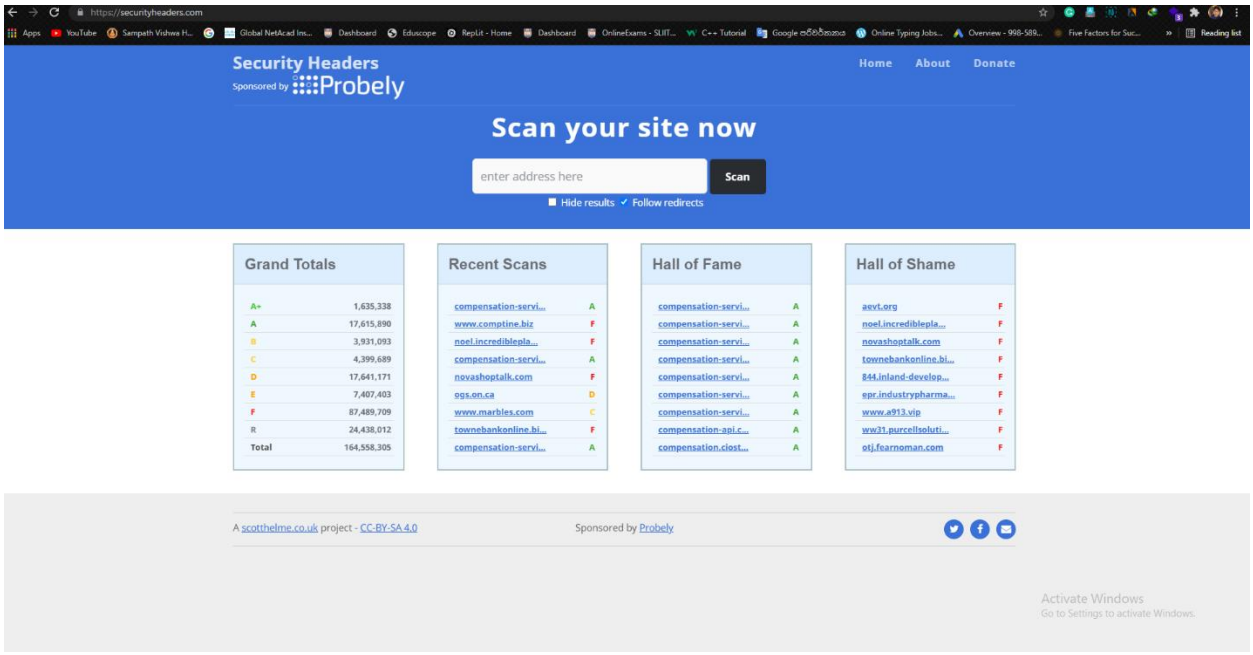


Figure 14 interface of www.securityheaders.com

It is possible to find services that will examine the HTTP response headers of other websites; nevertheless, I wanted to include a grading system in the findings. There are many layers of security provided by the HTTP response headers that this site analyzes, and it is critical that sites make use of these features. Hopefully, by offering a simple method for evaluating them, as well as more information on how to deploy missing headers, we can encourage the widespread use of security-based headers on the internet.

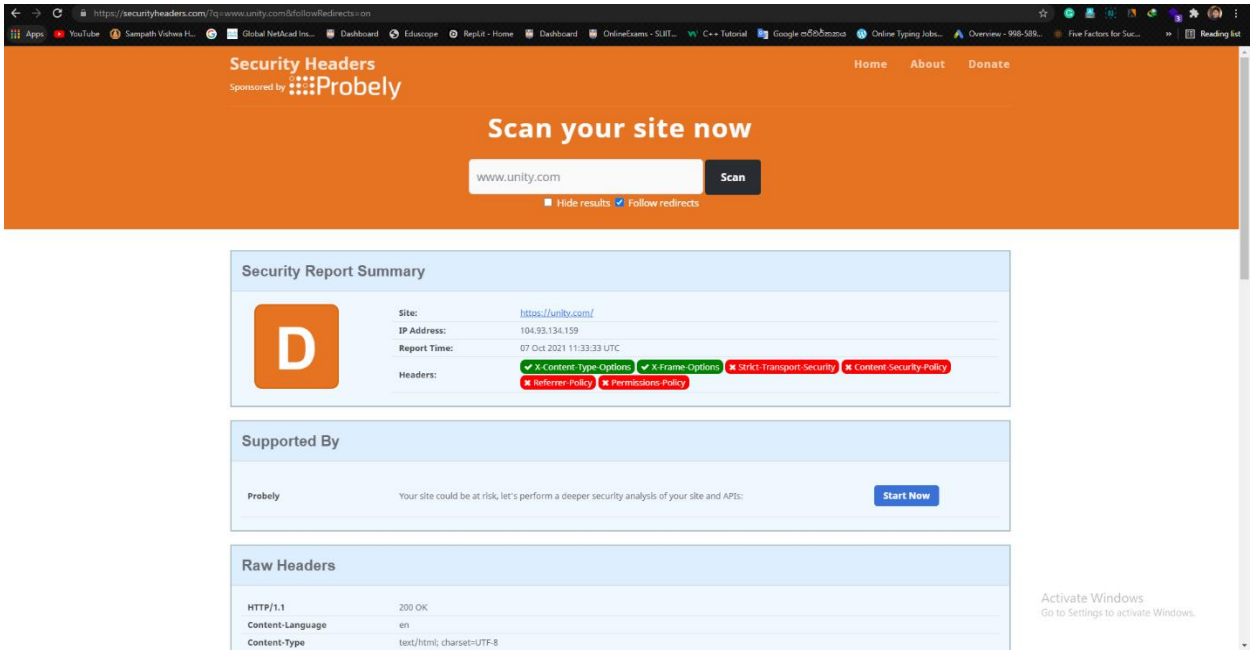


Figure 15 output after scanning provided site ,it shows about security headers that used in unity.com and missing headers and vulnerabilities

I gathered some most important information about missing http security headers of unity technologies.

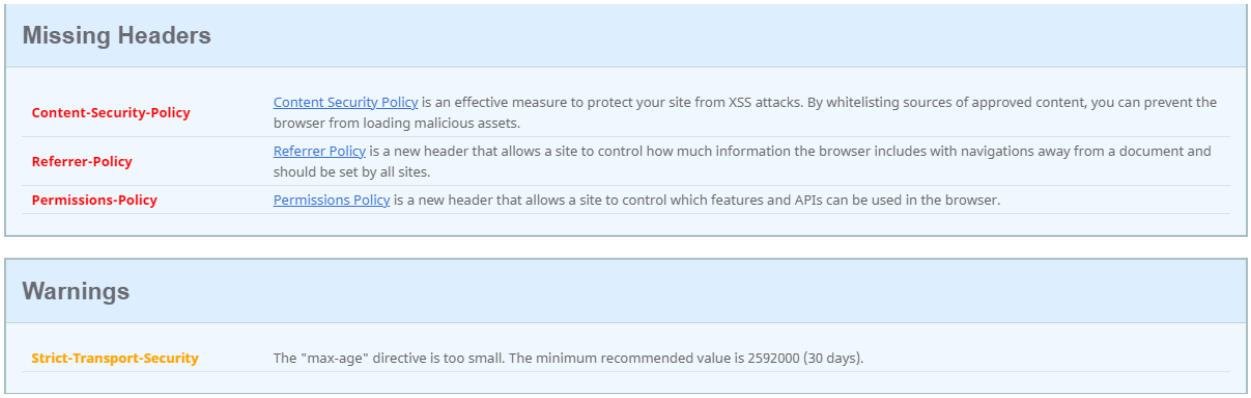


Figure 16 missing headers of unity.com

Built With.com

This tool can be used as a web technology information profiling tool, It is beneficial for the enumeration of web domains and crawling of their information.

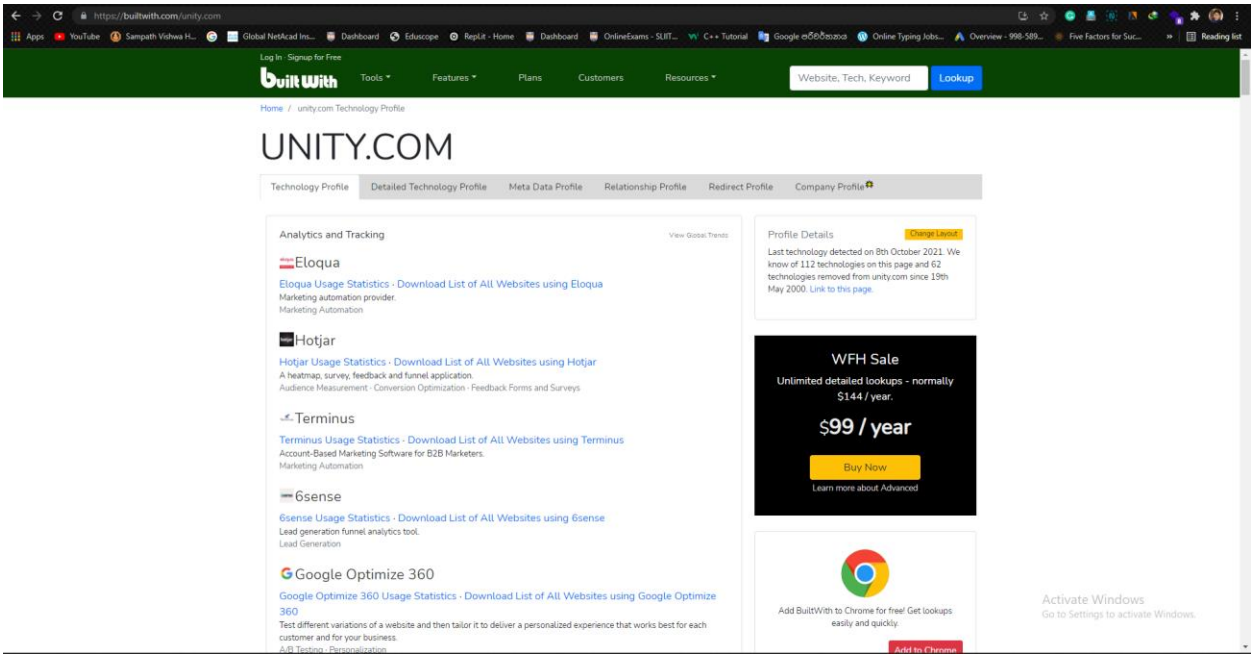


Figure 17 this site shows technologies that used in unity.com

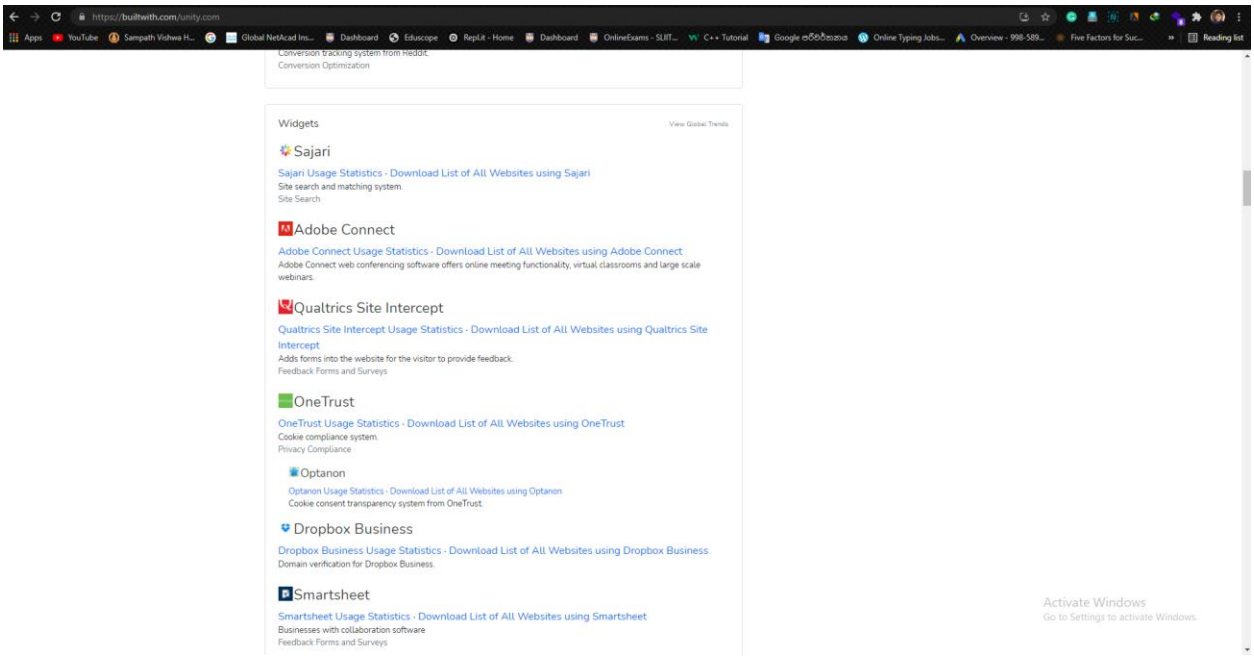


Figure 18 this site shows technologies that used in unity.com

Shodan

This provides information on all of the inter-connected devices inside the specified domain. If there is a public IP address that exposes a service on a certain port, then it will be listed in the Shodan database. Not only can we obtain the IP address, but we can also get web server data, banners, ISP, SSH, FTP, and other information.

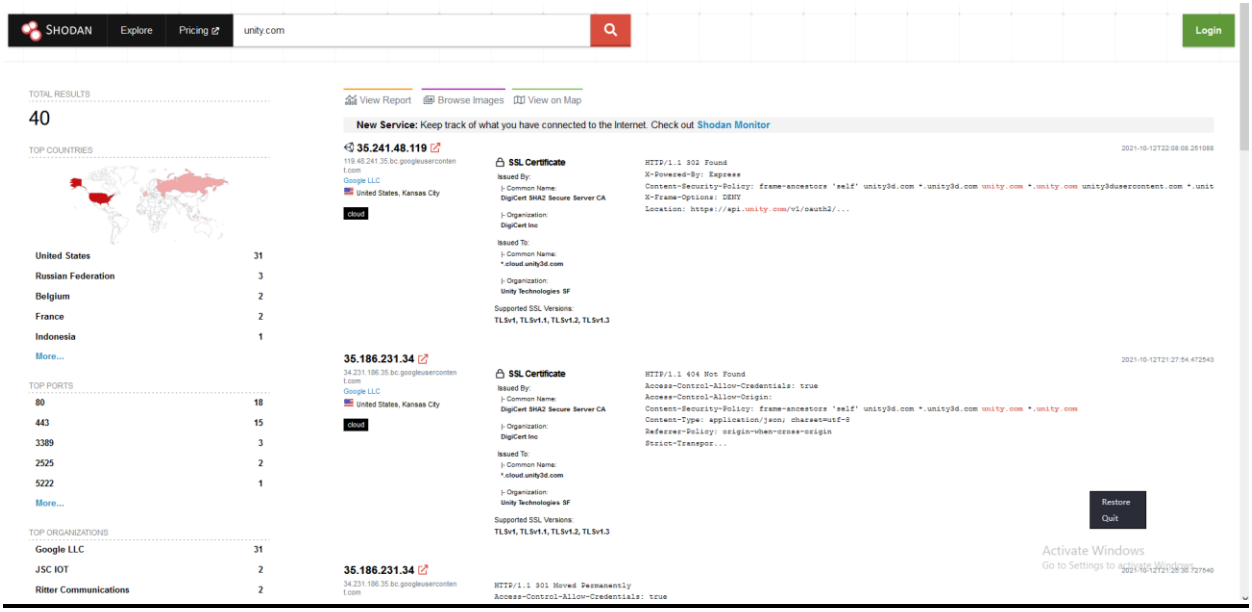


Figure 20 shodan shows interconnected devices to domain

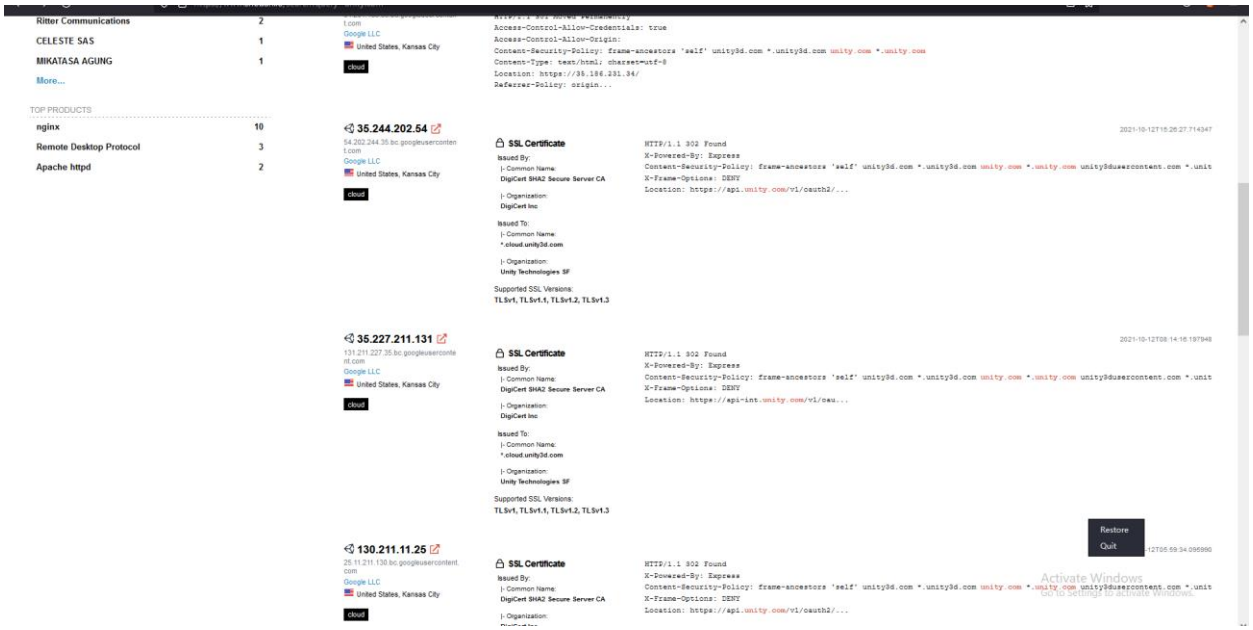


Figure 19 shodan shows interconnected devices to domain

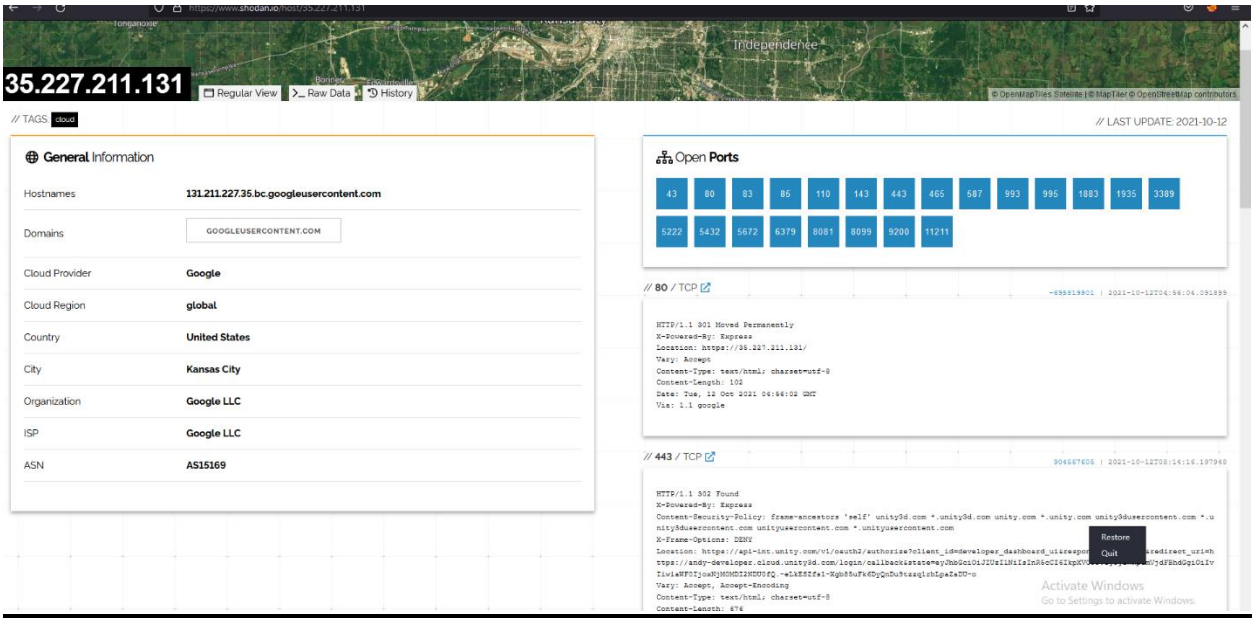


Figure 21 information about interconnected device and we can get information about open ports etc.

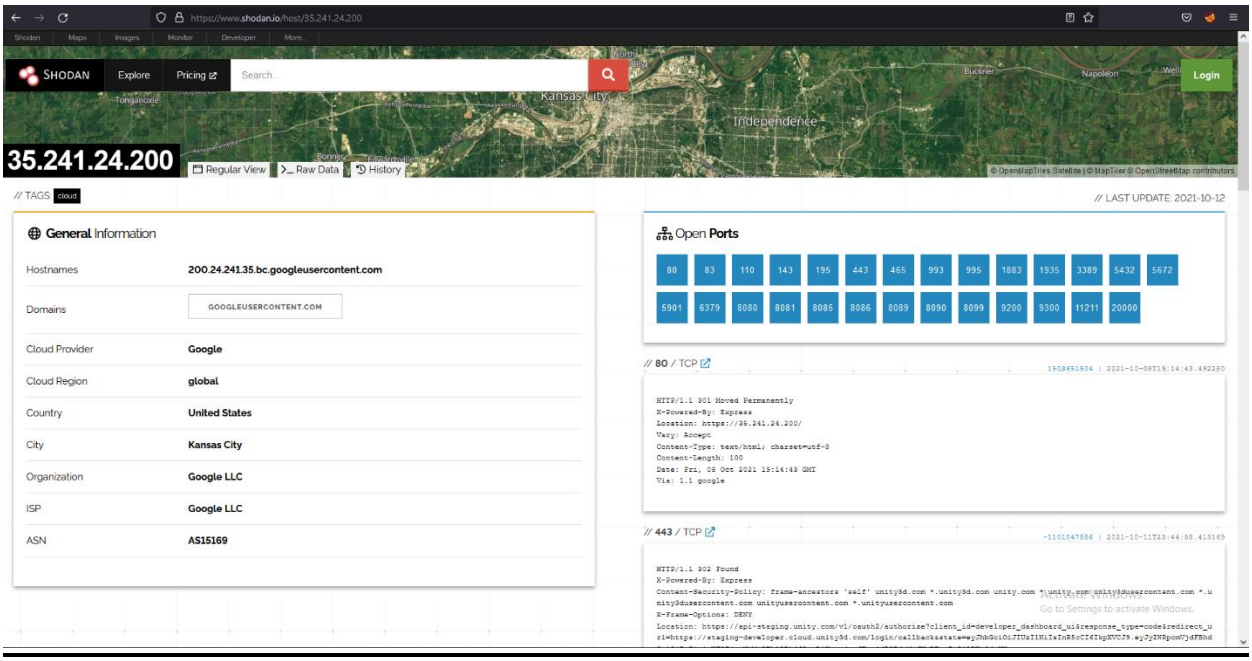


Figure 22 information about interconnected device and we can get information about open ports etc

Auditing and testing for Vulnerabilities

Nmap

Nmap ("Network Mapper") is a network discovery and security auditing tool that is free and open source (under the GNU General Public License). The tool is also helpful for many system and network managers for activities such as network inventory, managing service update schedules, and monitoring host or service uptime. What makes Nmap unique is that it makes use of raw IP packets in novel ways to determine what hosts are available on a network, what services (application name and version) those hosts are offering, what operating systems (and operating system versions) those hosts are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was created to scan huge networks quickly, although it is as effective when scanning a single host.

we can find about hosts, open ports, services etc. I did this Nmap scanning all subdomains also.

www.unity.com

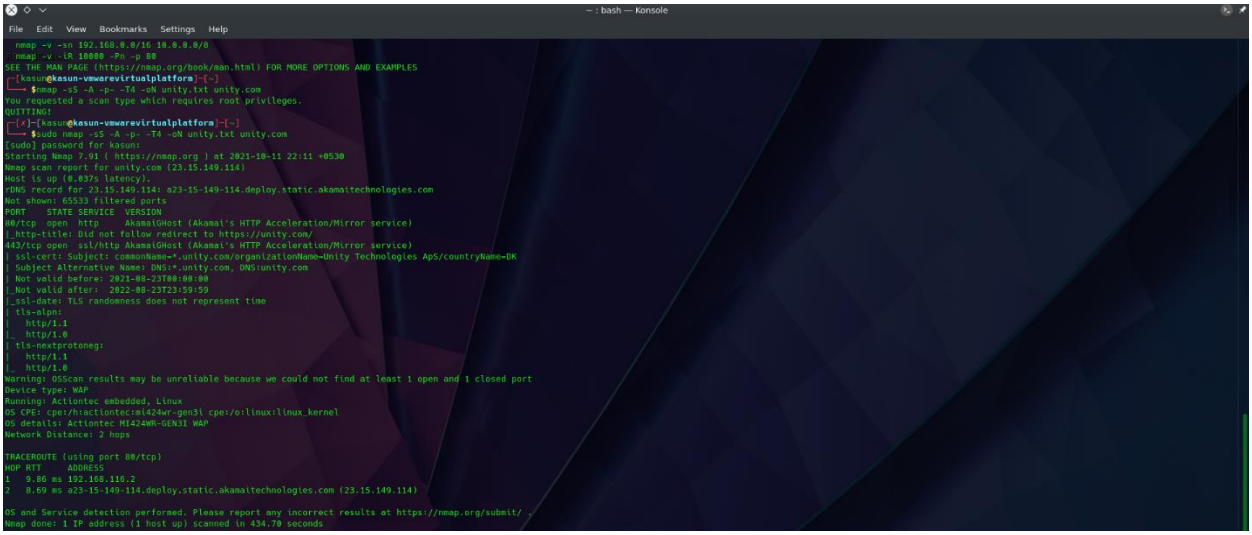


Figure 23 I nmap scan for unity.com this figure shows its output.

Id.unity.com

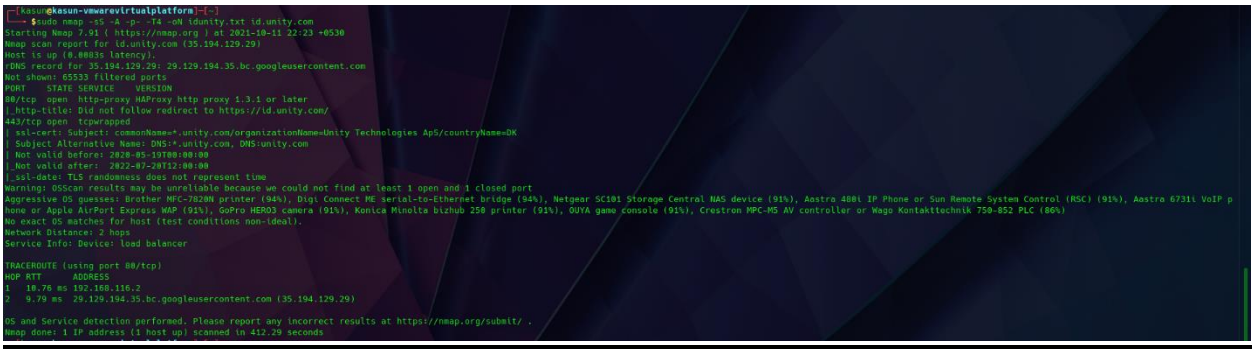


Figure 24 nmap scan for id.unity.com this figure shows its output I could not find open ports by scanning this domain.

Analytics.cloud.unity.com

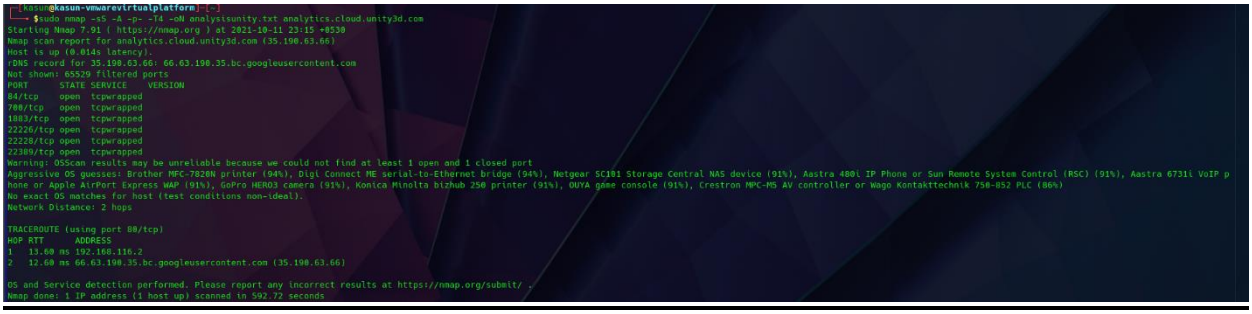


Figure 25 nmap scan for analytics.cloud.unity.com this figure shows its output I could not find open ports by scanning this domain.

pay.unity.com

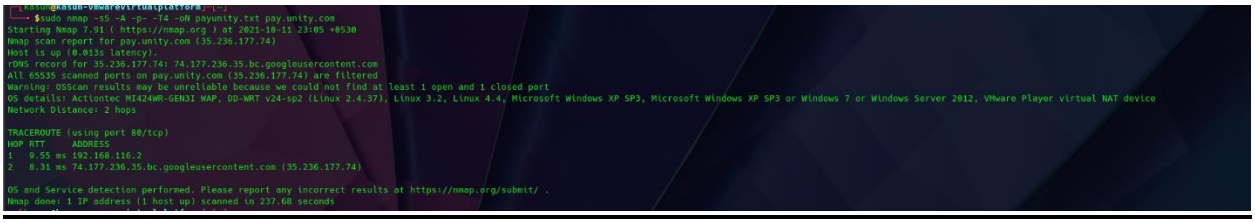
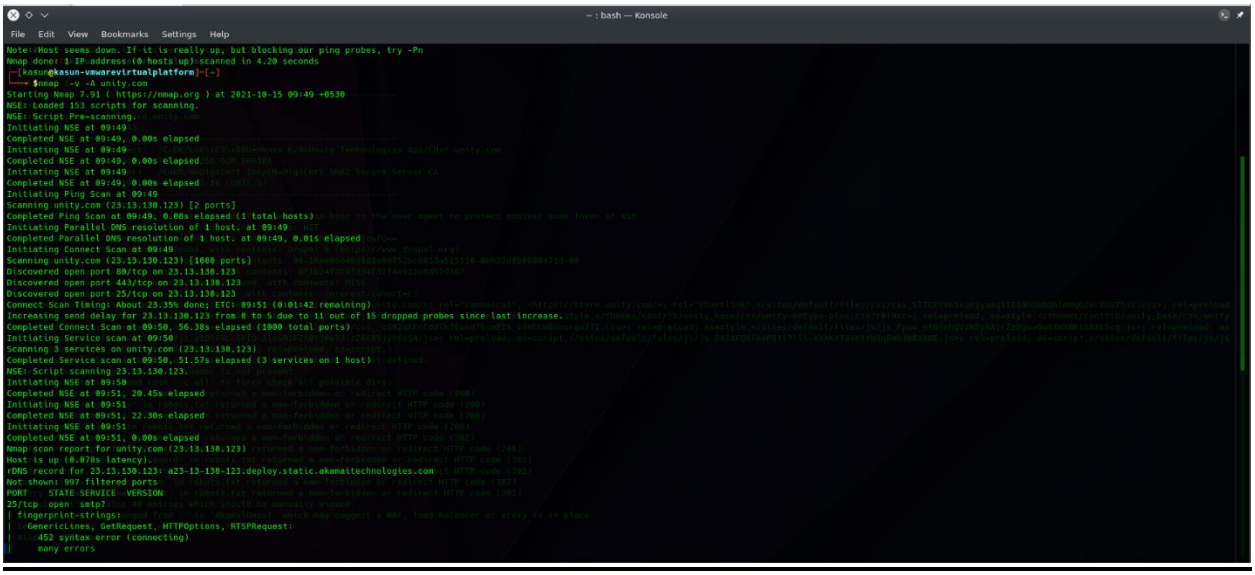
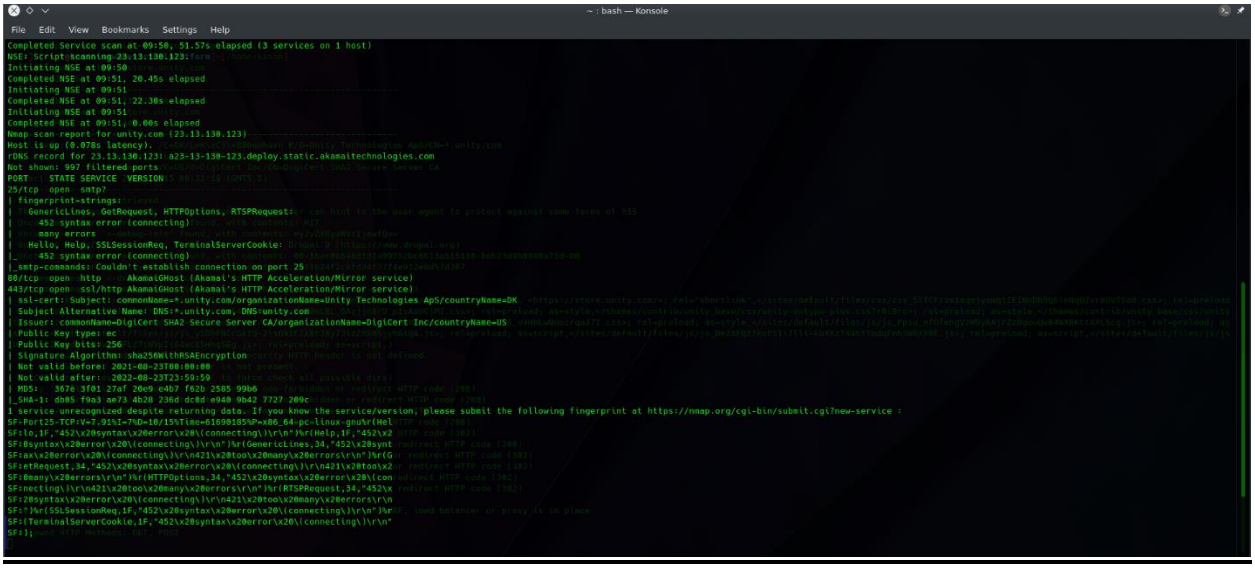


Figure 26 nmap scan for pay.unity.com this figure shows its output I could not find open ports by scanning this domain.

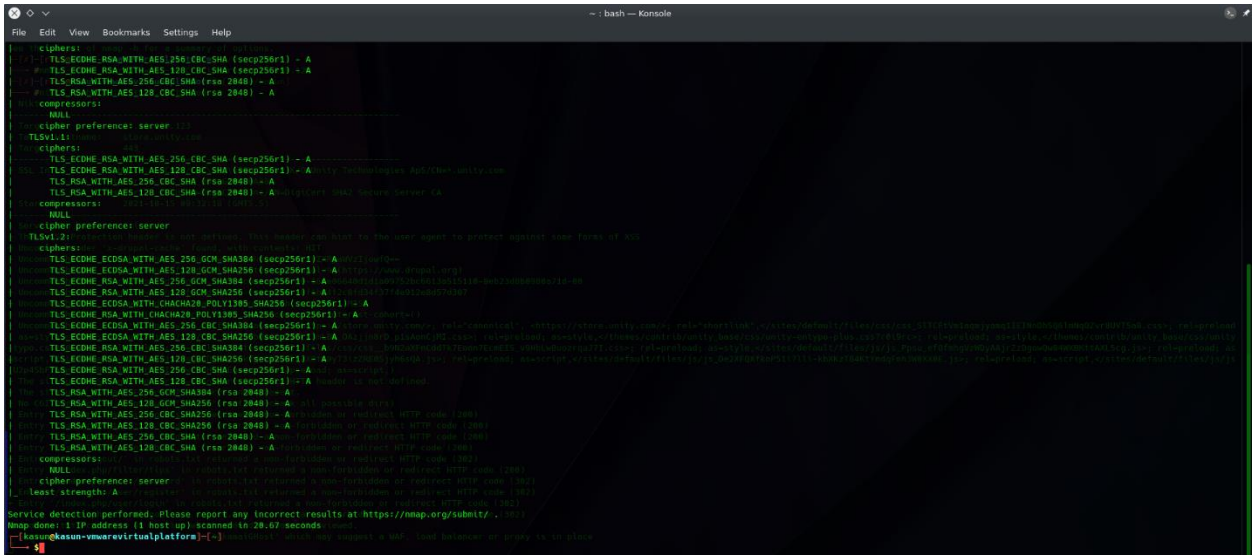
I scanned more and more about unity.com by using nmap tool.





Store.unity.com is a most important domain in unity.com therefore I did nmap scan for identify about their ciphers that they are using .

Nmap -sV –script ssl-enum-ciphers -p 443 (host)



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

Burp Suite

Burp Suite is a Web Penetration Testing framework that is built on Java. This set of tools, used by information security experts across the world, has become an industry standard. You may use Burp Suite to discover web application vulnerabilities as well as attack vectors that are impacting the online application. There are primarily two versions of burp suite available: the Community Edition and the Professional Edition. I've utilized the professional edition for this section.

I have performed a thorough scan, which included crawling all of their pertinent domain contents. Professional customers may choose from three different configurations, while the community version offers just two configurations. Auditing and crawling for professionals is available. I used the web crawling technique in this instance because I needed to search the whole domain contents in order to collect some sensitive information.

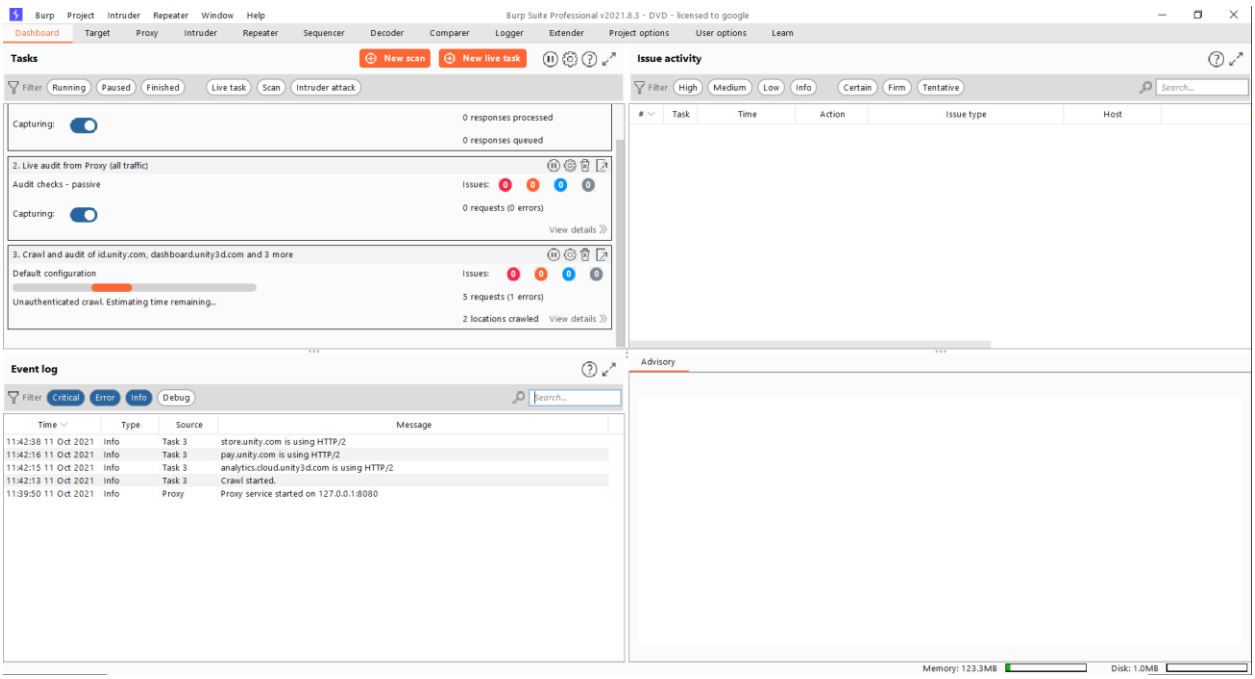


Figure 27 strating burp with crawl and audit

When the crawling process begins, a large number of content files from target lists are analyzed. As a result, we can observe a large number of security vulnerabilities being captured by the crawling process.

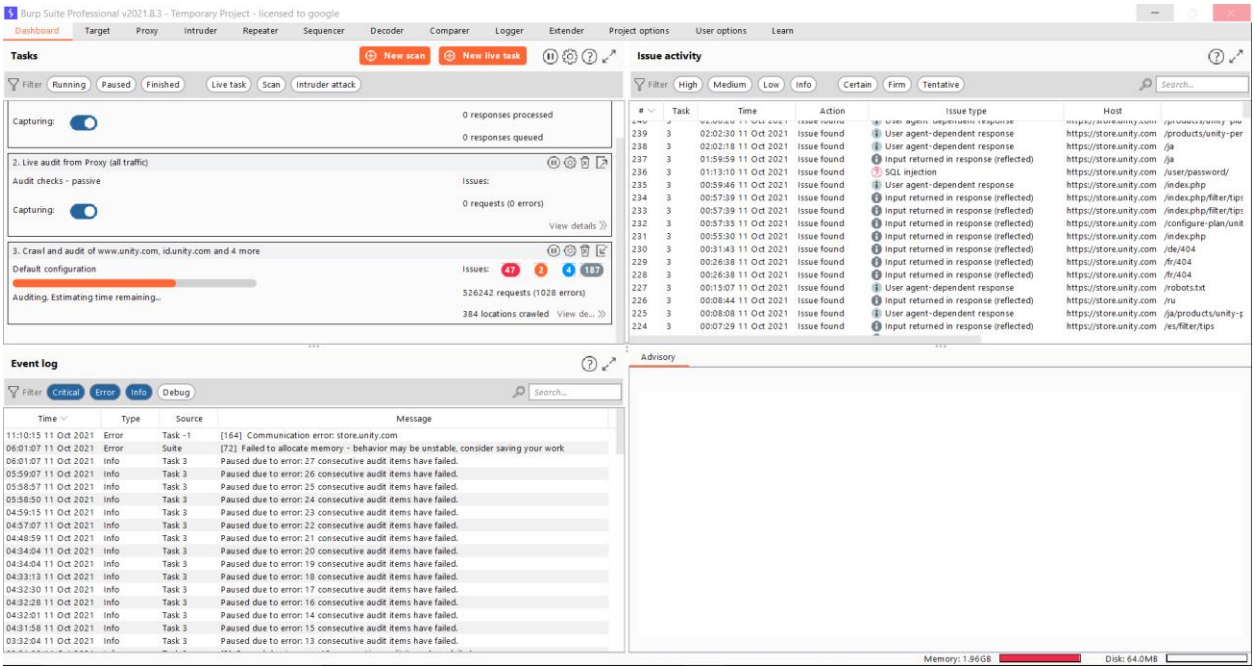


Figure 28 output after 6 hours in burp I could find 47 issues by this scan most of them are common vulnerabilities

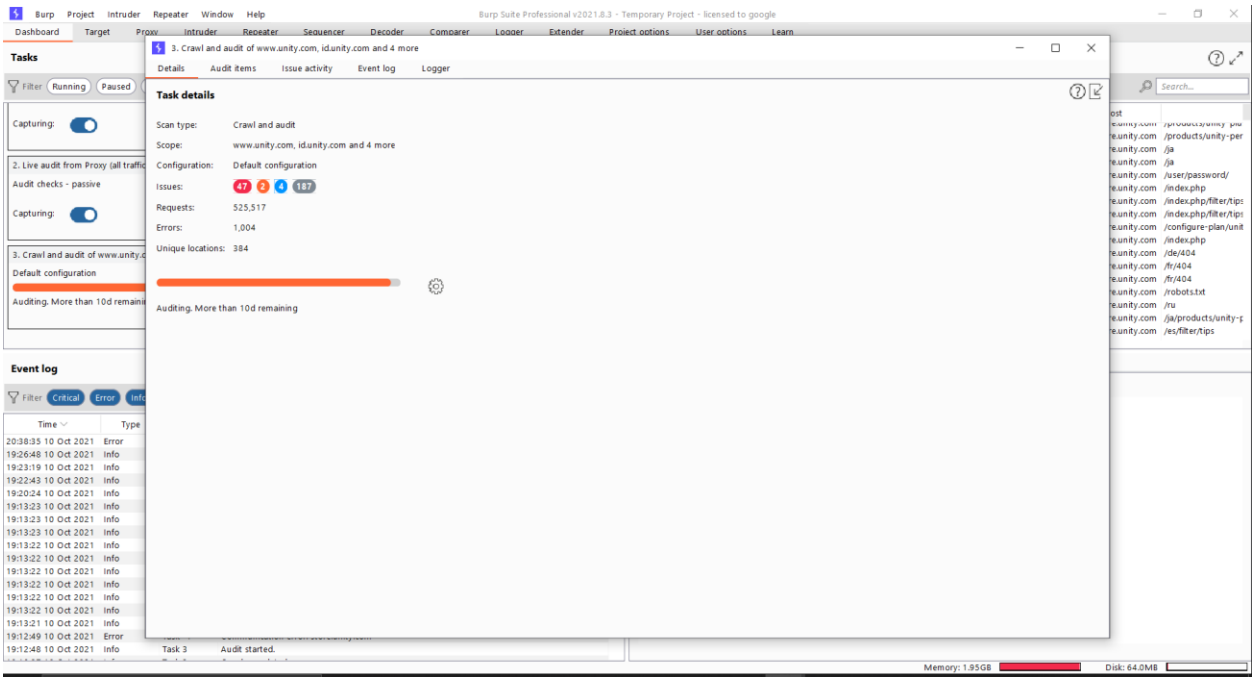


Figure 29 after 525,517 requests results I have got by burp suite scanning

I found bunch of issues from this tool but this tool takes more resources so I could not do the whole auding because out of memory I could 80% I found many issues related all domains.

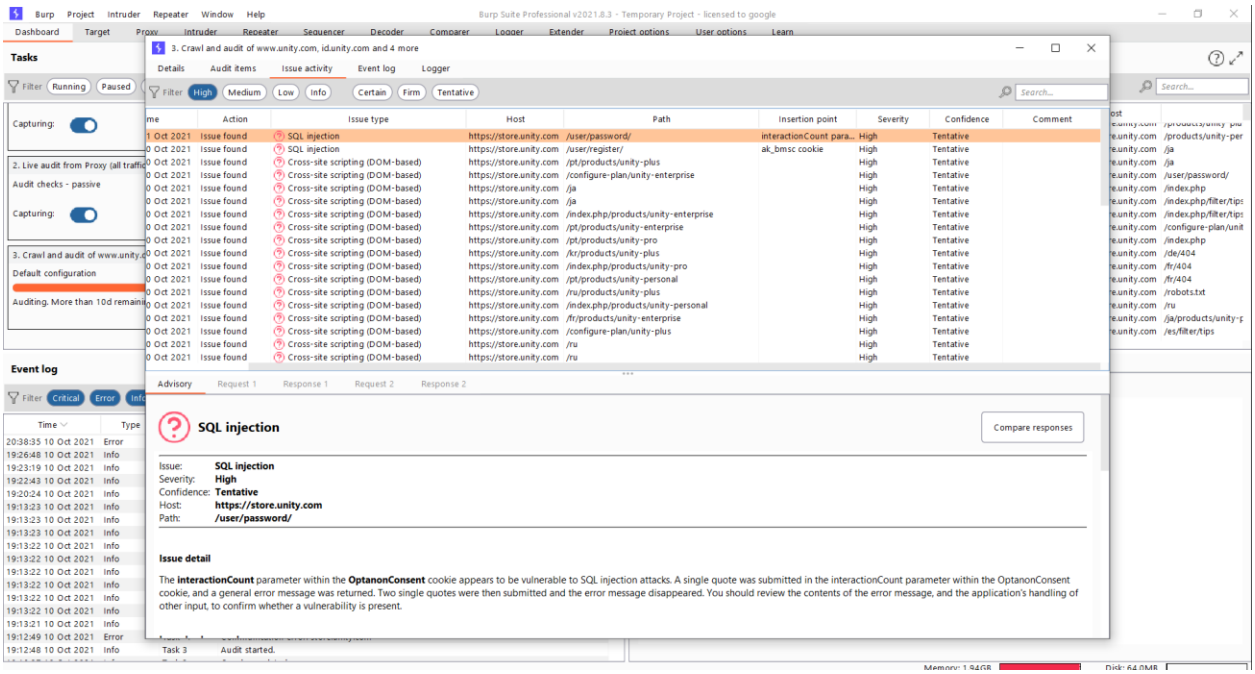


Figure 30 issues that I have found by burp suite scanning

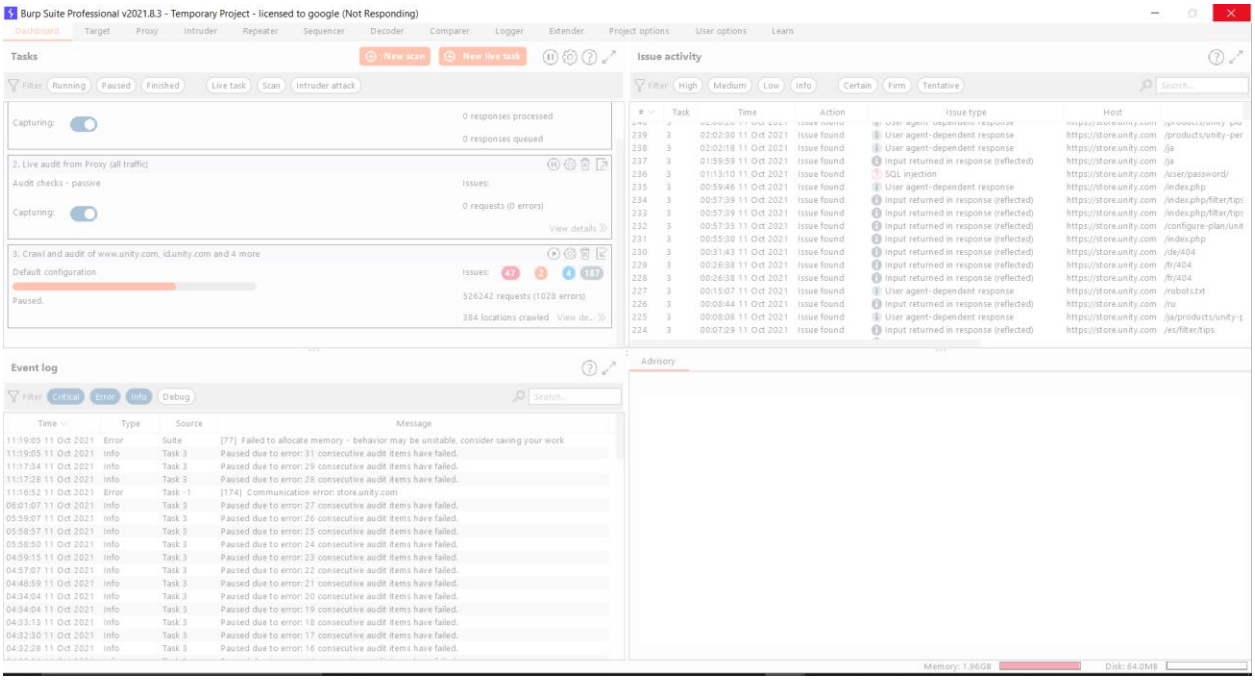


Figure 31 after 10 hours there are out of memory allocation therefore burp suite scanning was got error it was not responded.

Nikto Scanner

Nikto is a security application that scans a website for hundreds of potential security flaws. The Nikto web server scanner is available for free. This includes potentially hazardous files, incorrectly setup services, susceptible scripts, and other problems. It is free and open source, and it is organized using plugins that allow you to expand its features. These plugins are regularly updated with new security tests to keep them up to date.

To perform a basic scan against the target, the command "nikto -h http://www.unity.com" is entered into the terminal. I use parrot OS for security pen testers therefore ,Nikto tool is already installed in system.

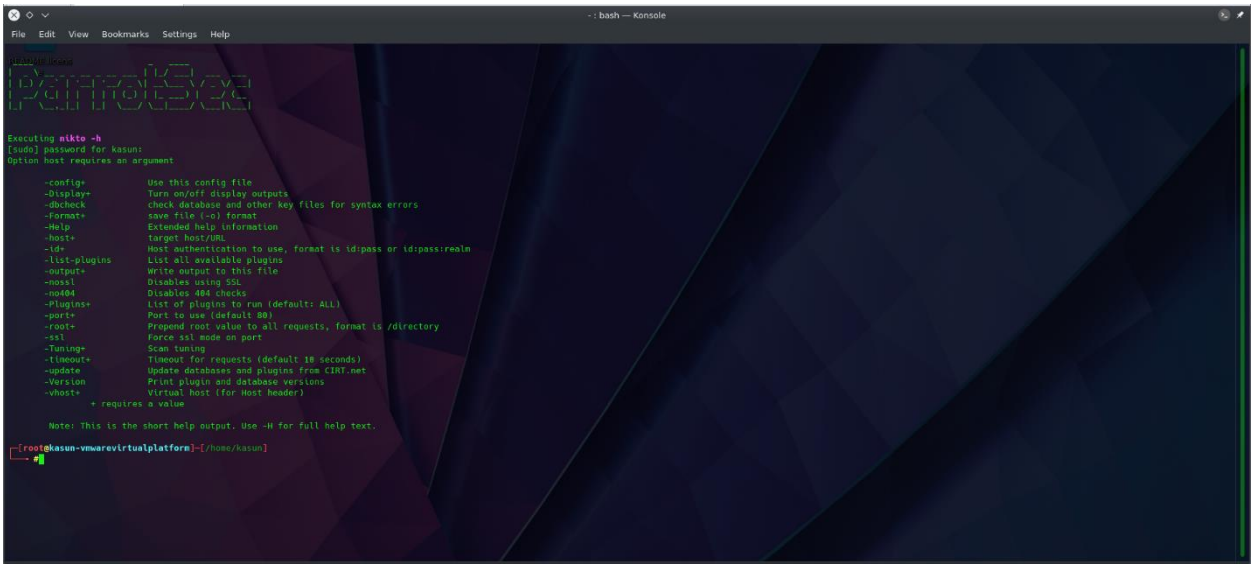


Figure 32 nikto interface and by this we can get some idea about commands

www.unity.com

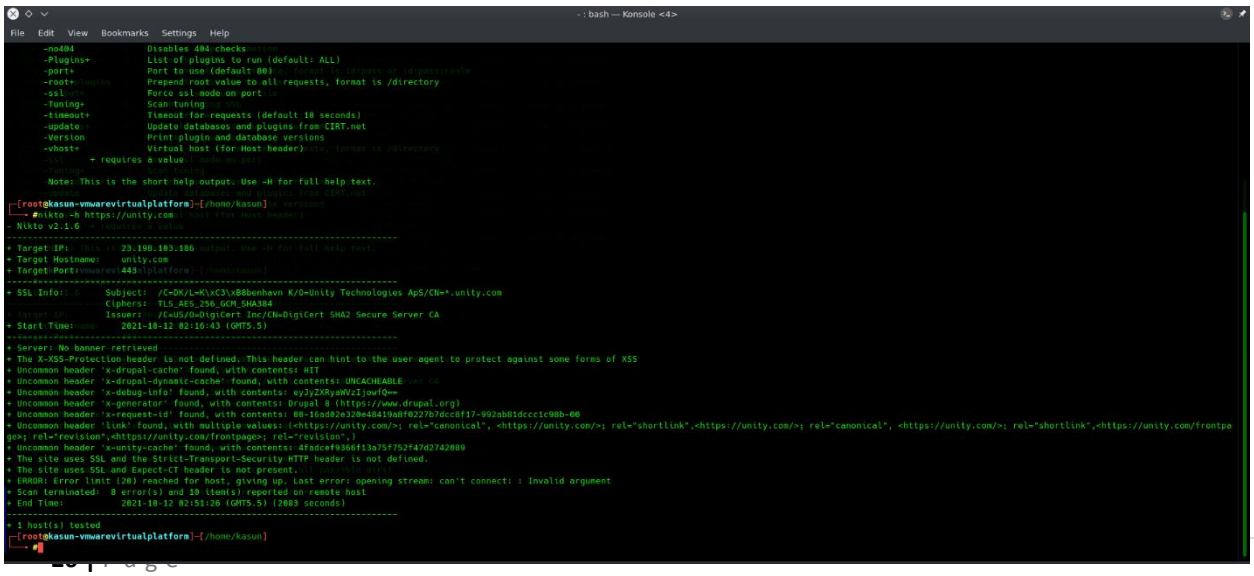


Figure 33 I scanned unity.com by nikto scan this figure shows some vulnerabilities of unity.com domain.

id.unity.com

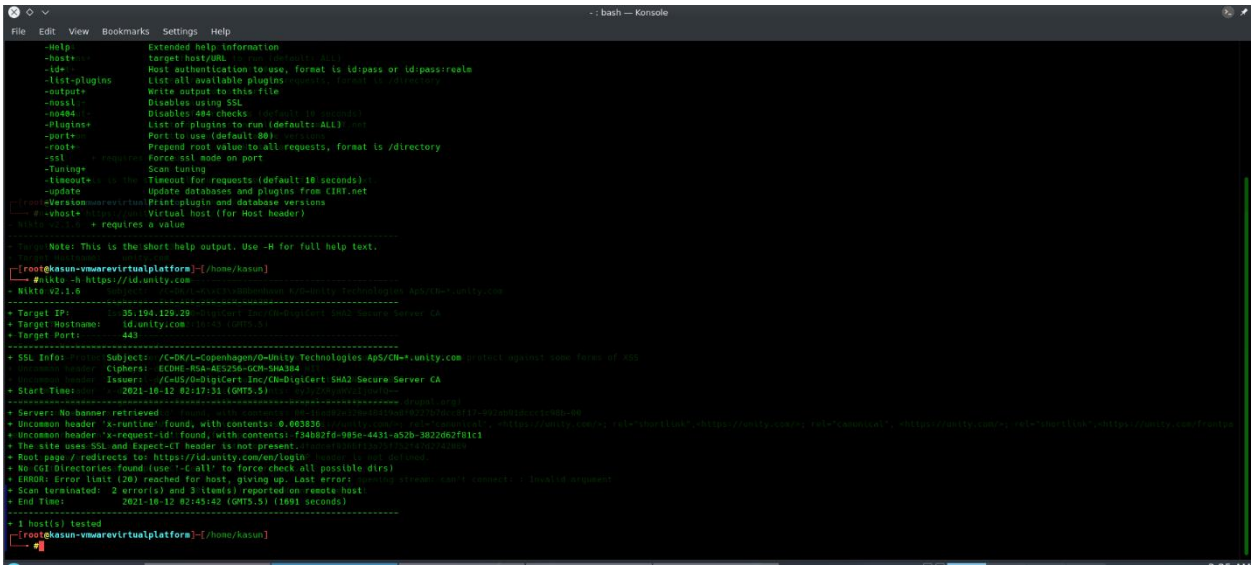


Figure 34 I scanned id.unity.com by nikto scan this figure shows some vulnerabilities of id.unity.com domain.

dashboard.unity3d.com

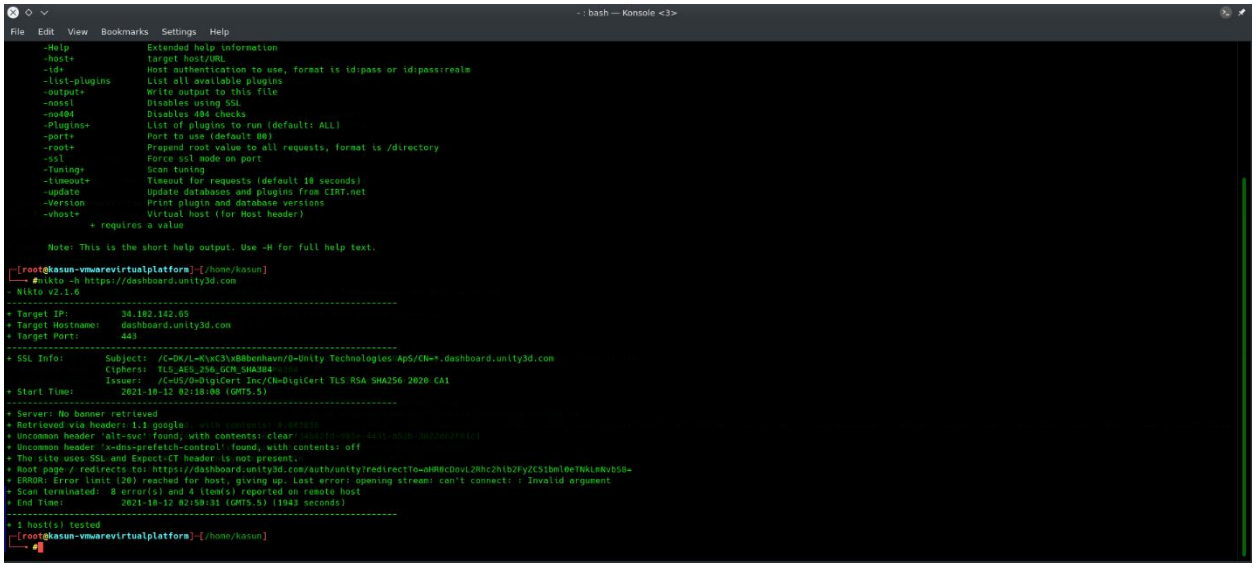
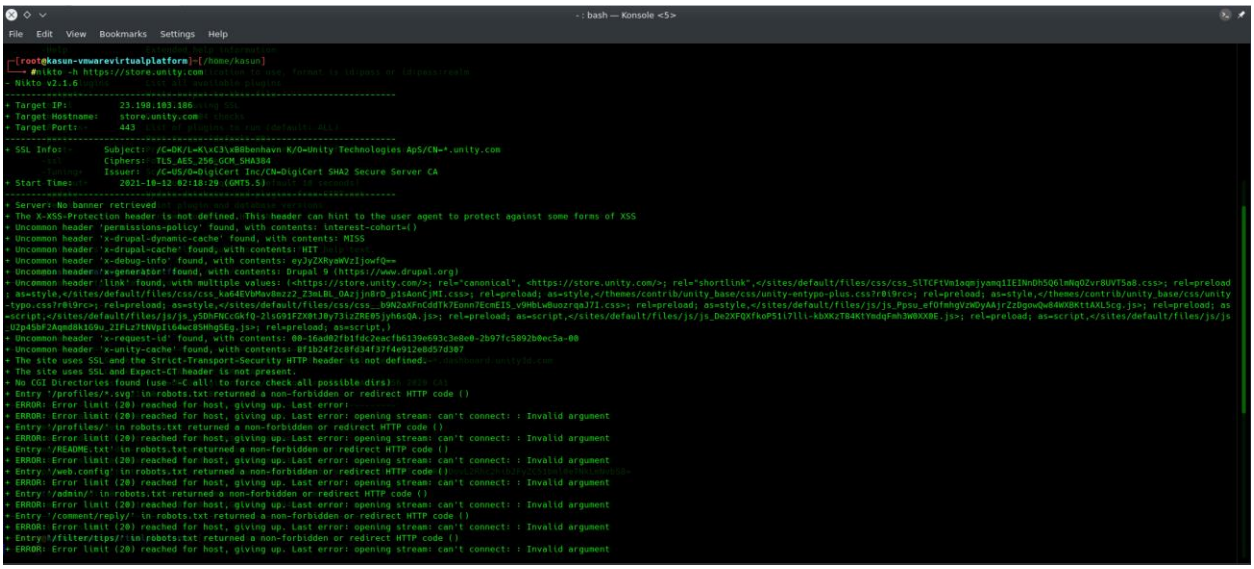


Figure 35 I scanned dashboard.unity.com by nikto scan this figure shows some vulnerabilities of domain.

store.unity.com



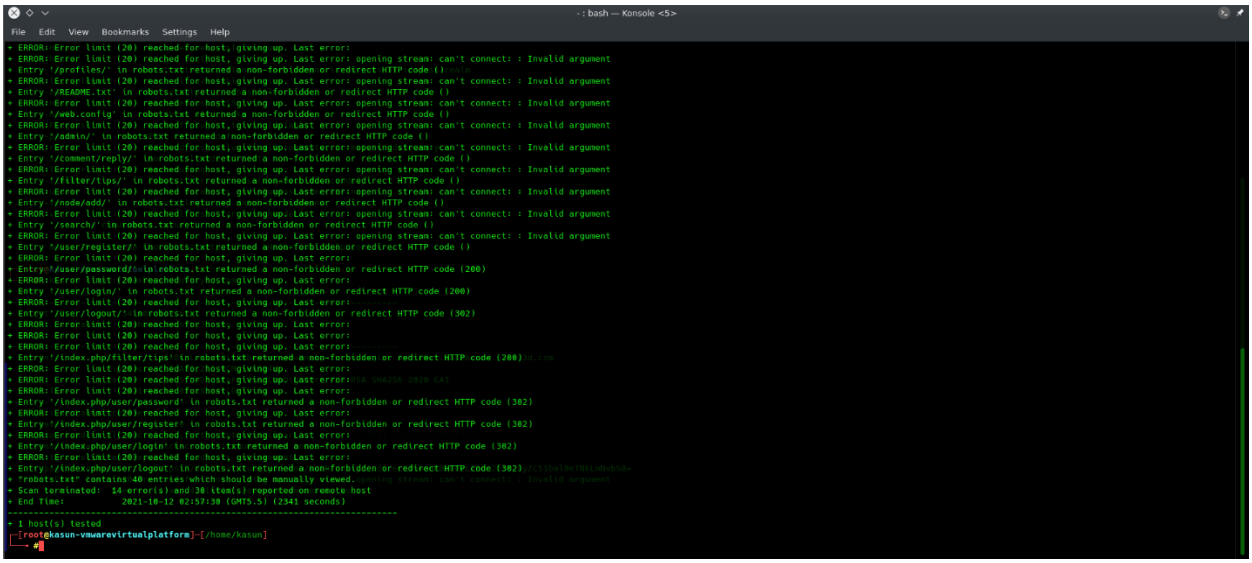


Figure 36 I scanned store.unity.com by nikto scan this figure shows some vulnerabilities of unity.com domain.

pay.unity.com

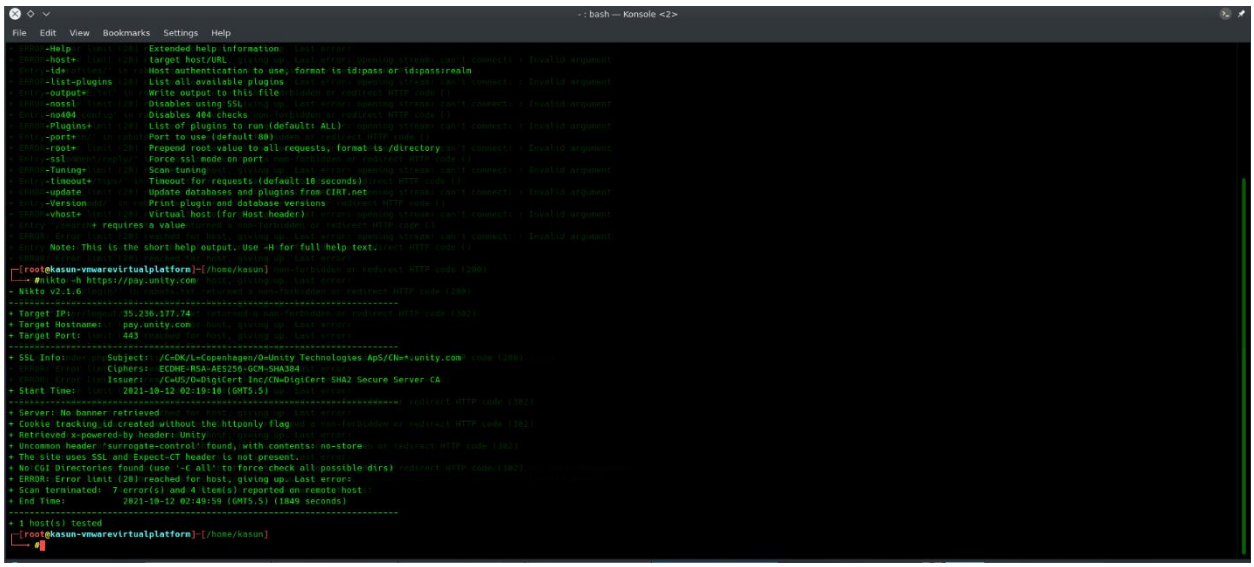


Figure 37 I scanned pay.unity.com by nikto scan this figure shows some vulnerabilities of domain.

Wafw00f

This tool is a python based tool which we can use for identify and fingerprint Web Application Firewall (WAF) products protecting a website.

I tested all in scope domains which bugcrowd provided and I got some information about firewalls which behind all the domains. Wafw00f shows the firewalls which the tool can identified. There can be a firewall or not .

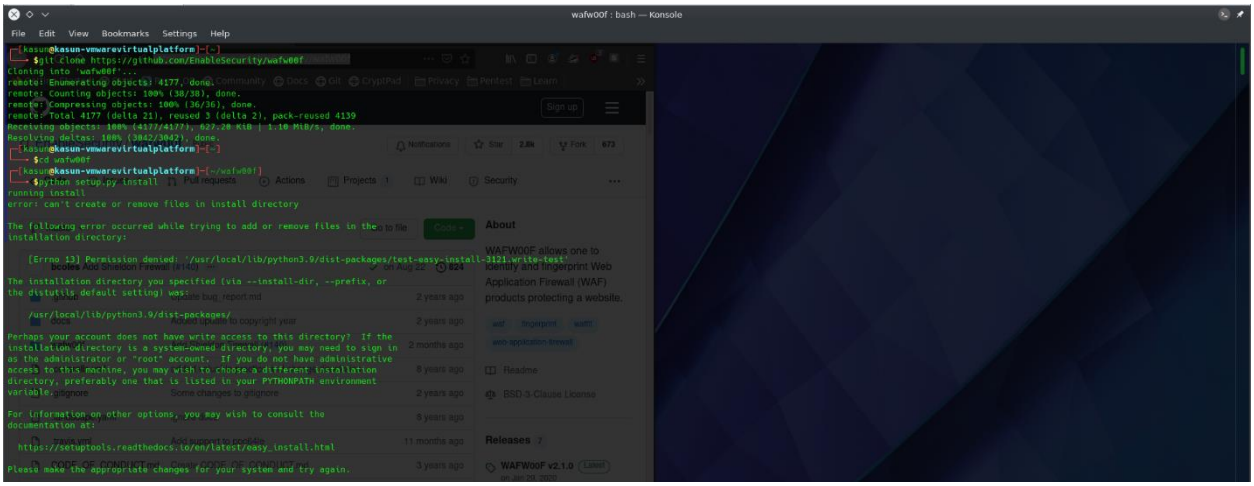


Figure 38 installation of wafw00f tool for scanning firewalls behind domains.

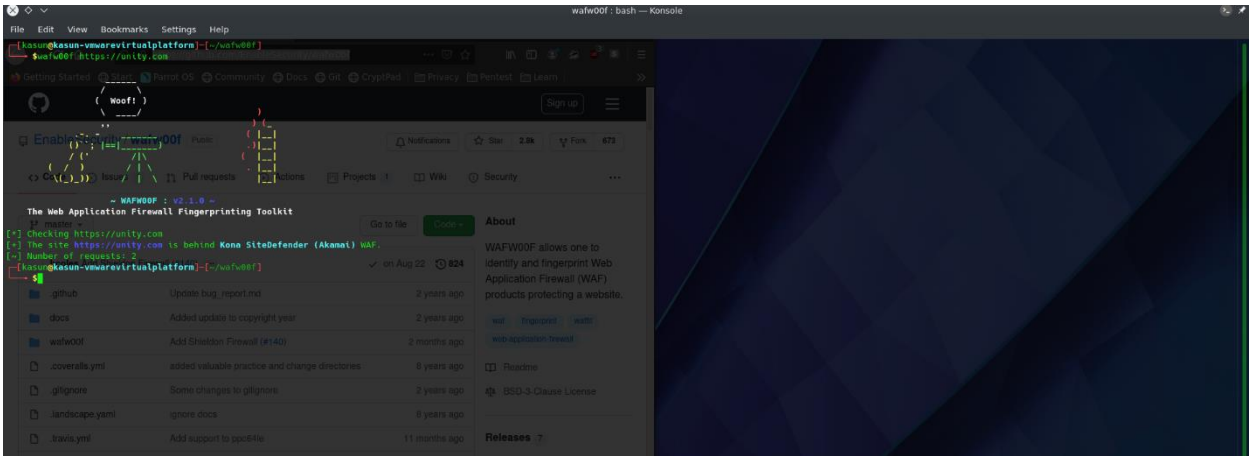


Figure 39 I scanned unity.com by wafw00f tool and I found a firewall behind the domain

id.unity.com

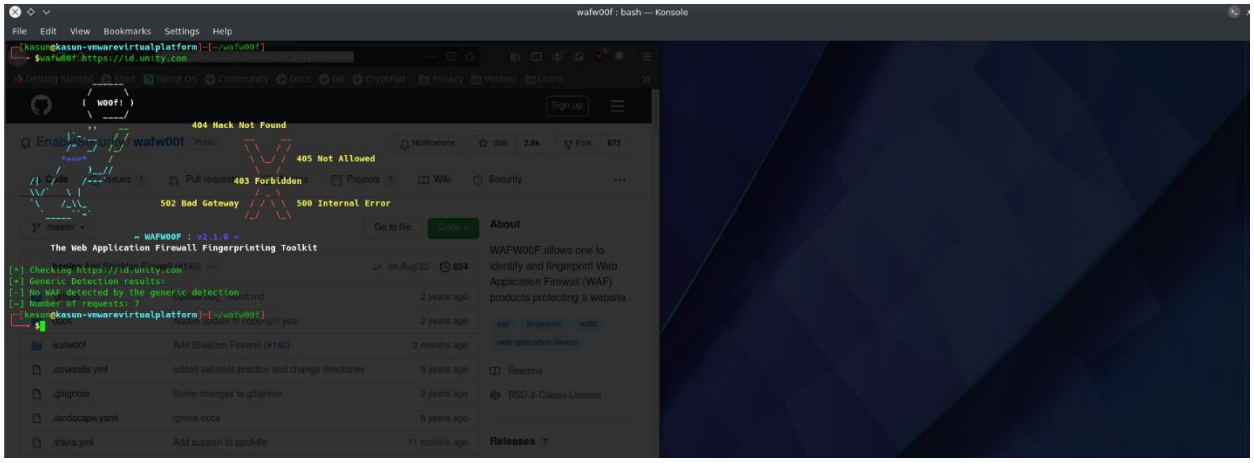


Figure 40 I scanned unity.com by wafw00f tool and I could not find a firewall behind the domain but there can be a firewall or not .tool could not find a firewall after scanning the domain

dashboard.unity3d.com

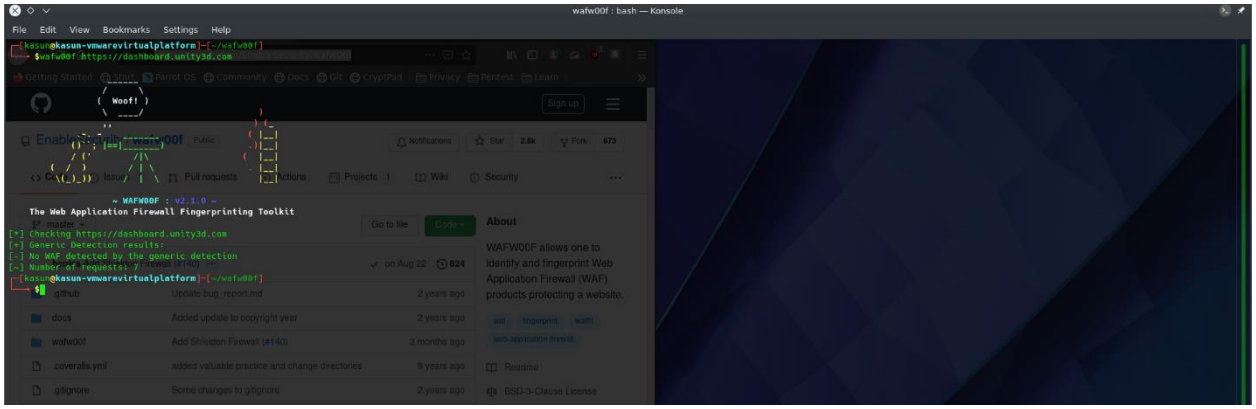


Figure 41 I scanned dashboard.unity.com by wafw00f tool and I could not find a firewall behind the domain but there can be a firewall or not .tool could not find a firewall after scanning the domain

store.unity.com

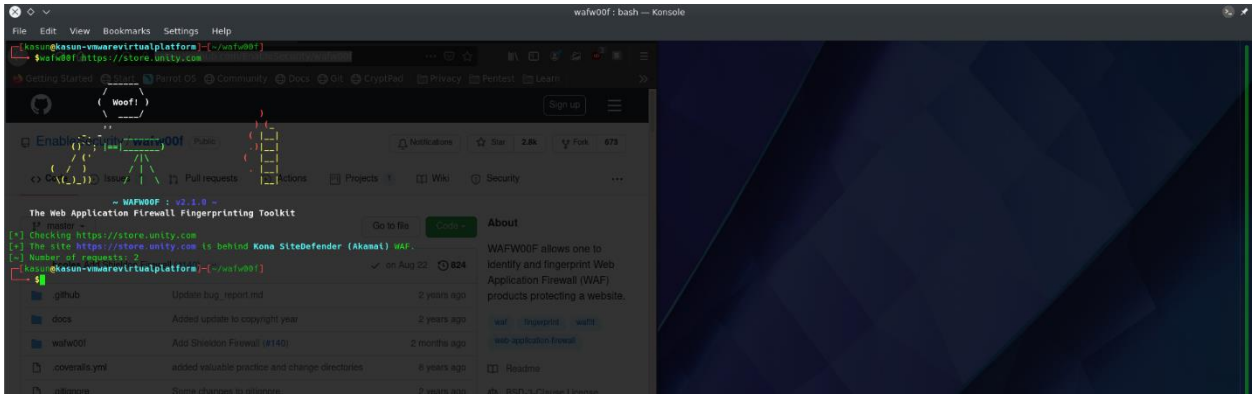


Figure 42 I scanned store.unity.com by wafw00f tool and I found a firewall behind the domain

pay.unity.com

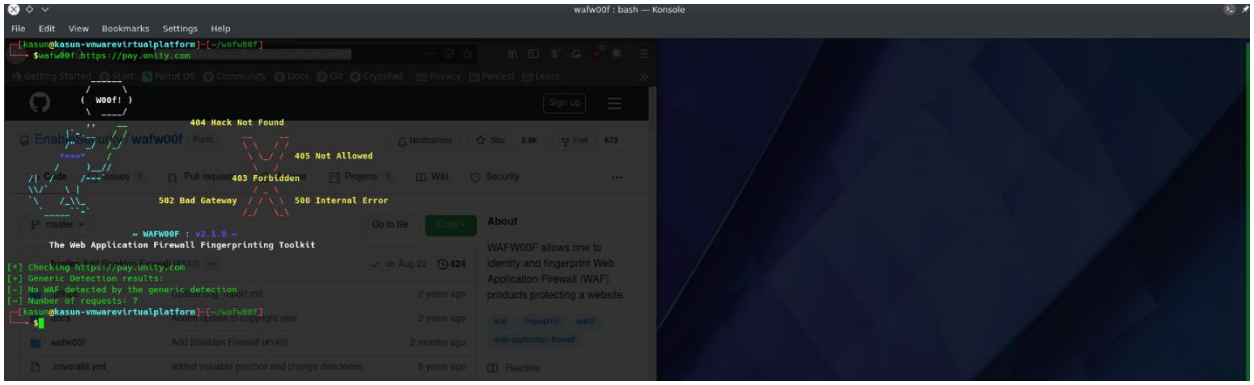


Figure 43 I scanned pay.unity.com by wafw00f tool and I could not find a firewall behind the domain but there can be a firewall or not .tool could not find a firewall after scanning the domain

analytics.cloud.unity3d.com

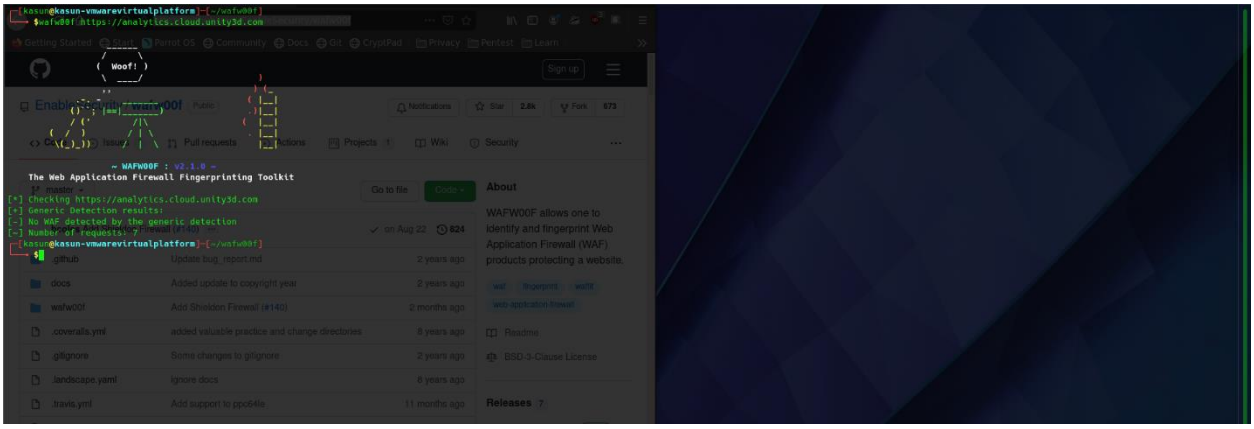


Figure 44 I scanned dashboard.unity.com by wafw00f tool and I could not find a firewall behind the domain but there can be a firewall or not .tool could not find a firewall after scanning the domain

OWASP ZAP

OWASP ZAP is a web application security scanner that is free and open-source. Because of this, it is intended for both beginners in application security and seasoned penetration testers seeking to sharpen their abilities. Open Web Application Security Project sponsors have named it a Flagship project, making it one of the most engaged.

I scanned main domain and 5 domains one by one by the tool.

www.unity.com

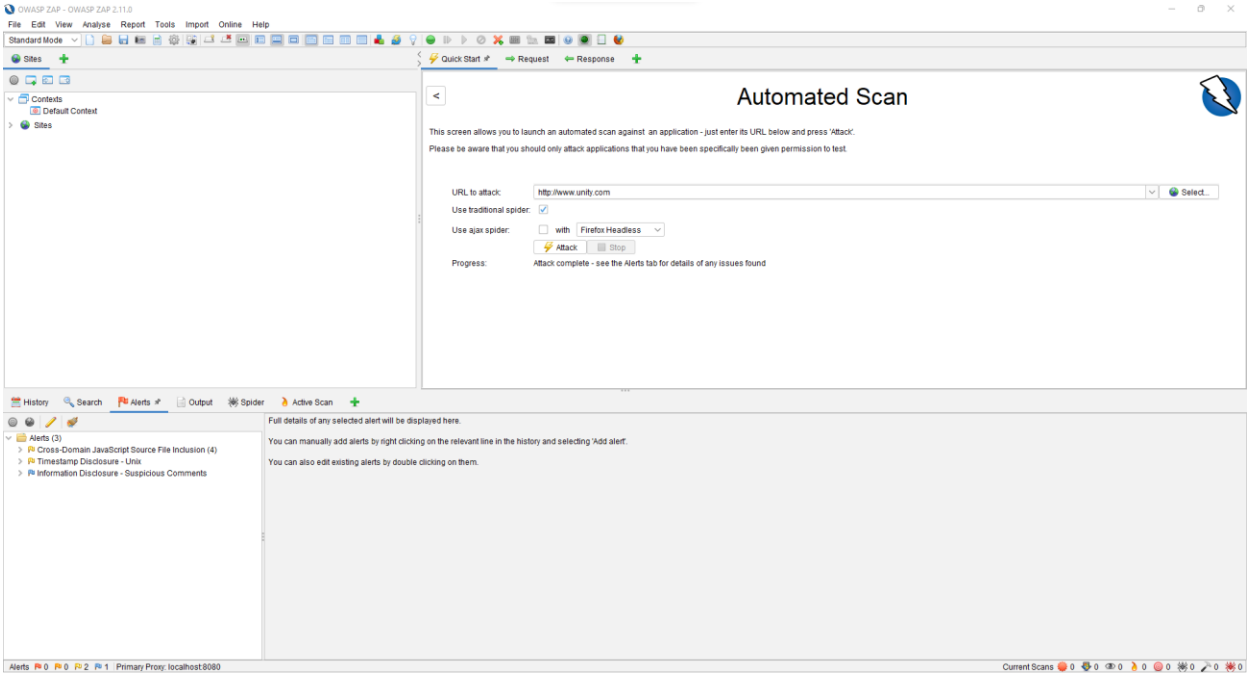


Figure 45 I scanned unity.com by owasap zap and I got 3 alerts after scanning whole site .

id.unity.com

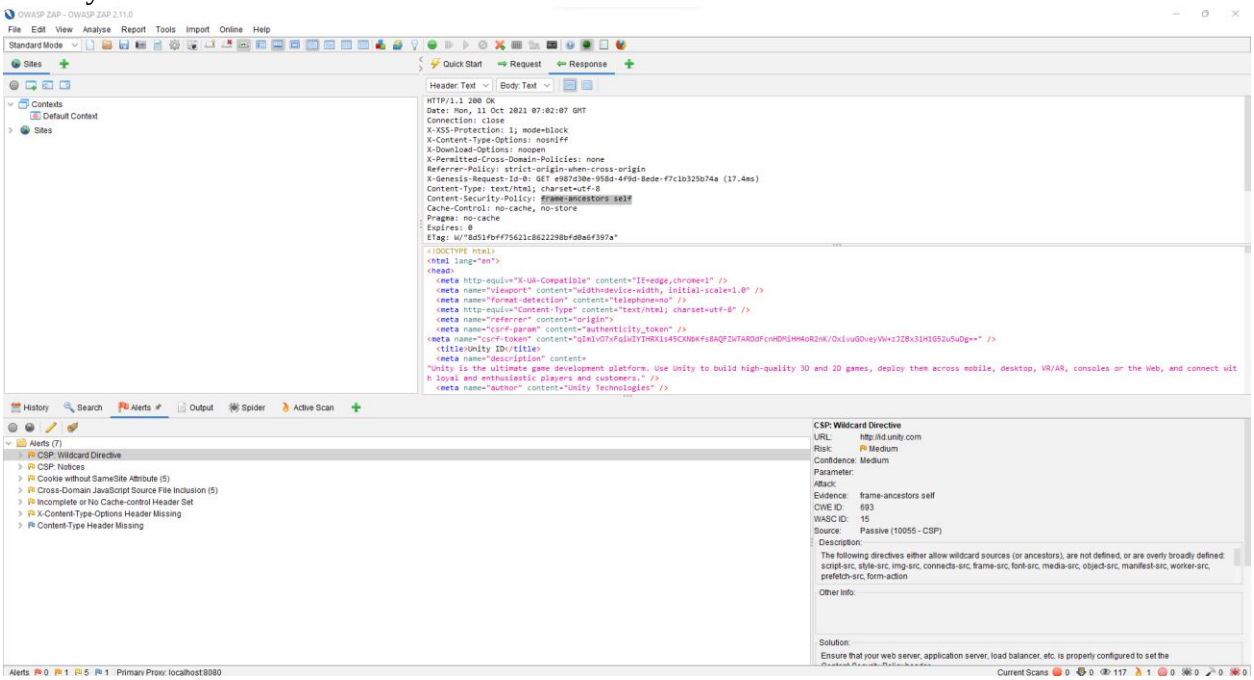


Figure 46 I scanned id.unity.com by owasap zap and I got 7 alerts after scanning whole domain .

dashboard.unity3d.com

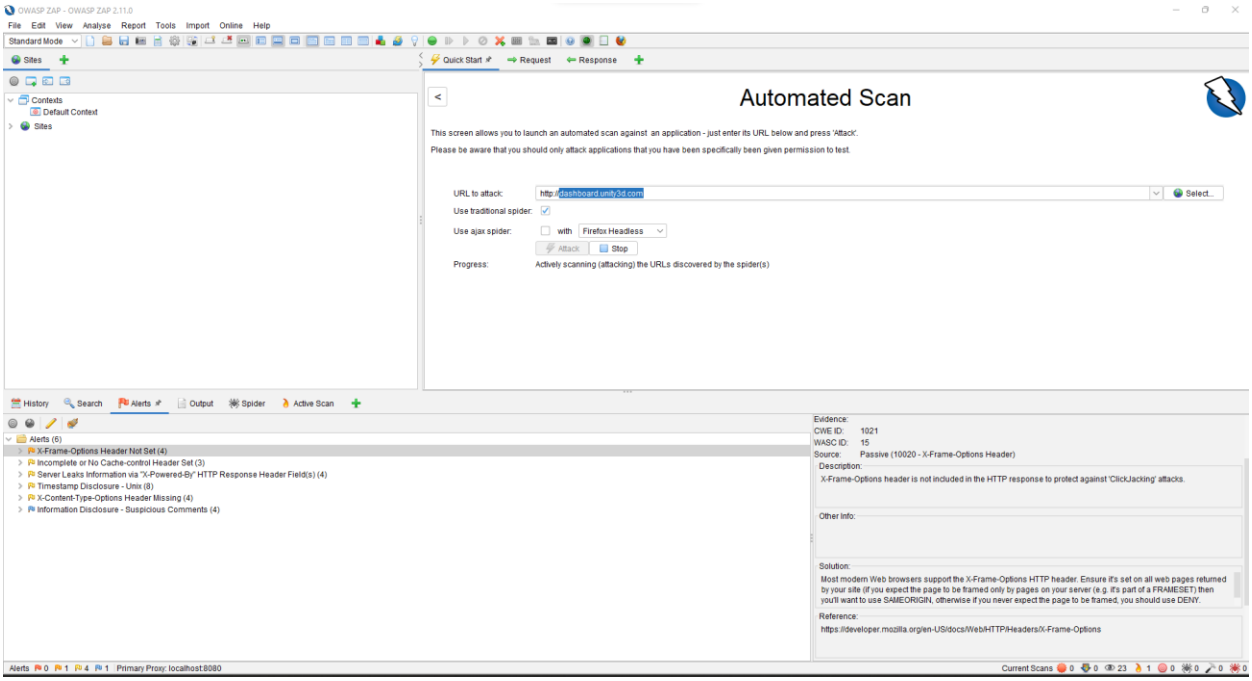


Figure 47 I scanned dashboard.unity.com by owasap zap and I got 3 alerts after scanning whole site .

Store.unity.com

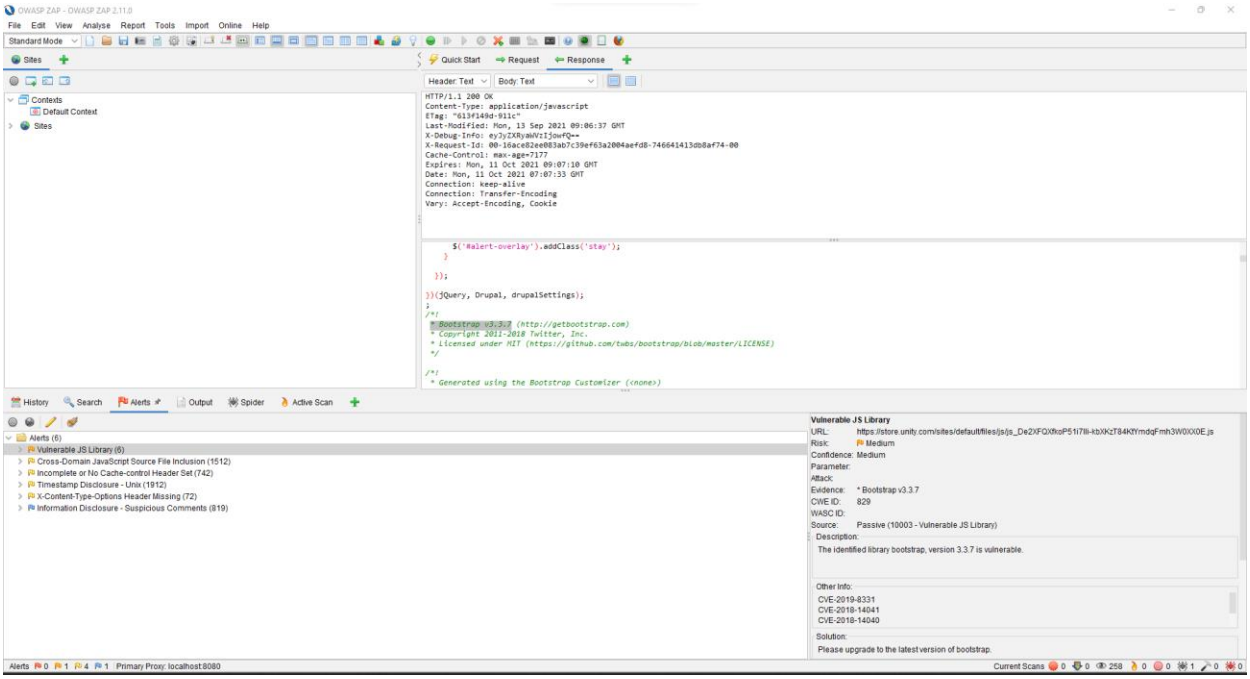


Figure 48 I scanned store.unity.com by owasp zap and I got 6 alerts after scanning whole domain .

analytics.cloud.unity3d.com

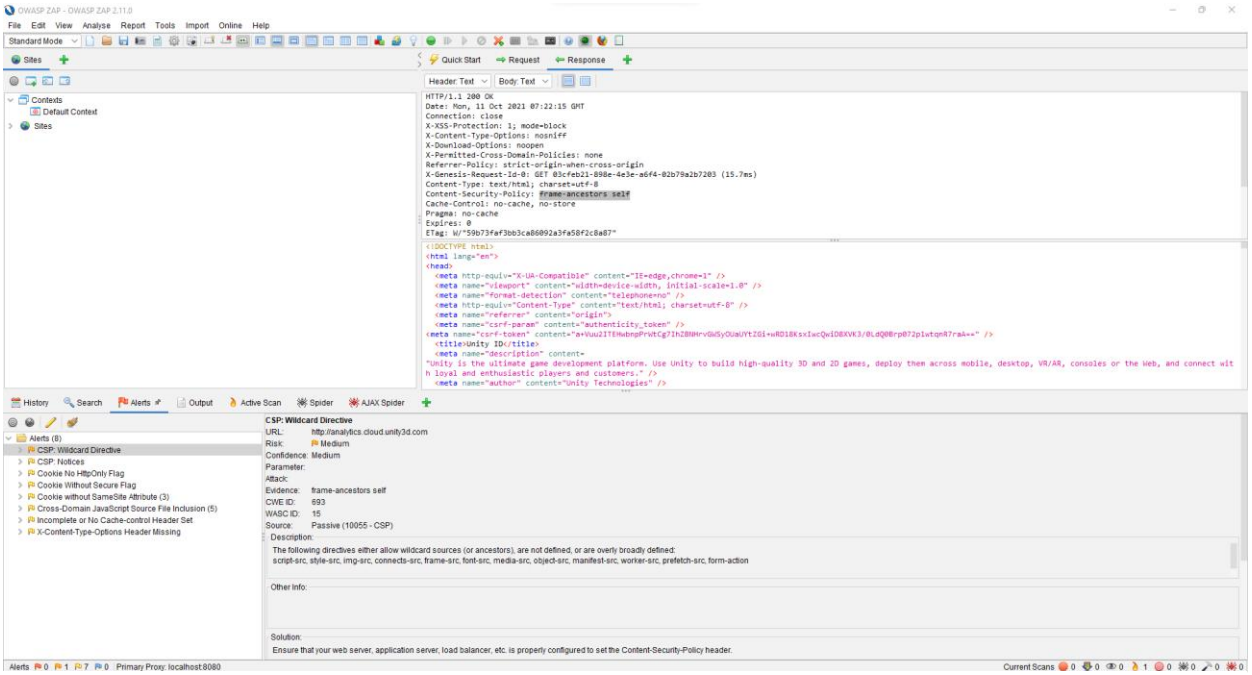


Figure 49 I scanned analytics.cloud.unity.com by owasp zap and I got 8 alerts after scanning whole domain .

Netspaker

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 scanner detects the following kinds of vulnerabilities

- 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

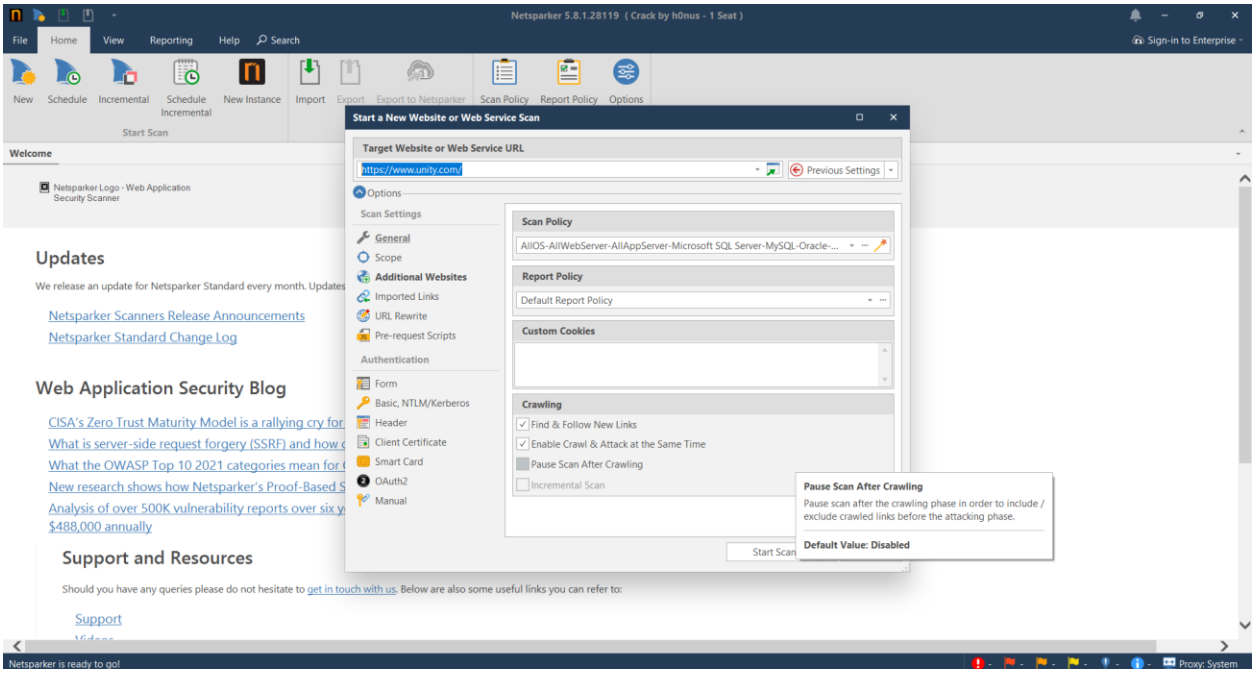


Figure 50 interface of netspaker tool

I scanned main domain and other 5 sub domains by this netspaker tool. In this netstat window, you may view information such as a comprehensive panel sitemap, problems, progress, and so on. As a result, we may control how many requests are granted to our target domain. It is possible to do this using a progress panel. I've got a number of high-level threats in domains.

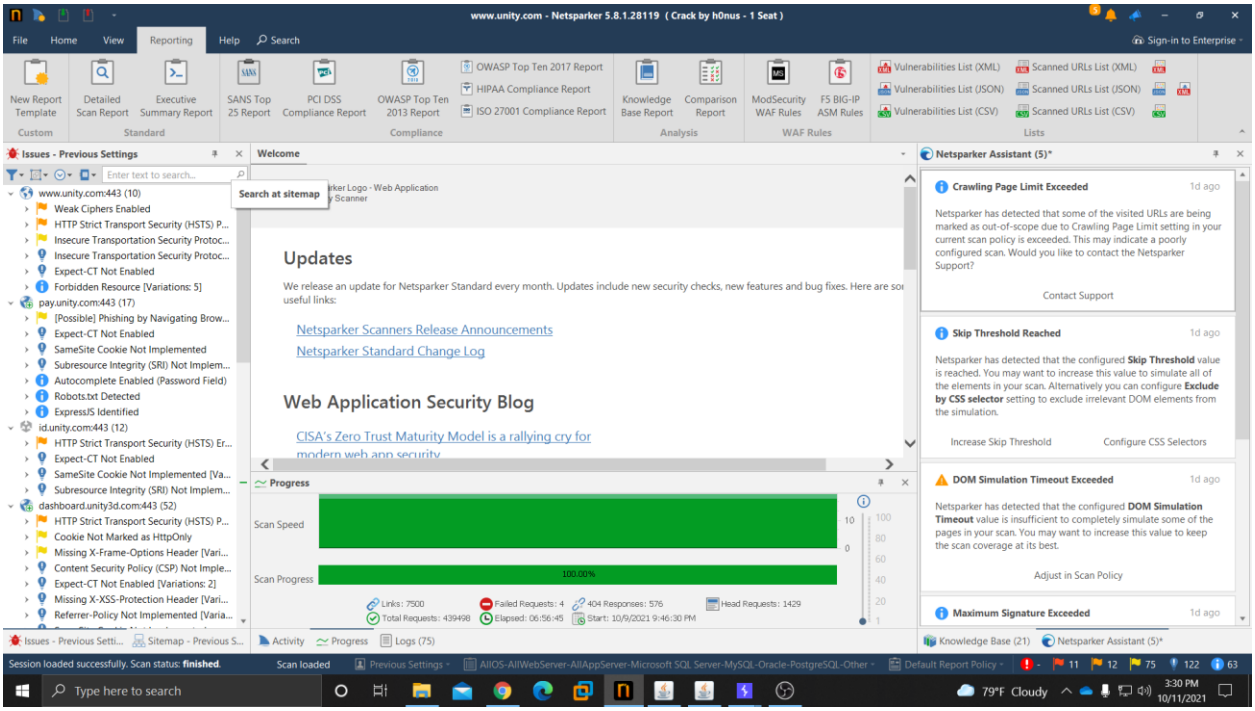


Figure 51 i scanned all in scope domains including

unity.com

id.unity.com

dashboard.unity.com

store.unity.com

pay.unity.com

analytics.cloud.unity.com

After 100% completion we can get a vulnerability scan report as a PDF.

Click here to get detailed Report

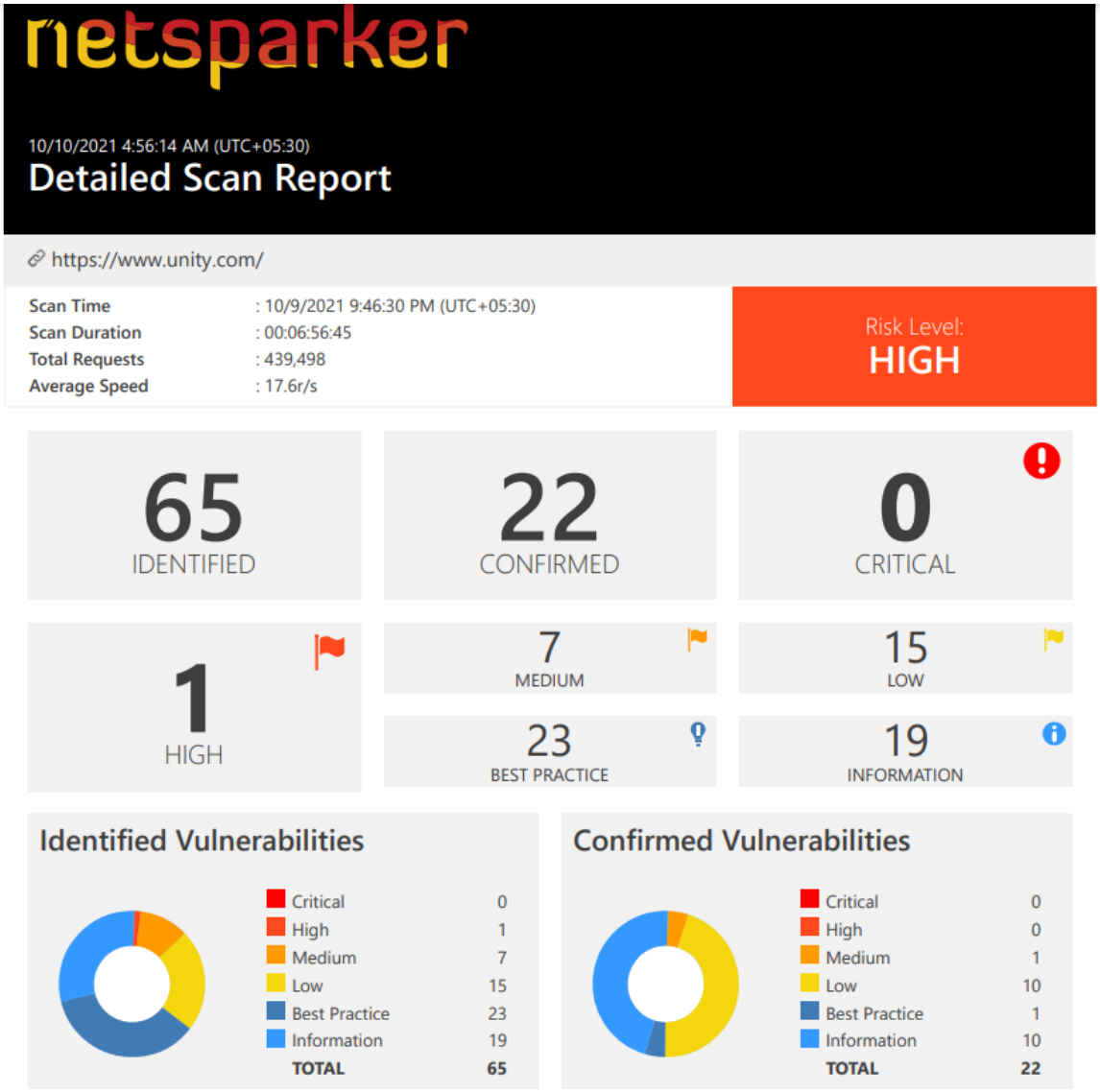
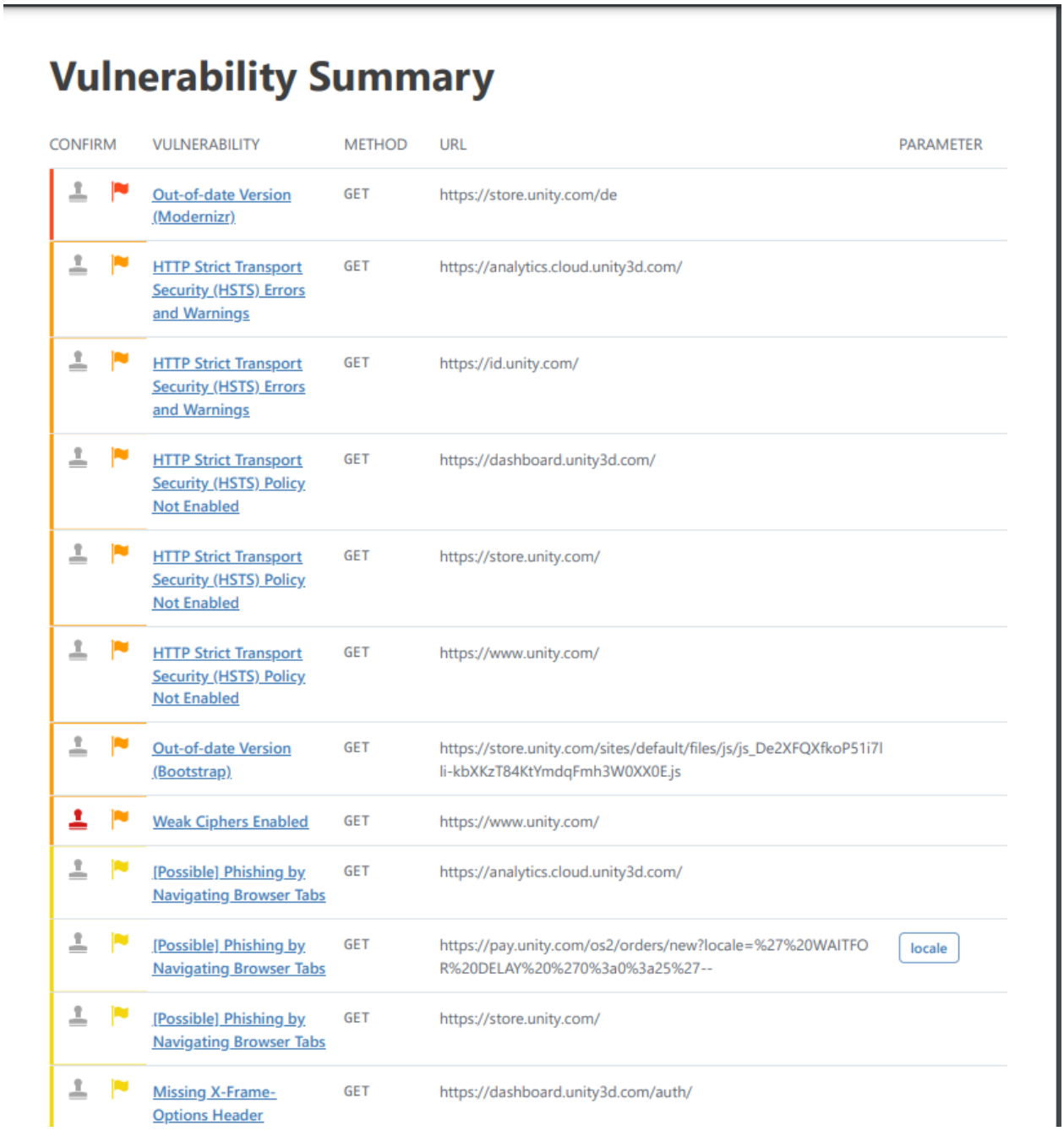


Figure 52 after about 7 hours scanning I got full detailed report regarding the vulnerabilities of in scope domains

unity.com,id.unity.com,dashboard.unity.com,store.unity.com,pay.unity.com,analytics.cloud.unity.com

We could find 1 high risk ,7 medium and 15 low vulnerabilities from all in scope domains by this scan.



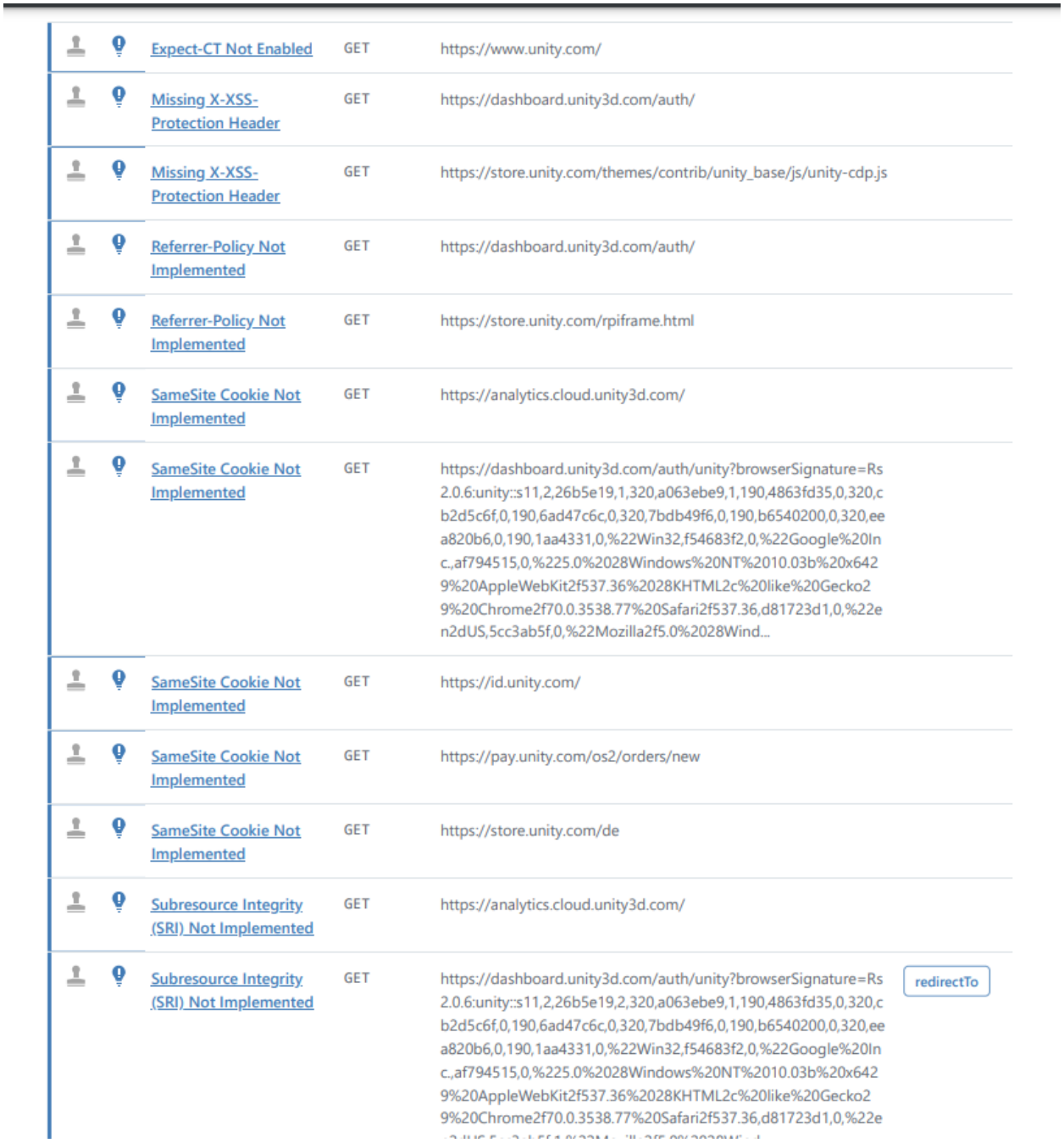
Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://store.unity.com/de	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://analytics.cloud.unity3d.com/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://id.unity.com/	
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://dashboard.unity3d.com/	
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://store.unity.com/	
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.unity.com/	
	Out-of-date Version (Bootstrap)	GET	https://store.unity.com/sites/default/files/js/js_De2XFQXfkoP51i7Ili-kbXKzT84KtYmdqFmh3W0XX0E.js	
	Weak Ciphers Enabled	GET	https://www.unity.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://analytics.cloud.unity3d.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://pay.unity.com/os2/orders/new?locale=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	locale
	[Possible] Phishing by Navigating Browser Tabs	GET	https://store.unity.com/	
	Missing X-Frame-Options Header	GET	https://dashboard.unity3d.com/auth/	

Figure 53 vulnerabilities of all subdomains and paths of them and details

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Cookie Not Marked as HttpOnly	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,1,320,a063ebe9,1,190,4863fd35,0,320,cb2d5c6f,0,190,6ad47c6c,0,320,7bdb49f6,0,190,b6540200,0,320,eea820b6,0,190,1aa4331,0,%22Win32,f54683f2,0,%22Google%20Inc.,af794515,0,%225.0%2028Windows%20NT%2010.03b%20x6429%20AppleWebKit2f537.36%2028KHTML2c%20like%20Gecko29%20Chrome2f70.0.3538.77%20Safari2f537.36,d81723d1,0,%22en2dUS,5cc3ab5f,0,%22Mozilla2f5.0%2028Wind...	
	Cookie Not Marked as HttpOnly	GET	https://store.unity.com/de	
	Cookie Not Marked as Secure	GET	https://analytics.cloud.unity3d.com/	
	Cookie Not Marked as Secure	GET	https://store.unity.com/de	
	Insecure Frame (External)	GET	https://store.unity.com/de	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://www.unity.com/	
	Internal Server Error	POST	https://analytics.cloud.unity3d.com/	
	User Controllable Cookie	GET	https://analytics.cloud.unity3d.com/	
	Windows Short Filename	OPTIONS	https://store.unity.com/ruthemes/store/images/*~1*%5ca.aspx?aspxerrorpath=/	
	Content Security Policy (CSP) Not Implemented	GET	https://dashboard.unity3d.com/auth/	
	Content Security Policy (CSP) Not Implemented	GET	https://store.unity.com/rpiframe.html	
	Expect-CT Not Enabled	GET	https://analytics.cloud.unity3d.com/	
	Expect-CT Not Enabled	GET	https://dashboard.unity3d.com/	
	Expect-CT Not Enabled	GET	https://id.unity.com/	

Figure 54 vulnerabilities of all subdomains and paths of them and details



Expect-CT Not Enabled	GET	https://www.unity.com/	
Missing X-XSS-Protection Header	GET	https://dashboard.unity3d.com/auth/	
Missing X-XSS-Protection Header	GET	https://store.unity.com/themes/contrib/unity_base/js/unity-cdp.js	
Referrer-Policy Not Implemented	GET	https://dashboard.unity3d.com/auth/	
Referrer-Policy Not Implemented	GET	https://store.unity.com/rpiframe.html	
SameSite Cookie Not Implemented	GET	https://analytics.cloud.unity3d.com/	
SameSite Cookie Not Implemented	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,1,320,a063ebe9,1,190,4863fd35,0,320,cb2d5c6f,0,190,6ad47c6c,0,320,7bdb49f6,0,190,b6540200,0,320,eea820b6,0,190,1aa4331,0,%22Win32,f54683f2,0,%22Google%20Inc.,af794515,0,%225.0%2028Windows%20NT%2010.03b%20x6429%20AppleWebKit2f537.36%2028KHTML2c%20like%20Gecko29%20Chrome2f70.0.3538.77%20Safari2f537.36,d81723d1,0,%22en2dUS,5cc3ab5f,0,%22Mozilla2f5.0%2028Wind...	
SameSite Cookie Not Implemented	GET	https://id.unity.com/	
SameSite Cookie Not Implemented	GET	https://pay.unity.com/os2/orders/new	
SameSite Cookie Not Implemented	GET	https://store.unity.com/de	
Subresource Integrity (SRI) Not Implemented	GET	https://analytics.cloud.unity3d.com/	
Subresource Integrity (SRI) Not Implemented	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,2,320,a063ebe9,1,190,4863fd35,0,320,cb2d5c6f,0,190,6ad47c6c,0,320,7bdb49f6,0,190,b6540200,0,320,eea820b6,0,190,1aa4331,0,%22Win32,f54683f2,0,%22Google%20Inc.,af794515,0,%225.0%2028Windows%20NT%2010.03b%20x6429%20AppleWebKit2f537.36%2028KHTML2c%20like%20Gecko29%20Chrome2f70.0.3538.77%20Safari2f537.36,d81723d1,0,%22e	redirectTo

Figure 55 vulnerabilities of all subdomains and paths of them and details

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Subresource Integrity (SRI) Not Implemented	GET	https://id.unity.com/c:/boot.ini	URI-BASED
	Subresource Integrity (SRI) Not Implemented	GET	https://pay.unity.com/c:/boot.ini	URI-BASED
	Subresource Integrity (SRI) Not Implemented	GET	https://store.unity.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.unity.com/	
	[Possible] Internal Path Disclosure (Windows)	GET	https://store.unity.com/themes/c:/apple-touch-icon.png?v=%2527	v
	Apache Web Server Identified	GET	https://analytics.cloud.unity3d.com/robots.txt	
	CDN Detected (Google Cloud CDN)	GET	https://dashboard.unity3d.com/	
	Content Security Policy (CSP) Keywords Not Used Within Single Quotes	GET	https://analytics.cloud.unity3d.com/	
	Email Address Disclosure	GET	https://store.unity.com/sites/default/files/js/js_y5DhFNCcGkfQ-2IsG91FZX0tJ0y73izZRE05jyh6sQA.js	
	ExpressJS Identified	GET	https://pay.unity.com/robots.txt	
	Generic Email Address Disclosure	GET	https://store.unity.com/themes/contrib/unity_base/css/unity-entypo-plus.css	
	Missing object-src in CSP Declaration	GET	https://analytics.cloud.unity3d.com/	
	Unexpected Redirect Response Body (Too Large)	GET	https://store.unity.com/download-nuo	

Figure 56 vulnerabilities of all subdomains and paths of them and details

Identified Vulnerabilities & Mitigations

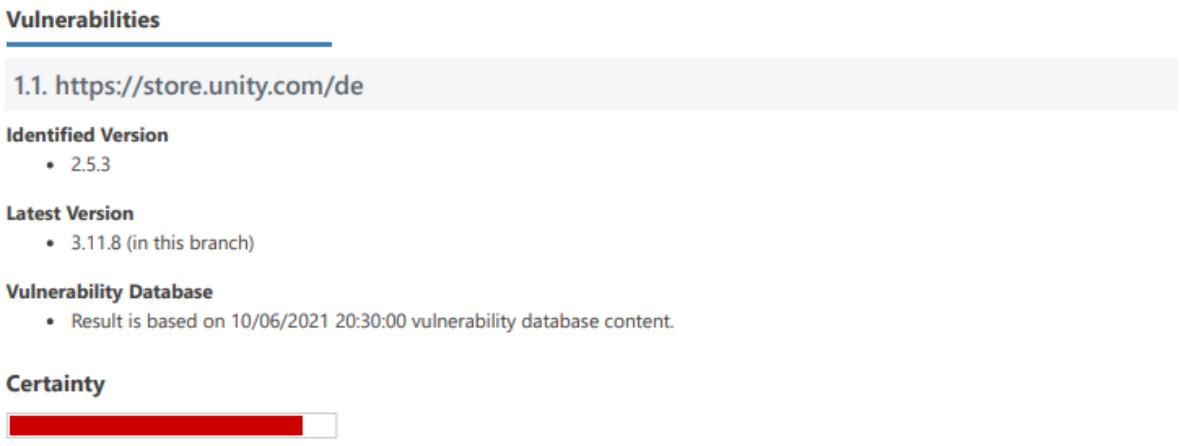
01.Out-of-date Version (Modernizr)

Severity: High

Path : https://store.unity.com/de

Impact : Netsparker discovered that the target web site is utilizing Modernizr and that it is out of date. Due to the fact that this is an outdated version of the program, it may be vulnerable to an attack. Identified version of the site is 2.5.3 according to vulnerability database version 1.1 to version 3.3.1 can be vulnerable to an attacks.

Countermeasures :
The latest version is 3.11.8 .company should pay attention about this latest version and should be updated.



02.HTTP Strict Transport Security (HSTS) Errors & Warnings

Severity: Medium

Paths : https://analytics.cloud.unity3d.com/
https://id.unity.com/

Impact : Netsparker discovered that the target web site consists errors during parsing of Strict-Transport Security Header. The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Countermeasures :

Immediately after the correction of the errors and warnings, you should consider include your domain in the HSTS preload list. Browsers will automatically connect to your website using HTTPS as a result of this, actively discouraging visitors from accessing your website using HTTP. HSTS will be enabled even before a user visits your website for the first time, thanks to the fact that this list is hardcoded into their browsers. This eliminates the requirement for Trust On First Use (TOFU), which has its own set of dangers and drawbacks. The faults and warnings on your website will prevent it from meeting the requirements to be included in the browser's preload list unless you correct them immediately.

03.Cookie Not marked as a Secure

Severity: Critical

Paths : https://analytics.cloud.unity3d.com/
https://store.unity.com/de

Impact : detected a session cookie that had not been designated as secure and sent it over HTTPS This implies that an attacker who is successful in intercepting the traffic, as a result of a successful man-in-the-middle attack, may be able to steal the cookie from the victim's computer. This vulnerability identified in two paths.

\

8.1. https://analytics.cloud.unity3d.com/

CONFIRMED

Identified Cookie(s)

- referrer

Cookie Source

- HTTP Header

Request

```
GET / HTTP/1.1
Host: analytics.cloud.unity3d.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _playnomics_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFVEkiJTYzODAxMTZhY2IxMzU0NWQ0ZGVmOGRkMTc2YTdiYzQ
zBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTZldGVJUDFPcmI3LzJkdFU1Ym1RYkU0Y3gwMFhIZU51MkJsM2xLVWl4Ykk9BjsARg%3D%
3D--3eb62891a15b341f64370b94e9bdfd6b219441c5
Referer: https://analytics.cloud.unity3d.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 331.5744 Total Bytes Received : 791 Body Length : 166 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: referrer=https%3A%2F%2Fanalytics.cloud.unity3d.com%2F; path=/

X-Rack-Cache: miss
Server: Apache
X-Runtime: 0.006904
Via: 1.1 google
Content-Type: text/html; charset=utf-8
X-Request-Id: de553d48ad6deda233a20b06a851c08d
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Alt-Svc: clear
Status: 302 Found
Transfer-Encoding: chunked
Location: https://core.cloud.unity3d.com/api/login/start?redirect=https%3A%2F%2Fanalytics.cloud.unity3
d.com%2F
Date: Sat, 09 Oct 2021 16:17:11 GMT
```

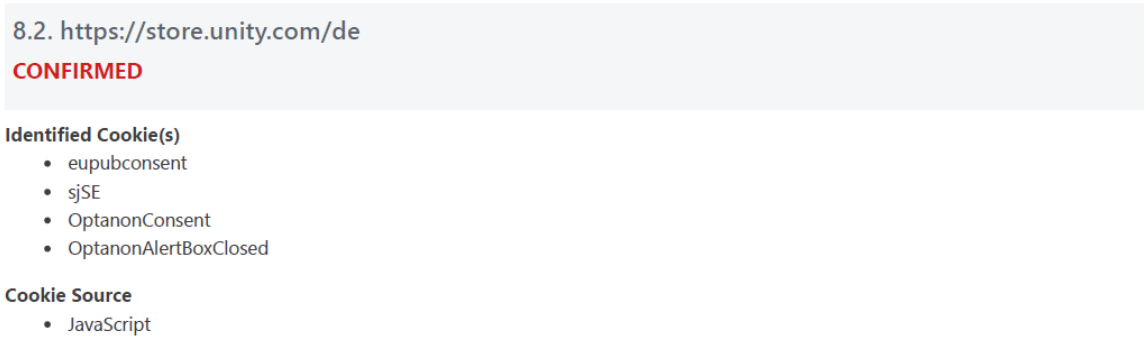


Figure 57 details about identified cookies

Countermeasures :

Secure any and all cookies that are utilized inside the program. It is not necessary to designate a cookie as secure if it is not associated with authentication or does not include any personally identifiable information.

04.HTTP Strict Transport Security (HSTS) Policy not Enabled

Severity: Medium

Paths : https://dashboard.unity3d.com/
https://store.unity.com/

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via an HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period during which the user agent shall access the server in only a secure fashion.
When a web application issues HSTS Policy to user agents, conformant user agents behave as follows: Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.) If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application

Impact :

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:
Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance,
http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error
message and do not allow the user to access the web application.

Countermeasures :

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

05.Out-of-date version of Bootstrap

Severity: Medium

Path : https://store.unity.com/sites/default/files/js/js_De2XFQXfkoP51i7lli-kbXKzT84KtYmdqFmh3W0XX0E.js

Impact : because of this older version site can be vulnerable for cross site script attacks.

Countermeasures : should upgrade a latest version

- CVE-2018-14040

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Affected Versions
1.0.0 to 3.3.7

External References
- CVE-2018-14042

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Affected Versions
3.0.0 to 3.3.7

External References
- CVE-2016-10735

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

Affected Versions
1.0.0 to 3.3.7

Figure 58 details about versions and vulnerabilities

06.Weak Ciphers Enabled

Severity: Medium

Paths : https://www.unity.com/

Impact : In certain cases, attackers may be able to decrypt SSL communication between your server and your website users.

5.1. https://www.unity.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Request

```
[NETSPARKER] SSL Connection
```

Countermeasures :

Actions To Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Figure 59 countermeasures for weak ciphers enabled vulnerability

07.Cookie Not Marked as HttpOnly

Severity: low

Paths : https://analytics.cloud.unity3d.com/
https://store.unity.com/de

Impact : As part of a cross-site scripting attack, the attacker may simply get the victim's cookies and hijack his or her Web browsing experience.

7.1. https://analytics.cloud.unity3d.com/

CONFIRMED

Identified Cookie(s)

- referrer

Cookie Source

- HTTP Header

Request

```
GET / HTTP/1.1
Host: analytics.cloud.unity3d.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _playnomics_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFVEkiJTYzODAxMTZhY2IxMzU0NWQ0ZGVmOGRkMTc2YTdiYzQ
zBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTZldGVJUDFPcmI3LzJkdFU1Ym1RYkU0Y3gwMFhIZU51MkJsM2xLVWl4Ykk9BjsARg%3D%
3D--3eb62891a15b341f64370b94e9bdfd6b219441c5
Referer: https://analytics.cloud.unity3d.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Figure 60 how we confirm this vulnerability we can identify this vulnerability by this request

Response

Response Time (ms) : 331.5744 Total Bytes Received : 791 Body Length : 166 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: referrer=https%3A%2F%2Fanalytics.cloud.unity3d.com%2F; path=/

X-Rack-Cache: miss
Server: Apache
X-Runtime: 0.006904
Via: 1.1 google
Content-Type: text/html; charset=utf-8
X-Request-Id: de553d48ad6deda233a20b06a851c08d
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Alt-Svc: clear
Status: 302 Found
Transfer-Encoding: chunked
Location: https://core.cloud.unity3d.com/api/login/start?redirect=https%3A%2F%2Fanalytics.cloud.unity3
d.com%2F
Date: Sat, 09 Oct 2021 16:17:11 GMT
X-UA-Compatible: IE=Edge
Cache-Control: no-cache, private

<html><body>You are being <a href="https://core.cloud.unity3d.com/api/login/start?redirect=https%3A%2F%
2Fanalytics.cloud.unity3d.com%2F">redirected</a>.</body></html>
```

Figure 61 by this response we can identify the vulnerability

Countermeasures :

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

08.Insecure Transportation Security Protocol Supported (TLS1.0)

Severity: low

Paths : https://unity.com/

Impact :

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Countermeasures :

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

58 / 185

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf`file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
  1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

  3. Locate a key named `Server`or create if it doesn't exist.
  4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

09.Missing X-frame Option Header

Severity: low

Paths : https://dashboard.unity3d.com/auth/
https://store.unity.com/admin/

Impact :

missing X-Frame-Options header was discovered, which indicates that this website may be at danger of being targeted by a clickjacking attack According to the X-Frame-Options HTTP header field, the browser shall display the sent resource in either a frame or an iframe, according to a policy specified in the header field. The header of HTTP replies may be declared by servers to avoid clickjacking attacks, ensuring that their content is not incorporated into other sites or frames.

Countermeasures :

Sending the appropriate X-Frame-Options in HTTP response headers, which instructs the browser not to allow framing from other domains, is essential for effective web development.

- X-Frame-Options: DENY. It totally prohibits the ability to be loaded in a frame or an iframe.
- X-Frame-Options: SAMEORIGIN It is only possible if the site that is being loaded has the same origin as the one that is being loaded.
- X-Frame-Options: ALLOW-FROM URL

10.Missing X-frame Protection Header

Severity: low

Paths : https://dashboard.unity3d.com/auth/
https://store.unity.com/themes/contrib/unity_base/js/unity-cdp.js

Impact : This website may be vulnerable to Cross-site Scripting (XSS) attacks due to a missing X-XSS-Protection header, which was discovered.

Countermeasures :

Include the following X-XSS-Protection header

- 1; mode=block

Conclusion

In average, the unity.com was well-designed and had many security mechanisms in place to defend itself from cyber-attacks when the audit was conducted. During the testing, only medium to low-risk vulnerabilities and best practices were discovered, and there were only one high-risk vulnerabilities discovered, which is a positive indication for a website's appearance of being safe and well-protected.

On the other hand, I was discovered that the website was susceptible to some of the most popular cyber threats that exist today, such as Cross-Site Scripting (XSS) and SQL Injections, Man in the middle attacks. Unity is one of the world's largest 3D development company, and the fact that such a well-equipped company is unable to effectively defend itself from the whole field of cyber assaults demonstrates just how complex the world of online and cyber security has become in the modern day.