

**Sri Lanka Institute of Information Technology**



**Assignment – Web Audit**  
**[www.unity.com](http://www.unity.com)**

**WEB SECURITY – IE2062**

<b>Student ID</b>	<b>Name</b>
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 Ruggahakotuwa, 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

Assignment – Web Audit .....	1
Introduction .....	4
Enumeration .....	5
<b>Sublist3r</b> .....	6
<b>Recon-ng</b> .....	9
<b>Crt.sh</b> .....	10
<b>Wappalyzer</b> .....	12
<b>Securityheaders.com</b> .....	14
<b>Built With.com</b> .....	16
<b>Shodan</b> .....	17
Auditing and testing for Vulnerabilities .....	19
<b>Nmap</b> .....	19
<b>Burp Suite</b> .....	23
<b>Nikto Scanner</b> .....	26
<b>Wafw00f</b> .....	30
<b>OWASP ZAP</b> .....	33
<b>Netspaker</b> .....	36
Identified Vulnerabilities & Mitigations.....	44
Conclusion.....	55

# 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](http://www.unity.com)
- [id.unity.com](http://id.unity.com)
- [dashboard.unity3d.com](http://dashboard.unity3d.com)
- [store.unity.com](http://store.unity.com)
- [pay.unity.com](http://pay.unity.com)
- [analytics.cloud.unity3d.com](http://analytics.cloud.unity3d.com)

## Enumeration

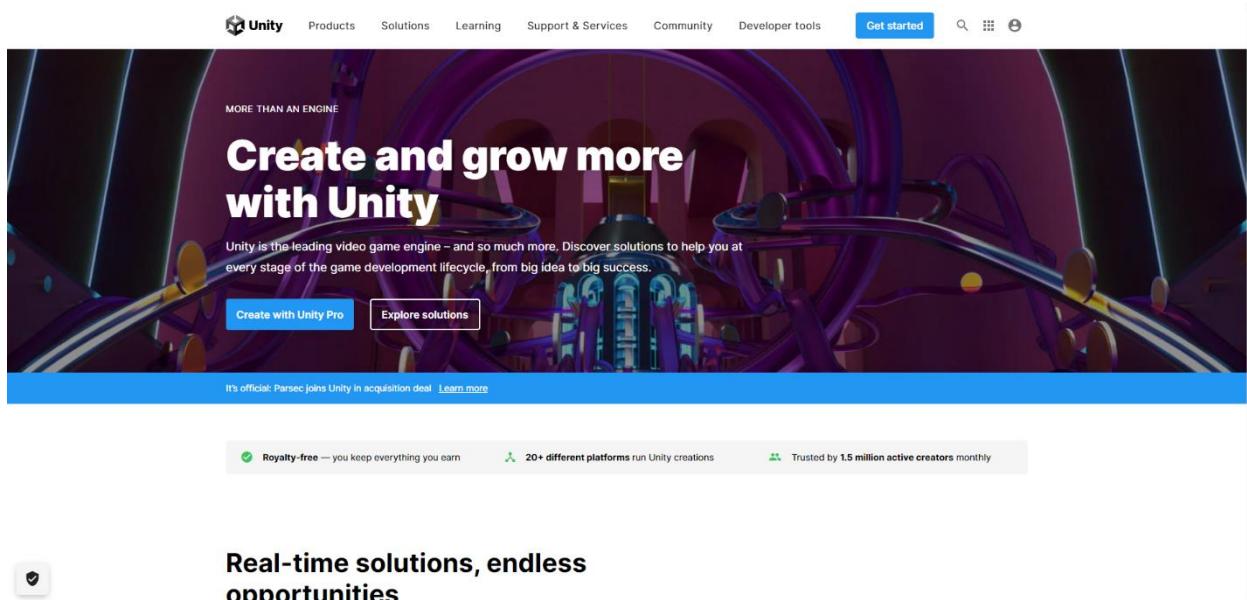


Figure 2 Unity.com website

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 “Sublist3r”.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 Sublist3r**

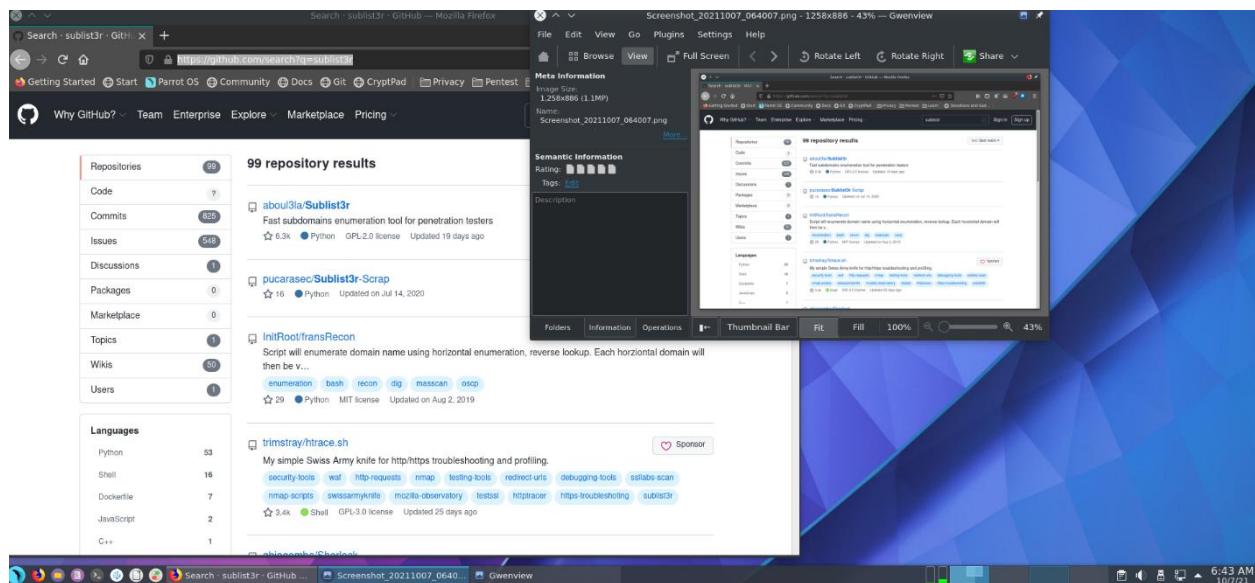
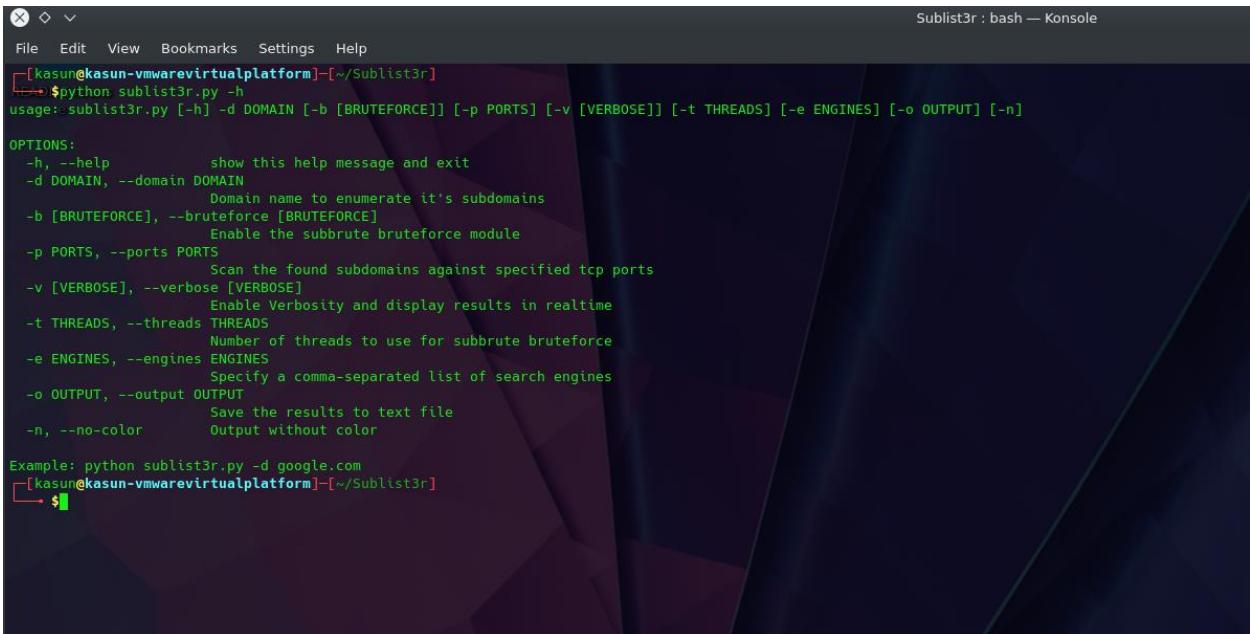


Figure 3 sublist3r in github

Step 02 : then execute the sublist3r.py and get help by typing -h

**#python sublist3r.py -h**



```
Sublist3r : bash — Konsole
File Edit View Bookmarks Settings Help
[kasun@kasun-vmwarevirtualplatform]~[~/Sublist3r]
$ python sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
-h, --help            show this help message and exit
-d DOMAIN, --domain DOMAIN
                      Domain name to enumerate it's subdomains
-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                      Enable the subbrute bruteforce module
-p PORTS, --ports PORTS
                      Scan the found subdomains against specified tcp ports
-v [VERBOSE], --verbose [VERBOSE]
                      Enable Verbosity and display results in realtime
-t THREADS, --threads THREADS
                      Number of threads to use for subbrute bruteforce
-e ENGINES, --engines ENGINES
                      Specify a comma-separated list of search engines
-o OUTPUT, --output OUTPUT
                      Save the results to text file
-n, --no-color         Output without color

Example: python sublist3r.py -d google.com
[kasun@kasun-vmwarevirtualplatform]~[~/Sublist3r]
$
```

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 sublist3r for enumerate all sub domains in unity.com

### #Python sublist3r.py -d unity.com

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

The screenshot shows a terminal window titled "Sublist3r : bash -". The terminal interface includes a menu bar with "File", "Edit", "View", "Bookmarks", "Settings", and "Help". Below the menu is a status bar with the text "Example: python sublist3r.py -d google.com". The main content area displays the command "\$python sublist3r.py -d unity.com" followed by the results of the subdomain enumeration. The results are as follows:

```
Example: python sublist3r.py -d google.com
[kasun@kasun-vmwarevirtualplatform] -[~/Sublist3r]
$python sublist3r.py -d unity.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for unity.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 177
stage.microsoftpartnercommunity.com
www.unibetcommunity.com
www.unity.com
aisummit2020.unity.com
wwwaisummit2020.unity.com
answers.unity.com
api.unity.com
monetization.api.unity.com
services.api.unity.com
staging.services.api.unity.com
api-channel.unity.com
api-connect.unity.com
api-int.unity.com
api-staging.unity.com
api-test.unity.com
api-udp.unity.com
apicallback-int.unity.com
apicallback-staging.unity.com
assetstore.unity.com
```

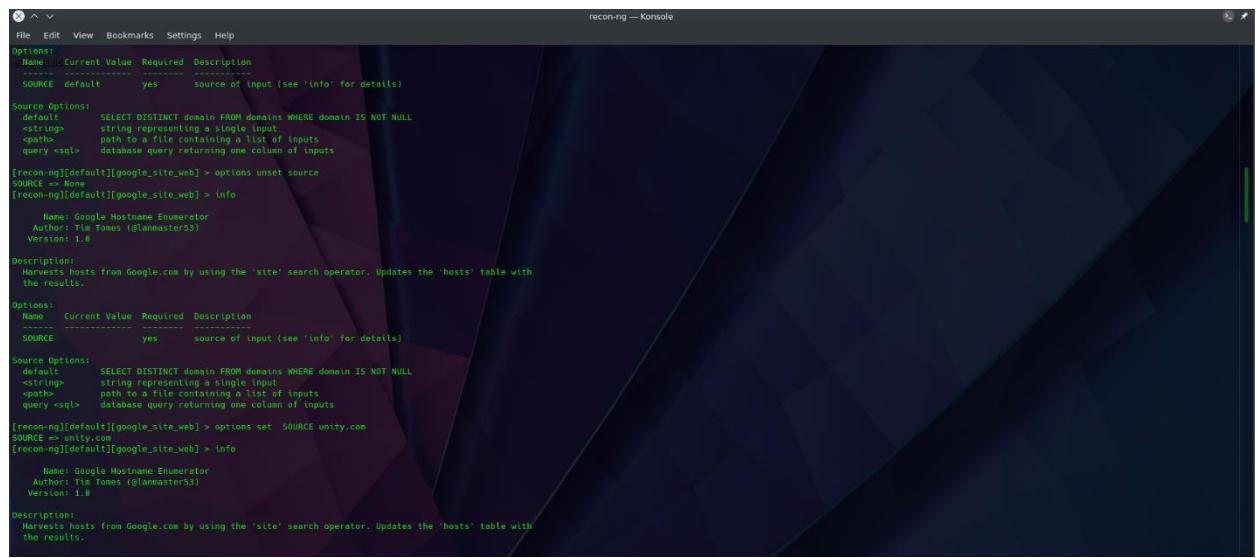
Figure 5 After scanning we can get list of subdomains of targeted domain

[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.



```
recon-ng -- Konsole
File Edit View Bookmarks Settings Help
Options:
  Name  Current Value  Required  Description
  -----  -----  -----
  SOURCE  default  yes      source of input (see 'info' for details)

Source Options:
  default  SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>  string representing a single input
  <path>  path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][google_site_web] > options unset source
SOURCE => None
[recon-ng][default][google_site_web] > info
  Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.8

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.

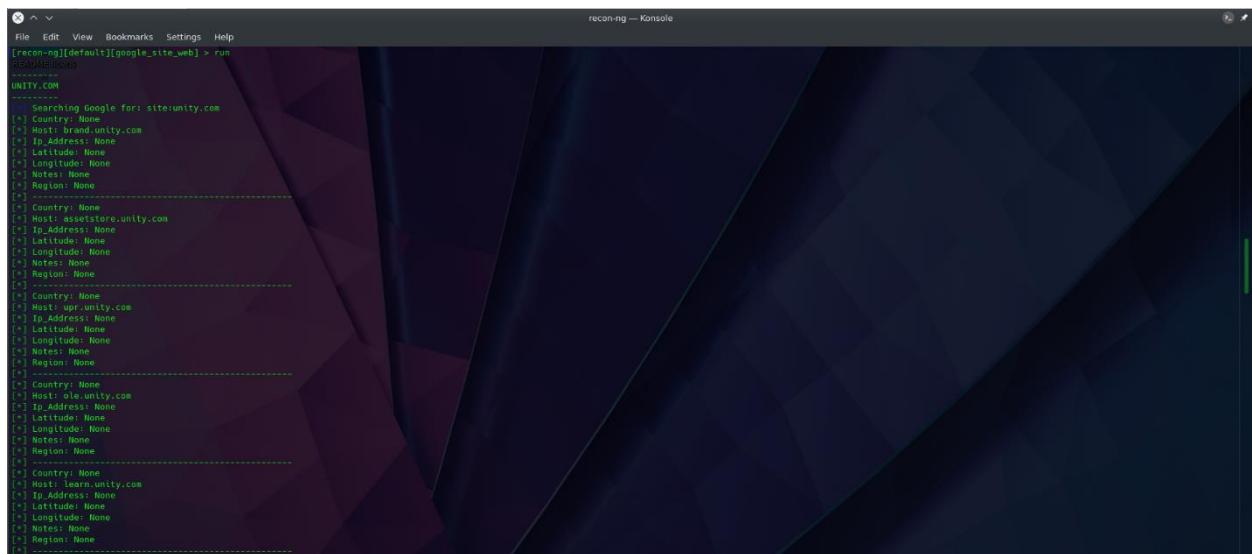
Options:
  Name  Current Value  Required  Description
  -----  -----  -----
  SOURCE  yes      source of input (see 'info' for details)

Source Options:
  default  SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>  string representing a single input
  <path>  path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][google_site_web] > options set SOURCE unity.com
SOURCE => unity.com
[recon-ng][default][google_site_web] > info
  Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.8

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
```

Figure 6 add a source to recon-ng tool



```
recon-ng -- Konsole
File Edit View Bookmarks Settings Help
[recon-ng][default][google_site_web] > run
RECONV1000G
UNITY.COM
  Searching Google for: site:unity.com
  [+] Country: None
  [+] Host: kread.unity.com
  [+] Ip_Address: None
  [+] Latitude: None
  [+] Longitude: None
  [+] Notes: None
  [+] Region: None
  [+] ...
  [+] Country: None
  [+] Host: assesture.unity.com
  [+] Ip_Address: None
  [+] Latitude: None
  [+] Longitude: None
  [+] Notes: None
  [+] Region: None
  [+] ...
  [+] Country: None
  [+] Host: upr.unity.com
  [+] Ip_Address: None
  [+] Latitude: None
  [+] Longitude: None
  [+] Notes: None
  [+] Region: None
  [+] ...
  [+] Country: None
  [+] Host: ole.unity.com
  [+] Ip_Address: None
  [+] Latitude: None
  [+] Longitude: None
  [+] Notes: None
  [+] Region: None
  [+] ...
  [+] Country: None
  [+] Host: unity.unity.com
  [+] Ip_Address: None
  [+] Latitude: None
  [+] Longitude: None
  [+] Notes: None
  [+] Region: None
  [+] ...
```

Figure 7 output of recon-ng after scanning

```
recon-ng — Konsole
File Edit View Bookmarks Settings Help
[]> Country: None
[]> Host: on.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: resources.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: id.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: store.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:play.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com
[]> Country: None
[]> Host: answers.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:play.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com
[]> No New Subdomains Found on the Current Page. Jumping to Result 201.
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:play.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com
```

Figure 8 output of recon-ng after scanning

```
recon-ng — Konsole
File Edit View Bookmarks Settings Help
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com
[]> Country: None
[]> Host: globalgamejam2021.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: forum.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: careers.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Country: None
[]> Host: globalgamejam2021.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:play.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com -site:globalgamejam2021.unity.com -site:forum.unity.com -site:careers.unity.com -site:support.unity.com
[]> Country: None
[]> Host: investors.unity.com
[]> Ip Address: None
[]> Latitude: None
[]> Longitude: None
[]> Notes: None
[]> Region: None
[]>
[]> Searching Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -site:upr.unity.com -site:ole.unity.com -site:learn.unity.com -site:blog.unity.com -site:on.unity.com -site:resources.unity.
com -site:id.unity.com -site:store.unity.com -site:answers.unity.com -site:globalgamejam2021.unity.com -site:forum.unity.com -site:careers.unity.com -site:support.unity.com
```

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.

crt.sh Certificate Search

Enter an Identity (Domain Name, Organization Name, etc),  
a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:

unity.com

Search Advanced

© Sedigo Limited 2015-2021. All rights reserved.

**5**

**crt.sh Identity Search**

Criteria Type: Identity Match: ILIKE Search: 'unity.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
	533942145	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CH3.0rLet's Encrypt CN=R3
	532645289	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CH3.0rLet's Encrypt CN=R3
	521288904	2021-10-01	2021-07-19	2022-08-13*	services.api.unity.com	services.api.unity.com	CH3.0rDigiCert Inc. CN=DigiCert TLS RSA SHA256 2020 CA1
	5313472016	2021-09-24	2021-09-02	2021-12-01	docs-stg.unity.com	docs-stg.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5275988459	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5311044591	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5211048558	2021-09-27	2021-09-27	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	520720229	2021-09-27	2021-09-27	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5297380118	2021-09-27	2021-09-27	2021-12-26	on.unity.com	on.unity.com	CH3.0rLet's Encrypt CN=R3
	527824337	2021-09-24	2021-09-23	2022-08-23*	unity.com	* unity.com	CH3.0rDigiCert Inc. CN=DigiCert SHA2 Secure Server CA
	5275988459	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CH3.0rLet's Encrypt CN=R3
	52759884439	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CH3.0rLet's Encrypt CN=R3
	5270704744	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CH3.0rLet's Encrypt CN=R3
	5270702229	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CH3.0rLet's Encrypt CN=R3
	5258194803	2021-09-21	2021-09-21	2021-12-20	www.unityforms-event.unity.com	unityforms-event.unity.com	CH3.0rLet's Encrypt CN=R3
	5258195521	2021-09-21	2021-09-21	2021-12-20	www.unityforms-event.unity.com	www.unityforms-event.unity.com	CH3.0rLet's Encrypt CN=R3
	5258192851	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5258192811	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5252195757	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CH3.0rLet's Encrypt CN=R3
	5304217606	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CH3.0rLet's Encrypt CN=R3
	5211395357	2021-09-19	2021-09-19	2021-12-12	sanc441 cdnwerk.com	sanc441 cdnwerk.com	CH3.0rLet's Encrypt CN=R3
	5211395309	2021-09-19	2021-09-19	2021-12-12	sanc441 cdnwerk.com	resources.unity.com	CH3.0rLet's Encrypt CN=R3
	5207202474	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CH3.0rLet's Encrypt CN=R3
	5207205636	2021-09-12	2021-09-12	2021-11-11	compass.unity.com	compass.unity.com	CH3.0rLet's Encrypt CN=R3
	5207205636	2021-09-12	2021-09-12	2021-11-11	compass.unity.com	unteness.unity.com	CH3.0rLet's Encrypt CN=R3
	5178743977	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rLet's Encrypt CN=R3
	51737380057	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rLet's Encrypt CN=R3
	5173722716	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5170827268	2021-09-26	2021-09-26	2021-12-05	docs-test.unity.com	docs-test.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160872410	2021-09-26	2021-09-26	2021-12-05	docs-test.unity.com	docs-test.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160872559	2021-09-04	2021-07-08	2021-10-26	docs-stg.unity.com	docs-stg.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160879932	2021-09-04	2021-08-19	2021-11-17	staging.services.unity.com	cdn.mars.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5152624990	2021-09-04	2021-08-29	2021-11-16	staging.services.unity.com	staging.services.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5136198204	2021-09-01	2021-08-31	2021-11-16	staging.services.unity.com	staging.services.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5136198204	2021-09-01	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5128908186	2021-08-31	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5128908186	2021-08-29	2021-08-29	2021-11-27	blog-api.unity.com	blog-api.unity.com	CH3.0rLet's Encrypt CN=R3
	5128627460	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CH3.0rLet's Encrypt CN=R3
	5128627464	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CH3.0rLet's Encrypt CN=R3
	5120315513	2021-08-28	2021-08-28	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104

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

crt.sh Identity Search

Criteria Type: Identity Match: ILIKE Search: 'unity.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
	533942145	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CH3.0rLet's Encrypt CN=R3
	532645289	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CH3.0rLet's Encrypt CN=R3
	521288904	2021-10-01	2021-07-19	2022-08-13*	services.api.unity.com	services.api.unity.com	CH3.0rDigiCert Inc. CN=DigiCert TLS RSA SHA256 2020 CA1
	5313472016	2021-09-24	2021-09-02	2021-12-01	docs-stg.unity.com	docs-stg.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5275988459	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5311044591	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5311048558	2021-09-27	2021-09-27	2021-12-28	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	520720229	2021-09-27	2021-09-27	2021-12-22	ole.unity.com	ole.unity.com	CH3.0rLet's Encrypt CN=R3
	5297380118	2021-09-27	2021-09-27	2021-12-26	on.unity.com	on.unity.com	CH3.0rLet's Encrypt CN=R3
	527824337	2021-09-24	2021-09-23	2022-08-23*	unity.com	* unity.com	CH3.0rDigiCert Inc. CN=DigiCert SHA2 Secure Server CA
	5275988459	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CH3.0rLet's Encrypt CN=R3
	52759884439	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CH3.0rLet's Encrypt CN=R3
	5270704744	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CH3.0rLet's Encrypt CN=R3
	5270702229	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CH3.0rLet's Encrypt CN=R3
	5258194803	2021-09-21	2021-09-21	2021-12-20	www.unityforms-event.unity.com	unityforms-event.unity.com	CH3.0rLet's Encrypt CN=R3
	5258195521	2021-09-21	2021-09-21	2021-12-20	www.unityforms-event.unity.com	www.unityforms-event.unity.com	CH3.0rLet's Encrypt CN=R3
	5258192851	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5258192811	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5252195757	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CH3.0rLet's Encrypt CN=R3
	5304217606	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CH3.0rLet's Encrypt CN=R3
	5211395357	2021-09-19	2021-09-19	2021-12-12	sanc441 cdnwerk.com	sanc441 cdnwerk.com	CH3.0rLet's Encrypt CN=R3
	5211395309	2021-09-19	2021-09-19	2021-12-12	sanc441 cdnwerk.com	resources.unity.com	CH3.0rLet's Encrypt CN=R3
	5207202474	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CH3.0rLet's Encrypt CN=R3
	5207205636	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CH3.0rLet's Encrypt CN=R3
	5178743977	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rLet's Encrypt CN=R3
	51737380057	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rLet's Encrypt CN=R3
	5173722716	2021-09-26	2021-09-26	2021-12-05	unteness.unity.com	unteness.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5170827268	2021-09-26	2021-09-26	2021-12-05	docs-test.unity.com	docs-test.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160872410	2021-09-26	2021-09-26	2021-12-05	docs-test.unity.com	docs-test.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160872559	2021-09-04	2021-07-08	2021-10-26	docs-stg.unity.com	docs-stg.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160879932	2021-09-04	2021-08-28	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5160879932	2021-09-04	2021-08-19	2021-11-17	staging.services.unity.com	staging.services.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5152624990	2021-09-02	2021-09-02	2021-12-04	staging.services.unity.com	staging.services.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104
	5136198204	2021-08-31	2021-08-31	2021-11-16	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5136198204	2021-08-31	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CH3.0rLet's Encrypt CN=R3
	5128908186	2021-08-29	2021-08-29	2021-11-27	blog-api.unity.com	blog-api.unity.com	CH3.0rLet's Encrypt CN=R3
	5128908186	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CH3.0rLet's Encrypt CN=R3
	5128627460	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CH3.0rLet's Encrypt CN=R3
	5128627464	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CH3.0rLet's Encrypt CN=R3
	5120315513	2021-08-28	2021-08-28	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CH3.0rGoogle Trust Services LLC CN=GTS CA 104

Activate Windows  
Go to Settings to activate Windows.

## 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.

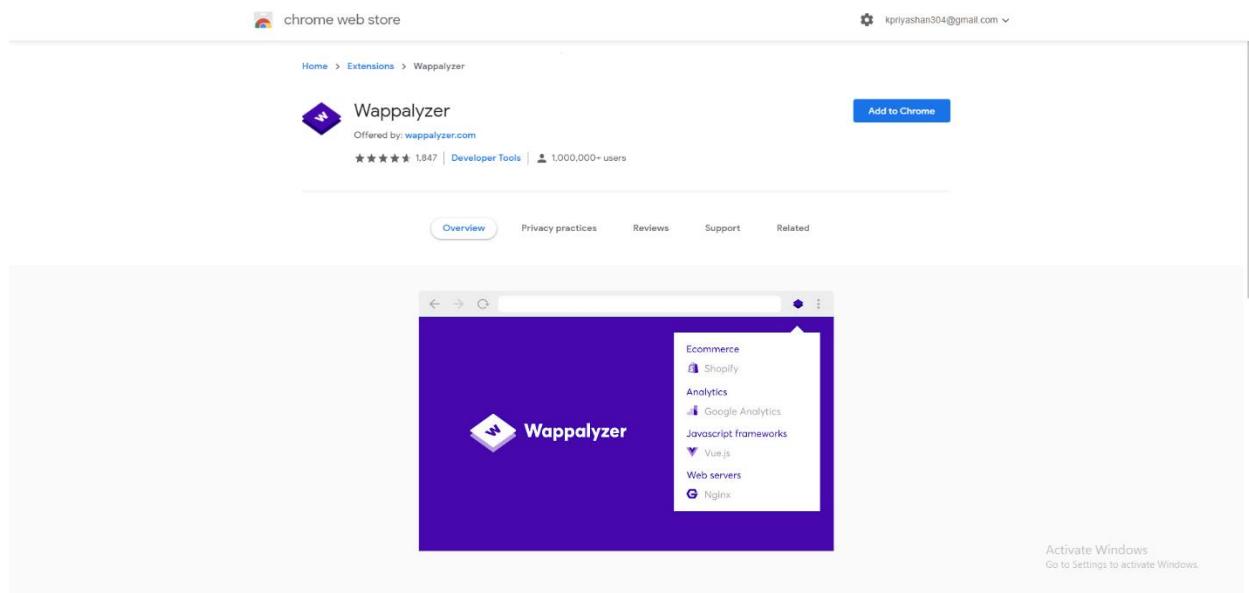


Figure 11 how to add extension to browser

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

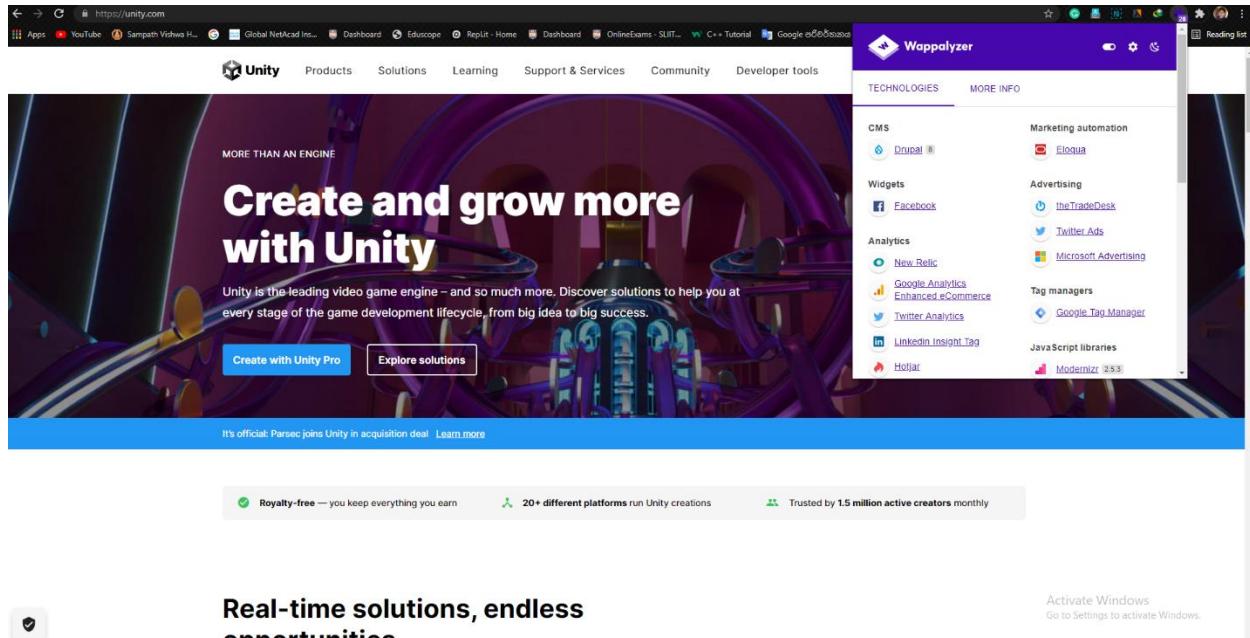


Figure 12 output of wappalyzer we can get information about technologies which site built

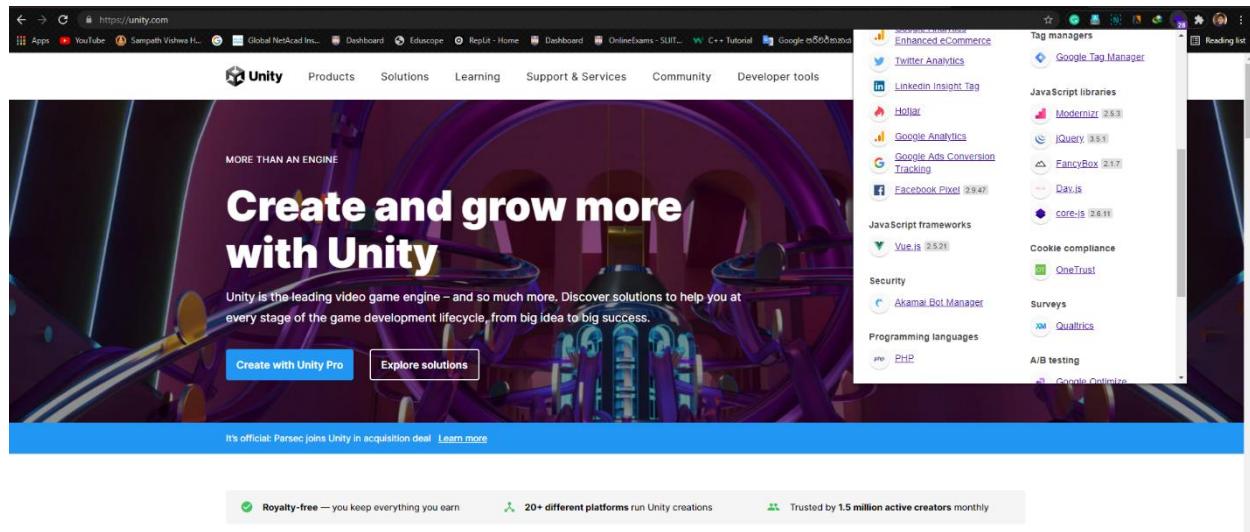


Figure 13 output of wappalyzer we can get information about technologies which site built

## 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](https://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.

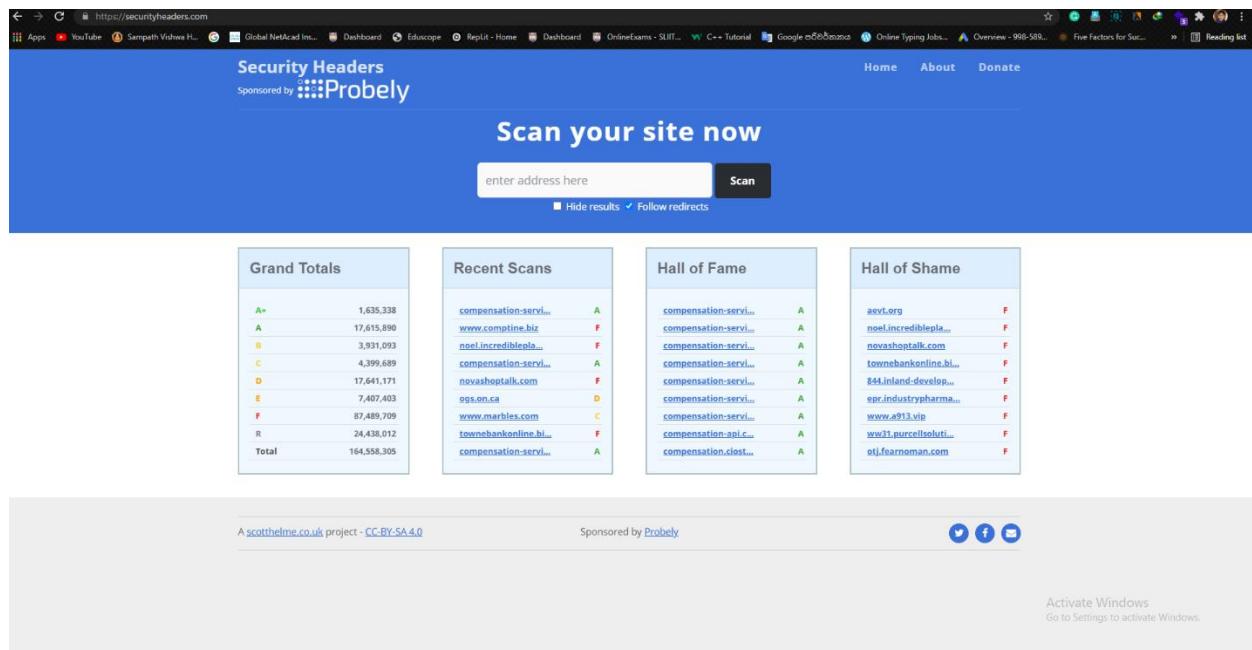


Figure 14 interface of www.securityheaders.com

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.

The screenshot shows the Security Headers website interface. At the top, there's a navigation bar with links like Home, About, and Donate. Below that is a search bar with the URL "www.unity.com" and a "Scan" button. Underneath the search bar are two checkboxes: "Hide results" and "Follow redirects". The main content area is titled "Security Report Summary". It displays the following information:

- Site:** <https://unity.com/>
- IP Address:** 104.93.134.159
- Report Time:** 07 Oct 2021 11:33:33 UTC
- Headers:** A list of checked and unchecked items:
  - ✓ Content-Type Options
  - ✓ X-Frame-Options
  - ✗ Strict-Transport-Security
  - ✗ Content-Security-Policy
  - ✗ Referrer-Policy
  - ✗ Permissions-Policy

Below this section is a "Supported By" section featuring Probely, with a "Start Now" button. The final section is "Raw Headers", which lists the following:

Header	Value
HTTP/1.1	200 OK
Content-Language	en
Content-Type	text/html; charset=UTF-8

On the right side of the page, there's a note: "Activate Windows. Go to Settings to activate Windows."

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.

The screenshot shows two sections of the Security Headers website:

### Missing Headers

This section lists three missing headers:

- Content-Security-Policy**: Described as an effective measure to protect your site from XSS attacks. Whitelisting sources of approved content can prevent the browser from loading malicious assets.
- Referrer-Policy**: Described as 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.
- Permissions-Policy**: Described as a new header that allows a site to control which features and APIs can be used in the browser.

### Warnings

This section lists one warning:

- Strict-Transport-Security**: The "max-age" directive is too small. The minimum recommended value is 2592000 (30 days).

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.

The screenshot shows the BuiltWith.com interface for the domain unity.com. At the top, there's a navigation bar with links for Log In, Signup for Free, Tools, Features, Plans, Customers, Resources, and a search bar containing 'Website, Tech, Keyword' with a 'Lookup' button. Below the navigation is a breadcrumb trail: Home / unity.com Technology Profile. The main content area has a title 'UNITY.COM' and a sub-section 'Technology Profile'. Under 'Technology Profile', there are tabs for Detailed Technology Profile, Meta Data Profile, Relationship Profile, Redirect Profile, and Company Profile. The left sidebar lists various technologies used on the site, each with a logo, name, and a link to 'Usage Statistics'. These include Eloqua, Hotjar, Terminus, 6sense, Google Optimize 360, and Sajari. To the right of the technology list is a 'Profile Details' box showing the last technology detected (8th October 2021), the number of technologies known (112), and a note about technologies removed since May 2000. Below this is a promotional box for 'WFH Sale' offering unlimited lookups for \$144/year. At the bottom right, there's an 'Add to Chrome' button and a note to activate Windows.

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

This screenshot shows the same BuiltWith.com interface for the domain unity.com, but with a different set of technologies listed in the sidebar. The sidebar includes Adobe Connect, Qualtrics Site Intercept, OneTrust, Optanon, Dropbox Business, and Smartsheet. The rest of the page structure is identical to Figure 17, with the 'WFH Sale' promotion and the 'Activate Windows' note at the bottom right.

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.

The screenshot shows the Shodan search interface for the domain 'unity.com'. The search bar at the top contains 'unity.com'. Below the search bar, the total number of results is displayed as 40. The interface includes several filters and statistics:

- TOP COUNTRIES:** United States (31), Russian Federation (3), Belgium (2), France (2), Indonesia (1).
- TOP PORTS:** 80 (18), 443 (15), 3389 (3), 2525 (2), 5222 (1).
- TOP ORGANIZATIONS:** Google LLC (31), JSC IOT (2), Ritter Communications (2).
- TOP PRODUCTS:** nginx (10), Remote Desktop Protocol (3), Apache httpd (2).

For each result, detailed information is provided, including the IP address, organization, location, and an SSL Certificate summary. For example, the first result is 35.241.48.119, which belongs to Google LLC in the United States, Kansas City, and is associated with a Digicert SHA2 Secure Server CA SSL certificate. The second result is 35.186.231.34, also from Google LLC in the United States, Kansas City, with a similar SSL certificate.

Figure 20 shodan shows interconnected devices to domain

The screenshot shows the Shodan search interface for the domain 'unity.com', identical to Figure 20. It displays 40 results across various categories: TOP COUNTRIES, TOP PORTS, TOP ORGANIZATIONS, and TOP PRODUCTS. Each result provides a detailed breakdown of the device's identity, location, and its SSL certificate configuration. For instance, the first result is 35.244.202.54, which is a Google LLC server in the United States, Kansas City, using an nginx product. Its SSL certificate is issued by Digicert SHA2 Secure Server CA. The second result is 35.227.211.131, another Google LLC server in the United States, Kansas City, also using nginx and featuring a similar SSL certificate.

Figure 19 shodan shows interconnected devices to domain

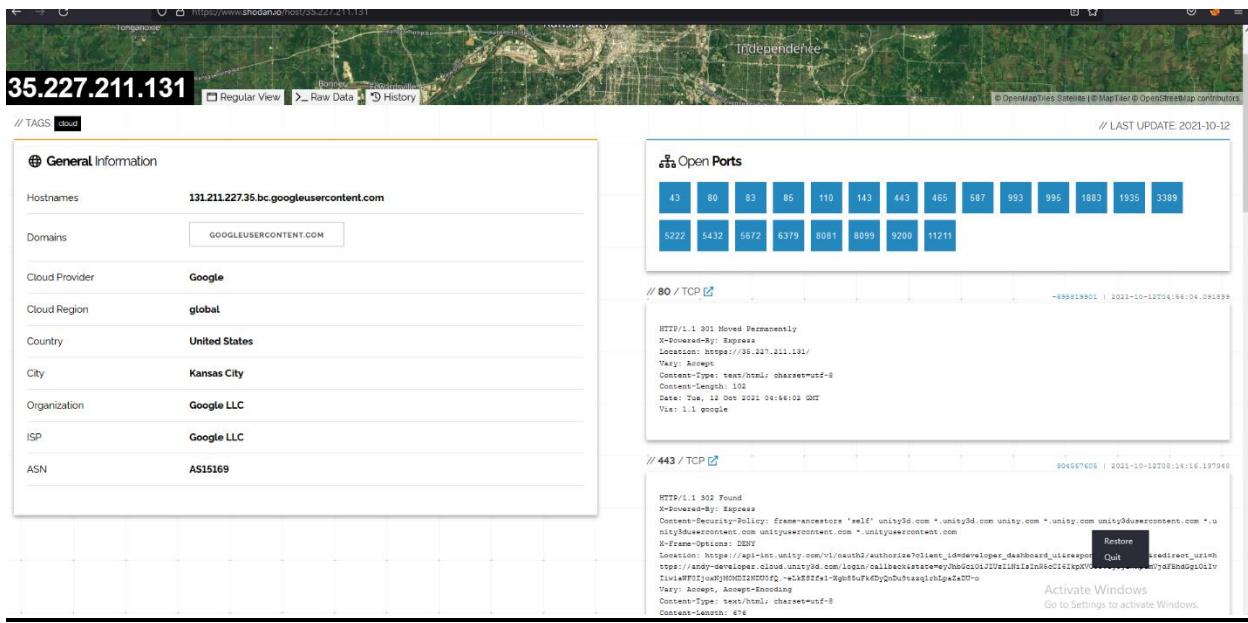


Figure 21 information about interconnected device and we can get information about open ports etc.

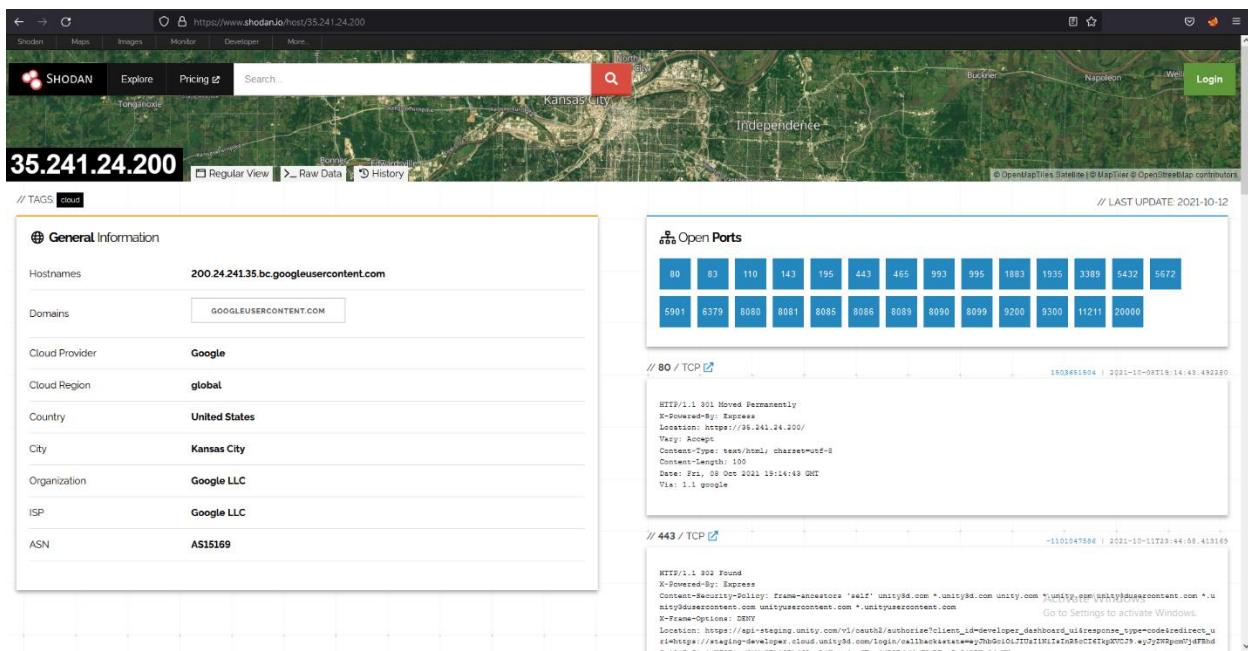


Figure 22 information about interconnected device and we can get information about open ports etc

# 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](http://www.unity.com)

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

[Id.unity.com](http://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](https://Analytics.cloud.unity.com)

```
[root@kali:~]# nmap -sV -T4 -O Nmap analysis.txt analytics.cloud.unity3d.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 23:15 +0530
Nmap scan report for analytics.cloud.unity3d.com (35.198.63.66)
Host is up (0.000s latency).
Nmap done: 1 IP address (1 host up) scanned in 59.72 seconds

[...]
```

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](http://pay.unity.com)

```
[root@localhost ~]# $udo nmap -sS -A -p- -T4 -oN penny.txt http://unity.com
Starting Nmap 7.01 ( https://nmap.org ) at 2021-10-11 23:05 +0530
Nmap scan report for http://unity.com (35.236.177.74)
Host is up (0.01s latency).
All 65535 scanned ports on http://unity.com (35.236.177.74) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops

TRACEROUTER (using port 80/tcp)
Hop RTT      ADDRESS
1.  9.55 ms  192.168.1.16.2
2.  8.31 ms  74.177.236.35.bc.googleusercontent.com (35.236.177.74)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) Scanned in 237.68 seconds
```

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.

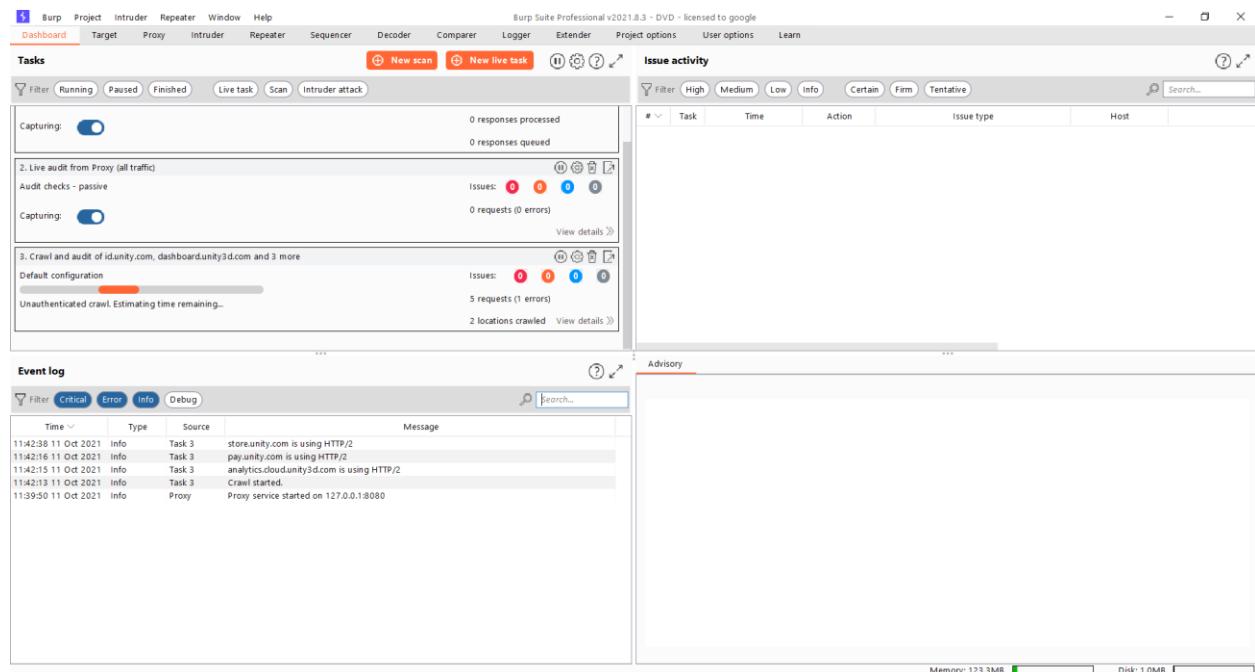


Figure 27 strating burp with crawl and audit

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.

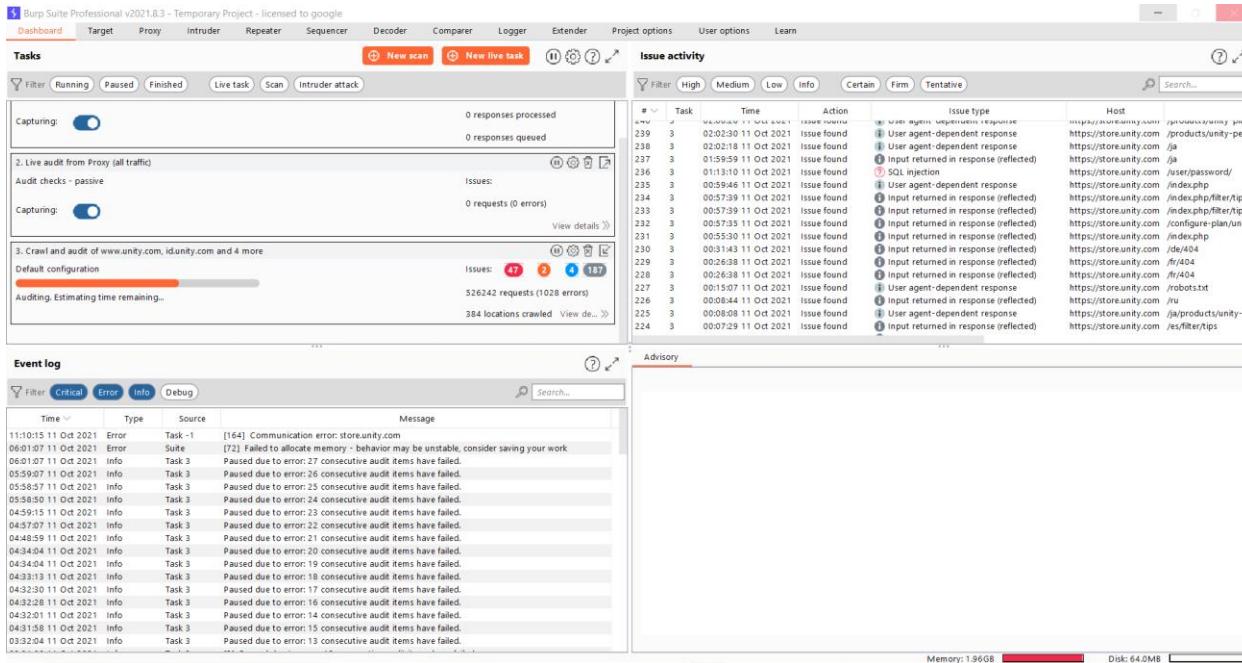


Figure 28 output after 6 hours in burp I could find 47 issues by this scan most of them are common vulnerabilities

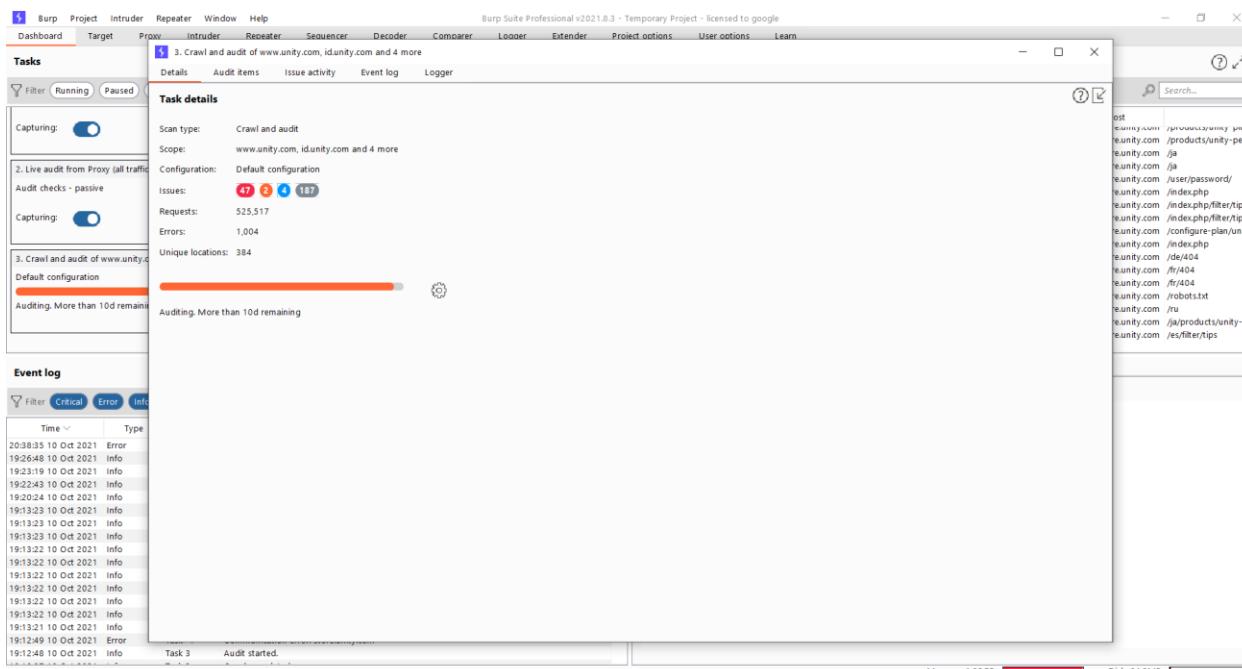


Figure 29 after 525,517 requests results I have got by burp suite scanning

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.

The screenshot shows the Burp Suite Professional interface. In the top navigation bar, the menu items are: Burp, Project, Intruder, Repeater, Window, Help. Below the menu is a toolbar with buttons for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The main window has several tabs: Tasks, Event log, Issue activity (which is selected), and Logger. Under the Tasks tab, there are sections for 'Capturing' (status: Running), 'Audit checks - passive' (status: 2: Live audit from Proxy (all traffic)), and 'Auditing' (status: Default configuration, Auditing. More than 10d remaining). The Issue activity tab displays a table of findings:

Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
1 Oct 2021	Issue found	SQL injection	https://store.unity.com	/user/password/	interactionCount para...	High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/pt/products/unity-plus	ak_bmsc cookie	High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/configure-plan/unity-enterprise		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/ja		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/index.php/products/unity-enterprise		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/pt/products/unity-enterprise		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/pt/products/unity-pro		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/products/unity-enterprise		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/index.php/products/unity-pro		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/products/unity-personal		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/pt/products/unity-plus		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/index.php/products/unity-personal		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/products/unity-enterprise		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/configure-plan/unity-plus		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/ja		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/products/unity-f		High	Tentative	
1 Oct 2021	Issue found	Cross-site scripting (DOM-based)	https://store.unity.com	/es/filter/tips		High	Tentative	

The right side of the interface shows a list of URLs for the Unity website. Below the table, there is a section for 'Event log' with tabs for Advisory, Request 1, Response 1, Request 2, and Response 2. A specific event for a 'SQL injection' is highlighted in the advisory log.

Figure 30 issues that I have found by burp suite scanning

The screenshot shows the Burp Suite Professional interface after 10 hours of scanning. The top navigation bar and toolbar are identical to Figure 30. The main window has tabs for Tasks, Event log, and Issue activity. The Task tab shows a progress bar for 'Default configuration' which is Paused. The Issue activity tab shows a table of findings, but it appears mostly empty or has very few entries. The Event log tab is selected and shows a large number of error messages. A detailed view of one error message is shown in the center panel:

Time: 11:19:45 11 Oct 2021, Type: Error, Source: [77] Failed to allocate memory - behavior may be unstable, consider saving your work. Message: Task 3 Paused due to error: 31 consecutive audit items have failed.

The Event log table shows many similar errors:

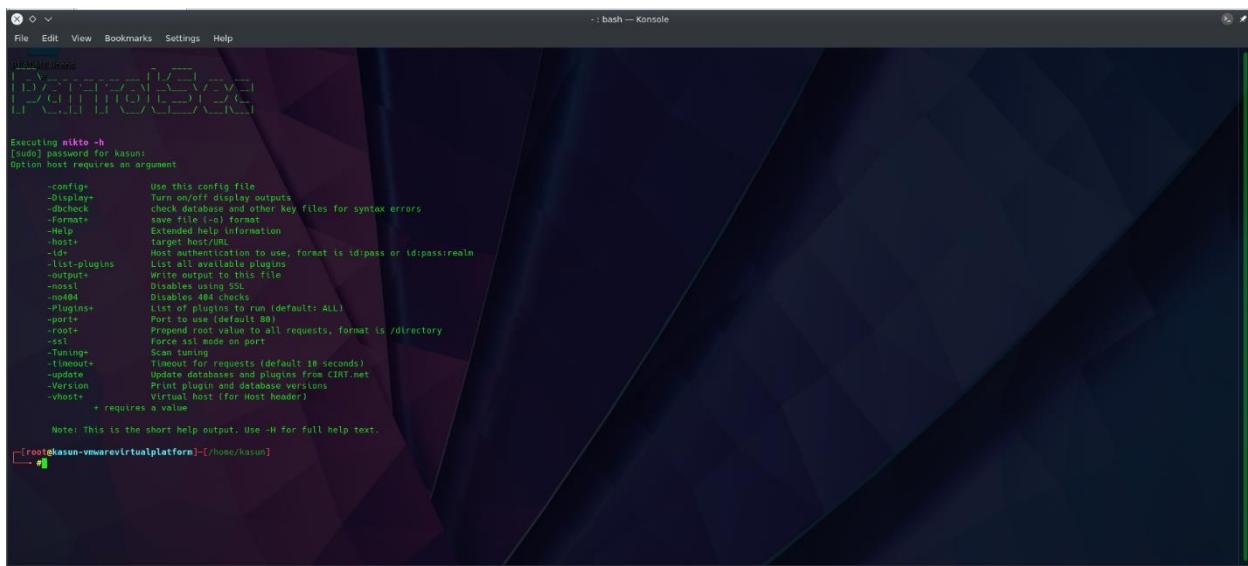
Time	Type	Source	Message
11:19:45 11 Oct 2021	Error	[77]	Failed to allocate memory - behavior may be unstable, consider saving your work
11:19:45 11 Oct 2021	Info	Task 3	Paused due to error: 31 consecutive audit items have failed.
11:17:32 11 Oct 2021	Info	Task 3	Paused due to error: 29 consecutive audit items have failed.
11:17:20 11 Oct 2021	Info	Task 3	Paused due to error: 28 consecutive audit items have failed.
11:16:53 11 Oct 2021	Error	Task 1	[174] Communication error: store.unity.com
11:16:53 11 Oct 2021	Error	Task 3	Paused due to error: 27 consecutive audit items have failed.
05:58:07 11 Oct 2021	Info	Task 3	Paused due to error: 26 consecutive audit items have failed.
05:58:07 11 Oct 2021	Info	Task 3	Paused due to error: 25 consecutive audit items have failed.
05:58:07 11 Oct 2021	Info	Task 3	Paused due to error: 24 consecutive audit items have failed.
04:59:15 11 Oct 2021	Error	Task 3	Paused due to error: 23 consecutive audit items have failed.
04:57:07 11 Oct 2021	Error	Task 3	Paused due to error: 22 consecutive audit items have failed.
04:48:59 11 Oct 2021	Error	Task 3	Paused due to error: 21 consecutive audit items have failed.
04:48:00 11 Oct 2021	Error	Task 3	Paused due to error: 20 consecutive audit items have failed.
04:48:00 11 Oct 2021	Error	Task 3	Paused due to error: 19 consecutive audit items have failed.
04:31:11 11 Oct 2021	Info	Task 3	Paused due to error: 18 consecutive audit items have failed.
04:31:11 11 Oct 2021	Info	Task 3	Paused due to error: 17 consecutive audit items have failed.
04:22:28 11 Oct 2021	Info	Task 3	Paused due to error: 16 consecutive audit items have failed.

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.



```
+ : bash — Konsole
File Edit View Bookmarks Settings Help
Executing nikto -h
[sudo] password for kasun:
Option host requires an argument

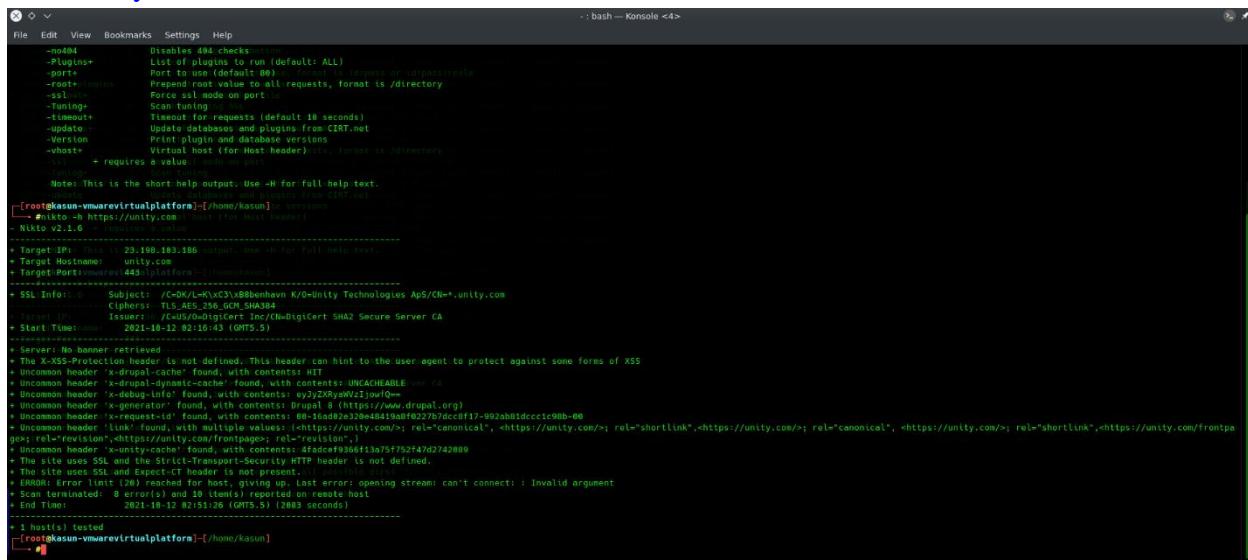
  -config=          Use this config file
  -display=         Turn on/off display outputs
  -dbscheck         Check database and other key files for syntax errors
  -format=          Define file (-o) format
  -Help             Extended help information
  -Host             Target host/URL
  -id=              Host authentication to use, format is id:pass or id:pass:realm
  -list-plugins     List all available plugins
  -output=          Write output to this file
  -port=            Port to use (default 80)
  -ssl=             Force ssl mode on port
  -Tuning           Scan tuning
  -timeout=         Timeout for requests (default 10 seconds)
  -update           Update databases and plugins from CIRT.net
  -Version          Print version and database versions
  -whost=           Virtual host (for Host header)
  -      + requires a value

  Note! This is the short help output. Use -H for full help text.

[root@kasun-vmwarevirtualplatform]~[~/home/kasun]
#
```

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

[www.unity.com](http://www.unity.com)



```
+ : bash — Konsole <4>
File Edit View Bookmarks Settings Help
  -no404           Disables 404 checks
  -plugins=         List of plugins to run (default: ALL)
  -port=            Port to use (default 80)
  -root=            Virtual host root value to all requests, format is /directory
  -ssl=             Force ssl mode on port
  -Tuning           Scan tuning
  -timeout=         Timeout for requests (default 10 seconds)
  -update           Update databases and plugins from CIRT.net
  -version          Print version and database versions
  -whost=           Virtual host (for Host header)
  -      + requires a value

  Note! This is the short help output. Use -H for full help text.

[root@kasun-vmwarevirtualplatform]~[~/home/kasun]# versions
  nikto -h https://unity.com/host (for Host header)
- Nikto v2.1.6
- Nikto is a security scanner for web servers
-----[SSL Info-----]
  Subject: /C=DK/L=K/x3/88b0nehm A/Unity Technologies Ap/CN=*.unity.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Current IP: 23.190.183.106
  Issuer: /C=US/O=DigiCert Inc/OU=DigiCert SHA2 Secure Server CA
  Start Time: 2021-10-12 02:16:43 (GMT+5)
-----[Server-----]
  Server: No banner retrieved
  The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
  Uncommon header 'x-drupal-cache' found, with contents: HIT
  Uncommon header 'x-drupal-dynamic-cache' found, with contents: UNCACHEABLE
  Uncommon header 'x-drupal-dynamic-reload' found, with contents: 0
  Uncommon header 'x-generator' found, with contents: Drupal 8 (https://www.drupal.org)
  Uncommon header '<x-request-id>' found, with contents: 00-1eadde2e320e4d419adbf0227b7dcdf17-992ab81dcc1c98b-00
  Uncommon header 'link' found, with multiple values: <https://unity.com/>; rel="canonical", <https://unity.com/>; rel="shortlink",<https://unity.com/>; rel="canonical",<https://unity.com/frontpage>; rel="shortlink",<https://unity.com/frontpage>; rel="canonical"
  The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
  The site uses SSL and Expect-CT header is not present.
-----[Error-----]
  ERROR: Error limit (20) reached for host, giving up. Last error: opening streams can't connect: : Invalid argument
  Scan terminated: 0 hosts tested (0 hosts up, 0 hosts down, 0 hosts partial)
  Total time: 2021-10-12 02:15:26 (GMT+5) (2083 seconds)

# 1 host(s) tested
[root@kasun-vmwarevirtualplatform]~[~/home/kasun]
#
```

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

## id.unity.com

```
- ; bash -- Konsole
File Edit View Bookmarks Settings Help
- - - - - ; bash -- Konsole
[+] Nikto v2.1.6
[+] Target IP: 34.120.204.121
[+] Target Hostname: id.unity.com
[+] Target Port: 443
[+] SSL Info: Subject: /C=DK/L=Copenhagen/OU=Unity Technologies ApS/CN=id.unity.com
[+] Ciphers: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
[+] Issuer: /C=US/O=digiCert Inc/CN=digiCert SHA2 Secure Server CA
[+] Start Time: 2021-10-12 02:17:51 (GMT+5.5)
[+] Server: No banner retrieved
[+] Retrieved via header: alt-svc found, with contents: clear-hsts=1; ma=2592000; h3-28
[+] Uncommon header 'x-request-id' found, with contents: f54b02fd-085e-4431-a52b-3822062701c1
[+] The site uses SSL and Expect-CT header is not present.
[+] Root page / redirects to: https://id.unity.com/en/login
[+] No dir/ directories found. Force check all downloadable dirs.
[+] Error limit (EDR) reached for host, giving up. Last error: opening stream: can't connect : Invalid argument
[+] Scan terminated: 2 error(s) and 3 item(s) reported on remote host
[+] End Time: 2021-10-12 02:45:42 (GMT5.5) (1691 seconds)

[+] 1 host(s) tested
[+] [root@kasun-vmwarevirtualplatform] [/home/kasun]
```

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

## dashboard.unity3d.com

```
- ; bash -- Konsole <3>
File Edit View Bookmarks Settings Help
- - - - - ; bash -- Konsole <3>
[+] Nikto v2.1.6
[+] Target IP: 34.182.142.05
[+] Target Hostname: dashboard.unity3d.com
[+] Target Port: 443
[+] SSL Info: Subject: /C=DK/L=KvCsxb0vhnhavn/OU=Unity Technologies ApS/CN=dashboard.unity3d.com
[+] Ciphers: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
[+] Issuer: /C=US/O=digiCert Inc/CN=digiCert TLS RSA SHA256 2020 CA1
[+] Start Time: 2021-10-12 02:18:08 (GMT5.5)
[+] Server: No banner retrieved
[+] Retrieved via header: alt-svc found, with contents: clear-hsts=1; ma=2592000; h3-28
[+] Uncommon header 'x-dns-prefetch-control' found, with contents: off
[+] The site uses SSL and Expect-CT header is not present.
[+] Root page / redirects to: https://dashboard.unity3d.com/auth/utility/redirectto@HHRcDovL2RhZhb2FyZCS1bmloetNKLdnvb5Bw=
[+] ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect : Invalid argument
[+] Scan terminated: 8 error(s) and 4 item(s) reported on remote host
[+] End Time: 2021-10-12 02:19:31 (GMT5.5) (1943 seconds)

[+] 1 host(s) tested
[+] [root@kasun-vmwarevirtualplatform] [/home/kasun]
```

Figure 35 I scanned dashboard.unity3d.com by nikto scan this figure shows some vulnerabilities of domain.

```

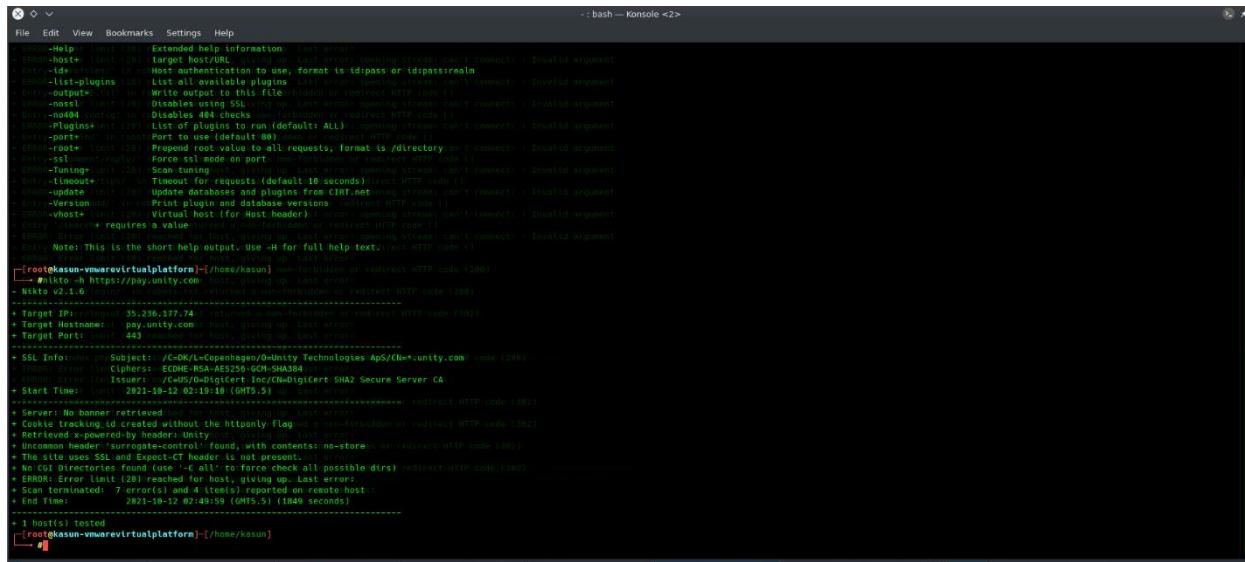
File Edit View Bookmarks Settings Help
https://store.unity.com
[+] http://store.unity.com:443
[+] https://store.unity.com:443
[+] nikto -h https://store.unity.com
[+] nikto -v2.1.6
[+] nikto -h https://store.unity.com
[+] nikto -h https://store.unity.com
[+] Target IP: 23.196.103.106
[+] Target Hostname: store.unity.com
[+] Target Port: 443
[+] Threads: 100 (try to keep threads below 80)
[+] Timeout: 10 sec
[+] Threads: 100 (try to keep threads below 80)
[+] Timeout: 10 sec
[+] SSL Info:
  Subject: /C=DE/OU=www.unity.com/CN=Unity Technologies APS/CN=*,unity.com
  Ciphers: TLS AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA Secure Server CA
  Start Time: 2021-10-12 02:18:29 (GMT+5)
[+] SSL Certificate Fingerprint: 00:16:AD:2F:B1:D2:CE:EF:FB:13:9E:93:C3:0E:0B:2B:97:CF:58:92:B0:E5:5A:00
[+] Server: No banner retrieved
[+] X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] Uncommon header 'permissions-policy' found, with contents: interest-cohort()
[+] Uncommon header 'x-drumsl-dynamic-cache' found, with contents: MISS
[+] Uncommon header 'x-drumsl-expire' found, with contents: 1634560000
[+] Uncommon header 'x-debug-info' found, with contents: eyJ2XbawVzjowQ==
[+] Uncommon header 'x-generator' found, with contents: drupal 9 (https://www.drupal.org)
[+] Uncommon header 'link' found, with multiple values: <https://store.unity.com/> rel="canonical", <https://store.unity.com/> rel="shortlink",</sites/default/files/css/css_517CFTvNlogjyomqIE3NnD560.mqQzvr8Uf7s0B.css>; rel="preload" type="text/css",</sites/default/files/css/css_517CFTvNlogjyomqIE3NnD560.mqQzvr8Uf7s0B.css>; rel="preload",<https://store.unity.com/sites/default/files/js/j.js.y5DHNCGKtq-21c09f2XX0t3y731z286E5yhQsQ.js>; rel="preload",<https://store.unity.com/sites/default/files/js/j.js.De2xF0xfk0p91i7lli-kbKXzT84Kt1Ydqfnh3W0XX0E.js>; rel="preload",<https://store.unity.com/sites/default/files/js/j.js.U2p4bfZAgnd8A19u_ZIfZ7tWp164w4cshng5g.js>; rel="preload",<script>
[+] Uncommon header 'x-request-id' found, with contents: 00:16:AD:2F:B1:D2:CE:EF:FB:13:9E:93:C3:0E:0B:2B:97:CF:58:92:B0:E5:5A:00
[+] Uncommon header 'x-strict-transport-security' found, with contents: max-age=31536000; includeSubDomains; preload
[+] The site uses SSL and Expect-CT header is not defined.
[+] The site uses 'Content-Security-Policy' header is not defined.
[+] The site uses 'Content-Security-Policy-Report-Only' header is not defined.
[+] CGI Directories found use '-C all' to force check all possible dirs
[+] Entry '/profiles/.svg' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Entry '/admin/.svg' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/robots.txt' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/web.config' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/comment/reply/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/filter/lops' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/index/add/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/search/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code ()
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/user/logout/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/user/logout?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/index.php/user/register?' in robots.txt returned a non-forbidden or redirect HTTP code (302)
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/index.php/user/login?' in robots.txt returned a non-forbidden or redirect HTTP code (302)
[+] Error: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: : Invalid argument
[+] Entry '/index.php/user/logout?' in robots.txt returned a non-forbidden or redirect HTTP code (502)
[+] "robots.txt" contains 40 entries which should be manually viewed. opening stream can't connect: : Invalid argument
[+] Scan terminated: 14 errors(s) and 38 items(s) reported on remote host
[+] End Time: 2021-10-12 02:57:38 (GMT+5) (2341 seconds)

1 host(s) tested
[+] 1

```

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

## pay.unity.com



```
- : bash -- Konsole <2>
File Edit View Bookmarks Settings Help
[+] http://pay.unity.com [+] http://pay.unity.com:443 [+] https://pay.unity.com [+] https://pay.unity.com:443
[+] Host: pay.unity.com [+] Target Host: pay.unity.com [+] Last error: connection stream can't connect: Invalid argument
[-] Id: - [+] Host: pay.unity.com [+] Target Host: pay.unity.com [+] Last error: connection stream can't connect: Invalid argument
[-] List-Plugins: [+] Host authentication to use, format is idpass or idpassrealm
[-] Plugins: [+] List all available plugins
[-] Output: [+] Write output to this file (default or redirect HTTP code)
[-] Plugins+Port: [+] List of plugins to run (default: ALL) - running streams can't connect: Invalid argument
[-] No-044: [+] Disables 404 checks
[-] Port: [+] Port to use (default: 80) - running streams can't connect: Invalid argument
[-] Plugins+Port: [+] List of plugins to run (default: ALL) - running streams can't connect: Invalid argument
[-] Port+: [+] Port to use (default: 80) - running streams can't connect: Invalid argument
[-] Plugins+Port: [+] Prepend host value to all requests, format is /directory [+] Last error: connection stream can't connect: Invalid argument
[-] Scan-Tuning: [+] Scan tune
[-] Tuning: [+] Scan tuning
[-] Timeout: [+] Timeout for requests (default: 10 seconds) - Last error: connection stream can't connect: Invalid argument
[-] Update: [+] Update database and plugins from CIRCT.net [+] Last error: connection stream can't connect: Invalid argument
[-] Version: [+] Print plugin and database versions [+] Last error: connection stream can't connect: Invalid argument
[-] Whois: [+] Virtual host (for Host-Header)
[-] Whois: [+] Whois requires a value
[-] Note: This is the short help output. Use -H for full help text [+] Last error: connection stream can't connect: Invalid argument
[+] Note: This is the short help output. Use -H for full help text [+] Last error: connection stream can't connect: Invalid argument

[+] Nikto v2.1.6 - Web Application Security Scanner [+] Nikto v2.1.6 - Web Application Security Scanner
[+] Target IP: 35.239.177.74 [+] Target IP: 35.239.177.74 [+] Last error: connection stream can't connect: Invalid argument
[+] Target Hostname: pay.unity.com [+] Target Hostname: pay.unity.com [+] Last error: connection stream can't connect: Invalid argument
[+] Target Port: 80 [+] Target Port: 443 [+] Last error: connection stream can't connect: Invalid argument
-----[+] SSL Info: [+] Subject: /CN=K/L/OpenSource/Unity Technologies ApS/CN=unity.com [+] End date (1886)
-----[+] Ciphers: ECDHE-RSA-AES256-GCM-SHA384 [+] Ciphers: ECDHE-RSA-AES256-GCM-SHA384
-----[+] Expired Date: [+] Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
-----[+] Start Time: 2021-08-12 02:19:10 (GMT+5) [+] Last error: connection stream can't connect: Invalid argument
-----[+] Server: No banner retrieved
-----[+] Cookie Tracking ID created without the httponly flag and a non-expiration or redirect HTTP code (1882)
-----[+] Retrieved x-powered-by header: Unity [+] Last error: connection stream can't connect: Invalid argument
-----[+] Uncommon header 'surrogate-control' found, with contents: no-store [+] Last error: connection stream can't connect: Invalid argument
-----[+] TLS 1.3 uses SNI and ECDHE-CT header [+] Last error: connection stream can't connect: Invalid argument
-----[+] No CGI Directories found (use -all- to force check all possible dirs) [+] Last error: connection stream can't connect: Invalid argument
-----[+] ERROR: Error limit (20) reached for host, giving up. Last errors:
-----[+] Scan terminated: 7 errors(s) and 4 item(s) reported on remote host:
-----[+] End Time: 2021-08-12 02:49:59 (GMT+5) (1849 seconds)

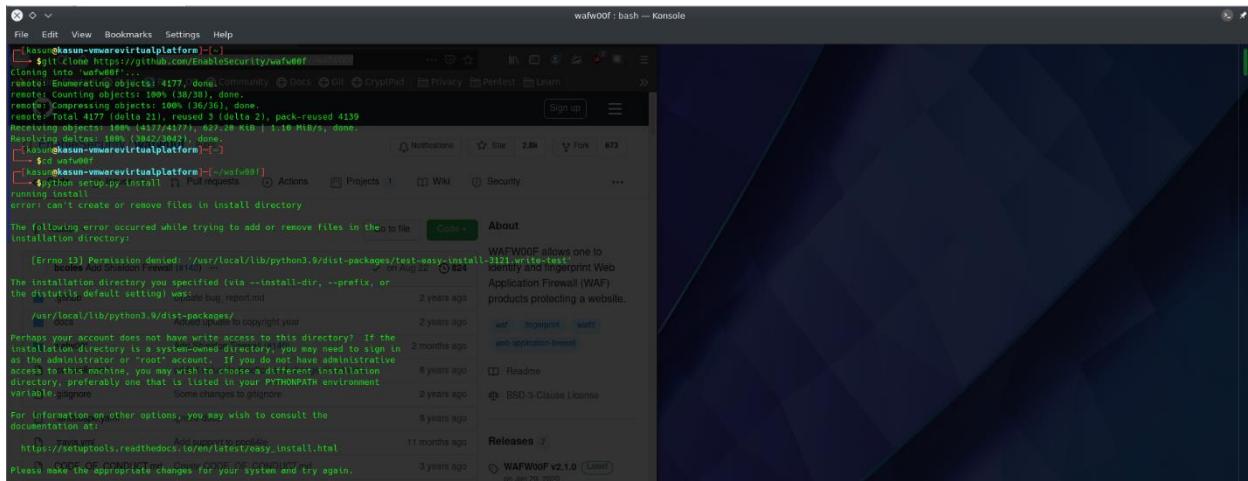
[+] 1 host(s) tested
[+] #
```

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 .



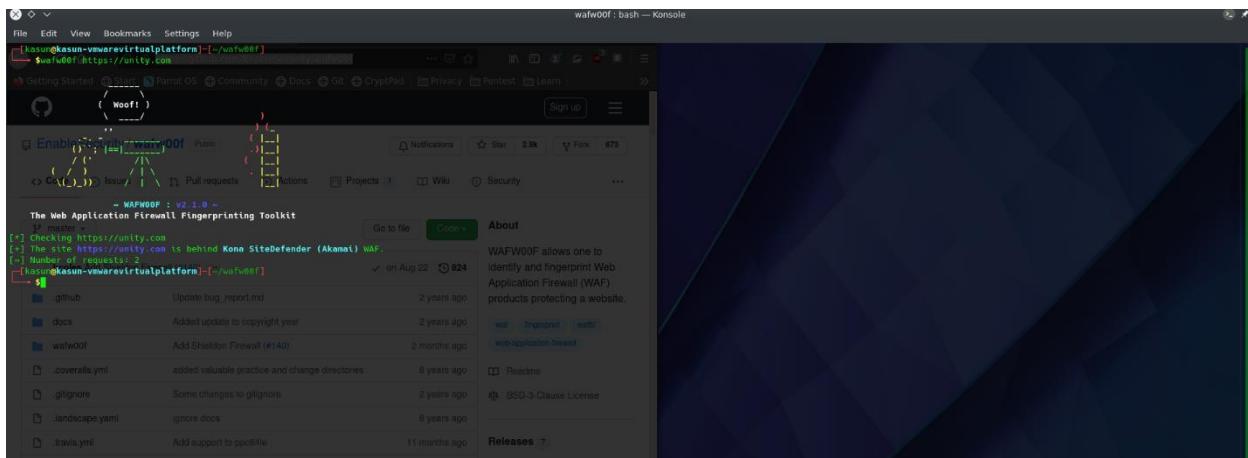
```
git clone https://github.com/EnableSecurity/wafw00f
Cloning into 'wafw00f'...
remote: Enumerating objects: 4177, done.
remote: Counting objects: 1000 (36/36), done.
remote: Compressing objects: 1000 (36/36), done.
remote: Total 4177 (delta 21), reused 3 (delta 2), pack-reused 4139
Receiving objects: 100% (4177/4177) | 627.20 KiB | 1.10 MiB/s, done.
Resolving deltas: 100% (36/36), done.
python setup.py install
running install
error: can't create or remove files in install directory

The following error occurred while trying to add or remove files in the directory:
installation directory:

[Errno 13] Permission denied: '/usr/local/lib/python3.9/dist-packages/test-easy-install-3.12.1/write-test'
The installation directory you specified (via --install-dir, --prefix, or
the distutils default setting) was not writable.

/usr/local/lib/python3.9/dist-packages/
  docs      Added update to copyright year
  pytests   Added update to copyright year
Perhaps your account does not have write access to this directory? If the
installation directory is listed in $PYTHONPATH, you might be able to run it
as the administrator or 'root' account. If you do not have administrative
access to this machine, you may wish to choose a different installation
directory, preferably one that is listed in the PYTHONPATH environment
variable.ignores  Some changes to ignore
For information on other options, you may wish to consult the
documentation at:
  https://setuptools.readthedocs.io/en/latest/easy_install.html
Please make the appropriate changes for your system and try again.
```

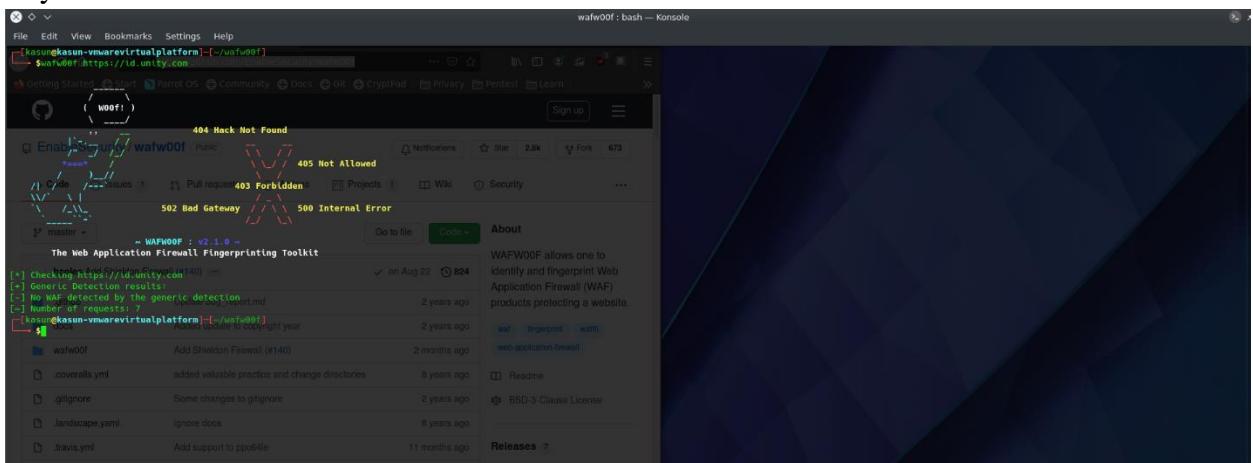
Figure 38 installation of wafw00f tool for scanning firewalls behind domains.



```
Getting Started  Fork! OS  Community  Docs  GitHub  CryptPad  Privacy  Pentest  Learn  Sign up  ...
WAFW00F : v2.1.0 - The Web Application Firewall Fingerprinting Toolkit
  master
  Checking https://unity.com
  the site https://unity.com is behind Kona SiteDefender (Akamai) WAF.
  No requests made.
[kasun@kasun-vmwarevirtualplatform:~/wafw00f]$
```

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

## id.unity.com

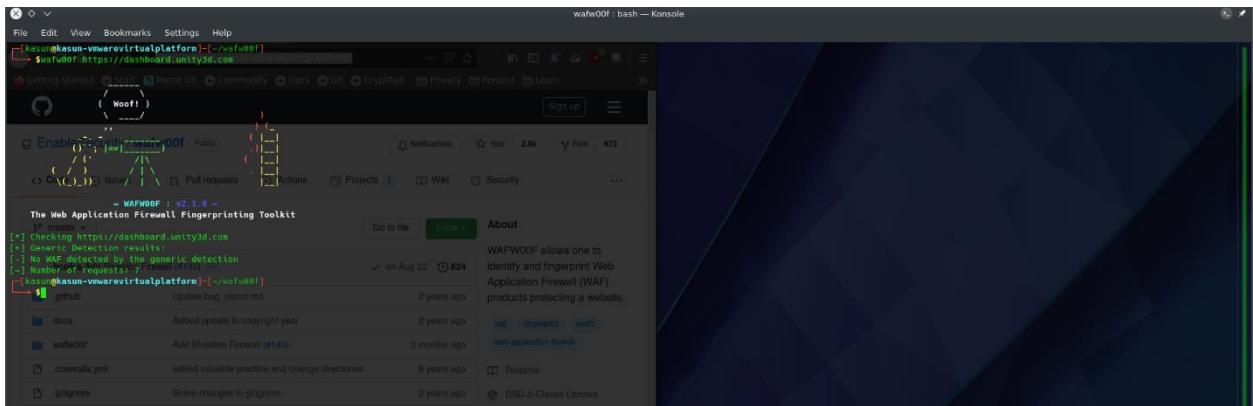


```
wafw00f : bash — Konsole
kasun@kasun-vmwarevirtualplatform:[~]/wafw00f
$ wafw00f https://id.unity.com
Getting Started · Start · About OS · Community · Docs · GitHub · CryptPad · Privacy · Pentest · Learn · ...
Sign up · ...
About · ...
WAFW00F allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.

[*] Checking https://id.unity.com [404]
[-] Generic Detection results:
[+] No WAF detected by the generic detection
[+] Number of requests: 7 / Total(10)
kasun@kasun-vmwarevirtualplatform:[~]/wafw00f
$
```

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

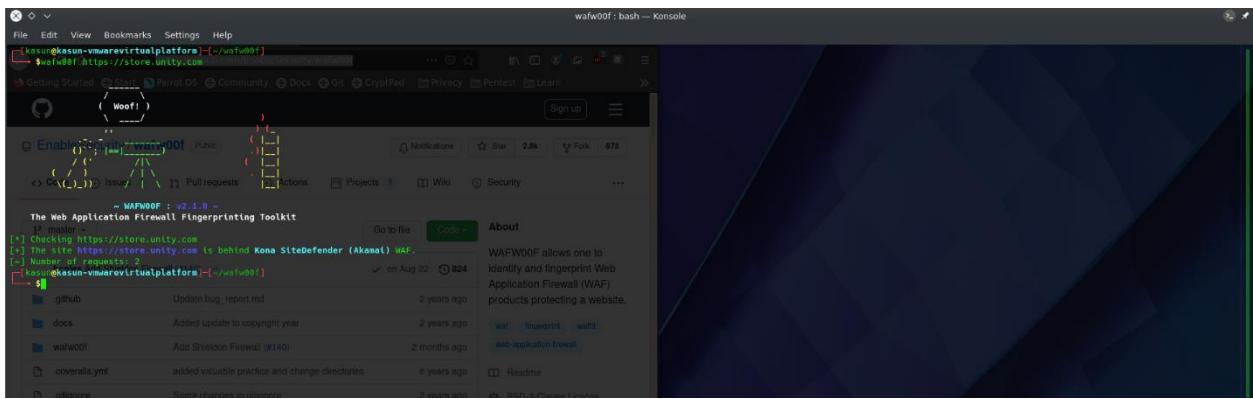


```
wafw00f : bash — Konsole
kasun@kasun-vmwarevirtualplatform:[~]/wafw00f
$ wafw00f https://dashboard.unity3d.com
Getting Started · Start · About OS · Community · Docs · GitHub · CryptPad · Privacy · Pentest · Learn · ...
Sign up · ...
About · ...
WAFW00F allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.

[*] Checking https://dashboard.unity3d.com
[-] Generic Detection results:
[+] No WAF detected by the generic detection
[+] Number of requests: 7 / Total(10)
kasun@kasun-vmwarevirtualplatform:[~]/wafw00f
$
```

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

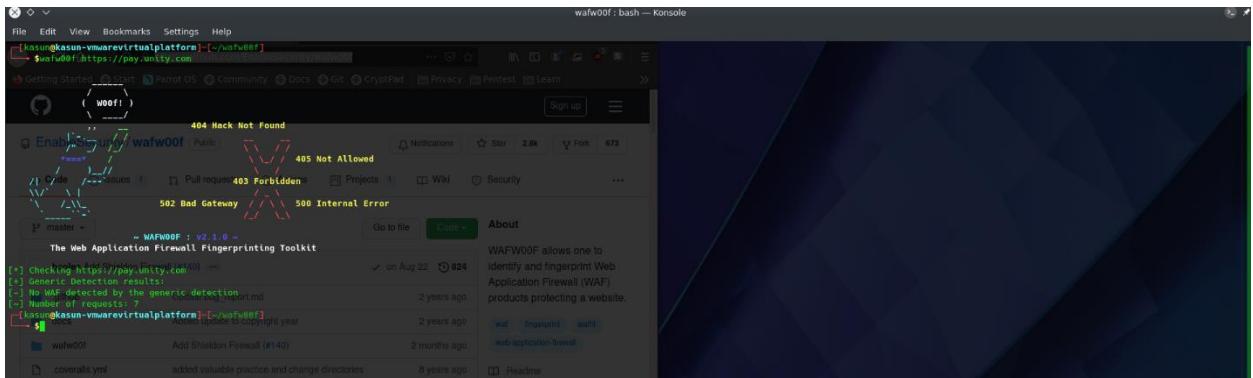
store.unity.com



```
wafw00f : bash — Konsole
kasun@kasun-vmwarevirtualplatform:~/wafw00f$ ./wafw00f https://store.unity.com
[*] Checking https://store.unity.com
[+] The site https://store.unity.com is behind Kona SiteDefender (Akamai) WAF.
[-] Number of requests: 2
kasun@kasun-vmwarevirtualplatform:~/wafw00f$
```

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

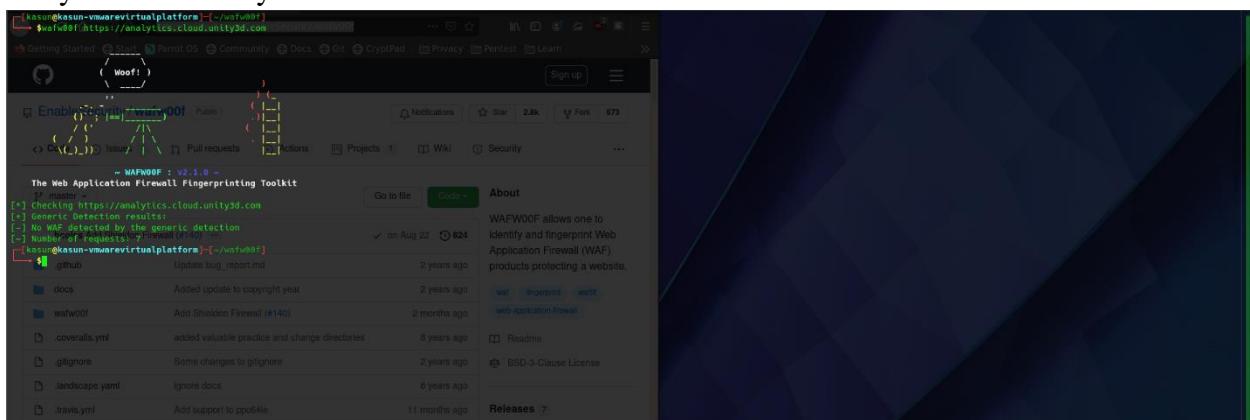
pay.unity.com



```
wafw00f : bash — Konsole
kasun@kasun-vmwarevirtualplatform:~/wafw00f$ ./wafw00f https://pay.unity.com
[*] Checking https://pay.unity.com
[+] Generic detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
kasun@kasun-vmwarevirtualplatform:~/wafw00f$
```

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



```
wafw00f : bash — Konsole
kasun@kasun-vmwarevirtualplatform:~/wafw00f$ ./wafw00f https://analytics.cloud.unity3d.com
[*] Checking https://analytics.cloud.unity3d.com
[+] Generic detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
kasun@kasun-vmwarevirtualplatform:~/wafw00f$
```

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](http://www.unity.com)

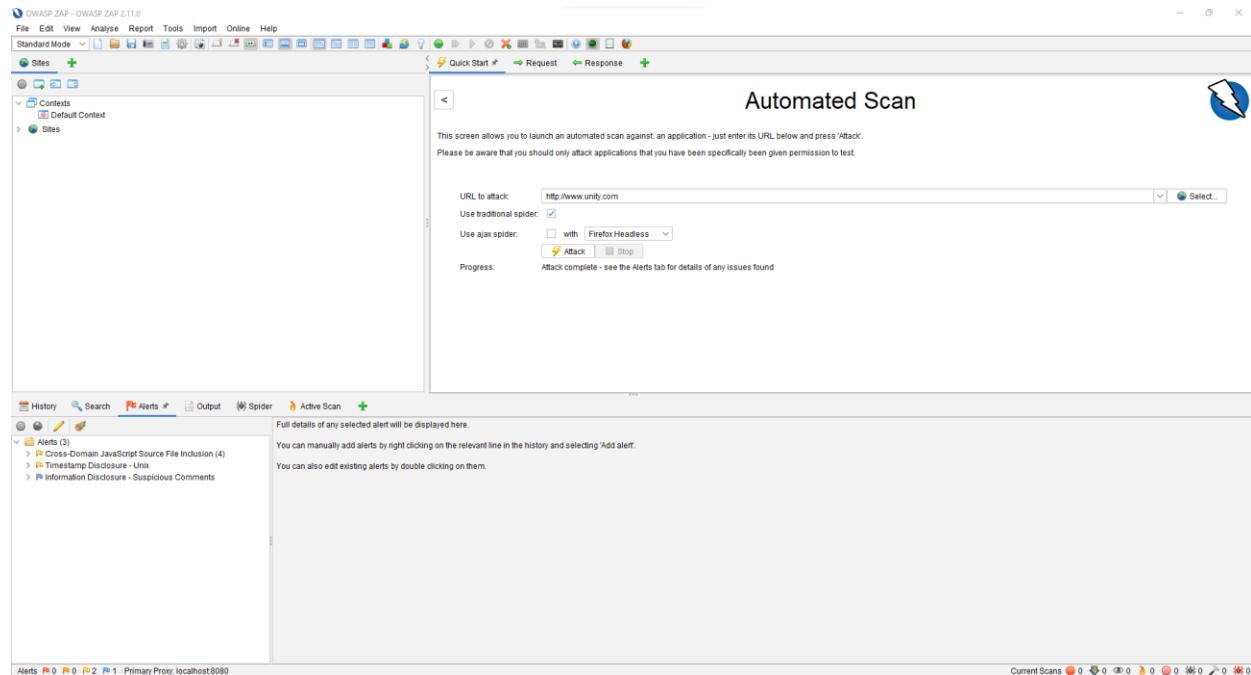


Figure 45 I scanned unity.com by owsap zap and I got 3 alerts after scanning whole site .

## id.unity.com

**CSP-Wildcard Directive**

URL: http://id.unity.com  
Risk: Medium  
Confidence: Medium  
Parameter:  
Attack: Evidence: frame-ancestors self  
CWE ID: 693  
WASC ID: 15  
Source: Passive (10055 - CSP)  
Description: The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:  
script-src, style-src, img-src, connects-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src, form-action  
Other Info:

**Solution:**  
Ensure that your web server, application server, load balancer, etc. is properly configured to set the

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

## dashboard.unity3d.com

**Attack**

URL to attack: http://dashboard.unity3d.com  
Use traditional spider:  Select...

Use ajax spider:  with: FireFox Headless  
Attack Stop  
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

**Alerts (3)**

> X-Frame-Options Header Not Set (2)  
> Incomplete or No Cache-control Header Set (3)  
> Server Leaks Information via 'X-Powered-By' HTTP Response Header Field(s) (4)  
> Timestamp Disclosure - Unix (8)  
> X-Content-Type-Options Header Missing (4)  
> Information Disclosure - Suspicious Comments (4)

**Evidence**  
CWE ID: 1021  
WASC ID: 15  
Source: Passive (10020 - X-Frame-Options Header)  
Description: X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.  
Other Info:

**Solution:**  
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY.  
Reference:  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

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

## Store.unity.com

The screenshot shows the OWASP ZAP 2.11.0 interface with a scan of the domain `store.unity.com`. The Alerts tab displays 6 alerts:

- Vulnerable JS Library (6)**
  - Cross-Domain JavaScript Source File Inclusion (1512)
  - Incomplete or No Cache-control Header Set (742)
  - Timestamp Disclosure - Unix (192)
  - X-Content-Type-Options Header Missing (72)
  - Information Disclosure - Suspicious Comments (819)

A detailed alert for `bootstrap.js` is expanded, showing the following details:

- Vulnerable JS Library**
- URL:** `https://store.unity.com/sites/default/files/js/_De2/F0X0fP517lI-kbXcT84kYm0gfmh3W0XOE.js`
- Confidence:** Medium
- Parameter:**
- Attack:**
- Evidence:** `* Bootstrap v3.7`
- CWE ID:** 829
- WASC ID:**
- Source:** Passive (10003 - Vulnerable JS Library)
- Description:** The identified library bootstrap, version 3.3.7 is vulnerable.
- Other Info:**
  - CVE-2018-8531
  - CVE-2018-14041
  - CVE-2018-14040
- Solution:** Please upgrade to the latest version of bootstrap.

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

## analytics.cloud.unity3d.com

The screenshot shows the OWASP ZAP 2.11.0 interface with a scan of the domain `analytics.cloud.unity3d.com`. The Alerts tab displays 8 alerts:

- CSP: Wildcard Directive (8)**
  - CSP: Notices
  - Cookie Without HttpOnly Flag
  - Cookie Without Secure Flag
  - Cookie without SameSite Attribute (3)
  - Cross-Domain JavaScript Source File Inclusion (5)
  - Incomplete or No Cache-control Header Set
  - X-Content-Type-Options Header Missing

A detailed alert for `CSP: Wildcard Directive` is expanded, showing the following details:

- CSP: Wildcard Directive**
- URL:** `http://analytics.cloud.unity3d.com`
- Confidence:** Medium
- Parameter:**
- Attack:**
- Evidence:** `frame-ancestors self`
- CWE ID:** 693
- WASC ID:**
- Source:** Passive (10055 - CSP)
- Description:** The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connects-src, frame-src, font-src, media-src, object-src, worker-src, prefetch-src, form-action
- Other Info:**
  - Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

Figure 49 I scanned analytics.cloud.unity.com by owasap 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

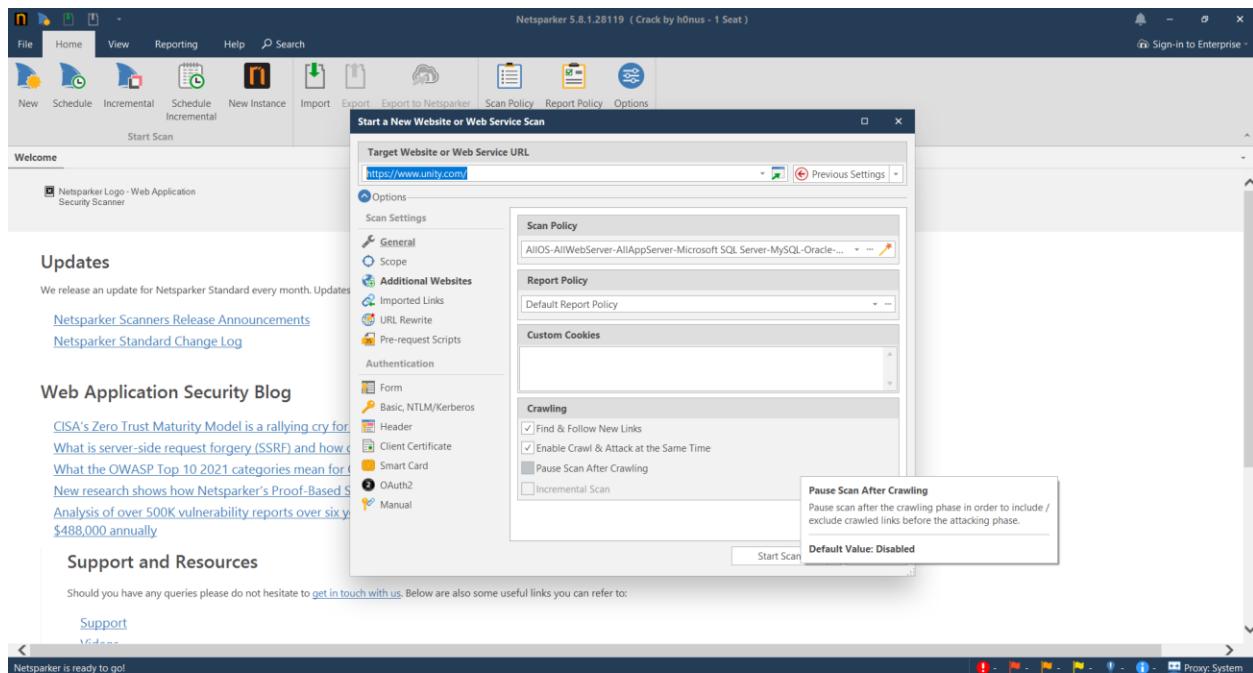


Figure 50 interface of netspaker tool

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.

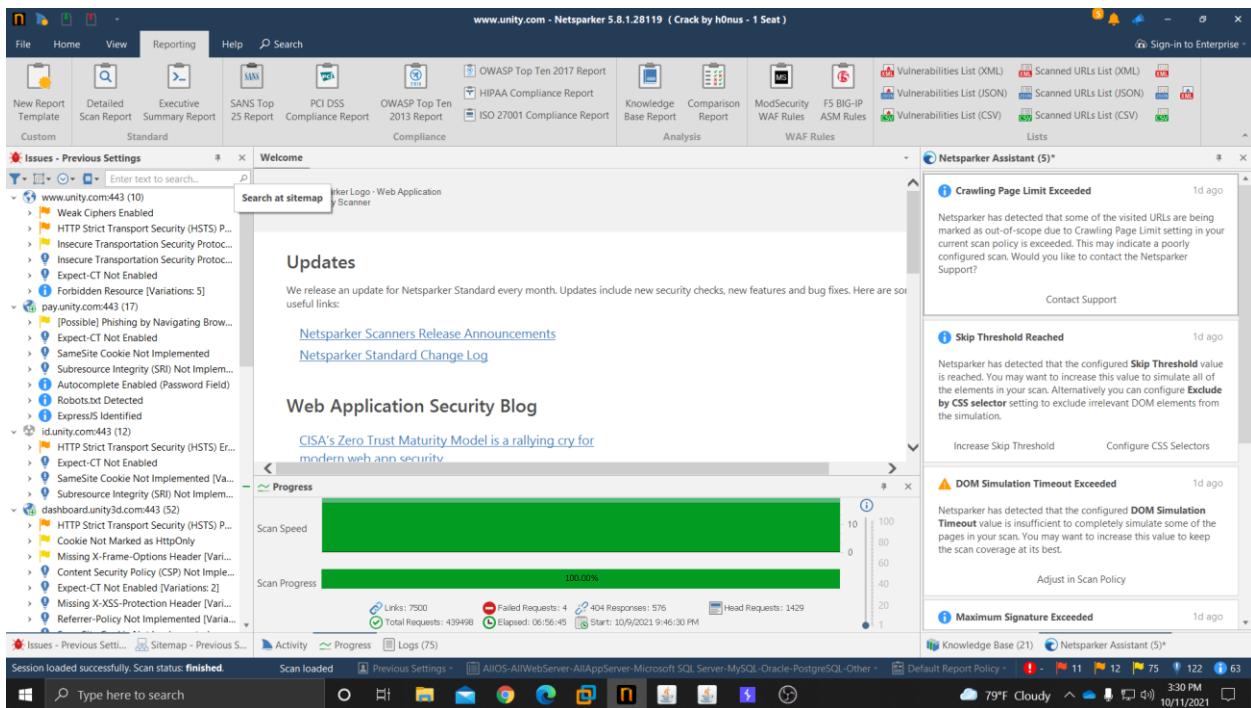


Figure 51 i scanned all in scope domains including

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\*\*](#)

# netsparker

10/10/2021 4:56:14 AM (UTC+05:30)

## Detailed Scan Report

🔗 https://www.unity.com/

Scan Time : 10/9/2021 9:46:30 PM (UTC+05:30)  
Scan Duration : 00:06:56:45  
Total Requests : 439,498  
Average Speed : 17.6r/s

Risk Level:  
**HIGH**

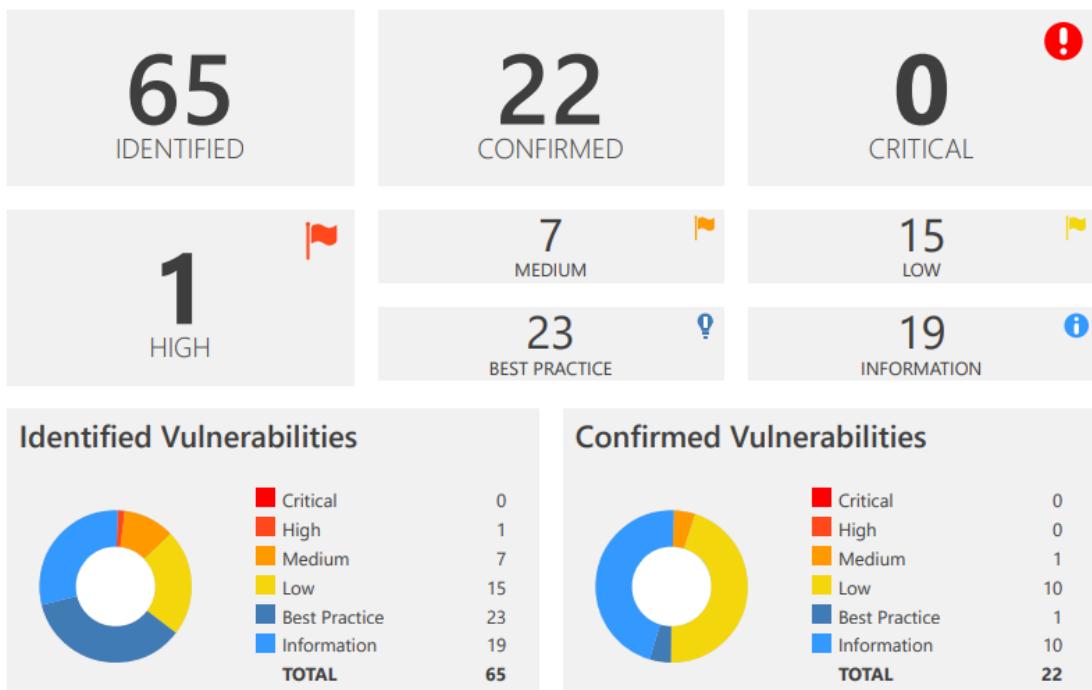


Figure 52 after about 7 hours scanning I got full detailed report regarding the vulnerabilities of in scope domains

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
!	<a href="#">Out-of-date Version (Modernizr)</a>	GET	https://store.unity.com/de	
!	<a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a>	GET	https://id.unity.com/	
!	<a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a>	GET	https://dashboard.unity3d.com/	
!	<a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a>	GET	https://store.unity.com/	
!	<a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a>	GET	https://www.unity.com/	
!	<a href="#">Out-of-date Version (Bootstrap)</a>	GET	https://store.unity.com/sites/default/files/js/js_De2XFQXfkoP51i7l li-kbXKzT84KtYmdqFmh3W0XX0E.js	
!	<a href="#">Weak Ciphers Enabled</a>	GET	https://www.unity.com/	
!	<a href="#">[Possible] Phishing by Navigating Browser Tabs</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">[Possible] Phishing by Navigating Browser Tabs</a>	GET	https://pay.unity.com/os2/orders/new?locale=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	locale
!	<a href="#">[Possible] Phishing by Navigating Browser Tabs</a>	GET	https://store.unity.com/	
!	<a href="#">Missing X-Frame-Options Header</a>	GET	https://dashboard.unity3d.com/auth/	

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

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	<a href="#">Cookie Not Marked as HttpOnly</a>	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,ee a820b6,0,190,1aa4331,0,%22Win32,f54683f2,0,%22Google%20In c,af794515,0,%225.0%2028Windows%20NT%2010.03b%20x642 9%20AppleWebKit2f537.36%2028KHTML2c%20like%20Gecko2 9%20Chrome2f70.0.3538.77%20Safari2f537.36,d81723d1,0,%22e n2dUS,5cc3ab5f,0,%22Mozilla2f5.0%2028Wind...	
!	<a href="#">Cookie Not Marked as HttpOnly</a>	GET	https://store.unity.com/de	
!	<a href="#">Cookie Not Marked as Secure</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">Cookie Not Marked as Secure</a>	GET	https://store.unity.com/de	
!	<a href="#">Insecure Frame (External)</a>	GET	https://store.unity.com/de	
!	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.0)</a>	GET	https://www.unity.com/	
!	<a href="#">Internal Server Error</a>	POST	https://analytics.cloud.unity3d.com/	
!	<a href="#">User Controllable Cookie</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">Windows Short Filename</a>	OPTIONS	https://store.unity.com/ruthemes/store/images/*~1*%5ca.aspx?a spxerrorpath=/	
!	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	https://dashboard.unity3d.com/auth/	
!	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	https://store.unity.com/rpiframe.html	
!	<a href="#">Expect-CT Not Enabled</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">Expect-CT Not Enabled</a>	GET	https://dashboard.unity3d.com/	
!	<a href="#">Expect-CT Not Enabled</a>	GET	https://id.unity.com/	

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

		<a href="#">Expect-CT Not Enabled</a>	GET	https://www.unity.com/
		<a href="#">Missing X-XSS-Protection Header</a>	GET	https://dashboard.unity3d.com/auth/
		<a href="#">Missing X-XSS-Protection Header</a>	GET	https://store.unity.com/themes/contrib/unity_base/js/unity-cdp.js
		<a href="#">Referrer-Policy Not Implemented</a>	GET	https://dashboard.unity3d.com/auth/
		<a href="#">Referrer-Policy Not Implemented</a>	GET	https://store.unity.com/rpiframe.html
		<a href="#">SameSite Cookie Not Implemented</a>	GET	https://analytics.cloud.unity3d.com/
		<a href="#">SameSite Cookie Not Implemented</a>	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,ee820b6,0,190,1aa4331,0,%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...
		<a href="#">SameSite Cookie Not Implemented</a>	GET	https://id.unity.com/
		<a href="#">SameSite Cookie Not Implemented</a>	GET	https://pay.unity.com/os2/orders/new
		<a href="#">SameSite Cookie Not Implemented</a>	GET	https://store.unity.com/de
		<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	https://analytics.cloud.unity3d.com/
		<a href="#">Subresource Integrity (SRI) Not Implemented</a>	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,ee820b6,0,190,1aa4331,0,%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...

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

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	https://id.unity.com/c:/boot.ini	URI-BASED
!	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	https://pay.unity.com/c:/boot.ini	URI-BASED
!	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	https://store.unity.com/	
!	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.1)</a>	GET	https://www.unity.com/	
!	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	https://store.unity.com/themes/c:/apple-touch-icon.png?v=%2527	v
!	<a href="#">Apache Web Server Identified</a>	GET	https://analytics.cloud.unity3d.com/robots.txt	
!	<a href="#">CDN Detected (Google Cloud CDN)</a>	GET	https://dashboard.unity3d.com/	
!	<a href="#">Content Security Policy (CSP) Keywords Not Used Within Single Quotes</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">Email Address Disclosure</a>	GET	https://store.unity.com/sites/default/files/js/js_y5DhFNCcGkfQ-21sG91FZX0tU0y73izZRE05jyh6sQA.js	
!	<a href="#">ExpressJS Identified</a>	GET	https://pay.unity.com/robots.txt	
!	<a href="#">Generic Email Address Disclosure</a>	GET	https://store.unity.com/themes/contrib/unity_base/css/unity-enty-po-plus.css	
!	<a href="#">Missing object-src in CSP Declaration</a>	GET	https://analytics.cloud.unity3d.com/	
!	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	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.

#### **Vulnerabilities**

1.1. <https://store.unity.com/de>

##### **Identified Version**

- 2.5.3

##### **Latest Version**

- 3.11.8 (in this branch)

##### **Vulnerability Database**

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

#### **Certainty**



## **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=BAh7B0kiD3Nlc3Npb25faWQG0gZFVEkiJTYzODAxMTZhY2IxMzU0NWQ0ZGVmOGRkMTc2YTdYzQ
zBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkimTzldGVJUDFPcmI3LzJkdFU1Ym1RYkU0Y3gwMFhIZU51MkJsM2xLvW14Ykk9BjsARG%3D%
3D--3eb62891a15b341f64370b94e9bdf6b219441c5
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: referer=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.unity3d.com%2F  
Date: Sat, 09 Oct 2021 16:17:11 GMT

8.2. <https://store.unity.com/de>

**CONFIRMED**

**Identified Cookie(s)**

- eupubconsent
- sjSE
- OptanonConsent
- OptanonAlertBoxClosed

**Cookie Source**

- JavaScript

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](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 [regedit32](#) or type [regedit](#), and then click OK.

b. In Registry Editor, locate the following registry key: [HKLW\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=BAh7B0kiD3Nlc3Npb25faWQG0gZFVEkiJTYzODAxMTZhY2IxMzU0NWQ0ZGVmOGRkMTc2YTdiYzQ
zBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkMTZldGVJUDFPcmI3LzJkdFU1Ym1RYkU0Y3gwMFhIZU51MkJsM2xLVWl4Ykk9BjsARg%3D%
3D--3eb62891a15b341f64370b94e9bdf6b219441c5
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.unity3d.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 Tunnel](#) to 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 regedit32 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\
```

- Locate a key named Server or create if it doesn't exist.
  - 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](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.