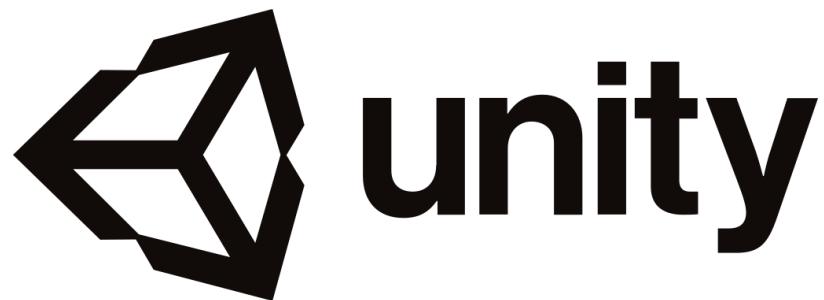




WEB AUDIT

WWW.UNITY.COM



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

Introduction	4
Enumeration	5
Sublist3r	6
Recon-ng	9
Crt.sh	10
Wappalyzer	12
Securityheaders.com	14
Built With.com	16
Shodan	17
Auditing and testing for Vulnerabilities	19
Nmap	19
Burp Suite	23
Nikto Scanner	26
Wafw00f	30
OWASP ZAP	33
Netspaker	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
- id.unity.com
- dashboard.unity3d.com
- store.unity.com
- pay.unity.com
- analytics.cloud.unity3d.com

Enumeration

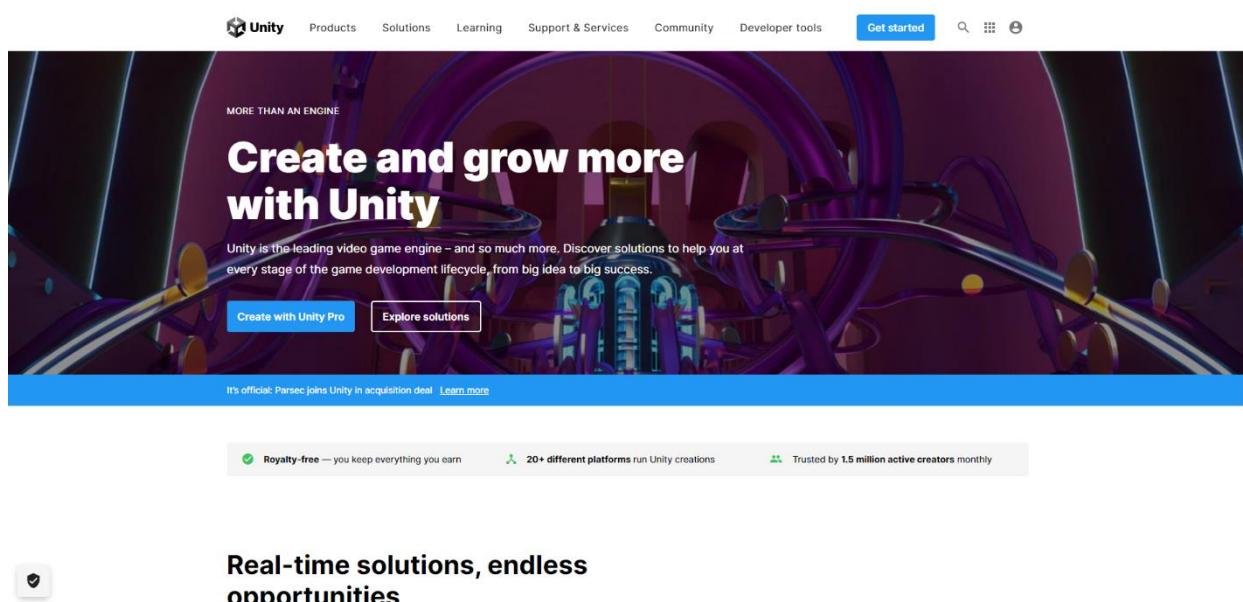


Figure 2 Unity.com website

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

Sublist3r

In beginning of the audit, my first step is enumerate subdomains of unity.com .For that process I used a tool named “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

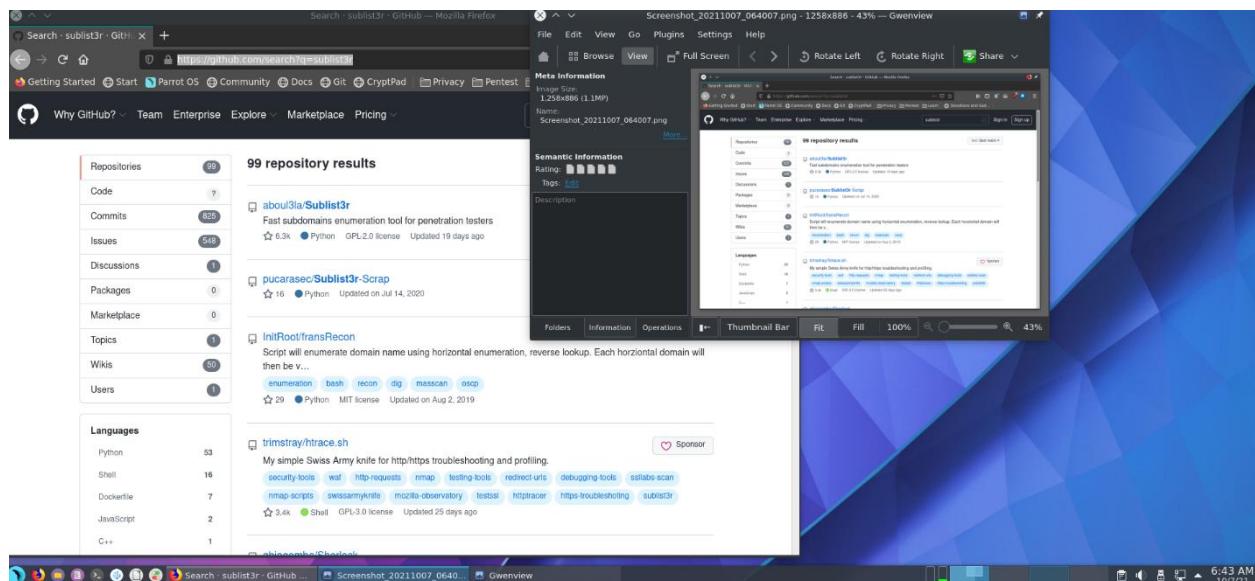
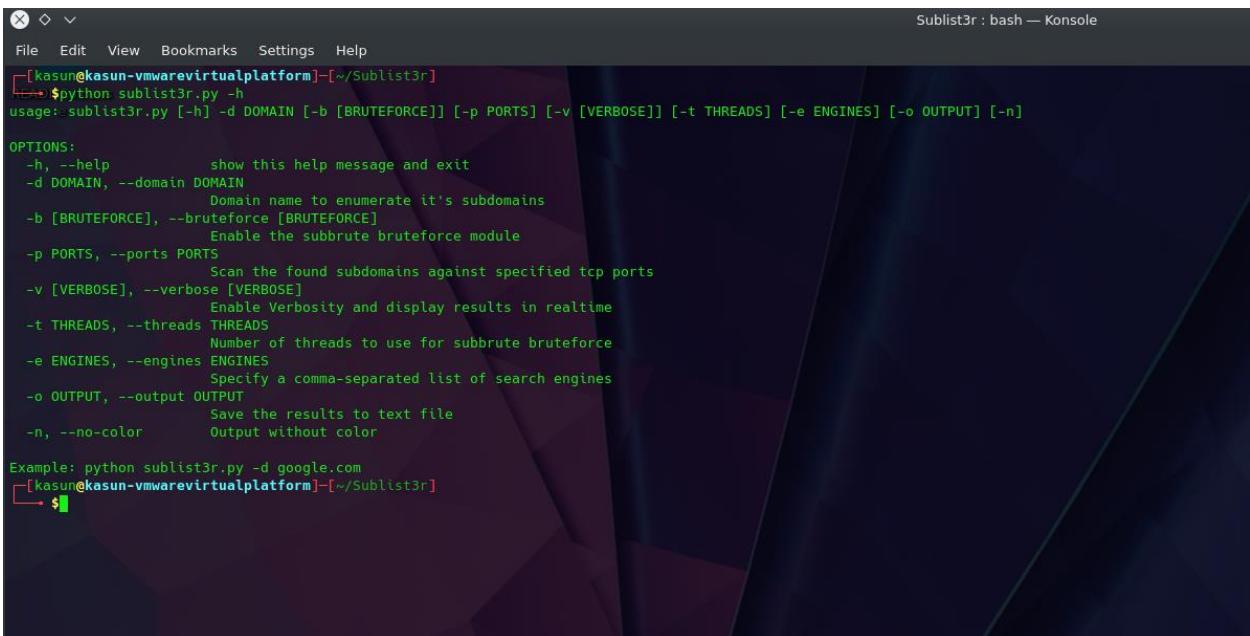


Figure 3 sublist3r in github

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

#python sublist3r.py -h



The screenshot shows a terminal window titled "Sublist3r : bash — Konsole". The command \$python sublist3r.py -h is run, displaying the tool's usage and options. The usage information includes:

```
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
```

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 has a dark background with a purple and blue geometric pattern. At the top, there's a menu bar with "File", "Edit", "View", "Bookmarks", "Settings", and "Help". Below the menu, there's some example usage information and a copyright notice. The main part of the terminal shows the progress of the subdomain enumeration for the domain "unity.com". It lists various search engines and databases checked, followed by a note about VirusTotal blocking requests. The final output shows 177 unique subdomains found, including "stage.microsoftpartnercommunity.com", "www.unibetcommunity.com", "www.unity.com", and numerous subdomains under "unity.com" such as "aisummit2020.unity.com", "answers.unity.com", "api.unity.com", etc.

```
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 — Konsola

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:
  Harvester 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
unity.com => unity.com
[recon-ng][default][google_site_web] > info

  Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.8

Description:
  Harvester 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][default][google_site_web] > run
-Explorers
-----
UNITY.COM
-----
[*] Searching Google for: site:unity.com
[*] Country: None
[*] Host: brandunity.com
[*] Ip.Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] To: None
[*] -----
[*] Country: None
[*] Host: assetstore.unity.com
[*] Ip.Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] To: None
[*] -----
[*] Country: None
[*] Host: app.unity.com
[*] Ip.Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] To: None
[*] -----
[*] Country: None
[*] Host: ole.unity.com
[*] Ip.Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] To: None
[*] -----
[*] Country: None
[*] Host: learn.unity.com
[*] Ip.Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] To: None
```

Figure 7 output of recon-*ng* after scanning

```
File Edit View Bookmarks Settings Help
recon-ng — Konsole

[*] Country: None
[*] Host: on.unity.com
[*] Ip: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Zip: None
[*] Country: None
[*] Host: resources.unity.com
[*] Ip: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Zip: None
[*] Country: None
[*] Host: identity.unity.com
[*] Ip: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Zip: None
[*] Country: None
[*] Host: store.unity.com
[*] Ip: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Zip: None
[*] Search 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:play.unity.com -site:on.unity.com -site:resources.unity.com -site:id.unity.com -site:store.unity.com
[*] Country: None
[*] Host: answers.unity.com
[*] Ip: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Zip: None
[*] Search 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:answers.unity.com
No New Subdomains Found on the Current Page. Jumping to Step 201.
[*] Search Google for: site:unity.com -site:brand.unity.com -site:assetstore.unity.com -sitesupr.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:answers.unity.com
```

Figure 8 output of recon-*ng* after scanning

```
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: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: forums.unity3d.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: support.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: forums.unity3d.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
[+] Country: None
[+] Host: forums.unity3d.com
[+] Ip:Address: None
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+]
```

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	CHUB_OrLet's Encrypt_CNR#3
	532645289	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CHUB_OrLet's Encrypt_CNR#3
	521288904	2021-10-01	2021-07-13	2022-08-13*	services.api.unity.com	* services.api.unity.com	CHUB_OndigCert 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	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5311044591	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	531104558	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	520720536	2021-09-27	2021-09-27	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5297380118	2021-09-27	2021-09-27	2021-12-26	on.unity.com	on.unity.com	CHUB_OrLet's Encrypt_CNR#3
	527824337	2021-09-24	2021-09-23	2022-08-23*	unity.com	* unity.com	CHUB_OndigCert Inc. CN=DigiCert SHA2 Secure Server.CA
	5278989459	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5278984439	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5270704744	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5270702329	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258194803	2021-09-21	2021-09-21	2021-12-20	www.uniforma-event.unity.com	uniforma-event.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258195521	2021-09-21	2021-09-21	2021-12-20	www.uniforma-event.unity.com	uniforma-event.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258192831	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258192811	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5252195757	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5362417070	2021-09-29	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5211395357	2021-09-19	2021-09-13	2021-12-12	sanc441.cdnfwrk.com	sanc441.cdnfwrk.com	CHUB_OrLet's Encrypt_CNR#3
	5207204274	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5207205636	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5207204277	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5178349377	2021-09-26	2021-09-26	2021-12-05	uniteuno.unity.com	uniteuno.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5173780057	2021-09-26	2021-09-26	2021-12-05	unite2020.unity.com	unite2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5173723716	2021-09-26	2021-09-26	2021-12-05	unite2020.unity.com	unite2020.unity.com	CHUB_OrGoogle 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	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160872410	2021-09-26	2021-09-26	2021-12-05	docs-uniteuno.unity.com	docs-uniteuno.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5160872359	2021-09-04	2021-07-08	2021-10-06	docs-stg.unity.com	docs-stg.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160872359	2021-09-04	2021-07-08	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160879932	2021-09-04	2021-07-19	2021-11-17	staging.services.api.unity.com	staging.services.api.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5152644900	2021-09-04	2021-07-19	2021-11-17	staging.services.api.unity.com	staging.services.api.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5152644918	2021-09-01	2021-09-18	2021-11-16	stagesservices.unity.com	stagesservices.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5136198204	2021-09-31	2021-09-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5136192419	2021-08-31	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128908186	2021-08-29	2021-08-29	2021-11-27	blog-api.unity.com	blog-api.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128627460	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128627464	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5120315513	2021-08-28	2021-08-28	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CHUB_OrGoogle 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	CHUB_OrLet's Encrypt_CNR#3
	532645289	2021-10-01	2021-10-01	2021-12-30	upo.unity.com	upo.unity.com	CHUB_OrLet's Encrypt_CNR#3
	521288904	2021-10-01	2021-07-13	2022-08-13*	services.api.unity.com	* services.api.unity.com	CHUB_OndigCert 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	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5311044591	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	531104558	2021-09-30	2021-09-29	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	520720536	2021-09-27	2021-09-27	2021-12-28	ole.unity.com	ole.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5297380118	2021-09-27	2021-09-27	2021-12-26	on.unity.com	on.unity.com	CHUB_OrLet's Encrypt_CNR#3
	527824337	2021-09-24	2021-09-23	2022-08-23*	unity.com	* unity.com	CHUB_OndigCert Inc. CN=DigiCert SHA2 Secure Server.CA
	5278989459	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5278984439	2021-09-24	2021-09-23	2021-12-22	support.unity.com	support.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5270704744	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5270702329	2021-09-23	2021-09-23	2021-12-22	globalgamejam2021.unity.com	globalgamejam2021.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258194803	2021-09-21	2021-09-21	2021-12-20	www.uniforma-event.unity.com	uniforma-event.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258195521	2021-09-21	2021-09-21	2021-12-20	www.uniforma-event.unity.com	uniforma-event.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258192831	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5258192811	2021-09-21	2021-09-21	2021-12-20	aisummit2020.unity.com	aisummit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5252195757	2021-09-30	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5362417070	2021-09-29	2021-09-29	2021-12-19	email.everyonesocial.unity.com	email.everyonesocial.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5211395357	2021-09-19	2021-09-13	2021-12-12	sanc441.cdnfwrk.com	sanc441.cdnfwrk.com	CHUB_OrLet's Encrypt_CNR#3
	5207204274	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5207205636	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5207204277	2021-09-12	2021-09-12	2021-12-11	compass.unity.com	compass.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5178349377	2021-09-26	2021-09-26	2021-12-05	uniteuno.unity.com	uniteuno.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5173780057	2021-09-26	2021-09-26	2021-12-05	unite2020.unity.com	unite2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5173723716	2021-09-26	2021-09-26	2021-12-05	unite2020.unity.com	unite2020.unity.com	CHUB_OrGoogle 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	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160872410	2021-09-26	2021-09-26	2021-12-05	docs-uniteuno.unity.com	docs-uniteuno.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5160872359	2021-09-04	2021-07-08	2021-10-06	docs-stg.unity.com	docs-stg.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160872359	2021-09-04	2021-07-08	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5160879932	2021-09-04	2021-07-19	2021-11-17	staging.services.api.unity.com	staging.services.api.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5152644900	2021-09-02	2021-09-02	2021-12-04	staging.services.api.unity.com	staging.services.api.unity.com	CHUB_OrGoogle Trust Services LLC CN=GTS CA 104
	5136198204	2021-08-31	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5136192419	2021-08-31	2021-08-31	2021-11-29	ufssummmit2020.unity.com	ufssummmit2020.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128908186	2021-08-29	2021-08-29	2021-11-27	blog-api.unity.com	blog-api.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128627460	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5128627464	2021-08-29	2021-08-29	2021-11-27	blog.unity.com	blog.unity.com	CHUB_OrLet's Encrypt_CNR#3
	5120315513	2021-08-28	2021-08-28	2021-11-26	cdn.mars.unity.com	cdn.mars.unity.com	CHUB_OrGoogle 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.

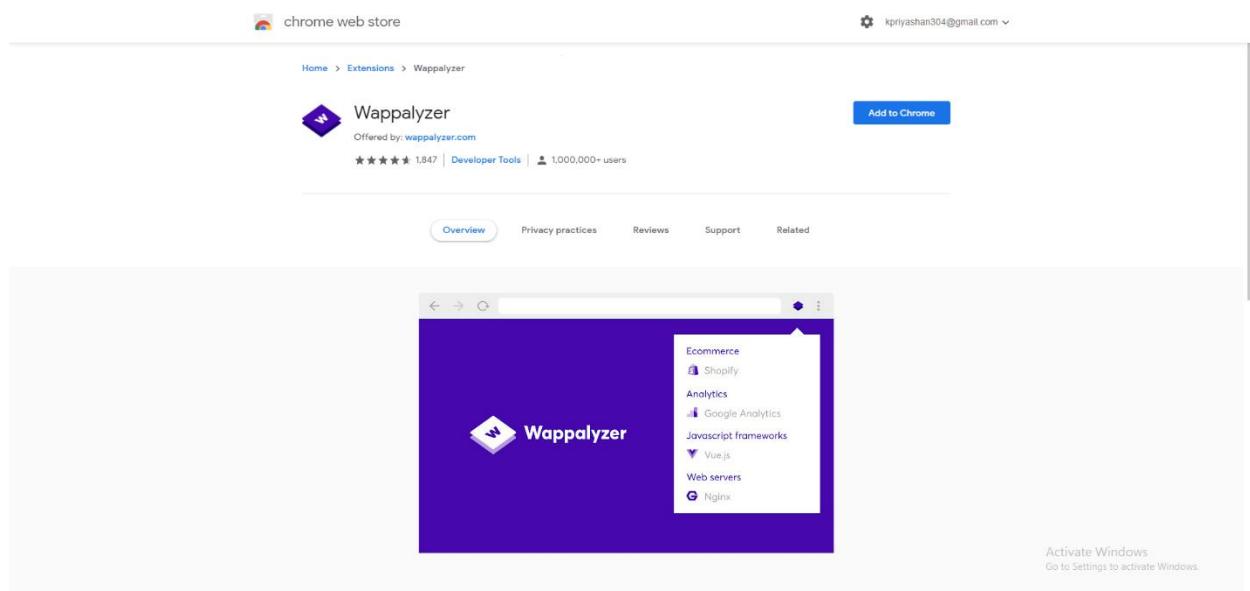


Figure 11 how to add extension to browser

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

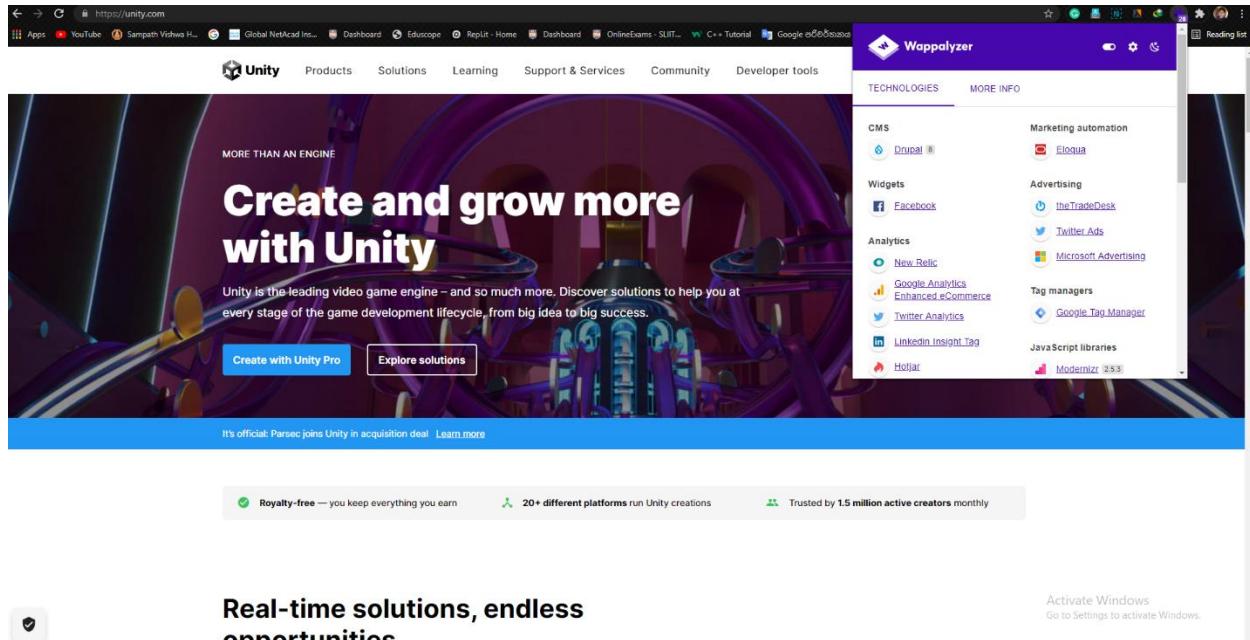


Figure 12 output of wappalyzer we can get information about technologies which site built

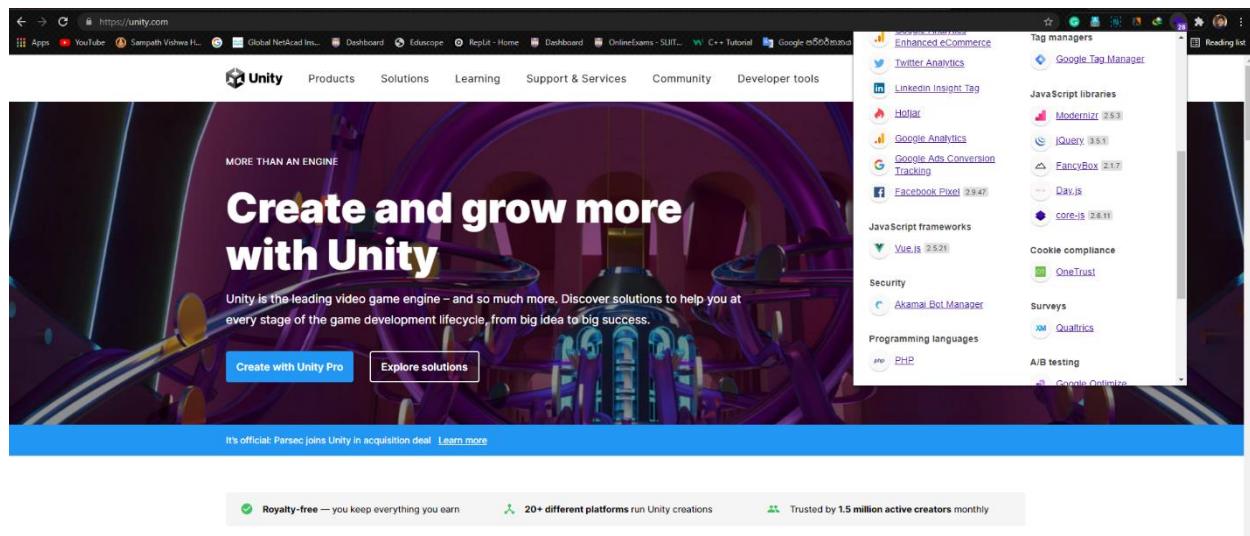


Figure 13 output of wappalyzer we can get information about technologies which site built

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 and enter the domain after that we can get all the details about security headers of the domain which we going to find.

The screenshot shows the homepage of Securityheaders.com. At the top, there's a search bar with the placeholder "enter address here" and a "Scan" button. Below the search bar are two checkboxes: "Hide results" and "Follow redirects". The main content area is divided into four sections:

- Grand Totals:** A table showing the count of sites for each grade: A+ (1,635,338), A (17,615,890), B (3,931,093), C (4,399,689), D (17,641,171), E (7,407,403), F (87,489,709), and R (24,438,012). The total is 164,558,305.
- Recent Scans:** A list of recent scans with their grades: compensation-servi... (A), www.comptine.biz (F), neel.incrediblepla... (F), compensation-servi... (A), compensation-servi... (F), compensation-servi... (A), compensation-servi... (D), compensation-servi... (C), compensation-servi... (F), compensation-servi... (A).
- Hall of Fame:** A list of sites with high scores: compensation-servi... (A), compensation-servi... (A).
- Hall of Shame:** A list of sites with low scores: aext.org (F), noel.incrediblepla... (F), nevalshopalk.com (F), townebankonline.bi... (F), 844.inland-develop... (F), epr.industrypharma... (F), www.a913.vip (F), www.31.purcellolut... (F), otj.fearnoman.com (F).

At the bottom of the page, there's a footer with the text "A scotthelme.co.uk project - CC-BY-SA 4.0", "Sponsored by Probely", social media icons for Twitter, Facebook, and LinkedIn, and a link to "Activate Windows".

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 to 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".

Security Report Summary

Grade: D

Site: <https://unity.com/>

IP Address: 104.93.134.159

Report Time: 07 Oct 2021 11:33:33 UTC

Headers:

- ✓ X-Content-Type-Options
- ✓ X-Frame-Options
- ✗ Strict-Transport-Security
- ✗ Content-Security-Policy
- ✗ Referrer-Policy
- ✗ Permissions-Policy

Supported By

Probely Your site could be at risk, let's perform a deeper security analysis of your site and APIs: [Start Now](#)

Raw Headers

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

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.

Missing Headers

Content-Security-Policy	Content-Security-Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

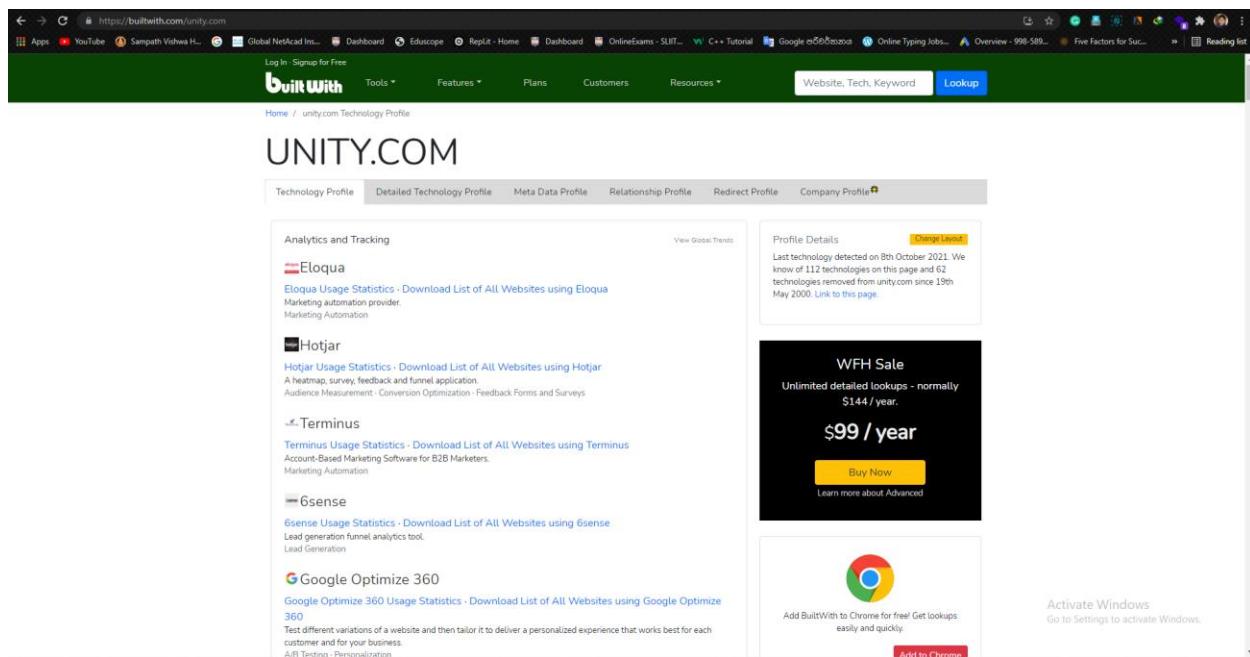
Warnings

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

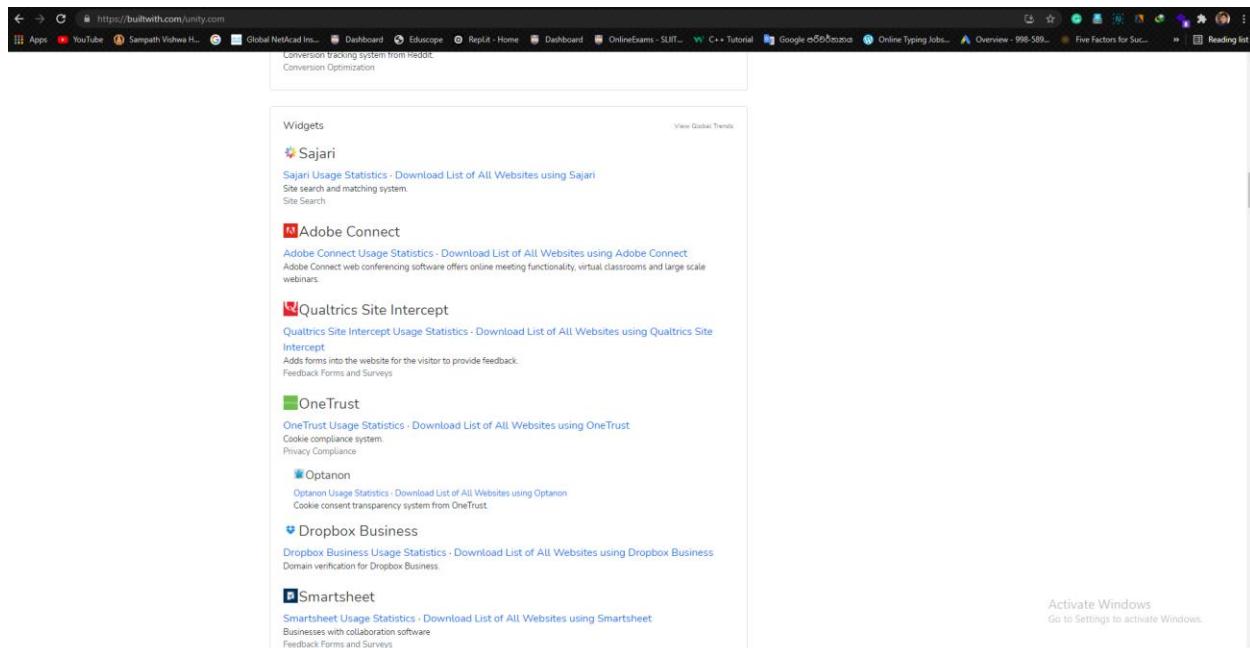
Built With.com

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. The main navigation bar includes 'Log In - Signup for Free', 'Tools', 'Features', 'Plans', 'Customers', 'Resources', and a search bar with 'Website, Tech, Keyword' and 'Lookup' buttons. Below the navigation is a breadcrumb trail: Home / unity.com Technology Profile. The main content area is titled 'UNITY.COM' and displays a 'Technology Profile' tab. On the left, there's a sidebar for 'Analytics and Tracking' which lists several tools: Eloqua, Hotjar, Terminus, 6sense, and Google Optimize 360. Each entry includes a small icon, a tool name, a brief description, and a 'View Global Trends' link. To the right of the sidebar is a 'Profile Details' box showing 'Last technology detected on 8th October 2021. We know of 112 technologies on this page and 62 technologies removed from unity.com since 19th May 2000. Link to this page.' Below this is a promotional box for 'WFH Sale' with a price of '\$99 / year' and a 'Buy Now' button. At the bottom right, there's a 'Activate Windows' section with a 'Go to Settings to activate Windows' link and an 'Add to Chrome' button next to a Google Chrome logo.

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



This screenshot shows the same BuiltWith.com interface for the domain unity.com, focusing on a different set of technologies. The sidebar for 'Conversion Backing System from Reddit' lists Adobe Connect, Qualtrics Site Intercept, OneTrust, Optanon, and Dropbox Business. Each entry follows the same structure: tool name, brief description, and a 'View Global Trends' link. The right side of the page features the same 'WFH Sale' promotion and 'Activate Windows' section as in Figure 17.

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'. At the top, there are navigation links for 'SHODAN', 'Explore', 'Pricing', and a search bar containing 'unity.com'. Below the search bar is a search button with a magnifying glass icon. To the right of the search bar is a 'Login' button.

TOTAL RESULTS: 40

TOP COUNTRIES:

- United States: 31
- Russian Federation: 3
- Belgium: 2
- France: 2
- Indonesia: 1

TOP PORTS:

Port	Count
80	18
443	15
3389	3
2525	2
5222	1

TOP ORGANIZATIONS:

Organization	Count
Google LLC	31
JSC IOT	2
Ritter Communications	2

SSL Certificate Details for 35.241.48.119:

- Issued By: Google LLC
- Common Name: *.cloud.unity3d.com
- Organization: Unity Technologies SF
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

SSL Certificate Details for 35.186.231.34:

- Issued By: Google LLC
- Common Name: *.cloud.unity3d.com
- Organization: Unity Technologies SF
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

SSL Certificate Details for 35.186.231.34 (Details):

- HTTP/1.1 301 Moved Permanently
- Access-Control-Allow-Credentials: true
- Content-Security-Policy: frame-ancestors 'self' unity3d.com *.unity3d.com unity.com *.unity.com
- X-Frame-Options: DENY
- Location: https://api.unity.com/v1/auth/h...

Activate Windows
Go to Settings to activate Windows
2021-10-12T21:27:54.472840

Figure 20 shodan shows interconnected devices to domain

The screenshot shows the Shodan search interface for the domain 'unity.com'. At the top, there are navigation links for 'SHODAN', 'Explore', 'Pricing', and a search bar containing 'unity.com'. Below the search bar is a search button with a magnifying glass icon. To the right of the search bar is a 'Login' button.

TOTAL RESULTS: 40

TOP COUNTRIES:

- United States: 31
- Russian Federation: 3
- Belgium: 2
- France: 2
- Indonesia: 1

TOP PORTS:

Port	Count
80	18
443	15
3389	3
2525	2
5222	1

TOP ORGANIZATIONS:

Organization	Count
Google LLC	31
JSC IOT	2
Ritter Communications	2

SSL Certificate Details for 35.244.202.54:

- Issued By: Google LLC
- Common Name: *.cloud.unity3d.com
- Organization: Unity Technologies SF
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

SSL Certificate Details for 35.227.211.131:

- Issued By: Google LLC
- Common Name: *.cloud.unity3d.com
- Organization: Unity Technologies SF
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

SSL Certificate Details for 130.211.11.25:

- Issued By: Google LLC
- Common Name: *.cloud.unity3d.com
- Organization: Unity Technologies SF
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

Activate Windows
Go to Settings to activate Windows
2021-10-12T10:20:27.714347

Activate Windows
Go to Settings to activate Windows
2021-10-12T01:29:30.727840

Activate Windows
Go to Settings to activate Windows
2021-10-12T01:29:30.727840

Figure 19 shodan shows interconnected devices to domain

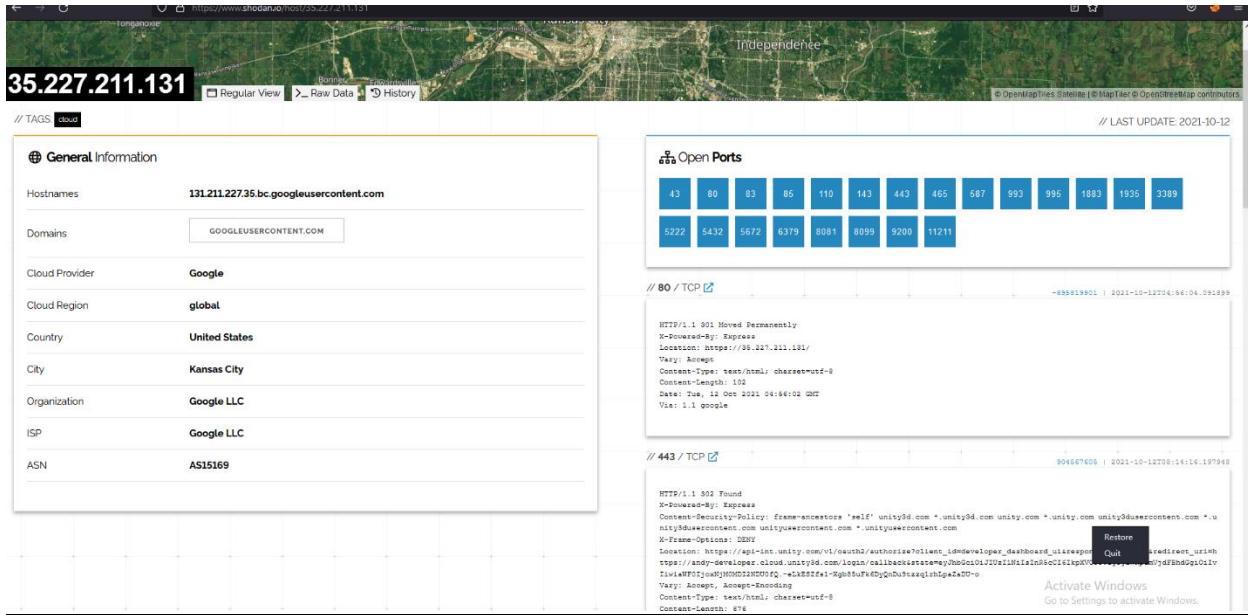


Figure 21 information about interconnected device and we can get information about open ports etc.

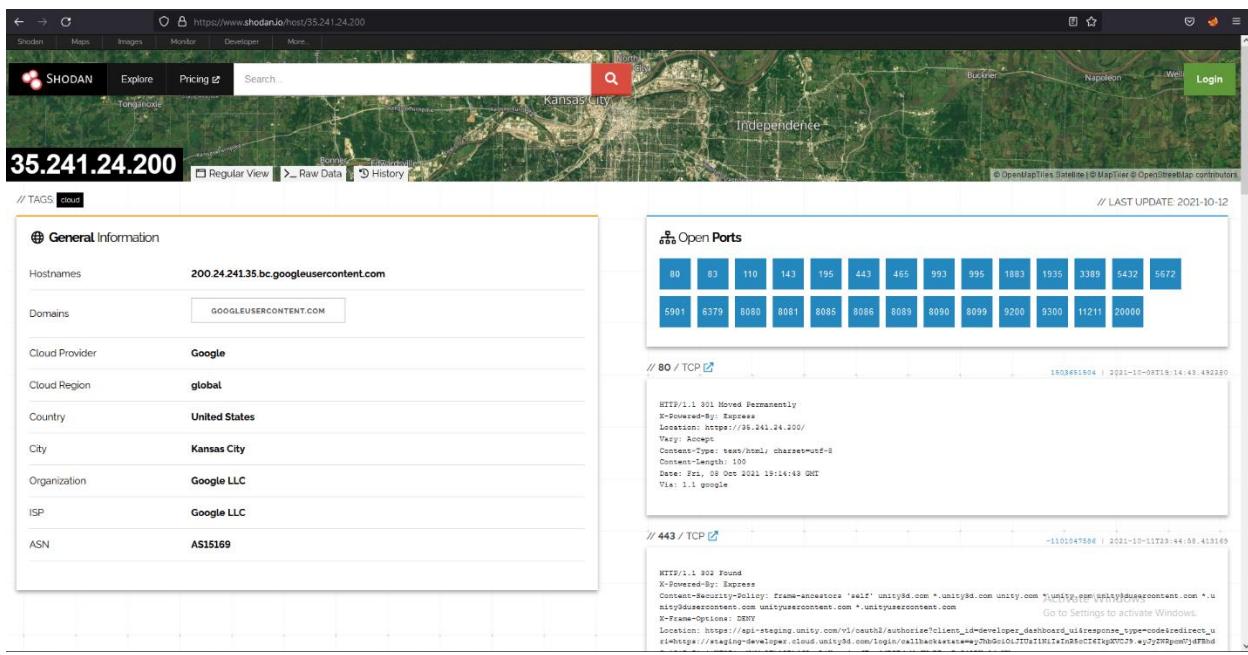


Figure 22 information about interconnected device and we can get information about open ports etc

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

```
File Edit View Bookmarks Settings Help
nmap -v -sn 192.168.0.6/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE https://nmap.org/book/man.html FOR MORE OPTIONS AND EXAMPLES
[+] kasan@kasan:~$ nmap -sV -A -p- -T4 -oN unity.txt unity.com
You requested a type which requires root privileges.
QUITTING!
[+] kasan@kasan:~$ nmap -sV -A -p- -T4 -oN unity.txt unity.com
[!] sudo password for kasan:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 22:11 +0530
Nmap scan report for unity.com (23.15.149.114)
Nmap done: 1 IP address (1 host up) scanned in 434.70 seconds
DNS record for 23.15.149.114: a23-15-149-114.deploy.static.akamaitechnologies.com
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
PORT      STATE SERVICE VERSION
|_http     open  http  AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
|_http/1.1  open  http  AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
|_http/1.1  closed http  AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
|_ssl-cert: Subject: commonName=unity.com/organizationName=Unity Technologies ApS/countryName=DK
|_Subject Alternative Name: DNS1:unity.com,DNS:unity.com
|_Not valid before: 2021-08-23T08:08:08Z
|_Not valid after:  2022-08-23T23:59:59Z
|_ssl-dstest: TLS randomness does not represent time
|_tls-alpn:
|   http/1.1
|   http/2.0
|_tcp       open  portmap: portmap
|_tcp       open  http-0.9: http-0.9
|_tcp       open  http/1.1
|_tcp       open  http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: embedded-device
Running: Actiontec embedded, Linux
OS CPE: cpe:/hi:actiontec:m1424wr-gen3l cpe:/o:linux:linux_kernel
OS details: Actiontec M1424WR-GEN3L WAP
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  9.86 ms   192.168.116.2
2  8.69 ms   a23-15-149-114.deploy.static.akamaitechnologies.com (23.15.149.114)

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 434.70 seconds
```

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

Id.unity.com

```
[kasum@kasum-vmwarevirtualplatform ~]$ ./nmap nmap -sS -A -T4 -O id.unity.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 22:23 +0530
Nmap scan report for id.unity.com (35.194.129.29)
Host is up (0.0003s latency).
rDNS record for 35.194.129.29: 29.129.194.35.bc.googleusercontent.com
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http-proxy  HAProxy http proxy 3.1.1 or later
|_http-title: Did not follow redirect to https://id.unity.com/
443/tcp   open  tcprwapped
|_http-title: Site may be available over https://id.unity.com/
|_Subject Alternative Name: DNS=id.unity.com, DNS=id.unity.com
|_Not valid before: 2020-05-19T08:00:00
|_Not valid after: 2022-07-29T12:00:00
|_Last-Update: TLS randomness does not represent time
Warning: OS scan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Brother MFC-7820N printer (94%), Digi Connect ME serial-to-Ethernet bridge (94%), Netgear SC101 Storage Central NAS device (91%), Astra 480i IP Phone or Sun Remote System Control (RSC) (91%), Astra 6731L VoIP p-home or Apple AirPort Express WAP (91%), GoPro HERO3 camera (91%), Konica Minolta bizhub 256 printer (91%), OUYA game console (91%), Crestron MPC-H5 AV controller or Wago Kontakttechnik 750-852 PLC (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Device: load balancer

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  10.79 ms  192.168.1.16.2
2  9.79 ms  29.129.194.35.bc.googleusercontent.com (35.194.129.29)

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 412.29 seconds
```

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

```
[kasum@kasum-vmwarevirtualplatform ~]$ ./nmap nmap -sS -A -T4 -O 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 (0.013s latency).
rDNS record for 35.198.63.66: 66.63.198.35.bc.googleusercontent.com
Not shown: 65529 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http-proxy  HAProxy http proxy 3.1.1 or later
|_http-title: Did not follow redirect to https://analytics.cloud.unity3d.com/
443/tcp   open  tcprwapped
|_http-title: Site may be available over https://analytics.cloud.unity3d.com/
|_Subject Alternative Name: DNS=analytics.cloud.unity3d.com, DNS=analytics.cloud.unity3d.com
|_Not valid before: 2020-05-19T08:00:00
|_Not valid after: 2022-07-29T12:00:00
|_Last-Update: TLS randomness does not represent time
Warning: OS scan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Brother MFC-7820N printer (94%), Digi Connect ME serial-to-Ethernet bridge (94%), Netgear SC101 Storage Central NAS device (91%), Astra 480i IP Phone or Sun Remote System Control (RSC) (91%), Astra 6731L VoIP p-home or Apple AirPort Express WAP (91%), GoPro HERO3 camera (91%), Konica Minolta bizhub 256 printer (91%), OUYA game console (91%), Crestron MPC-H5 AV controller or Wago Kontakttechnik 750-852 PLC (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  13.60 ms  192.168.1.16.2
2  12.69 ms  66.63.198.35.bc.googleusercontent.com (35.198.63.66)

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 509.72 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

```
[kasum@kasum-vmwarevirtualplatform ~]$ ./nmap nmap -sS -A -T4 -O pay.unity.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 23:05 +0530
Nmap scan report for pay.unity.com (35.236.177.74)
Host is up (0.013s latency).
rDNS record for 35.236.177.74: 74.177.236.35.bc.googleusercontent.com
All 65535 ports are closed (filtered)
Warning: OS scan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GB101 WAP, CD-WRT v24-sp2 (Linux 2.6.37), 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

TRACEROUTE (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.

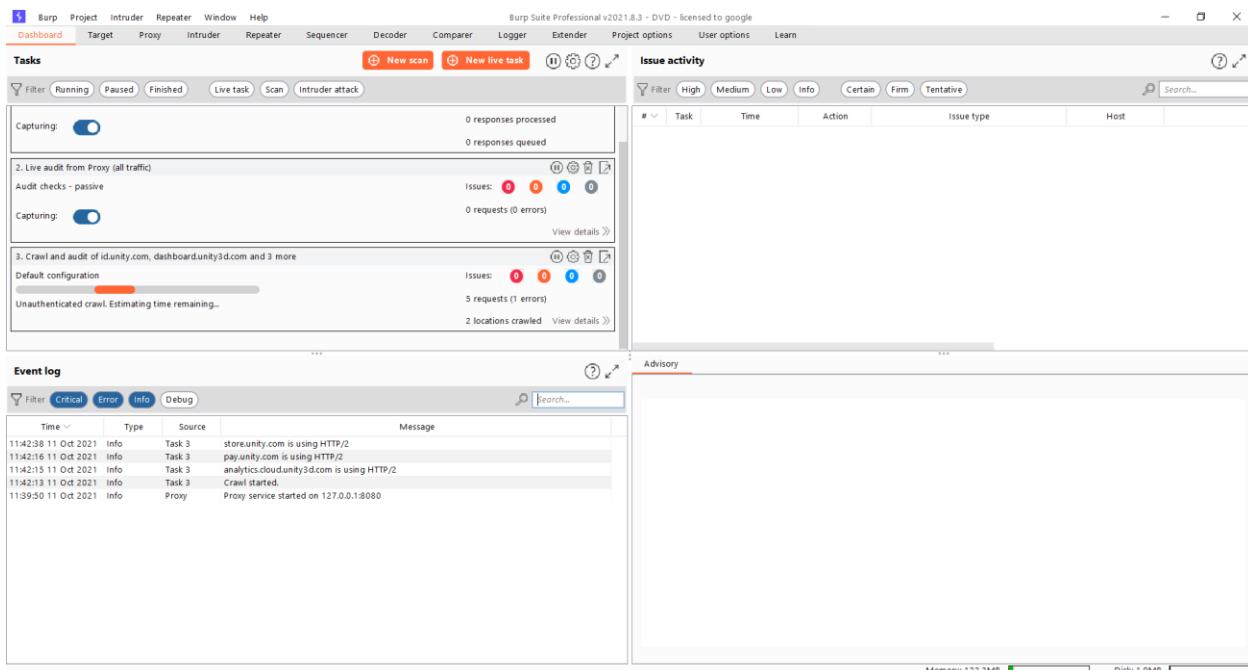


Figure 27 strating burp with crawl and audit

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.

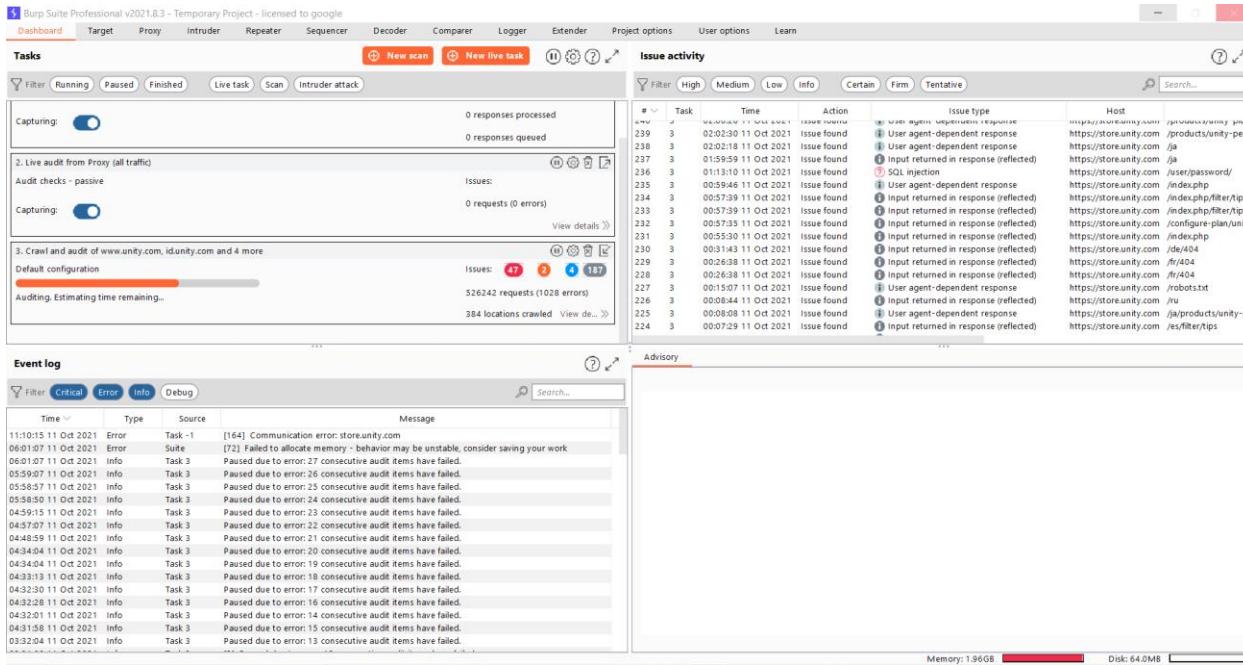


Figure 28 output after 6 hours in burp I could find 47 issues by this scan most of them are common vulnerabilities

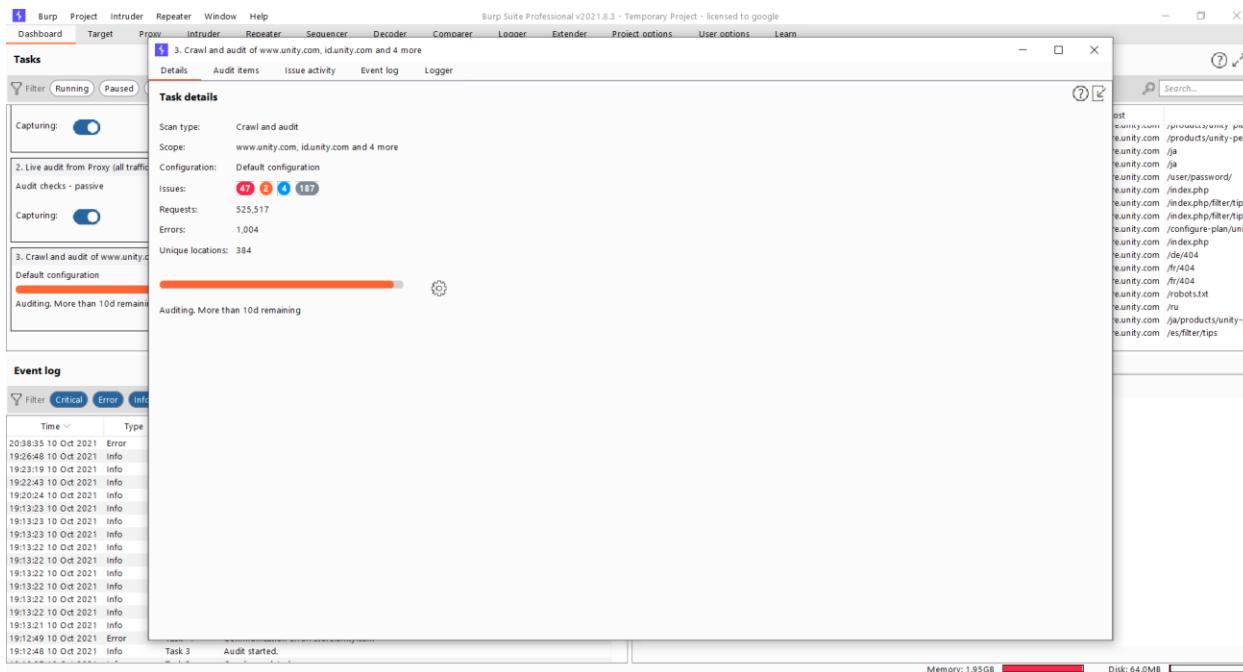


Figure 29 after 525,517 requests results I have got by burp suite scanning

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

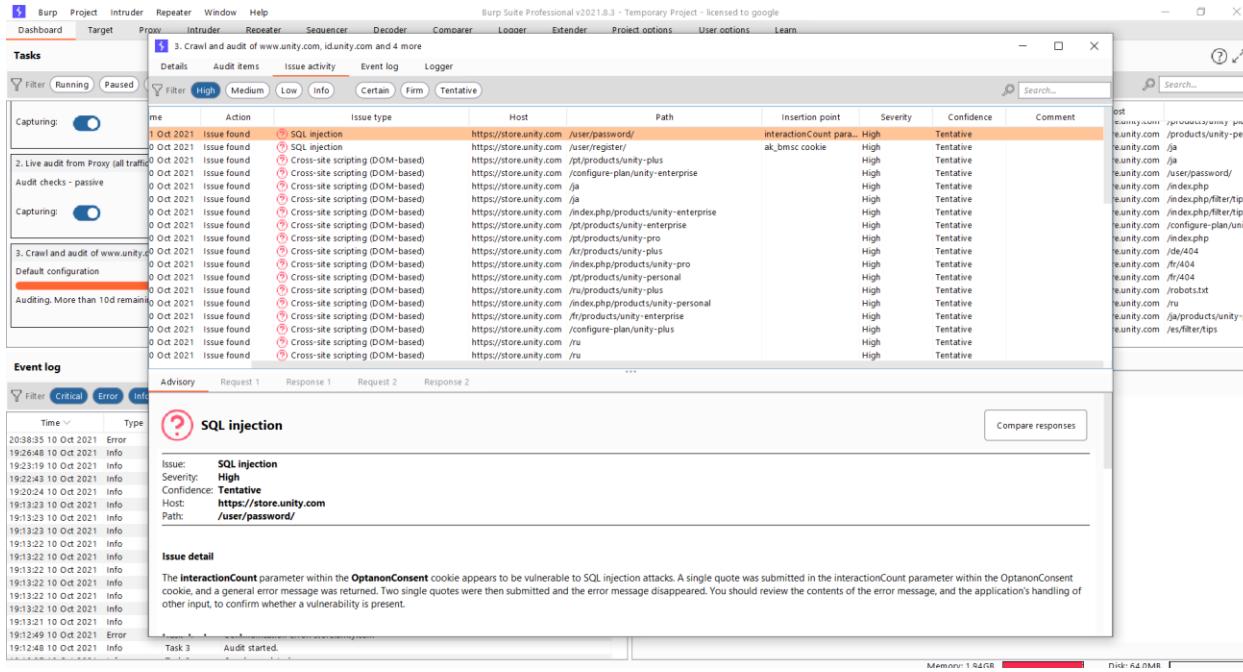


Figure 30 issues that I have found by burp suite scanning

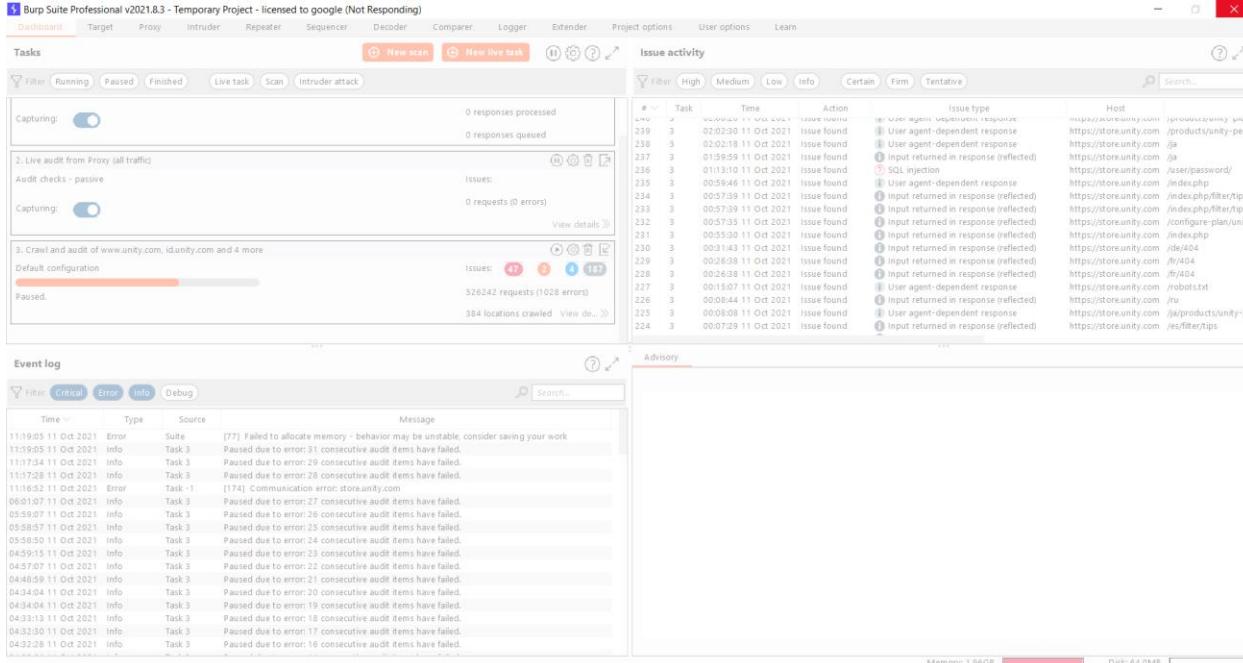
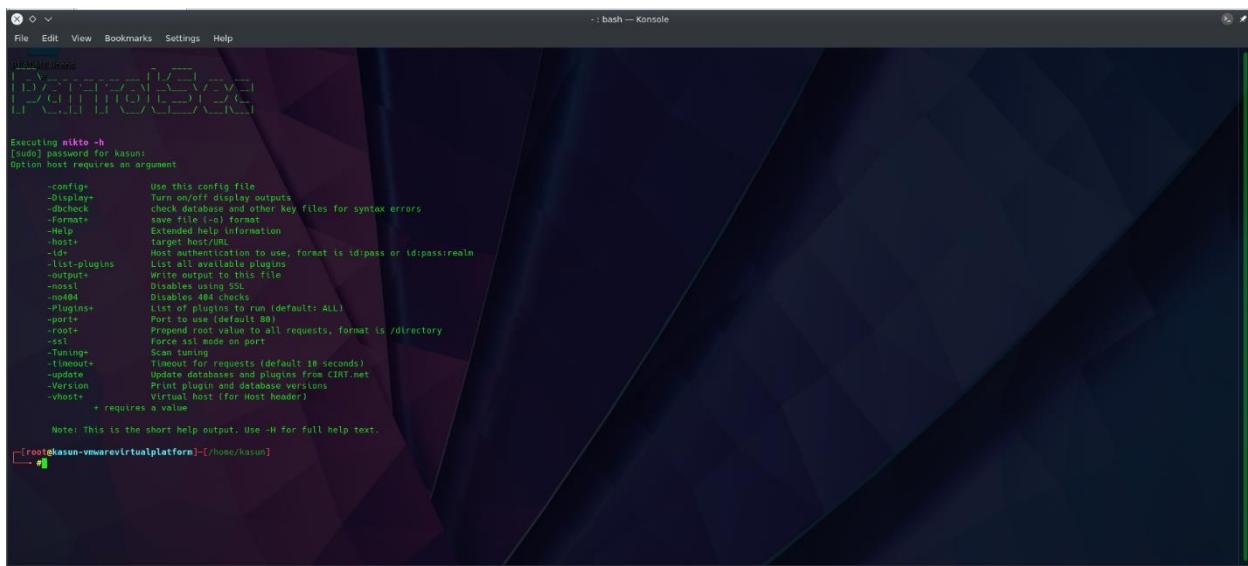


Figure 31 after 10 hours there are out of memory allocation therefore burp suite scanning was got error it was not responded.

Nikto Scanner

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

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



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

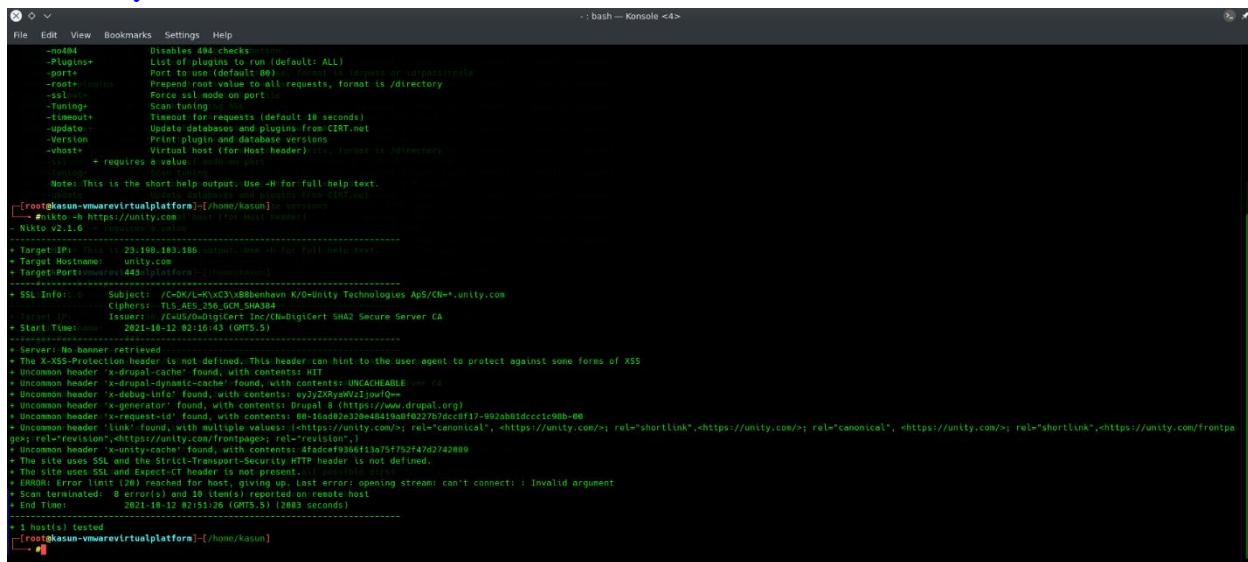
  -config=          Use this config file
  -display=         Turn on/off display outputs
  -dbscheck         Check database and other key files for syntax errors
  -format=          File type (-o) format
  -Help             Extended help information
  -Host             Target host/URL
  -id=              Host authentication to use, format is id:pass or id:pass:realm
  -list-plugins     List all available plugins
  -output=          Write output to this file
  -ssl              SSL enabled
  -no404            Disables 404 checks
  -plugins=         List of plugins to run (default: ALL)
  -port=            Port to use (default: 80)
  -root=            Prepend 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]
#
```

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

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=            Prepend 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]# nikto -h https://unity.com/host (for Host header)
- Nikto v2.1.6 - http://www.nikto.org
-----[SSL Info]-----[+]- Subject: /C=DK/L=K/x3/88b0hem W/Unity Technologies Ap/CN=*.unity.com
[+]- Ciphers: TLS_AES_256_GCM_SHA384
[+]- Cert Issuer: /C=US/O=DigiCert Inc/OU=DigiCert SHA2 Secure Server CA
[+]- Start Time: 2021-10-12 02:16:43 (GMT+5)
-----[+]- 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: UNCACHEABLE;ver=CA
[+]- Uncommon header 'x-drupal-dynamic-cache' found, with contents: UNCACHEABLE;ver=CA
[+]- Uncommon header 'x-dynamic-cache' found, with contents: UNCACHEABLE;ver=CA
[+]- Uncommon header 'x-generator' found, with contents: Drupal 8 (https://www.drupal.org)
[+]- Uncommon header 'x-request-id' found, with contents: 00-1eadde2320e4d419ad0f0227b7dcdf17-992ab81dcc1c98b-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="revision",<https://unity.com/frontpage>; rel="shortlink"
[+]- 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 limit (20) reached for host, giving up. Last error: opening streams can't connect: : Invalid argument
  Scan terminated: 0 hosts tested in 00:00:00.000000 (real), 00:00:00.000000 (user), 00:00:00.000000 (os)
  Total time: 00:00:00.000000 (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
-Host          Target host/URL
-Id           Host authentication to use, format is id:pass or idipass:realm
-List-Plugins List all available plugins
-Output       Write output to this file
-NoSsl        Disables using SSL
-No404       Disables 404 checks
-Plugins+     List of plugins to run (defaults: ALL)
-Port         Port to use (default: 80); versions
-Root        Prepend root value to all requests, format is /directory
-Ssl          Scan using SSL mode on port
-Timing       Scan timing
-Timeout+    Timeout for requests (default: 10 seconds)
-Update      Update databases and plugins from CIRT.net
-Version     Print plugin and database versions
-Vhost       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]
[root@kasun-vmwarevirtualplatform]# nikto -h https://id.unity.com
- Nikto v2.1.6
+ Target IP: 34.120.209.121
+ Target Hostname: id.unity.com
+ Target Port: 443
-----[SSL Info]-[Subject: /C=DK/L=Copenhagen/C=Unity Technologies ApS/CN=id.unity.com] protect against some forms of RCE
+ Ciphers: ECDHE-RSA-AES256-GCM-SHA384
+ ISSUER: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2021-10-12 02:17:31 (GMT+5.5)
+ Server: No banner retrieved
+ Retrieved via header: alt-svc found, with contents: clear-hsts=0; ma=2592000; v=B3
+ Uncommon header 'x-request-id' found, with contents: f54b02fd-085e-443f-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/redirectories found, with contents: /index.html
+ Error limit (EDR) reached, giving up. Last error: opening stream: can't connect : Invalid argument
+ Scan terminated: 2 errors(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
-Host          Target host/URL
-Id           Host authentication to use, format is id:pass or idipass:realm
-List-Plugins List all available plugins
-Output       Write output to this file
-NoSsl        Disables using SSL
-No404       Disables 404 checks
-Plugins+     List of plugins to run (defaults: ALL)
-Port         Port to use (default: 80); versions
-Root        Prepend root value to all requests, format is /directory
-Ssl          Force ssl mode on port
-Timing       Scan tuning
-Timeout+    Timeout for requests (default: 10 seconds)
-Update      Update databases and plugins from CIRT.net
-Version     Print plugin and database versions
-Vhost       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]
[root@kasun-vmwarevirtualplatform]# nikto -h https://dashboard.unity3d.com
- Nikto v2.1.6
+ Target IP: 34.182.142.05
+ Target Hostname: dashboard.unity3d.com
+ Target Port: 443
-----[SSL Info]-[Subject: /C=DK/L=KvxC5xb8vnhaavn/0-Unity Technologies ApS/CN=dashboard.unity3d.com] protect against some forms of RCE
+ Ciphers: TLS_AES_256_GCM_SHA384
+ 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=0; ma=2592000; v=B3
+ 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~ahW8cDovL2Rh2hb2FyZCS1bm0etNKLdnvb5Bw
+ 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.

```
-:bash — Konsole <5>
File Edit View Bookmarks Settings Help
https://store.unity.com
[nikto -h https://store.unity.com]
[+] Target IP: 23.198.193.106
[+] Target Hostname: store.unity.com
[+] Target Port: 443
[+] Threads: 100 (try to keep connections open through reusing them)
[+] Timeout: 10 (seconds)
[+] Threads: 100 (try to keep connections open through reusing them)
[+] Timeout: 10 (seconds)

+ Target IP: 23.198.193.106
+ Target Hostname: store.unity.com
+ Target Port: 443
+ 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)
+       Version: OpenSSL/1.1.1f-fips
+       OS: Linux
+       Server: Apache/2.4.41 (Ubuntu)
+       Server banner: 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-dpr':dynamic-cache, found, with contents: M15
+       Uncommon header 'x-dpr':dynamic-cache, found, with contents: M15
+       Uncommon header 'x-debug-info' found, with contents: eyJ2XbawvZjzjow==
+       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_STICKTVMlogjyomqIE3NnD500.MdqQvr8UVT5oB.css>; rel=preload
+       Uncommon header 'x-request-id' found, with contents: 00-16ad92fb1fd2ecfb139e993c3e0e8-2b97fc5892bdec5a-00
+       Uncommon header 'x-ua-compatible' found, with contents: IE=11,chrome=1
+       The site uses SSL and Expect-CT header is not defined.
+       The site uses SSL and Strict-Transport-Security header is not defined.
+       The site uses SSL and X-Content-Type-Options header is not present.
+       No 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 '/robots.txt' in robots.txt returned a non-forbidden or redirect HTTP code ()
+       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 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 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 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 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 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 limit (20) reached for host, giving up. Last error: opening stream can't connect: Invalid argument
+       Entry '/filter/https://bin/robots.txt' returned a non-forbidden or redirect HTTP code ()
+       Error limit (20) reached for host, giving up. Last error: opening stream can't connect: Invalid argument
+       Entry '/user/password' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+       Error limit (20) reached for host, giving up. Last error:
+       Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+       Error limit (20) reached for host, giving up. Last error:
+       Entry '/user/logout/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+       Error limit (20) reached for host, giving up. Last error:
+       Entry '/index.php/user/register' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+       Error limit (20) reached for host, giving up. Last error:
+       Entry '/index.php/user/login' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+       Error limit (20) reached for host, giving up. Last error:
+       Entry '/index.php/user/logout' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+       "robots.txt" contains 40 entries which should be manually viewed. opening stream can't connect: Invalid argument
+       Scan terminated: 14 errors() and 38 items() reported on remote host
+       End Time: 2021-10-12 02:57:38 (GMT+5) (2341 seconds)

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

```
-:bash — Konsole <5>
File Edit View Bookmarks Settings Help
https://store.unity.com
[nikto -h https://store.unity.com]
[+] Target IP: 23.198.193.106
[+] Target Hostname: store.unity.com
[+] Target Port: 443
[+] Threads: 100 (try to keep connections open through reusing them)
[+] Timeout: 10 (seconds)
[+] Threads: 100 (try to keep connections open through reusing them)
[+] Timeout: 10 (seconds)

+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ 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 (200)
+ 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 (200)
+ 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 (200)
+ 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 (200)
+ 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 (200)
+ 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 (200)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream can't connect: Invalid argument
+ Entry '/filter/https://bin/robots.txt' 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/password' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ 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:
+ 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:
+ 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:
+ Entry '/index.php/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:
+ "robots.txt" contains 40 entries which should be manually viewed. opening stream can't connect: Invalid argument
+ Scan terminated: 14 errors() and 38 items() 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

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

Wafw00f

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

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

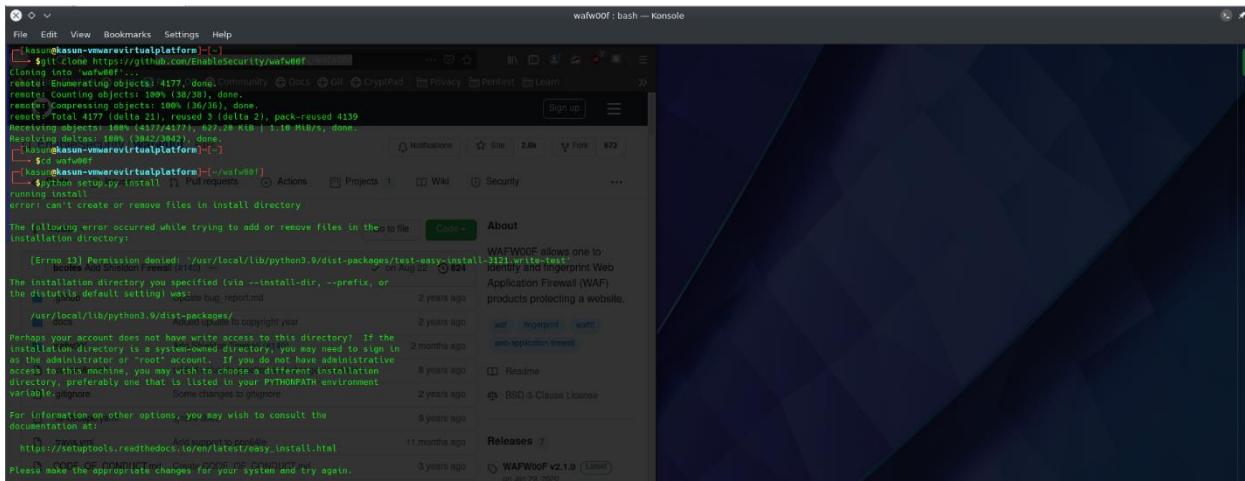


Figure 38 installation of wafw00f tool for scanning firewalls behind domains.

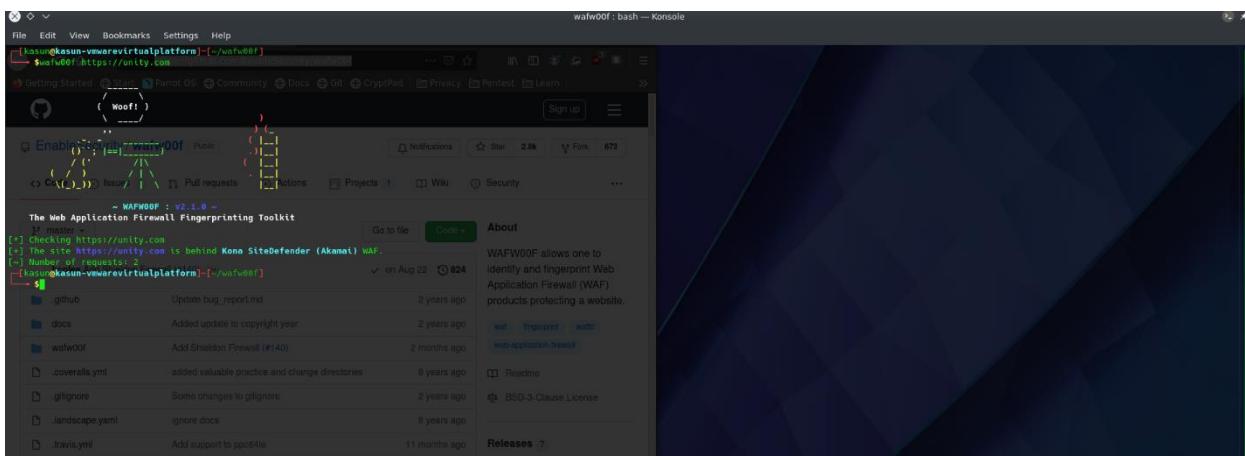
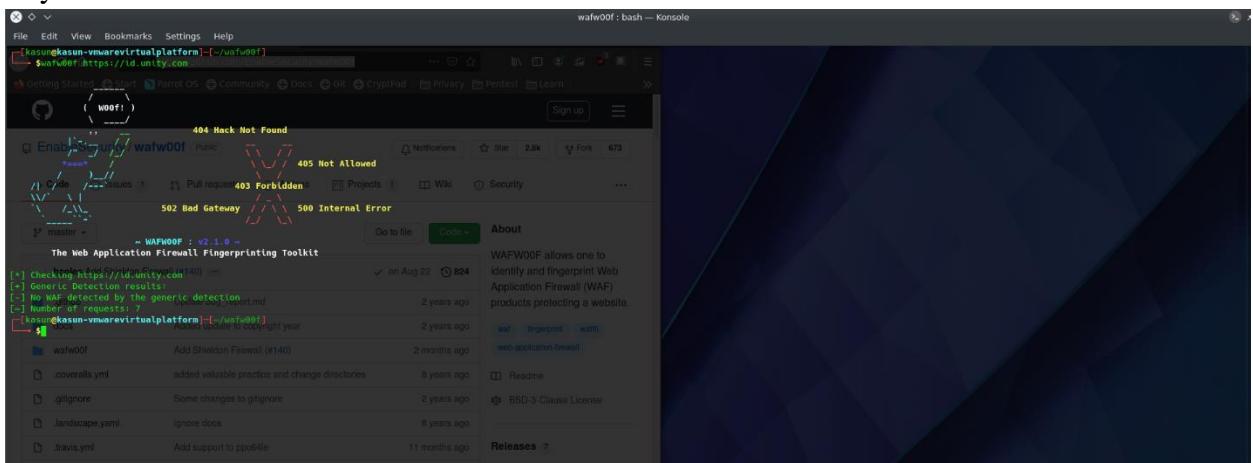


Figure 39 I scanned unity.com by wafw00f tool and I found a firewall behind the domain

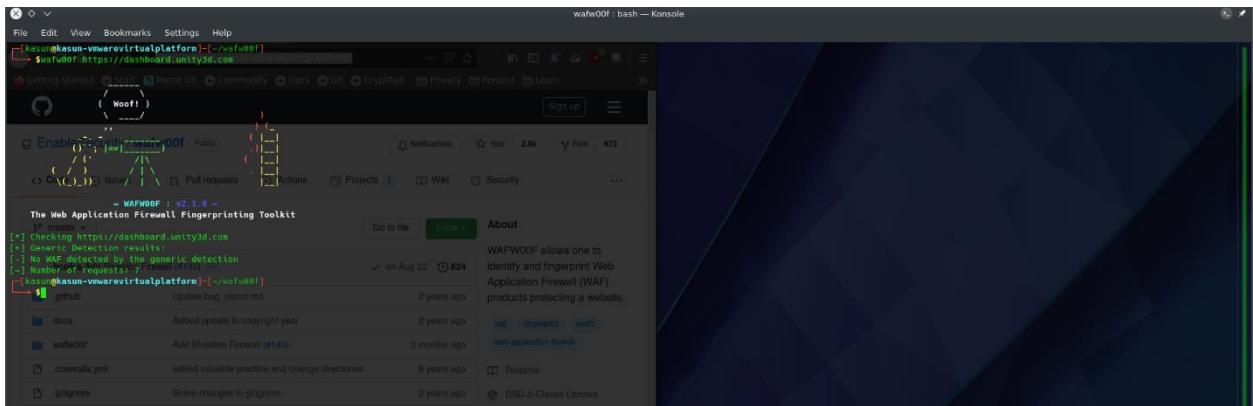
id.unity.com



```
wafw00f : bash — Konsole
kasus@kasun-vmwarevirtualplatform:[~]/wafw00f
$ wafw00f https://id.unity.com
[*] Checking https://id.unity.com [404]
[-] Generic Detection results:
[+] No WAF detected by the generic detection
[+] Number of requests: 7 / Total(110) ...
kasus@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
kasus@kasun-vmwarevirtualplatform:[~]/wafw00f
$ wafw00f https://dashboard.unity3d.com
[*] Checking https://dashboard.unity3d.com
[-] Generic Detection results:
[+] No WAF detected by the generic detection
[+] Number of requests: 7 / Total(110) ...
kasus@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

The screenshot shows the wafw00f tool's user interface. At the top, there's a terminal window with the command `wafw00f https://store.unity.com`. Below the terminal is a GitHub repository page for "wafw00f". The repository has 2.8k stars and 673 forks. The README file indicates that WAFW00F is a Web Application Firewall Fingerprinting Toolkit. The terminal output shows that the site `https://store.unity.com` is behind Kona SiteDefender (Akamai) WAF, with 2 requests made on Aug 22, 2024.

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

pay.unity.com

The screenshot shows the wafw00f tool's user interface. At the top, there's a terminal window with the command `wafw00f https://pay.unity.com`. Below the terminal is a GitHub repository page for "wafw00f". The repository has 2.8k stars and 673 forks. The README file indicates that WAFW00F is a Web Application Firewall Fingerprinting Toolkit. The terminal output shows generic detection results, stating that no WAF was detected by the generic detection method, with 7 requests made on Aug 22, 2024.

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

The screenshot shows the wafw00f tool's user interface. At the top, there's a terminal window with the command `wafw00f https://analytics.cloud.unity3d.com`. Below the terminal is a GitHub repository page for "wafw00f". The repository has 2.8k stars and 673 forks. The README file indicates that WAFW00F is a Web Application Firewall Fingerprinting Toolkit. The terminal output shows generic detection results, stating that no WAF was detected by the generic detection method, with 7 requests made on Aug 22, 2024.

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.

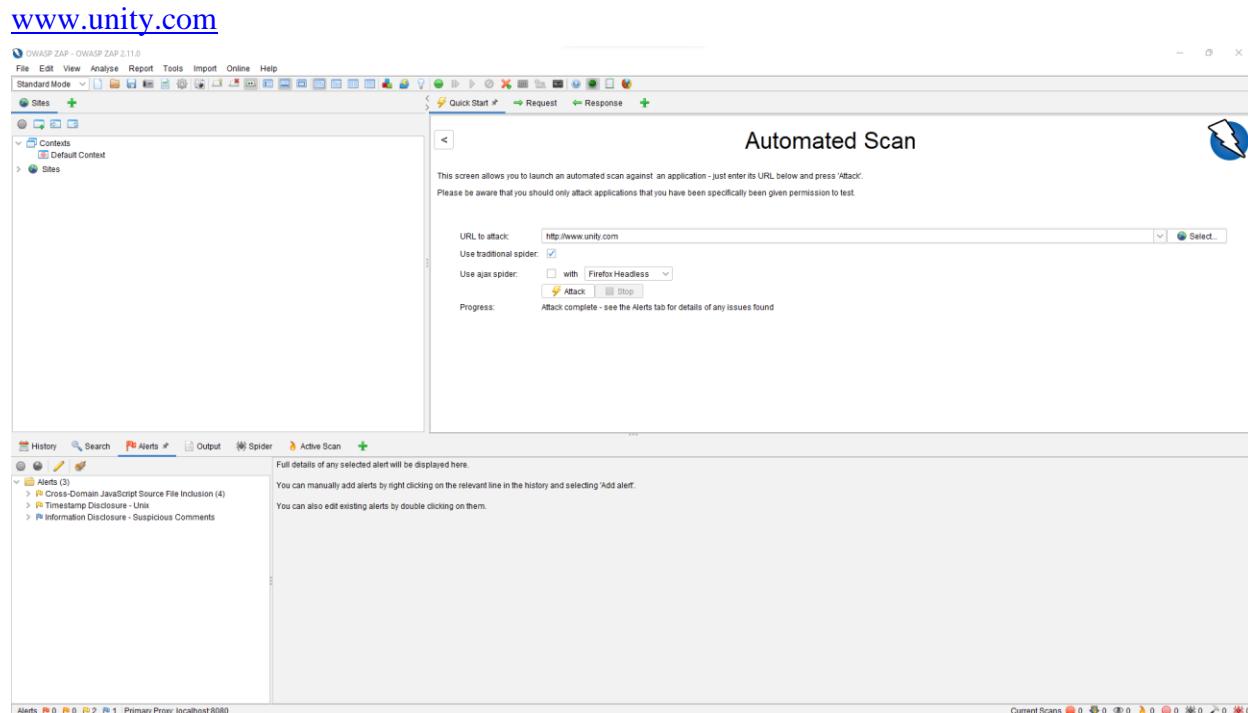


Figure 45 I scanned unity.com by owasap zap and I got 3 alerts after scanning whole site .

id.unity.com

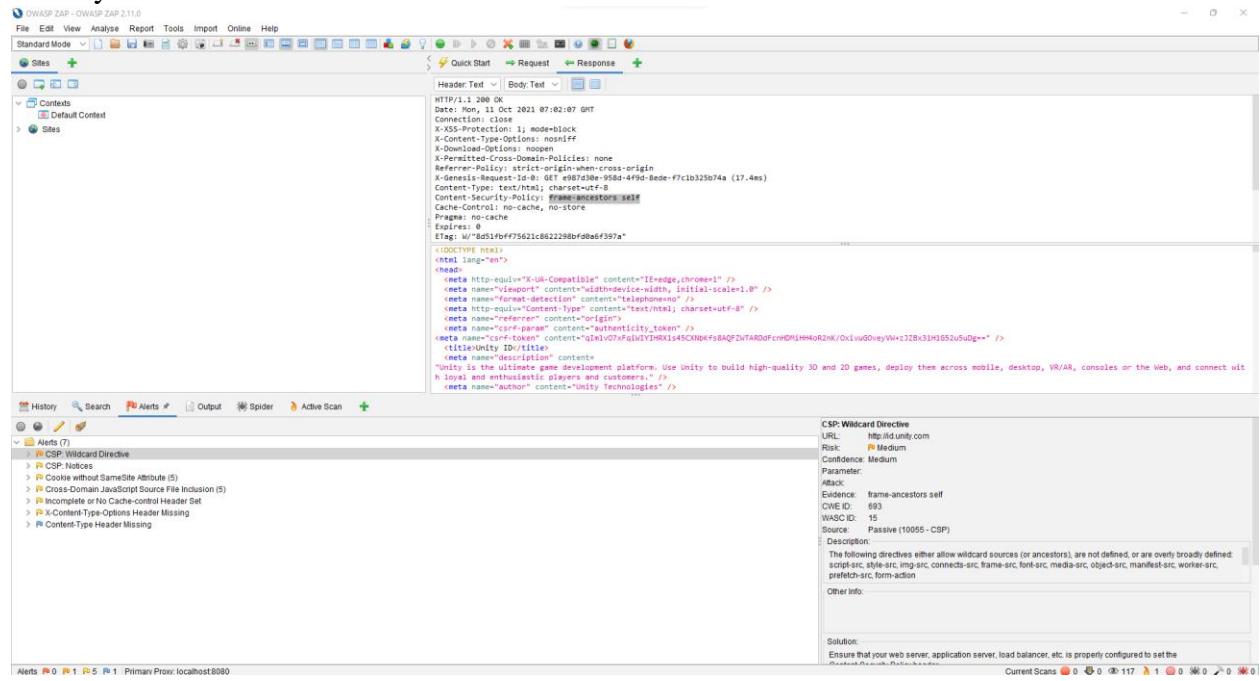


Figure 46 I scanned id.unity.com by owasap zap and I got 7 alerts after scanning whole domain .

dashboard.unity3d.com

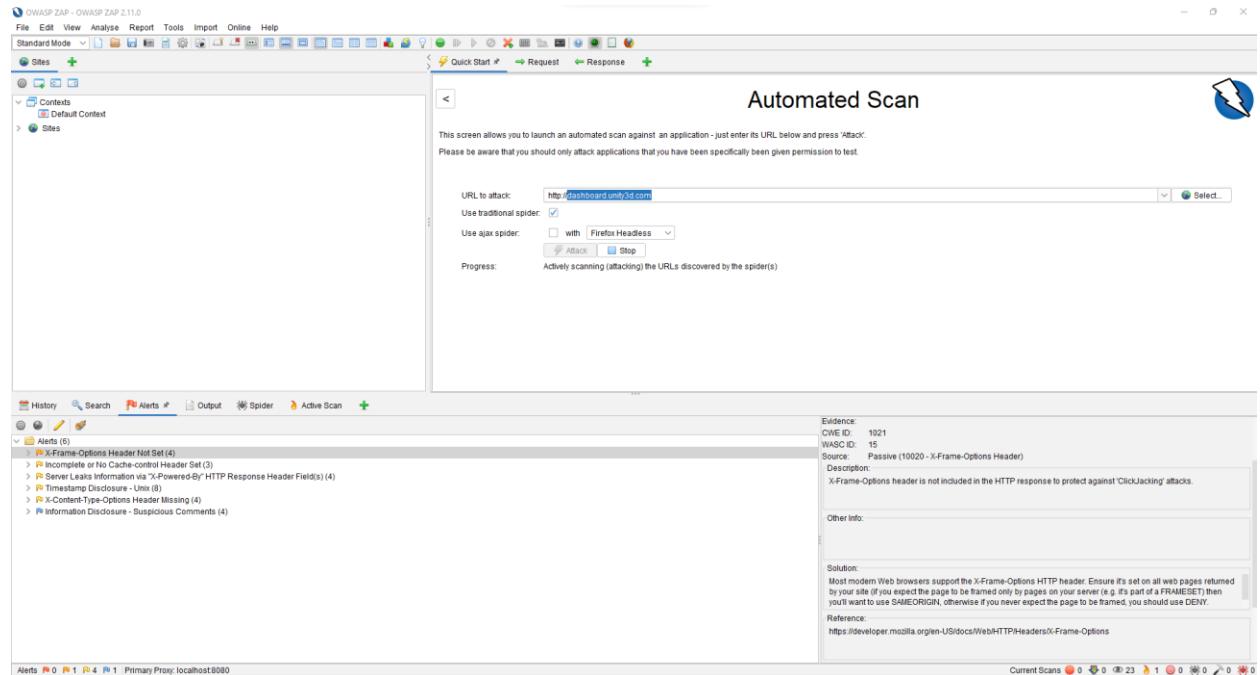


Figure 47 I scanned dashboard.unity.com by owasap zap and I got 3 alerts after scanning whole site .

Store.unity.com

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 the 'Vulnerable JS Library' is expanded, showing the following information:

- Vulnerable JS Library**
- URL:** https://store.unity.com/sites/default/files/js/js_De2fFOXoP517lI-kbXcT84kYm0gfm3W0XOE.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**
- CSP Notices
- Cross-Domain JavaScript Source File Inclusion (5)
- 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 the 'CSP Wildcard Directive' is expanded, showing the following information:

- 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 .

Netsparker

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

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

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

Netsparker 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

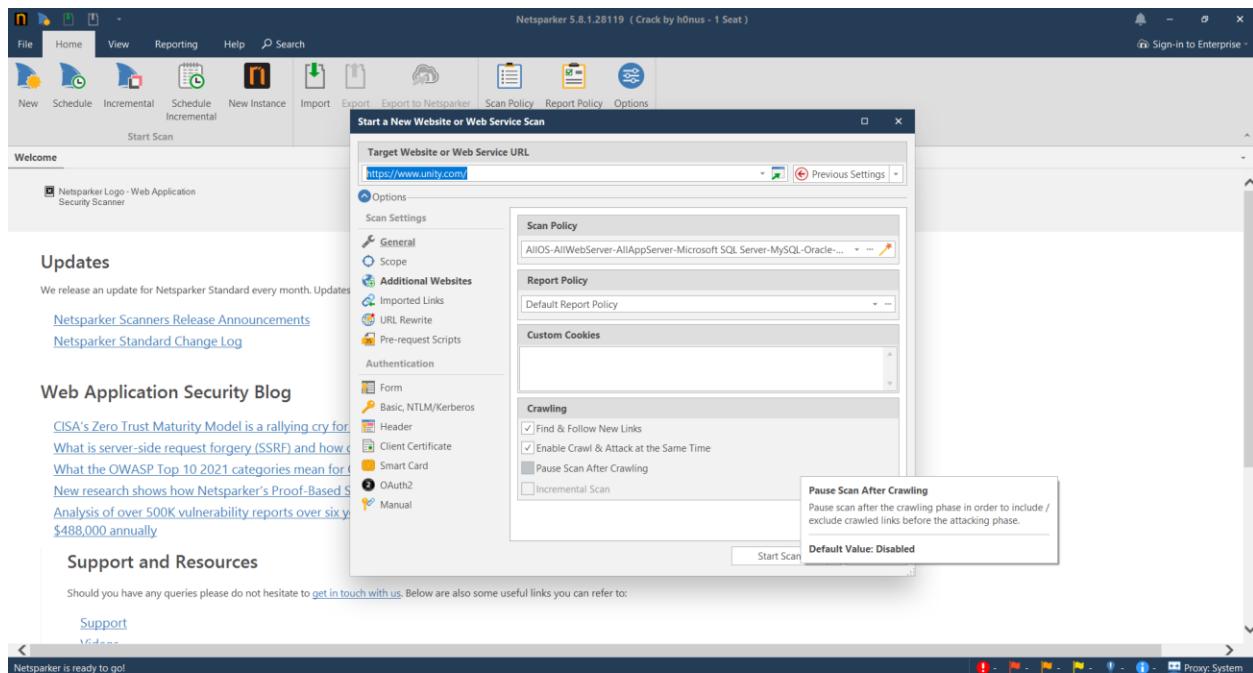


Figure 50 interface of netspaker tool

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.

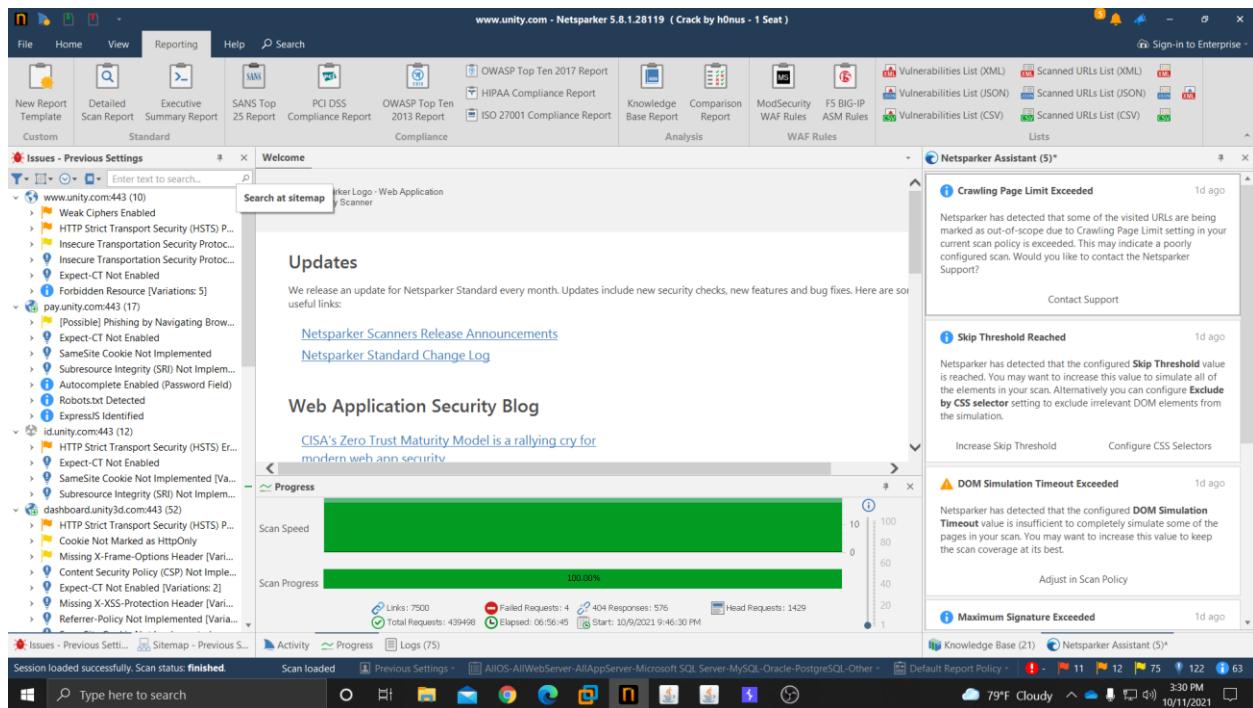


Figure 51 i scanned all in scope domains including

- 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**](#)



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

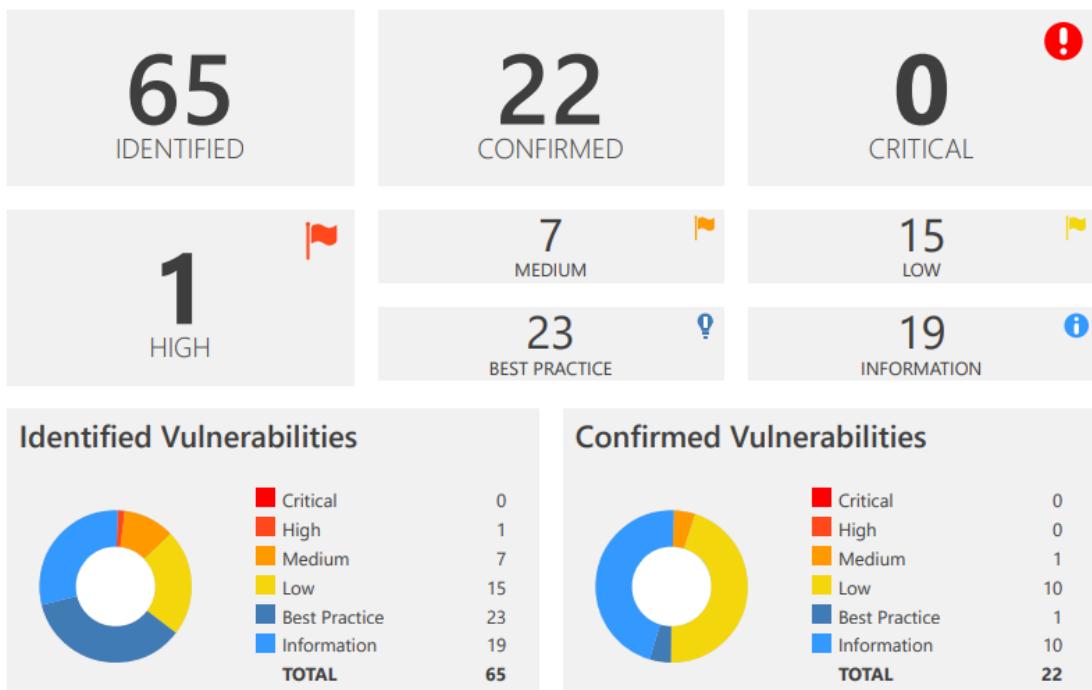


Figure 52 after about 7 hours scanning I got full detailed report regarding the vulnerabilities of in scope domains

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

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

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	Cookie Not Marked as HttpOnly	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,1,320,a063ebe9,1,190,4863fd35,0,320,c b2d5c6f,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...	
!	Cookie Not Marked as HttpOnly	GET	https://store.unity.com/de	
!	Cookie Not Marked as Secure	GET	https://analytics.cloud.unity3d.com/	
!	Cookie Not Marked as Secure	GET	https://store.unity.com/de	
!	Insecure Frame (External)	GET	https://store.unity.com/de	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://www.unity.com/	
!	Internal Server Error	POST	https://analytics.cloud.unity3d.com/	
!	User Controllable Cookie	GET	https://analytics.cloud.unity3d.com/	
!	Windows Short Filename	OPTIONS	https://store.unity.com/ruthemes/store/images/*~1%5ca.aspx?a spxerrorpath=/	
!	Content Security Policy (CSP) Not Implemented	GET	https://dashboard.unity3d.com/auth/	
!	Content Security Policy (CSP) Not Implemented	GET	https://store.unity.com/rpiframe.html	
!	Expect-CT Not Enabled	GET	https://analytics.cloud.unity3d.com/	
!	Expect-CT Not Enabled	GET	https://dashboard.unity3d.com/	
!	Expect-CT Not Enabled	GET	https://id.unity.com/	

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

		Expect-CT Not Enabled	GET	https://www.unity.com/
		Missing X-XSS-Protection Header	GET	https://dashboard.unity3d.com/auth/
		Missing X-XSS-Protection Header	GET	https://store.unity.com/themes/contrib/unity_base/js/unity-cdp.js
		Referrer-Policy Not Implemented	GET	https://dashboard.unity3d.com/auth/
		Referrer-Policy Not Implemented	GET	https://store.unity.com/rpiframe.html
		SameSite Cookie Not Implemented	GET	https://analytics.cloud.unity3d.com/
		SameSite Cookie Not Implemented	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,1,320,a063ebe9,1,190,4863fd35,0,320,cb2d5c6f,0,190,6ad47c6c,0,320,7bdb49f6,0,190,b6540200,0,320,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...
		SameSite Cookie Not Implemented	GET	https://id.unity.com/
		SameSite Cookie Not Implemented	GET	https://pay.unity.com/os2/orders/new
		SameSite Cookie Not Implemented	GET	https://store.unity.com/de
		Subresource Integrity (SRI) Not Implemented	GET	https://analytics.cloud.unity3d.com/
		Subresource Integrity (SRI) Not Implemented	GET	https://dashboard.unity3d.com/auth/unity?browserSignature=Rs2.0.6:unity::s11,2,26b5e19,2,320,a063ebe9,1,190,4863fd35,0,320,cb2d5c6f,0,190,6ad47c6c,0,320,7bdb49f6,0,190,b6540200,0,320,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
!	Subresource Integrity (SRI) Not Implemented	GET	https://id.unity.com/c:/boot.ini	URI-BASED
!	Subresource Integrity (SRI) Not Implemented	GET	https://pay.unity.com/c:/boot.ini	URI-BASED
!	Subresource Integrity (SRI) Not Implemented	GET	https://store.unity.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.unity.com/	
!	[Possible] Internal Path Disclosure (Windows)	GET	https://store.unity.com/themes/c:/apple-touch-icon.png?v=%2527	v
!	Apache Web Server Identified	GET	https://analytics.cloud.unity3d.com/robots.txt	
!	CDN Detected (Google Cloud CDN)	GET	https://dashboard.unity3d.com/	
!	Content Security Policy (CSP) Keywords Not Used Within Single Quotes	GET	https://analytics.cloud.unity3d.com/	
!	Email Address Disclosure	GET	https://store.unity.com/sites/default/files/js/js_y5DhFNCCGkfQ-21sG91FZX0tU0y73izZRE05jyh6sQA.js	
!	ExpressJS Identified	GET	https://pay.unity.com/robots.txt	
!	Generic Email Address Disclosure	GET	https://store.unity.com/themes/contrib/unity_base/css/unity-enty-po-plus.css	
!	Missing object-src in CSP Declaration	GET	https://analytics.cloud.unity3d.com/	
!	Unexpected Redirect Response Body (Too Large)	GET	https://store.unity.com/download-nuo	

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

Identified Vulnerabilities & Mitigations

01. Out-of-date Version (Modernizr)

Severity: High

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

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

Countermeasures :

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

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=BAh7B0kiD3Nlc3Npb25faWQG0gZFVEkiJTYzODAxMTZhY2IxMzU0NWQ0ZGVmOGRkMTc2YTdiYzQ
zBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkimTzldGVJUDFPcmI3LzJkdFU1Ym1RYkU0Y3gwMFhIZU51MkJsM2xLvWl4Ykk9BjsARG%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: 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-Nginx-Cache: MISS
```

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

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: [HKEY_LOCAL_MACHINE\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.**
 - Click on Start and then Run, type regedit32 or regedit, and then click OK.
 - 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

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

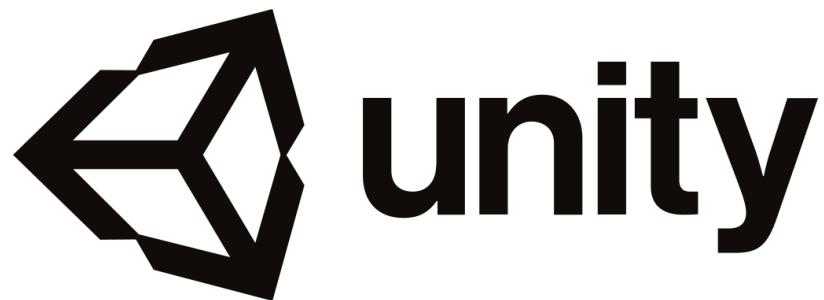
In average, the unity.com was well-designed and had many security mechanisms in place to defend itself from cyber-attacks when the audit was conducted. During the testing, only medium to low-risk vulnerabilities and best practices were discovered, and there were only one high-risk vulnerabilities discovered, 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.



WEB AUDIT

WWW.UNITY.COM



K.K.K.P. Kumara