



Web Security – IE2062

3. TikTok Bug Bounty

A D A Ihansa

IT22899606

Web Audit

tiktok.com

Contents

Introduction to Bug Bounty program and audit scope.....	4
Information gathering phase.....	6
Finding active subdomains and their states	6
Sublist3r	6
HTTPProbe	9
Netcraft.....	10
Spiderfoot.....	11
Google Dorks	13
Directory and services enumeration.....	16
Dirbuster.....	16
Gobuster	17
Nmap	18
Automated Testing	19
OWASP ZAP	19
Manual Testing	27
SQL injection.....	27
Checking for Insecure HTTP methods	28
Conclusion.....	30
References	30

Introduction to Bug Bounty program and audit scope

TikTok is a leading platform for short-form mobile videos, aiming to inspire creativity and bring joy to its users. It's a global hub for capturing and sharing life's moments, fostering a community where everyone can be a creator. TikTok's mission is to present the world's creativity, knowledge, and everyday important moments through its videos, making it a vibrant space for diverse content and expression.

In hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

tiktok.com









































































careers.tiktok.com

com.tiktok.tv

developers.tiktok.com

shop.tiktok.com

The bug bounty program specifies the eligible subdomains within its scope, stating that any subdomain falling under tiktok.com is included.

Asset name 	Type 	Coverage 	Max. severity 	Bounty 	Last update 
com.tiktok.tv TikTok TV app	Android: Play Store	In scope	 Critical	 Eligible	Mar 2, 2023
com.zhiliao.musically.livewallpaper	Android: Play Store	In scope	 Critical	 Eligible	Mar 2, 2023
641062073 iOS Store Download.	iOS: App Store	In scope	 Critical	 Eligible	Jan 23, 2023
1591003012 TikTok Shop Seller Center iOS Store Download.	iOS: App Store	In scope	 Critical	 Eligible	Oct 2, 2023
shop.tiktok.com TikTok Shop	Domain	In scope	 Critical	 Eligible	Mar 2, 2023
com.ss.android.ugc.now Play Store Download.	Android: Play Store	In scope	 Critical	 Eligible	Jan 23, 2023
com.tiktokshop.seller TikTok Shop Seller Center Play Store Download.	Android: Play Store	In scope	 Critical	 Eligible	Oct 2, 2023
 pay.tokopediiax.com	Domain	In scope	 Critical	 Eligible	 Apr 4, 2024
www.pangleglobal.com	Domain	In scope	 Critical	 Eligible	Oct 2, 2023
 affiliate-id.tokopedia.com	Domain	In scope	 Critical	 Eligible	 Apr 4, 2024
fp-sg.tiktokv.com	Domain	In scope	 Critical	 Eligible	Jan 15, 2024
com.zhiliaoapp.musically Play Store Download	Android: Play Store	In scope	 Critical	 Eligible	Jan 23, 2023
creatormarketplace.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
835599320 iOS Store Download	iOS: App Store	In scope	 Critical	 Eligible	Jan 23, 2023
 shop-id.tokopedia.com	Domain	In scope	 Critical	 Eligible	 Apr 4, 2024
1235601864 iOS Store Download	iOS: App Store	In scope	 Critical	 Eligible	Jan 23, 2023
com.ss.android.ugc.trill Play Store Download	Android: Play Store	In scope	 Critical	 Eligible	Jan 23, 2023
effecthouse.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
live-backstage.tiktok.com	Domain	In scope	 Critical	 Eligible	Mar 6, 2023
business.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
academy-outbound-ads.tiktok.com	Domain	In scope	 Critical	 Eligible	Oct 2, 2023
*.tiktok.com	Other	In scope	 Critical	 Eligible	Jan 23, 2023
careers.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
developers.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
 seller-id.tokopedia.com	Domain	In scope	 Critical	 Eligible	 Apr 4, 2024
ads.tiktok.com	Domain	In scope	 Critical	 Eligible	Jan 23, 2023
partner.tiktokshop.com	Domain	In scope	 Critical	 Eligible	Mar 2, 2023
*.tiktokv.com	Other	In scope	 Critical	 Eligible	Jan 23, 2023

Information gathering phase.

The initial phase of information gathering, commonly known as reconnaissance or recon, is crucial for obtaining insights into the nature and behavior of the target. This phase holds significant importance during audits or attacks as it facilitates the identification of potential vulnerabilities by gaining a deeper understanding of the target.

There are two main methods for conducting information gathering scans:

1. Active Scanning: This method involves generating substantial activity on the target system, often resulting in the retrieval of extensive information.
2. Passive Scanning: In contrast to active scanning, this approach minimizes disruption to the target system, albeit typically providing fewer comprehensive results compared to active scanning.

In bug bounty programs, where details about the underlying architecture of systems are usually not disclosed (referred to as black box pentesting), specific tools and techniques are essential for gathering insights into their services, devices, and exposed information. This enables testers to develop a better understanding of the systems they are assessing..

Finding active subdomains and their states

Sublist3r

Sublist3r, a Python tool, is specifically designed to reveal subdomains linked to a specified target website. Utilizing search engines and diverse online services, it systematically scours the web for available subdomains associated with the designated target domain. Given the opportunity to explore any subdomain within reddit.com, it is recommended to identify additional subdomains for testing objectives.

To install Sublist3r, navigate to its GitHub repository at <https://github.com/aboul3la/Sublist3r.git>. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

...

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

...

Please note that Sublist3r necessitates either Python 2.7 or Python 3.4 to operate smoothly.

After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

sudo pip install -r requirements.txt

After installing the requirements, enter

`python3 sublist3r.py -d <domain_name>`

to find subdomains under the mentioned domain.

**In some Linux distributions, there will be an error saying that "[!] Error: Virustotal probably now is blocking our requests". To avoid this you will need to get the API key from VirusTotal by creating an account. After the API key has been obtained, export it to an environment variable using, export VT_APIKEY=<API key>. This will work most of the time, but this is not a must.*

Since I need to check the subdomains after, I am writing the results to a file using -o switch.

```
(kali㉿kali)-[~/Desktop/Tools/Sublist3r]
$ python3 sublist3r.py -d tiktok.com -o /home/kali/Documents/audit/tiktok/tiktok.txt

File System

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tiktok.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
[-] Saving results to file: /home/kali/Documents/audit/tiktok/tiktok.txt
[-] Total Unique Subdomains Found: 83
www.tiktok.com
tracking.infobip.account.tiktok.com
activity.tiktok.com
ads.tiktok.com
ads-service.tiktok.com
affiliate.tiktok.com
analytics.tiktok.com
apac-marketing.tiktok.com
business.tiktok.com
business-suite.tiktok.com
business-tips.tiktok.com
careers.tiktok.com
creatormarketplace.tiktok.com
datahub.tiktok.com
developer-sg.tiktok.com
developers.tiktok.com
discover.tiktok.com
e.tiktok.com
link.e.tiktok.com
effecthouse.tiktok.com
eu.tiktok.com
business-sso.eu.tiktok.com
```

Upon examining for accessible subdomains, the next step involves identifying those that are operational. This can be accomplished by employing an additional tool known as 'httprobe'.

HTTPProbe

This tool can find domains that are up and running. To find active subdomains under this site, I am using the text file generated before by the sublist3r and writing the active subdomains to another new file.

```
(kali@kali)-[~/Desktop/Tools/Sublist3r]
$ httpprobe < /home/kali/Documents/audit/tiktok/tiktok.txt > /home/kali/Documents/audit/tiktok/active_tiktok.txt
```


Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.

```
(kali@kali)-[~/Desktop/Tools/Sublist3r]
$ cat /home/kali/Documents/audit/tiktok/active_tiktok.txt
https://ads.tiktok.com
https://www.tiktok.com
http://www.tiktok.com
https://activity.tiktok.com
https://business.tiktok.com
https://analytics.tiktok.com
http://ads.tiktok.com
http://business.tiktok.com
https://tracking.infobip.account.tiktok.com
http://activity.tiktok.com
https://affiliate.tiktok.com
https://business-suite.tiktok.com
http://analytics.tiktok.com
http://business-suite.tiktok.com
https://creatormarketplace.tiktok.com
http://tracking.infobip.account.tiktok.com
http://creatormarketplace.tiktok.com
https://effecthouse.tiktok.com
http://affiliate.tiktok.com
https://getstarted.tiktok.com
http://effecthouse.tiktok.com
http://getstarted.tiktok.com
https://in.tiktok.com
https://link.e.tiktok.com
http://in.tiktok.com
https://live-backstage.tiktok.com
https://developers.tiktok.com
http://live-backstage.tiktok.com
https://livecenter.tiktok.com
https://m.tiktok.com
http://m.tiktok.com
https://apac-marketing.tiktok.com
http://livecenter.tiktok.com
https://eu-marketing.tiktok.com
https://music.tiktok.com
https://gaming.tiktok.com
http://apac-marketing.tiktok.com
http://link.e.tiktok.com
http://music.tiktok.com
http://eu-marketing.tiktok.com
https://livesend.tiktok.com
https://discover.tiktok.com
http://developers.tiktok.com
http://gaming.tiktok.com
https://newsroom.tiktok.com
```

Netcraft






Netcraft, an internet services firm, offers online security solutions. Their services encompass automated vulnerability scanning and application security. No downloads or intricate setups are necessary as these services are accessible online.

By utilizing Netcraft search feature on their website, users can retrieve various details including site rank, IP address, SSL/TLS versions in use, hosting country, and hosting company.

[LEARN MORE](#)[REPORT FRAUD](#)

Site report for <https://tiktok.com>


► 🔍 [Look up another site?](#)

Share:     

Background

Site title	TikTok - Make Your Day	Date first seen	April 2012
Site rank	32734	Primary language	English
Description	Not Present		

Network

Site	https://tiktok.com	Domain	tiktok.com
Netblock Owner	Amazon.com, Inc.	Nameserver	ns-440.awsdns-55.com
Hosting company	Amazon	Domain registrar	gandi.net
Hosting country	 US	Nameserver organisation	whois.markmonitor.com
IPv4 address	3.162.140.48 (VirusTotal)	Organisation	TIKTOK LTD, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, Cayman Islands
IPv4 autonomous systems	AS16509	DNS admin	awsdns-hostmaster@amazon.com

For full site report: [Site report for https://tiktok.com | Netcraft](#)

This data is publicly accessible, and some details regarding the system and its technology can be uncovered through available sources.

Since, many users utilize this website, and considering that the IP addresses match those of my specified targets, I only obtain a Netcraft report for this domain. However, reports for the other mentioned subdomains can also be retrieved from Netcraft.

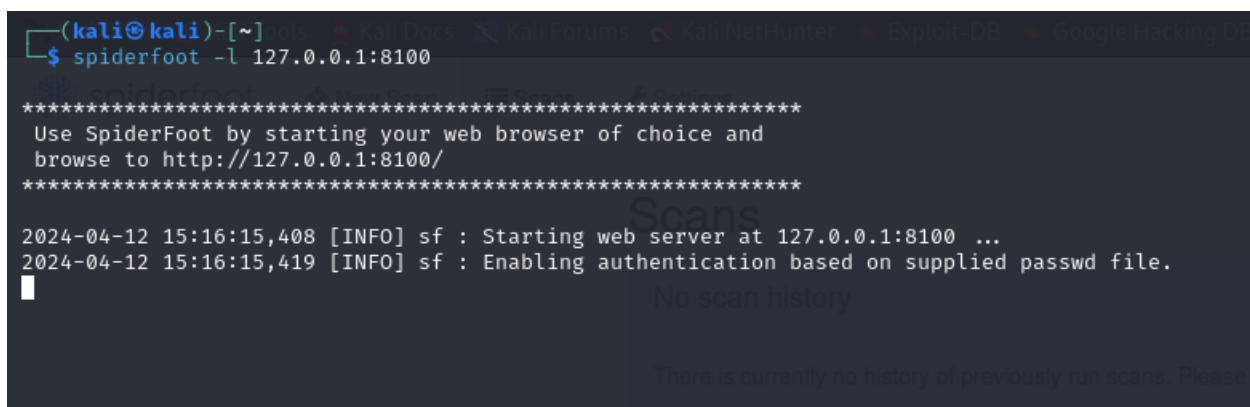
Spiderfoot

SpiderFoot is an open-source intelligence (OSINT) automation tool that is designed to simplify the process of gathering and analyzing data. It integrates with a wide range of data sources and provides an intuitive web-based interface or a command-line option. SpiderFoot is equipped with over 200 modules for various data analysis tasks, including host/sub-domain/TLD enumeration/extraction, email address, phone number and human name extraction, and much more. It also offers export options in CSV, JSON, and GEXF formats, and integrates with the TOR network for dark web searches. SpiderFoot is a powerful tool for both offensive and defensive reconnaissance, making it an asset in the field of cybersecurity.

Using spiderfoot

It must be setup, before using this tool.

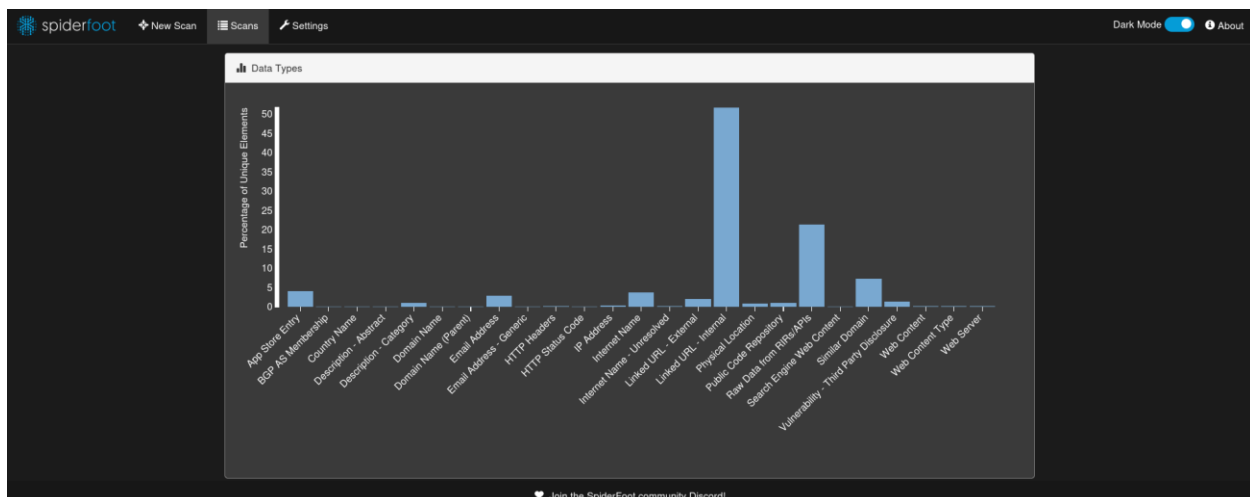
Spiderfoot -l 127.0.0.1:8100

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The command \$ spiderfoot -l 127.0.0.1:8100 has been entered. The output shows a series of asterisks, followed by instructions to use SpiderFoot via a web browser at http://127.0.0.1:8100/. Another series of asterisks follows. Then, two log messages are displayed: '2024-04-12 15:16:15,408 [INFO] sf : Starting web server at 127.0.0.1:8100 ...' and '2024-04-12 15:16:15,419 [INFO] sf : Enabling authentication based on supplied passwd file.' Below these, a cursor is visible. In the background, a semi-transparent window titled 'Scans' is visible, showing 'No scan history' and a message: 'There is currently no history of previously run scans. Please'.

To utilize the Spiderfoot tool, which is hosted on localhost (127.0.0.1) at port 8100, just launch a web browser and enter `http://127.0.0.1:8100` in the address bar.

After the scanner loads, proceed to "New scan" and tailor your scan type according to the scope of your investigation. There are various modules at your disposal that can be activated or deactivated based on your permissions. Since you're engaging in a passive information gathering phase, opt for the 'footprint' option to crawl and collect information about the website.

Spiderfoot results

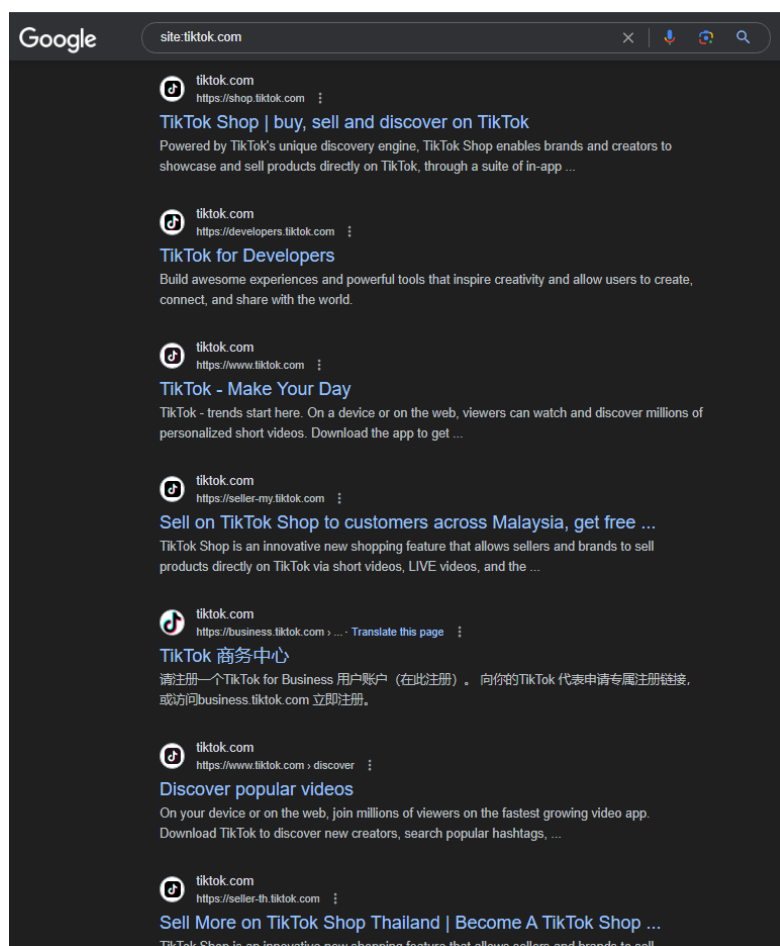


The scan has produced noteworthy findings, such as usernames, SSL certificates, and physical addresses. A significant portion of this data seems to be publicly accessible information and links leading to external websites. However, it's essential to highlight those usernames, especially when coupled with their corresponding email addresses, could potentially become avenues for social engineering or spear phishing attacks. Nevertheless, it's important to acknowledge that addressing such concerns lies beyond the boundaries of this assessment.

Google Dorks

Google Dorks, also known as Google Hacking or Google Dorking, are specialized search queries that leverage Google's powerful search engine to unearth specific information and vulnerabilities that might not be accessible through standard searches. These are advanced search queries that use special operators to find specific information in Google's databases. They can be used to uncover hidden data or vulnerabilities on websites. By employing these dorks, you can focus on specific search results, unveiling hidden gems that ordinary searches might miss. They are valuable for security research but also pose risks if used maliciously. For example, they can reveal sensitive or private information about websites and the companies, organizations, and individuals that own and operate them. Google Dorks are a powerful tool for information gathering and vulnerability scanning, but they should be used responsibly to avoid unintended consequences.

site:tiktok.com operator searches for websites that has “**tiktok.com**” in their domains.



Certainly, the appearance of subdomains in search results illustrates a common utilization of Google Dorking. This method facilitates the discovery of different file types and pages that are exposed by a specific website on the internet, whether it's deliberate or unintentional. Through the refinement of search queries, users can unearth information and potentially pinpoint vulnerabilities or confidential data that might be accessible online.

During a search for various file types exposed on the internet, I came across some intriguing and possibly concerning PDFs within this subdomain.


Google

site:tiktok.com filetype:pdf

× | 🔊 🌐 🔍


All Images Shopping Videos News More Tools

About 379 results (0.23 seconds)

 **tiktok.com**
https://www.tiktok.com › business › library › Tik... PDF

Best Practices Playbook


Whether you're a beginner starting out with TikTok for the first time or already know your way around the platform, this playbook is chock-full of the ...

 **tiktok.com**
https://www.tiktok.com › business › library › Stor... PDF

Formatos narrativos para


No sorprende el hecho de que las empresas que muestran autenticidad en sus contenidos tienen más éxito en TikTok. Pero las que realmente alcanzan un nivel ...

6 pages

 **tiktok.com**
https://www.tiktok.com › Top_Tips_One_Pager_PT PDF

7 ótimas sugestões para - criar vídeos no ...


O TikTok proporciona uma experiência de ecrã inteiro envolvente. Comparados com os vídeos que não se adaptam ao ecrã, os vídeos que usam a relação de aspeto ...

 **tiktok.com**
https://www.tiktok.com › business › library › boas... PDF

Brasil

Ads Manager, você precisa que tipo de visitantes são através da jornada de usuário com um evento de meio de funil como Add to Cart.

3 pages

 **tiktok.com**
https://www.tiktok.com › business › library › Stor... PDF

PowerPoint 演示文稿

אין זה מפתיע שעסקים שמציגים תוכן אותנטי מצליחים יותר ב- TikTok. אבל העסקים שהביצועים שלהם הם ברמה אחת מעל כולם הם אלה שיוצרים מעורבות וחיבור עמוקים ...

The management of information and files within this subdomain appears to be efficient, as no additional significant files were uncovered apart from the previously mentioned PDFs.

Directory and services enumeration

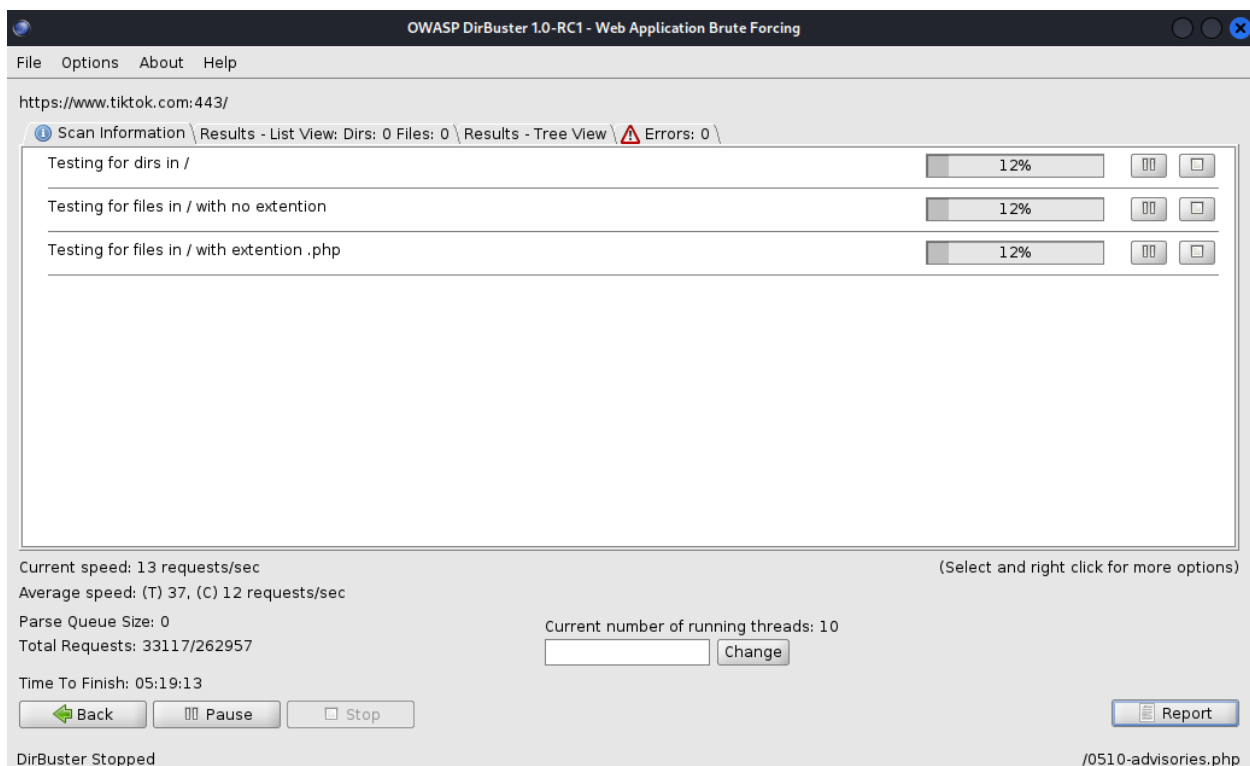
Dirbuster

DirBuster, a web content scanner developed by OWASP, utilizes brute force methods to uncover different directories within a target website. By scrutinizing HTTP responses and their associated response codes, the tool detects concealed or referenced directories. Built in Java, DirBuster supports multi-threading to expedite directory scanning and produce a comprehensive file and folder structure of the target site.

Employing this tool facilitates the identification of directories or files that might be accessible yet not overtly exposed. Furthermore, it offers a glimpse into the server's file and folder arrangement, assisting in comprehending its structure and potential vulnerabilities.

Domain: www.tiktok.com

After running the scan for some time, DirBuster encountered errors and ceased functioning. Upon further investigation, it appeared that DirBuster was unable to access the domain.



Gobuster

Enumerating hidden directories and files is a prevalent method of attacking an application. This approach can yield valuable information for executing specific attacks. Although numerous tools are available for this purpose, their effectiveness varies. Gobuster, a command-line tool implemented in Go, stands out among them. Go is a programming language known for its fast-processing capabilities, excellent concurrency support, and speed. However, Gobuster lacks the feature of recursive directory exploration. Typically, this isn't a significant issue as most scanners can compensate for this limitation.

As Dibuster failed to enumerate, I tried with gobuster for dir enumeration. But still gobuster also failed to enumerate hidden directories.

```
(kali@kali)~$ gobuster dir -u https://tiktok.com -t 50 -w /usr/share/dirb/wordlists/common.txt -x .php,.html -b 301

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: https://tiktok.com
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 301
[+] User Agent: gobuster/3.6
[+] Extensions: php,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
Progress: 13842 / 13845 (99.98%)
Finished
```

Nmap

Nmap, also known as Network Mapper, is a flexible port scanner engineered to probe hosts and reveal their open ports, associated services, port statuses, running service versions, and the operating system in use, among other details. This open-source tool serves various purposes, offering valuable insights into network configurations and potential vulnerabilities. Additionally, Nmap supports the execution of scripts on target systems to exploit vulnerabilities or gather additional information.

Upon installation, you can access the available options by typing "nmap -h" in your command line interface. For a more detailed understanding of how the tool operates, you can consult the manual page by entering "man nmap" in your command line interface. *Note that some options may require administrator / super user privileges.

*Note that some options may require administrator / super user privileges.

I am using the following scan options for this assessment.

sudo nmap <host name> -sS -sV -O -oN <filename>

-sS: Enables SYN scan (also known as Stealth scan).

-sV: Enables version detection. It tries to detect the version of the service running in that port.

-O: Enables Operating System detection.

-oN : Outputs the scan results to text file

Scanned results for <https://www.tiktok.com/>

```
(kali@kali) ~ - /Desktop/Tools/Sublist3r
$ sudo nmap tiktok.com -sS -sV -O -oN /home/kali/Documents/audit/tiktok/nmap_tiktok.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 14:07 EDT
Nmap scan report for tiktok.com (108.156.133.118)
Host is up (0.018s latency).
Other addresses for tiktok.com (not scanned): 108.156.133.4 108.156.133.46 108.156.133.28
rDNS record for 108.156.133.118: server-108-156-133-118.sin2.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp?
80/tcp    open  http    Amazon CloudFront httpd
443/tcp   open  ssl/http Amazon CloudFront httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.94SVN|I=7KD-4/18|Time=6621616C|P=x86_64-pc-linux-gnu|H
SF:ello,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\
SF:n")|Xr(Genericlines,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")|Xr(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecog
SF:nized\r\n")|Xr(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unr
SF:ecognized\r\n")|Xr(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x2
SF:unrecognized\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

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 37.54 seconds
```

Scanned results for <https://www.careerstiktok.com/>

```
(kali@kali) ~/Desktop/Tools/Sublist3r
$ sudo nmap careers.tiktok.com -s -sV -O -eN /home/kali/Documents/audit/tiktok/nmap_careers_tiktok.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 14:12 EDT
Nmap scan report for careers.tiktok.com (104.75.84.10)
Host is up (0.0096s latency).
Other addresses for careers.tiktok.com (not scanned): 104.75.84.8
rDNS record for 104.75.84.10: a104-75-84-10.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp    open  ssl/http  AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose WAP
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X (87%), Ubiquiti embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 4.15 - 5.8 (87%), Linux 5.0 - 5.4 (87%), Linux 5.3 - 5.4 (87%), Linux 2.6.32 (87%), Linux 5.0 (86%), Linux 5.0 - 5.5 (86%), Ubiquiti WAP (Linux 2.6.32) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 9 hops

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 44.62 seconds
```

Automated Testing

For automated testing, I've selected OWASP ZAP widely used tool within the industry.

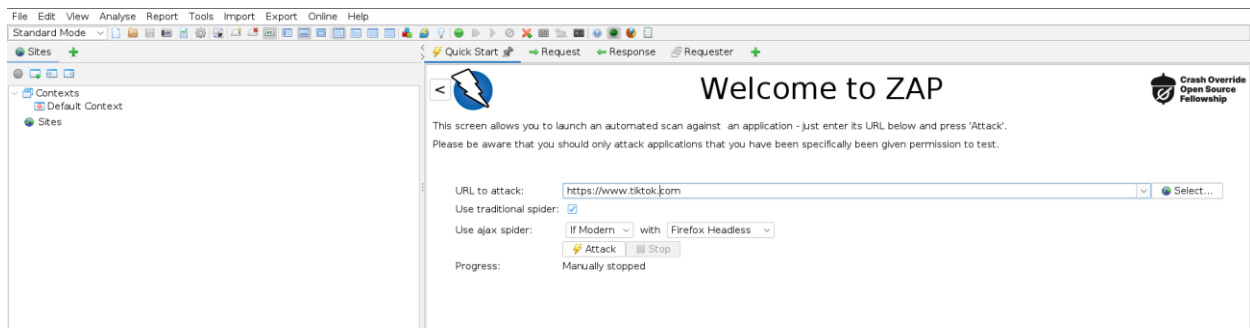
OWASP ZAP

The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is a well-known open-source vulnerability scanner recognized for its ability to operate as a Man-in-the-Middle (MITM) proxy. It evaluates various vulnerabilities by examining responses from the web application or server. OWASP ZAP is notably user-friendly and offers customization options through the installation of modules, allowing for efficient management of results.

Within this proxy, there are primarily two types of scans available:

1. **Automated Scan:** Users input the target URL and initiate the attack. The behavior can be customized by selecting the ZAP mode, triggering all scripts against the target to detect vulnerabilities and generate reports accordingly.
2. **Manual Explore:** Users can navigate to the target web application and begin exploration. During manual exploration, ZAP HUD (Heads Up Display) captures each page, while the ZAP proxy records responses.

For this assessment, I am running ZAP in automated mode.



After entering the target URL in the designated textbox, simply click on "Attack" to begin the scanning process. Once finished, you can generate a detailed report of the findings by clicking on "Report."

Below are screenshots illustrating the results obtained after scanning several domains.

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence			
Risk		User Confirmed	High	Medium	Low
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	5 (20.8%)	0 (0.0%)	1 (4.2%)
	Low	0 (0.0%)	3 (12.5%)	8 (33.3%)	1 (4.2%)
	Informational	0 (0.0%)	2 (8.3%)	1 (4.2%)	3 (12.5%)
	Total	0 (0.0%)	10 (41.7%)	9 (37.5%)	5 (20.8%)
		Total			
		24 (100%)			

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	1 (4.2%)
CSP: Wildcard Directive	Medium	15 (62.5%)
CSP: script-src unsafe-eval	Medium	8 (33.3%)
CSP: script-src unsafe-inline	Medium	7 (29.2%)
CSP: style-src unsafe-inline	Medium	15 (62.5%)
Content Security Policy (CSP) Header Not Set	Medium	147 (612.5%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1 (4.2%)
CSP: Notices	Low	15 (62.5%)
Cookie No HttpOnly Flag	Low	1 (4.2%)
Cookie Without Secure Flag	Low	1 (4.2%)
Cookie with SameSite Attribute None	Low	2 (8.3%)
Cookie without SameSite Attribute	Low	6 (25.0%)

Information Disclosure - Debug Error Messages	Low	1 (4.2%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	11 (45.8%)
Strict-Transport-Security Header Not Set	Low	147 (612.5%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	1 (4.2%)
Timestamp Disclosure - Unix	Low	156 (650.0%)
Content Security Policy (CSP) Report-Only Header Found	Informational	1 (4.2%)
Information Disclosure - Suspicious Comments	Informational	8 (33.3%)
Loosely Scoped Cookie	Informational	7 (29.2%)
Modern Web Application	Informational	7 (29.2%)
Re-examine Cache-control Directives	Informational	8 (33.3%)
Session Management Response Identified	Informational	13 (54.2%)
Total		24

*Please note that these vulnerabilities are rated according to the OWASP risk rating methodology, which can be found in this link. [OWASP Risk Rating Methodology](#).

Below are the vulnerabilities detected within this domain, along with their impacts. The insights provided, including screenshots and remedies, are sourced from the report generated by OWASP ZAP and the Netsparker website. [<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities>])

<https://www.tiktok.com> (1)

Absence of Anti-CSRF Tokens (1)

▼ GET <https://www.tiktok.com/community-guidelines>

Alert tags

- [OWASP_2021_A01](#)
- [WSTG-v42-SESS-05](#)
- [OWASP_2017_A05](#)

Alert description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.
- * The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Other info

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "s"].

Request

- Request line and header section (660 bytes)
- ▼ Request body (0 bytes)

Response

- Status line and header section (5554 bytes)
- Response body (888710 bytes)

Evidence

```
<form role="search" action="/community-guidelines/"
method="GET" class="css-805zfn ejeyabp4">
```

Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▼ GET https://www.tiktok.com/share

Alert tags

- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)

Alert description

HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied.

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 (i.e. HTTP layered over TLS/SSL).

Request

- Request line and header section (645 bytes)
- ▼ Request body (0 bytes)

Response

- Status line and header section (7215 bytes)
- ▼ Response body (69 bytes)

Redirecting to /404?fromUrl=/share.

Solution

Ensure that only one component in your stack: code, web server, application server, load balancer, etc. is configured to set or add a HTTP Strict-Transport-Security (HSTS) header.

<https://www.tiktok.com> (3)

Information Disclosure - Suspicious Comments (1)

▼ GET <https://www.tiktok.com>

Alert tags	<ul style="list-style-type: none">• OWASP 2021_A01• WSTG-v42-INFO-05• OWASP 2017_A03
Alert description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Other info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id="__UNIVERSAL_DATA_FOR_REHYDRATION_" type="application/json">{"__DEFAULT_SCOPE_": {"webapp.app-context":{"language":""," see evidence field for the suspicious comment/snippet.
Request	<ul style="list-style-type: none">► Request line and header section (229 bytes)▼ Request body (0 bytes)
Response	<ul style="list-style-type: none">► Status line and header section (6527 bytes)► Response body (152066 bytes)
Evidence	user
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Re-examine Cache-control Directives (1)

▼ GET <https://www.tiktok.com/robots.txt>

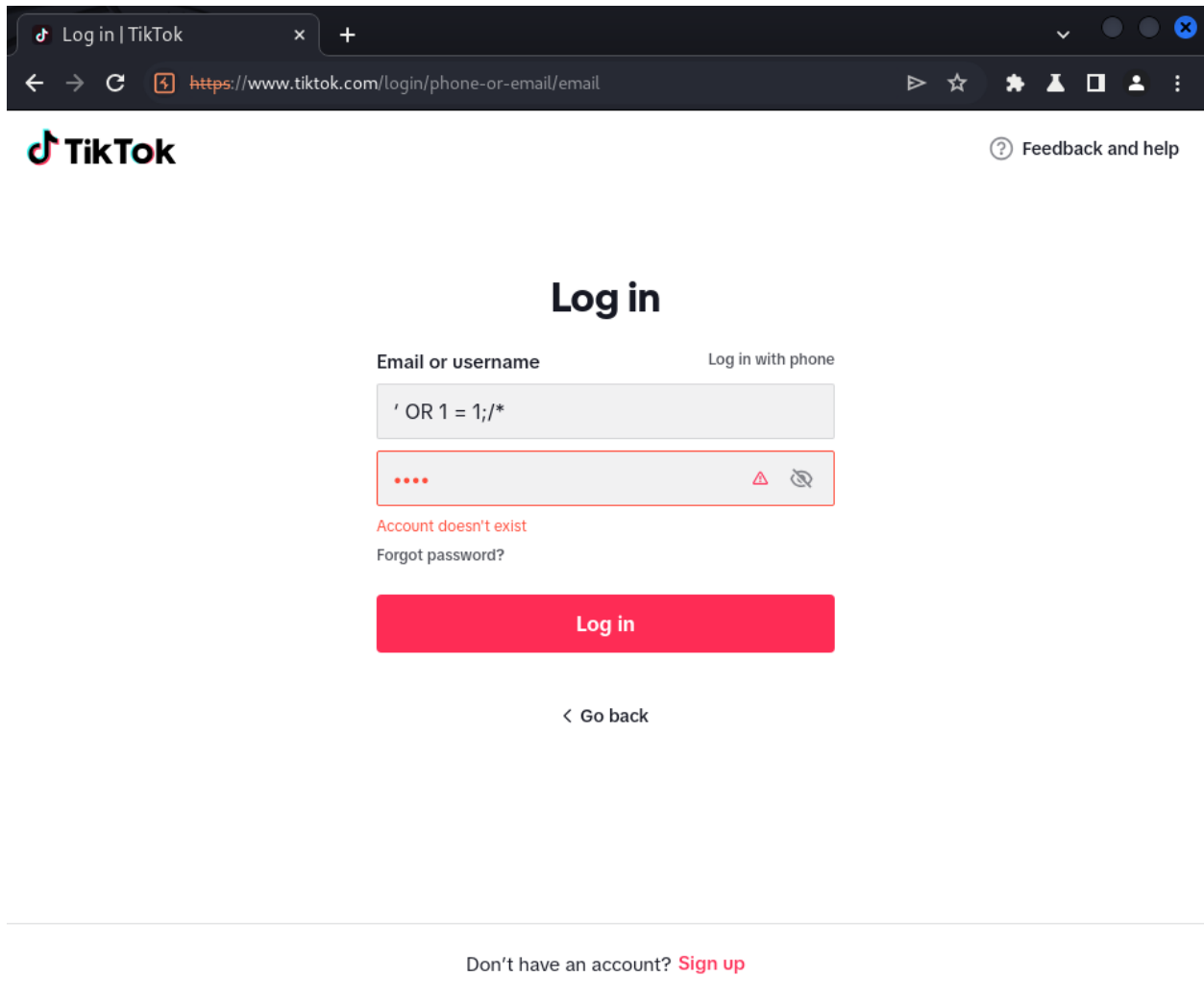
Alert tags	<ul style="list-style-type: none">• WSTG-v42-ATHN-06
Alert description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Request	<ul style="list-style-type: none">► Request line and header section (240 bytes)► Request body (0 bytes)
Response	<ul style="list-style-type: none">► Status line and header section (1097 bytes)► Response body (535 bytes)
Parameter	cache-control
Evidence	max-age=0, no-cache, no-store
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Manual Testing

SQL injection

If this page is vulnerable to SQL injection attack the Query will be executed as:

SELECT * FROM users WHERE email address = ' OR 1 = 1;/* AND password = */--



The screenshot shows a web browser window with the TikTok login page. The address bar displays the URL `https://www.tiktok.com/login/phone-or-email/email`. The page features the TikTok logo and a "Feedback and help" link. The main heading is "Log in". Below it, there are two input fields: "Email or username" and "Log in with phone". The "Email or username" field contains the SQL injection payload: `' OR 1 = 1;/*`. The password field is masked with red dots and has a red warning icon. Below the password field, a red error message states "Account doesn't exist". There is a link for "Forgot password?". A red "Log in" button is present, and below it is a "< Go back" link. At the bottom, there is a link for "Don't have an account? Sign up".

Log in | TikTok

https://www.tiktok.com/login/phone-or-email/email

TikTok

Feedback and help

Log in

Email or username Log in with phone

' OR 1 = 1;/*

.....

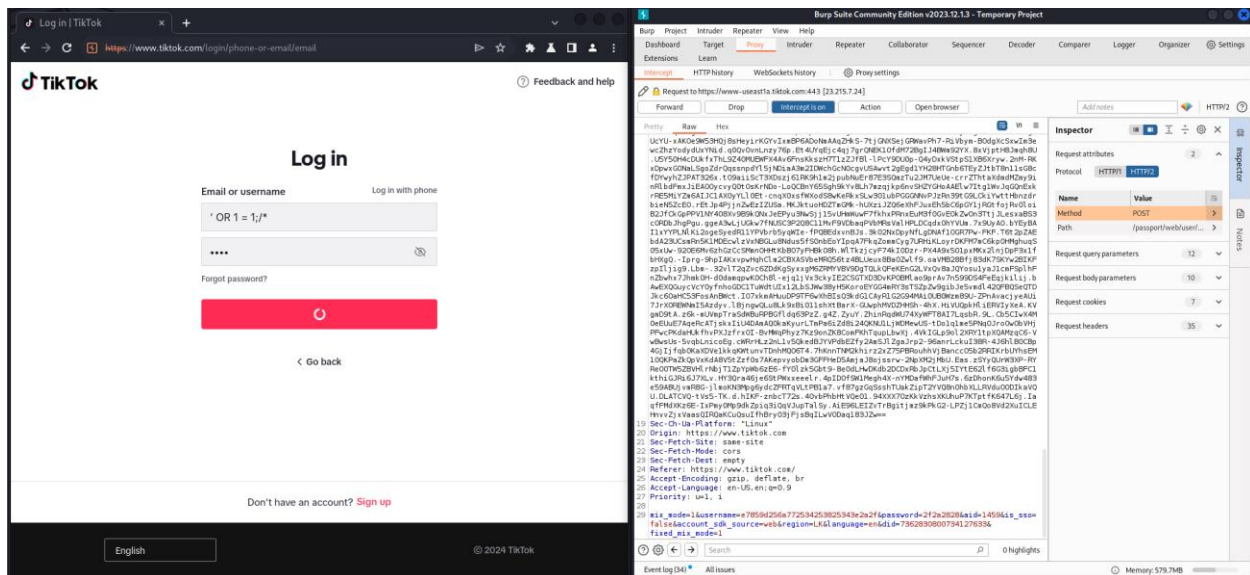
Account doesn't exist

Forgot password?

Log in

< Go back

Don't have an account? Sign up

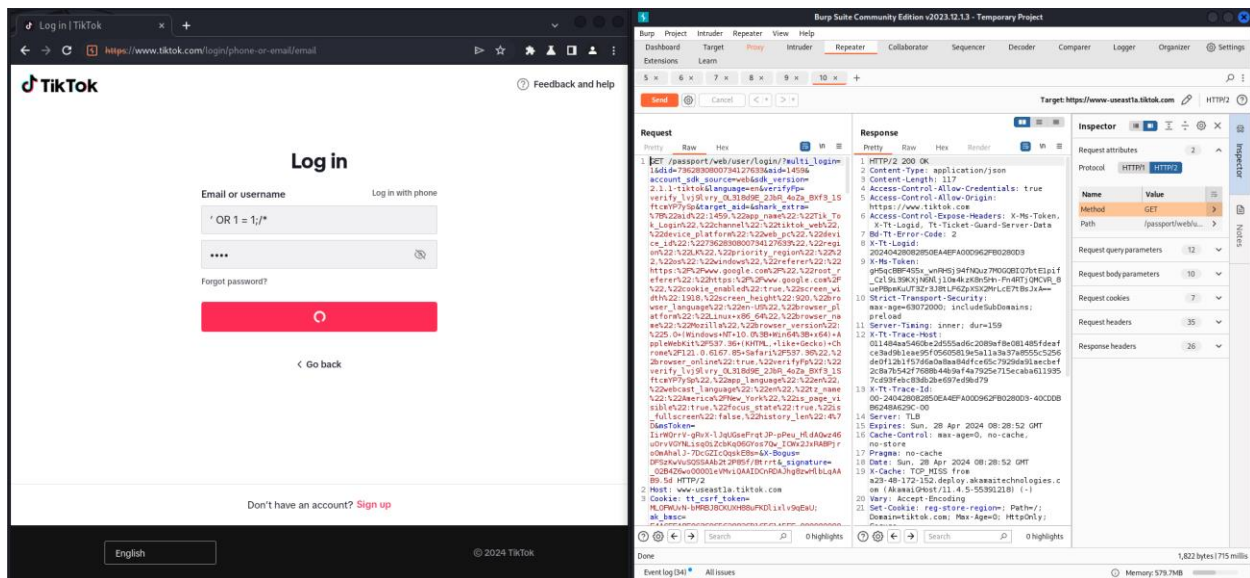


They have implemented password policies, so I attempted to intercept the request and conduct SQL injection, but I was unsuccessful. The system is well secured against SQL injection.

Checking for Insecure HTTP methods

Specific HTTP methods, particularly DELETE and PUT, pose potential security threats to the server. The DELETE method has the capability to eliminate resources from the server, while the PUT method can upload and execute files. However, these methods need to be used with care as they could potentially jeopardize the Confidentiality, Integrity, and Availability of the server and its users.

To determine the HTTP methods that are supported, I utilized the Burp proxy to capture requests and the Repeater to alter the request method. This allowed me to dispatch the altered requests to the server and scrutinize the responses.



The server only supports the POST method. Therefore, no insecure methods were utilized on the server.

Conclusion

The web application, along with its associated authorization gateway, showcases a commendable level of upkeep and control, particularly from a cybersecurity standpoint. While there have been occurrences of information exposure, these can be suitably handled, and their corresponding risk quotient is evaluated to be minimal. It's worth noting that all detected security weaknesses fell into the categories of either being Informational or of Low severity. Moreover, the vulnerabilities that were categorized as Low are not readily exploitable, as has been evidenced in the past.

It's also important to highlight that the application's security measures are regularly updated to keep up with the evolving threat landscape. Regular security audits are conducted to identify and rectify any potential vulnerabilities. The application also employs a robust encryption mechanism to protect sensitive data and ensure secure communication. Additionally, the application's user authentication process is designed to prevent unauthorized access, further enhancing its security posture. Despite the presence of some low-level vulnerabilities, the overall security of the web application and its authorization portal is well-maintained and managed. This reflects the commitment to security and the proactive approach taken towards identifying and addressing potential security issues.

References

[OWASP Top Ten | OWASP Foundation](#)

[WSTG - Stable | OWASP Foundation](#)

[ZAP \(zaproxy.org\)](#)

[GitHub - aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers](#)

[GitHub - tomnomnom/httpprobe: Take a list of domains and probe for working HTTP and HTTPS servers](#)

[Kali Tools | Kali Linux Tools](#)

[Netcraft | Leader in Phishing Detection, Cybercrime Disruption and Website Takedown](#)

[Nmap: the Network Mapper - Free Security Scanner](#)

