



Sri Lanka Institute of Information Technology

Vulnerability Assessment – Web Audit

<https://www.tiktok.com>

**Individual Assignment
IE2062 – Web Security**

Submitted by:

Student Registration Number	Student Name
IT19013756	M. H. D. V. JAYASINGHE

Date of submission
24th of October in 2020

Acknowledgement

I would like to express my deep gratuity for his invaluable guidance and advice, Dr. Lakmal rupasinghe the lecture in charge of Web security, which was vital to the initiation of this web audit.

I also want to thank Ms. Chethna Lyanapathirana, Ms. Lanisha Ruggahakotuwa and Ms. Chathu Udagedra for the help and guidance they have given us during this Web audit.

Contents

1.1.	Vulnerability Scanning (Discovery).....	3
1.2.1.	About used tools	4
1.2.2.	Scanning and generating reports	8
1.2.3.	Full – Domain scan from OWASP Acunetix Tool	87
2.	SUMMARY OF REPORT	90
3.	REFERENCES	91

1.1. Vulnerability Scanning (Discovery)

In this part, I use some vulnerability scanning tools for scan sub domains. After the consideration, my information gathering part, I choose eleven live subdomains to do the scanning furthermore.

Chosen subdomains

1. activity.tiktok.com
2. ads.tiktok.com
3. artists.tiktok.com
4. business.tiktok.com
5. careers.tiktok.com
6. creatormarketplace.tiktok.com
7. datahub.tiktok.com
8. developers.tiktok.com
9. login.tiktok.com
10. musician.tiktok.com
11. support.tiktok.com

I perform **Burp suite** and **Netsparker** scans for each of above subdomains. And I received the vulnerability reports from above tools. And finally, I perform a full domain scan using by **OWSAP Acunetix** web audit tool.

1.2.1. About used tools

1. Burp Suite professional

Burp Suite is a Java framework for web applications to test and analyze security. In Burp Suite has a proxy server, a spider, an intruder, and a so-called repeater.

Proxy server :

- Burp Suite can be set up as a proxy server, running the webserver on a proxy server, and all traffic from a browser to a web page can be accessed. Until forwarding, Burp Suite also provides the option of changing all messages. This helps you to simulate some exceptional situations.

Spider :

- The Burp Suite spider is a tool for analyzing and mapping the various website pages. The features associated with this can also often be mapped. Spider tests cookies and connects to these web applications to do so.

Intruder :

- The intruder is a method for automating web-based attacks. One condition is that the application and HTTP protocol have already been detailed known to the user. This tool provides a widely configurable HTTP request-generating algorithm. This tool can test and detect vulnerabilities such as SQL, cross-site scripts, manipulation of parameters and even brutal force.

Repeater :

- This is a tool for carrying out stress checks. You should create an HTTP request. It can be submitted several times. You can look, for example, at what happens if you receive a request involving a lot of computer power, and if a request has been received 1000 times in a row.

In Burp Suite professional version can make scans and generate the report about scans.

The image contains three vertically stacked screenshots of the Burp Suite Professional v2020.9.2 interface, demonstrating its functionality for network scanning and reporting.

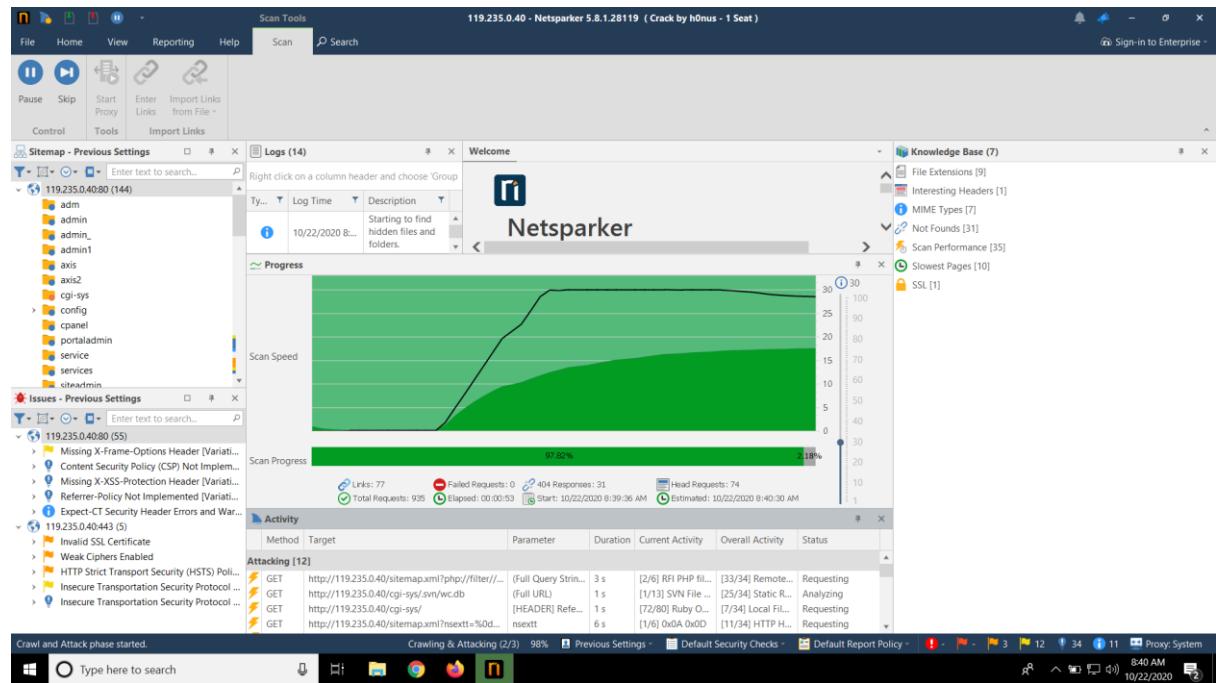
- Screenshot 1: FoxyProxy Options - Mozilla Firefox**
This screenshot shows the "FoxyProxy Options" extension settings in Mozilla Firefox. A single proxy entry named "burpSuite" is listed, which is configured to use port 127.0.0.1. The "On" button is selected, indicating the proxy is active. The interface includes a sidebar with various configuration options like "Add", "Import Settings", and "Delete All".
- Screenshot 2: Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia**
This screenshot displays the main Burp Suite interface. It features a "Tasks" panel on the left showing three active scanning jobs: "Live proxy traffic from Proxy (all traffic)", "Live audit from Proxy (all traffic)", and "Live audit from Proxy (all traffic)". The "Issue activity" panel on the right lists detected issues, and the "Event log" panel at the bottom shows system logs. The top navigation bar includes tabs for "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options".
- Screenshot 3: Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia**
This screenshot shows the "Intercept" tab of the Burp Suite interface. It displays a list of captured requests, with the first one highlighted. The request details show a POST to https://activity.libre.com:443 with a status of 200 OK. The "Actions" dropdown menu is open, showing options like "Forward", "Drop", "Interception", "Action", and "Open Browser". The bottom status bar indicates "Memory: 82.0MB" and "Disk: 30KB".

2. Netsparker

Netsparker is a web application security scanner that is automated and fully configurable, allowing us to search and detect security defects for websites, web applications and Web services. Notwithstanding the medium or language that is being constructed, Netsparker will search all forms of web apps.

Netsparker is the only online web-scanner that automatically utilizes read-only and safely identified vulnerabilities to validate identified problems. It also provides evidence of the flaw, so we do not have to spend time testing it manually. For example, the database name shows proof of exploit in the event of a detected SQL injection vulnerability.

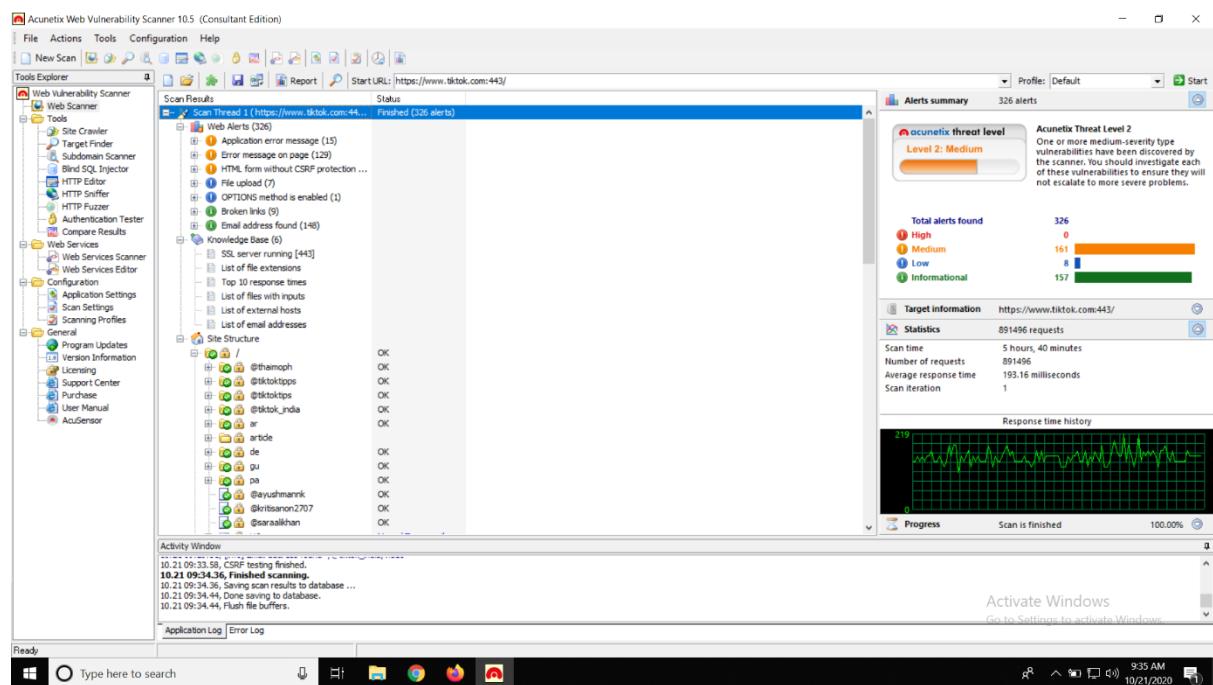
Netsparker scanning technology allows you to easily secure web applications without any issues, so you can concentrate on fixing the bugs that you have reported.



3. OWASP Acunetix

Acunetix is an automated web app security testing tool that tests for vulnerabilities including SQL injection, cross-site scripting, and other exploitable vulnerabilities for the auditing of your web application. Acunetix uses the HTTP / HTTPS protocol to search any websites or web applications that are accessible through a web browser.

A creative and compelling solution to analyze web applications, including JavaScript, AJAX & Web 2.0 off-the-shelf applications, off-the-shelf and custom applications. Acunetix has an advanced crawler who can locate virtually any file. This is critical because it is difficult to verify what is not found.

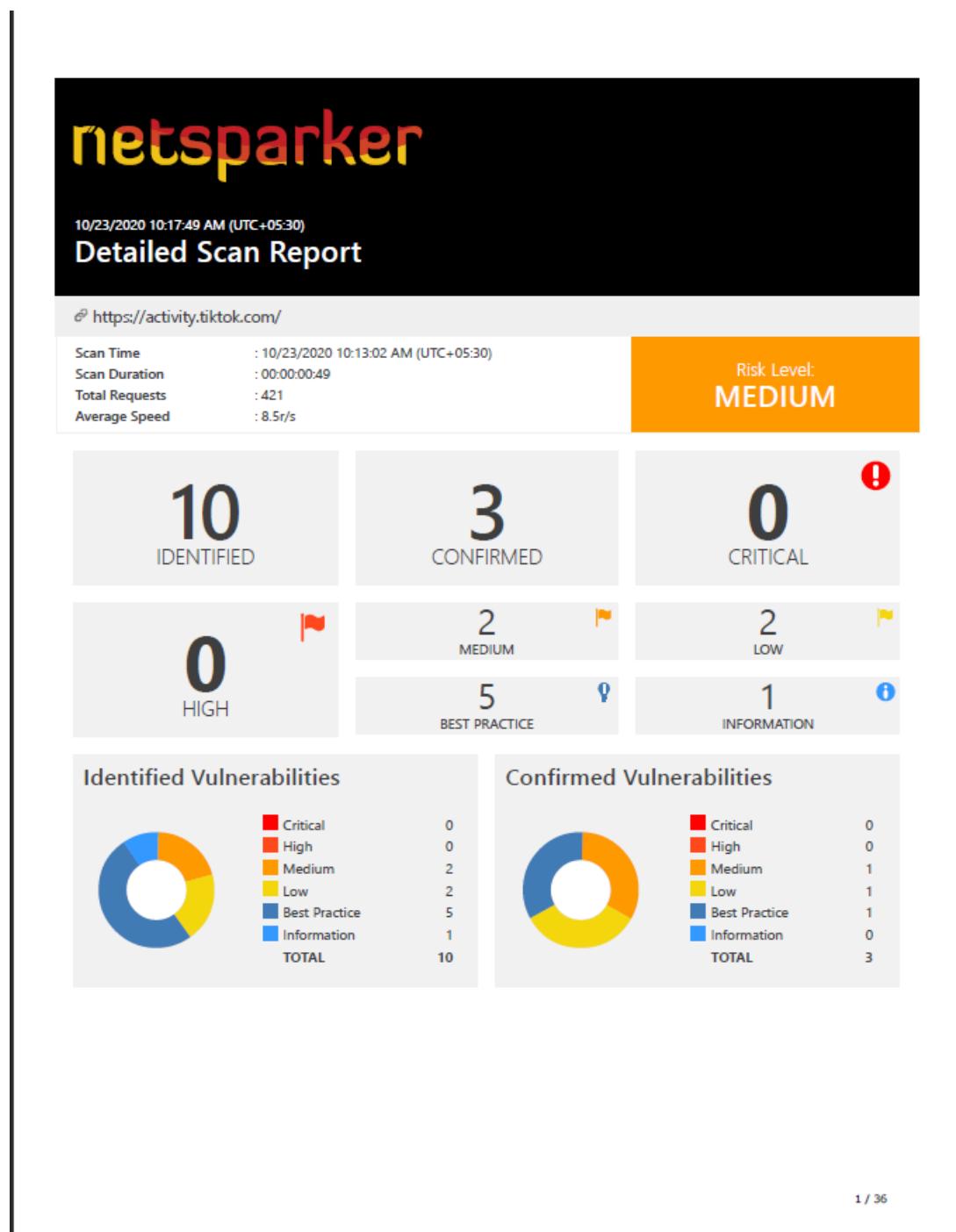


1.2.2. Scanning and generating reports

1. activity.tiktok.com

Netsparker Scanning

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domains.

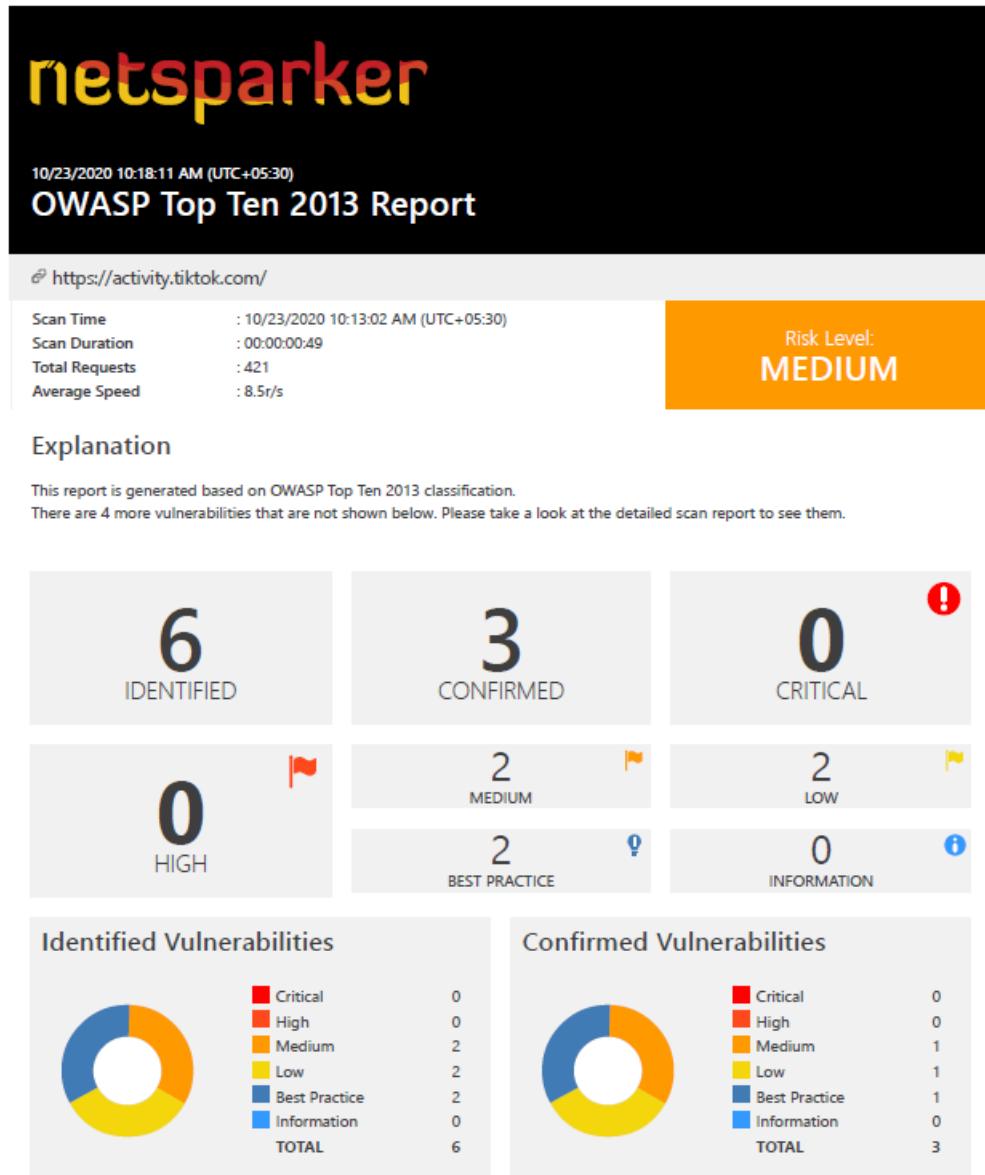


Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://activity.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://activity.tiktok.com/	
!	Missing X-Frame-Options Header	GET	https://activity.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://activity.tiktok.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://activity.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://activity.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://activity.tiktok.com/	
!	Referrer-Policy Not Implemented	GET	https://activity.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://activity.tiktok.com/	
!	Nginx Web Server Identified	GET	https://activity.tiktok.com/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.



Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://activity.tiktok.com/	MEDIUM
	Missing X-Frame-Options Header	GET	https://activity.tiktok.com/	LOW
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://activity.tiktok.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://activity.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://activity.tiktok.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://activity.tiktok.com/	BEST PRACTICE

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. The title bar indicates it's version v2020.9.2, licensed to Uncia. The main window is titled "3. Crawl and audit of activity.tiktok.com". The "Task details" tab is selected, showing the following information:

Scan type:	Crawl and audit
Scope:	activity.tiktok.com
Configuration:	Default configuration
Issues:	1 0 0 2
Requests:	589
Errors:	2
Unique locations:	2

A progress bar at the bottom of the task details section shows "Audit finished." Below this, there's a log pane with the following entries:

Time	Type	Task	Message
06:04:57 23 Oct 2020	Error	Task 10	[3] Crawl was configured to use a browser, but a browser could not be started.
06:04:54 23 Oct 2020	Info	Task 13	Audit started.

The "Audit items" tab is also visible, showing a table of results:

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://activity.tiktok.com	/robots.txt	Errors: request time...	0 0	0 0 0 0 0	0 0 0	0 0 0	352	2	4
2	http://activity.tiktok.com	/	Done	0 0	0 0 0 0 0	0 0 0	0 0 0	233		3

At the bottom of the screen, a terminal window is open on a Kali Linux system, showing the command "java -Xms1g -Xmx1g -jar burp.jar &". The status bar at the bottom of the desktop environment shows "Memory: 196.7MB" and "Disk: 16.0MB".

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity		Confidence			Total
		Certain	Firm	Tentative	
High		1	0	0	1
Medium		0	0	0	0
Low		0	0	0	0
Information		2	0	0	2

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

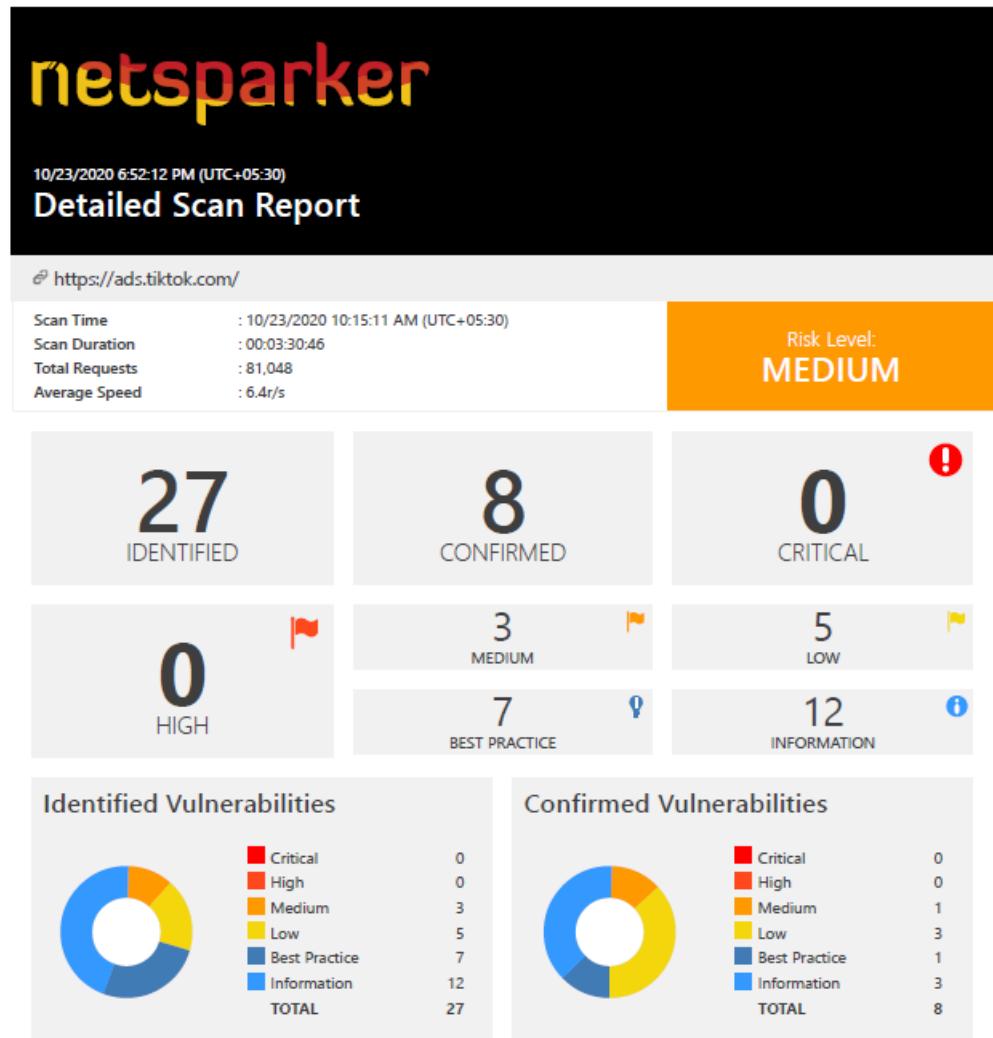
1. External service interaction (DNS)
2. HTML does not specify charset
3. TLS certificate

Vulnerabilities

1. External service interaction (DNS) - **High**
2. HTML does not specify charset - **Information**
3. TLS certificate - **Information**

2. ads.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

Vulnerability Summary

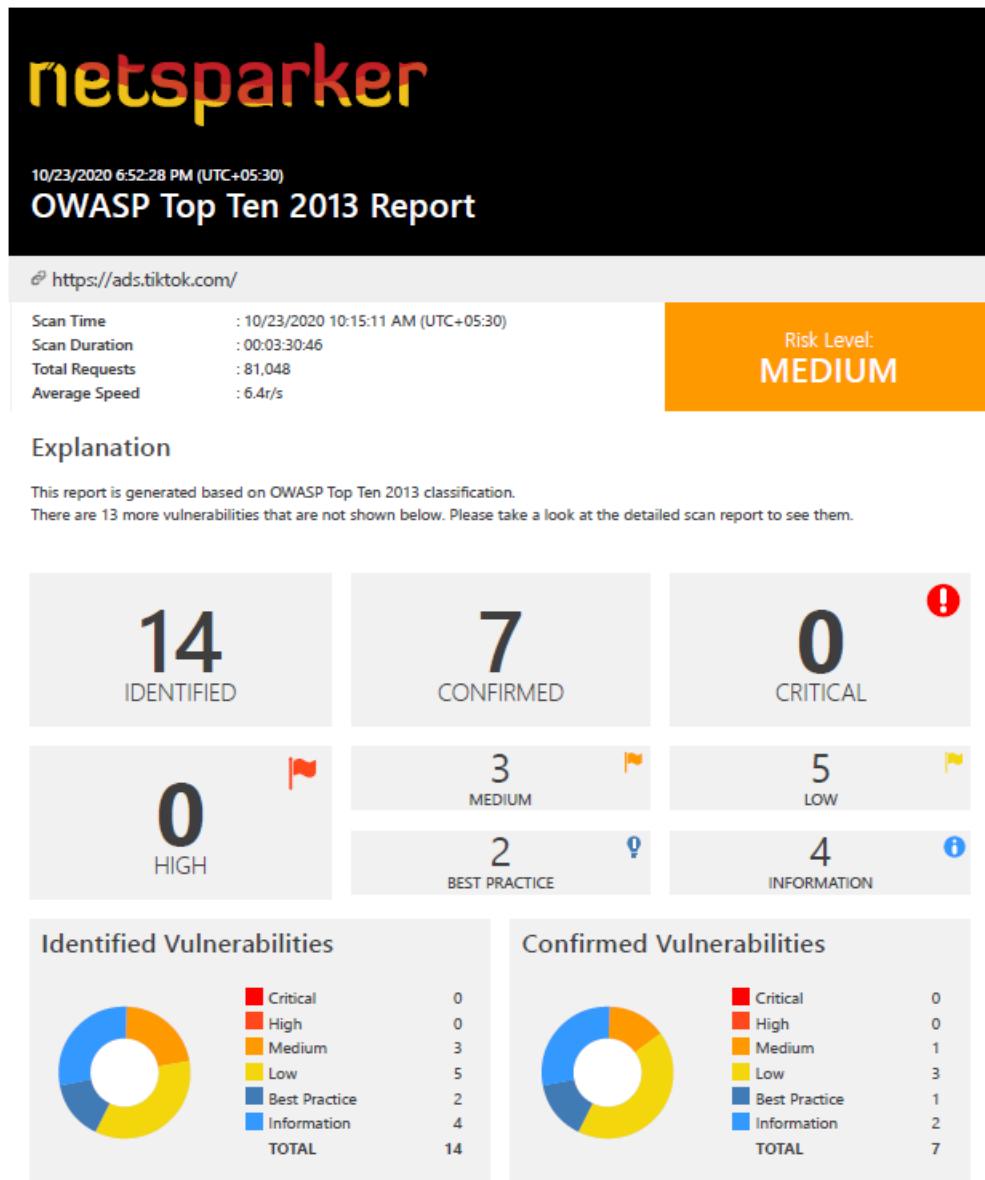
CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ads.tiktok.com/	
!	Out-of-date Version (jQuery)	GET	https://ads.tiktok.com/manager/	
!	Weak Ciphers Enabled	GET	https://ads.tiktok.com/	
!	[Possible] Phishing by Navigating Browser Tabs	GET	https://ads.tiktok.com/homepage/?%2F%2Fr87%3Fcom%2F%3F=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	%2F%2Fr87%3Fcom%2F%3F
!	Missing X-Frame-Options Header	GET	https://ads.tiktok.com/api/	
!	Cookie Not Marked as HttpOnly	GET	https://ads.tiktok.com/	
!	Cookie Not Marked as Secure	GET	https://ads.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://ads.tiktok.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://ads.tiktok.com/manager/	
!	Expect-CT Not Enabled	GET	https://ads.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://ads.tiktok.com/api/	
!	Referrer-Policy Not Implemented	GET	https://ads.tiktok.com/api/	
!	SameSite Cookie Not Implemented	GET	https://ads.tiktok.com/	
!	Subresource Integrity (SRI) Not Implemented	GET	https://ads.tiktok.com/manager/	

2 / 99

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://ads.tiktok.com/	
!	[Possible] Internal Path Disclosure (Windows)	GET	https://ads.tiktok.com/help/?nsextt=%2522%252bnetsparker(0x027706)%252b%2522	nsextt
!	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://ads.tiktok.com/i18n/	
!	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://ads.tiktok.com/i18n/	
!	data: Used in a Content Security Policy (CSP) Directive	GET	https://ads.tiktok.com/i18n/	
!	default-src Used in Content Security Policy (CSP)	GET	https://ads.tiktok.com/i18n/	
!	Missing object-src in CSP Declaration	GET	https://ads.tiktok.com/i18n/	
!	Nginx Web Server Identified	GET	https://ads.tiktok.com/	
!	Out-of-date Version (Vue.js)	GET	https://ads.tiktok.com/manager/	
!	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://ads.tiktok.com/i18n/	
!	Cross-site Referrer Leakage through Referrer-Policy	GET	https://ads.tiktok.com/manager/	
!	Forbidden Resource	POST	https://ads.tiktok.com/	
!	OPTIONS Method Enabled	OPTIONS	https://ads.tiktok.com/manager/	

3 / 99

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.



1 / 49

Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ads.tiktok.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	https://ads.tiktok.com/	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://ads.tiktok.com/homepage/?%2F%2Fr87%3Fcom%2F%3F=%27%20WAITFOR%20DELAY%20%27%3a0%3a25%27--	LOW
	Missing X-Frame-Options Header	GET	https://ads.tiktok.com/api/	LOW
	OPTIONS Method Enabled	OPTIONS	https://ads.tiktok.com/manager/	INFORMATION
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://ads.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://ads.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://ads.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://ads.tiktok.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://ads.tiktok.com/api/	BEST PRACTICE
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://ads.tiktok.com/manager/	INFORMATION
	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://ads.tiktok.com/i18n/	INFORMATION
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES				
2 / 49				

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
	Out-of-date Version (jQuery)	GET	https://ads.tiktok.com/manager/	MEDIUM
	Out-of-date Version (Vue.js)	GET	https://ads.tiktok.com/manager/	INFORMATION

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurp ▾ Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia". Below the title bar, the menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The main navigation bar has tabs for "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". The current tab is "Proxy". A sub-menu bar for the "Proxy" tab shows "4. Crawl and audit of ads.tiktok.com". Below the sub-menu, there are tabs for "Details", "Audit items", "Issue activity", and "Event log".

Task details

Scan type: Crawl and audit
Scope: ads.tiktok.com
Configuration: Default configuration
Issues: 10 (with 10 icons)
Requests: 2,273
Errors: 2
Unique locations: 1

A progress bar at the bottom indicates the audit is finished.

Event Log

Date	Time	Level	Task	Message
06-04-57	23 Oct 2020	Error	Task 10	[3] Crawl was configured to use a browser, but a browser could not be started.
06-04-54	23 Oct 2020	Info	Task 13	Audit started.

Results

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://ads.tiktok.com	/	Errors: request time...	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	574	2	5
2	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	432	3	3
3	https://ads.tiktok.com	/robots.txt	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	334	4	4
4	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	713	5	5
5	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	213	3	3

Event Log

Date	Time	Level	Task	Message
06-04-57	23 Oct 2020	Error	Task 10	[3] Crawl was configured to use a browser, but a browser could not be started.
06-04-54	23 Oct 2020	Info	Task 13	Audit started.

Results

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://ads.tiktok.com	/	Errors: request time...	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	574	2	5
2	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	432	3	3
3	https://ads.tiktok.com	/robots.txt	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	334	4	4
4	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	713	5	5
5	http://ads.tiktok.com	/	Done	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	213	3	3

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	1	0	0	1
	Medium	0	0	0	0
	Low	0	0	0	0
	Information	9	1	0	10

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

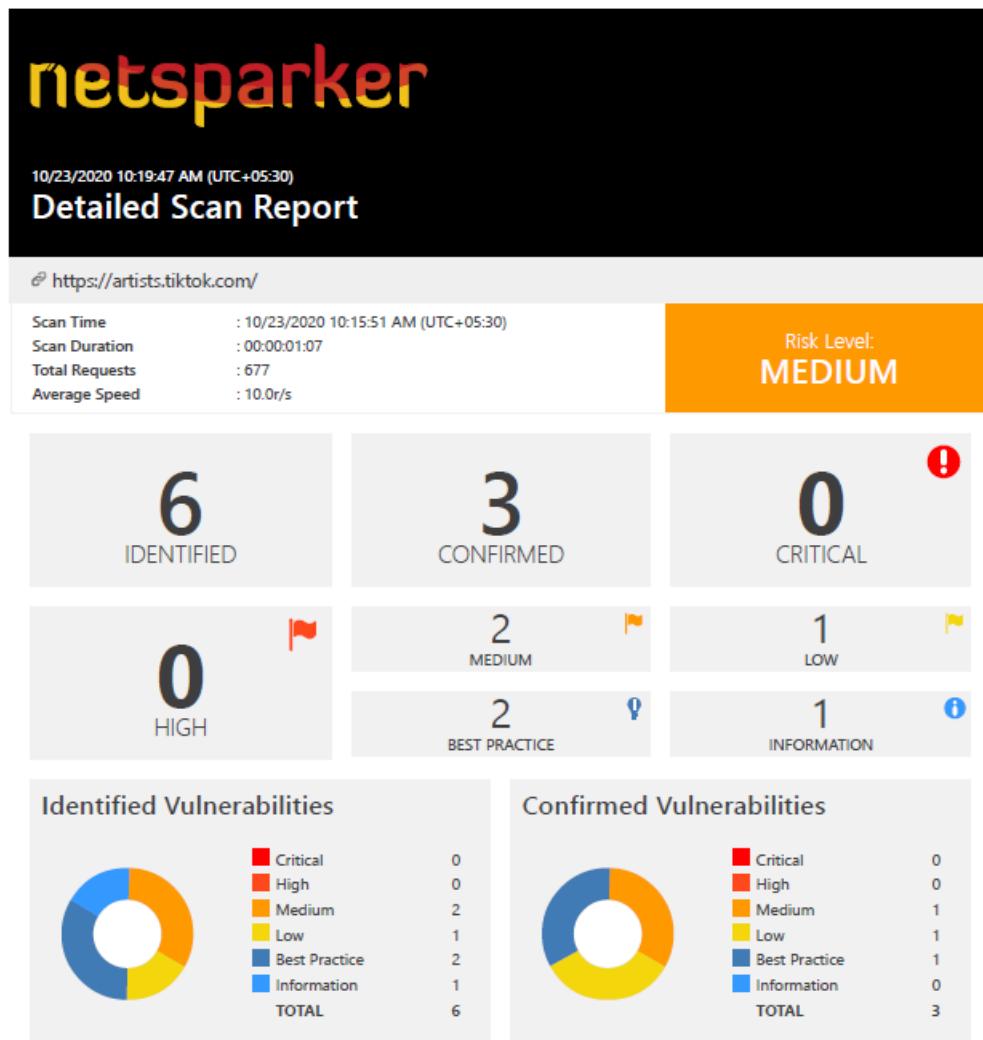
1. External service interaction (DNS)
2. Input returned in response (reflected)
 - 2.1. <http://ads.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - 2.2. <http://ads.tiktok.com/homepage/> [name of an arbitrarily supplied URL parameter]
 - 2.3. <https://ads.tiktok.com/homepage/> [name of an arbitrarily supplied URL parameter]
3. TLS cookie without secure flag set
4. Cookie scoped to parent domain
 - 4.1. <http://ads.tiktok.com/>
 - 4.2. <https://ads.tiktok.com/robots.txt>
5. Cookie without HttpOnly flag set
 - 5.1. <http://ads.tiktok.com/>
 - 5.2. <https://ads.tiktok.com/robots.txt>
6. Frameable response (potential Clickjacking)
7. TLS certificate

Vulnerabilities

1. External service interaction (DNS) - **High**
2. Input returned in response (reflected) - **Information**
 - http://ads.tiktok.com/ [name of an arbitrarily supplied URL parameter]
 - http://ads.tiktok.com/homepage/ [name of an arbitrarily supplied URL parameter]
 - https://ads.tiktok.com/homepage/ [name of an arbitrarily supplied URL parameter]
3. TLS cookie without secure flag set - **Information**
4. Cookie scoped to parent domain - **Information**
 - http://ads.tiktok.com/
 - https://ads.tiktok.com/robots.txt
5. Cookie without HttpOnly flag set - **Information**
 - http://ads.tiktok.com/
 - https://ads.tiktok.com/robots.txt
6. Frameable response (potential Clickjacking) - **Information**
7. TLS certificate - **Information**

3. artists.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domains.

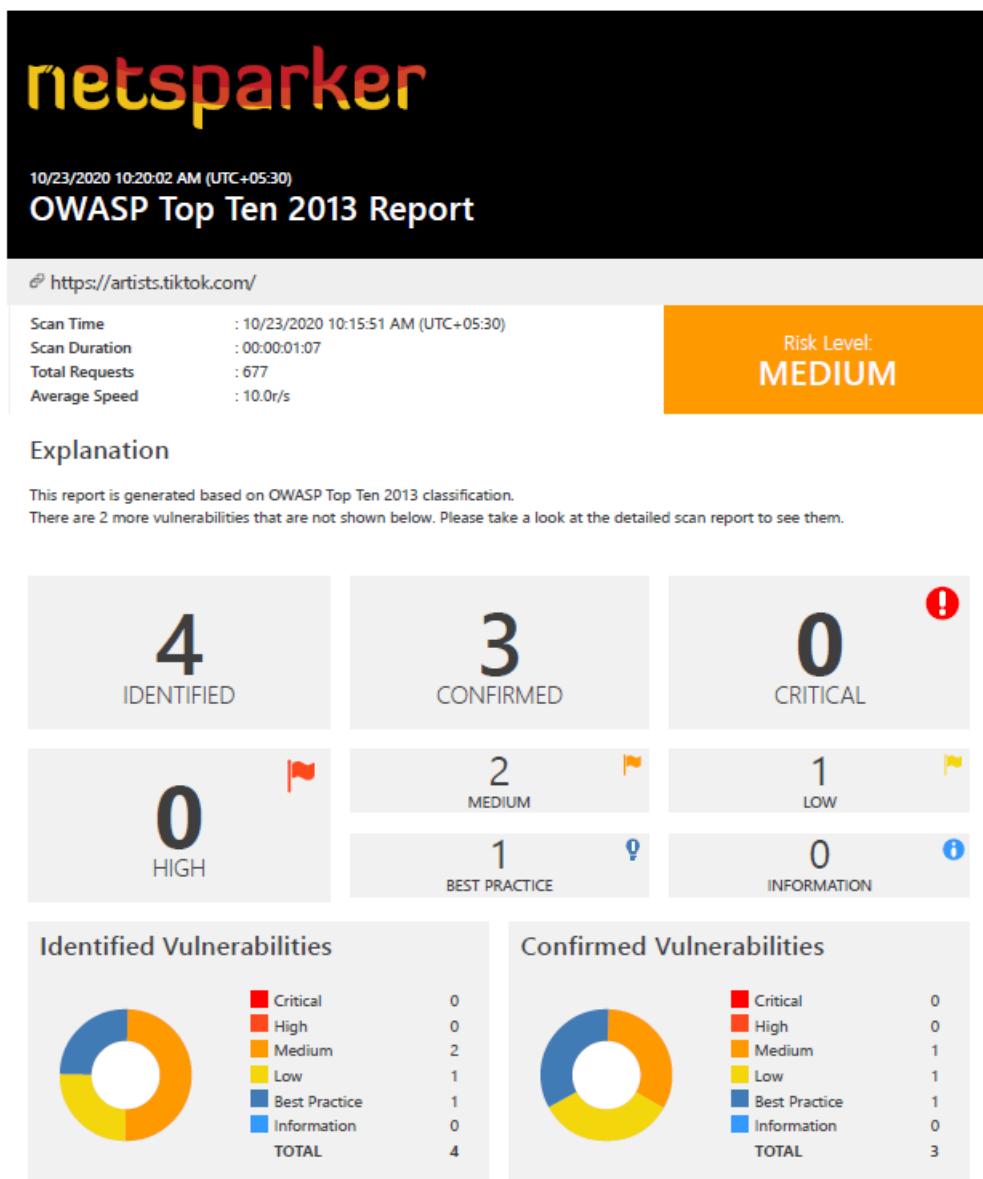


Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://artists.tiktok.com/	
	Weak Ciphers Enabled	GET	https://artists.tiktok.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://artists.tiktok.com/	
	Expect-CT Not Enabled	GET	https://artists.tiktok.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://artists.tiktok.com/	
	Nginx Web Server Identified	GET	https://artists.tiktok.com/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

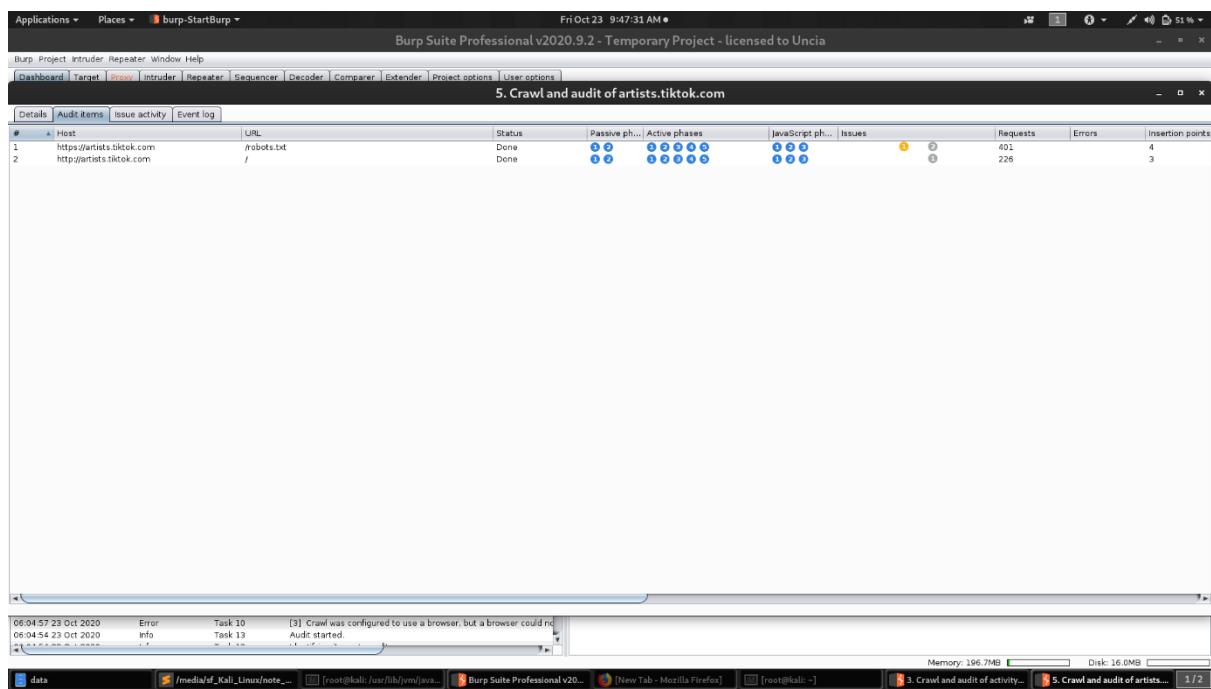
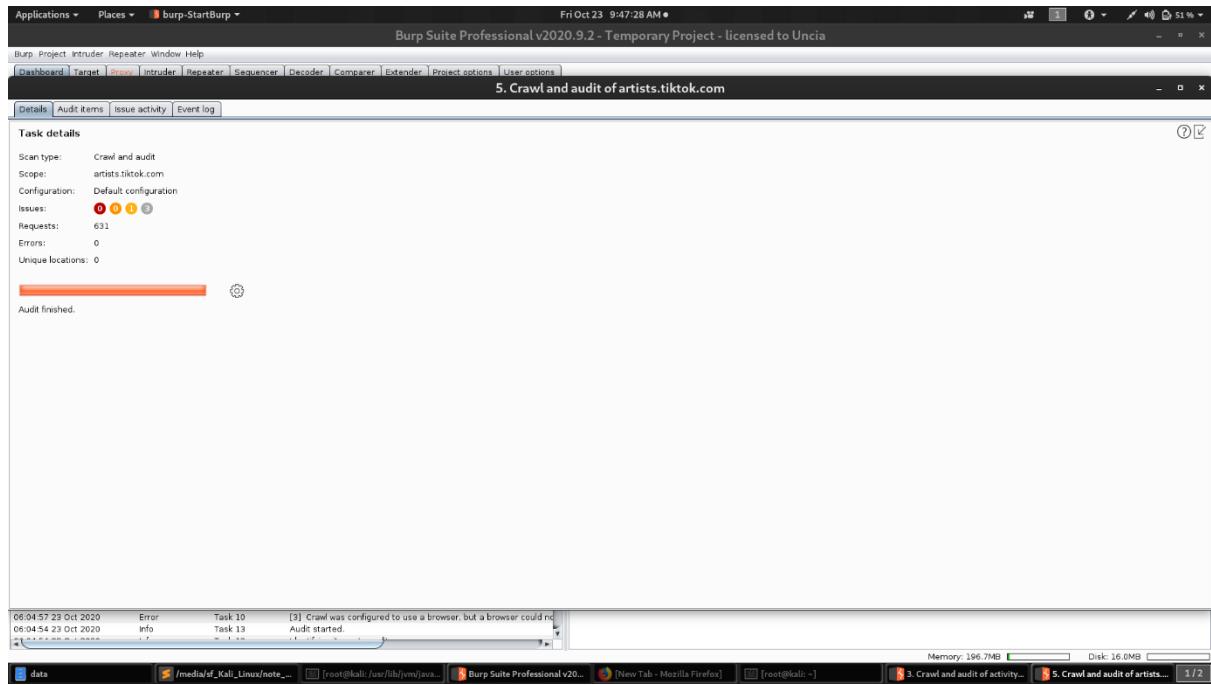


Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://artists.tiktok.com/	MEDIUM
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://artists.tiktok.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://artists.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://artists.tiktok.com/	BEST PRACTICE

Burp Suite Scanning



Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity		Confidence			Total
		Certain	Firm	Tentative	
High		0	0	0	0
Medium		0	0	0	0
Low		1	0	0	1
Information		3	0	0	3

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

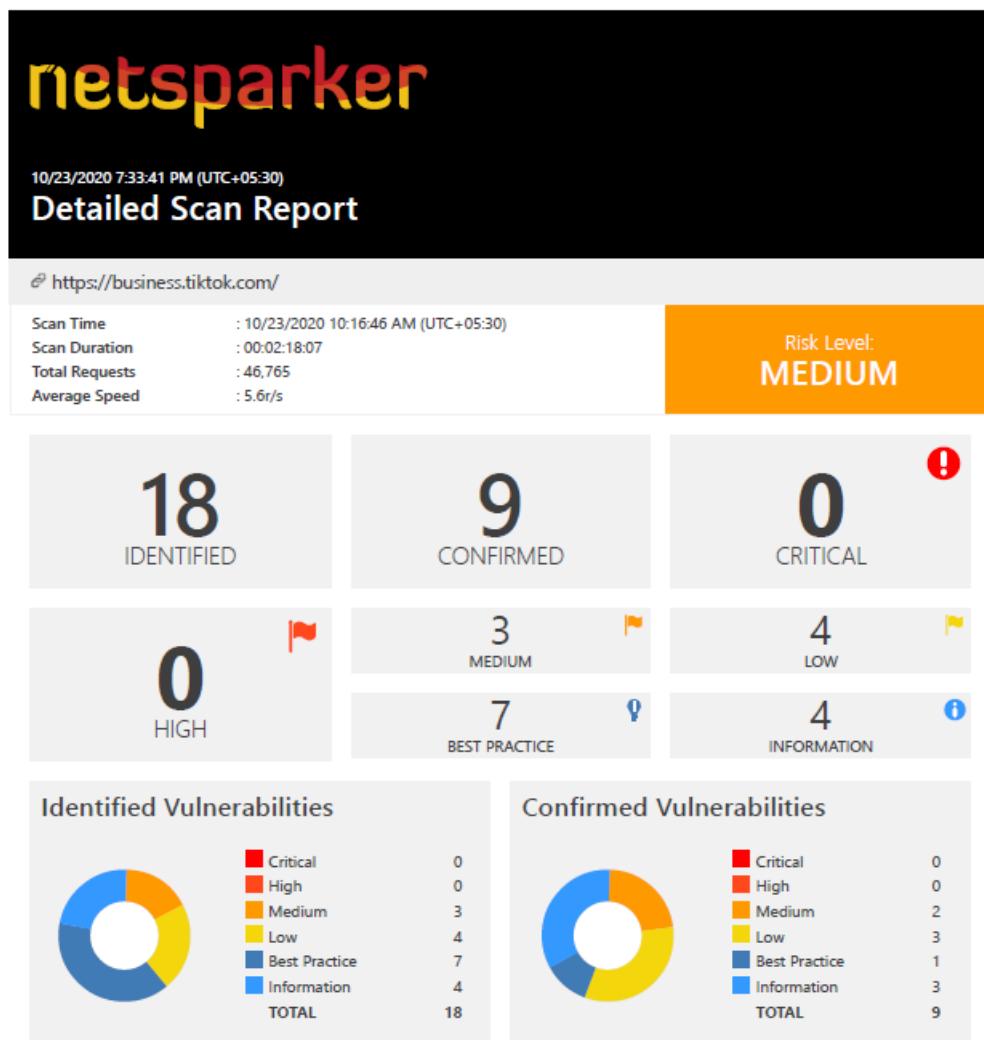
1. Strict transport security not enforced
2. Input returned in response (reflected)
 - 2.1. <http://artists.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - 2.2. <https://artists.tiktok.com/robots.txt> [name of an arbitrarily supplied URL parameter]
3. TLS certificate

Vulnerabilities

1. Strict transport security not enforced – **Low**
2. Input returned in response (reflected) – **Information**
 - <http://artists.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - <https://artists.tiktok.com/robots.txt> [name of an arbitrarily supplied URL parameter]
3. TLS certificate – **Information**

4. business.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domains.



Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://business.tiktok.com/	
!	Active Mixed Content over HTTPS	GET	https://business.tiktok.com/31ecd969.bbc4add9.js	
!	Weak Ciphers Enabled	GET	https://business.tiktok.com/	
!	Missing X-Frame-Options Header	GET	https://business.tiktok.com/api/attrib/trace/logging/	
!	Cookie Not Marked as HttpOnly	GET	https://business.tiktok.com/api/v1/bm/user/	
!	Cookie Not Marked as Secure	GET	https://business.tiktok.com/api/v1/bm/user/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://business.tiktok.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://business.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://business.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://business.tiktok.com/	
!	Referrer-Policy Not Implemented	GET	https://business.tiktok.com/api/attrib/trace/logging/	
!	SameSite Cookie Not Implemented	GET	https://business.tiktok.com/api/v1/bm/user/	
!	Subresource Integrity (SRI) Not Implemented	GET	https://business.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://business.tiktok.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	Nginx Web Server Identified	GET	https://business.tiktok.com/	
!	Cross-site Referrer Leakage through Referrer-Policy	GET	https://business.tiktok.com/	
!	Forbidden Resource	POST	https://business.tiktok.com/api/v1/bm/user/	
!	OPTIONS Method Enabled	OPTIONS	https://business.tiktok.com/api/attrib/trace/logging/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

netsparker

10/23/2020 7:33:58 PM (UTC+05:30)
OWASP Top Ten 2013 Report

🔗 <https://business.tiktok.com/>

Scan Time	: 10/23/2020 10:16:46 AM (UTC+05:30)
Scan Duration	: 00:02:18.07
Total Requests	: 46,765
Average Speed	: 5.6/r/s

Risk Level: **MEDIUM**

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 7 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

11 IDENTIFIED	8 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	4 LOW
	2 BEST PRACTICE	2 INFORMATION

Identified Vulnerabilities

Vulnerability Type	Count
Critical	0
High	0
Medium	3
Low	4
Best Practice	2
Information	2
TOTAL	11

Confirmed Vulnerabilities

Vulnerability Type	Count
Critical	0
High	0
Medium	2
Low	3
Best Practice	1
Information	2
TOTAL	8

Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	Cookie Not Marked as HttpOnly	GET	https://business.tiktok.com/api/v1/bm/user/	LOW
	Missing X-Frame-Options Header	GET	https://business.tiktok.com/api/attrib/trace/logging/	LOW
	OPTIONS Method Enabled	OPTIONS	https://business.tiktok.com/api/attrib/trace/logging/	INFORMATION
A6 - SENSITIVE DATA EXPOSURE				
	Active Mixed Content over HTTPS	GET	https://business.tiktok.com/31ecd969.bbc4add9.js	MEDIUM
	Weak Ciphers Enabled	GET	https://business.tiktok.com/	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://business.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://business.tiktok.com/api/v1/bm/user/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://business.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://business.tiktok.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://business.tiktok.com/api/attrib/trace/logging/	BEST PRACTICE
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://business.tiktok.com/	INFORMATION

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurp ▾" and "Fri Oct 23 9:48:29 AM". The main window title is "6. Crawl and audit of business.tiktok.com". The "Task details" tab is selected, displaying the following information:

- Scan type: Crawl and audit
- Scope: business.tiktok.com
- Configuration: Default configuration
- Issues: 657 (with three red circular icons)
- Requests: 657
- Errors: 2
- Unique locations: 2

A progress bar at the bottom of the task details panel indicates "Audit finished." Below this, a log viewer shows two entries:

```
06:04:57 23 Oct 2020 Error Task 10 [8] Crawl was configured to use a browser, but a browser could not be found.
06:04:54 23 Oct 2020 Info Task 13 Audit started.
```

At the very bottom of the screen, there is a terminal window with several tabs open, including "Burp Suite Professional v20...", "Mozilla Firefox", and "root@kali:~". The terminal shows the command "ls" and its output, which includes "data", "media", and "3. Crawl and audit of activity...".

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurp ▾" and "Fri Oct 23 9:48:31 AM". The main window title is "6. Crawl and audit of business.tiktok.com". The "Audit items" tab is selected, displaying a table of audit results:

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://business.tiktok.com	/robots.txt	Errors: request time...	● ●	● ● ● ● ●	● ● ●	● ○	434	2	4
2	http://business.tiktok.com	/	Done	● ●	● ● ● ● ●	● ● ●	● ○	219		3

Below the audit items table, a log viewer shows the same two entries as the previous screenshot:

```
06:04:57 23 Oct 2020 Error Task 10 [8] Crawl was configured to use a browser, but a browser could not be found.
06:04:54 23 Oct 2020 Info Task 13 Audit started.
```

At the very bottom of the screen, there is a terminal window with several tabs open, including "Burp Suite Professional v20...", "Mozilla Firefox", and "root@kali:~". The terminal shows the command "ls" and its output, which includes "data", "media", and "3. Crawl and audit of activity...".

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	1	0	0	1
	Medium	0	0	0	0
	Low	1	0	0	1
	Information	7	1	0	8

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

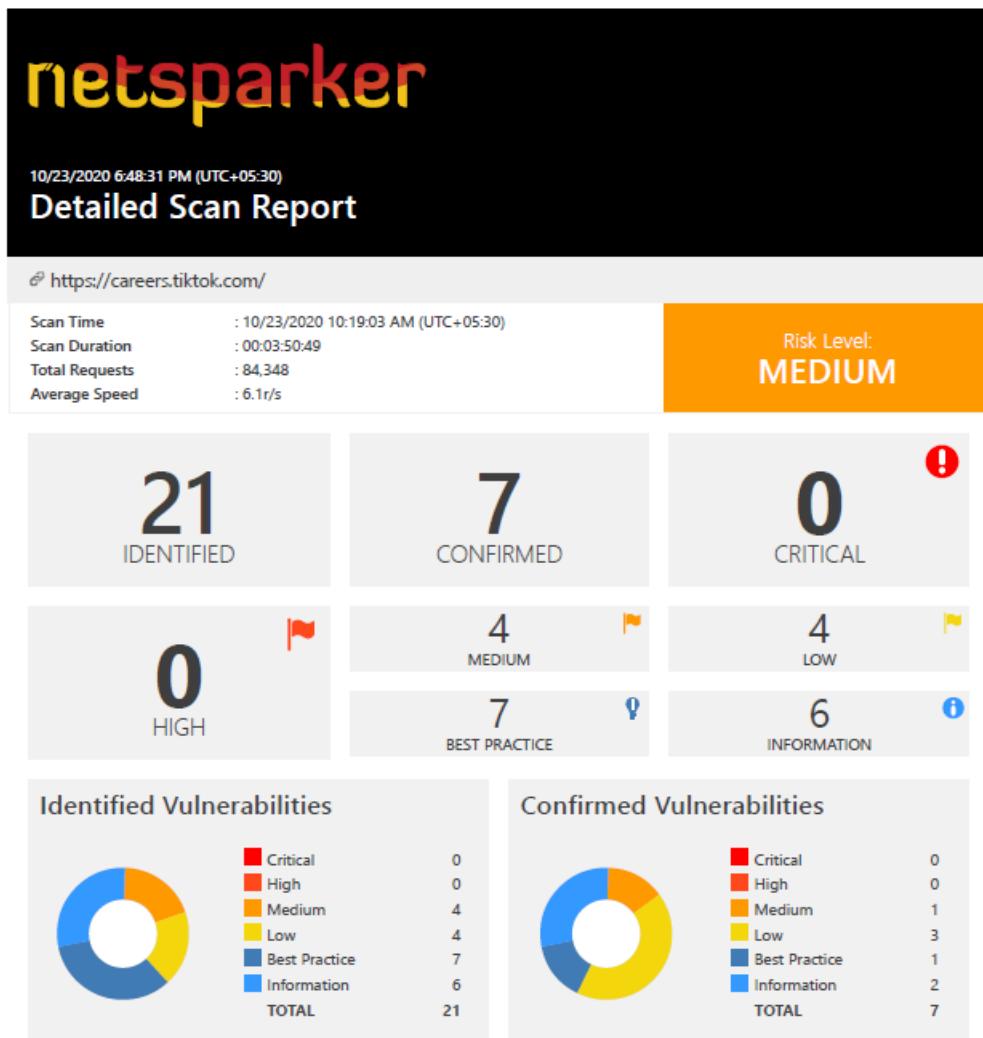
1. External service interaction (DNS)
 2. Strict transport security not enforced
 3. Cross-domain script include
 4. DOM data manipulation (DOM-based)
 5. Backup file
 - 5.1. <https://business.tiktok.com/robots.exe>
 - 5.2. <https://business.tiktok.com/robots.jar>
 - 5.3. <https://business.tiktok.com/robots.txt.zip>
 - 5.4. <https://business.tiktok.com/robots.zip>
 6. Cacheable HTTPS response
 7. TLS certificate
-

Vulnerabilities

1. External service interaction (DNS) – **High**
2. Strict transport security not enforced – **Low**
3. Cross-domain script include – **Information**
4. DOM data manipulation (DOM-based) – **Information**
5. Backup file – **Information**
 - <https://business.tiktok.com/robots.exe>
 - <https://business.tiktok.com/robots.jar>
 - <https://business.tiktok.com/robots.txt.zip>
 - <https://business.tiktok.com/robots.zip>
6. Cacheable HTTPS response – **Information**
7. TLS certificate – **Information**

5. [careers.tiktok.com](#)

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domains.



Vulnerability Summary for subdomain

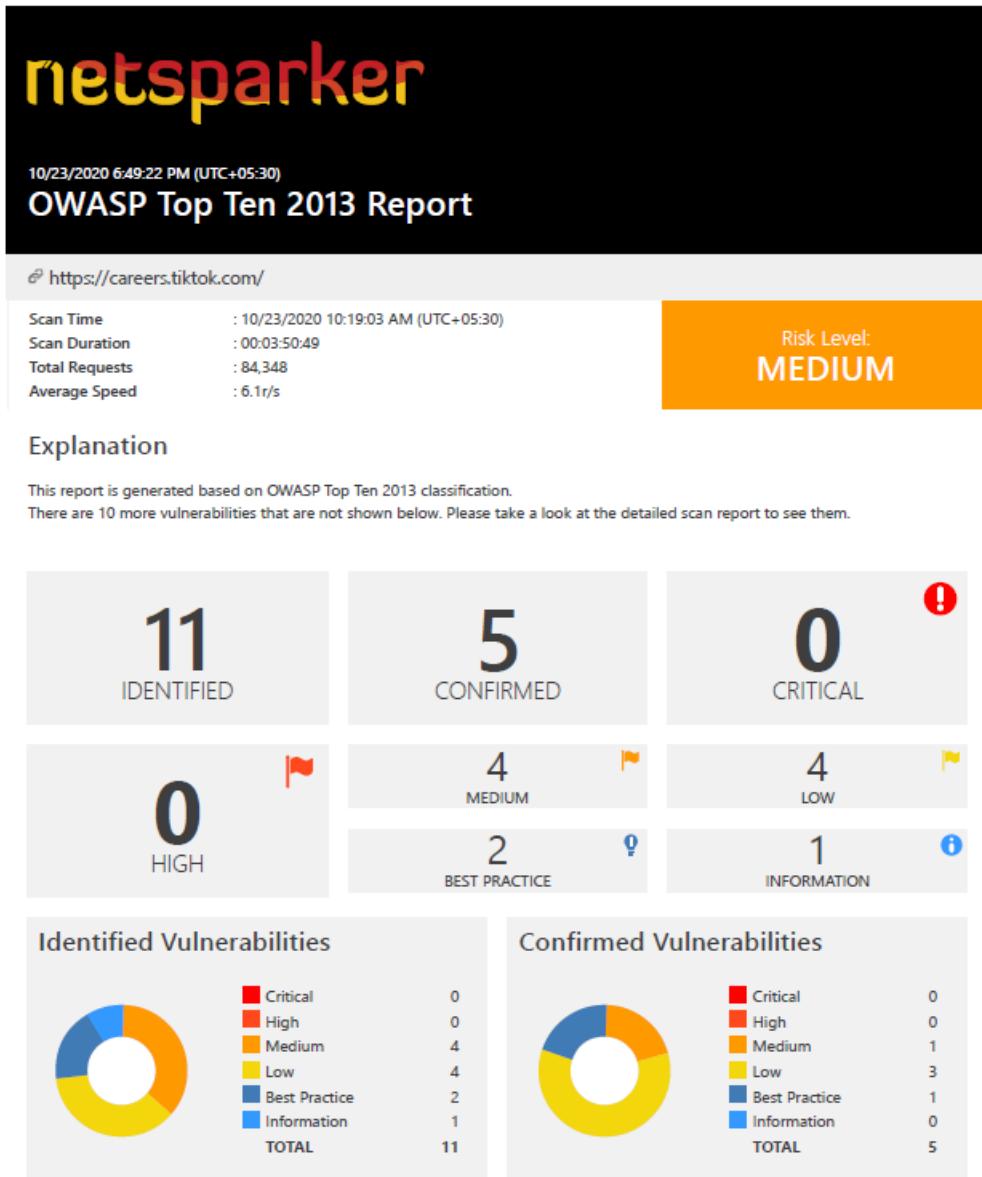
Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=%27%3e%3cnet%20spark%3dnetsparker(0x002CEA)%3e&pageSize=10	currentPage
!	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=1&pageSize=%27%3e%3cnet%20spark%3dnetsparker(0x031F1)%3e	pageSize
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://careers.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://careers.tiktok.com/	
!	Missing X-Frame-Options Header	GET	https://careers.tiktok.com/position/detail/6859833971854821646	
!	Cookie Not Marked as HttpOnly	GET	https://careers.tiktok.com/position	
!	Cookie Not Marked as Secure	POST	https://careers.tiktok.com/api/v1/csrf/token	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://careers.tiktok.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://careers.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://careers.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://careers.tiktok.com/api/v1/search/job/posts	
!	Referrer-Policy Not Implemented	GET	https://careers.tiktok.com/position/detail/6859833971854821646	
!	SameSite Cookie Not Implemented	POST	https://careers.tiktok.com/api/v1/csrf/token	
!	Subresource Integrity (SRI) Not Implemented	GET	https://careers.tiktok.com/	

2 / 76

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://careers.tiktok.com/	
	[Possible] Login Page Identified	GET	https://careers.tiktok.com/position	
	Nginx Web Server Identified	GET	https://careers.tiktok.com/	
	Out-of-date Version (lodash)	GET	https://careers.tiktok.com/	
	Web Application Firewall Detected	GET	https://careers.tiktok.com/?ns=%3cscript%3ealert(0)%3c%2fscript%3e	
	Forbidden Resource	GET	https://careers.tiktok.com/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3CscRipt%3Enetspark(0x000184)%3C/scRipt%3E	
	Robots.txt Detected	GET	https://careers.tiktok.com/robots.txt	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

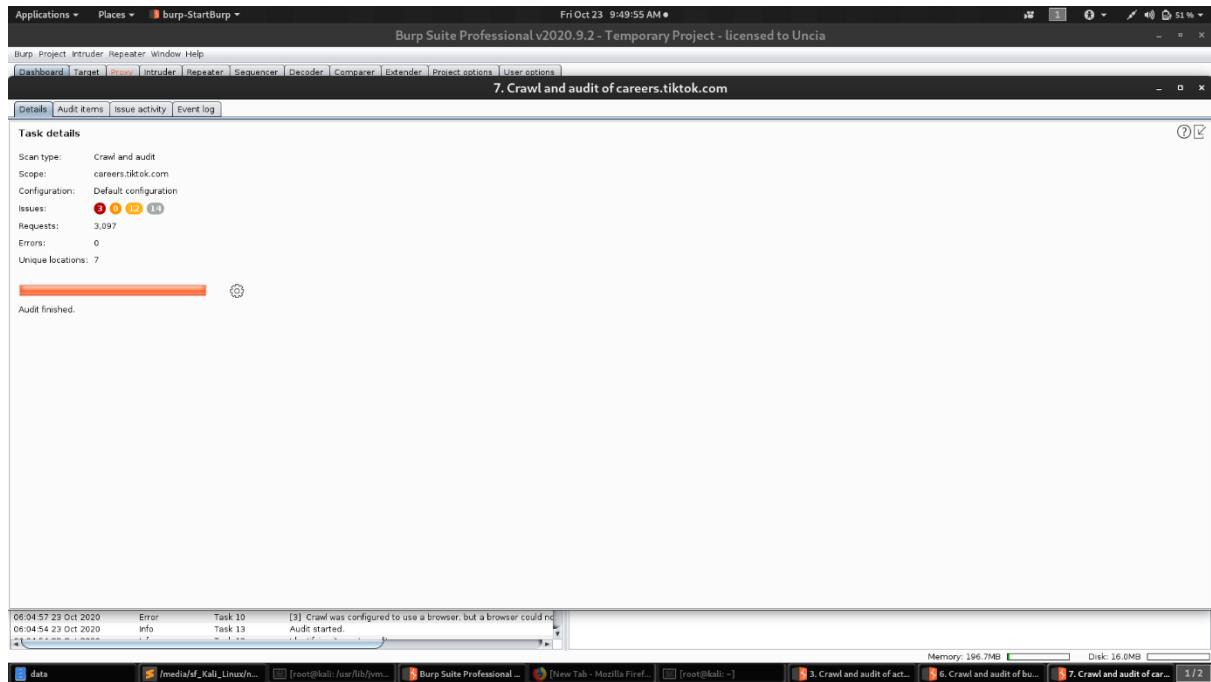


Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - CROSS-SITE SCRIPTING (XSS)				
	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=1&pageSize=%27%3e%3cnet%20sparker%3dnetspark(0x0031F1)%3e	MEDIUM
	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=%27%3e%3cnet%20sparker%3dnetspark(0x002CEA)%3e&pageSize=10	MEDIUM
A5 - SECURITY MISCONFIGURATION				
	Cookie Not Marked as HttpOnly	GET	https://careers.tiktok.com/position	LOW
	Missing X-Frame-Options Header	GET	https://careers.tiktok.com/position/detail/6859833971854821646	LOW
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://careers.tiktok.com/	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://careers.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	POST	https://careers.tiktok.com/api/v1/csrf/token	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://careers.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://careers.tiktok.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://careers.tiktok.com/position/detail/6859833971854821646	BEST PRACTICE
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES				
	Out-of-date Version (Lodash)	GET	https://careers.tiktok.com/	INFORMATION

Burp Suite Scanning



Task details

Scan type: Crawl and audit

Scope: careers.tiktok.com

Configuration: Default configuration

Issues: 0

Requests: 3,097

Errors: 0

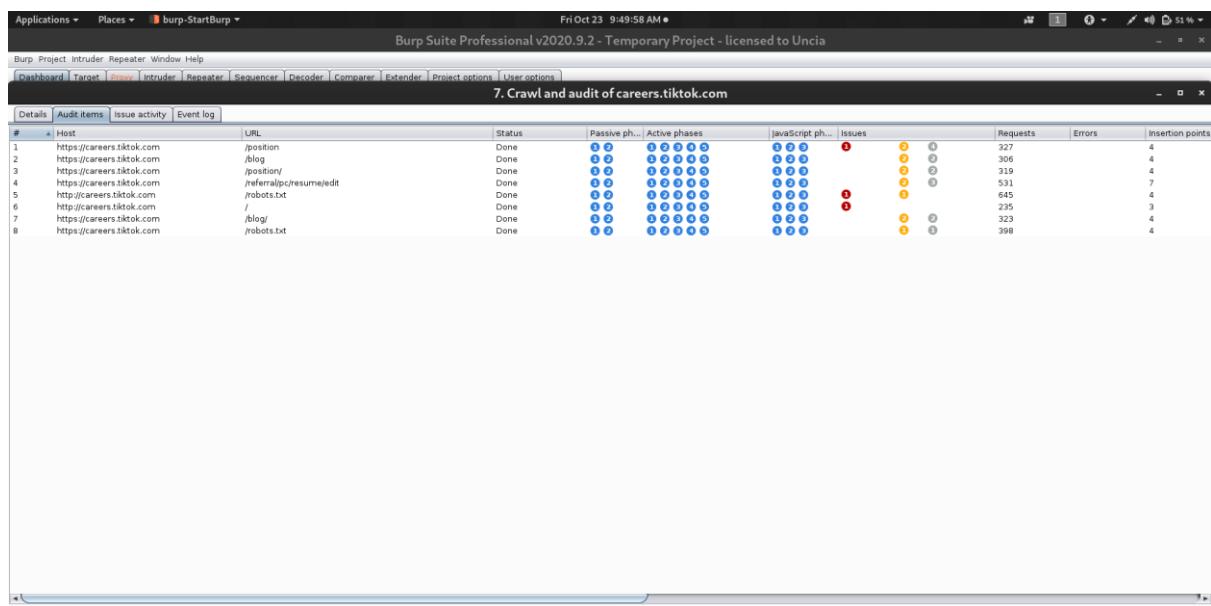
Unique locations: 7

Audit finished.

06:04:57 23 Oct 2020 Error Task 10 [3] Crawl was configured to use a browser, but a browser could not be started.

06:04:54 23 Oct 2020 Info Task 13 Audit started.

data /media/d/_Kali_Linux/n... root@kali:~# Burp Suite Professional - [New Tab - Mozilla Fire... -] [root@kali:~] 3. Crawl and audit of act... 6. Crawl and audit of bu... 7. Crawl and audit of ca... 1/2



#	Host	URL	Status	Passive ph...	Active phas...	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://careers.tiktok.com	/position	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	327	4	
2	https://careers.tiktok.com	/blog/	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	300	4	
3	https://careers.tiktok.com	/position/	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	319	4	
4	https://careers.tiktok.com	/referral/p/resume/edit	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	531	7	
5	http://careers.tiktok.com	/robots.txt	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	645	4	
6	http://careers.tiktok.com	/	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	235	3	
7	https://careers.tiktok.com	/blog/	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	323	4	
8	https://careers.tiktok.com	/robots.txt	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	0	398	4	

06:04:57 23 Oct 2020 Error Task 10 [3] Crawl was configured to use a browser, but a browser could not be started.

06:04:54 23 Oct 2020 Info Task 13 Audit started.

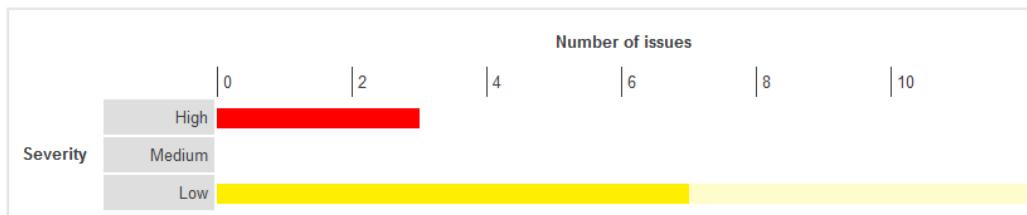
data /media/d/_Kali_Linux/n... root@kali:~# Burp Suite Professional - [New Tab - Mozilla Fire... -] [root@kali:~] 3. Crawl and audit of act... 6. Crawl and audit of bu... 7. Crawl and audit of ca... 1/2

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence				Total
	Certain	Firm	Tentative		
High	3	0	0		3
Medium	0	0	0		0
Low	7	0	5		12
Information	14	0	0		14

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. External service interaction (DNS)

- 1.1. <http://careers.tiktok.com/>
- 1.2. <http://careers.tiktok.com/robots.txt>
- 1.3. <https://careers.tiktok.com/position>

Contents

1. External service interaction (DNS)

- 1.1. <http://careers.tiktok.com/>
- 1.2. <http://careers.tiktok.com/robots.txt>
- 1.3. <https://careers.tiktok.com/position>

2. Open redirection (DOM-based)

- 2.1. <https://careers.tiktok.com/blog>
- 2.2. <https://careers.tiktok.com/blog/>
- 2.3. <https://careers.tiktok.com/position>
- 2.4. <https://careers.tiktok.com/position/>
- 2.5. <https://careers.tiktok.com/referral/pc/resume/edit>

3. Unencrypted communications

4. Strict transport security not enforced

- 4.1. <https://careers.tiktok.com/blog>
- 4.2. <https://careers.tiktok.com/blog/>
- 4.3. <https://careers.tiktok.com/position>
- 4.4. <https://careers.tiktok.com/position/>
- 4.5. <https://careers.tiktok.com/referral/pc/resume/edit>
- 4.6. <https://careers.tiktok.com/robots.txt>

5. Cross-domain script include

- 5.1. <https://careers.tiktok.com/blog>
- 5.2. <https://careers.tiktok.com/blog/>
- 5.3. <https://careers.tiktok.com/position>
- 5.4. <https://careers.tiktok.com/position/>
- 5.5. <https://careers.tiktok.com/referral/pc/resume/edit>

6. Backup file

7. Robots.txt file

8. Cacheable HTTPS response

- 8.1. <https://careers.tiktok.com/blog>
- 8.2. <https://careers.tiktok.com/blog/>
- 8.3. <https://careers.tiktok.com/position>
- 8.4. <https://careers.tiktok.com/position/>
- 8.5. <https://careers.tiktok.com/referral/pc/resume/edit>
- 8.6. <https://careers.tiktok.com/robots.txt>

9. TLS certificate

Vulnerabilities

1. External service interaction (DNS) – High

- <http://careers.tiktok.com/>
- <http://careers.tiktok.com/robots.txt>
- <https://careers.tiktok.com/position>

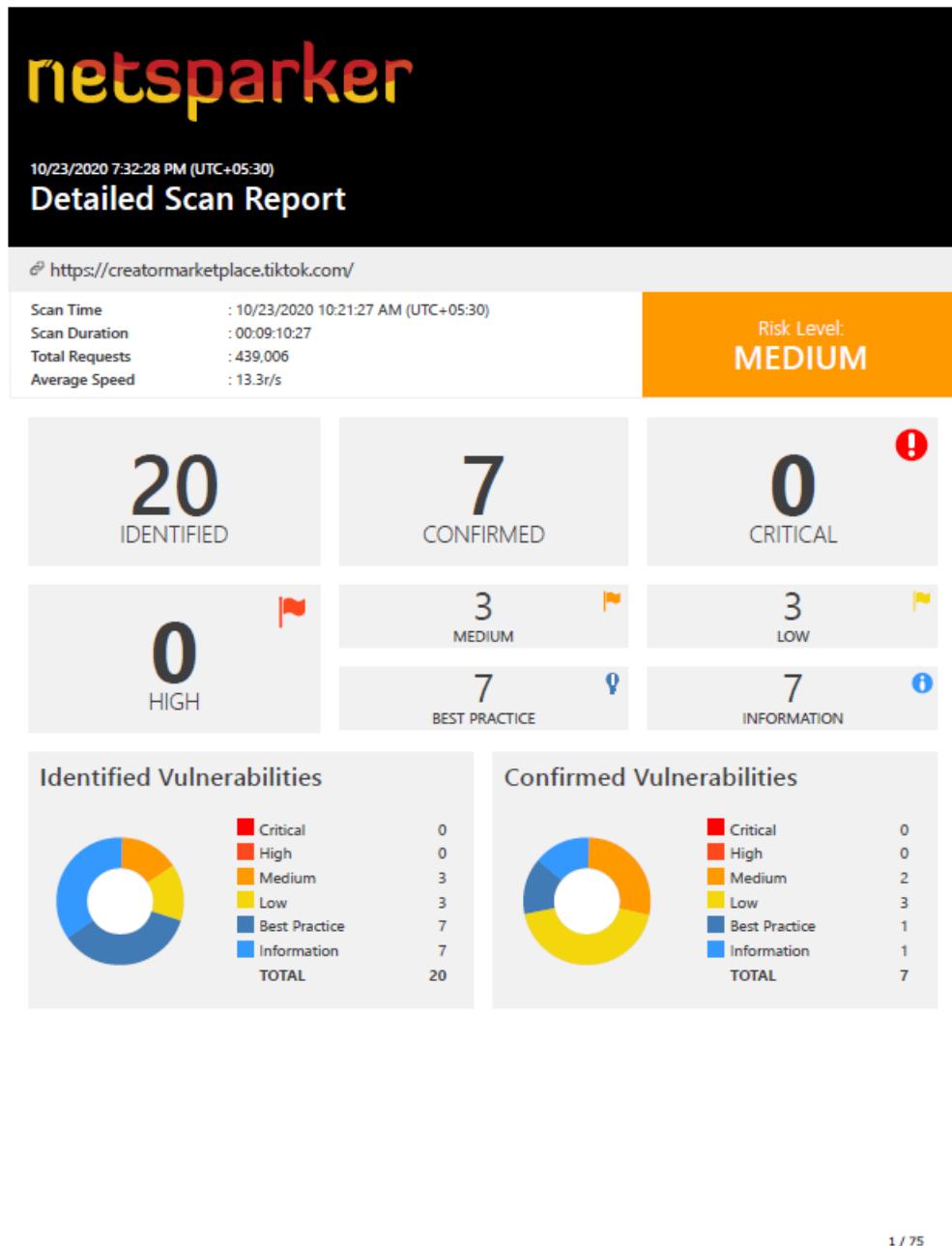
2. Open redirection (DOM-based) – Low

- <https://careers.tiktok.com/blog>
- <https://careers.tiktok.com/blog/>
- <https://careers.tiktok.com/position>
- <https://careers.tiktok.com/position/>

- <https://careers.tiktok.com/referral/pc/resume/edit>
3. Unencrypted communications – **Low**
 4. Strict transport security not enforced – **Low**
 - <https://careers.tiktok.com/blog>
 - <https://careers.tiktok.com/blog/>
 - <https://careers.tiktok.com/position>
 - <https://careers.tiktok.com/position/>
 - <https://careers.tiktok.com/referral/pc/resume/edit>
 - <https://careers.tiktok.com/robots.txt>
 5. Cross-domain script include – **Information**
 - <https://careers.tiktok.com/blog>
 - <https://careers.tiktok.com/blog/>
 - <https://careers.tiktok.com/position>
 - <https://careers.tiktok.com/position/>
 - <https://careers.tiktok.com/referral/pc/resume/edit>
 6. Backup file – **Information**
 7. Robots.txt file – **Information**
 8. Cacheable HTTPS response – **Information**
 - <https://careers.tiktok.com/blog>
 - <https://careers.tiktok.com/blog/>
 - <https://careers.tiktok.com/position>
 - <https://careers.tiktok.com/position/>
 - <https://careers.tiktok.com/referral/pc/resume/edit>
 - <https://careers.tiktok.com/robots.txt>
 9. TLS certificate – **Information**

6. [creatormarketplace.tiktok.com](#)

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://creatormarketplace.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (SSLv3)	GET	https://creatormarketplace.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://creatormarketplace.tiktok.com/	
!	Cookie Not Marked as HttpOnly	GET	https://creatormarketplace.tiktok.com/	
!	Cookie Not Marked as Secure	POST	https://creatormarketplace.tiktok.com/v/api/tool/metrics/tea/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://creatormarketplace.tiktok.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://creatormarketplace.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://creatormarketplace.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://creatormarketplace.tiktok.com/	
!	Referrer-Policy Not Implemented	GET	https://creatormarketplace.tiktok.com/	
!	SameSite Cookie Not Implemented	POST	https://creatormarketplace.tiktok.com/v/api/tool/metrics/tea/	
!	Subresource Integrity (SRI) Not Implemented	GET	https://creatormarketplace.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://creatormarketplace.tiktok.com/	
!	[Possible] Internal Path Disclosure (Windows)	GET	https://creatormarketplace.tiktok.com/v/api/advertiser/knowledge_search/?limit=10&page=1&query=%2F%2fr87.com%2fn%2fj%2F%3f0x08D176&total_count=3	query

2 / 75

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Email Address Disclosure	GET	https://creatormarketplace.tiktok.com/v/api/advertiser/protocol_detail/?protocol_id=20040911&protocol_type=1	
	Generic Email Address Disclosure	GET	https://creatormarketplace.tiktok.com/v/api/advertiser/protocol_detail/?protocol_id=20051101&protocol_type=1	
	Nginx Web Server Identified	GET	https://creatormarketplace.tiktok.com/	
	Out-of-date Version (Lodash)	GET	https://creatormarketplace.tiktok.com/help	
	Out-of-date Version (Vue.js)	GET	https://creatormarketplace.tiktok.com/	
	Forbidden Resource	POST	https://creatormarketplace.tiktok.com/v/api/tool/metrics/tea/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.



Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	Cookie Not Marked as HttpOnly	GET	https://creatormarketplace.tiktok.com/	LOW
A6 - SENSITIVE DATA EXPOSURE				
	Insecure Transportation Security Protocol Supported (SSLv3)	GET	https://creatormarketplace.tiktok.com/	MEDIUM
	Weak Ciphers Enabled	GET	https://creatormarketplace.tiktok.com/	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://creatormarketplace.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	POST	https://creatormarketplace.tiktok.com/v/api/tool/metrics/tea/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://creatormarketplace.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://creatormarketplace.tiktok.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://creatormarketplace.tiktok.com/	BEST PRACTICE
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES				
	Out-of-date Version (Lodash)	GET	https://creatormarketplace.tiktok.com/help	INFORMATION
	Out-of-date Version (Vue.js)	GET	https://creatormarketplace.tiktok.com/	INFORMATION

2 / 32

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurp ▾" and "Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia". The status bar at the bottom indicates "Fri Oct 23 9:51:23 AM".

The main window displays a "Task details" section for "8. Crawl and audit of creatormarketplace.tiktok.com". The "Scan type" is set to "Crawl and audit", the "Scope" is "creatormarketplace.tiktok.com", and the "Configuration" is "Default configuration". The "Issues" section shows 1 critical, 0 informational, and 7 low-severity issues. The "Audit progress" bar is nearly complete.

Below the task details is a "Logs" section showing audit logs from 06-04-57 to 06-04-54. The logs indicate "Task 10" was configured to use a browser but failed, and "Task 13" started.

The bottom of the window shows a tab bar with several tabs open, including "data", "/media/d/_Kali_Linux/n...", "root@kali: /usr/lib/... (New Tab - Mozilla Fire...)", "Burp Suite Professional - (New Tab - Mozilla Fire...)", "3. Crawl and audit of act...", "4. Crawl and audit of bu...", "5. Crawl and audit of cre...", and "8. Crawl and audit of cre...". The status bar at the bottom right shows "Memory: 196.7MB" and "Disk: 16.0MB".

This screenshot shows the same Burp Suite interface, but the main window now displays the "Audit items" table for the "8. Crawl and audit of creatormarketplace.tiktok.com" task. The table lists 6 URLs with their status, passive phases, active phases, JavaScript phases, and various metrics like Requests, Errors, and Insertion points.

#	Host	URL	Status	Passive ph...	Active phas...	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://creatormarketplace.tiktok.com	/register	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	552	6	6
2	https://creatormarketplace.tiktok.com	/login	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	471	6	6
3	https://creatormarketplace.tiktok.com	/protocol	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	471	6	6
4	https://creatormarketplace.tiktok.com	/contact	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	530	6	6
5	http://creatormarketplace.tiktok.com	/	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	248	3	3
6	https://creatormarketplace.tiktok.com	/robots.txt	Done	⊕ ⊕	⊕ ⊕ ⊕ ⊕ ⊕	⊕ ⊕ ⊕	1	384	4	4

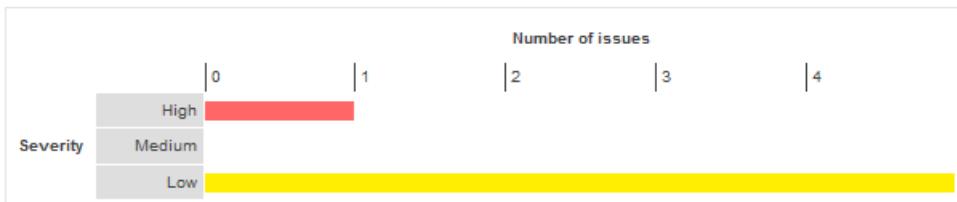
The bottom of the window shows the same tab bar and status bar as the previous screenshot.

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	1	0	1
	Medium	0	0	0	0
	Low	5	0	0	5
	Information	6	1	0	7

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. SQL injection

2. Strict transport security not enforced

- 2.1. <https://creatormarketplace.tiktok.com/contact>
- 2.2. <https://creatormarketplace.tiktok.com/login>
- 2.3. <https://creatormarketplace.tiktok.com/protocol>
- 2.4. <https://creatormarketplace.tiktok.com/register>
- 2.5. <https://creatormarketplace.tiktok.com/robots.txt>

3. Cross-domain script include

- 3.1. <https://creatormarketplace.tiktok.com/contact>
- 3.2. <https://creatormarketplace.tiktok.com/login>
- 3.3. <https://creatormarketplace.tiktok.com/protocol>
- 3.4. <https://creatormarketplace.tiktok.com/register>
- 3.5. <https://creatormarketplace.tiktok.com/robots.txt>

4. DOM data manipulation (DOM-based)

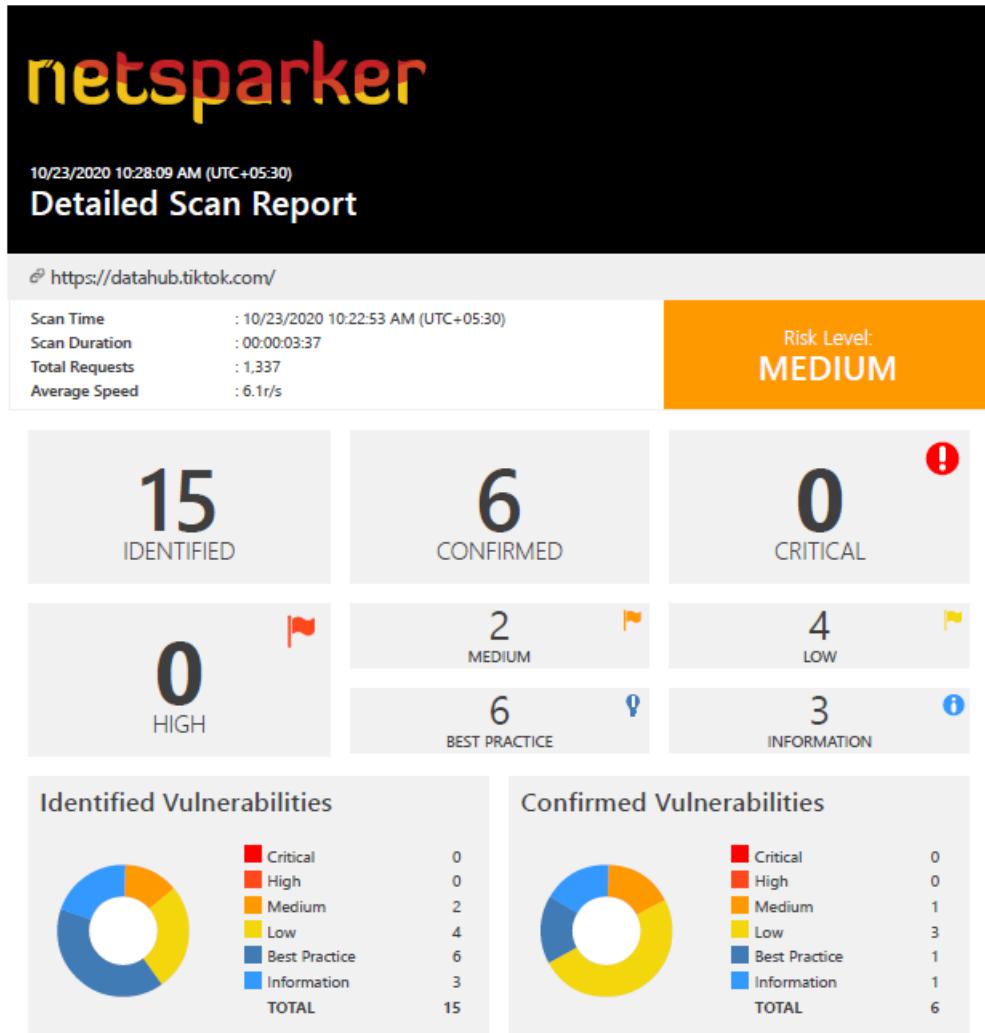
5. TLS certificate

Vulnerabilities

1. SQL injection – **High**
2. Strict transport security not enforced – **Low**
 - <https://creatormarketplace.tiktok.com/contact>
 - <https://creatormarketplace.tiktok.com/login>
 - <https://creatormarketplace.tiktok.com/protocol>
 - <https://creatormarketplace.tiktok.com/register>
 - <https://creatormarketplace.tiktok.com/robots.txt>
3. Cross-domain script include – **Information**
 - <https://creatormarketplace.tiktok.com/contact>
 - <https://creatormarketplace.tiktok.com/login>
 - <https://creatormarketplace.tiktok.com/protocol>
 - <https://creatormarketplace.tiktok.com/register>
 - <https://creatormarketplace.tiktok.com/robots.txt>
4. DOM data manipulation (DOM-based) – **Information**
5. TLS certificate – **Information**

7. [datahub.tiktok.com](#)

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
+	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://datahub.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://datahub.tiktok.com/	
+	Version Disclosure (Nginx)	GET	https://datahub.tiktok.com/	
!	Cookie Not Marked as HttpOnly	GET	https://datahub.tiktok.com/page/home	
!	Cookie Not Marked as Secure	GET	https://datahub.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://datahub.tiktok.com/	
+	Content Security Policy (CSP) Not Implemented	GET	https://datahub.tiktok.com/	
+	Expect-CT Not Enabled	GET	https://datahub.tiktok.com/	
+	Missing X-XSS-Protection Header	GET	https://datahub.tiktok.com/i18n_tdh/api/v1/user_account	
+	SameSite Cookie Not Implemented	GET	https://datahub.tiktok.com/	
+	Subresource Integrity (SRI) Not Implemented	GET	https://datahub.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://datahub.tiktok.com/	
+	Nginx Web Server Identified	GET	https://datahub.tiktok.com/	
+	Out-of-date Version (Nginx)	GET	https://datahub.tiktok.com/	
!	Forbidden Resource	POST	https://datahub.tiktok.com/	

2 / 55

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

netsparker

10/23/2020 10:29:03 AM (UTC+05:30)
OWASP Top Ten 2013 Report

🔗 <https://datahub.tiktok.com/>

Scan Time : 10/23/2020 10:22:53 AM (UTC+05:30)	Scan Duration : 00:00:03:37	Total Requests : 1,337	Average Speed : 6.1r/s	Risk Level: MEDIUM
--	-----------------------------	------------------------	------------------------	---------------------------

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 7 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

8 IDENTIFIED	5 CONFIRMED	0  CRITICAL
0  HIGH	2  MEDIUM	4  LOW
	1  BEST PRACTICE	1  INFORMATION

Identified Vulnerabilities



Critical	0
High	0
Medium	2
Low	4
Best Practice	1
Information	1
TOTAL	8

Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	3
Best Practice	1
Information	0
TOTAL	5

Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	Cookie Not Marked as HttpOnly	GET	https://datahub.tiktok.com/page/home	LOW
	Version Disclosure (Nginx)	GET	https://datahub.tiktok.com/	LOW
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://datahub.tiktok.com/	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://datahub.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://datahub.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://datahub.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://datahub.tiktok.com/	BEST PRACTICE
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES				
	Out-of-date Version (Nginx)	GET	https://datahub.tiktok.com/	INFORMATION

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurm" and "Fri Oct 23 9:52:29 AM". The main window title is "Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia". Below the title bar, the navigation bar includes "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". The current tab is "Proxy". A sub-header "9. Crawl and audit of datahub.tiktok.com" is displayed. The main content area has tabs: "Details", "Audit items", "Issue activity", and "Event log". The "Details" tab is selected, showing the following information:

Scan type:	Crawl and audit
Scope:	datahub.tiktok.com
Configuration:	Default configuration
Issues:	2
Requests:	7,341
Errors:	2
Unique locations:	4
Audit finished.	

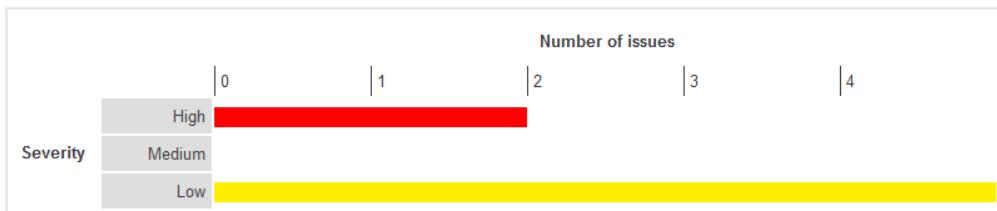
Below the details, there is a progress bar with a circular indicator. The status message "Audit finished." is displayed. The "Audit items" tab is also visible, showing a table of audit results. The table has columns: #, Host, URL, Status, Passive ph..., Active phases, JavaScript ph..., Issues, Requests, Errors, and Insertion points. The table contains 9 rows of data, corresponding to the URLs listed in the "Audit items" tab. The bottom of the screen shows a terminal window with the command "data" and its output, along with other open browser tabs for "Burp Suite Professional v2020.9..." and "Mozilla Firefox".

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity		Confidence			Total
		Certain	Firm	Tentative	
High		2	0	0	2
Medium		0	0	0	0
Low		5	0	0	5
Information		14	2	0	16

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. External service interaction (DNS)

- 1.1. <http://datahub.tiktok.com/>
- 1.2. <http://datahub.tiktok.com/robots.txt>

Contents

1. External service interaction (DNS)

- 1.1. <http://datahub.tiktok.com/>
- 1.2. <http://datahub.tiktok.com/robots.txt>

2. Unencrypted communications

3. Strict transport security not enforced

- 3.1. <https://datahub.tiktok.com/>
- 3.2. <https://datahub.tiktok.com/jupyterhub-dev/hub/>
- 3.3. <https://datahub.tiktok.com/page/main/data>
- 3.4. <https://datahub.tiktok.com/robots.txt>

4. Referer-dependent response

5. TLS cookie without secure flag set

- 5.1. <https://datahub.tiktok.com/>
- 5.2. <https://datahub.tiktok.com/jupyterhub-dev/hub/>
- 5.3. <https://datahub.tiktok.com/page/main/data>
- 5.4. <https://datahub.tiktok.com/robots.txt>

6. Cross-domain script include

- 6.1. <https://datahub.tiktok.com/>
- 6.2. <https://datahub.tiktok.com/page/main/data>

7. Cookie without HttpOnly flag set

- 7.1. <http://datahub.tiktok.com/robots.txt>
- 7.2. <https://datahub.tiktok.com/>
- 7.3. <https://datahub.tiktok.com/page/main/data>
- 7.4. <https://datahub.tiktok.com/robots.txt>

8. Cacheable HTTPS response

- 8.1. <https://datahub.tiktok.com/>
- 8.2. <https://datahub.tiktok.com/page/main/data>
- 8.3. <https://datahub.tiktok.com/robots.txt>

9. Base64-encoded data in parameter

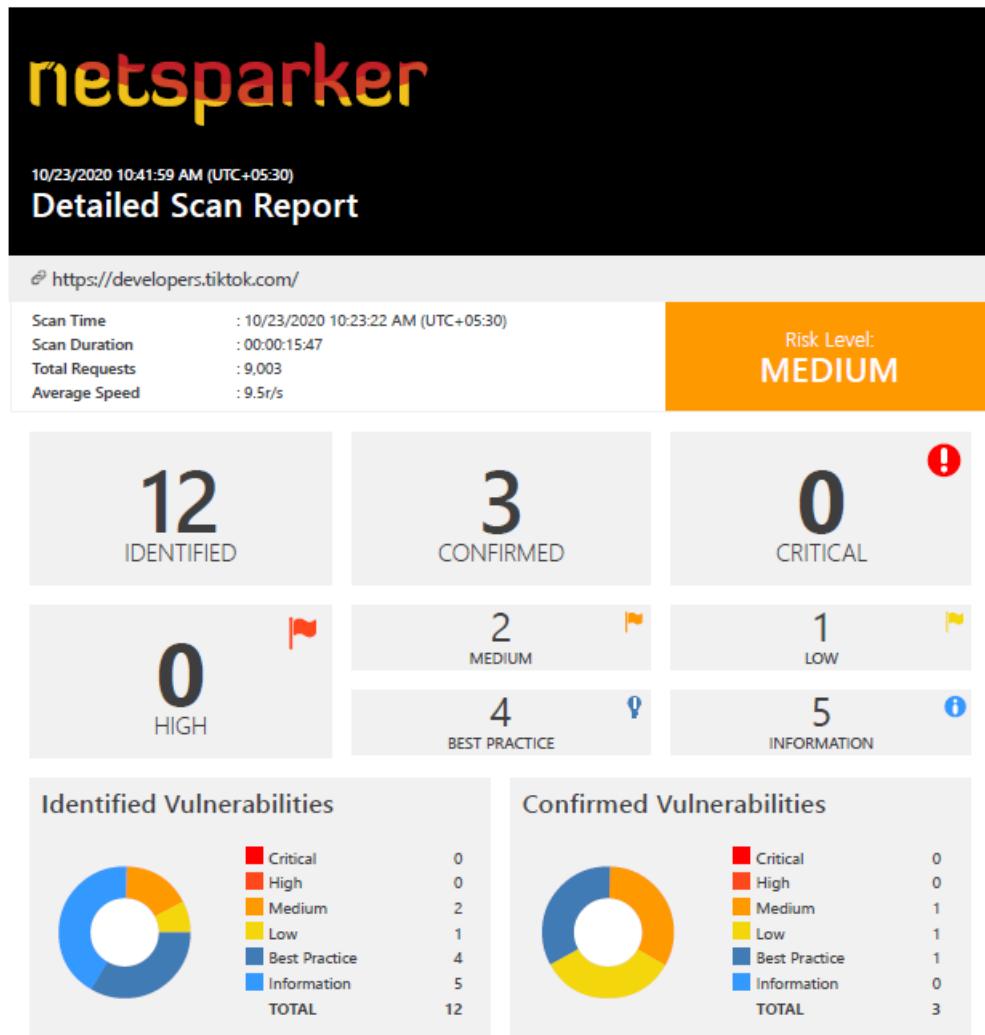
10. TLS certificate

Vulnerabilities

1. External service interaction (DNS) – **High**
 - <http://datahub.tiktok.com/>
 - <http://datahub.tiktok.com/robots.txt>
2. Unencrypted communications – **Low**
3. Strict transport security not enforced – **Low**
 - <https://datahub.tiktok.com/>
 - <https://datahub.tiktok.com/jupyterhub-dev/hub/>
 - <https://datahub.tiktok.com/page/main/data>
 - <https://datahub.tiktok.com/robots.txt>
4. Referrer-dependent response – **Information**
5. TLS cookie without secure flag set
 - <https://datahub.tiktok.com/>
 - <https://datahub.tiktok.com/jupyterhub-dev/hub/>
 - <https://datahub.tiktok.com/page/main/data>
 - <https://datahub.tiktok.com/robots.txt>
6. Cross-domain script include – **Information**
 - <https://datahub.tiktok.com/>
 - <https://datahub.tiktok.com/page/main/data>
7. Cookie without HttpOnly flag set – **Information**
 - <http://datahub.tiktok.com/robots.txt>
 - <https://datahub.tiktok.com/>
 - <https://datahub.tiktok.com/page/main/data>
 - <https://datahub.tiktok.com/robots.txt>
8. Cacheable HTTPS response – **Information**
 - <https://datahub.tiktok.com/>
 - <https://datahub.tiktok.com/page/main/data>
 - <https://datahub.tiktok.com/robots.txt>
9. Base64-encoded data in parameter – **Information**
10. TLS certificate – **Information**

8. developers.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://developers.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://developers.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://developers.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://developers.tiktok.com/	
!	Missing X-XSS-Protection Header	POST	https://developers.tiktok.com/aweme/v2/platform/tt/user/confir m/	
!	Subresource Integrity (SRI) Not Implemented	GET	https://developers.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://developers.tiktok.com/	
!	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://developers.tiktok.com/	
!	data: Used in a Content Security Policy (CSP) Directive	GET	https://developers.tiktok.com/	
!	Missing object-src in CSP Declaration	GET	https://developers.tiktok.com/	
!	Nginx Web Server Identified	GET	https://developers.tiktok.com/	
!	Out-of-date Version (React)	GET	https://developers.tiktok.com/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

netsparker

10/23/2020 10:04:32 PM (UTC+05:30)
OWASP Top Ten 2013 Report

🔗 <https://developers.tiktok.com/>

Scan Time : 10/23/2020 9:53:12 PM (UTC+05:30)	Scan Duration : 00:00:09:45	Total Requests : 10,145	Average Speed : 17.3r/s	Risk Level: MEDIUM
---	-----------------------------	-------------------------	-------------------------	---------------------------

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 7 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

8
IDENTIFIED

5
CONFIRMED

0 !
CRITICAL

0 !
HIGH

2 !
MEDIUM

3 !
LOW

1 ?
BEST PRACTICE

2 i
INFORMATION

Identified Vulnerabilities	
Critical	0
High	0
Medium	2
Low	3
Best Practice	1
Information	2
TOTAL	8

Confirmed Vulnerabilities	
Critical	0
High	0
Medium	1
Low	3
Best Practice	1
Information	0
TOTAL	5

Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://developers.tiktok.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	https://developers.tiktok.com/	LOW
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://developers.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://developers.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://developers.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://developers.tiktok.com/	BEST PRACTICE
	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://developers.tiktok.com/	INFORMATION
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES				
	Out-of-date Version (React)	GET	https://developers.tiktok.com/	INFORMATION

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. At the top, the title bar reads "Applications ▾ Places ▾ burp-StartBurp ▾" and "Fri Oct 23 9:53:18 AM". The main window title is "10. Crawl and audit of developers.tiktok.com". Below the title bar, there's a navigation bar with tabs: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The "Proxy" tab is selected.

The main content area displays the "Task details" for task 10. It shows the following information:

- Scan type: Crawl and audit
- Scope: developers.tiktok.com
- Configuration: Default configuration
- Issues: 3 (with three colored circles: red, orange, yellow)
- Requests: 590
- Errors: 0
- Unique locations: 2

A progress bar at the bottom indicates "Audit finished." A status message below the progress bar says "[3] Crawl was configured to use a browser, but a browser could not be found." The status bar at the bottom of the window shows "Memory: 196.7MB" and "Disk: 16.0MB".

At the bottom of the main window, there's a toolbar with icons for Details, Audit items, Issue activity, and Event log. Below this toolbar, there's a table titled "Audit items" showing two entries:

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	http://developers.tiktok.com	/	Done	● ●	● ● ● ● ●	● ● ●	●	219	3	
2	https://developers.tiktok.com	/robots.txt	Done	● ●	● ● ● ● ●	● ● ●	●	363	4	

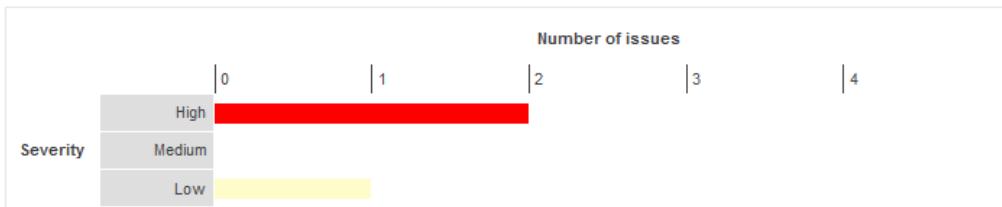
The status bar at the very bottom of the screen shows "data" and several open tabs in a terminal or browser environment, including "/media/sf_Kali_Linux/note_pad...", "[root@kali: /usr/lib/vm]/java-11...", "Burp Suite Professional v2020.9...", "[New Tab - Mozilla Firefox]", "[root@kali: -]", and "10. Crawl and audit of developers... 1/2".

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	2	0	0	2
	Medium	0	0	0	0
	Low	0	0	1	1
	Information	2	0	0	2

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. External service interaction (DNS)

- 1.1. <http://developers.tiktok.com/>
- 1.2. <https://developers.tiktok.com/robots.txt>

2. Open redirection (DOM-based)

3. Cross-domain script include

4. TLS certificate

Vulnerabilities

1. External service interaction (DNS) – **High**

- <http://developers.tiktok.com/>
- <https://developers.tiktok.com/robots.txt>

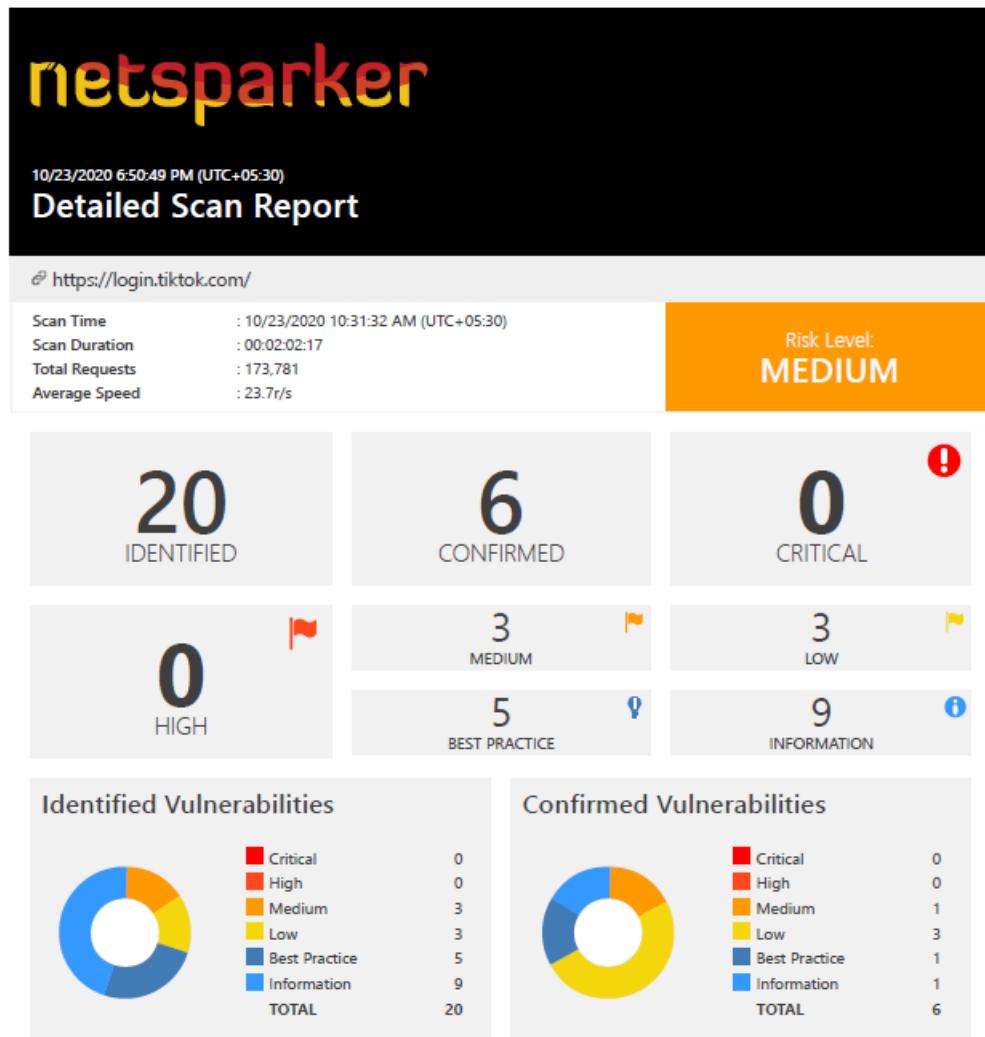
2. Open redirection (DOM-based) – **Low**

3. Cross-domain script include – **Information**

4. TLS certificate – **Information**

9. login.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

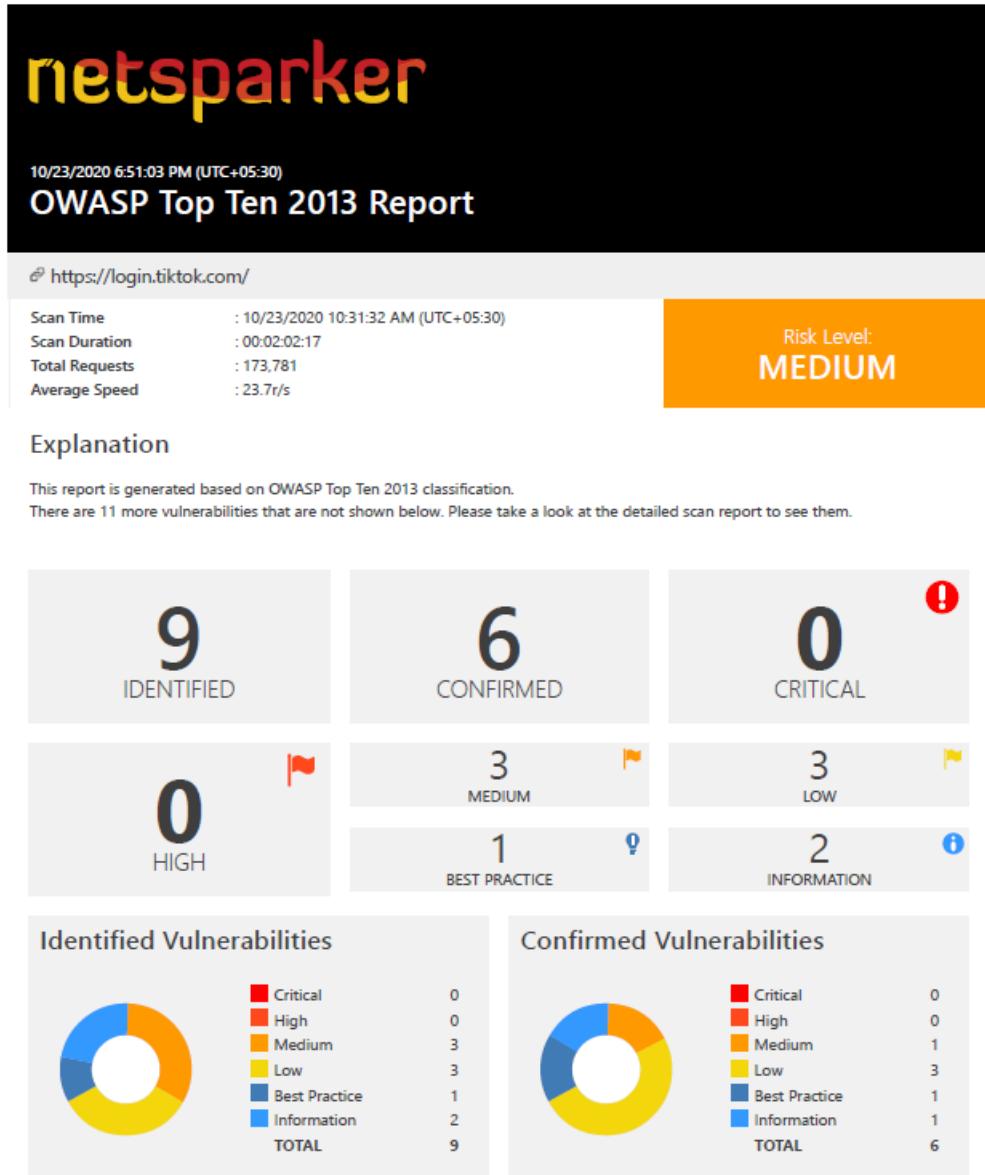
Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	[Possible] Password Transmitted over Query String	GET	https://login.tiktok.com/sitemap.xml	
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://login.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://login.tiktok.com/	
!	Cookie Not Marked as HttpOnly	GET	https://login.tiktok.com/open-search.gz	
!	Cookie Not Marked as Secure	GET	https://login.tiktok.com/open-search.gz	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://login.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://login.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://login.tiktok.com/passport/web/account/	
!	SameSite Cookie Not Implemented	GET	https://login.tiktok.com/open-search.gz	
!	Subresource Integrity (SRI) Not Implemented	GET	https://login.tiktok.com/open-search.gz	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://login.tiktok.com/	
!	[Possible] Login Page Identified	GET	https://login.tiktok.com/sitemap.xml	
!	An Unsafe Content Security Policy (CSP), Directive in Use	GET	https://login.tiktok.com/open-search.gz	
!	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://login.tiktok.com/open-search.gz	

2 / 70

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	data: Used in a Content Security Policy (CSP) Directive	GET	https://login.tiktok.com/open-search.gz	
!	default-src Used in Content Security Policy (CSP)	GET	https://login.tiktok.com/open-search.gz	
!	Missing object-src in CSP Declaration	GET	https://login.tiktok.com/open-search.gz	
!	Nginx Web Server Identified	GET	https://login.tiktok.com/	
!	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://login.tiktok.com/open-search.gz	
!	OPTIONS Method Enabled	OPTIONS	https://login.tiktok.com/.well-known/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

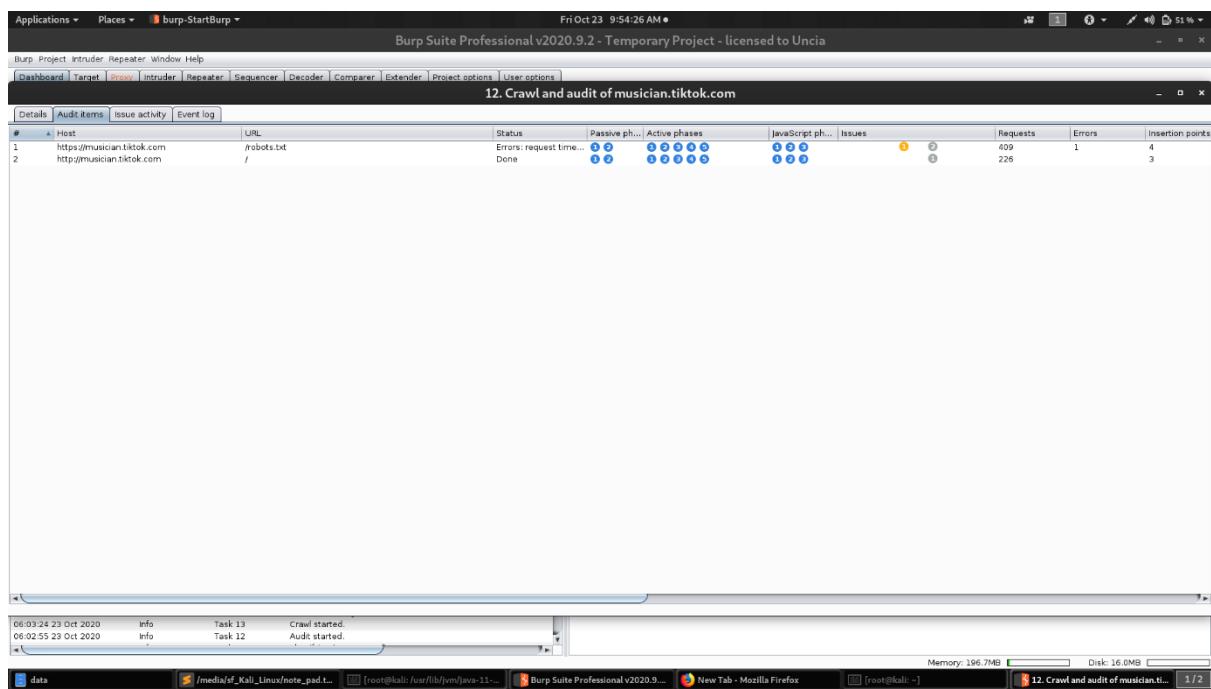
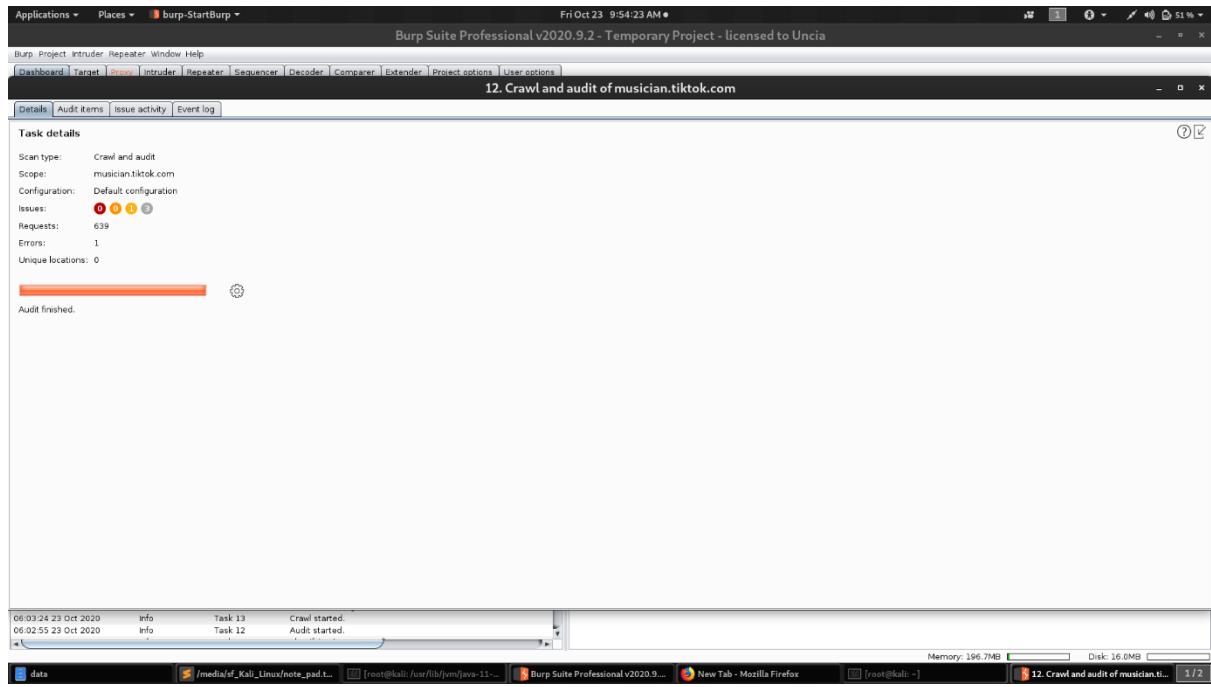


Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	Cookie Not Marked as HttpOnly	GET	https://login.tiktok.com/open-search.gz	LOW
	OPTIONS Method Enabled	OPTIONS	https://login.tiktok.com/.well-known/	INFORMATION
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://login.tiktok.com/	MEDIUM
	[Possible] Password Transmitted over Query String	GET	https://login.tiktok.com/sitemap.xml	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://login.tiktok.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://login.tiktok.com/open-search.gz	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://login.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://login.tiktok.com/	BEST PRACTICE
	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://login.tiktok.com/open-search.gz	INFORMATION

Burp Suite Scanning



Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	0	0	0	0
	Information	6	1	0	7

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

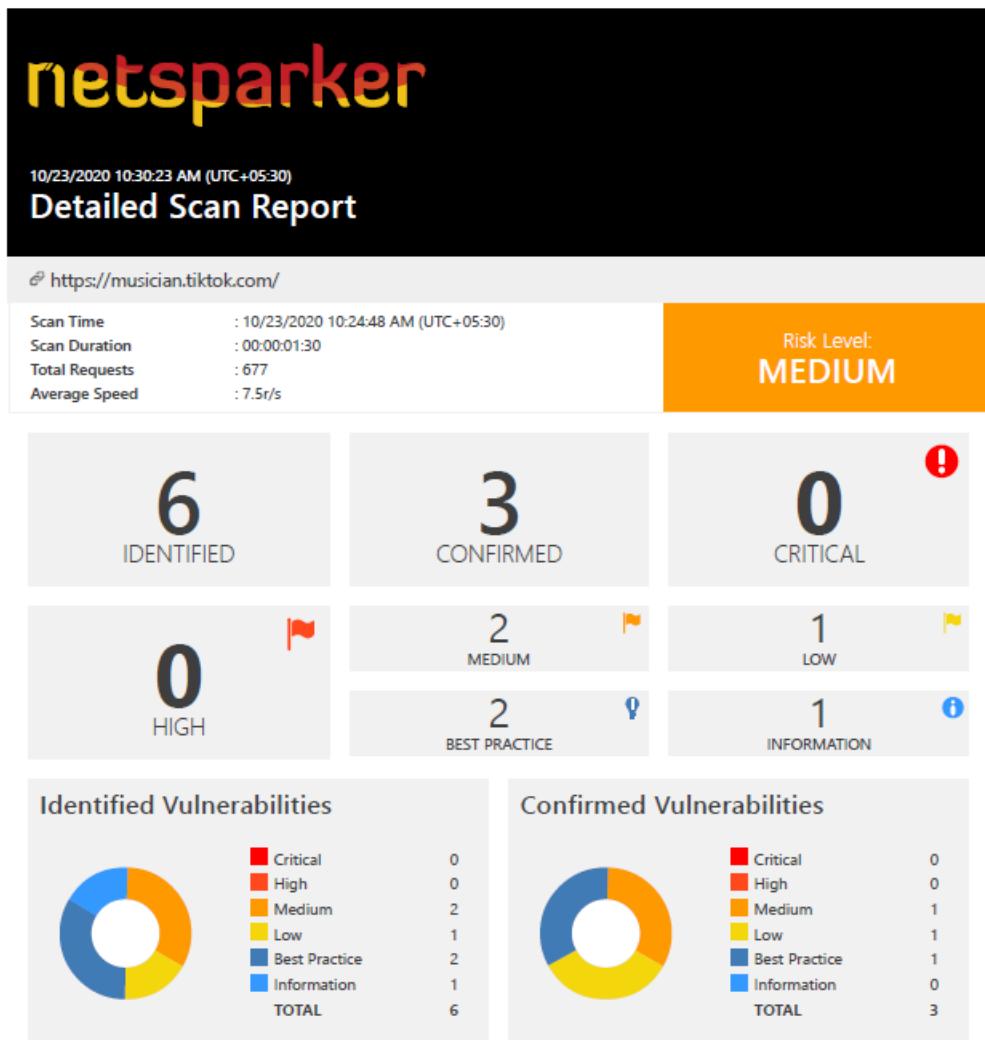
1. User agent-dependent response
2. Duplicate cookies set
3. Input returned in response (reflected)
 - 3.1. <http://login.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - 3.2. <https://login.tiktok.com/robots.txt> [User-Agent HTTP header]
4. Cookie scoped to parent domain
5. Cross-domain script include
6. TLS certificate

Vulnerabilities

1. User agent-dependent response – **Information**
2. Duplicate cookies set – **Information**
3. Input returned in response (reflected) – **Information**
 - <http://login.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - <https://login.tiktok.com/robots.txt> [User-Agent HTTP header]
4. Cookie scoped to parent domain – **Information**
5. Cross-domain script include – **Information**
6. TLS certificate – **Information**

10.musician.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain

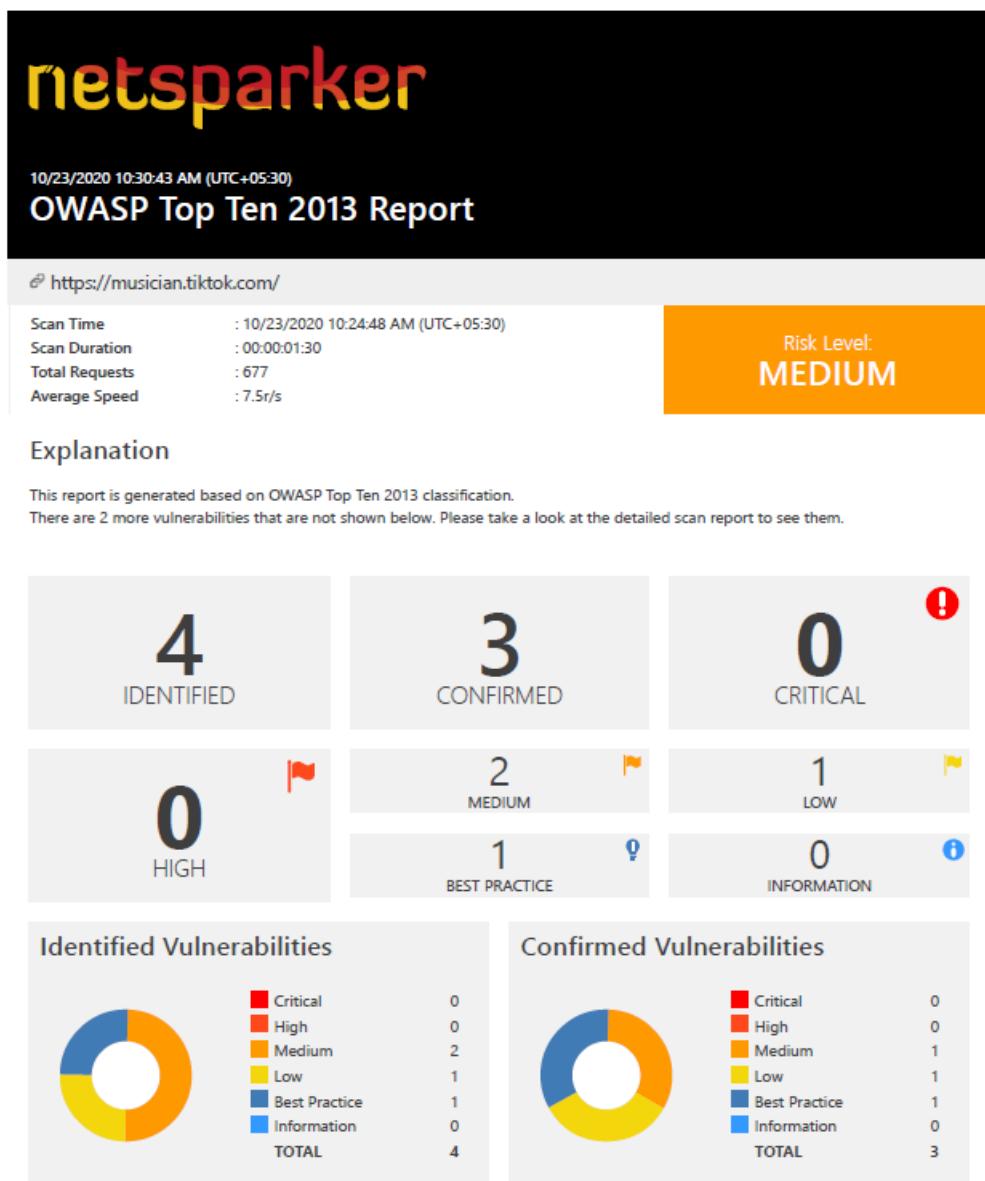


Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://musician.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://musician.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://musician.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://musician.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://musician.tiktok.com/	
!	Nginx Web Server Identified	GET	https://musician.tiktok.com/	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

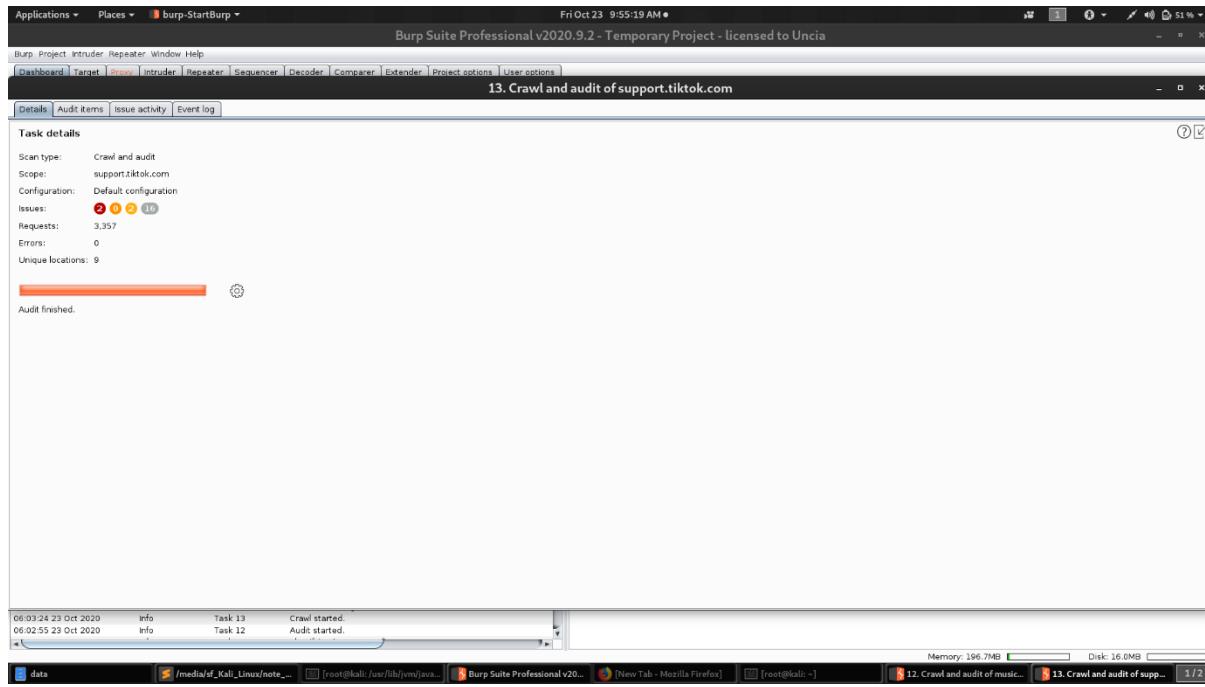


Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A6 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://musician.tiktok.com/	MEDIUM
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://musician.tiktok.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://musician.tiktok.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://musician.tiktok.com/	BEST PRACTICE

Burp Suite Scanning



#	Host	URL	Status	Passive ph...	Active phas...	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	https://support.tiktok.com	/enusing-tiktok	Done	██████	██████████	██████	0	300	5	
2	https://support.tiktok.com	/enusing-tiktok/	Done	██████	██████████	██████	0	317	5	
3	https://support.tiktok.com	/robots.txt	Done	██████	██████████	██████	0	371	4	
4	https://support.tiktok.com	/tosnode/stemaps/sitemap.xml	Done	██████	██████████	██████	0	493	7	
5	https://support.tiktok.com	/en/my-account-settings/	Done	██████	██████████	██████	0	301	5	
6	https://support.tiktok.com	/en/privacy-safety	Done	██████	██████████	██████	0	297	5	
7	http://support.tiktok.com	/	Done	██████	██████████	██████	0	301	5	
8	http://support.tiktok.com	/	Done	██████	██████████	██████	0	219	3	
9	https://support.tiktok.com	/en/my-account-settings	Done	██████	██████████	██████	0	143	5	
10	http://support.tiktok.com	/robots.txt	Done	██████	██████████	██████	0	603	4	

The bottom status bar displays "Memory: 196.7MB" and "Disk: 16.0MB". The task bar at the bottom of the screen shows several open tabs, including "data", "/media/sf_Kali_Linux/note...", "[root@kali: /usr/lib/jvm/java...]", "Burp Suite Professional v20...", "[New Tab - Mozilla Firefox]", "[root@kali: ~]", "12. Crawl and audit of music...", "13. Crawl and audit of sup...", and "1 / 2".

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	1	0	0	1
	Information	3	0	0	3

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

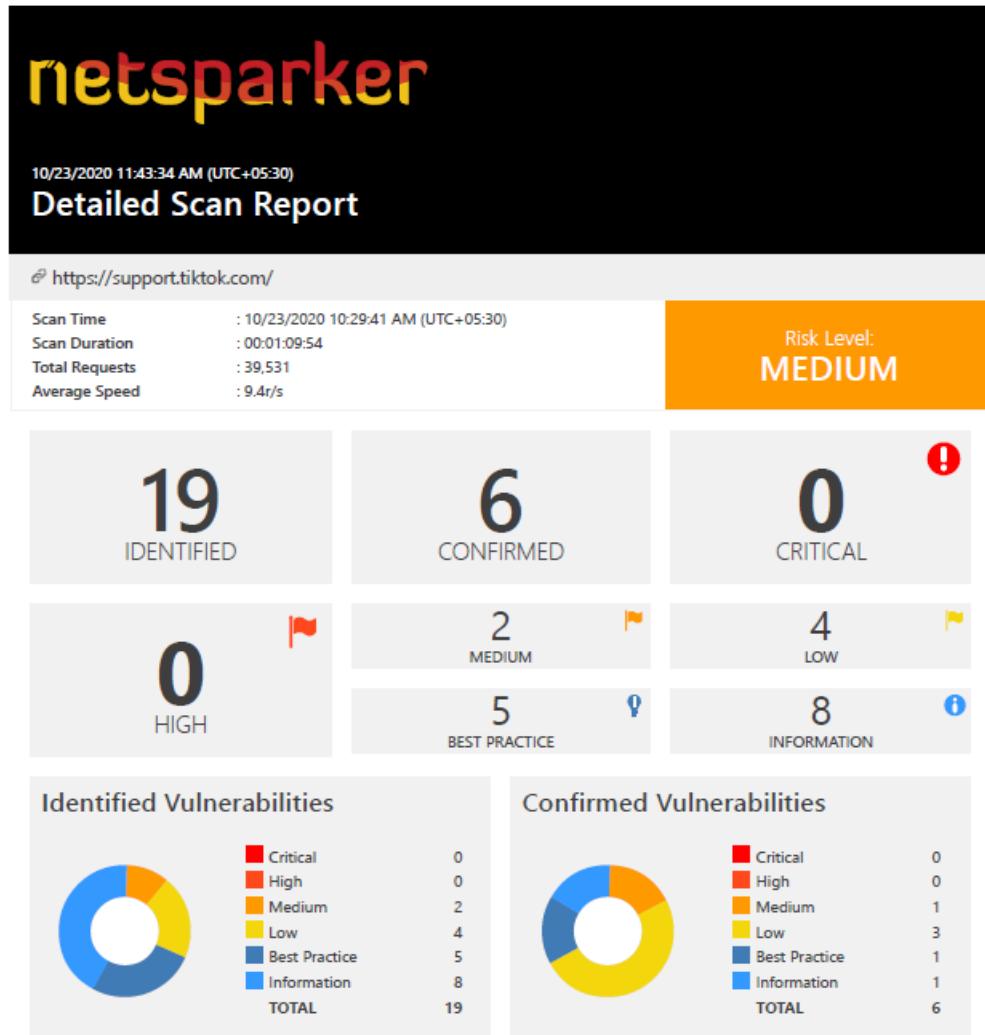
1. Strict transport security not enforced
2. Input returned in response (reflected)
 - 2.1. <http://musician.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - 2.2. <https://musician.tiktok.com/robots.txt> [name of an arbitrarily supplied URL parameter]
3. TLS certificate

Vulnerabilities

1. Strict transport security not enforced – **Low**
2. Input returned in response (reflected) – **Information**
 - <http://musician.tiktok.com/> [name of an arbitrarily supplied URL parameter]
 - <https://musician.tiktok.com/robots.txt> [name of an arbitrarily supplied URL parameter]
3. TLS certificate – **Information**

11.support.tiktok.com

This is the detail report of Netsparker scan. I upload “Netsparker Scanning - Detail reports” folder in drive. This folder contains the full reports of sub domain



Vulnerability Summary for subdomain

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://support.tiktok.com/	
!	Weak Ciphers Enabled	GET	https://support.tiktok.com/	
!	Misconfigured Access-Control-Allow-Origin Header	GET	https://support.tiktok.com/web/api/v2/support/	URI-BASED
!	Cookie Not Marked as HttpOnly	GET	https://support.tiktok.com/ur/using-tiktok/record-a-video-without-holding-the-button-default	
!	Cookie Not Marked as Secure	GET	https://support.tiktok.com/ur/using-tiktok/record-a-video-without-holding-the-button-default	
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://support.tiktok.com/	
!	Expect-CT Not Enabled	GET	https://support.tiktok.com/	
!	Missing X-XSS-Protection Header	GET	https://support.tiktok.com/web/api/v2/support/categoryList/	
!	SameSite Cookie Not Implemented	GET	https://support.tiktok.com/ur/using-tiktok/record-a-video-without-holding-the-button-default	
!	Subresource Integrity (SRI) Not Implemented	GET	https://support.tiktok.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://support.tiktok.com/	
!	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://support.tiktok.com/	
!	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://support.tiktok.com/	

2 / 68

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	data: Used in a Content Security Policy (CSP) Directive	GET	https://support.tiktok.com/	
	default-src Used in Content Security Policy (CSP)	GET	https://support.tiktok.com/	
	Missing object-src in CSP Declaration	GET	https://support.tiktok.com/	
	Nginx Web Server Identified	GET	https://support.tiktok.com/	
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://support.tiktok.com/	
	Robots.txt Detected	GET	https://support.tiktok.com/robots.txt	

This is the OWASP Top Ten 2013 Report of Netsparker scan. I upload “Netsparker Scanning - OWASP Top Ten 2013 Reports” folder in drive. This folder contains the full reports of sub domains.

netsparker

10/23/2020 11:44:25 AM (UTC+05:30)
OWASP Top Ten 2013 Report

<https://support.tiktok.com/>

Scan Time : 10/23/2020 10:29:41 AM (UTC+05:30)	Scan Duration : 00:01:09:54	Total Requests : 39,531	Average Speed : 9.4r/s	Risk Level: MEDIUM
--	-----------------------------	-------------------------	------------------------	---------------------------

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 11 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

8 IDENTIFIED	5 CONFIRMED	0 CRITICAL
0 HIGH	2 MEDIUM	4 LOW
	1 BEST PRACTICE	1 INFORMATION

Identified Vulnerabilities	Confirmed Vulnerabilities																												
<table border="1"><tr><td>Critical</td><td>0</td></tr><tr><td>High</td><td>0</td></tr><tr><td>Medium</td><td>2</td></tr><tr><td>Low</td><td>4</td></tr><tr><td>Best Practice</td><td>1</td></tr><tr><td>Information</td><td>1</td></tr><tr><td>TOTAL</td><td>8</td></tr></table>	Critical	0	High	0	Medium	2	Low	4	Best Practice	1	Information	1	TOTAL	8	<table border="1"><tr><td>Critical</td><td>0</td></tr><tr><td>High</td><td>0</td></tr><tr><td>Medium</td><td>1</td></tr><tr><td>Low</td><td>3</td></tr><tr><td>Best Practice</td><td>1</td></tr><tr><td>Information</td><td>0</td></tr><tr><td>TOTAL</td><td>5</td></tr></table>	Critical	0	High	0	Medium	1	Low	3	Best Practice	1	Information	0	TOTAL	5
Critical	0																												
High	0																												
Medium	2																												
Low	4																												
Best Practice	1																												
Information	1																												
TOTAL	8																												
Critical	0																												
High	0																												
Medium	1																												
Low	3																												
Best Practice	1																												
Information	0																												
TOTAL	5																												

Vulnerability Summary for subdomain

Vulnerabilities By OWASP 2013

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://support.tiktok.com/	MEDIUM
!	Cookie Not Marked as HttpOnly	GET	https://support.tiktok.com/ur/using-tiktok/record-a-video-without-holding-the-button-default	LOW
!	Misconfigured Access-Control-Allow-Origin Header	GET	https://support.tiktok.com/web/api/v2/support/	LOW
A6 - SENSITIVE DATA EXPOSURE				
!	Weak Ciphers Enabled	GET	https://support.tiktok.com/	MEDIUM
!	Cookie Not Marked as Secure	GET	https://support.tiktok.com/ur/using-tiktok/record-a-video-without-holding-the-button-default	LOW
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://support.tiktok.com/	LOW
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://support.tiktok.com/	BEST PRACTICE
!	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://support.tiktok.com/	INFORMATION

Burp Suite Scanning

The screenshot shows the Burp Suite Professional interface. The title bar indicates the application is running on a Linux system (root@kali) and the task is "3. Crawl and audit of login.tiktok.com". The main window displays the "Task details" tab, which provides summary statistics: Scan type: Crawl and audit; Scope: login.tiktok.com; Configuration: Default configuration; Issues: 0 (red), 0 (orange), 0 (yellow), 7 (grey); Requests: 1.132; Errors: 1; Unique locations: 1. A progress bar at the bottom shows the audit has finished.

#	Host	URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion points
1	http://login.tiktok.com	/	Done	0 0	0 0 0 0 0	0 0 0	0	431	3	
2	http://login.tiktok.com	/	Errors: request time...	0 0	0 0 0 0 0	0 0 0	0	227	1	3
3	https://login.tiktok.com	/robots.txt	Done	0 0	0 0 0 0 0	0 0 0	0	469		4

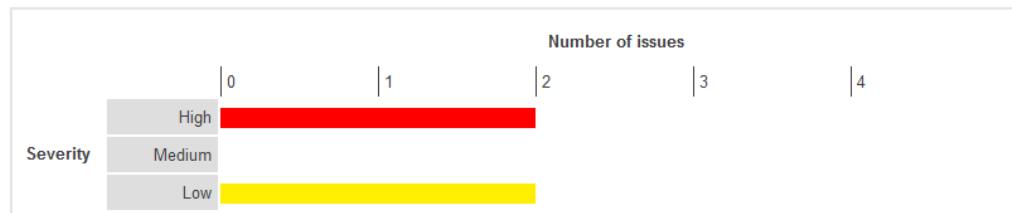
The status bar at the bottom of the window shows the path root@kali: /usr/lib/jvm/java-11-openjdk-amd64/bin/burp-StartBurp, the application name Burp Suite Professional v2020.9.2, and Mozilla Firefox.

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity		Confidence			Total
		Certain	Firm	Tentative	
High		2	0	0	2
Medium		0	0	0	0
Low		2	0	0	2
Information		16	0	0	16

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. External service interaction (DNS)

- 1.1. [http://support.tiktok.com/](https://support.tiktok.com/)
- 1.2. <https://support.tiktok.com/en/using-tiktok/>

2. Strict transport security not enforced

- 2.1. <https://support.tiktok.com/robots.txt>
- 2.2. <https://support.tiktok.com/tos/node/sitemaps/sitemap.xml>

3. Cross-domain script include

- 3.1. <https://support.tiktok.com/en/my-account-settings>
- 3.2. <https://support.tiktok.com/en/my-account-settings/>
- 3.3. <https://support.tiktok.com/en/privacy-safety>
- 3.4. <https://support.tiktok.com/en/privacy-safety/>
- 3.5. <https://support.tiktok.com/en/using-tiktok>
- 3.6. <https://support.tiktok.com/en/using-tiktok/>

4. Robots.txt file

5. Cacheable HTTPS response

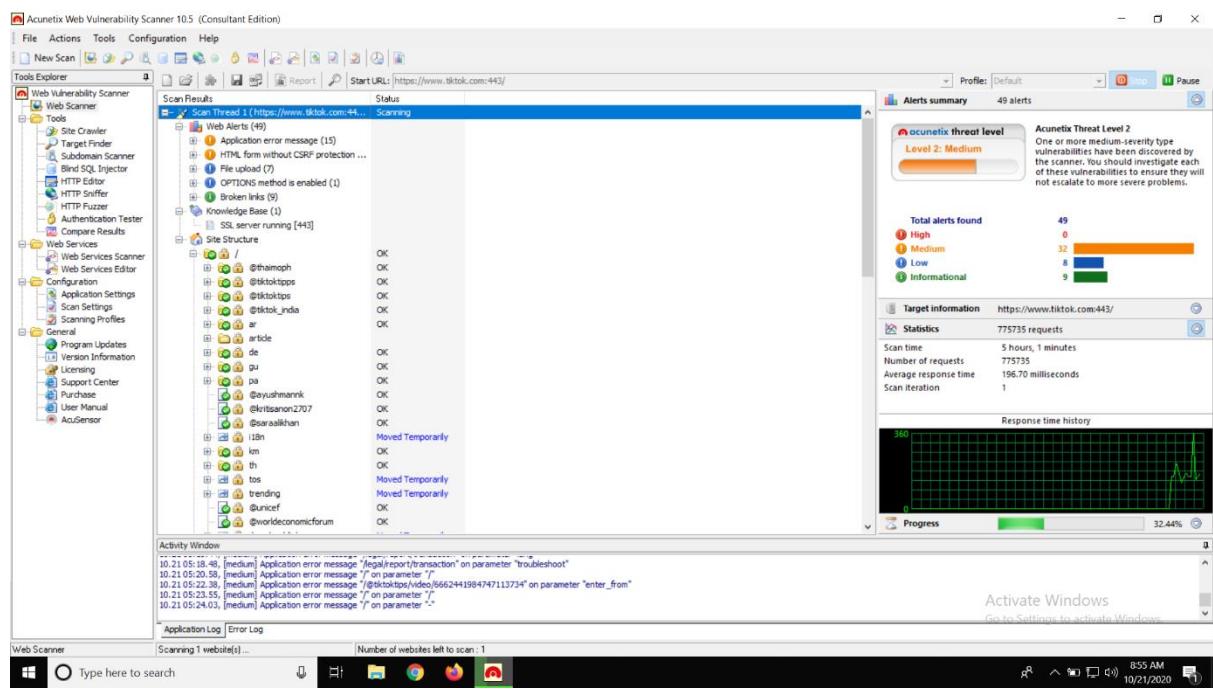
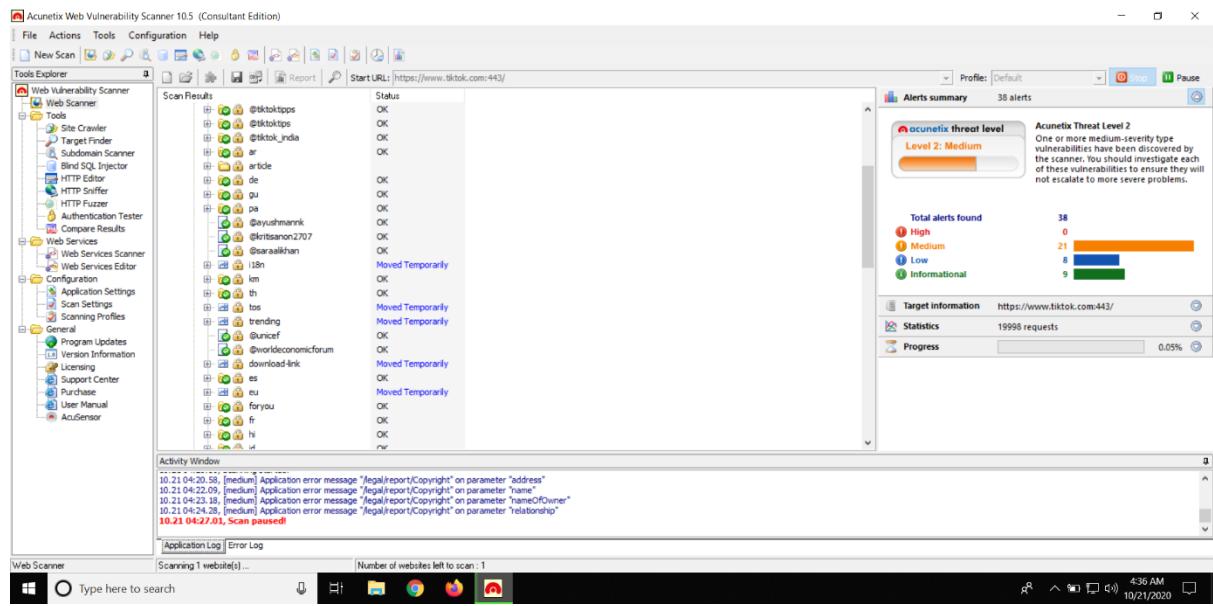
- 5.1. <https://support.tiktok.com/en/my-account-settings>
- 5.2. <https://support.tiktok.com/en/my-account-settings/>
- 5.3. <https://support.tiktok.com/en/privacy-safety>
- 5.4. <https://support.tiktok.com/en/privacy-safety/>
- 5.5. <https://support.tiktok.com/en/using-tiktok>
- 5.6. <https://support.tiktok.com/en/using-tiktok/>
- 5.7. <https://support.tiktok.com/robots.txt>
- 5.8. <https://support.tiktok.com/tos/node/sitemaps/sitemap.xml>

6. TLS certificate

Vulnerabilities

1. External service interaction (DNS) – **High**
 - <http://support.tiktok.com/>
 - <https://support.tiktok.com/en/using-tiktok/>
2. Strict transport security not enforced – **Low**
 - <https://support.tiktok.com/robots.txt>
 - <https://support.tiktok.com/tos/node/sitemaps/sitemap.xml>
3. Cross-domain script include – **Information**
 - <https://support.tiktok.com/en/my-account-settings>
 - <https://support.tiktok.com/en/my-account-settings/>
 - <https://support.tiktok.com/en/privacy-safety>
 - <https://support.tiktok.com/en/privacy-safety/>
 - <https://support.tiktok.com/en/using-tiktok>
 - <https://support.tiktok.com/en/using-tiktok/>
4. Robots.txt file – **Information**
5. Cacheable HTTPS response – **Information**
 - <https://support.tiktok.com/en/my-account-settings>
 - <https://support.tiktok.com/en/my-account-settings/>
 - <https://support.tiktok.com/en/privacy-safety>
 - <https://support.tiktok.com/en/privacy-safety/>
 - <https://support.tiktok.com/en/using-tiktok>
 - <https://support.tiktok.com/en/using-tiktok/>
 - <https://support.tiktok.com/robots.txt>
 - <https://support.tiktok.com/tos/node/sitemaps/sitemap.xml>
6. TLS certificate – **Information**

1.2.3. Full – Domain scan from OWASP Acunetix Tool



Scan of https://www.tiktok.com:443/

Scan details

Scan information	
Start time	10/21/2020 3:53:42 AM
Finish time	10/21/2020 9:34:36 AM
Scan time	5 hours, 40 minutes
Profile	Default
Server information	
Responsive	True
Server banner	nginx
Server OS	Unknown

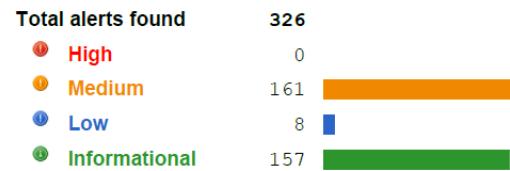
Threat level



Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution



Acunetix Threat Level 2 : One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Scanned 283 URLs. Found 151 vulnerable.

I uploaded the full report of Acunetix tool into the drive

Vulnerabilities

1. Application error message

Severity	Medium
Type	Validation
Reported by module	Scripting (XSS.script)

2. Error message on page

Severity	Medium
Type	Validation
Reported by module	Scripting (Text_Search_Dir.script)

3. HTML form without CSRF protection

Severity	Medium
Type	Informational
Reported by module	Crawler

4. File upload

Severity	Low
Type	Informational
Reported by module	Crawler

5. OPTIONS method is enabled

Severity	Low
Type	Validation
Reported by module	Scripting (Options_Server_Method.script)

6. Broken links

Severity	Informational
Type	Informational
Reported by module	Crawler

7. Email address found

Severity	Informational
Type	Informational
Reported by module	Scripting (Text_Search_Dir.script)

2. SUMMARY OF REPORT

In this report I performed several scanning tools and mechanisms to analyze the my target domain (<https://www.tiktok.com>). And my target is found a vulnerability from OWASP top 10 vulnerabilities. In the beginning of web audit, I gather the information about this website using passive information gathering mechanism and active information gathering mechanism.

In passive information gathering part I used my windows 10 machine and Kali Linux machine to gather information. In this part I used these :

- Ping command
- Whatweb command
- Whois feature
- Google -Fu
- Wayback machine

After the that part I perform active information gathering using by following tool in my Kali Linux machine :

- Sublist3r tool
- Angryfuzzer tool
- Redhawk tool
- Zenmap tool

After the information gathering part, I begin the scanning to chosen subdomains of tiktok.com. In this part I used following tools and scanners from my windows 10 machine and Kali Linux machine :

- Netsparker
- Burp Suite
- Acunetix

After all of scans I found some of vulnerabilities I mention all of them on WEB-AUDIT part of this report.

3. REFERENCES

- [1] “What is Vulnerability Assessment? | Top 5 Vulnerability Scanning Tools.” <https://cwatch.comodo.com/blog/website-security/vulnerability-assessment/> (accessed Oct. 24, 2020).
- [2] “OWASP Top Ten Web Application Security Risks | OWASP.” <https://owasp.org/www-project-top-ten/> (accessed Oct. 24, 2020).
- [3] “OWASP Top 10 Security Vulnerabilities 2020 | Sucuri.” <https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/> (accessed Oct. 24, 2020).
- [4] “(100) Nahamsec - YouTube.” <https://www.youtube.com/channel/UCCZDt7MuC3Hzs6IH4xODLBw> (accessed Oct. 24, 2020).
- [5] “(100) The Cyber Mentor - YouTube.” <https://www.youtube.com/channel/UC0ArlFuFYMpEewyRBzdLHiw> (accessed Oct. 24, 2020).
- [6] “(100) CS2 - SLIIT - YouTube.” <https://www.youtube.com/channel/UCrPSaHBuh7IQ6N30eHtUCwQ> (accessed Oct. 24, 2020).
- [7] “(100) HackerSploit - YouTube.” <https://www.youtube.com/channel/UC0ZTPkdxlAKf-V33tqXwi3Q> (accessed Oct. 24, 2020).
- [8] “OSINT Framework.” <https://osintframework.com/> (accessed Oct. 24, 2020).