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 Rugghahakotuwa and Ms. Chathu Udagedra for the help and guidance they have given us during this Web audit.

Contents

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.

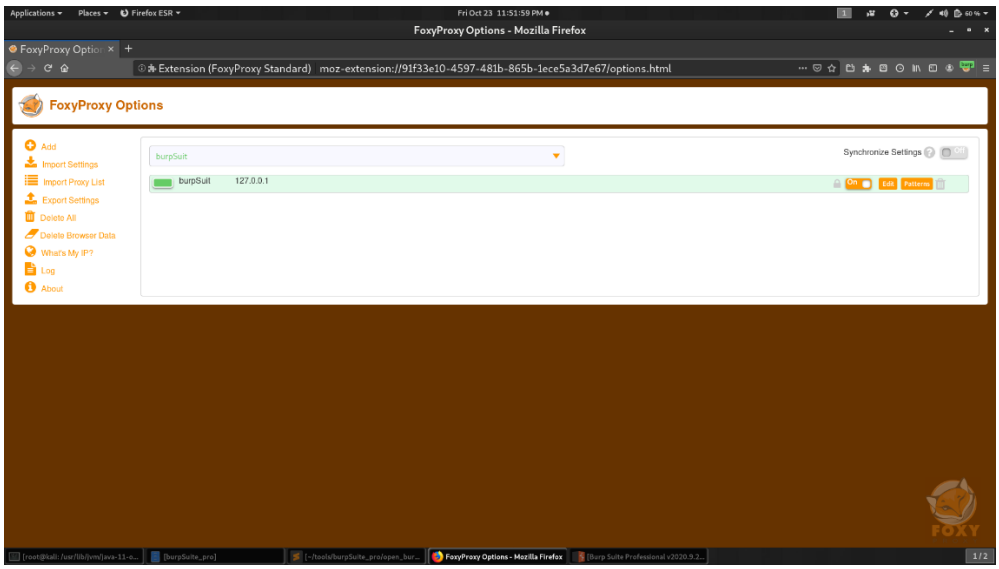
Intruder :

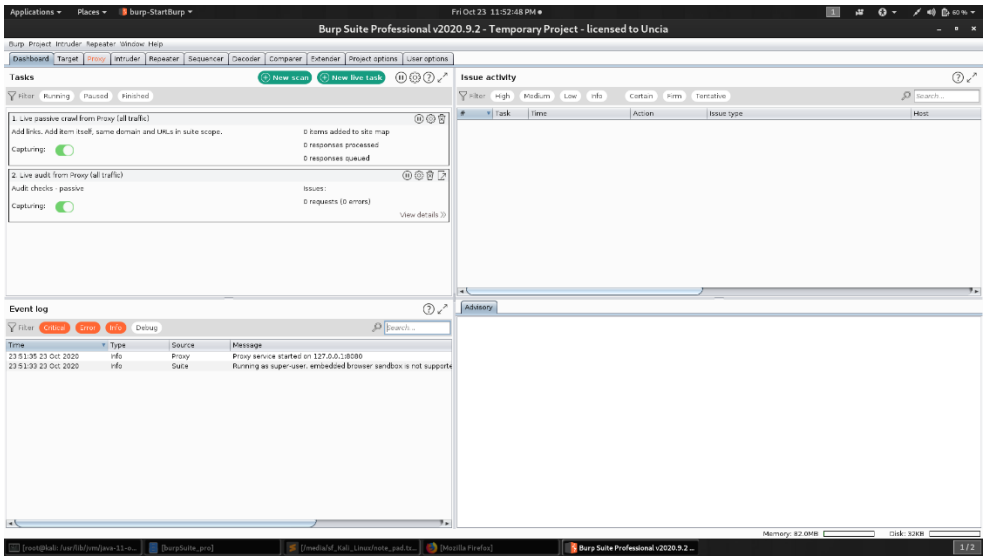
- The intruder is a method for automating web-based attacks. One condition is that the application and HTTP protocol have already been detailed known to the user. This tool provides a widely configurable HTTP request-generating algorithm. This tool can test and detect vulnerabilities such as SQL, cross-site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

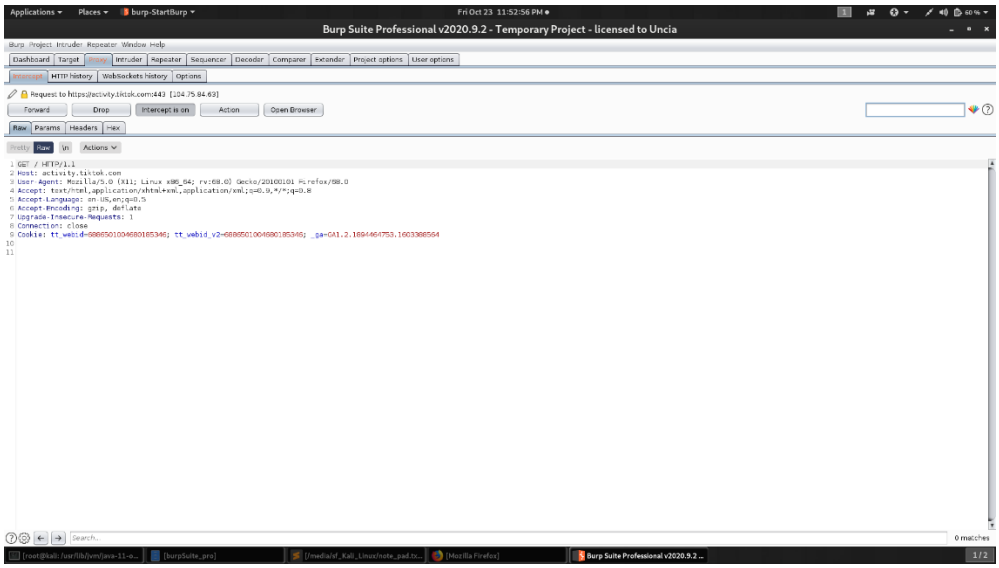
Repeater :

- 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.





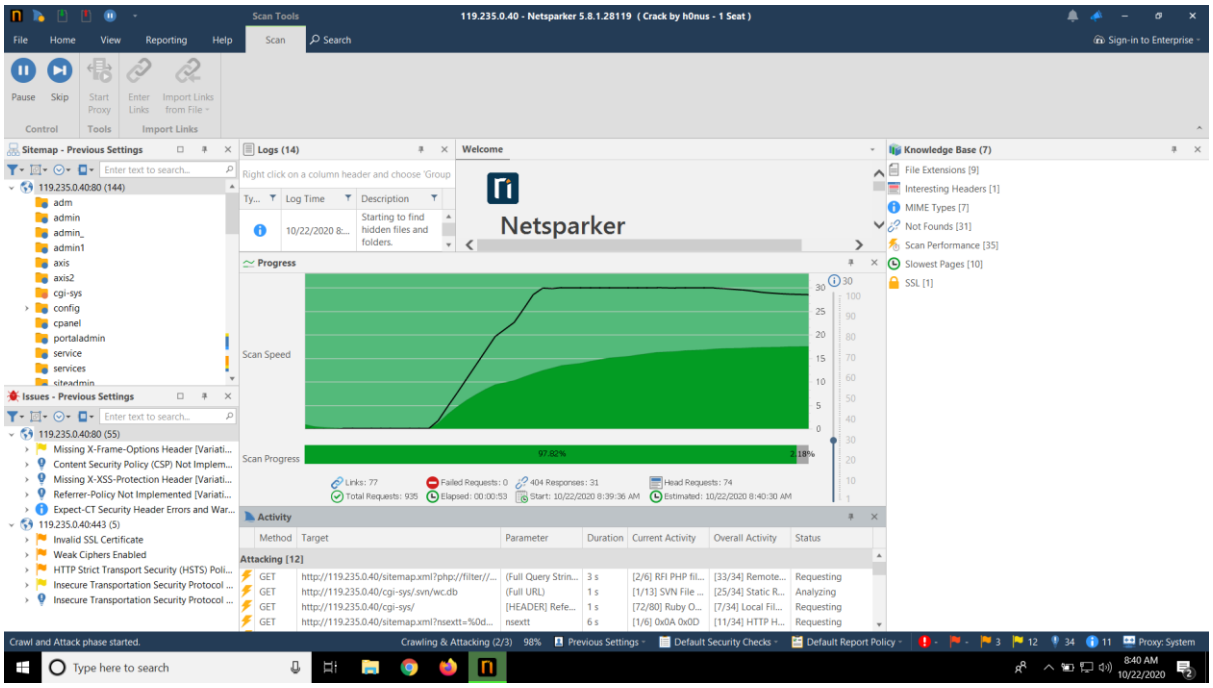


2. Netsparker

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.

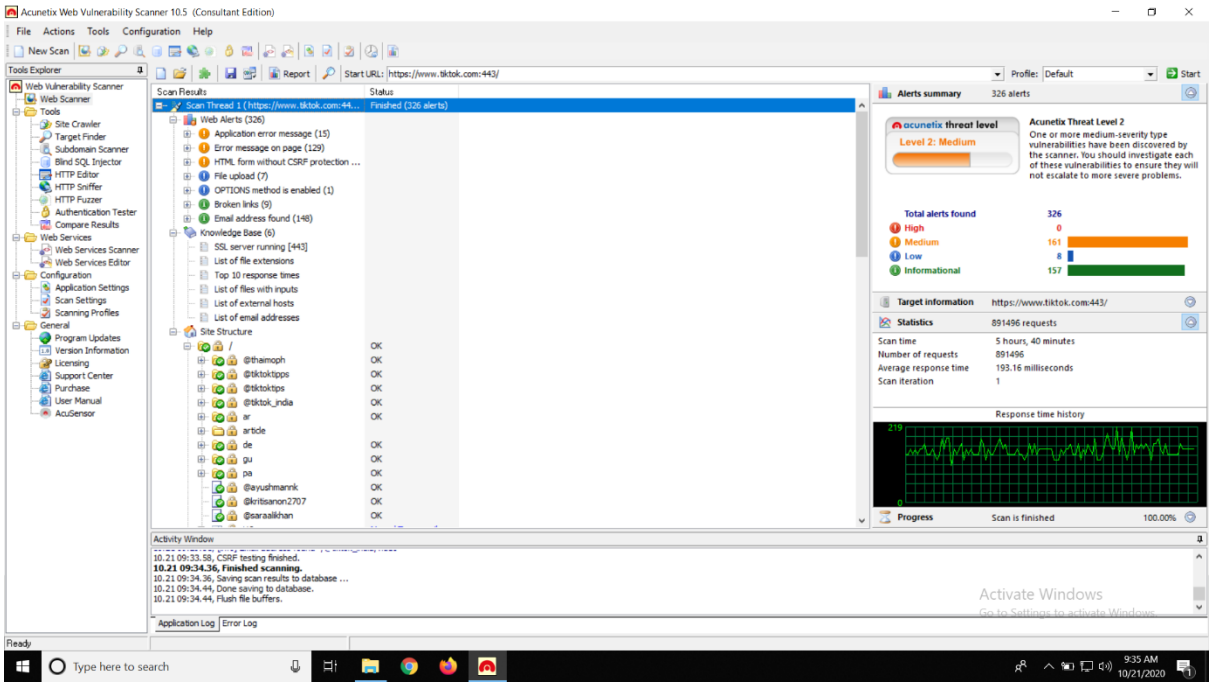
Netsparker scanning technology allows you to easily secure web applications without any issues, so you can concentrate on fixing the bugs that you have reported.



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.

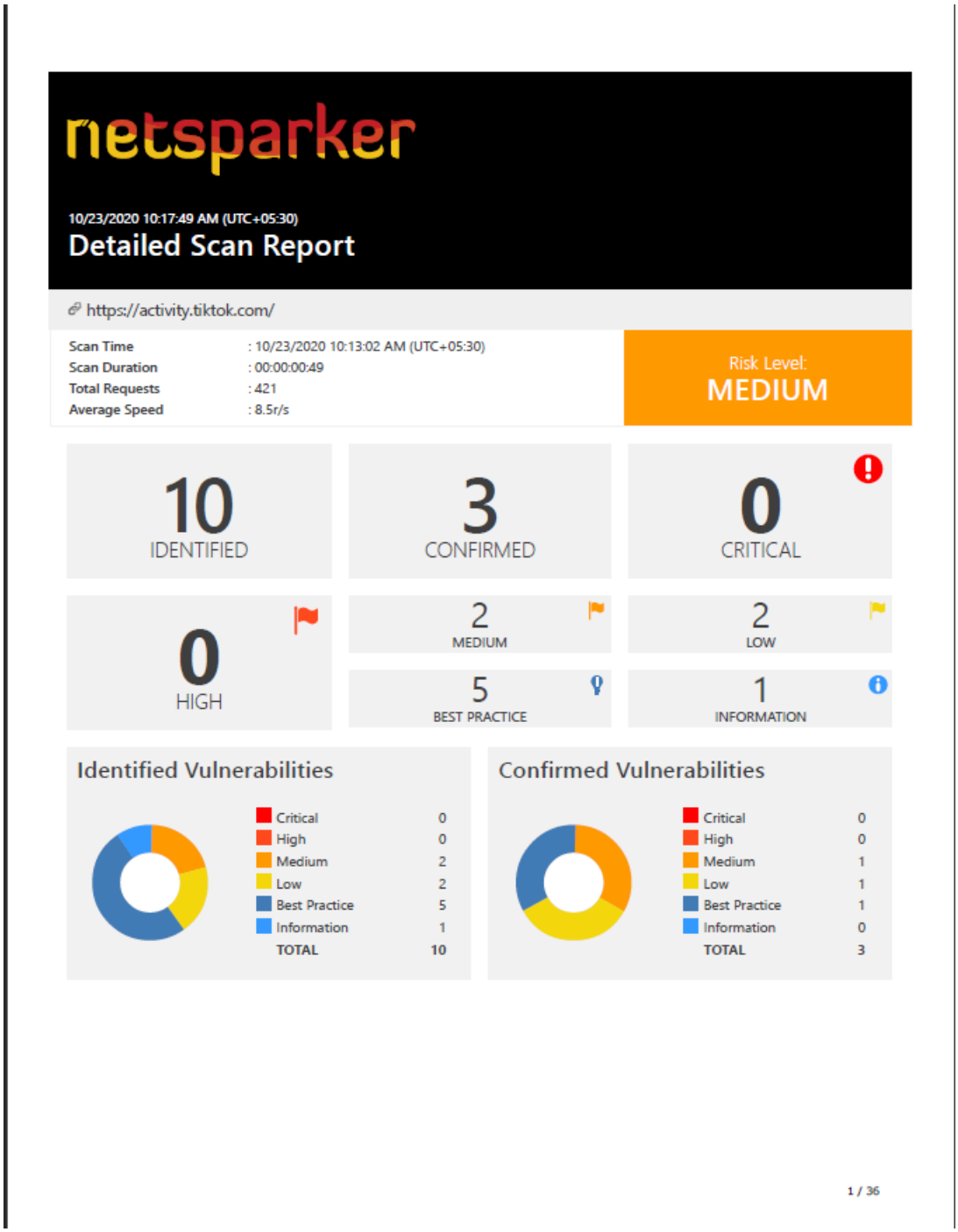


1.2.2. Scanning and generating reports

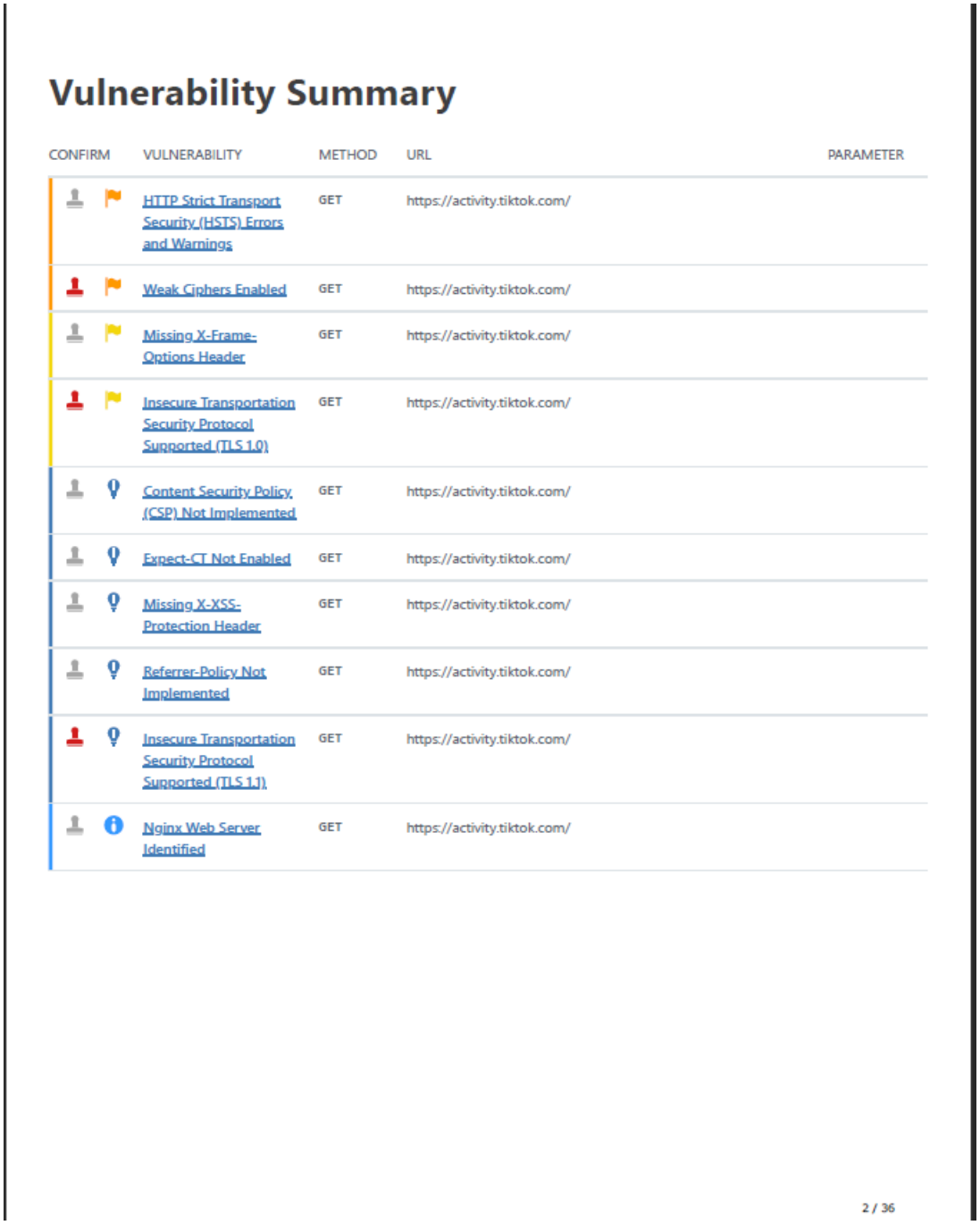
1. activity.tiktok.com

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

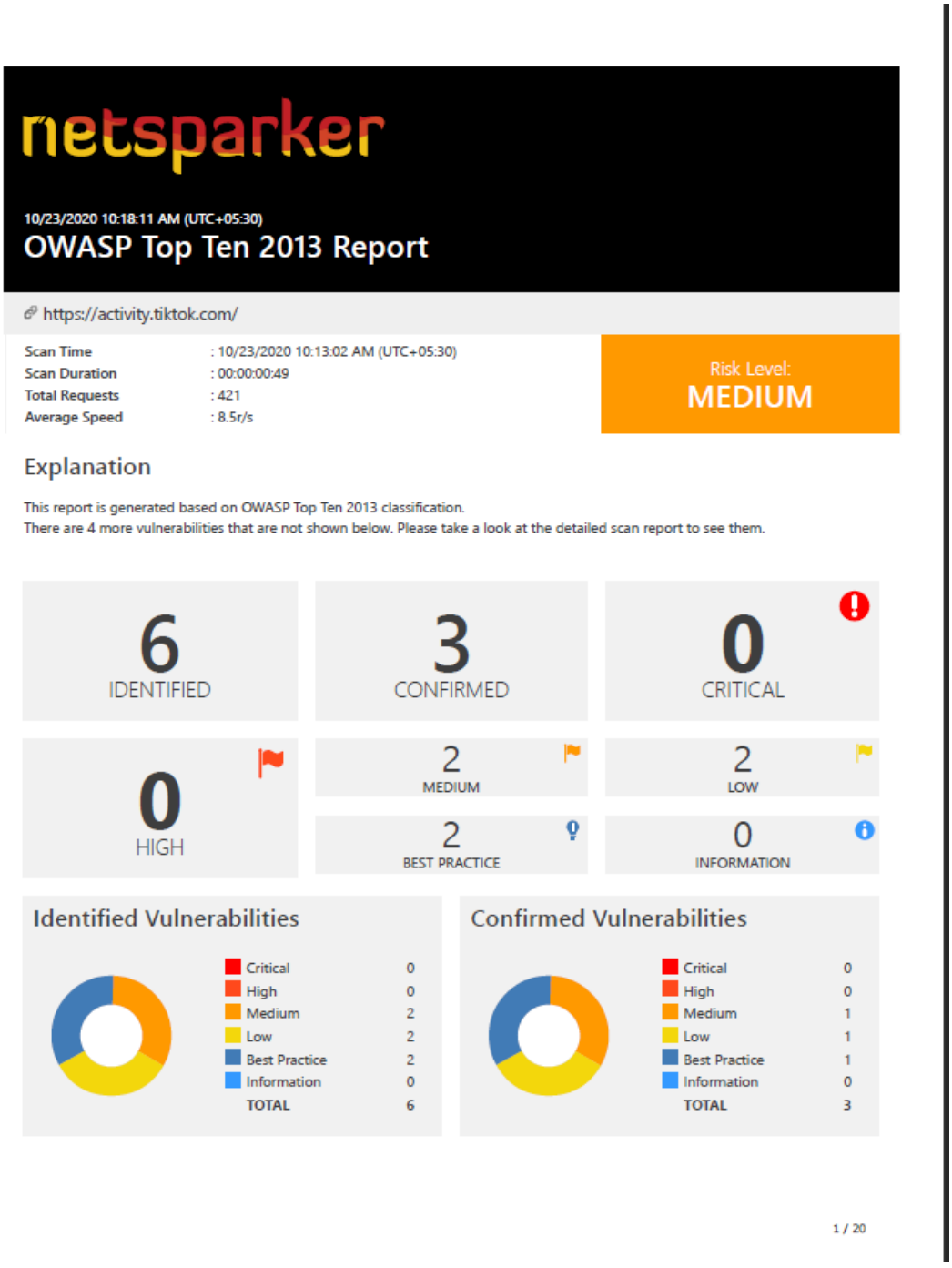


Vulnerability Summary

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/	

2 / 36

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 10:18:11 AM (UTC+05:30)

OWASP Top Ten 2013 Report

https://activity.tiktok.com/

Scan Time	: 10/23/2020 10:13:02 AM (UTC+05:30)
Scan Duration	: 00:00:00:49
Total Requests	: 421
Average Speed	: 8.5r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 4 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

6 IDENTIFIED	3 CONFIRMED	0 CRITICAL
0 HIGH	2 MEDIUM	2 LOW
	2 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	2
Best Practice	2
Information	0
TOTAL	6

Confirmed Vulnerabilities

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

1 / 20

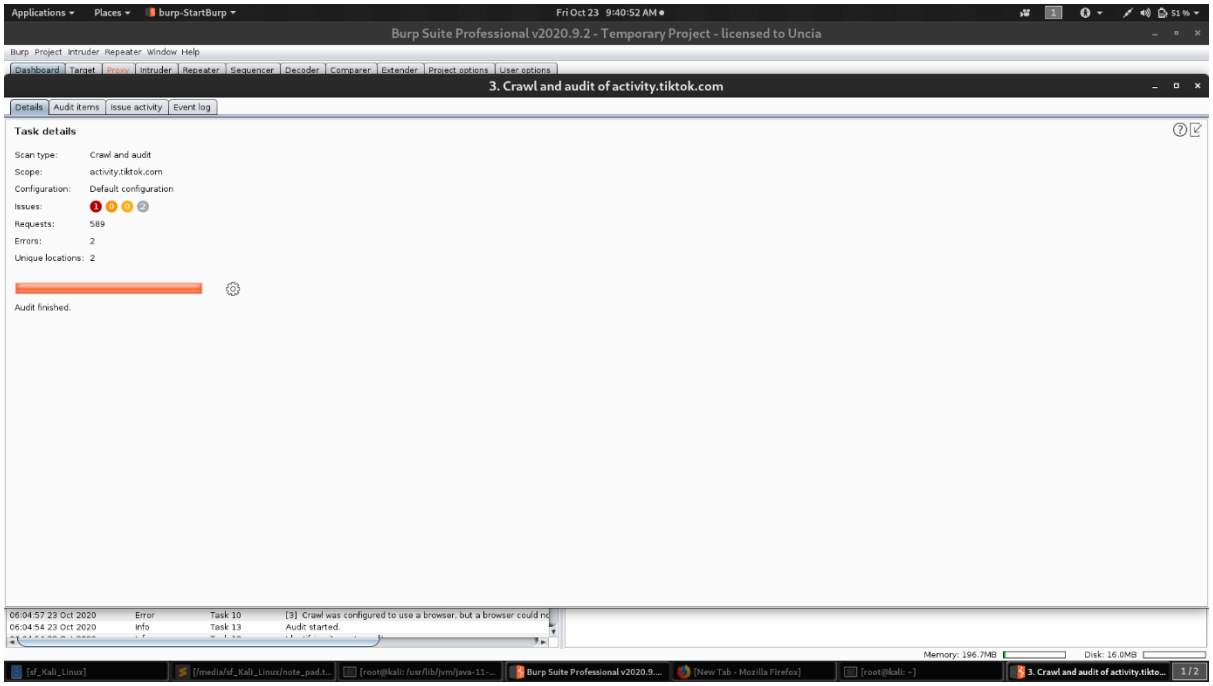
Vulnerability Summary for subdomain

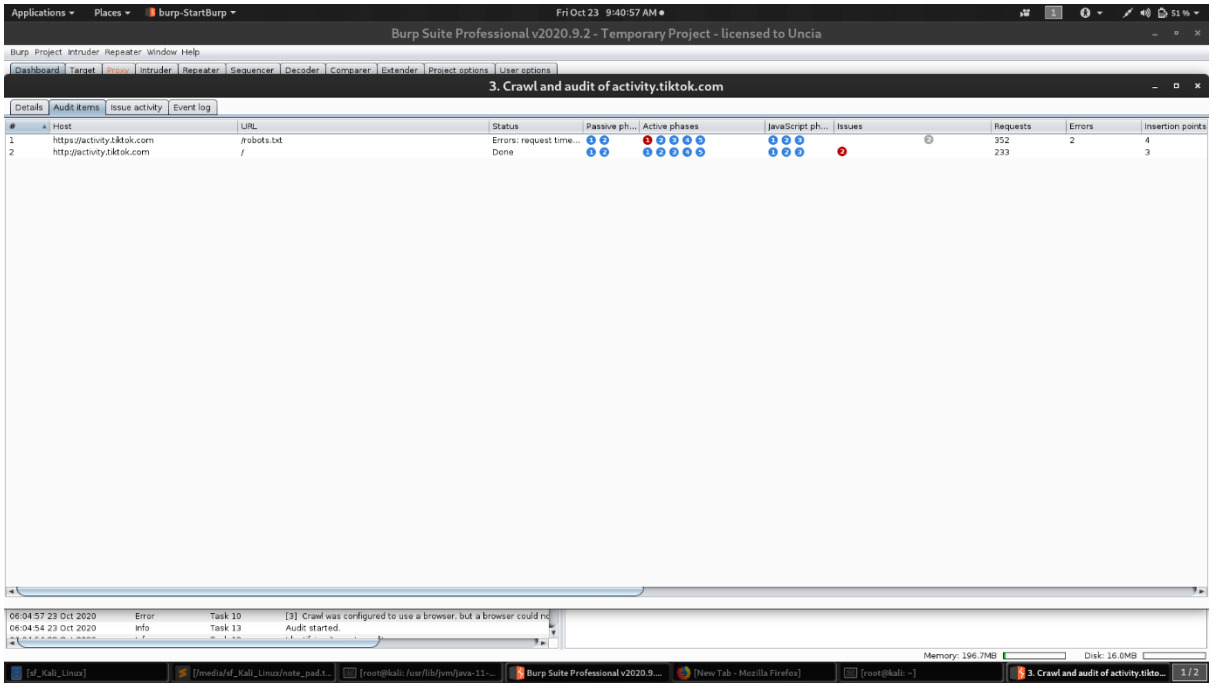
Vulnerabilities By OWASP 2013

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

2 / 20

Burp Suite Scanning





Burp Scanner Report

BURPSUITE PROFESSIONAL

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	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.

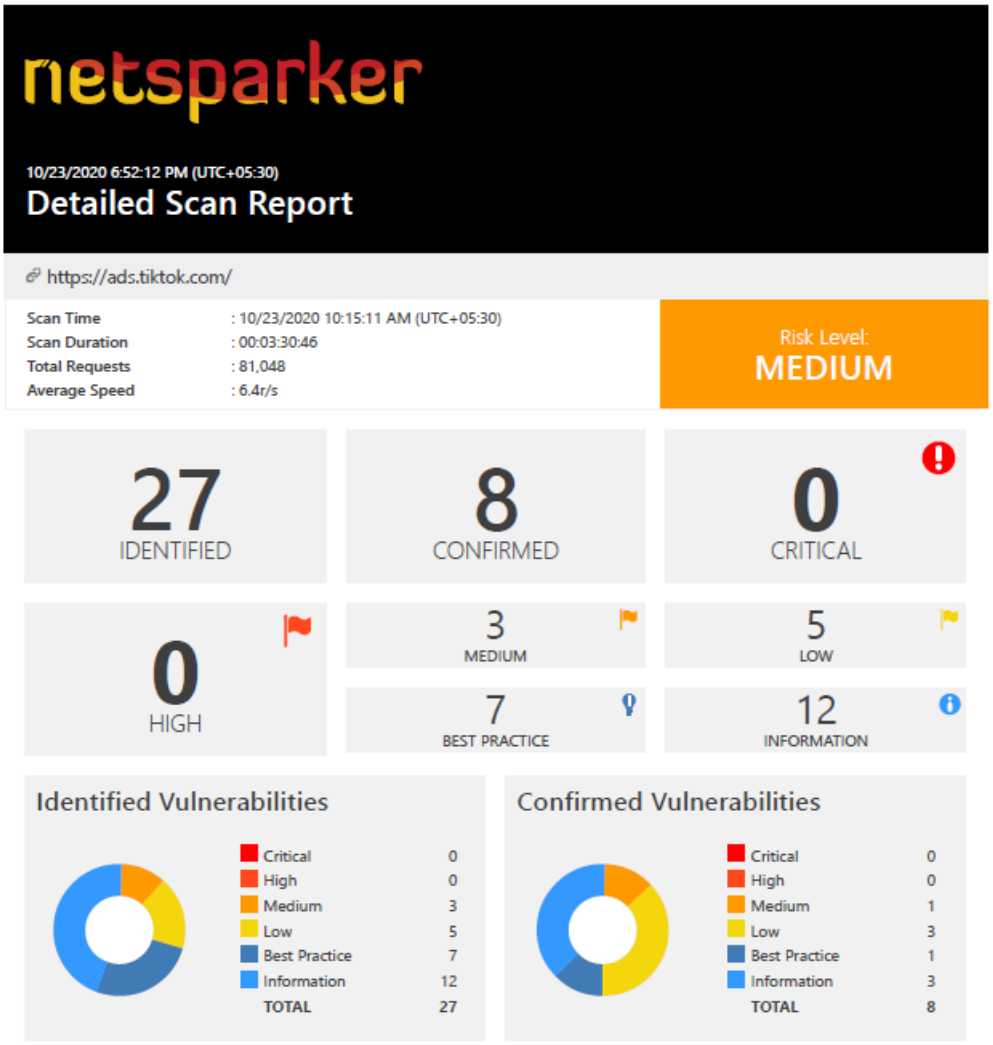
Contents

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



1 / 99

Vulnerability Summary for subdomain

Vulnerability Summary

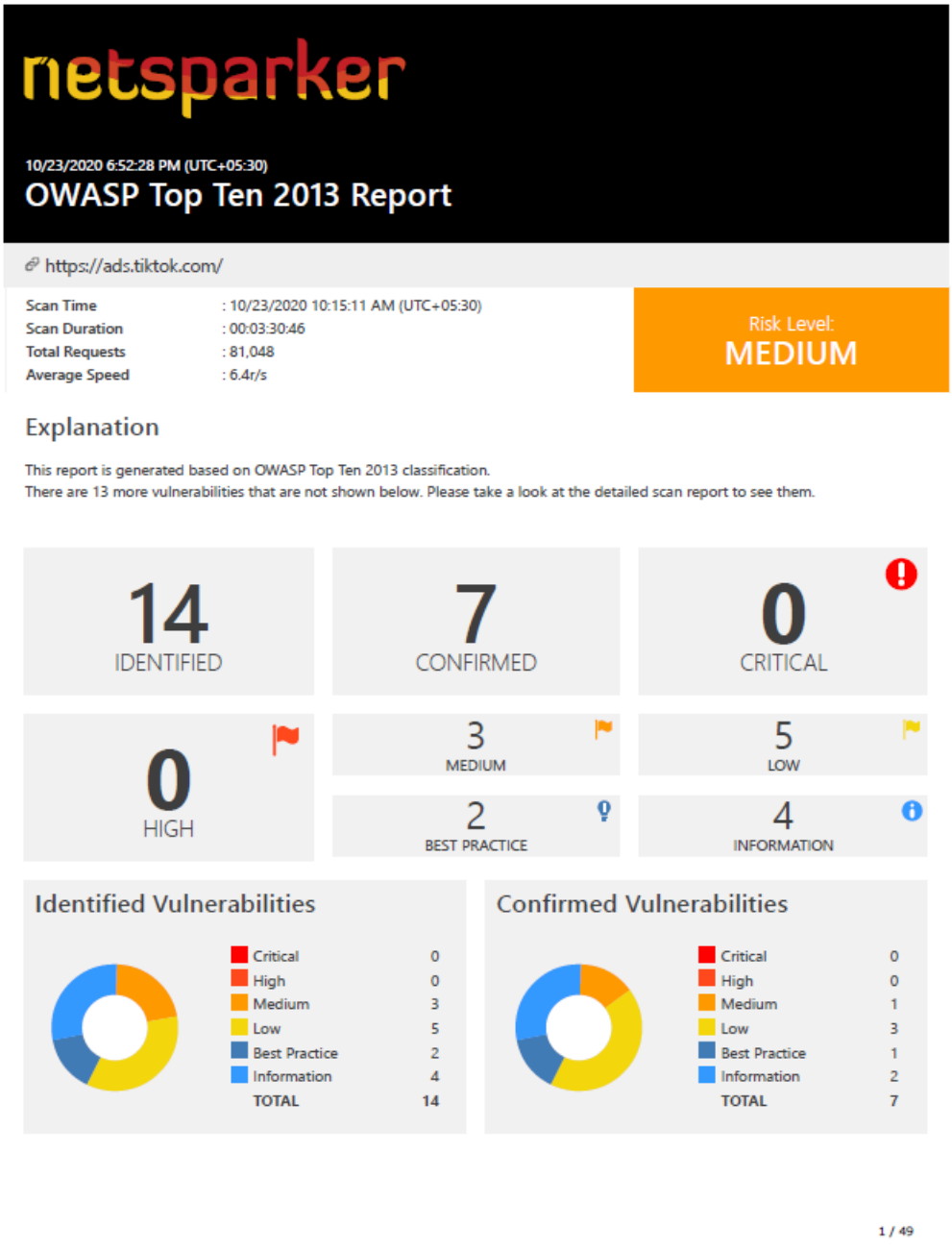
CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ads.tiktok.com/	
	Out-of-date Version (jQuery)	GET	https://ads.tiktok.com/manager/	
	Weak Ciphers Enabled	GET	https://ads.tiktok.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	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.



netsparker

10/23/2020 6:52:28 PM (UTC+05:30)

OWASP Top Ten 2013 Report

https://ads.tiktok.com/

Scan Time	: 10/23/2020 10:15:11 AM (UTC+05:30)
Scan Duration	: 00:03:30:46
Total Requests	: 81,048
Average Speed	: 6.4r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 13 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

14 IDENTIFIED	7 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	5 LOW
	2 BEST PRACTICE	4 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	5
Best Practice	2
Information	4
TOTAL	14

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	3
Best Practice	1
Information	2
TOTAL	7

1 / 49

Vulnerability Summary for subdomain

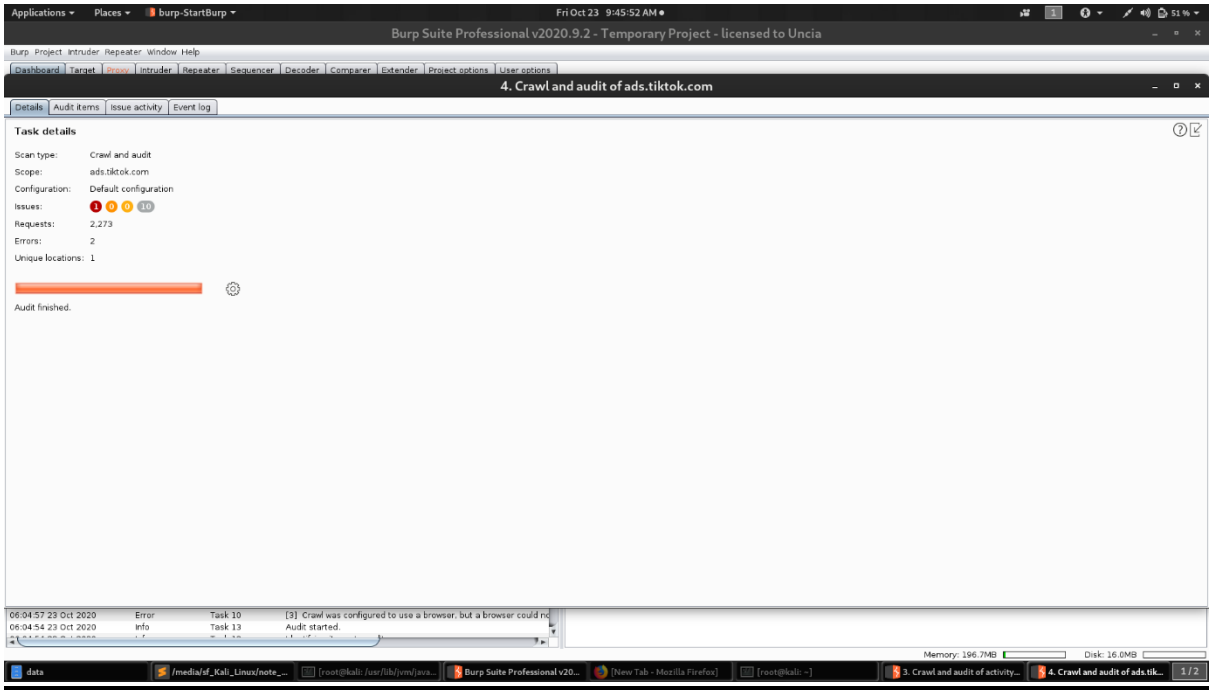
Vulnerabilities By OWASP 2013

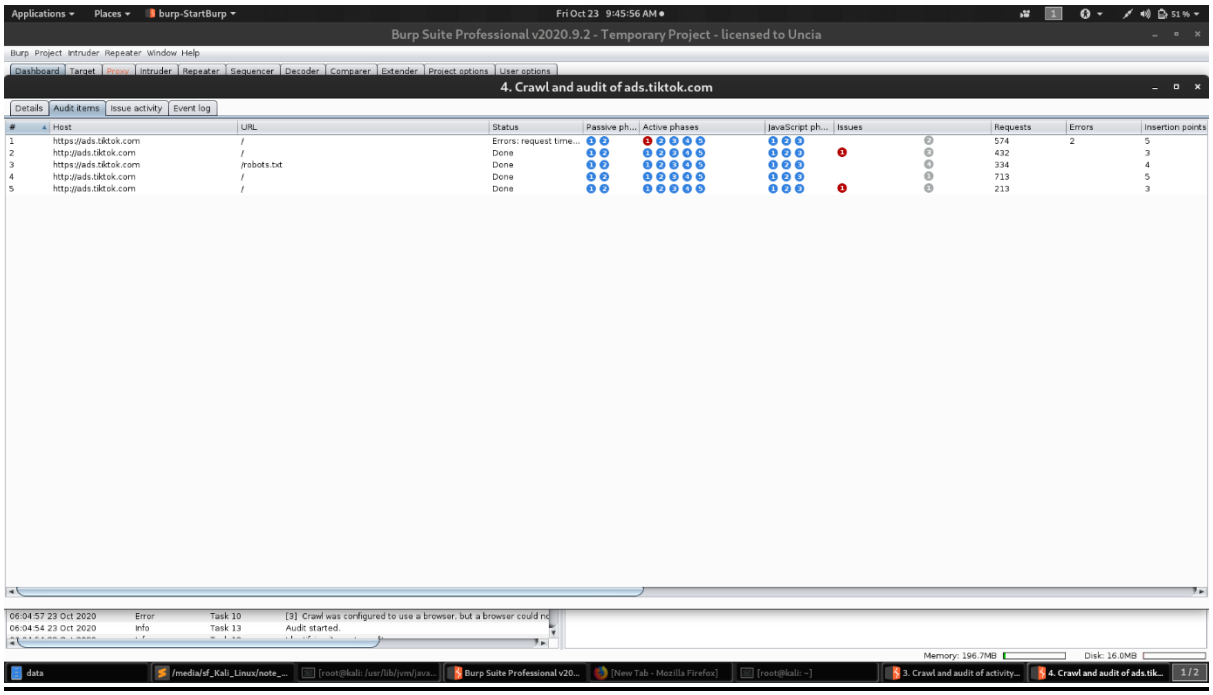
CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A5 - SECURITY MISCONFIGURATION				
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ads.tiktok.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	https://ads.tiktok.com/	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://ads.tiktok.com/homepage/?%2F%2Fr87%3Fcom%2F%3F=%27%20WAITFOR%20DELAY%20%270%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





Burp Scanner Report

BURPSUITE PROFESSIONAL

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

Vulnerabilities

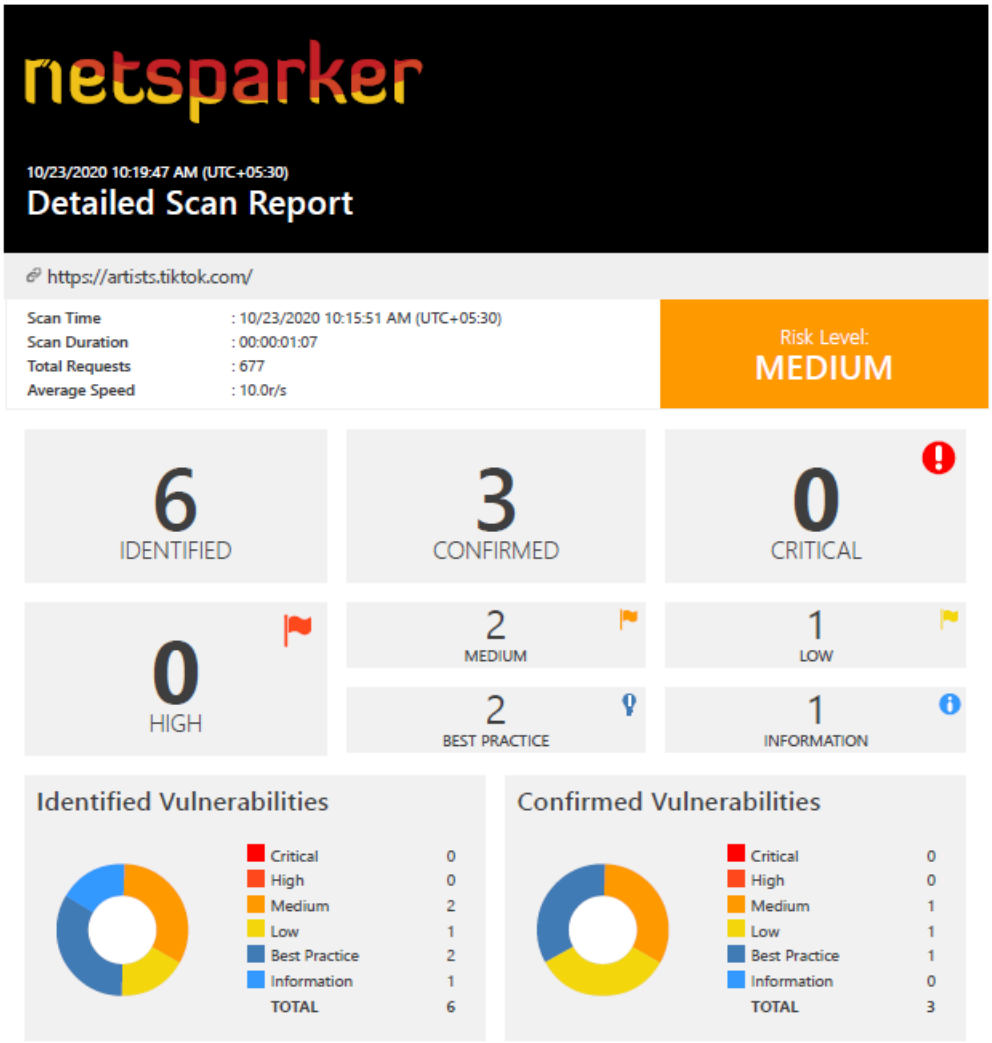
1. External service interaction (DNS) - High
2. Input returned in response (reflected) - Information
    - http://ads.tiktok.com/ [name of an arbitrarily supplied URL parameter]
    - http://ads.tiktok.com/homepage/ [name of an arbitrarily supplied URL parameter]
    - https://ads.tiktok.com/homepage/ [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.



1 / 23

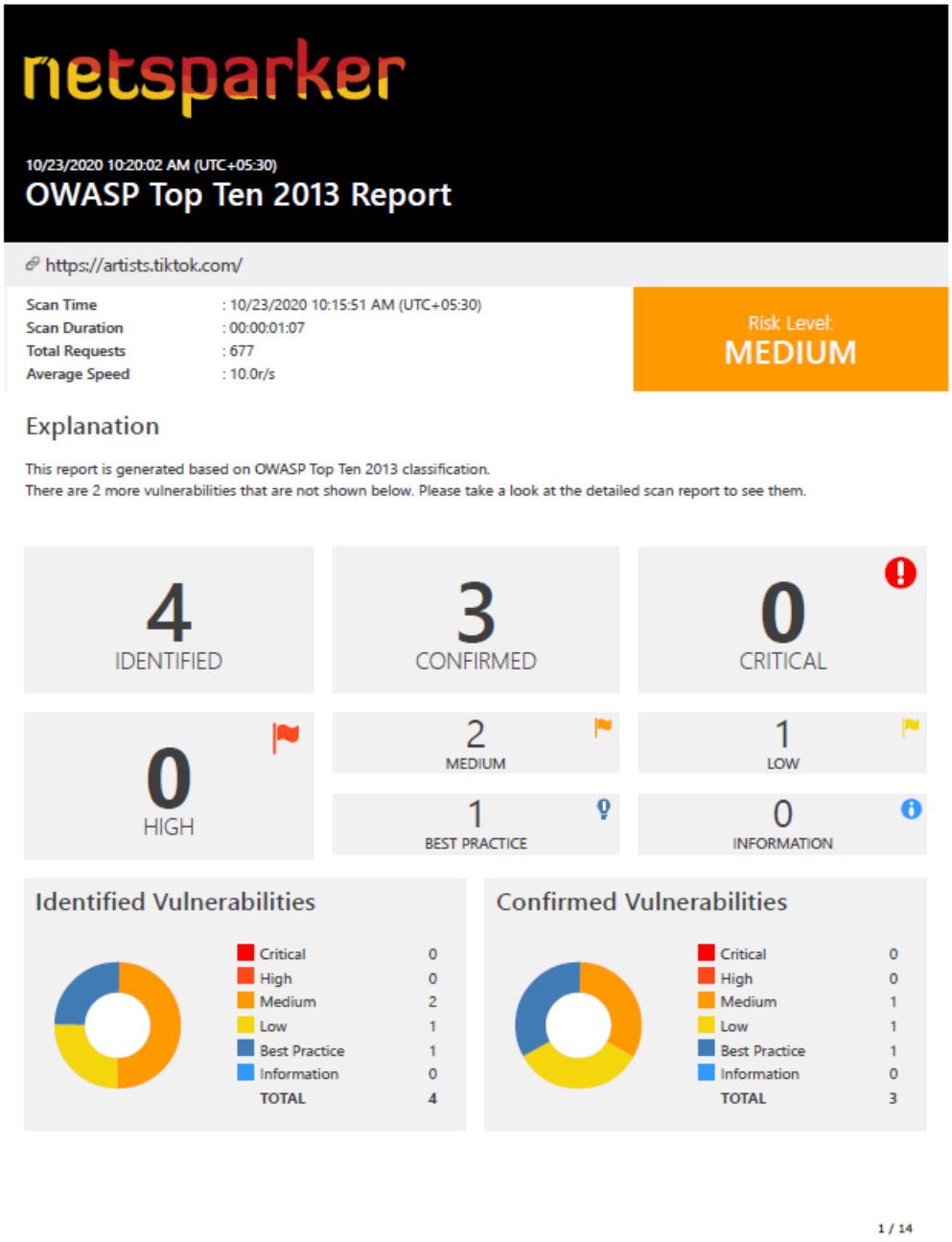
Vulnerability Summary for subdomain

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/	

2 / 23

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 10:20:02 AM (UTC+05:30)

OWASP Top Ten 2013 Report

https://artists.tiktok.com/

Scan Time	: 10/23/2020 10:15:51 AM (UTC+05:30)
Scan Duration	: 00:00:01:07
Total Requests	: 677
Average Speed	: 10.0r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 2 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

4 IDENTIFIED	3 CONFIRMED	0 CRITICAL
0 HIGH	2 MEDIUM	1 LOW
	1 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities

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

Confirmed Vulnerabilities

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

1 / 14

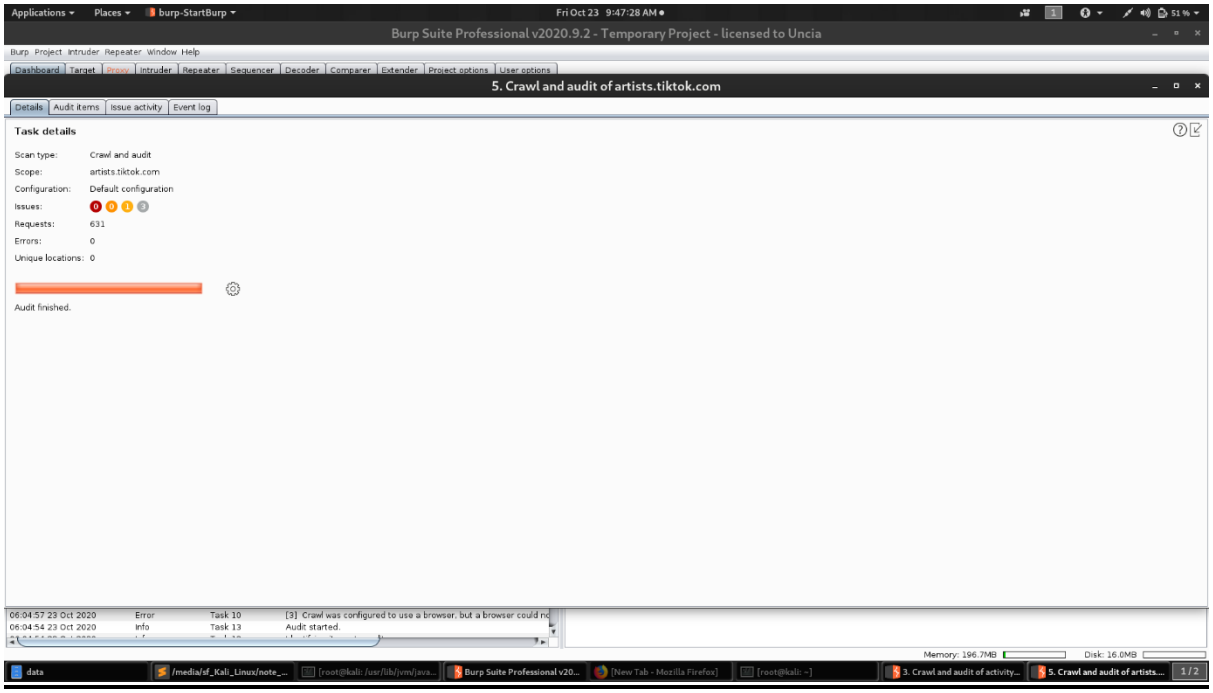
Vulnerability Summary for subdomain

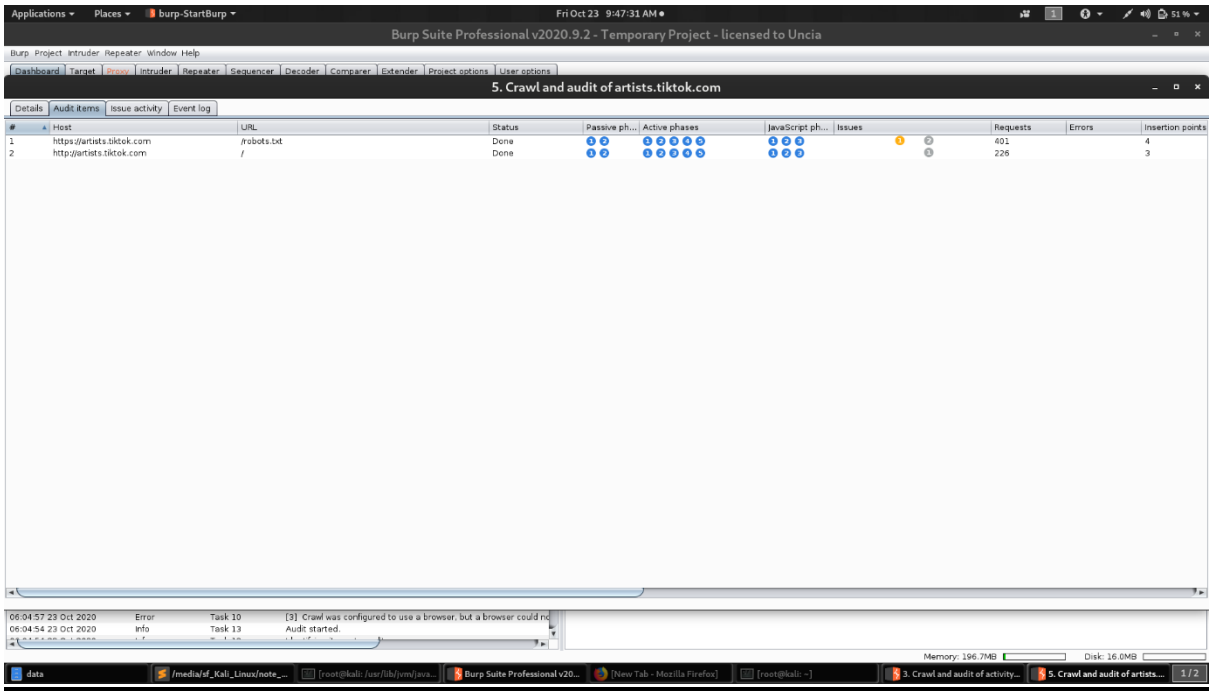
Vulnerabilities By OWASP 2013

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

2 / 14

Burp Suite Scanning





Burp Scanner Report

BURPSUITE PROFESSIONAL

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.

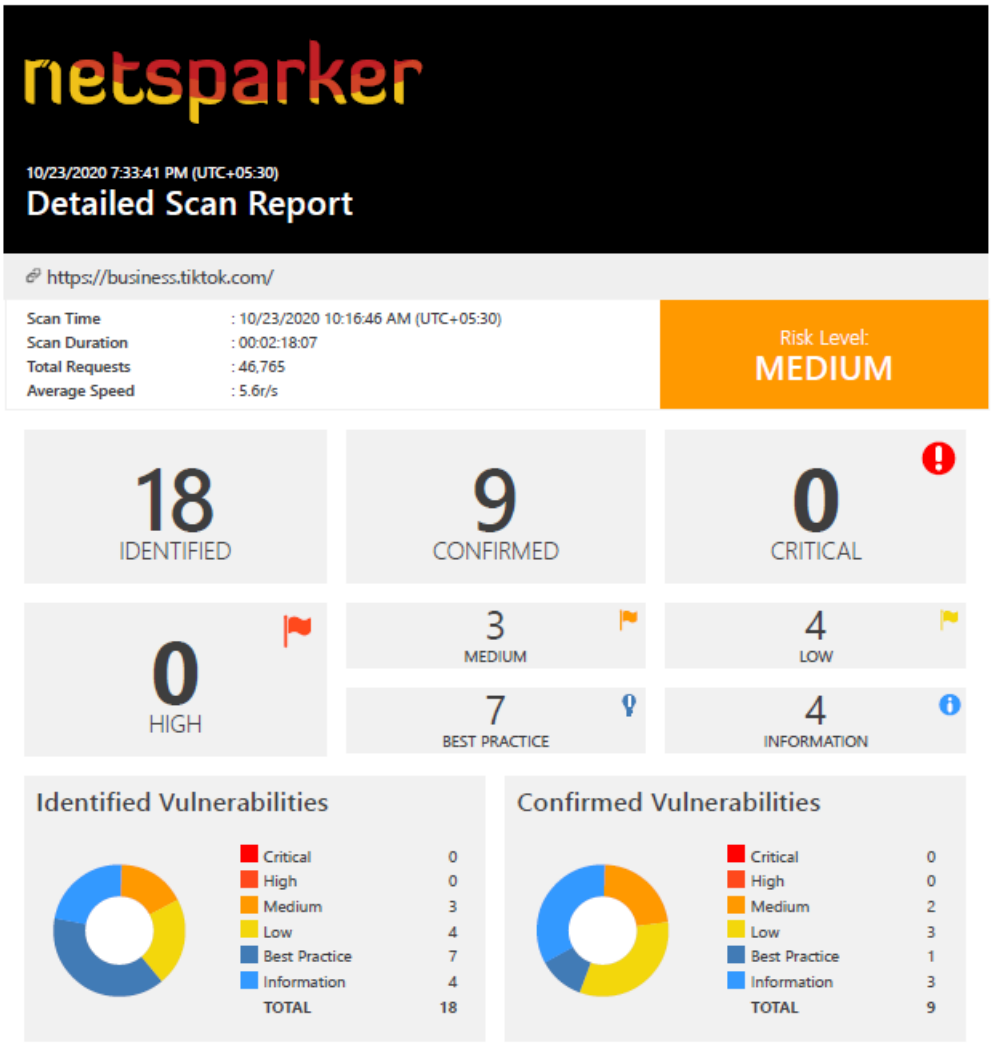
Contents

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.



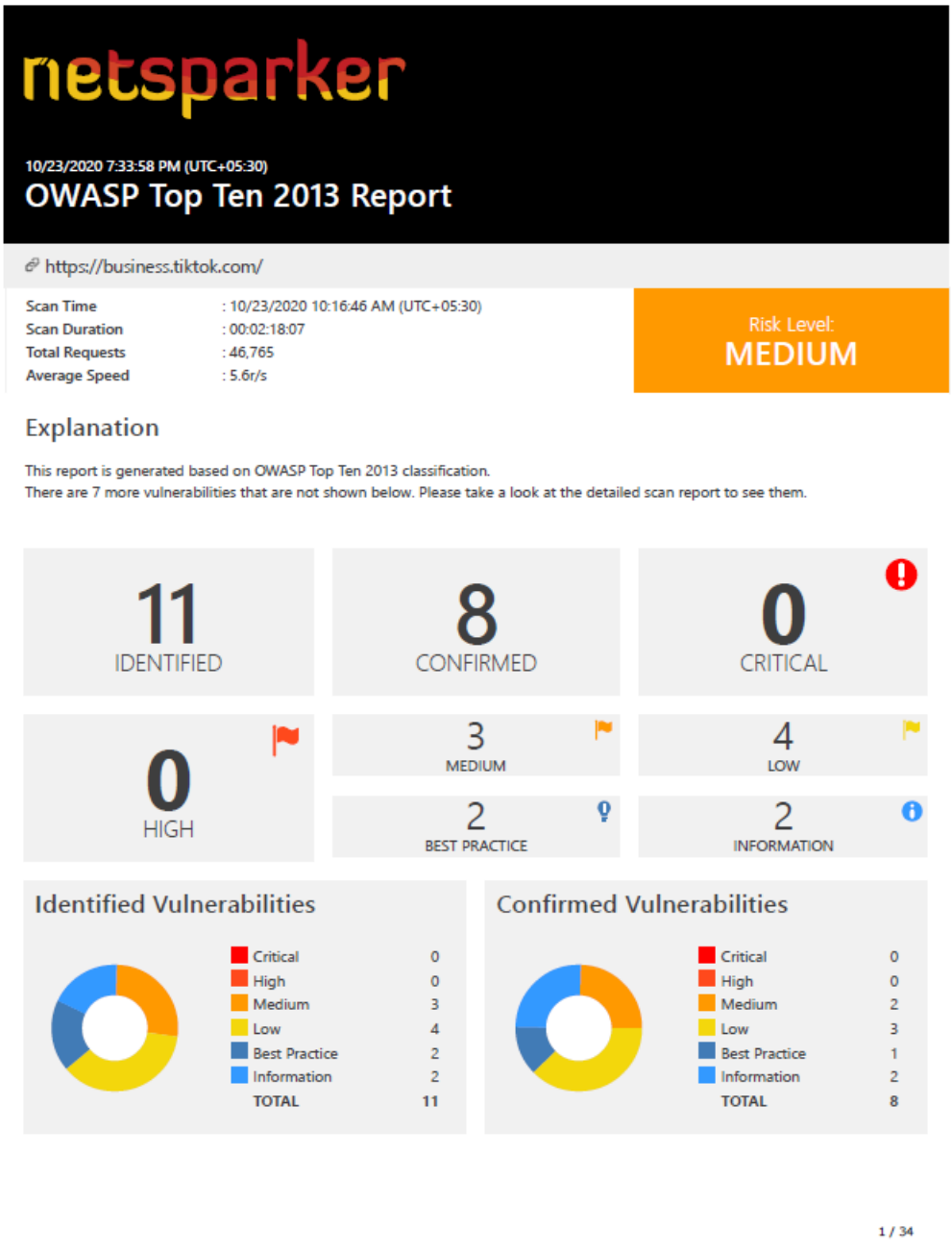
Vulnerability Summary for subdomain

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	: 5.6r/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

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

Confirmed Vulnerabilities

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

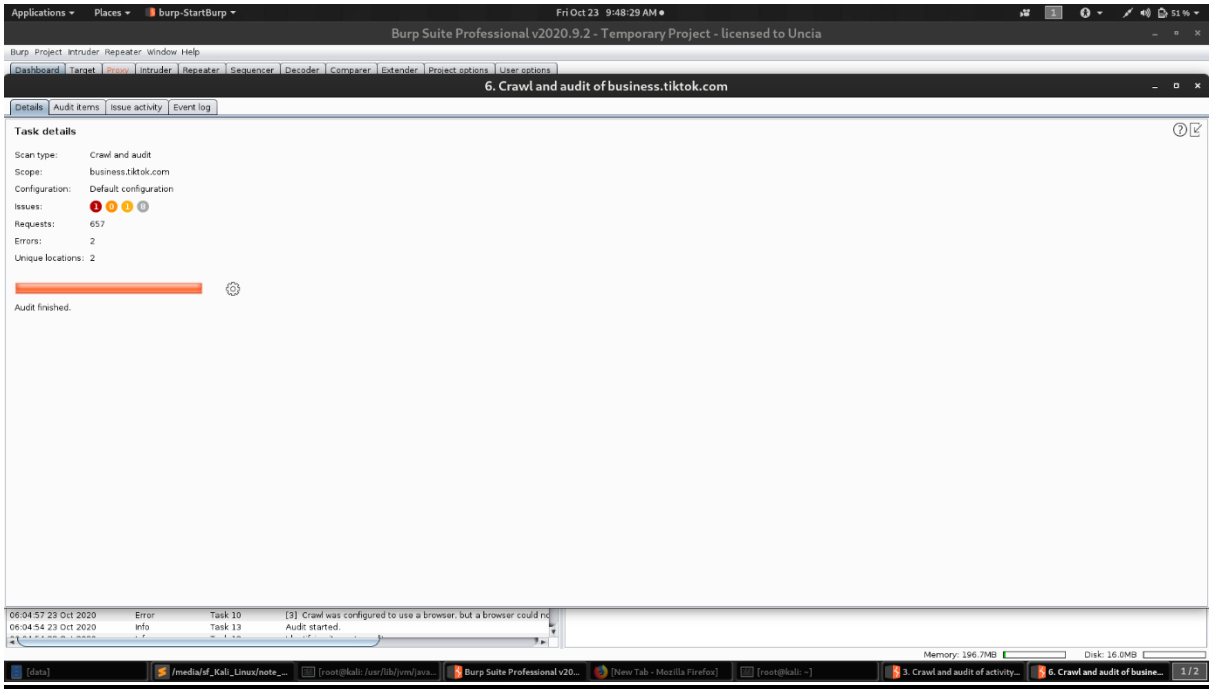
1 / 34

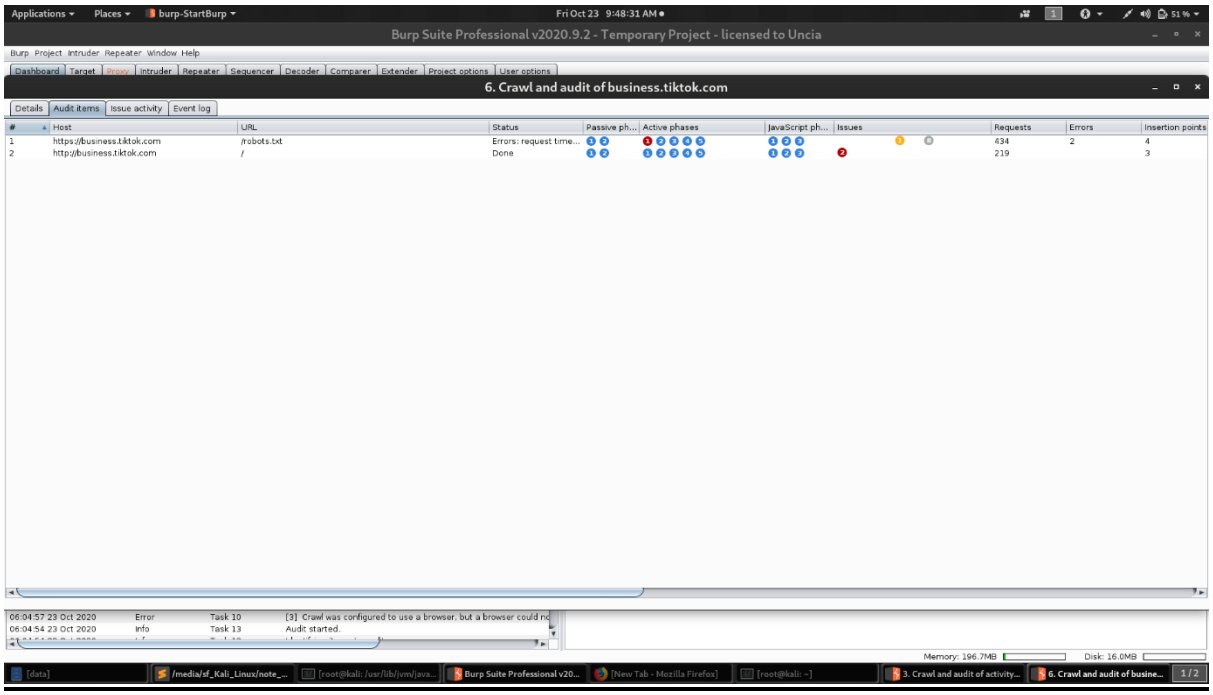
Vulnerability Summary for subdomain

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





Burp Scanner Report

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			
	Certain	Firm	Tentative	Total
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.

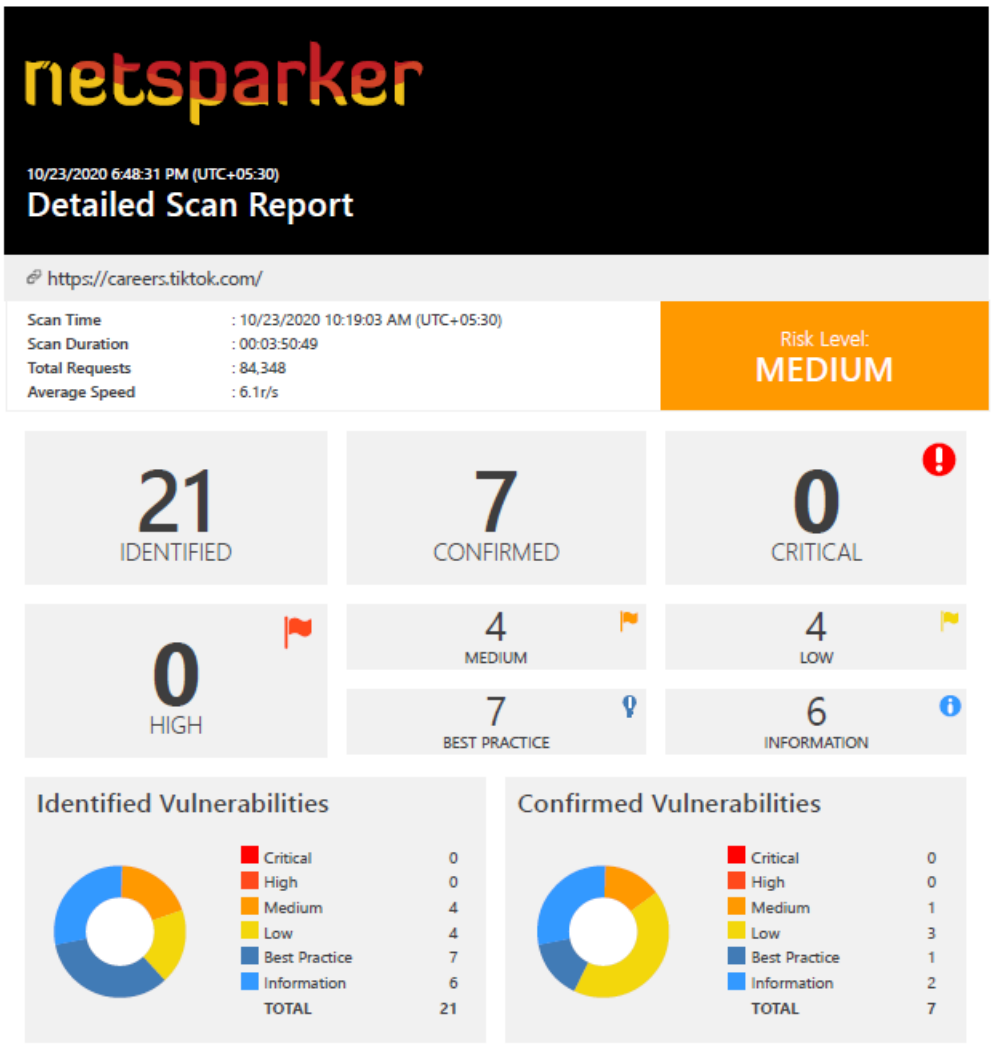
Contents

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.



1 / 76

Vulnerability Summary for subdomain

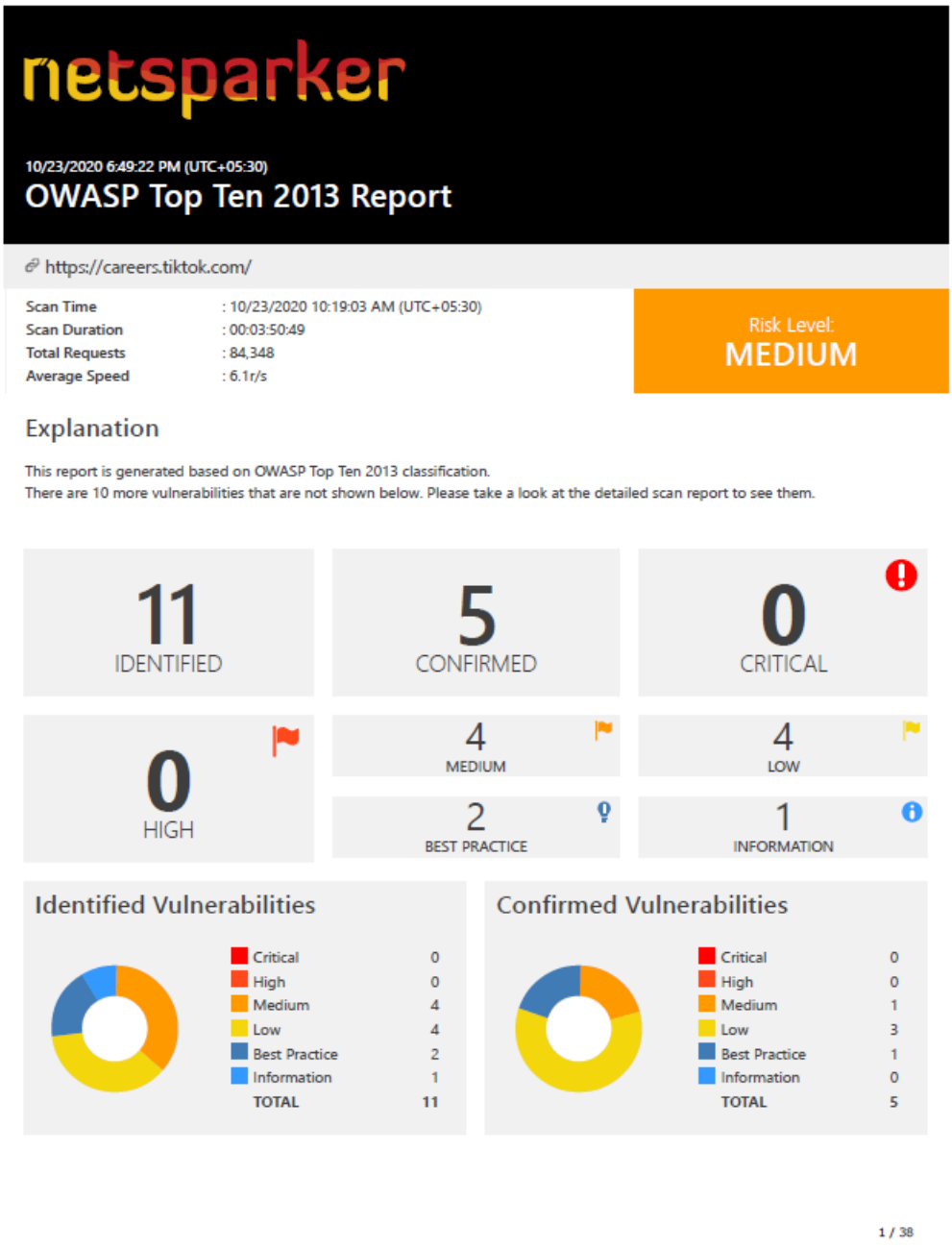
Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=%27%3e%3cnet%20sparker%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%20sparker%3dnetsparker(0x0031F1)%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	ns
	Forbidden Resource	GET	https://careers.tiktok.com/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000184)%3C/scRipt%3E	nsextt
	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.



netsparker

10/23/2020 6:49:22 PM (UTC+05:30)

OWASP Top Ten 2013 Report

https://careers.tiktok.com/

Scan Time	: 10/23/2020 10:19:03 AM (UTC+05:30)
Scan Duration	: 00:03:50:49
Total Requests	: 84,348
Average Speed	: 6.1r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 10 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

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

Identified Vulnerabilities

Critical	0
High	0
Medium	4
Low	4
Best Practice	2
Information	1
TOTAL	11

Confirmed Vulnerabilities

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

1 / 38

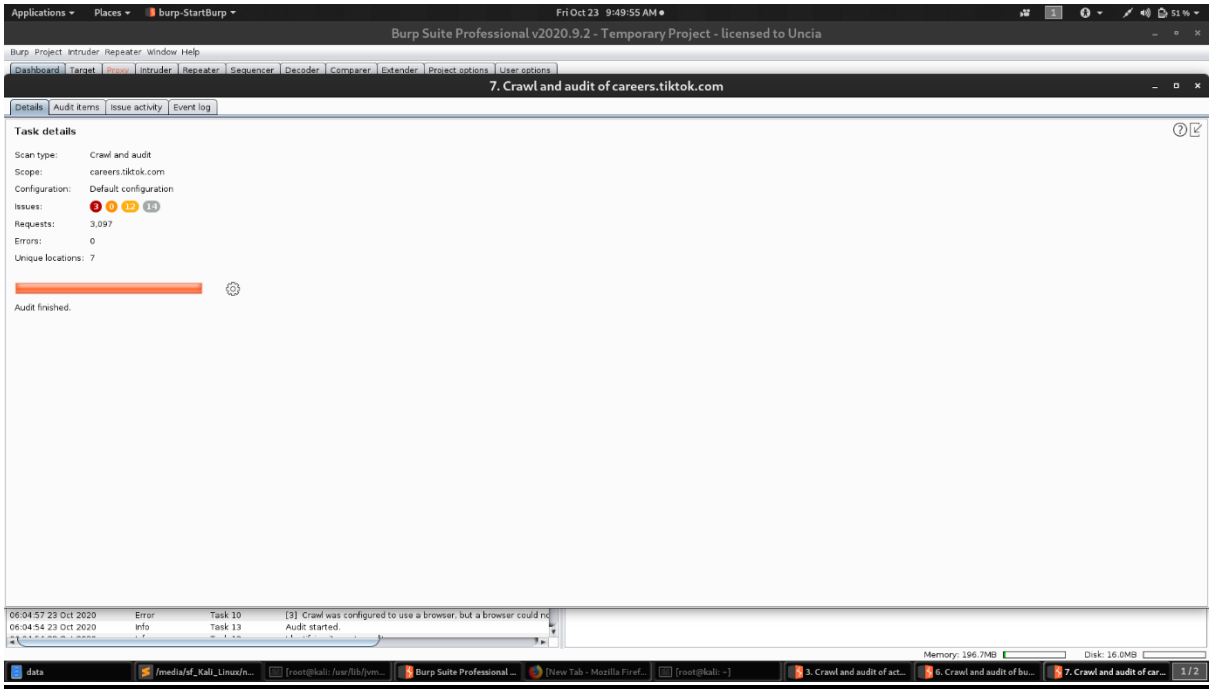
Vulnerability Summary for subdomain

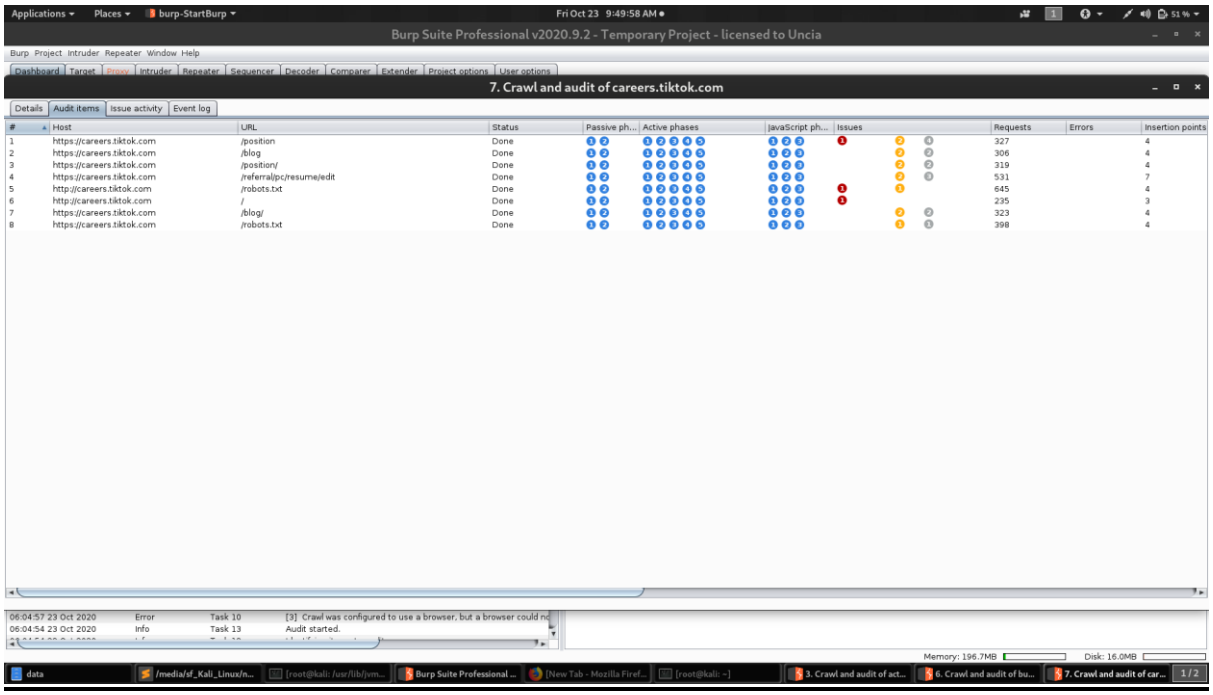
Vulnerabilities By OWASP 2013

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%3dnetsparker(0x0031F1)%3e	MEDIUM
	[Possible] Cross-site Scripting	GET	https://careers.tiktok.com/api/v1/public/cms/ttevent/list?currentPage=%27%3e%3cnet%20sparker%3dnetsparker(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

2 / 38

Burp Suite Scanning





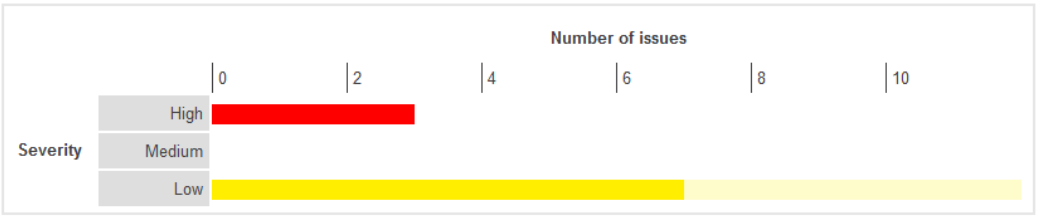
Burp Scanner Report

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			
	Certain	Firm	Tentative	Total
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

Contents

Vulnerabilities

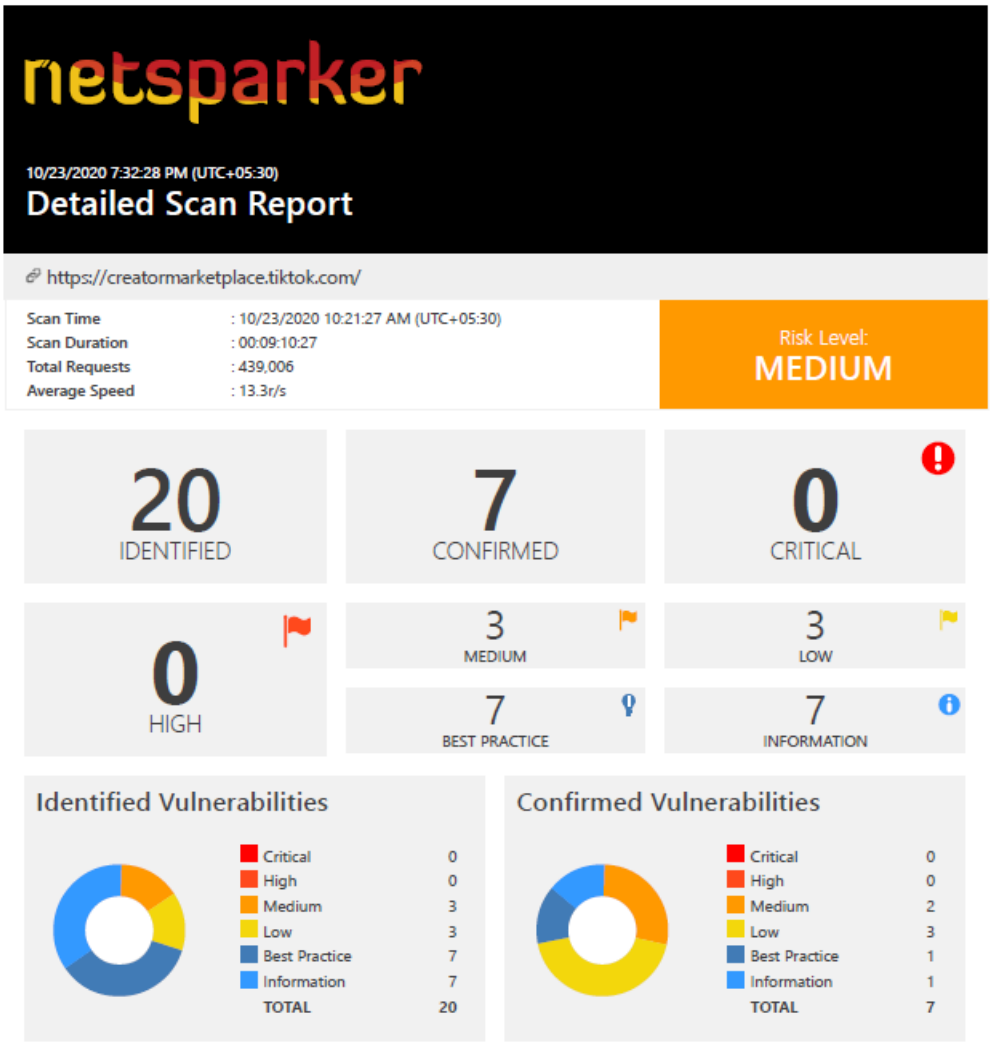
1. External service interaction (DNS) – High
   - http://careers.tiktok.com/
   - http://careers.tiktok.com/robots.txt
   - https://careers.tiktok.com/position
2. Open redirection (DOM-based) – Low
   - https://careers.tiktok.com/blog
   - https://careers.tiktok.com/blog/
   - https://careers.tiktok.com/position
   - 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


netsparker

10/23/2020 7:32:28 PM (UTC+05:30)

Detailed Scan Report

https://creatormarketplace.tiktok.com/

Scan Time	: 10/23/2020 10:21:27 AM (UTC+05:30)
Scan Duration	: 00:09:10:27
Total Requests	: 439,006
Average Speed	: 13.3r/s

Risk Level: MEDIUM

20 IDENTIFIED	7 CONFIRMED	0 CRITICAL	
0 HIGH	3 MEDIUM	3 LOW	
	7 BEST PRACTICE	7 INFORMATION	

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	3
Best Practice	7
Information	7
TOTAL	20

Confirmed Vulnerabilities

Critical	0
High	0
Medium	2
Low	3
Best Practice	1
Information	1
TOTAL	7

1 / 75

Vulnerability Summary for subdomain

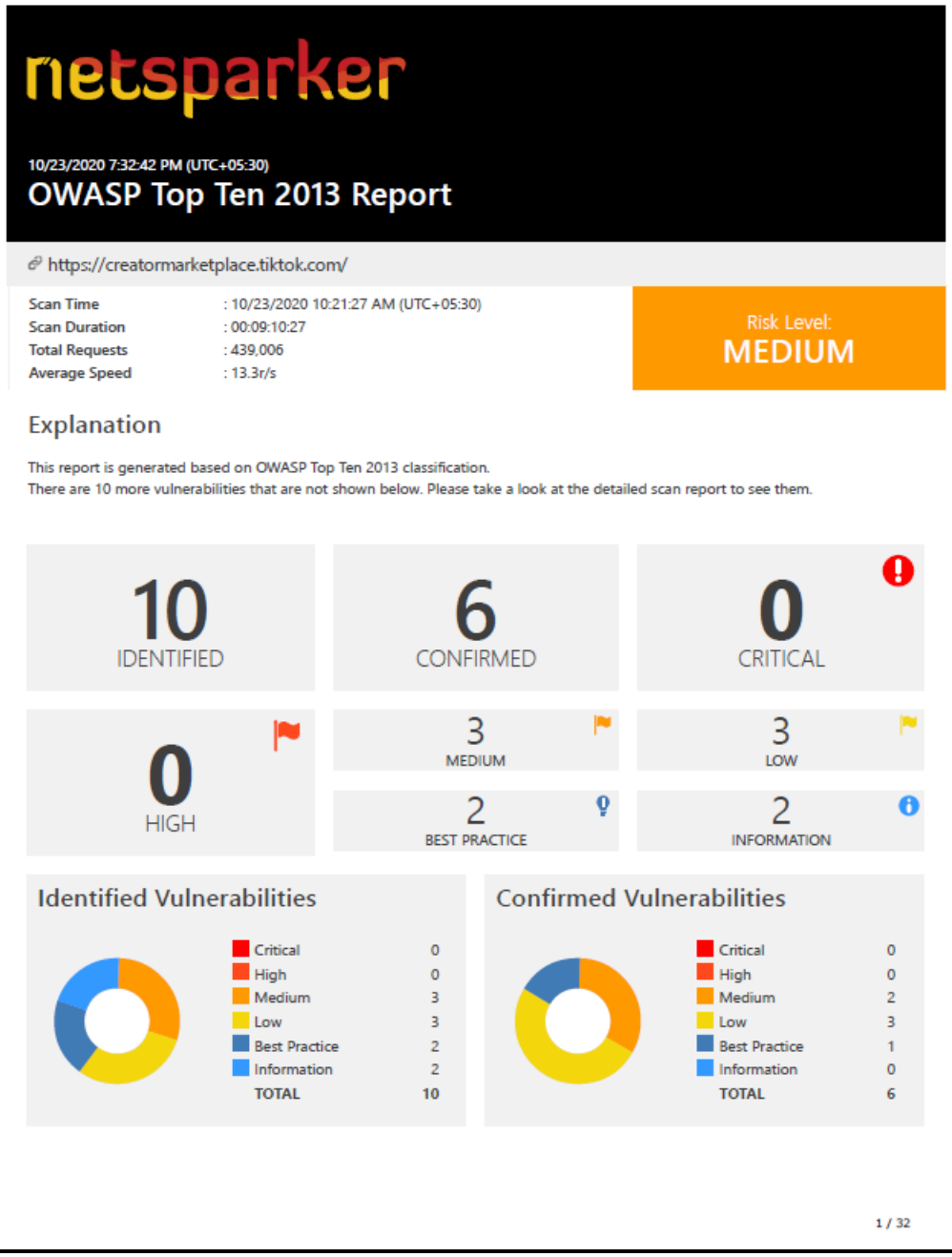
Vulnerability Summary

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.



netsparker

10/23/2020 7:32:42 PM (UTC+05:30)

OWASP Top Ten 2013 Report

https://creatormarketplace.tiktok.com/

Scan Time	: 10/23/2020 10:21:27 AM (UTC+05:30)
Scan Duration	: 00:09:10:27
Total Requests	: 439,006
Average Speed	: 13.3r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 10 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

10 IDENTIFIED

6 CONFIRMED

0 CRITICAL

0 HIGH

3 MEDIUM

3 LOW

2 BEST PRACTICE

2 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	3
Best Practice	2
Information	2
TOTAL	10

Confirmed Vulnerabilities

Critical	0
High	0
Medium	2
Low	3
Best Practice	1
Information	0
TOTAL	6

1 / 32

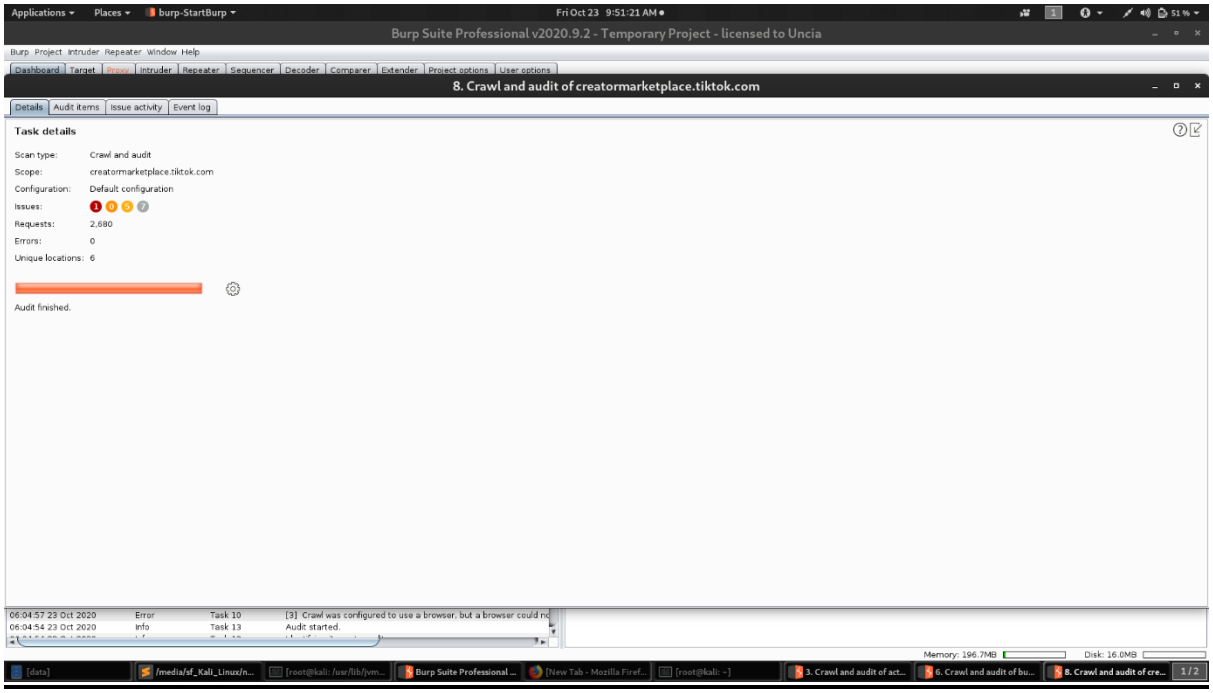
Vulnerability Summary for subdomain

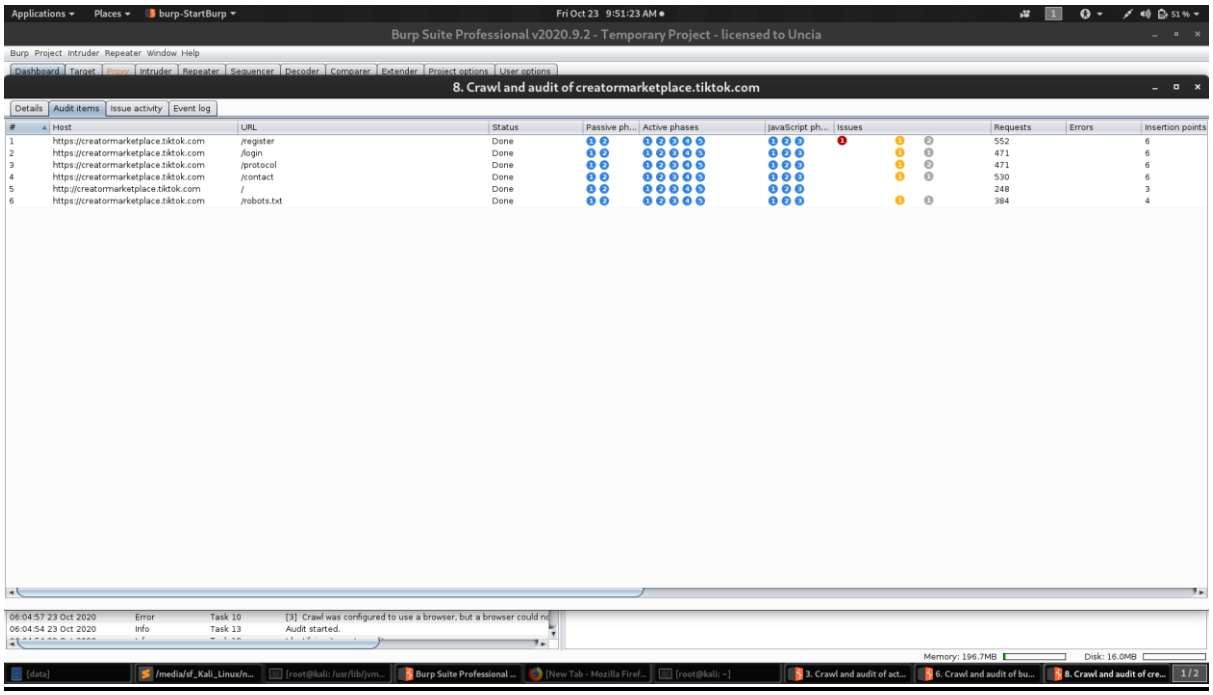
Vulnerabilities By OWASP 2013

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





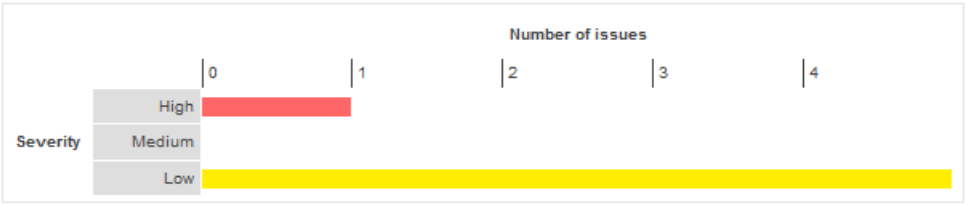
Burp Scanner Report

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			
	Certain	Firm	Tentative	Total
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.



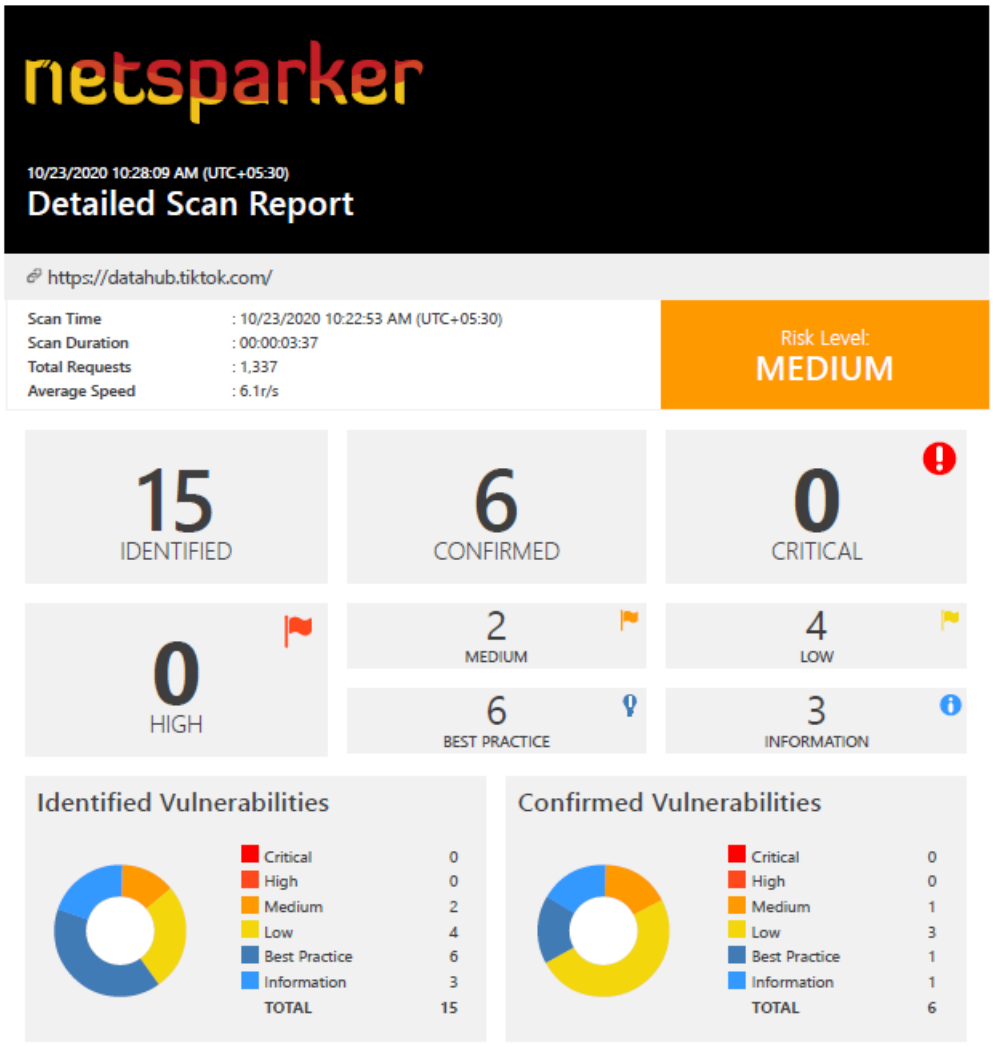
Contents

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



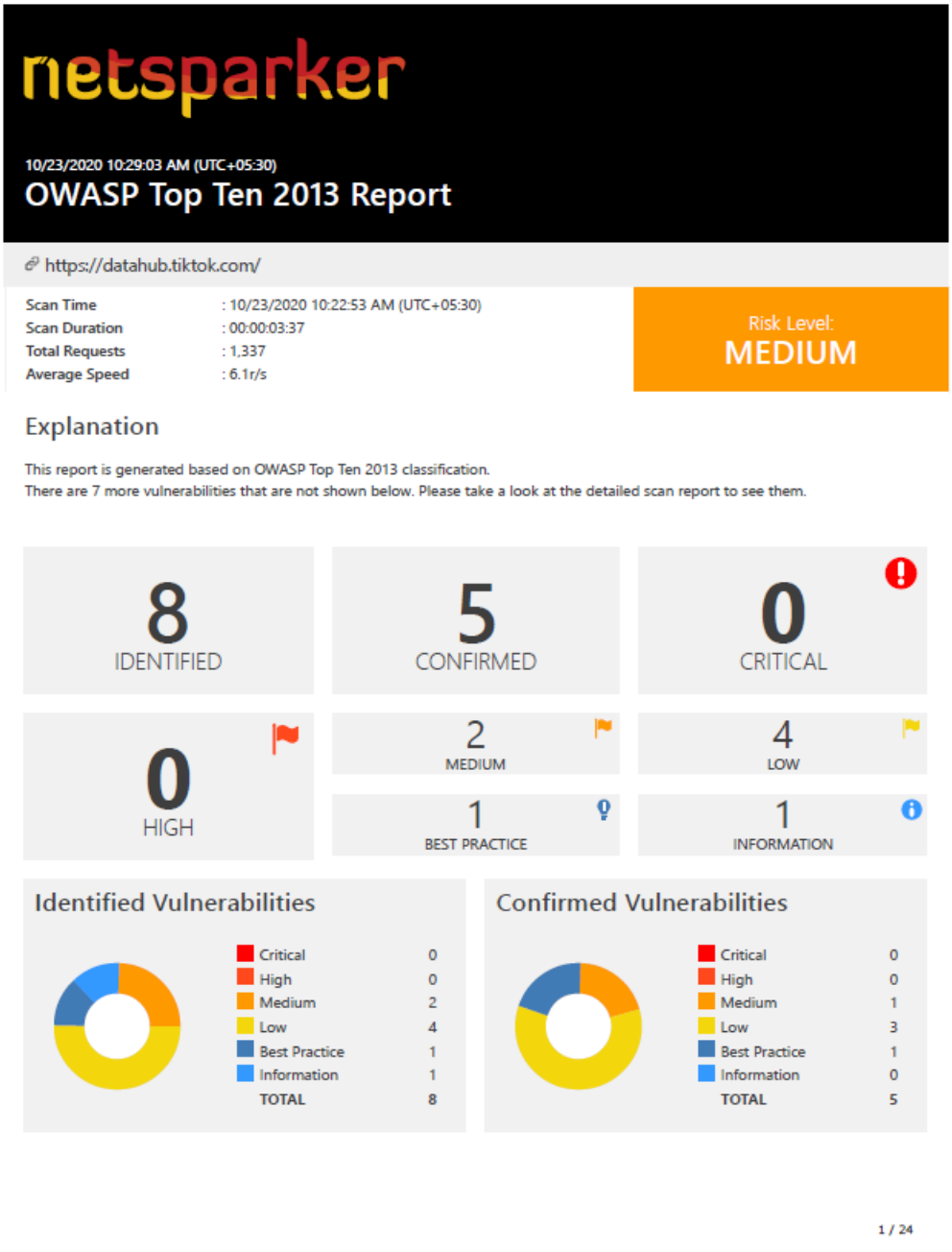
Vulnerability Summary for subdomain

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

1 / 24

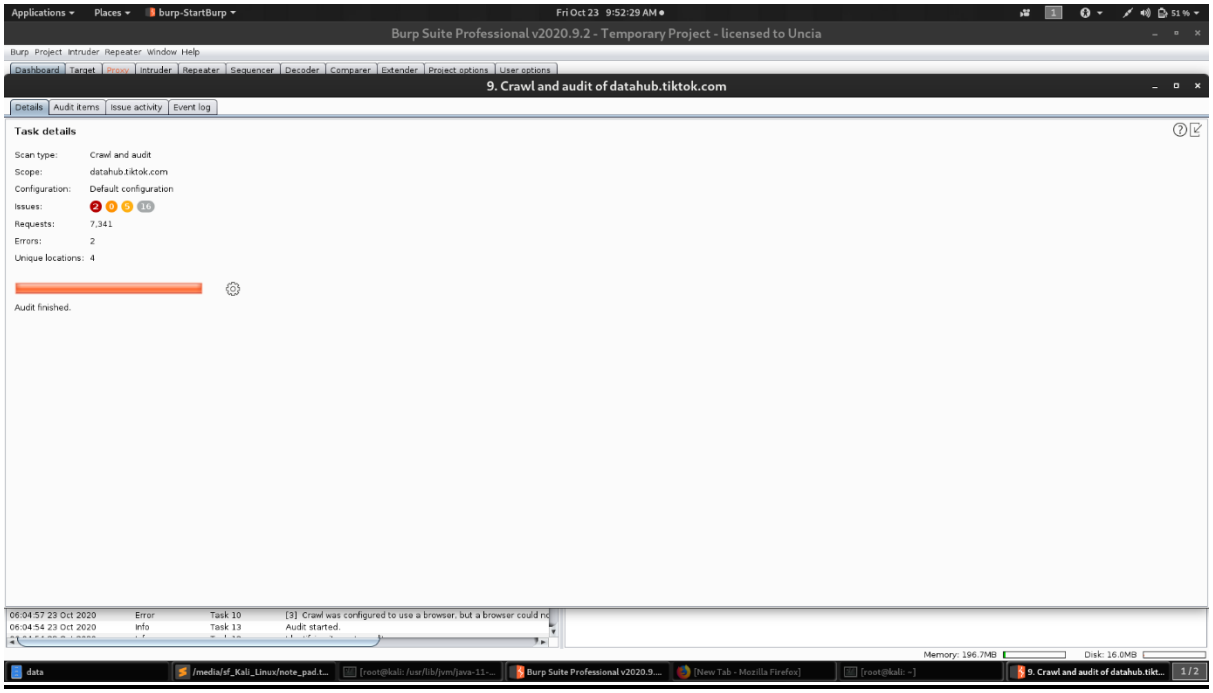
Vulnerability Summary for subdomain

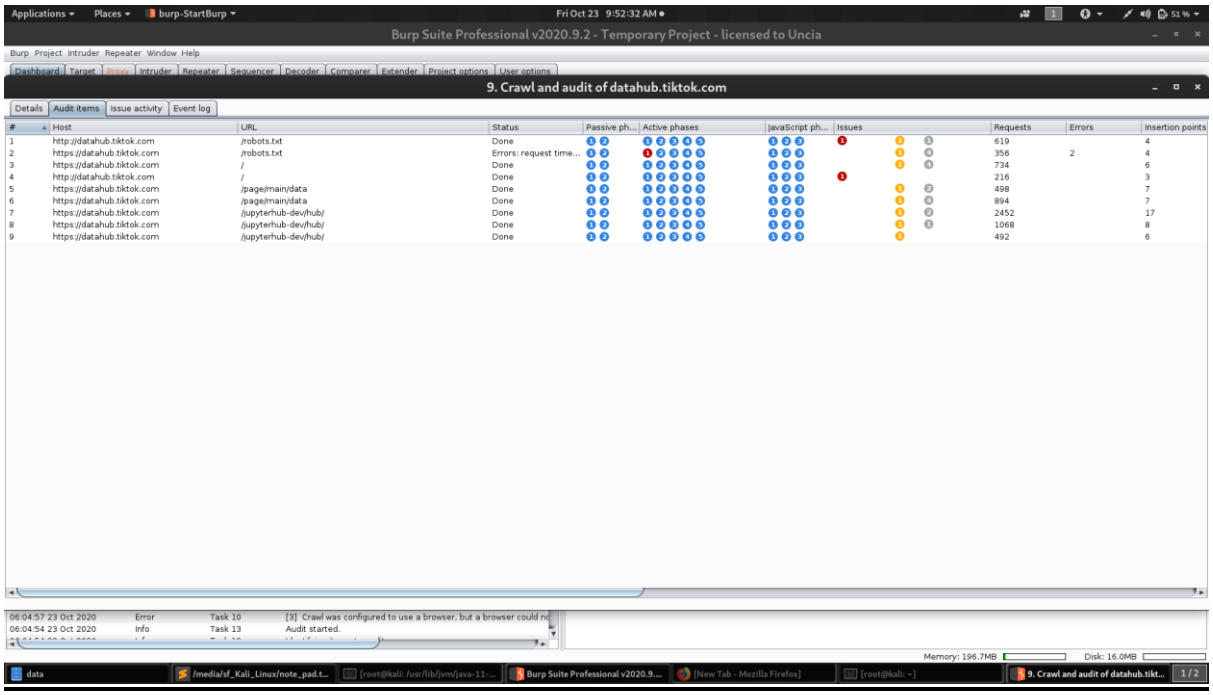
Vulnerabilities By OWASP 2013

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

2 / 24

Burp Suite Scanning





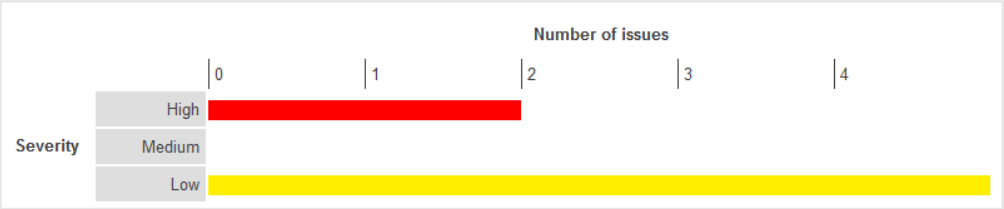
Burp Scanner Report

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	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

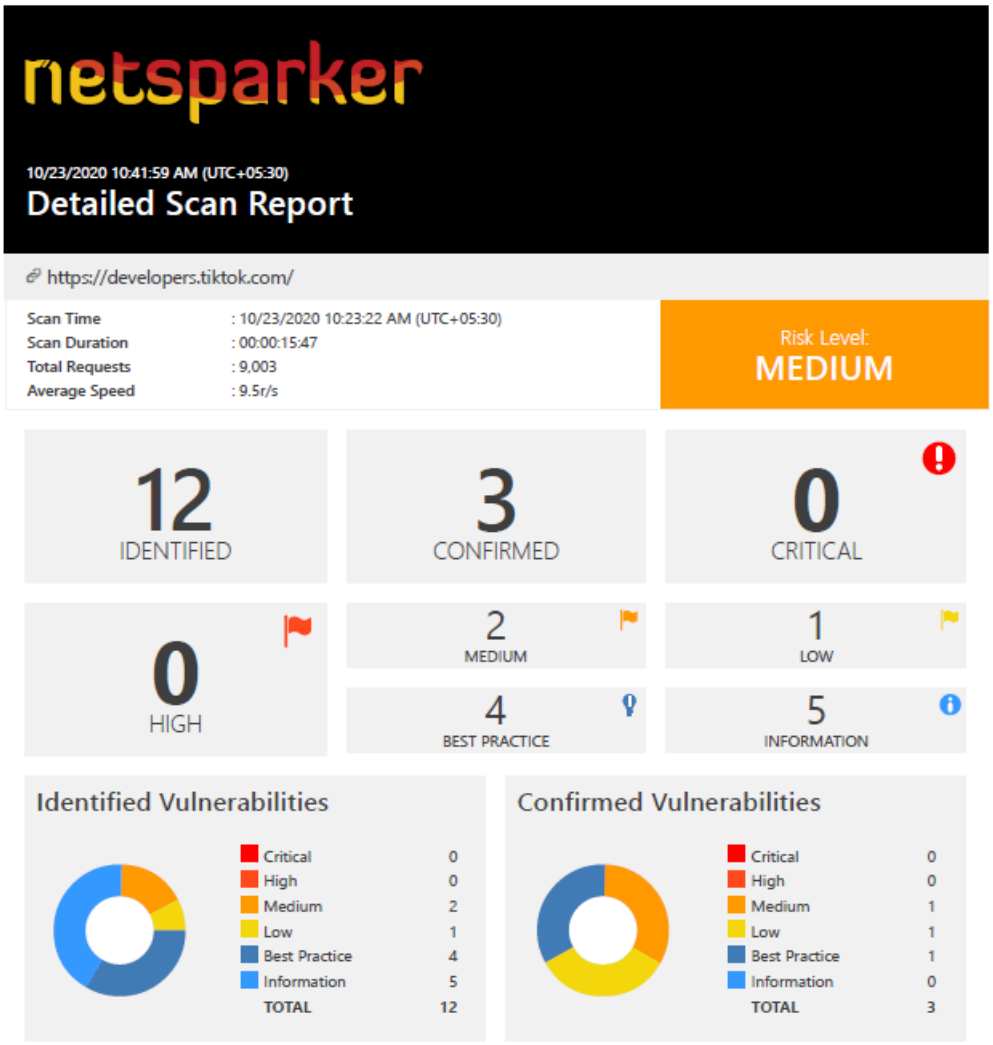
Contents

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



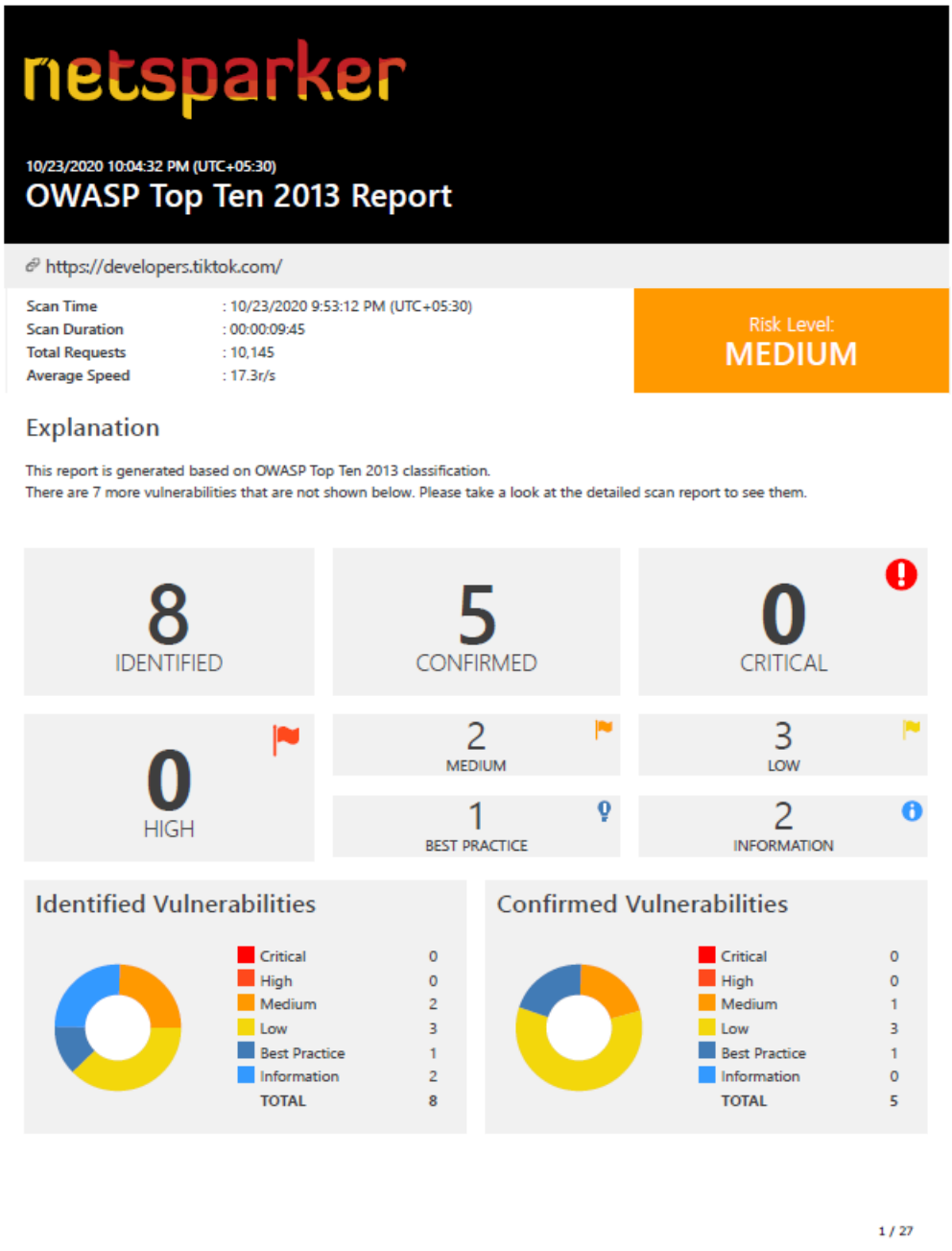
Vulnerability Summary for subdomain

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/confirm/	
	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/	

2 / 43

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 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

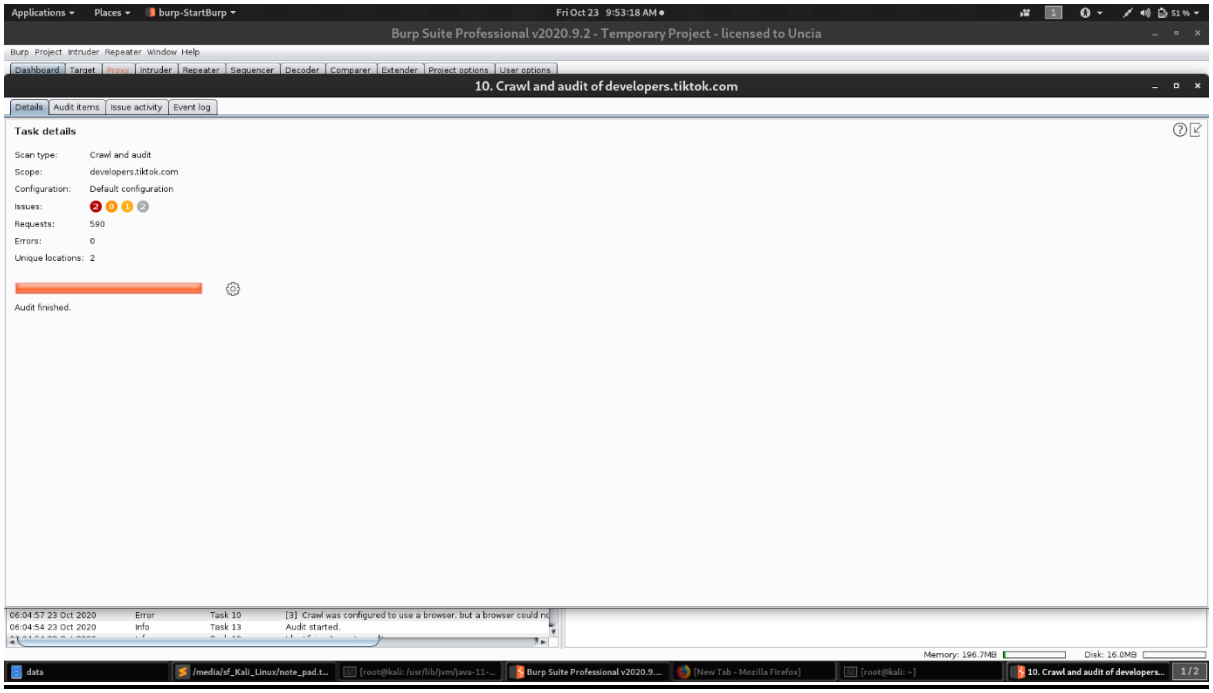
1 / 27

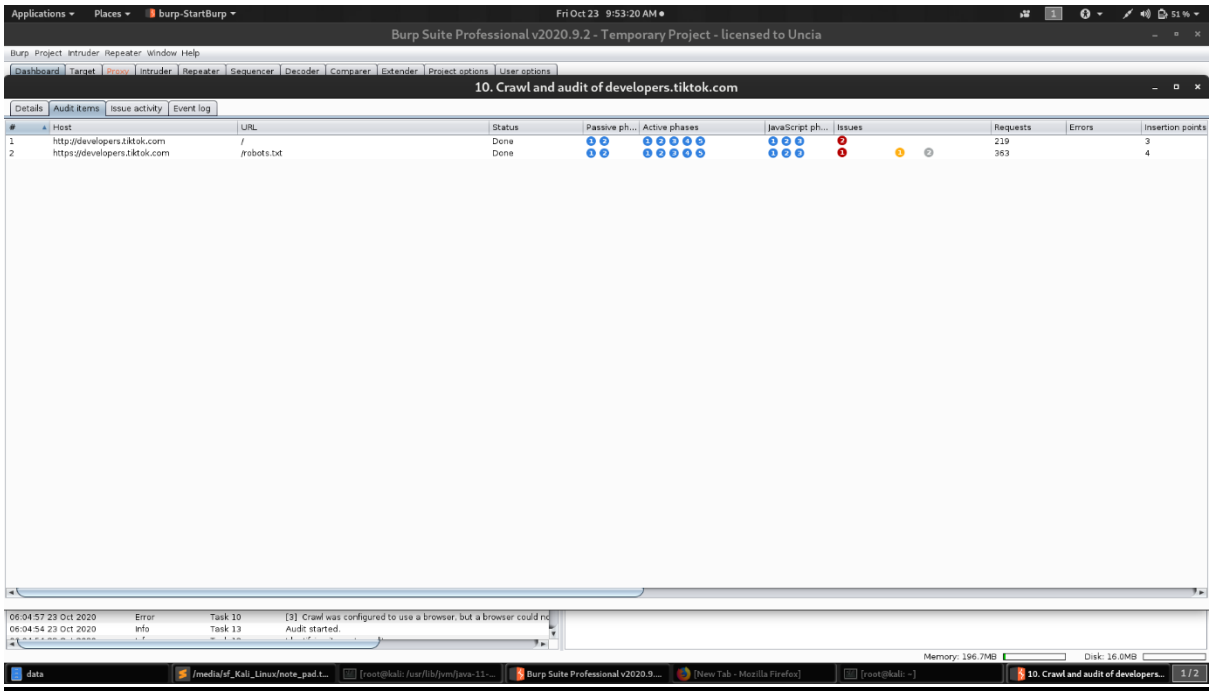
Vulnerability Summary for subdomain

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





Burp Scanner Report

BURPSUITE PROFESSIONAL

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.

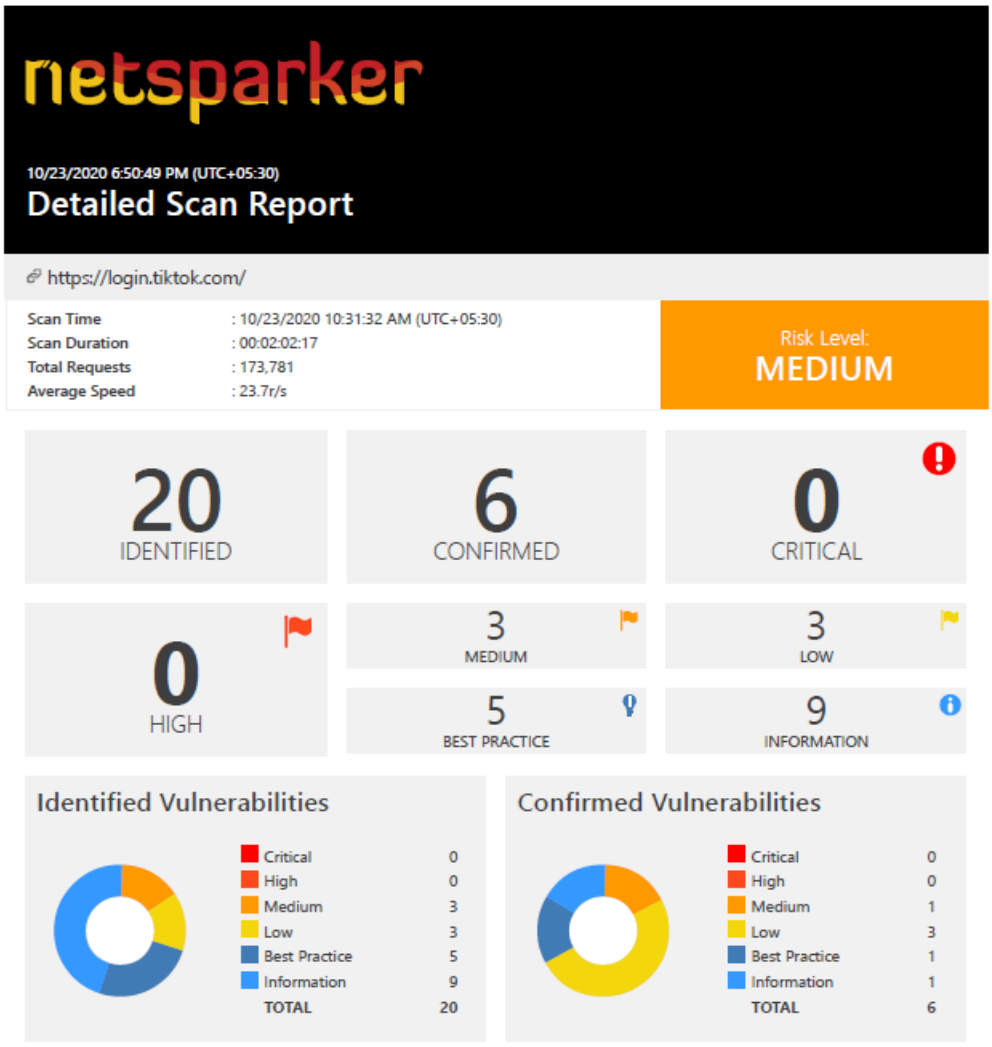
Contents

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



1 / 70

Vulnerability Summary for subdomain

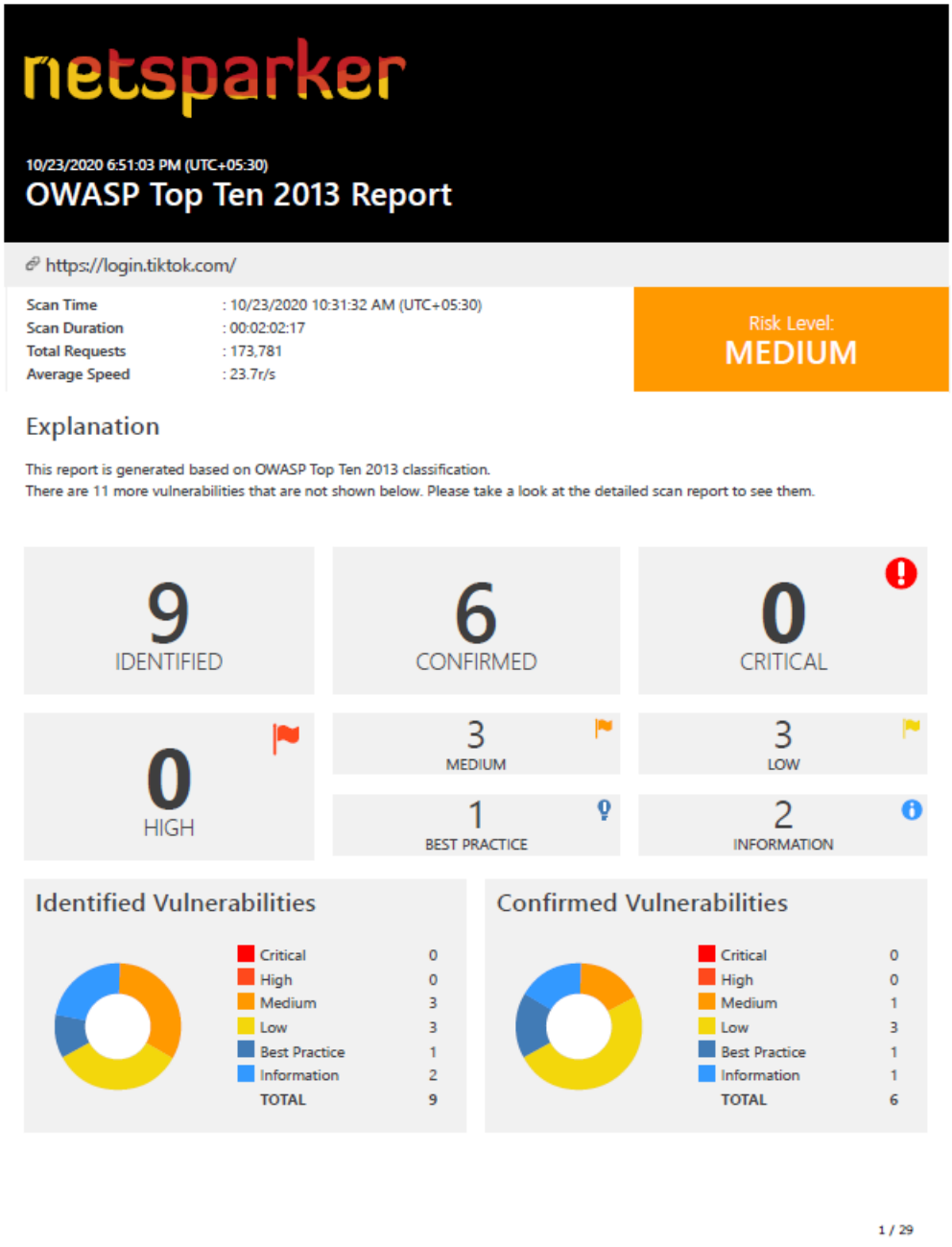
Vulnerability Summary

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.



netsparker

10/23/2020 6:51:03 PM (UTC+05:30)

OWASP Top Ten 2013 Report

https://login.tiktok.com/

Scan Time	: 10/23/2020 10:31:32 AM (UTC+05:30)
Scan Duration	: 00:02:02:17
Total Requests	: 173,781
Average Speed	: 23.7r/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.

9 IDENTIFIED	6 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	3 LOW
	1 BEST PRACTICE	2 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	3
Best Practice	1
Information	2
TOTAL	9

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	3
Best Practice	1
Information	1
TOTAL	6

1 / 29

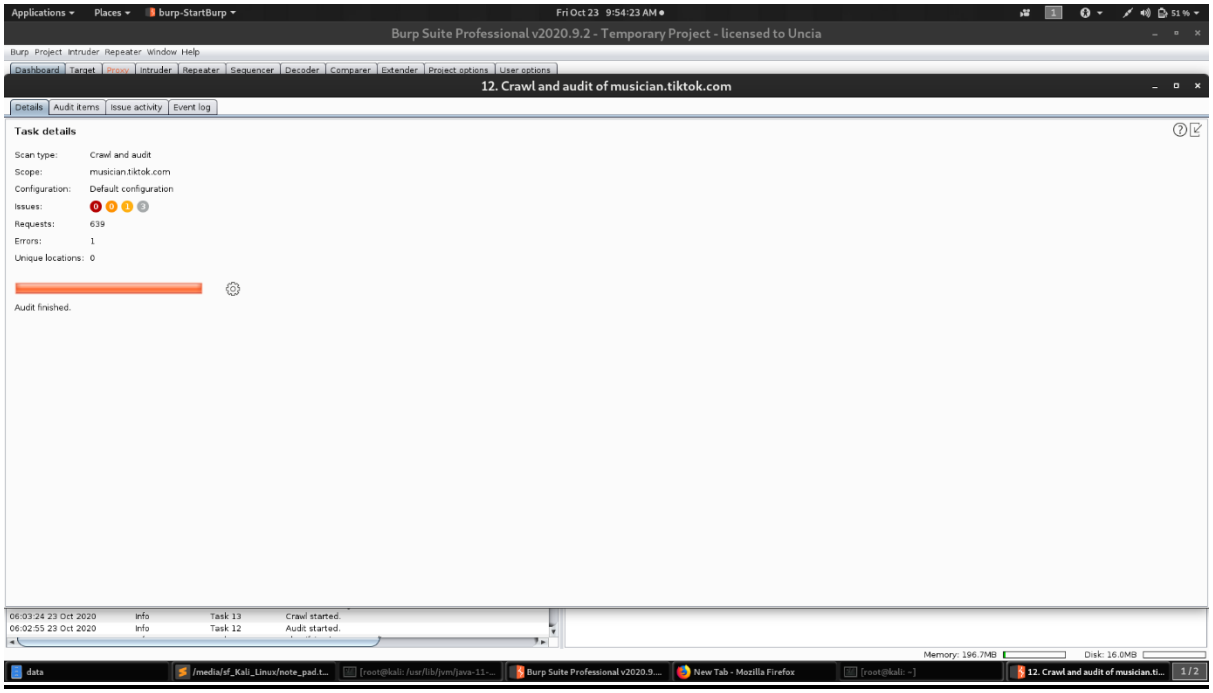
Vulnerability Summary for subdomain

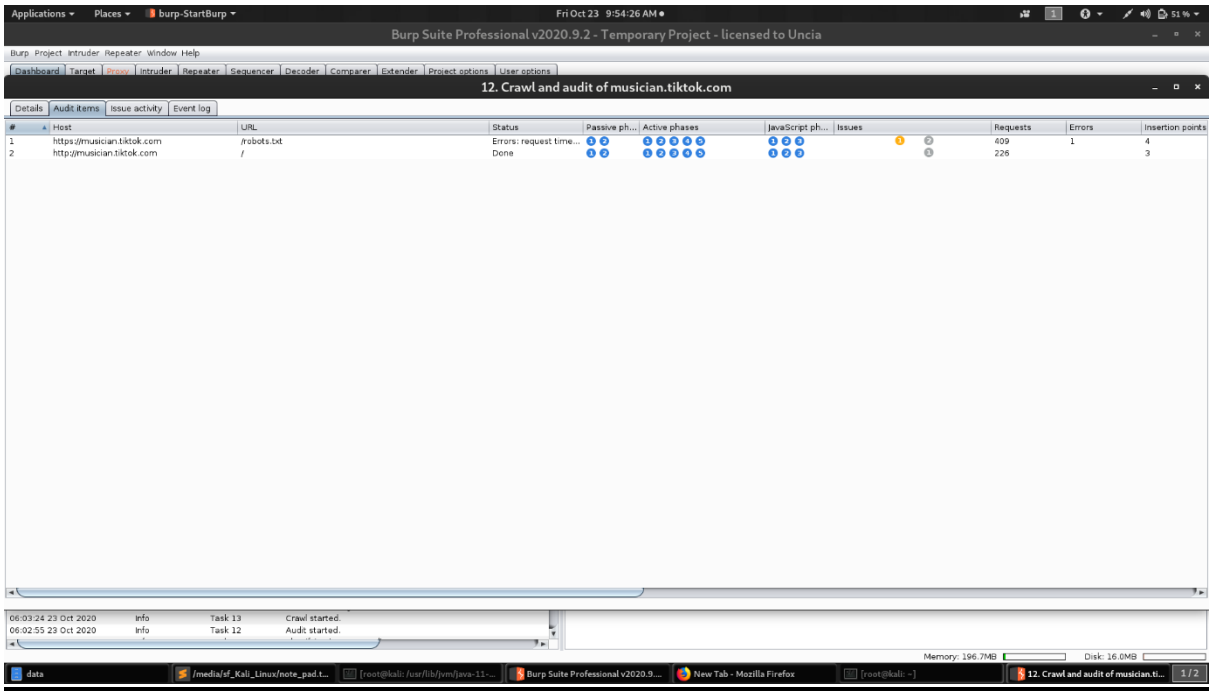
Vulnerabilities By OWASP 2013

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

2 / 29

Burp Suite Scanning





Burp Scanner Report

BURPSUITE PROFESSIONAL

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.

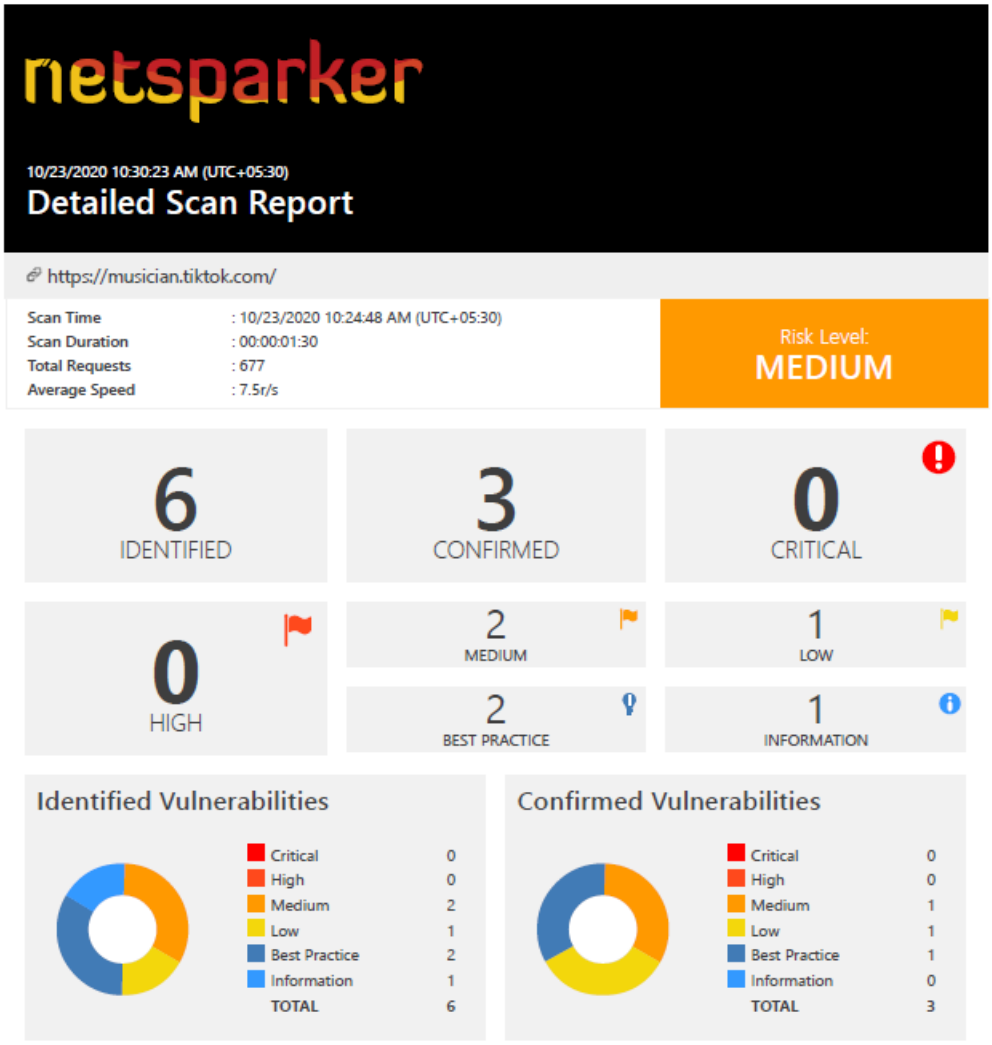
Contents

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



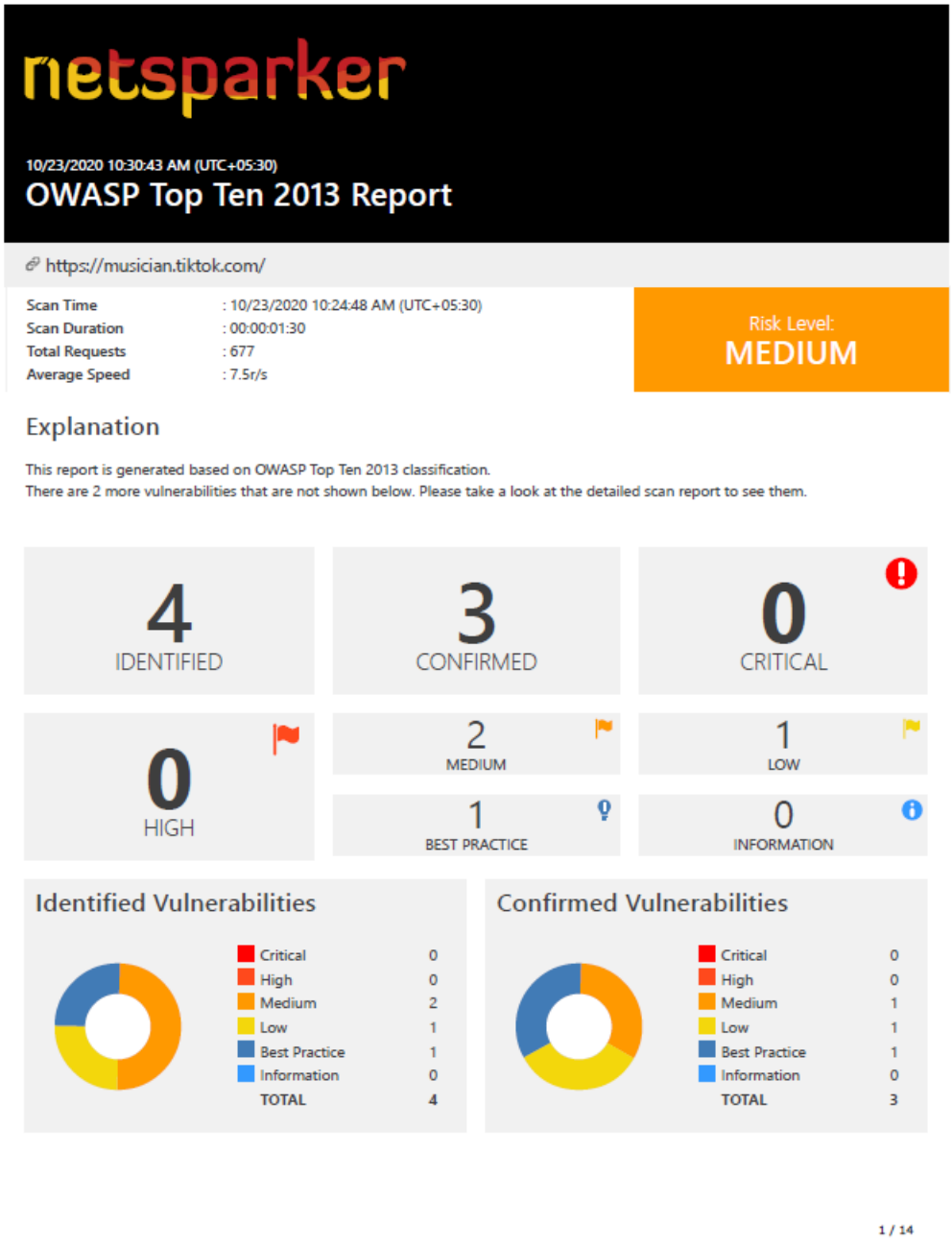
Vulnerability Summary for subdomain

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/	

2 / 23

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 10:30:43 AM (UTC+05:30)

OWASP Top Ten 2013 Report

https://musician.tiktok.com/

Scan Time	: 10/23/2020 10:24:48 AM (UTC+05:30)
Scan Duration	: 00:00:01:30
Total Requests	: 677
Average Speed	: 7.5r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 2 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

IDENTIFIED	CONFIRMED	CRITICAL
4	3	0

HIGH	MEDIUM	LOW
0	2	1

BEST PRACTICE	INFORMATION
1	0

Identified Vulnerabilities

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

Confirmed Vulnerabilities

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

1 / 14

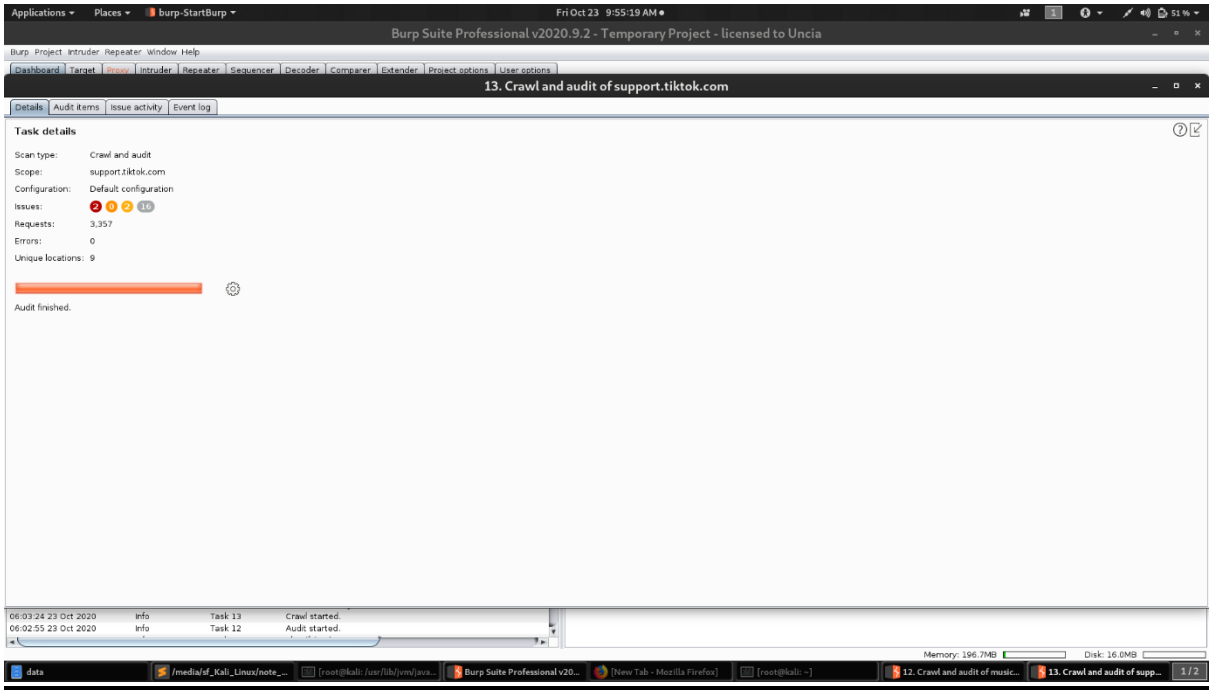
Vulnerability Summary for subdomain

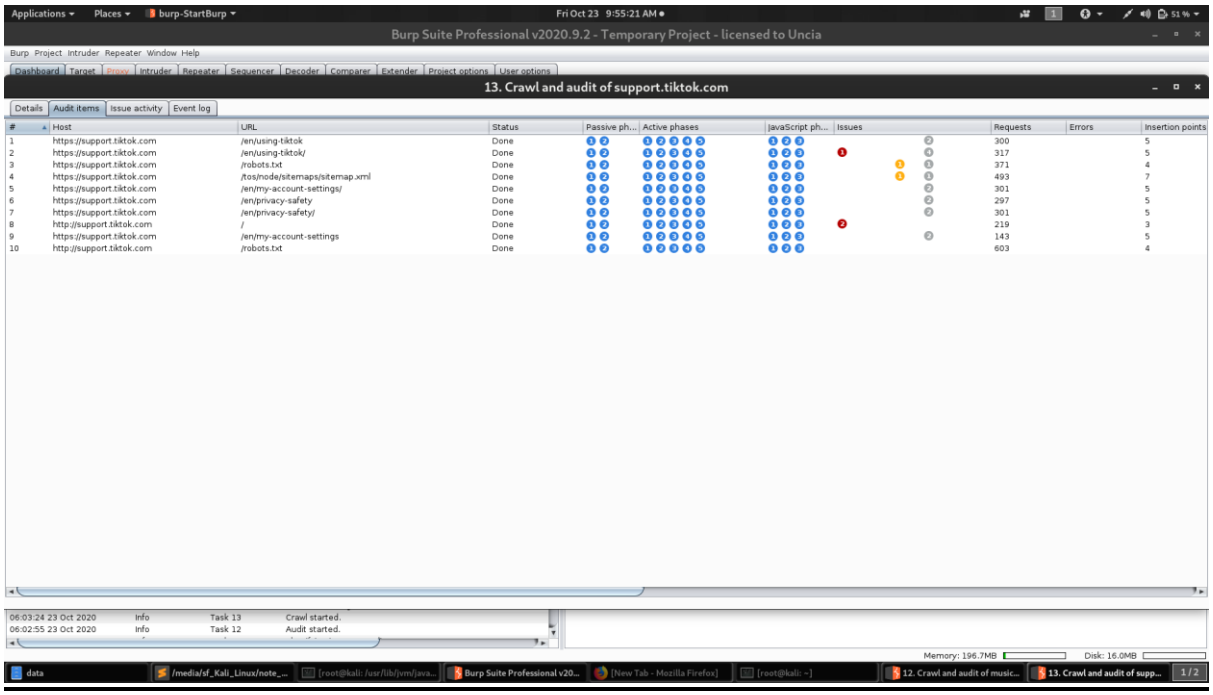
Vulnerabilities By OWASP 2013

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

2 / 14

Burp Suite Scanning





Burp Scanner Report

BURPSUITE PROFESSIONAL

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.

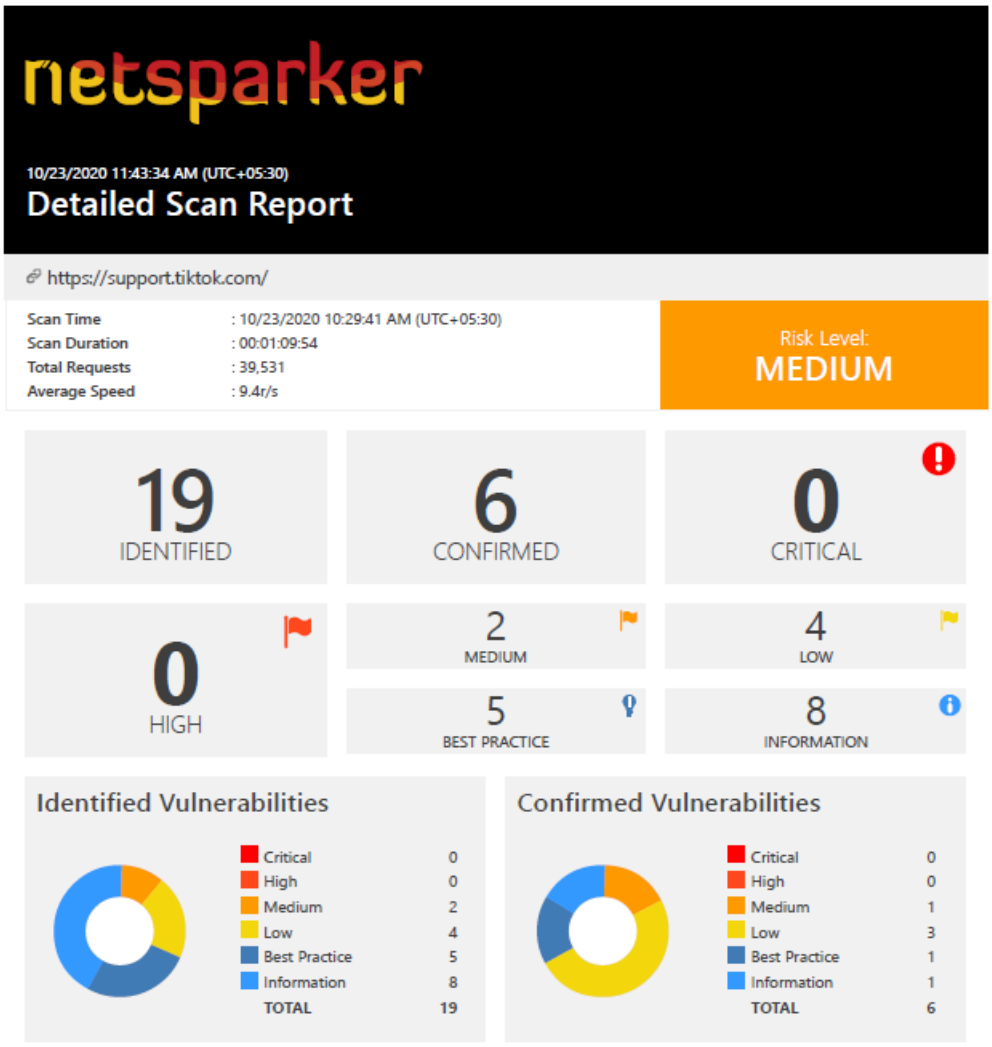
Contents

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

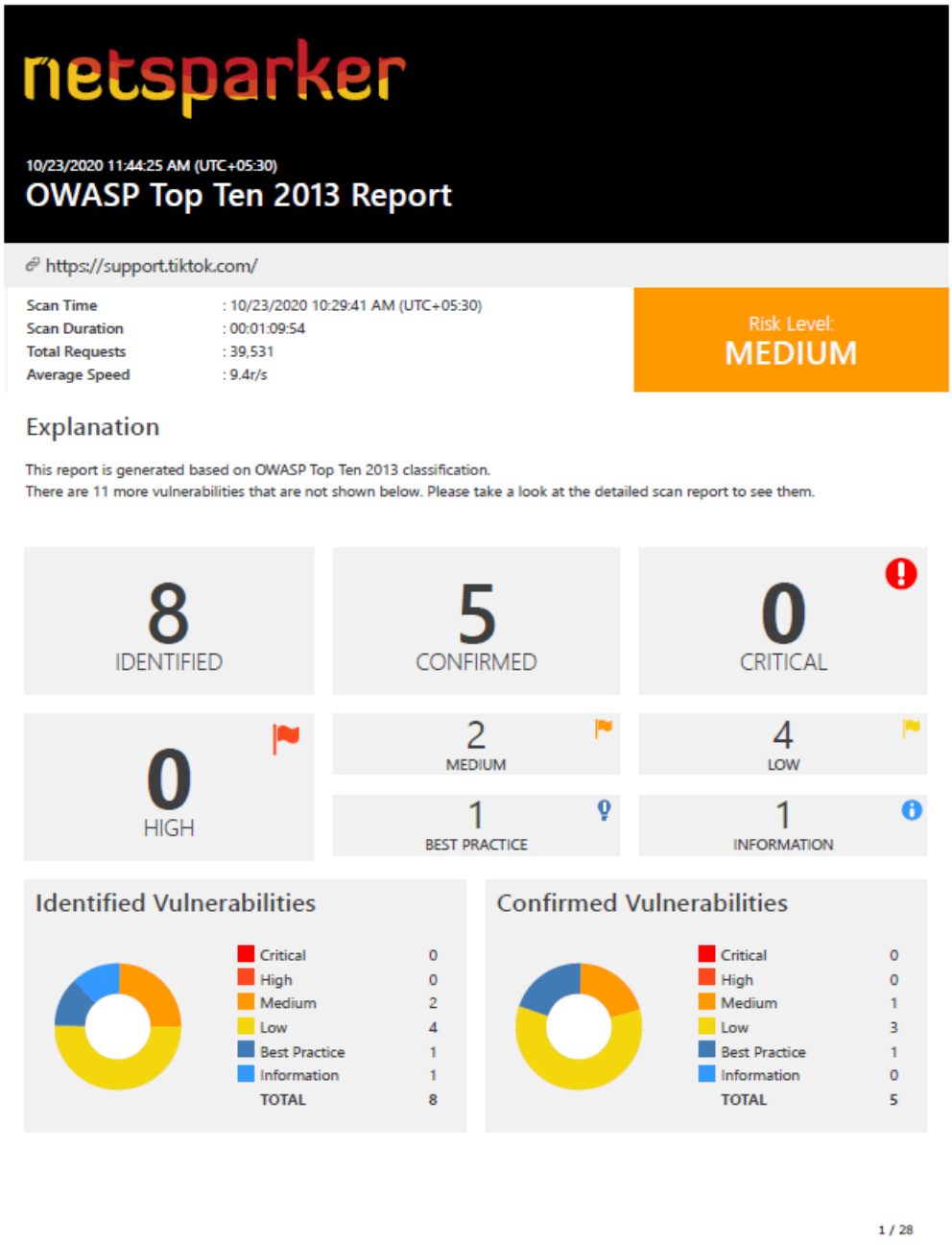
Vulnerability Summary

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

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

1 / 28

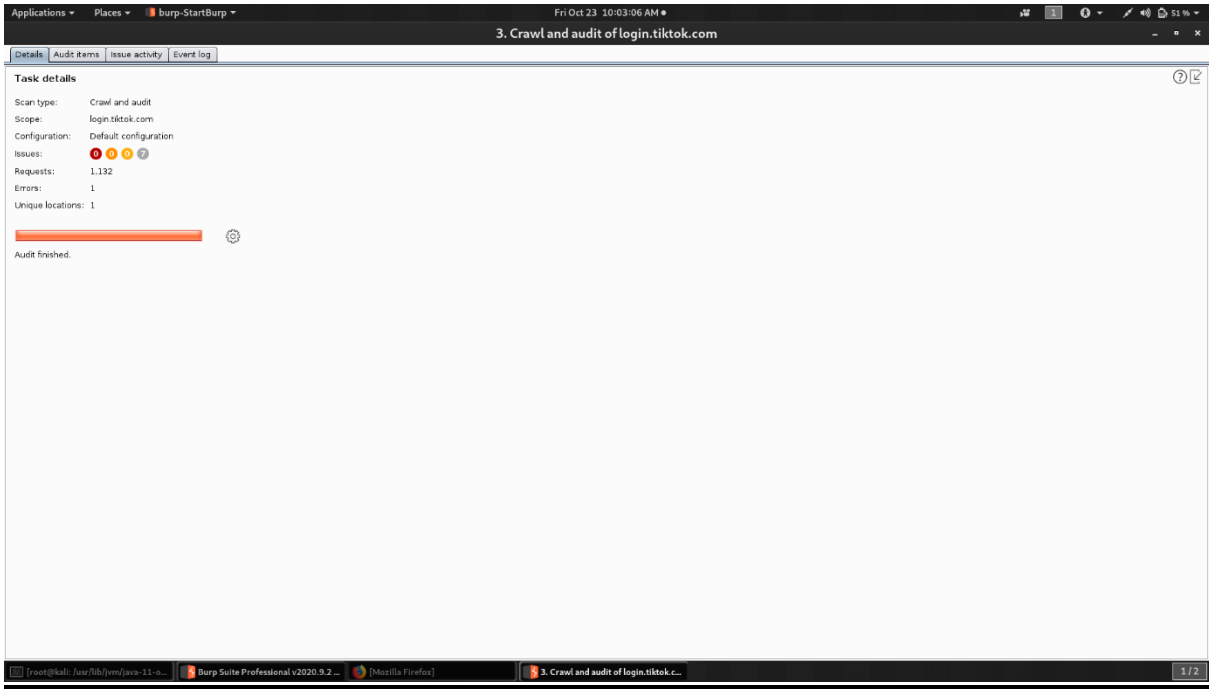
Vulnerability Summary for subdomain

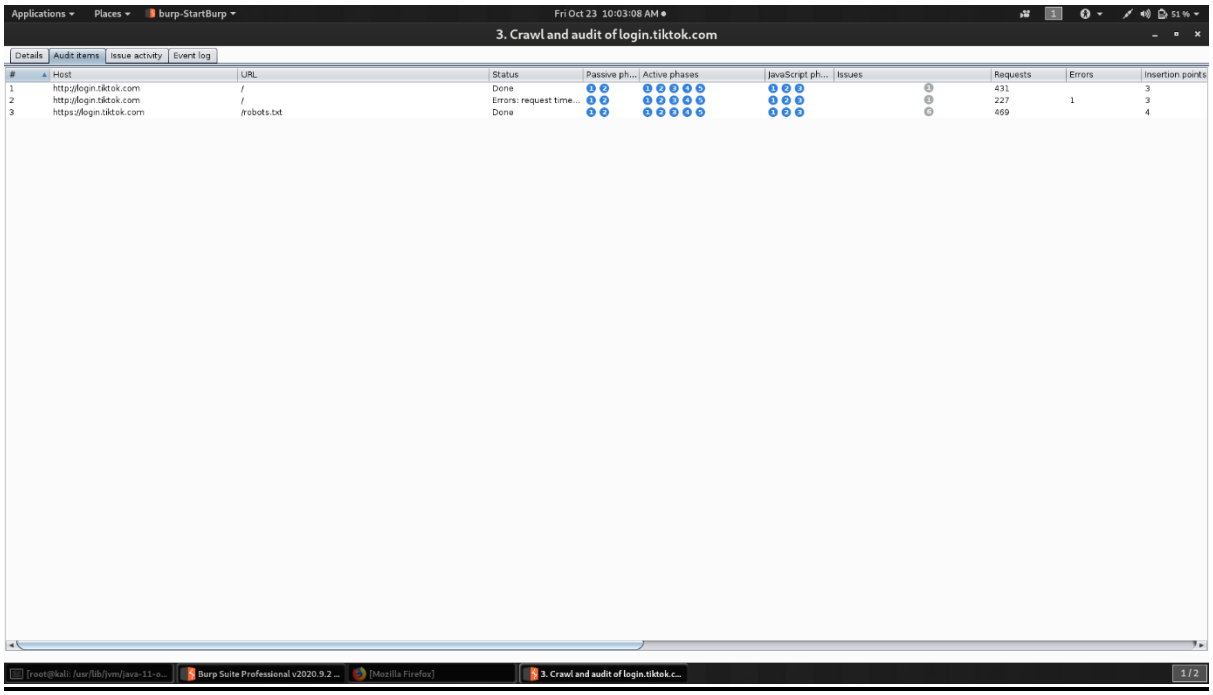
Vulnerabilities By OWASP 2013

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

2 / 28

Burp Suite Scanning





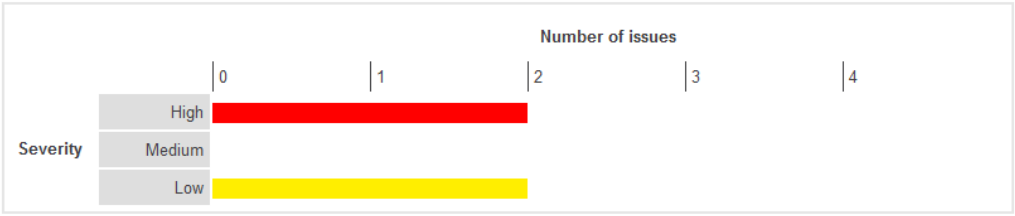
Burp Scanner Report

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			
	Certain	Firm	Tentative	Total
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.

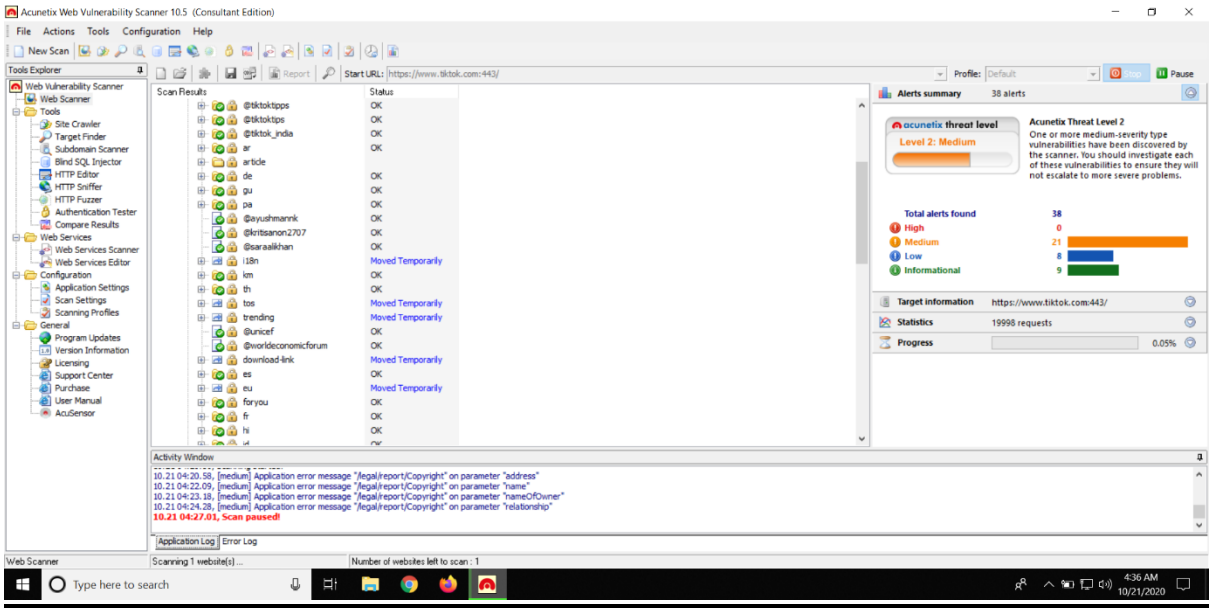


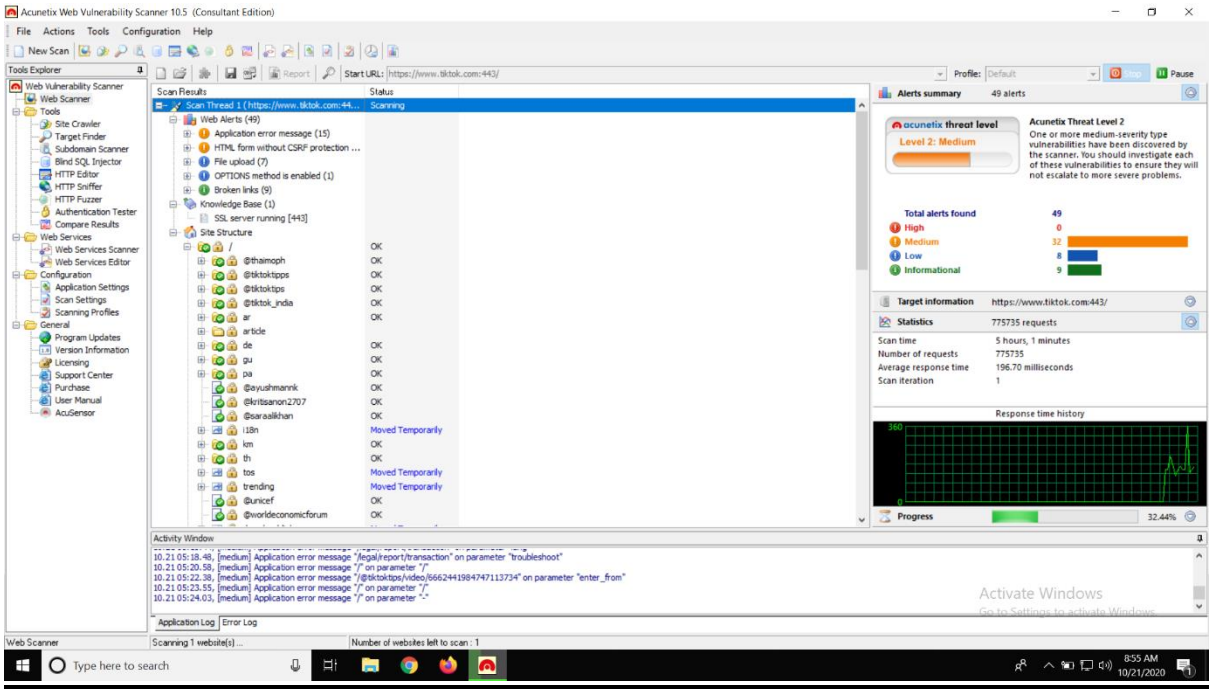
Contents

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

Total alerts found	**326**
High	0
Medium	161
Low	8
Informational	157

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 vulnerbilities. 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 may 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).