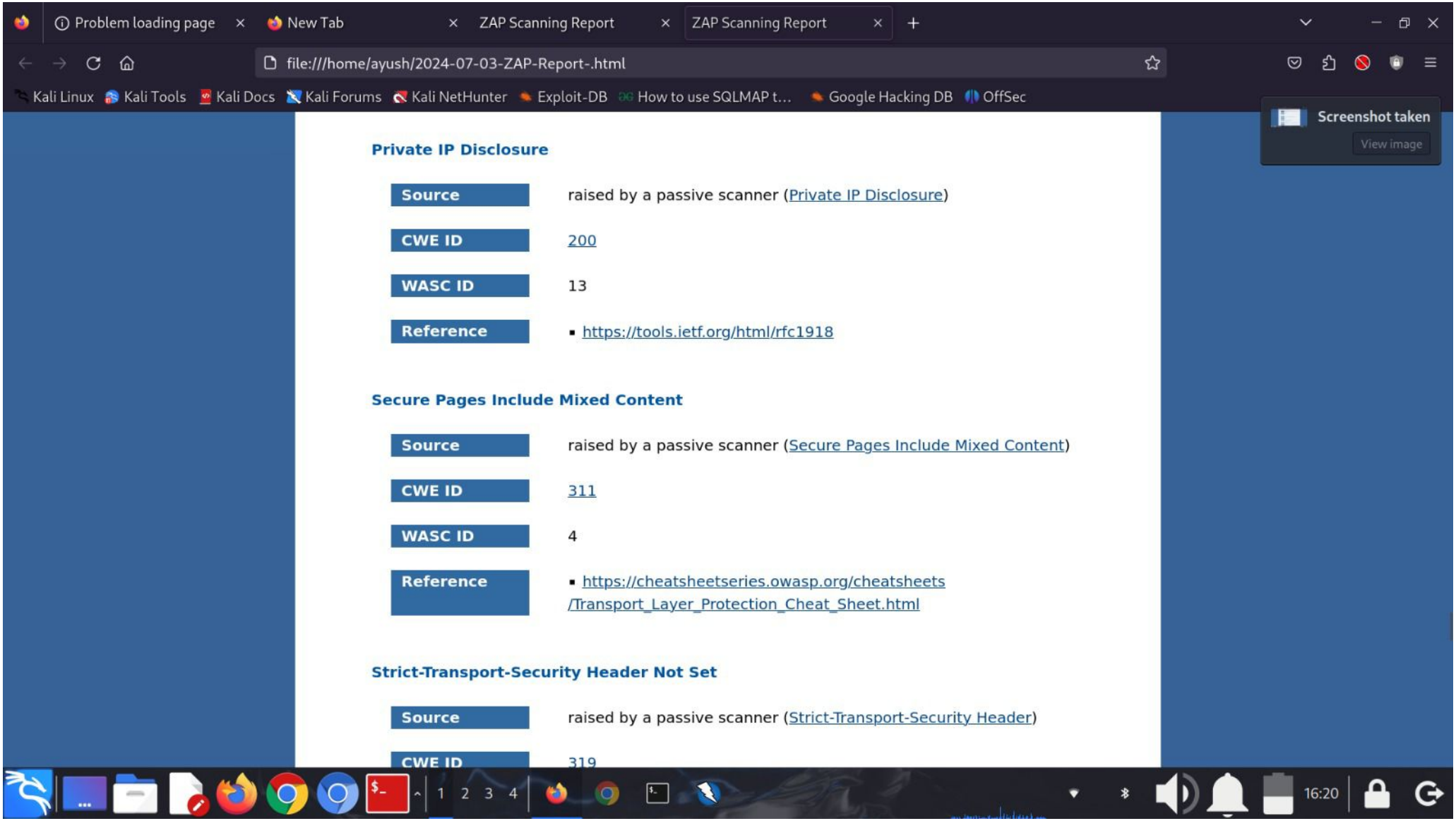
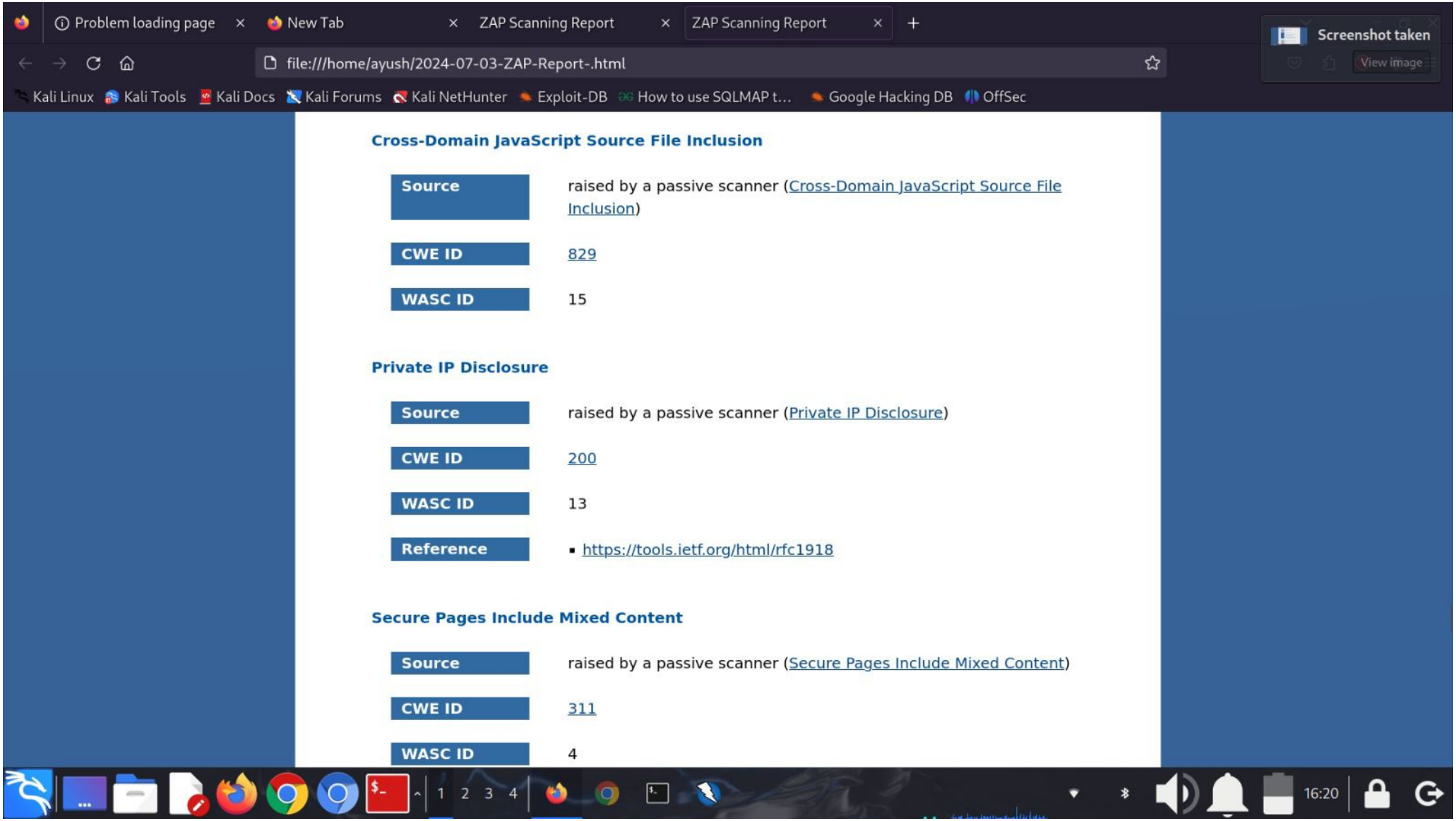
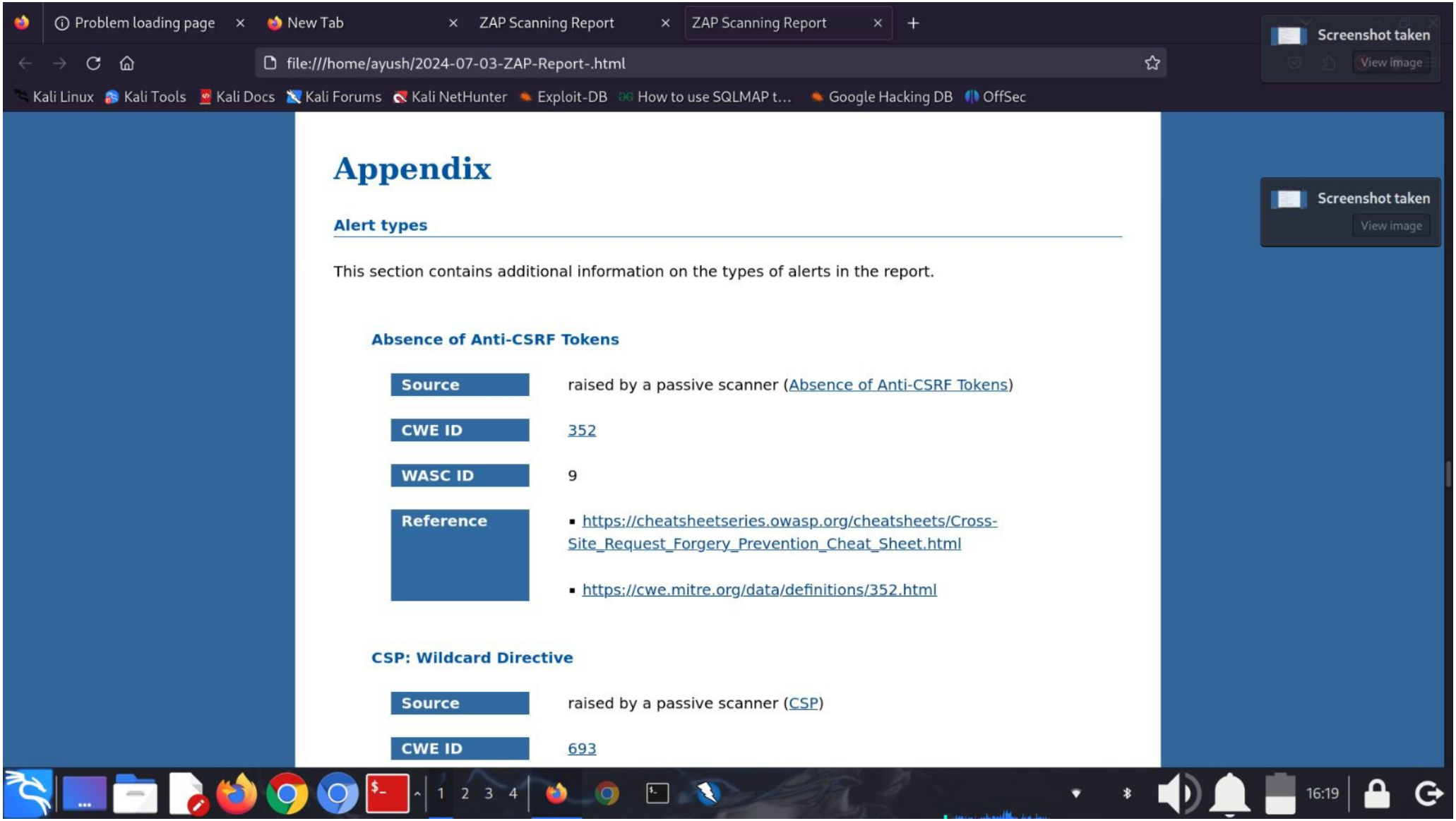
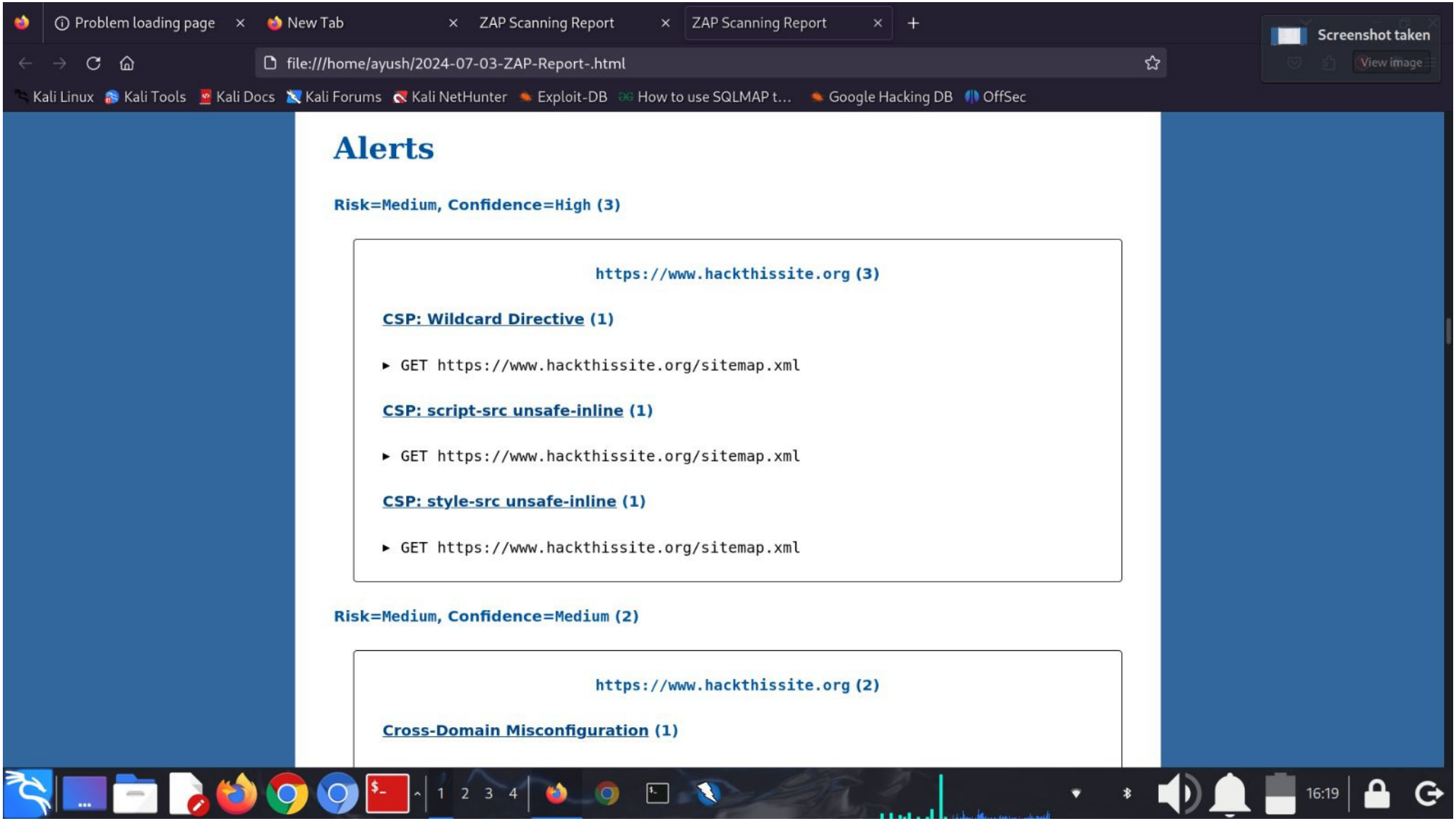
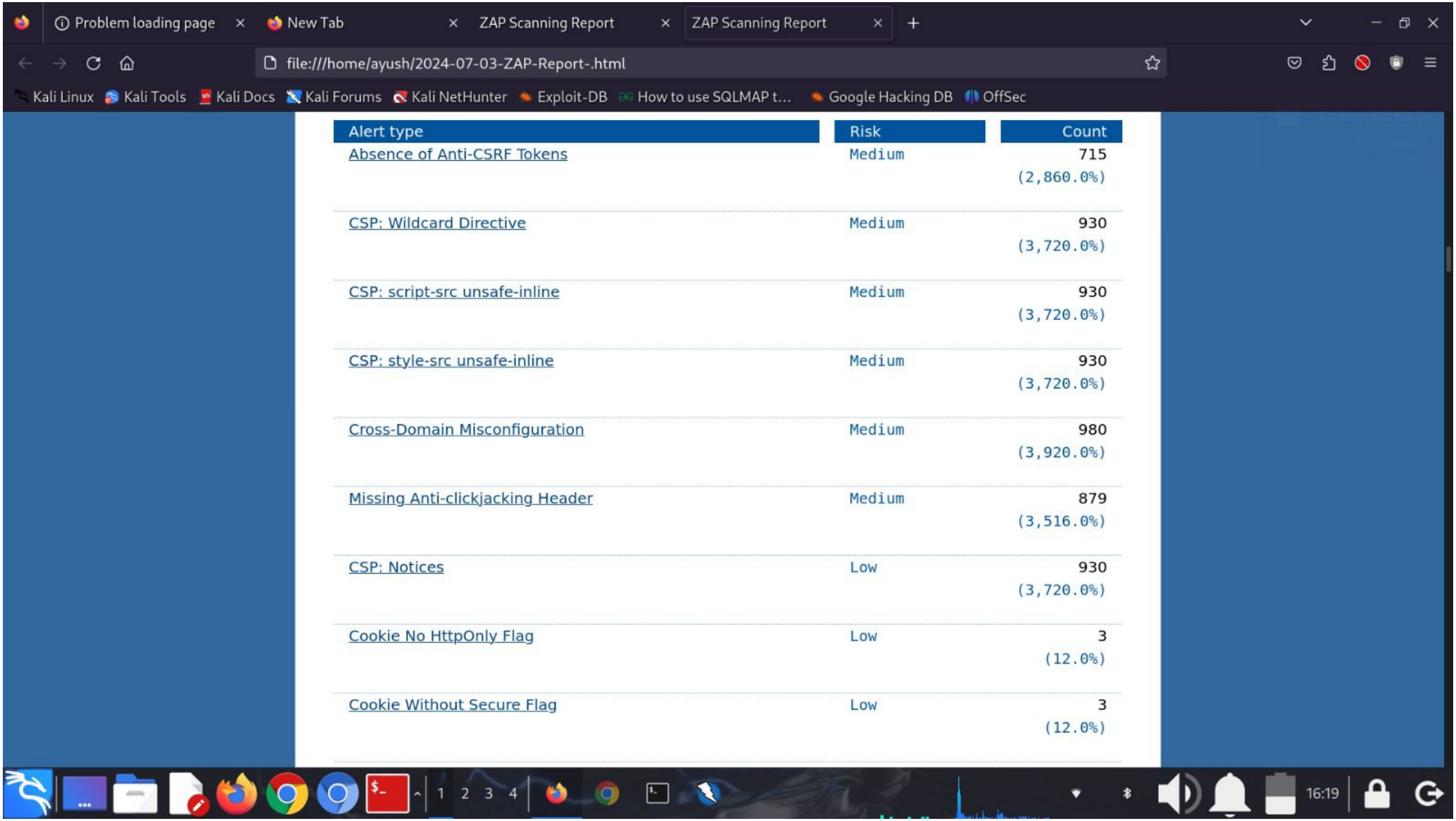

Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Screenshot taken
View image
Private IP Disclosure
Source
raised by a passive scanner (Private IP Disclosure)
CWE ID
200
WASC ID
13
Reference
https://tools.ietf.org/html/rfc1918
Secure Pages Include Mixed Content
Source
raised by a passive scanner (Secure Pages Include Mixed Content)
CWE ID
311
WASC ID
4
Reference
https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
Strict-Transport-Security Header Not Set
Source
raised by a passive scanner (Strict-Transport-Security Header)
CWE ID
319
1 2 3 4
16:20

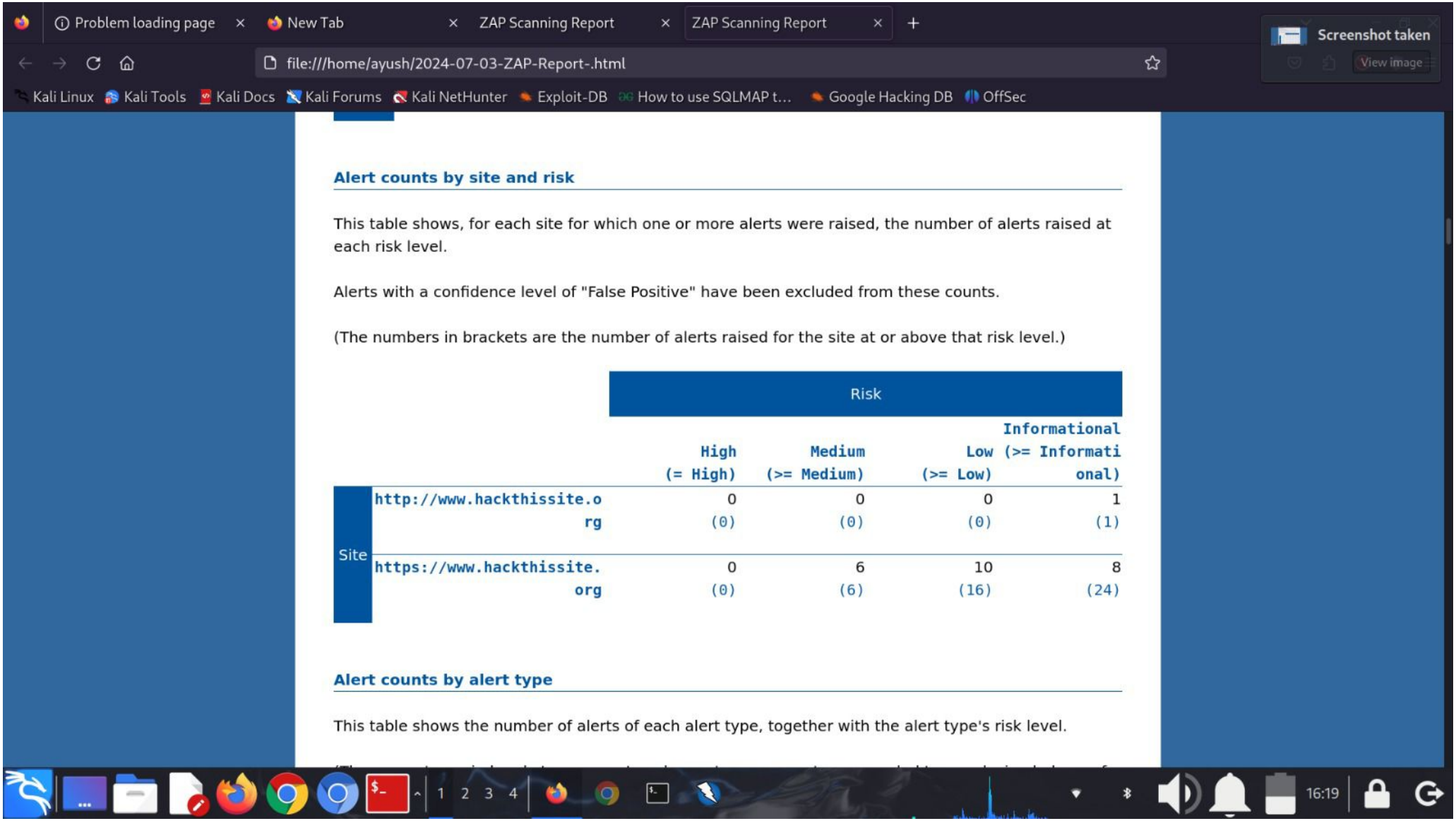

Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
Screenshot taken
View image
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Cross-Domain JavaScript Source File Inclusion
Source
raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID
829
WASC ID
15
Private IP Disclosure
Source
raised by a passive scanner (Private IP Disclosure)
CWE ID
200
WASC ID
13
Reference
https://tools.ietf.org/html/rfc1918
Secure Pages Include Mixed Content
Source
raised by a passive scanner (Secure Pages Include Mixed Content)
CWE ID
311
WASC ID
4
1 2 3 4
16:20

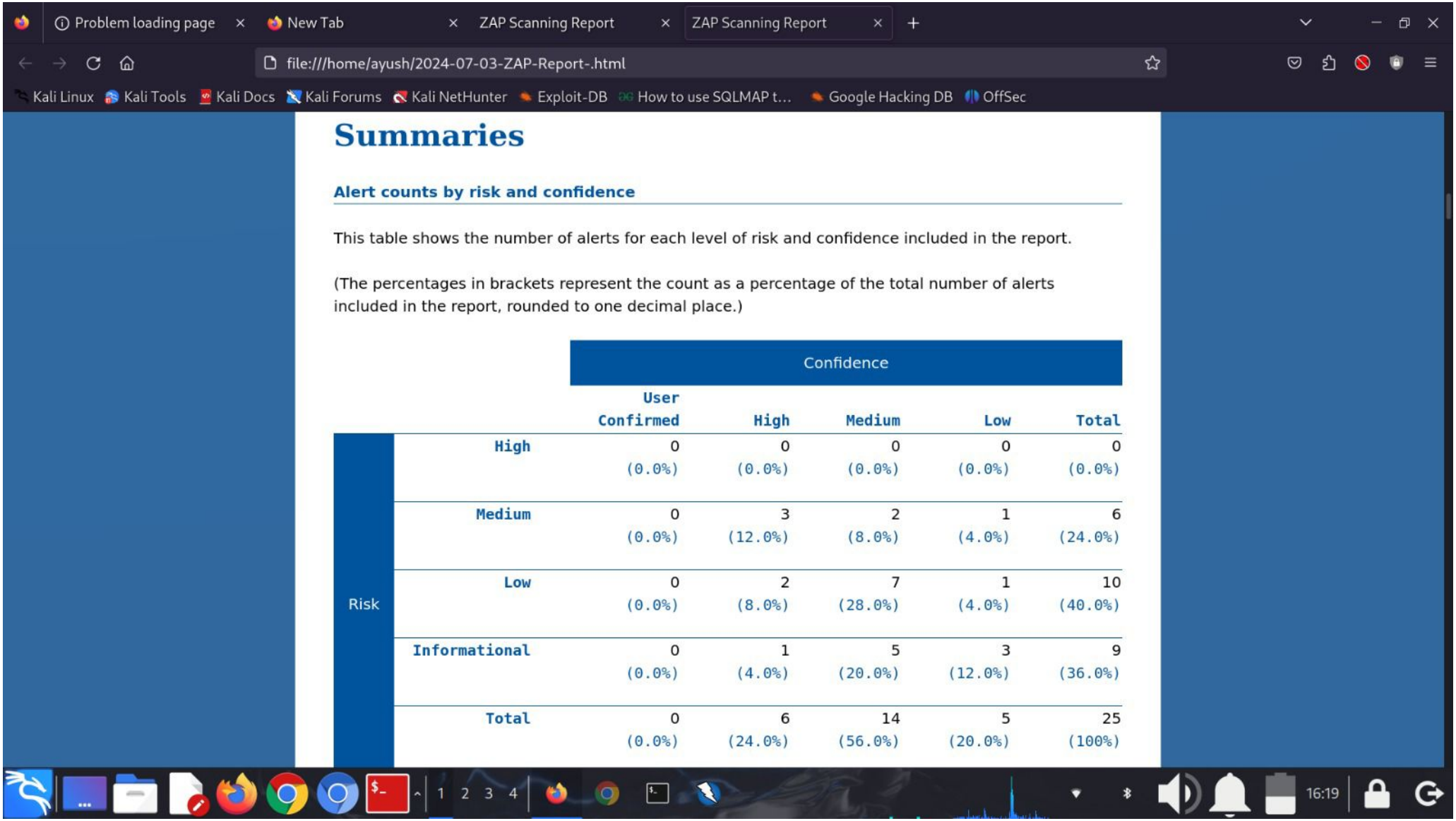

Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
CSP: Notices
Source
raised by a passive scanner (CSP)
CWE ID
693
WASC ID
15
Reference
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
https://github.com/HtmlUnit/htmlunit-csp
https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
Cookie No HttpOnly Flag
Source
raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID
1004
WASC ID
13
1 2 3 4
16:20


Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Screenshot taken
View image
Screenshot taken
View image
Appendix
Alert types
This section contains additional information on the types of alerts in the report.
Absence of Anti-CSRF Tokens
Source
raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID
352
WASC ID
9
Reference
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/352.html
CSP: Wildcard Directive
Source
raised by a passive scanner (CSP)
CWE ID
693
1 2 3 4
16:19


Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
Screenshot taken
View image
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Alerts
Risk=Medium, Confidence=High (3)
https://www.hackthissite.org (3)
CSP: Wildcard Directive (1)
▸ GET https://www.hackthissite.org/sitemap.xml
CSP: script-src unsafe-inline (1)
▸ GET https://www.hackthissite.org/sitemap.xml
CSP: style-src unsafe-inline (1)
▸ GET https://www.hackthissite.org/sitemap.xml
Risk=Medium, Confidence=Medium (2)
https://www.hackthissite.org (2)
Cross-Domain Misconfiguration (1)
1 2 3 4
16:19


Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Alert type
Risk
Count
Absence of Anti-CSRF Tokens
Medium
715
(2,860.0%)
CSP: Wildcard Directive
Medium
930
(3,720.0%)
CSP: script-src unsafe-inline
Medium
930
(3,720.0%)
CSP: style-src unsafe-inline
Medium
930
(3,720.0%)
Cross-Domain Misconfiguration
Medium
980
(3,920.0%)
Missing Anti-clickjacking Header
Medium
879
(3,516.0%)
CSP: Notices
Low
930
(3,720.0%)
Cookie No HttpOnly Flag
Low
3
(12.0%)
Cookie Without Secure Flag
Low
3
(12.0%)
1 2 3 4
16:19


Problem loading page
New Tab
ZAP Scanning Report
ZAP Scanning Report
file:///home/ayush/2024-07-03-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
How to use SQLMAP t...
Google Hacking DB
OffSec
Screenshot taken
View image
Alert counts by site and risk
This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.
Alerts with a confidence level of "False Positive" have been excluded from these counts.
(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)
Risk
High (= High)
Medium (>= Medium)
Low (>= Low)
Informational (>= Informational)
Site
http://www.hackthissite.org
0 (0)
0 (0)
0 (0)
1 (1)
https://www.hackthissite.org
0 (0)
6 (6)
10 (16)
8 (24)
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
16:19



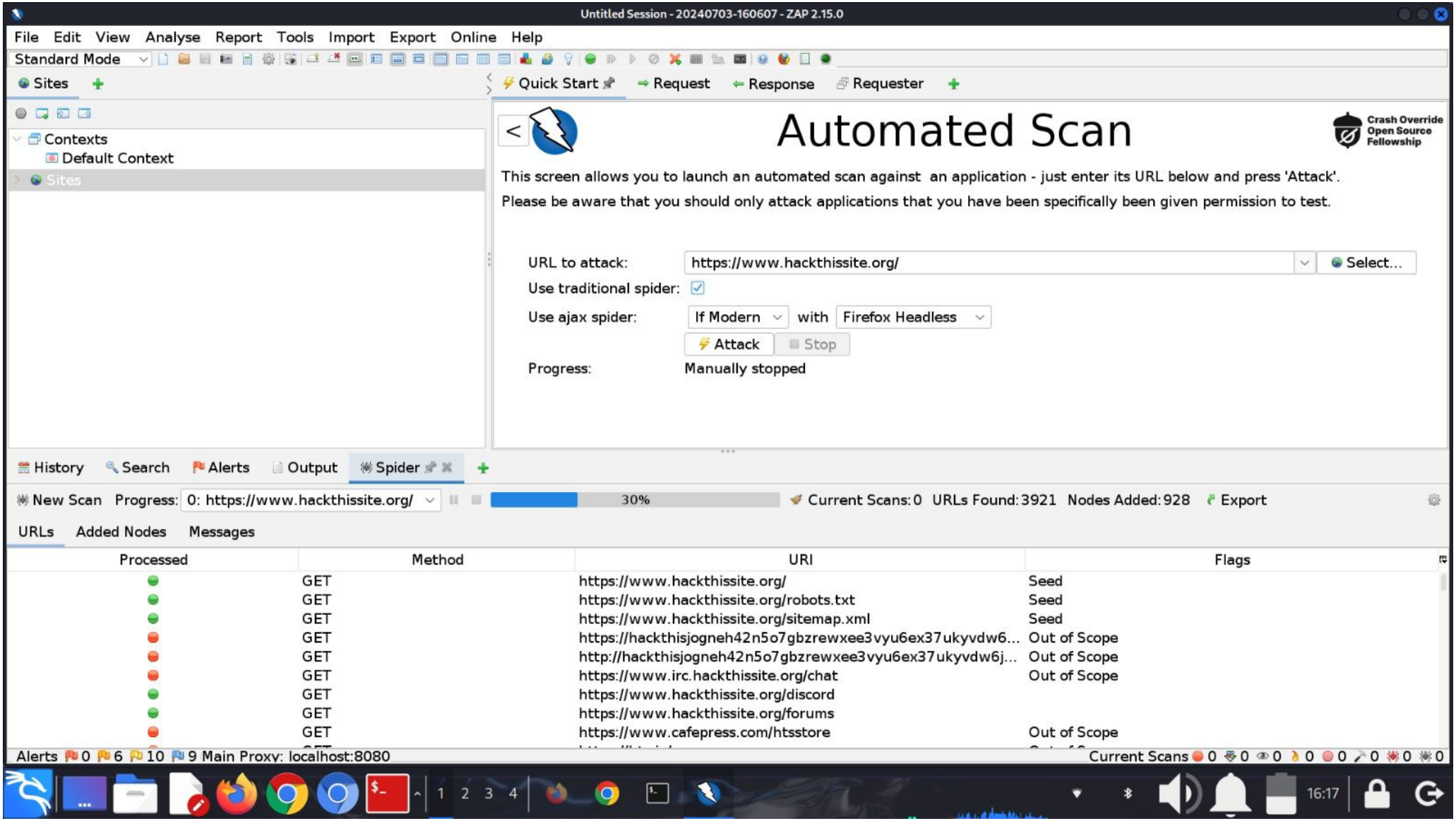
Summaries

Alert counts by risk and confidence

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

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

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	3 (12.0%)	2 (8.0%)	1 (4.0%)	6 (24.0%)
	Low	0 (0.0%)	2 (8.0%)	7 (28.0%)	1 (4.0%)	10 (40.0%)
	Informational	0 (0.0%)	1 (4.0%)	5 (20.0%)	3 (12.0%)	9 (36.0%)
	Total	0 (0.0%)	6 (24.0%)	14 (56.0%)	5 (20.0%)	25 (100%)


Untitled Session - 20240703-160607 - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
Crash Override Open Source Fellowship
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
https://www.hackthissite.org/
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox Headless
Attack
Stop
Progress:
Manually stopped
History
Search
Alerts
Output
Spider
New Scan
Progress:
0: https://www.hackthissite.org/
30%
Current Scans: 0
URLs Found: 3921
Nodes Added: 928
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET https://www.hackthissite.org/ Seed
GET https://www.hackthissite.org/robots.txt Seed
GET https://www.hackthissite.org/sitemap.xml Seed
GET https://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6... Out of Scope
GET http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6j... Out of Scope
GET https://www.irc.hackthissite.org/chat Out of Scope
GET https://www.hackthissite.org/discord
GET https://www.hackthissite.org/forums
GET https://www.cafepress.com/htsstore Out of Scope
Alerts 0 6 10 9 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0
16:17