PRACTICAL – 10

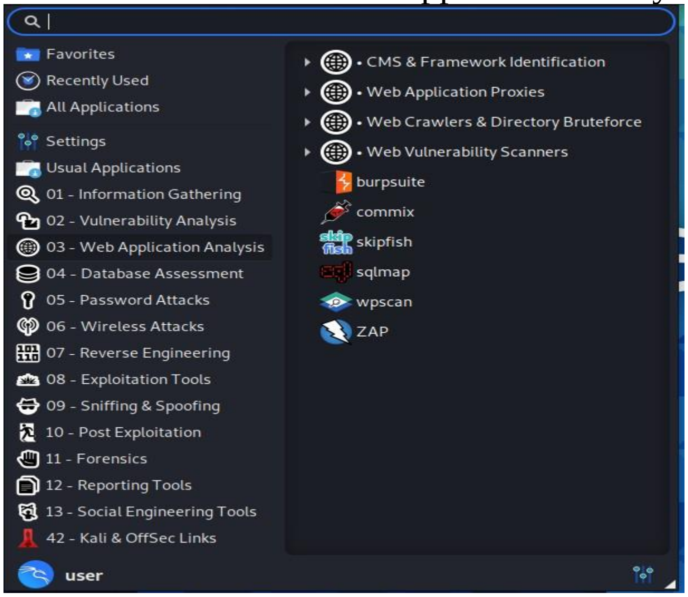
AIM: Find out Web Application Vulnerability using OWASP-ZAP tool

Tools:-
OWASP-ZAP

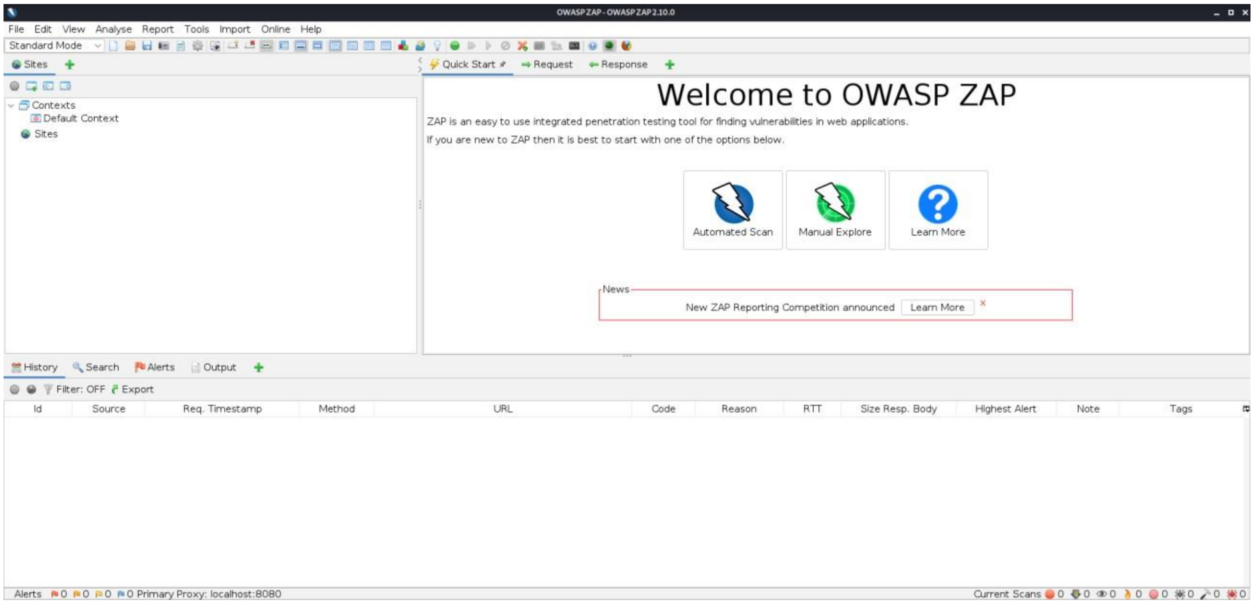
- OWASP ZAP is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- For security purposes, companies use paid tools, but OWASP ZAP is a great open-source alternative that makes Penetration Testing easier for testers.
- OWASP ZAP is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using https.
- It can also run in a daemon mode which is then controlled via a REST API.
- ZAP was added to the ThoughtWorks Technology Radar in May 2015 in the Trial ring.
- ZAP was originally forked from Paros, another pentesting proxy. Simon Bennetts, the project lead, stated in 2014 that only 20% of ZAP's source code was still from Paros.
- Some of the built in features include: Intercepting proxy server, Traditional and AJAX Web crawlers, Automated scanner, Passive scanner, Forced browsing, Fuzzer, WebSocket support, Scripting languages, and Plug-n-Hack support.
- It has a plugin-based architecture and an online 'marketplace' which allows new or updated features to be added. The GUI control panel is easy to use.

Practical:

We can find ZAP in Web Application Analysis.



The main screen looks like this

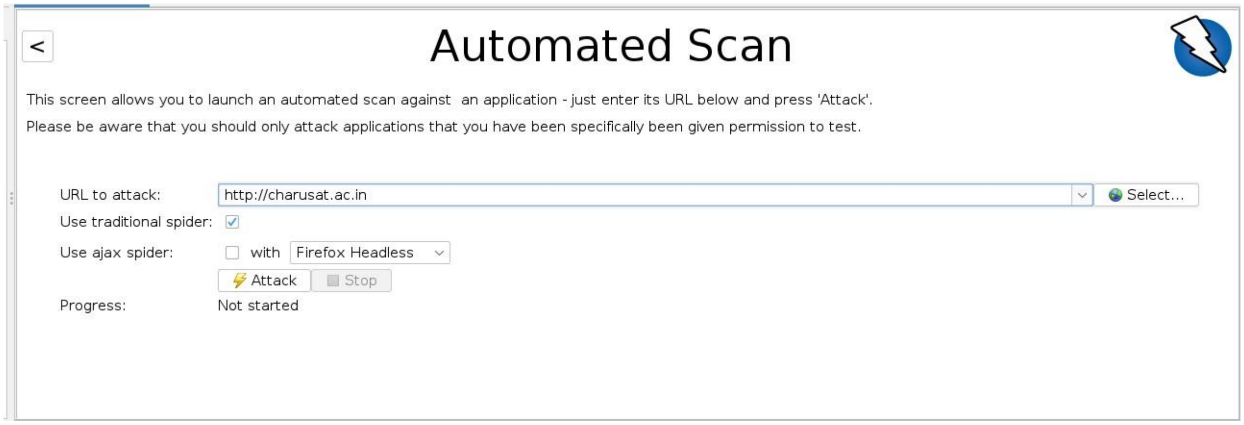


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

We Will go to Automated Scan and type in the website we want to attack(lets take https://charusat.ac.in)



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

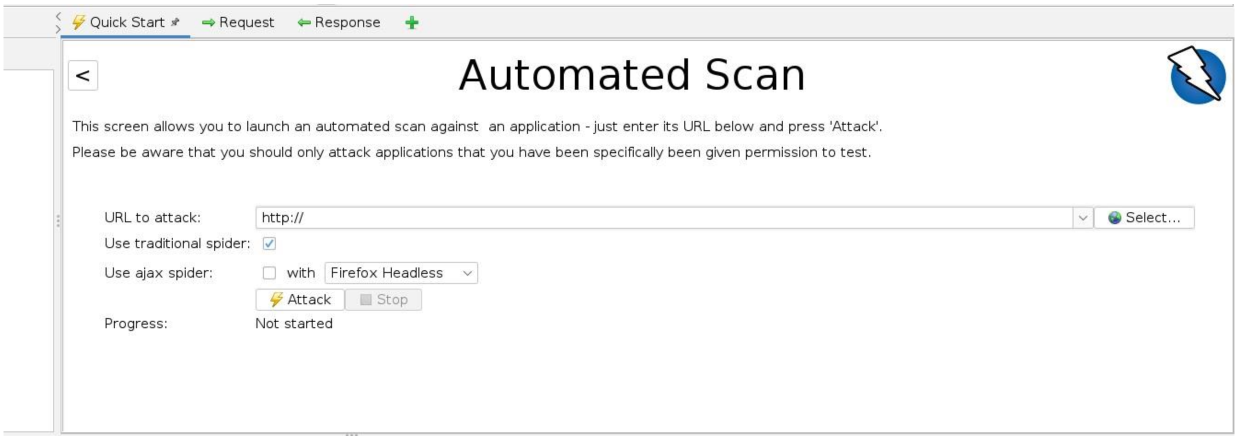
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://charusat.ac.in

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started



Automated Scan

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.

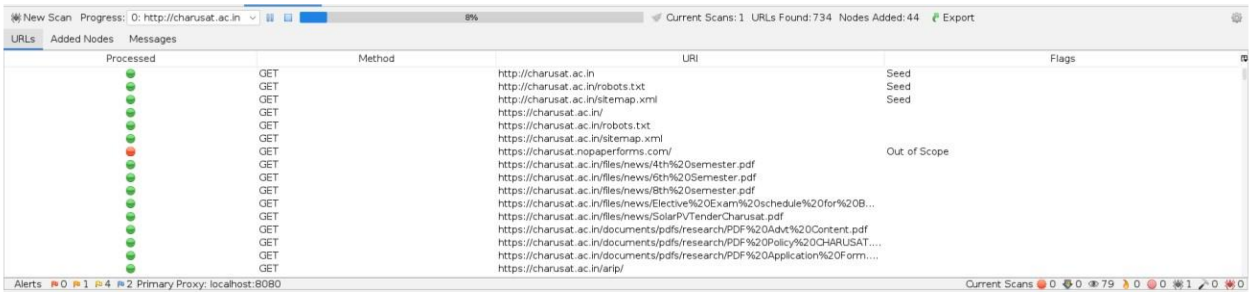
URL to attack: http://

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

In the spider tab we will find all the pages and More information will be available in the message tab.

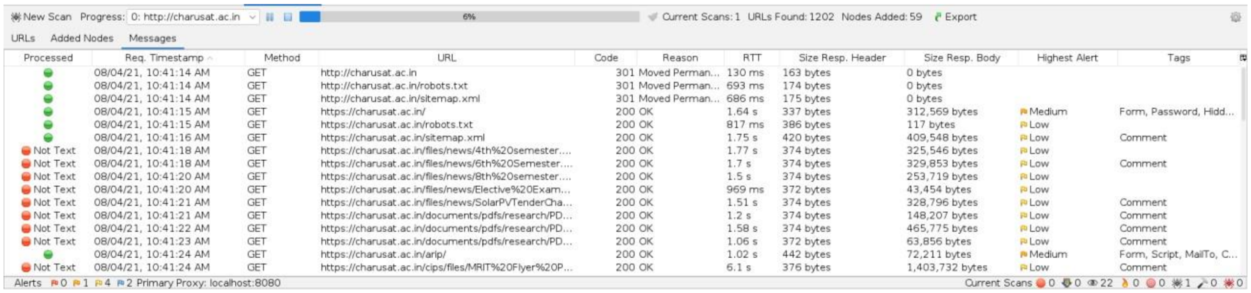


New Scan Progress: 0: http://charusat.ac.in 8% Current Scans: 1 URLs Found: 734 Nodes Added: 44 Export

URLs Added Nodes Messages

Processed	Method	URI	Flags
🟢	GET	http://charusat.ac.in	Seed
🟢	GET	http://charusat.ac.in/robots.txt	Seed
🟢	GET	http://charusat.ac.in/sitemap.xml	Seed
🟢	GET	https://charusat.ac.in/	
🟢	GET	https://charusat.ac.in/robots.txt	
🟢	GET	https://charusat.ac.in/sitemap.xml	
🔴	GET	https://charusat.nopaperforms.com/	Out of Scope
🟢	GET	https://charusat.ac.in/files/news/4th%20semester.pdf	
🟢	GET	https://charusat.ac.in/files/news/6th%20Semester.pdf	
🟢	GET	https://charusat.ac.in/files/news/8th%20semester.pdf	
🟢	GET	https://charusat.ac.in/files/news/Elective%20Exam%20schedule%20for%20B...	
🟢	GET	https://charusat.ac.in/files/news/SolarPVTenderCharusat.pdf	
🟢	GET	https://charusat.ac.in/documents/pdfs/research/PDF%20Advt%20Content.pdf	
🟢	GET	https://charusat.ac.in/documents/pdfs/research/PDF%20Policy%20CHARUSAT....	
🟢	GET	https://charusat.ac.in/documents/pdfs/research/PDF%20Application%20Form....	
🟢	GET	https://charusat.ac.in/arip/	

Alerts 0 1 4 2 Primary Proxy: localhost:8080 Current Scans 0 0 79 0 0 1 0 0



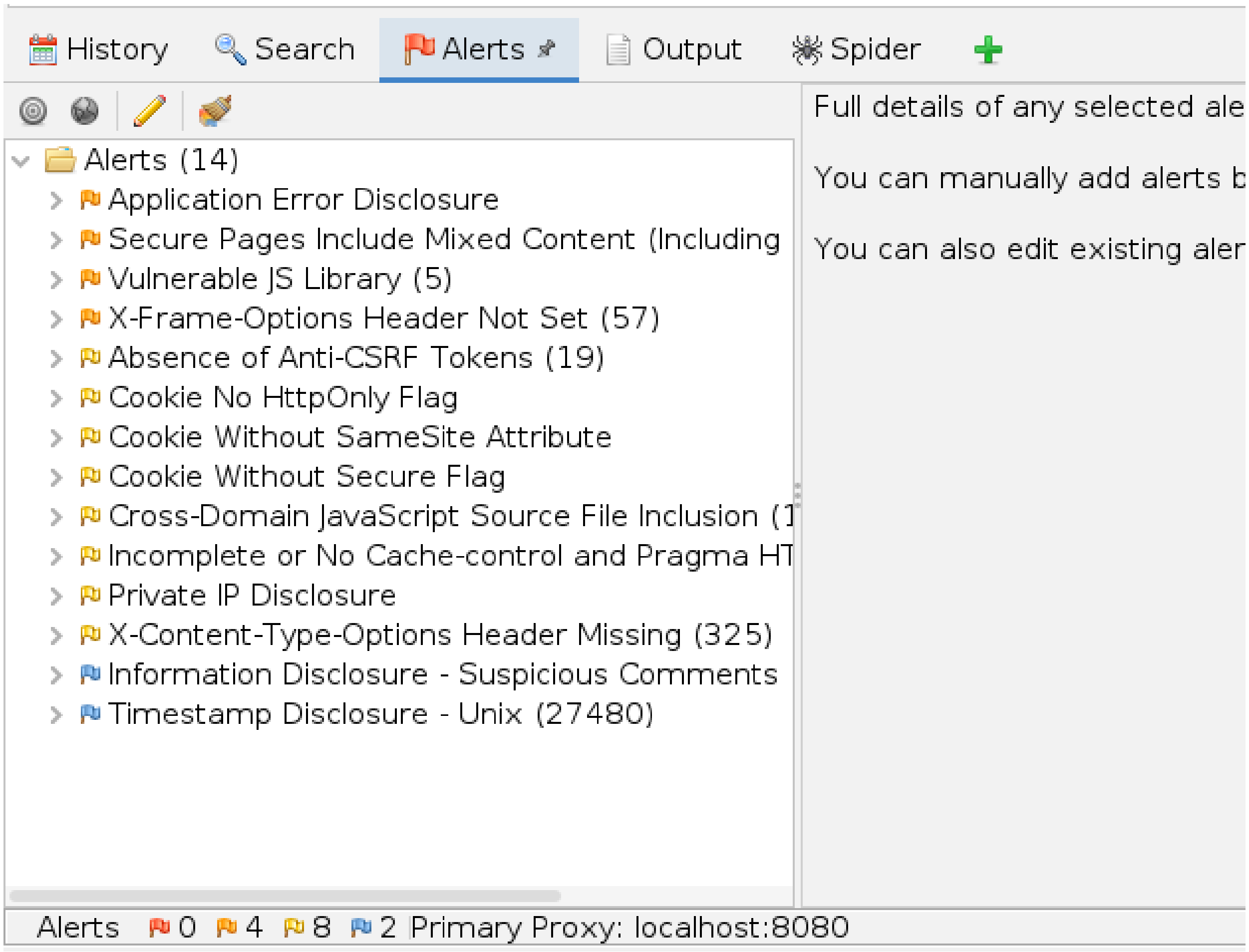
New Scan Progress: 0: http://charusat.ac.in 6% Current Scans: 1 URLs Found: 1202 Nodes Added: 59 Export

URLs Added Nodes Messages

Processed	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Tags
🟢	08/04/21, 10:41:14 AM	GET	http://charusat.ac.in	301	Moved Perman...	130 ms	163 bytes	0 bytes		
🟢	08/04/21, 10:41:14 AM	GET	http://charusat.ac.in/robots.txt	301	Moved Perman...	693 ms	174 bytes	0 bytes		
🟢	08/04/21, 10:41:14 AM	GET	http://charusat.ac.in/sitemap.xml	301	Moved Perman...	686 ms	175 bytes	0 bytes		
🟢	08/04/21, 10:41:15 AM	GET	https://charusat.ac.in/	200	OK	1.64 s	337 bytes	312,569 bytes	Medium	Form, Password, Hidd...
🟢	08/04/21, 10:41:15 AM	GET	https://charusat.ac.in/robots.txt	200	OK	817 ms	386 bytes	117 bytes	Low	
🟢	08/04/21, 10:41:16 AM	GET	https://charusat.ac.in/sitemap.xml	200	OK	1.75 s	420 bytes	409,548 bytes	Low	Comment
🔴 Not Text	08/04/21, 10:41:18 AM	GET	https://charusat.ac.in/files/news/4th%20semester....	200	OK	1.77 s	374 bytes	325,546 bytes	Low	
🔴 Not Text	08/04/21, 10:41:18 AM	GET	https://charusat.ac.in/files/news/6th%20Semester....	200	OK	1.7 s	374 bytes	329,853 bytes	Low	Comment
🔴 Not Text	08/04/21, 10:41:20 AM	GET	https://charusat.ac.in/files/news/8th%20semester....	200	OK	1.5 s	374 bytes	253,719 bytes	Low	
🔴 Not Text	08/04/21, 10:41:20 AM	GET	https://charusat.ac.in/files/news/Elective%20Exam...	200	OK	969 ms	372 bytes	43,454 bytes	Low	
🔴 Not Text	08/04/21, 10:41:21 AM	GET	https://charusat.ac.in/files/news/SolarPVTenderCha...	200	OK	1.51 s	374 bytes	328,796 bytes	Low	Comment
🔴 Not Text	08/04/21, 10:41:21 AM	GET	https://charusat.ac.in/documents/pdfs/research/PD...	200	OK	1.2 s	374 bytes	148,207 bytes	Low	Comment
🔴 Not Text	08/04/21, 10:41:22 AM	GET	https://charusat.ac.in/documents/pdfs/research/PD...	200	OK	1.58 s	374 bytes	465,775 bytes	Low	Comment
🔴 Not Text	08/04/21, 10:41:23 AM	GET	https://charusat.ac.in/documents/pdfs/research/PD...	200	OK	1.06 s	372 bytes	63,856 bytes	Low	Comment
🟢	08/04/21, 10:41:24 AM	GET	https://charusat.ac.in/arip/	200	OK	1.02 s	442 bytes	72,211 bytes	Medium	Form, Script, MailTo, C...
🔴 Not Text	08/04/21, 10:41:24 AM	GET	https://charusat.ac.in/cips/files/MRIT%20Flyer%20P...	200	OK	6.1 s	376 bytes	1,403,732 bytes	Low	Comment

Alerts 0 1 4 2 Primary Proxy: localhost:8080 Current Scans 0 0 22 0 0 1 0 0

In the alert tab we will see alert with flags of different colours and we can see the summary of it in bottom section too which will show the numbers of alerts.



Alerts (14)

- Application Error Disclosure
- Secure Pages Include Mixed Content (Including
- Vulnerable JS Library (5)
- X-Frame-Options Header Not Set (57)
- Absence of Anti-CSRF Tokens (19)
- Cookie No HttpOnly Flag
- Cookie Without SameSite Attribute
- Cookie Without Secure Flag
- Cross-Domain JavaScript Source File Inclusion (1
- Incomplete or No Cache-control and Pragma HT
- Private IP Disclosure
- X-Content-Type-Options Header Missing (325)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (27480)

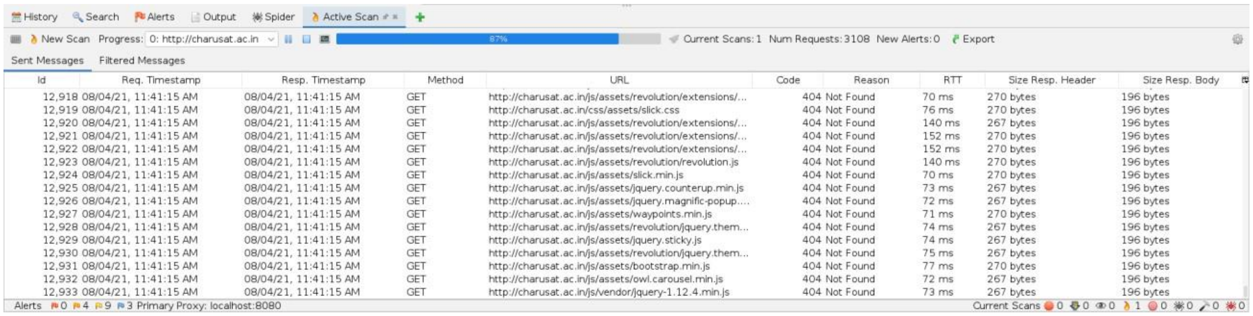
Full details of any selected ale

You can manually add alerts b

You can also edit existing aler

Alerts 0 4 8 2 Primary Proxy: localhost:8080

After spider scan is completed, active scan will begin.



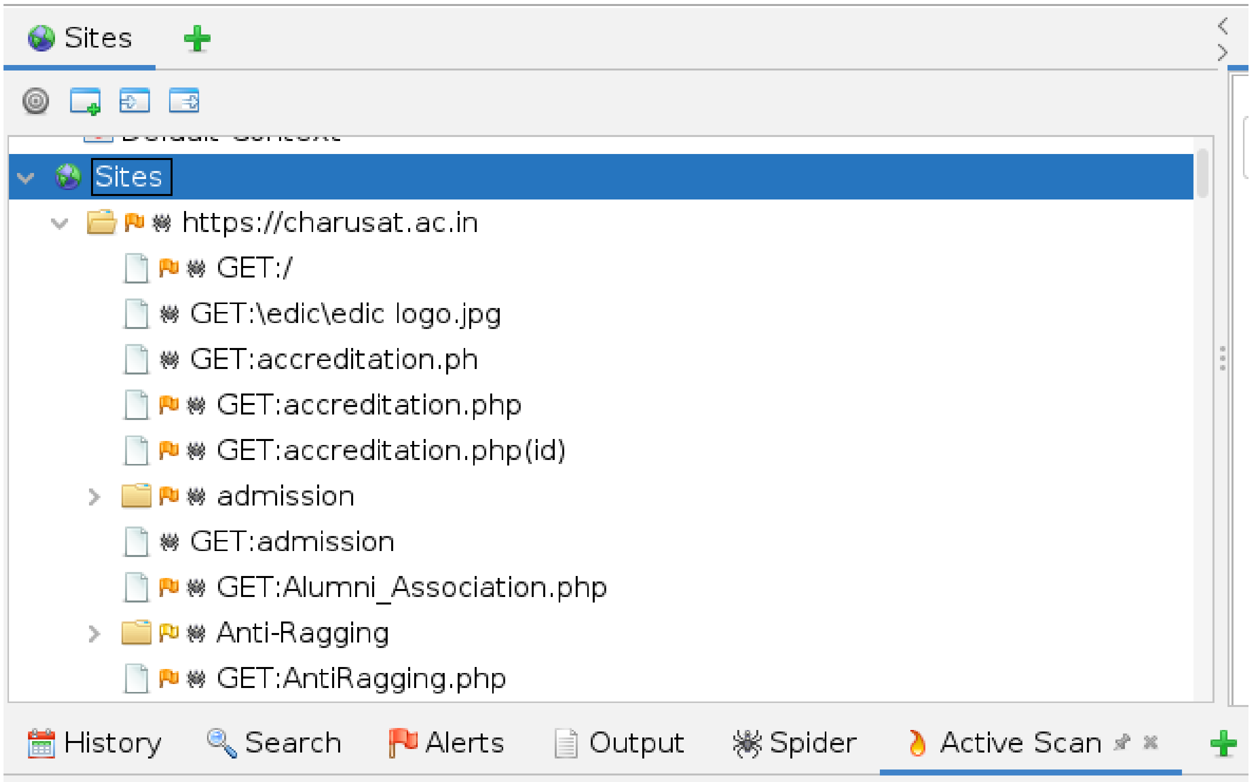
Progress: 0: http://charusat.ac.in Current Scans: 1 Num Requests: 3108 New Alerts: 0

Sent Messages Filtered Messages

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
12,918	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/extensions/...	404	Not Found	70 ms	270 bytes	196 bytes
12,919	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/css/assets/slick.css	404	Not Found	76 ms	270 bytes	196 bytes
12,920	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/extensions/...	404	Not Found	140 ms	267 bytes	196 bytes
12,921	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/extensions/...	404	Not Found	152 ms	270 bytes	196 bytes
12,922	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/extensions/...	404	Not Found	152 ms	270 bytes	196 bytes
12,923	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/revolution.js	404	Not Found	140 ms	270 bytes	196 bytes
12,924	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/slick.min.js	404	Not Found	70 ms	270 bytes	196 bytes
12,925	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/jquery.counterup.min.js	404	Not Found	73 ms	267 bytes	196 bytes
12,926	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/jquery.magnific-popup....	404	Not Found	72 ms	267 bytes	196 bytes
12,927	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/waypoints.min.js	404	Not Found	71 ms	270 bytes	196 bytes
12,928	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/jquery.them...	404	Not Found	74 ms	267 bytes	196 bytes
12,929	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/jquery.sticky.js	404	Not Found	74 ms	267 bytes	196 bytes
12,930	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/revolution/jquery.them...	404	Not Found	75 ms	267 bytes	196 bytes
12,931	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/bootstrap.min.js	404	Not Found	77 ms	270 bytes	196 bytes
12,932	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/assets/owl.carousel.min.js	404	Not Found	72 ms	267 bytes	196 bytes
12,933	08/04/21, 11:41:15 AM	08/04/21, 11:41:15 AM	GET	http://charusat.ac.in/js/vendor/jquery-1.12.4.min.js	404	Not Found	73 ms	267 bytes	196 bytes

Alerts 0 4 9 3 Primary Proxy: localhost:8080 Current Scans 0 0 0 1 0 0 0 0

We can also see the content of website of the left side.



```
Default Context
Sites
  https://charusat.ac.in
    GET:/
    GET:\edic\edic logo.jpg
    GET:accreditation.ph
    GET:accreditation.php
    GET:accreditation.php(id)
    admission
    GET:admission
    GET:Alumni_Association.php
    Anti-Ragging
    GET:AntiRagging.php
```

Conclusion:

In this practical we learned about OWASP-ZAP tool and performed Web Application Vulnerability using the tool on different websites.