Mariam Osama Saleh
9/16/2023

Introduction to OWASP ZAP

Contents

Mariam Osama Saleh
9/16/2023

What is OWASP ZAP and Why

ZAP (sometimes referred to as Zed Attack Proxy or OWASP ZAP) is an open-source application security testing tool that is popular among software developers, enterprise security teams, and penetration testers alike. Specifically, ZAP is a dynamic application security testing tool, which means that it runs active tests against the running application. These tests identify potential security vulnerabilities within the application and backing APIs, equipping engineers with the information to fix any found issues.

One thing that sets ZAP apart from other web application security testing tools is its ability to be automated. While it is still frequently used by penetration testers or individuals running manual security tests, ZAP's automation via API has allowed it to be used at scale within engineering teams such as Facebook, Intuit, and more.

ZAP can be used to identify a wide range of vulnerabilities, including SQL injection, cross-site scripting (XSS), insecure direct object references (IDOR), and broken authentication and session management.

ZAP works by acting as a proxy server between the user's browser and the web application being tested. This allows ZAP to intercept and inspect all traffic between the browser and the web application, both requests and responses. ZAP can then use this information to identify vulnerabilities and generate reports.

ZAP is a very versatile tool and can be used in a variety of ways. It can be used to perform manual security testing, automated security testing, and continuous integration/continuous delivery (CI/CD) security testing. ZAP can also be used to create custom security scans and to integrate with other security tools.

Mariam Osama Saleh
9/16/2023

Here are some of the key features and benefits of OWASP ZAP:

- It is open-source and free to use.
- It is easy to install and use, even for beginners.
- It can be used to identify a wide range of vulnerabilities.
- It is very versatile and can be used in a variety of ways.
- It is actively maintained and updated.
- Can be used in CI/CD for automated testing.
- Works well with tools like Burp Suite.
- It is actively maintained and updated.
- It is extensible.
- It is well-documented.
- It has a large community.

ZAP can be used to improve the security of Kubernetes clusters by identifying and fixing vulnerabilities in the applications running in the cluster.

One of the key advantages of using OWASP ZAP in a Kubernetes cluster is that it can be used to perform automated security testing. This can be done by integrating ZAP with a continuous integration/continuous delivery (CI/CD) pipeline. This allows ZAP to scan the applications in the cluster as part of the build and deployment process. This helps to ensure that the applications are secure before they are deployed to production.

Another advantage of using OWASP ZAP in a Kubernetes cluster is that it can be used to perform dynamic security testing. This means that ZAP can scan the applications while they are running in production. This can be used to identify vulnerabilities that may not be detected by static analysis tools or by automated security testing tools.

Finally, OWASP ZAP can be used to perform manual security testing. This can be done by using ZAP to scan the applications in the cluster manually. This is useful for identifying vulnerabilities that may not be detected by automated security testing tools.

Overall, OWASP ZAP is a powerful and versatile tool that can be used to improve the security of Kubernetes clusters. It can be used to perform automated security testing, dynamic security testing, and manual security testing. ZAP can also be integrated with CI/CD pipelines to automate the security testing process.

Mariam Osama Saleh
9/16/2023

How to install OWASP ZAP

- Linux Installation:
  1. Update Your Linux System
     Before installing OWASP ZAP, it's essential to update your system to ensure that you have the latest packages and security patches. To update your system, open the terminal and type the following command:

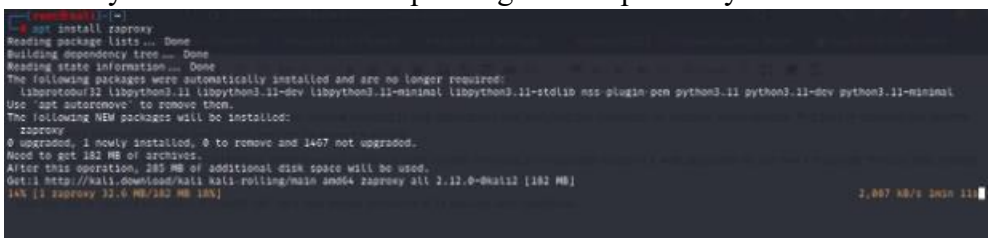
     sudo apt-get update

     Press Enter, and the system will start updating. This may take a few minutes depending on the speed of your internet connection and the number of updates available.

  2. Install OWASP ZAP
     Once your system is up to date, you can install OWASP ZAP. To do so, type the following command in the terminal:

     sudo apt install zaproxy

     Press Enter, and the system will start downloading and installing OWASP ZAP. This may take a few minutes depending on the speed of your internet connection.



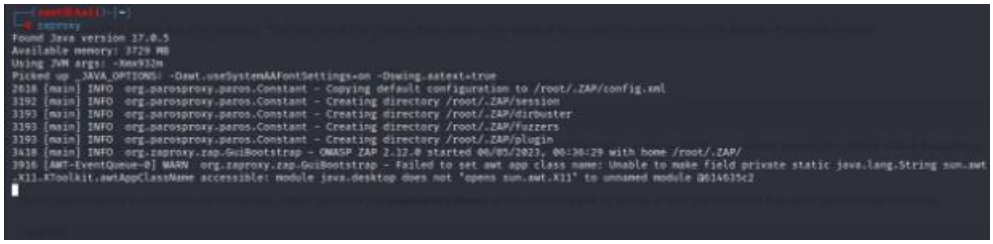
  3. Launch OWASP ZAP

     Once the installation is complete, you can launch OWASP ZAP from the application menu or the command line. To launch it from the command line, type the following command:

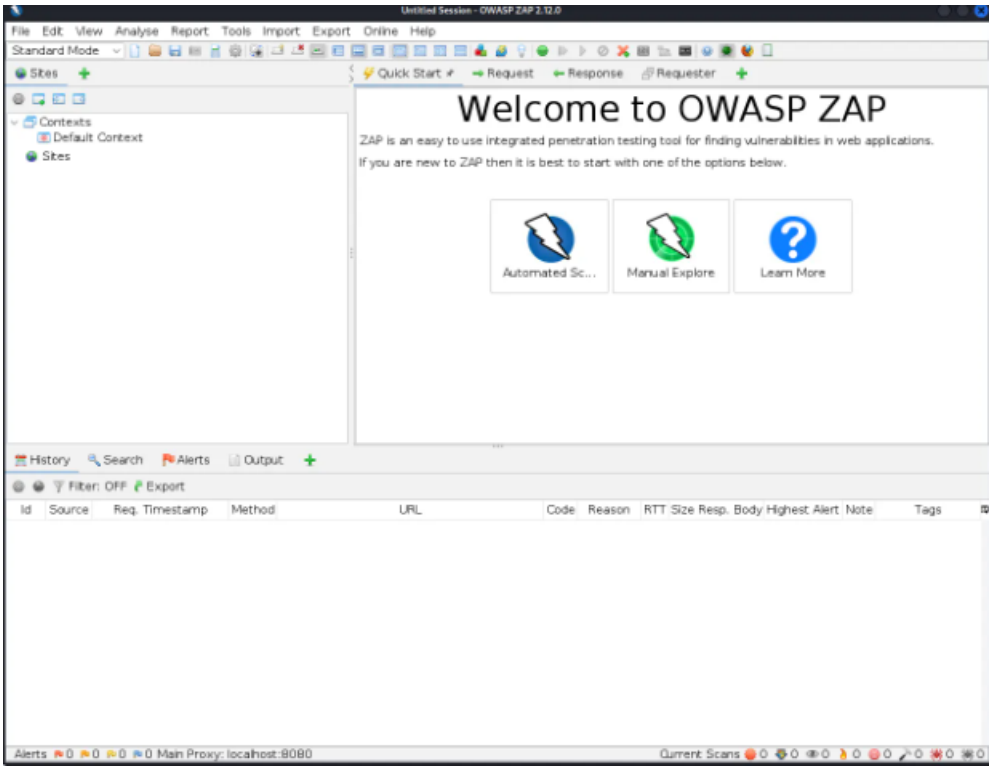
     zaproxy

Mariam Osama Saleh
9/16/2023

Press Enter, and the OWASP ZAP interface will launch. You can now start using OWASP ZAP to test the security of your web applications.



after a few minutes, OWASP ZAP will open up.



- Windows Installation:
  OWASP ZAP Download on Windows
  The first step in setting up OWASP ZAP is to download it on your machine. OWASP ZAP is available for Windows, Mac, and Linux operating systems, and can be downloaded from the OWASP ZAP website.

  How to Install OWASP ZAP on Windows
  Once you have downloaded the appropriate installer for your operating system, simply follow the on-screen instructions to install OWASP ZAP on your machine. The installation process may take a few minutes depending on your system's performance and the size of the installer.

  Guiding Video

Mariam Osama Saleh
9/16/2023

FAQ:

1. Can OWASP ZAP handle authentication-protected applications?
   Yes, OWASP ZAP has robust support for handling authentication-protected applications. It provides various authentication methods, such as form-based authentication, HTTP authentication, and even custom authentication scripts. You can configure OWASP ZAP to simulate user logins and maintain session cookies during your security scans.
2. How can I use OWASP ZAP for API security testing?
   OWASP ZAP is not limited to web application testing; it can also be used for API security testing. You can configure ZAP to intercept and analyze API calls, send requests, and inspect responses. By following specific guidelines, such as setting up authentication and handling custom headers, you can effectively test the security of your APIs.
3. Can OWASP ZAP be integrated into my CI/CD pipeline?
   Yes, OWASP ZAP provides command-line options and a comprehensive API that allows for seamless integration into continuous integration and continuous delivery (CI/CD) pipelines. You can automate security scans using OWASP ZAP and incorporate it as part of your automated testing and deployment process.
4. Does OWASP ZAP support scripting and automation?
   Absolutely! OWASP ZAP supports scripting using various languages like ZAP API, Python, and JavaScript. You can create custom scripts to automate repetitive tasks, perform targeted security checks, and extend the functionality of OWASP ZAP to suit your specific testing requirements.
5. Can OWASP ZAP generate detailed reports of vulnerabilities?
   Yes, OWASP ZAP provides comprehensive reporting capabilities. You can generate detailed reports containing information about identified vulnerabilities, their severity, and suggested remediation steps. The reports can be exported in various formats, such as HTML, XML, JSON, and more, making it easy to share findings with stakeholders.

Mariam Osama Saleh
9/16/2023

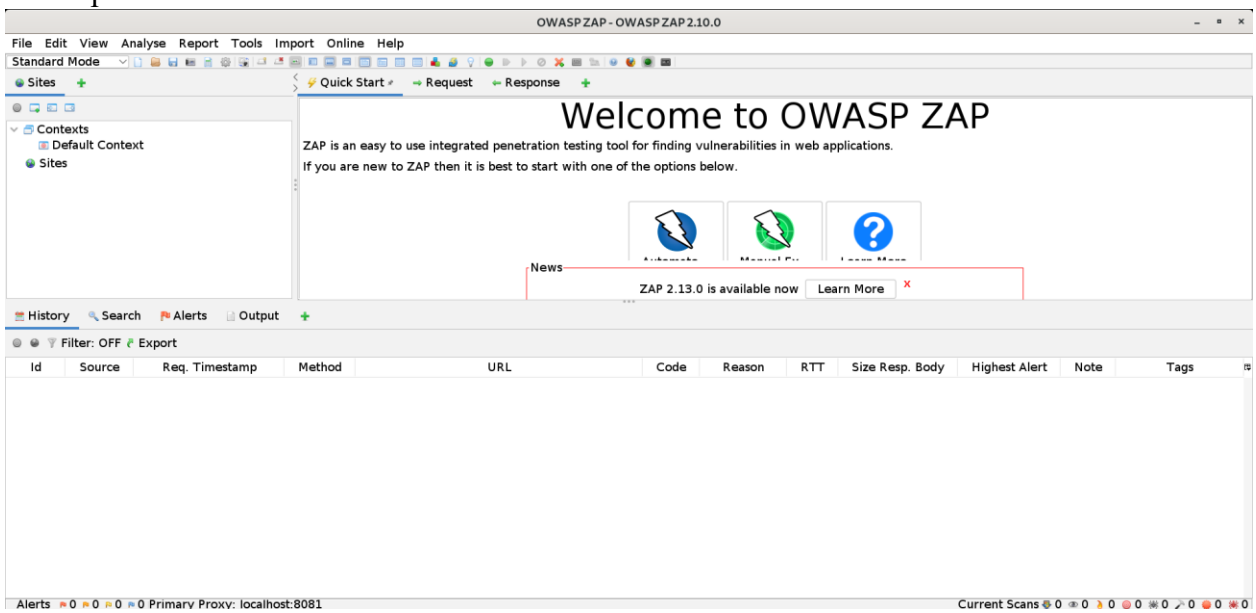
DEMO

OWASP ZAP Web-App Scanning Steps:

1) After booting Metasploitable and logging in, run the command “ifconfig” to get the system’s IP address.

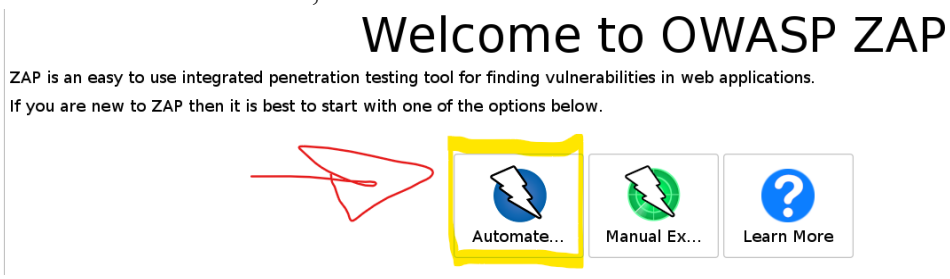
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:be:97:11
          inet addr:192.168.232.129  Bcast:192.168.232.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febe:9711/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31176 (30.4 KB)  TX bytes:38344 (37.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37973 (37.0 KB)  TX bytes:37973 (37.0 KB)
```

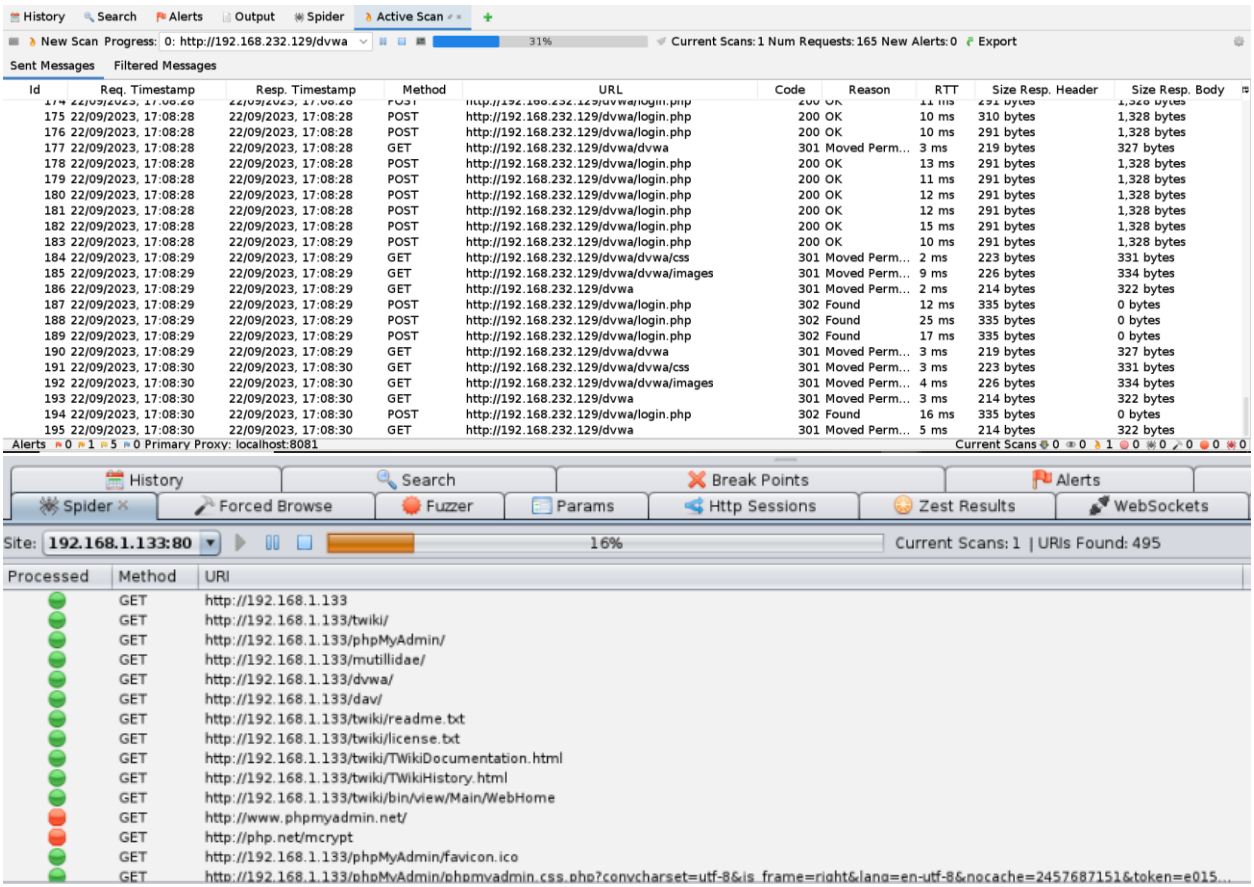
2) Now open OWASP ZAP tool



Mariam Osama Saleh
9/16/2023

3) Now, simple input the address (http://192.168.232.129/dvwa/ in my case) into the ‘URL to attack’ box and select, “Attack”:





It will also list any security issues it finds and place them under the “Alerts” tab.

4) Clicking on the tab will show the following alerts:

- Alerts (6)
  - Path Traversal (8)
  - Cookie set without HttpOnly flag (165)
  - Password Autocomplete in browser (139)
  - Private IP disclosure (4535)
  - X-Content-Type-Options header missing (4686)
  - X-Frame-Options header not set (4631)

Each folder contains different types of security issues.

5) Click to expand "Path Traversal" folder. As an example.

- Alerts (6)
  - Path Traversal (8)
    - GET: http://192.168.1.133/mutillidae/?page=%2Fetc%2Fpasswd
    - GET: http://192.168.1.133/mutillidae/index.php?forwardurl=https://addons.moz
    - GET: http://192.168.1.133/mutillidae/index.php?page=%2Fetc%2Fpasswd
    - GET: http://192.168.1.133/mutillidae/index.php?page=%2Fetc%2Fpasswd&use
    - POST: http://192.168.1.133/mutillidae/index.php?page=%2Fetc%2Fpasswd
    - POST: http://192.168.1.133/mutillidae/index.php?page=source-viewer.php
    - POST: http://192.168.1.133/mutillidae/index.php?page=source-viewer.php
    - POST: http://192.168.1.133/mutillidae/index.php?page=text-file-viewer.php

On the right side you will see an explanation of the issue:

Path Traversal

URL:	http://192.168.1.133/mutillidae/index.php?page=%2Fetc%2Fpasswd
Risk:	High
Reliability:	Warning
Parameter:	page
Attack:	root:x:0:0
Evidence:	root:x:0:0
CWE Id:	22
WASC Id:	33

Description:

Mariam Osama Saleh
9/16/2023

It is tagged as a red flag “High” level warning. OWASP ZAP then explains the error:

“The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal…
The most basic Path Traversal attack uses the “../” special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the “../” sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding (“..%u2216” or “..%c0%af”) of the forward slash character, backslash characters (“..\”) on Windows-based servers, URL encoded characters “%2e%2e%2f”), and double URL encoding (“..%255c”) of the backslash character…“

Basically this means that we can view files or folders on the webserver just by using a special sequence. And OWASP ZAP gives us the exact command to enter:

http://192.168.1.133/mutillidae/?page=%2Fetc%2Fpasswd

The command above will list a webpage on the Metasploitable server. If we enter this URL in a web browser on our Kali system, it will go to the Metasploitable server and pull up a certain webpage, the “?page=” part followed by the webpage to display.

The page requested in the alert is “%2Fetc%2Fpasswd”. Now this may not look like much, but if you are familiar with Linux, the command becomes “/etc/passwd”, which is the location of the server’s password file!

Entering this command in the web browser in Kali (using your Metasploitable IP address) will return this:

You see what appears to be a normal web page control interface, but if you look in the center window you see this information:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false snmp:x:115:65534::/var/lib/snmp:/bin/false

This is the content of the Linux password file.

For every alert that OWASP-ZAP finds, it also includes a solution to protect your system from the vulnerability found. As seen below:

Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist).

Automatic scanning is just one feature of OWASP-ZAP, but you can see how easy it us to find and correct some serious vulnerabilities very quickly. OWASP-ZAP is a great tool for both penetration testers and software coders.