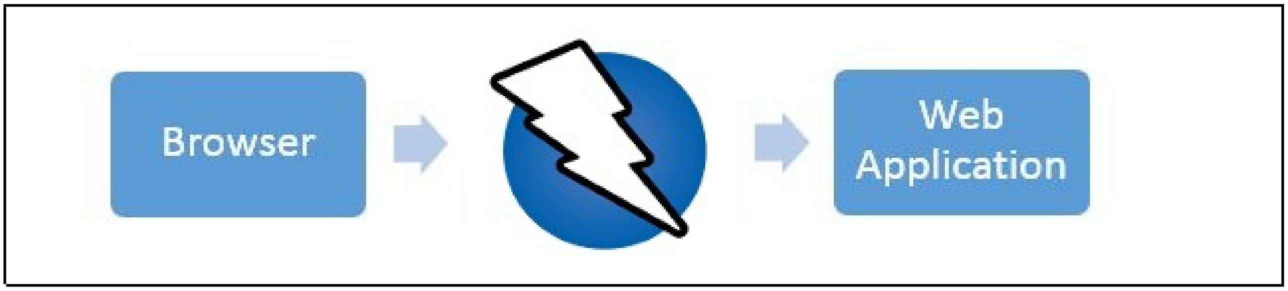
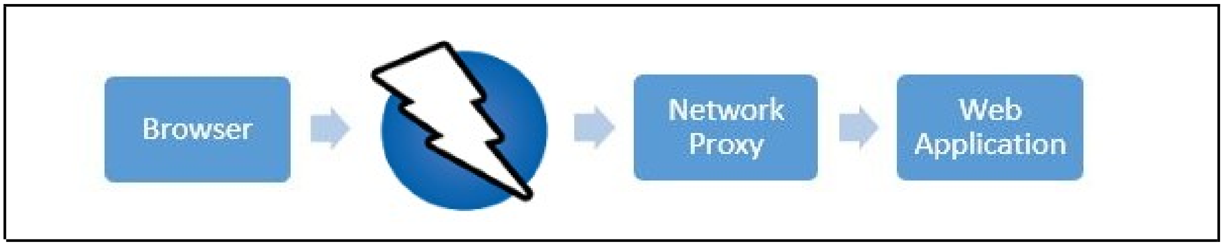
ZAP (Zed Attack Proxy)

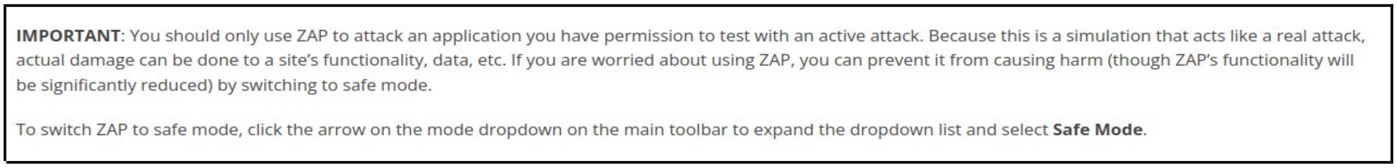
At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.



If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.



1. 1. ZAP provides functionality for a range of skill levels – from developers, to testers new to security testing, to security testing specialists.
2. ZAP has versions for each major OS and Docker, so you are not tied to a single OS.
3. ZAP is open-source, the source code can be examined to see exactly how the functionality is implemented.



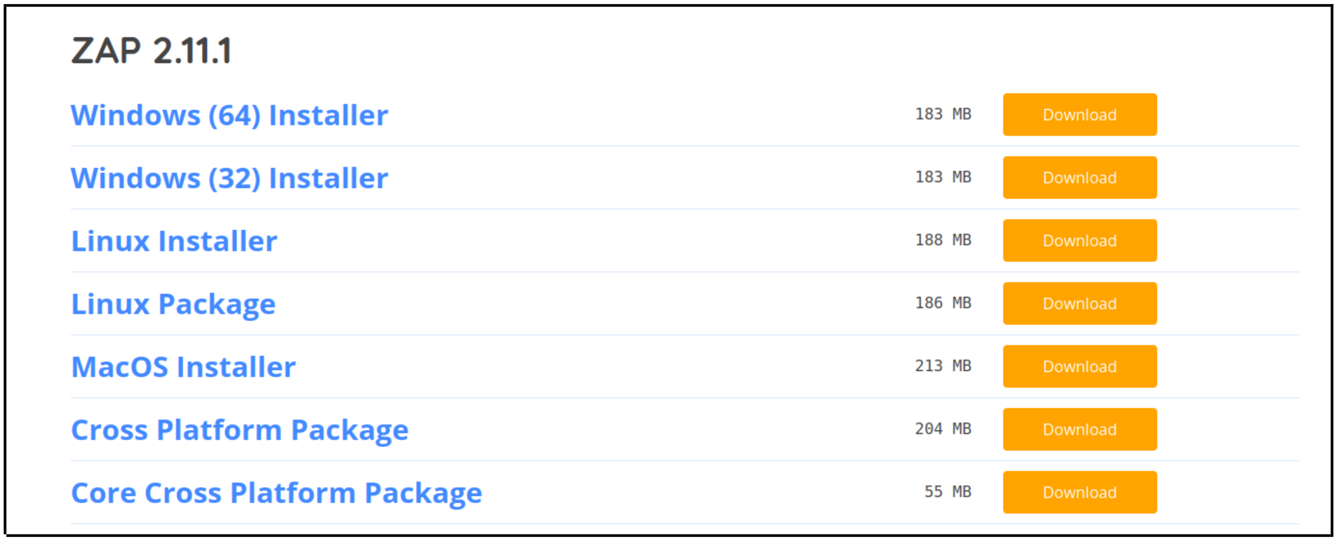
IMPORTANT: You should only use ZAP to attack an application you have permission to test with an active attack. Because this is a simulation that acts like a real attack, actual damage can be done to a site’s functionality, data, etc. If you are worried about using ZAP, you can prevent it from causing harm (though ZAP’s functionality will be significantly reduced) by switching to safe mode.

To switch ZAP to safe mode, click the arrow on the mode dropdown on the main toolbar to expand the dropdown list and select **Safe Mode**.

Installing ZAP

To download ZAP, follow this link https://www.zaproxy.org/download/

Choose the appropriate installer for your system and click Download button.I will explain how you can download and install the ZAP of the Linux version.

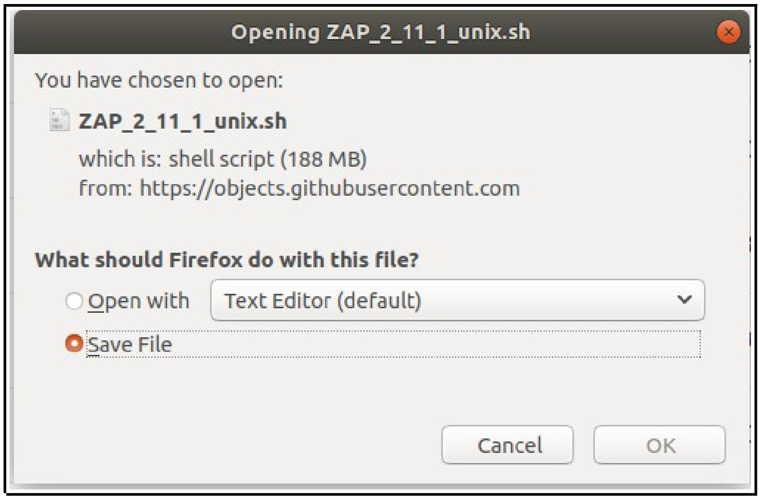


ZAP 2.11.1

Windows (64) Installer	183 MB	Download
Windows (32) Installer	183 MB	Download
Linux Installer	188 MB	Download
Linux Package	186 MB	Download
MacOS Installer	213 MB	Download
Cross Platform Package	204 MB	Download
Core Cross Platform Package	55 MB	Download

1- Click Download button for Linux Installer

2- Choose Save File option then click OK



Opening ZAP_2_11_1_unix.sh

You have chosen to open:

ZAP_2_11_1_unix.sh

which is: shell script (188 MB)
from: https://objects.githubusercontent.com

What should Firefox do with this file?

○ Open with Text Editor (default)

● Save File

4- Open Terminal and go to the directory that you download ZAP Linux Installer.

5- Write this command to install ZAP which is extended such as .sh. The installer’s name may change because of the installer’s version, so type your installer’s name which is .sh extended file.

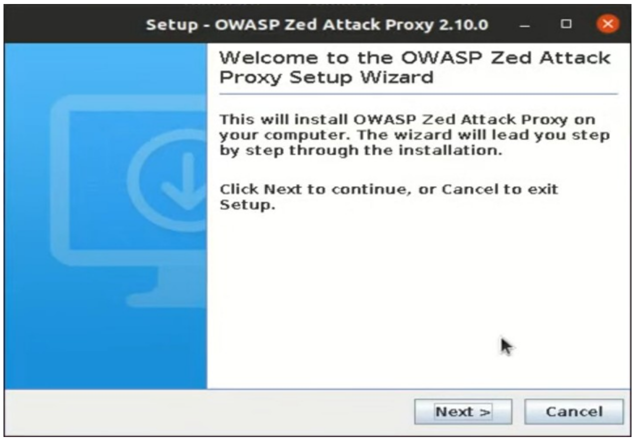
→
```
chmod o+x ZAP_2_11_1_unix.sh
```

→
```
./ZAP_2_11_1_unix.sh
```

If you face with an error, write this command with sudo at the beginning of the command. Otherwise do not execute this code

→
```
sudo ./ZAP_2_11_1_unix.sh
```

6-Click Next



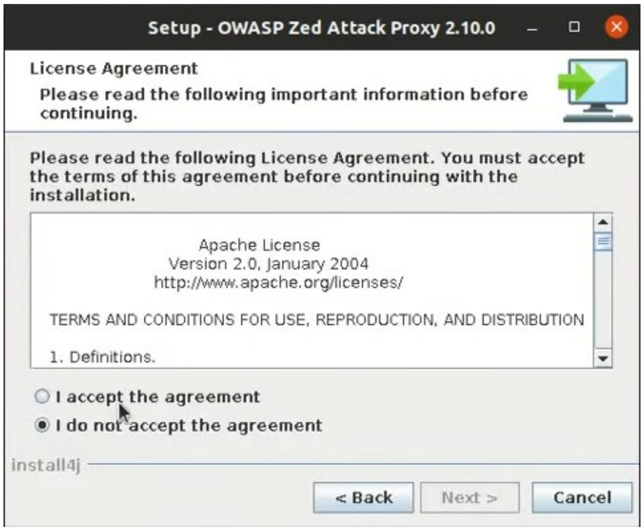
Setup - OWASP Zed Attack Proxy 2.10.0

Welcome to the OWASP Zed Attack Proxy Setup Wizard

This will install OWASP Zed Attack Proxy on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

7-Accept the agreement



Setup - OWASP Zed Attack Proxy 2.10.0

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

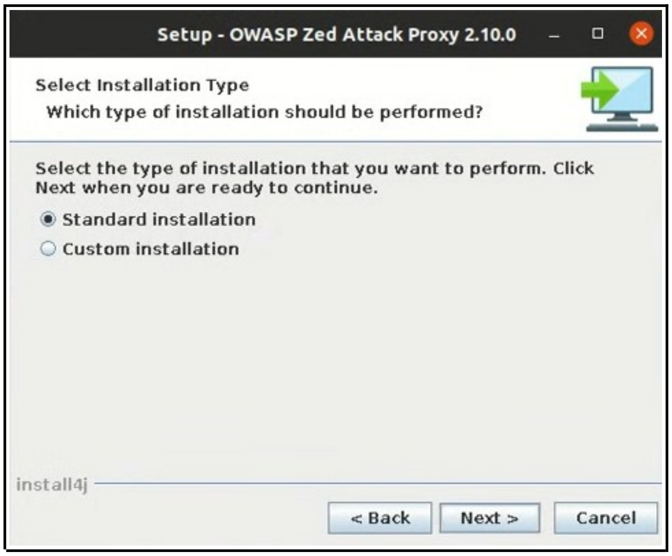
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

○ I accept the agreement

● I do not accept the agreement

8- Choose Standard installation



Setup - OWASP Zed Attack Proxy 2.10.0

Select Installation Type

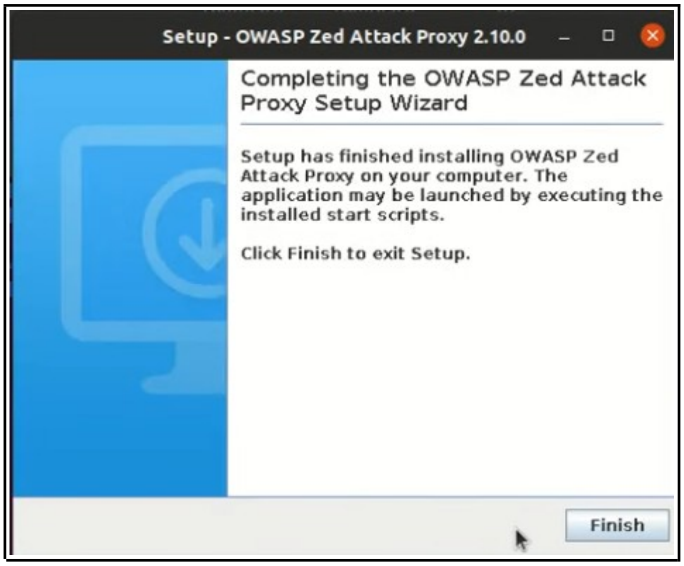
Which type of installation should be performed?

Select the type of installation that you want to perform. Click Next when you are ready to continue.

● Standard installation

○ Custom installation

9- If you see this, installation is successful. OWASP ZAP can be run successfully.



Setup - OWASP Zed Attack Proxy 2.10.0

Completing the OWASP Zed Attack Proxy Setup Wizard

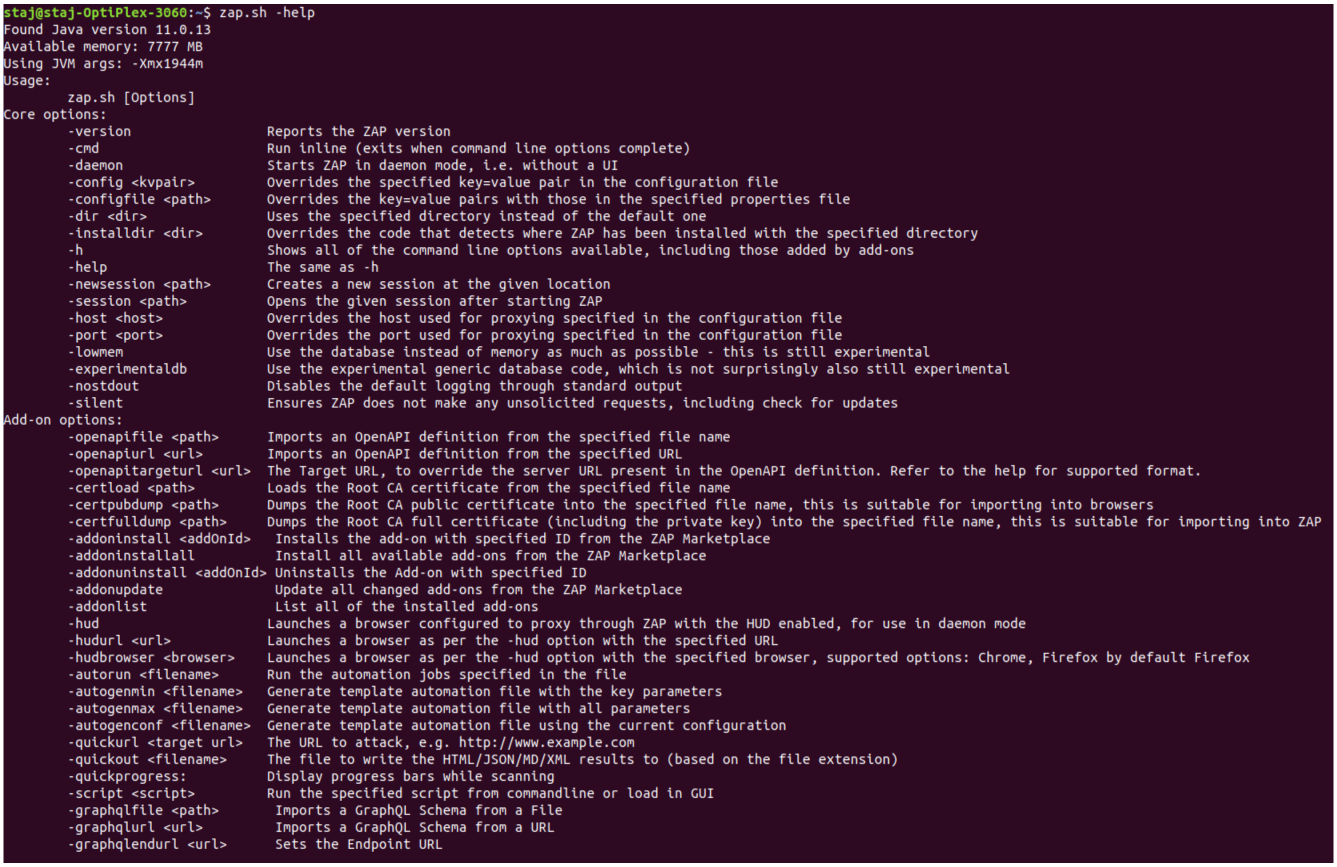
Setup has finished installing OWASP Zed Attack Proxy on your computer. The application may be launched by executing the installed start scripts.

Click Finish to exit Setup.

After these steps, we can run OWASP ZAP successfully. We will use OWASP ZAP on Linux Command Line.How to run and use OWASP ZAP with command line interfece will be explained in next step.

ZAP Command Line Interface

When you type “ zap.sh -help “, you can see the usage of ZAP from command line.



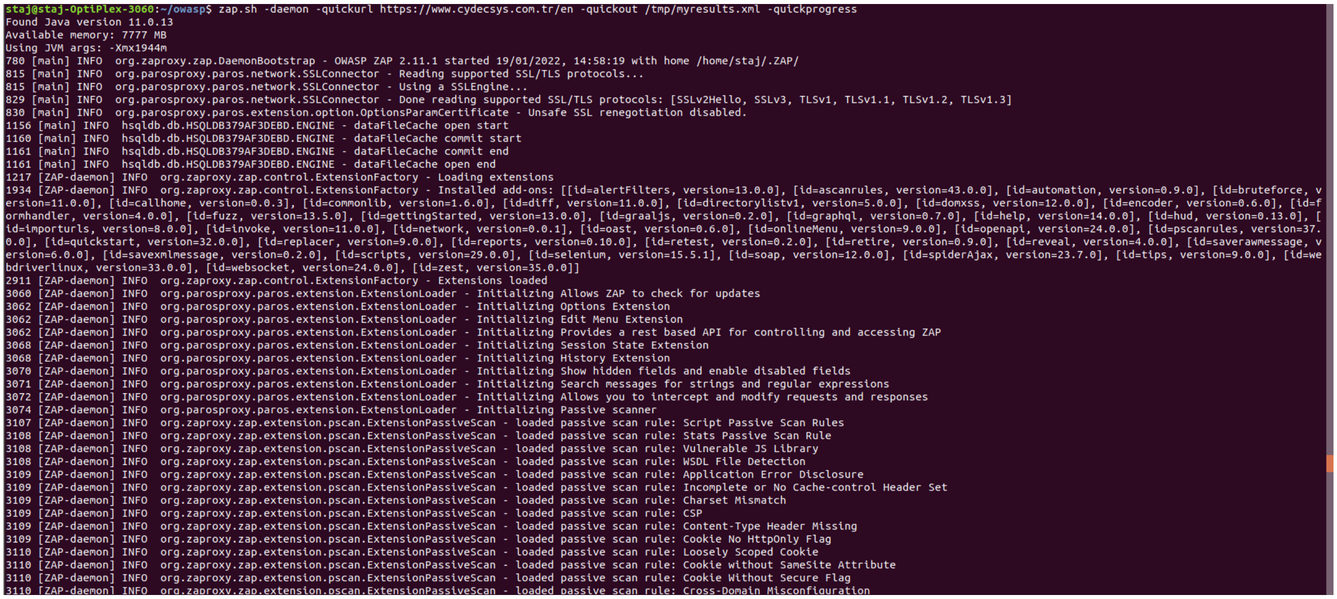
```
staj@staj-OptiPlex-3060:~$ zap.sh -help
Found Java version 11.0.13
Available memory: 7777 MB
Using JVM args: -Xmx1944m
Usage:
        zap.sh [Options]
Core options:
        -version                 Reports the ZAP version
        -cmd                     Run inline (exits when command line options complete)
        -daemon                  Starts ZAP in daemon mode, i.e. without a UI
        -config <kvpair>         Overrides the specified key=value pair in the configuration file
        -configfile <path>       Overrides the key=value pairs with those in the specified properties file
        -dir <dir>               Uses the specified directory instead of the default one
        -installdir <dir>        Overrides the code that detects where ZAP has been installed with the specified directory
        -h                       Shows all of the command line options available, including those added by add-ons
        -help                    The same as -h
        -newsession <path>       Creates a new session at the given location
        -session <path>          Opens the given session after starting ZAP
        -host <host>             Overrides the host used for proxying specified in the configuration file
        -port <port>             Overrides the port used for proxying specified in the configuration file
        -lowmem                  Use the database instead of memory as much as possible - this is still experimental
        -experimentaldb          Use the experimental generic database code, which is not surprisingly also still experimental
        -nostdout                Disables the default logging through standard output
        -silent                  Ensures ZAP does not make any unsolicited requests, including check for updates
Add-on options:
        -openapifile <path>      Imports an OpenAPI definition from the specified file name
        -openapiurl <url>        Imports an OpenAPI definition from the specified URL
        -openapitargeturl <url>  The Target URL, to override the server URL present in the OpenAPI definition. Refer to the help for supported format.
        -certload <path>         Loads the Root CA certificate from the specified file name
        -certpubdump <path>      Dumps the Root CA public certificate into the specified file name, this is suitable for importing into browsers
        -certfulldump <path>     Dumps the Root CA full certificate (including the private key) into the specified file name, this is suitable for importing into ZAP
        -addoninstall <addOnId>   Installs the add-on with specified ID from the ZAP Marketplace
        -addoninstallall          Install all available add-ons from the ZAP Marketplace
        -addonuninstall <addOnId> Uninstalls the Add-on with specified ID
        -addonupdate              Update all changed add-ons from the ZAP Marketplace
        -addonlist                List all of the installed add-ons
        -hud                     Launches a browser configured to proxy through ZAP with the HUD enabled, for use in daemon mode
        -hudurl <url>            Launches a browser as per the -hud option with the specified URL
        -hudbrowser <browser>    Launches a browser as per the -hud option with the specified browser, supported options: Chrome, Firefox by default Firefox
        -autorun <filename>      Run the automation jobs specified in the file
        -autogenmin <filename>   Generate template automation file with the key parameters
        -autogenmax <filename>   Generate template automation file with all parameters
        -autogenconf <filename>  Generate template automation file using the current configuration
        -quickurl <target url>   The URL to attack, e.g. http://www.example.com
        -quickout <filename>     The file to write the HTML/JSON/MD/XML results to (based on the file extension)
        -quickprogress:          Display progress bars while scanning
        -script <script>         Run the specified script from commandline or load in GUI
        -graphqlfile <path>       Imports a GraphQL Schema from a File
        -graphqlurl <url>         Imports a GraphQL Schema from a URL
        -graphqlendurl <url>      Sets the Endpoint URL
```

I’ll use ZAP from command line without User Interface so that I will use “ -daemon ” option. Also I will use “ -quickurl “ option to specify the site which will be attacked and “ -quickout “ option to write the results of the attack. If you want to see progress bar while scanning, you can type “-quickprogress “ option, but it does not effect the result of the scan, so it does not mandatory.

To attack website, do this command.

→ zap.sh -daemon -quickurl [website which will be attacked] -quickout [results file directory] - quickprogress

Example: zap.sh -daemon -quickurl http://scanme.nmap.org/ -quickout /tmp/myresults.xml -quickprogress

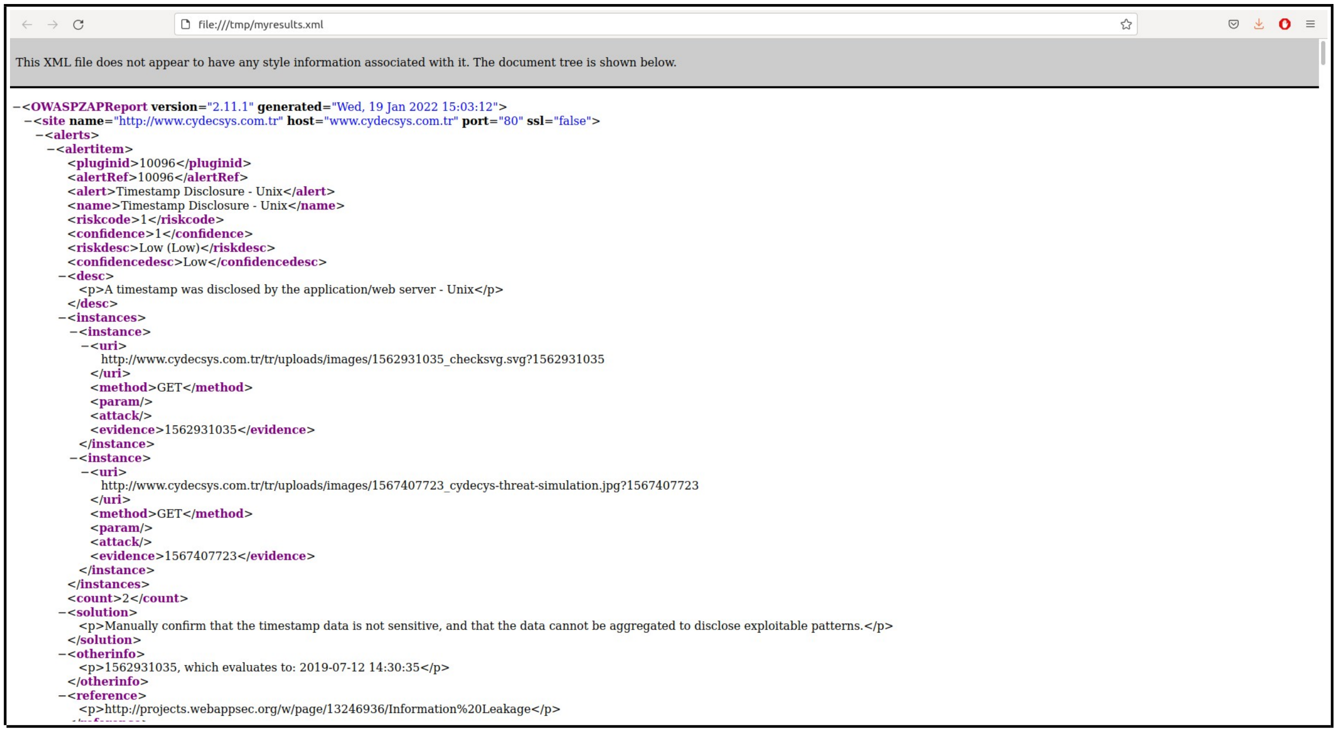


```
staj@staj-OptiPlex-3060:~/owasp$ zap.sh -daemon -quickurl https://www.cydecsys.com.tr/en -quickout /tmp/myresults.xml -quickprogress
Found Java version 11.0.13
Available memory: 7777 MB
Using JVM args: -Xmx1944m
780 [main] INFO  org.zaproxy.zap.DaemonBootstrap - OWASP ZAP 2.11.1 started 19/01/2022, 14:58:19 with home /home/staj/.ZAP/
815 [main] INFO  org.parosproxy.paros.network.SSLConnector - Reading supported SSL/TLS protocols...
815 [main] INFO  org.parosproxy.paros.network.SSLConnector - Using a SSLEngine...
829 [main] INFO  org.parosproxy.paros.network.SSLConnector - Done reading supported SSL/TLS protocols: [SSLv2Hello, SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3]
830 [main] INFO  org.parosproxy.paros.extension.option.OptionsParamCertificate - Unsafe SSL renegotiation disabled.
1156 [main] INFO  hsqldb.db.HSQLDB379AF3DEBD.ENGINE - dataFileCache open start
1160 [main] INFO  hsqldb.db.HSQLDB379AF3DEBD.ENGINE - dataFileCache commit start
1161 [main] INFO  hsqldb.db.HSQLDB379AF3DEBD.ENGINE - dataFileCache commit end
1161 [main] INFO  hsqldb.db.HSQLDB379AF3DEBD.ENGINE - dataFileCache open end
1217 [ZAP-daemon] INFO  org.zaproxy.zap.control.ExtensionFactory - Loading extensions
1934 [ZAP-daemon] INFO  org.zaproxy.zap.control.ExtensionFactory - Installed add-ons: [[id=alertFilters, version=13.0.0], [id=ascanrules, version=43.0.0], [id=automation, version=0.9.0], [id=bruteforce, v
ersion=11.0.0], [id=callhome, version=0.0.3], [id=commonlib, version=1.6.0], [id=diff, version=11.0.0], [id=directorylistv1, version=5.0.0], [id=domxss, version=12.0.0], [id=encoder, version=0.6.0], [id=f
ormhandler, version=4.0.0], [id=fuzz, version=13.5.0], [id=gettingStarted, version=13.0.0], [id=graaljs, version=0.2.0], [id=graphql, version=0.7.0], [id=help, version=14.0.0], [id=hud, version=0.13.0], [
id=importurls, version=8.0.0], [id=invoke, version=11.0.0], [id=network, version=0.0.1], [id=oast, version=0.6.0], [id=onlineMenu, version=9.0.0], [id=openapi, version=24.0.0], [id=pscanrules, version=37.
0.0], [id=quickstart, version=32.0.0], [id=replacer, version=9.0.0], [id=reports, version=0.10.0], [id=retest, version=0.2.0], [id=retire, version=0.9.0], [id=reveal, version=4.0.0], [id=saverawmessage, v
ersion=6.0.0], [id=savexmlmessage, version=0.2.0], [id=scripts, version=29.0.0], [id=selenium, version=15.5.1], [id=soap, version=12.0.0], [id=spiderAjax, version=23.7.0], [id=tips, version=9.0.0], [id=we
bdriverlinux, version=33.0.0], [id=websocket, version=24.0.0], [id=zest, version=35.0.0]]
2911 [ZAP-daemon] INFO  org.zaproxy.zap.control.ExtensionFactory - Extensions loaded
3060 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Allows ZAP to check for updates
3062 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Options Extension
3062 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Edit Menu Extension
3062 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Provides a rest based API for controlling and accessing ZAP
3068 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Session State Extension
3068 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing History Extension
3070 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Show hidden fields and enable disabled fields
3071 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Search messages for strings and regular expressions
3072 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Allows you to intercept and modify requests and responses
3074 [ZAP-daemon] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Passive scanner
3107 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Script Passive Scan Rules
3108 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Stats Passive Scan Rule
3108 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Vulnerable JS Library
3108 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: WSDL File Detection
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Application Error Disclosure
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Incomplete or No Cache-control Header Set
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Charset Mismatch
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: CSP
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Content-Type Header Missing
3109 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie No HttpOnly Flag
3110 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Loosely Scoped Cookie
3110 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie without SameSite Attribute
3110 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie Without Secure Flag
3110 [ZAP-daemon] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cross-Domain Misconfiguration
```

After all these, you can see the results in the file.

→ firefox [results file directory]

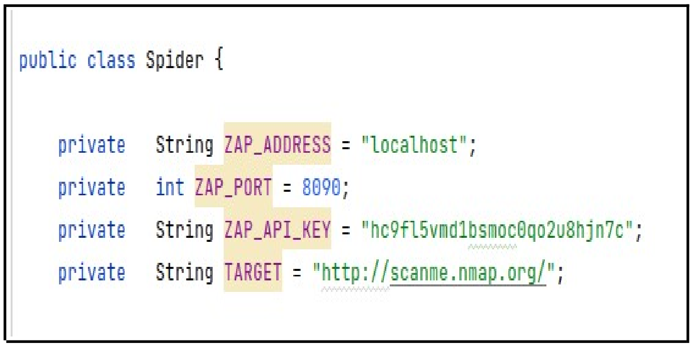
Example: firefox /tmp/myresults.xml



This XML file does not appear to have any style information associated with it. The document tree is shown below.

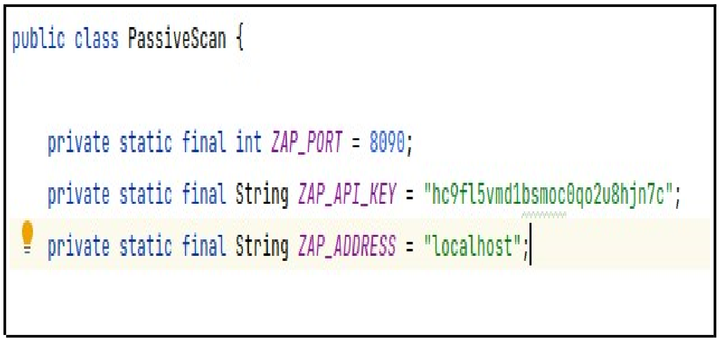
```
−<OWASPZAPReport version="2.11.1" generated="Wed, 19 Jan 2022 15:03:12">
  −<site name="http://www.cydecsys.com.tr" host="www.cydecsys.com.tr" port="80" ssl="false">
    −<alerts>
      −<alertitem>
          <pluginid>10096</pluginid>
          <alertRef>10096</alertRef>
          <alert>Timestamp Disclosure - Unix</alert>
          <name>Timestamp Disclosure - Unix</name>
          <riskcode>1</riskcode>
          <confidence>1</confidence>
          <riskdesc>Low (Low)</riskdesc>
          <confidencedesc>Low</confidencedesc>
        −<desc>
            <p>A timestamp was disclosed by the application/web server - Unix</p>
          </desc>
        −<instances>
          −<instance>
            −<uri>
                http://www.cydecsys.com.tr/tr/uploads/images/1562931035_checksvg.svg?1562931035
              </uri>
              <method>GET</method>
              <param/>
              <attack/>
              <evidence>1562931035</evidence>
            </instance>
          −<instance>
            −<uri>
                http://www.cydecsys.com.tr/tr/uploads/images/1567407723_cydecys-threat-simulation.jpg?1567407723
              </uri>
              <method>GET</method>
              <param/>
              <attack/>
              <evidence>1567407723</evidence>
            </instance>
          </instances>
          <count>2</count>
        −<solution>
            <p>Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.</p>
          </solution>
        −<otherinfo>
            <p>1562931035, which evaluates to: 2019-07-12 14:30:35</p>
          </otherinfo>
        −<reference>
            <p>http://projects.webappsec.org/w/page/13246936/Information%20Leakage</p>
```

ZAP Communication with Java



```
public class Spider {

    private   String ZAP_ADDRESS = "localhost";
    private   int ZAP_PORT = 8090;
    private   String ZAP_API_KEY = "hc9fl5vmd1bsmoc0qo2u8hjn7c";
    private   String TARGET = "http://scanme.nmap.org/";
```

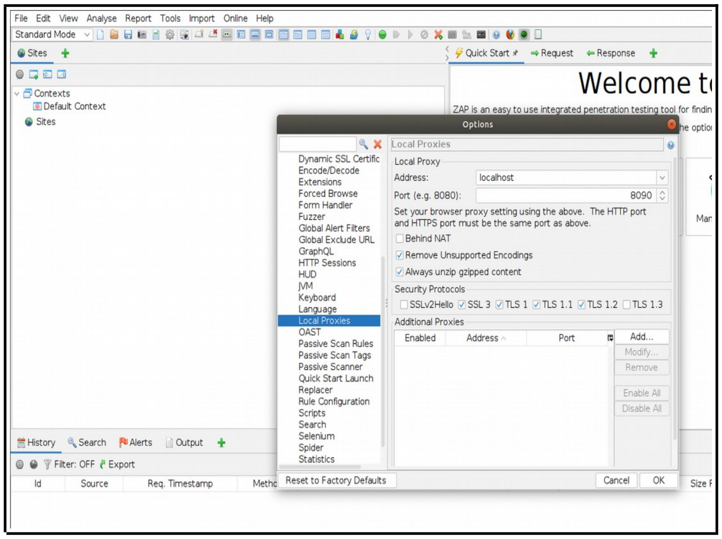


```
public class PassiveScan {

    private static final int ZAP_PORT = 8090;
    private static final String ZAP_API_KEY = "hc9fl5vmd1bsmoc0qo2u8hjn7c";
    private static final String ZAP_ADDRESS = "localhost";
```

We have to type these values before we run our program.
In Spider class,type our target website Url to the TARGET variable.

To find ZAP_PORT, go to Tools → Options → Local Proxies → Port
To find ZAP_ADDRESS, go to Tools → Options → Local Proxies → Address



ZAP is an easy to use integrated penetration testing tool for findin

Local Proxies

Local Proxy

Address: localhost

Port (e.g. 8080): 8090

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

☐ Behind NAT
☑ Remove Unsupported Encodings
☑ Always unzip gzipped content

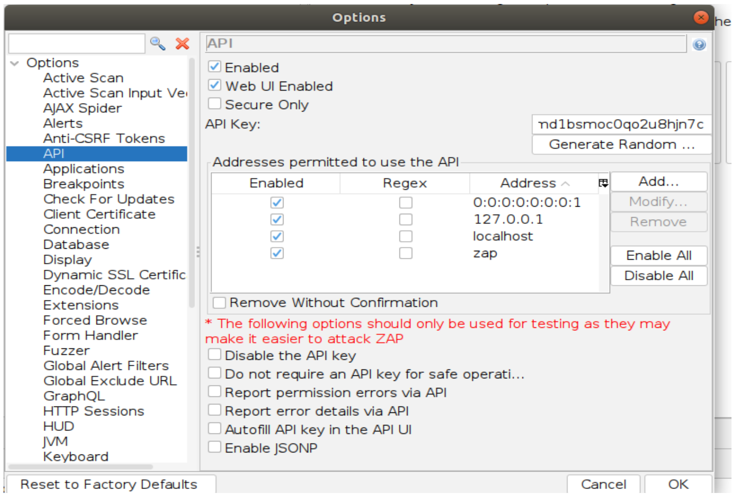
Security Protocols

☐ SSLv2Hello ☑ SSL 3 ☑ TLS 1 ☑ TLS 1.1 ☑ TLS 1.2 ☐ TLS 1.3

Additional Proxies

Enabled	Address	Port

To find ZAP_API_KEY, go to Tools → Options → API → API Key



API

☑ Enabled
☑ Web UI Enabled
☐ Secure Only

API Key: nd1bsmoc0qo2u8hjn7c

Addresses permitted to use the API

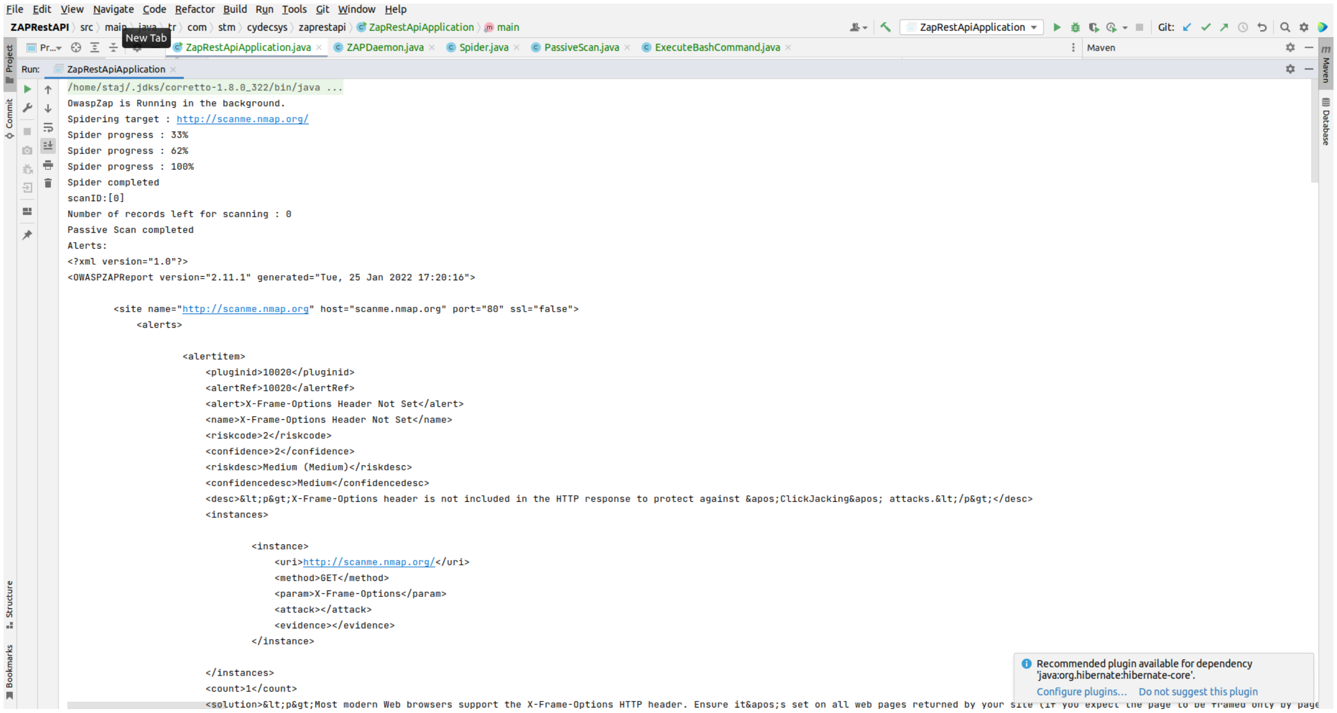
Enabled	Regex	Address
☑	☐	0:0:0:0:0:0:0:1
☑	☐	127.0.0.1
☑	☐	localhost
☑	☐	zap

☐ Remove Without Confirmation

* The following options should only be used for testing as they may make it easier to attack ZAP

☐ Disable the API key
☐ Do not require an API key for safe operati...
☐ Report permission errors via API
☐ Report error details via API
☐ Autofill API key in the API UI
☐ Enable JSONP

After all these steps, we can run our Java Program.


File Edit View Navigate Code Refactor Build Run Tools Git Window Help
ZAPRestAPI src main java tr com stm cydecsys zaprestapi ZapRestApiApplication main
New Tab
ZapRestApiApplication
Git:
Pr...
ZapRestApiApplication.java
ZAPDaemon.java
Spider.java
PassiveScan.java
ExecuteBashCommand.java
Maven
Run: ZapRestApiApplication
Project
Commit
Structure
Bookmarks
Database

```
/home/staj/.jdks/corretto-1.8.0_322/bin/java ...
OwaspZap is Running in the background.
Spidering target : http://scanme.nmap.org/
Spider progress : 33%
Spider progress : 62%
Spider progress : 100%
Spider completed
scanID:[0]
Number of records left for scanning : 0
Passive Scan completed
Alerts:
<?xml version="1.0"?>
<OWASPZAPReport version="2.11.1" generated="Tue, 25 Jan 2022 17:20:16">

        <site name="http://scanme.nmap.org" host="scanme.nmap.org" port="80" ssl="false">
            <alerts>

                <alertitem>
                    <pluginid>10020</pluginid>
                    <alertRef>10020</alertRef>
                    <alert>X-Frame-Options Header Not Set</alert>
                    <name>X-Frame-Options Header Not Set</name>
                    <riskcode>2</riskcode>
                    <confidence>2</confidence>
                    <riskdesc>Medium (Medium)</riskdesc>
                    <confidencedesc>Medium</confidencedesc>
                    <desc>&lt;p&gt;X-Frame-Options header is not included in the HTTP response to protect against &apos;ClickJacking&apos; attacks.&lt;/p&gt;</desc>
                    <instances>

                        <instance>
                            <uri>http://scanme.nmap.org/</uri>
                            <method>GET</method>
                            <param>X-Frame-Options</param>
                            <attack></attack>
                            <evidence></evidence>
                        </instance>

                    </instances>
                    <count>1</count>
                    <solution>&lt;p&gt;Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it&apos;s set on all web pages returned by your site (if you expect the page to be framed only by page
```

Recommended plugin available for dependency 'java:org.hibernate:hibernate-core'.
Configure plugins... Do not suggest this plugin

If you see this, you did everything correctly.