OWASP ZAP

OWASP ZAP: The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience including developers and functional testers who are new to penetration testing.

OWASP (Open Web Application Security Project)

OWASP (Open Web Application Security Project) is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications.

ZAP (Zed Attack Proxy)

The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. ... OWASP Zed Attack Proxy Web Site

WebGoat

WebGoat is a free online tool used to test and uncover application flaws that might otherwise go unnoticed. Issues with SQL injection and cross-site scripting (XSS) often fly under the security radar and issues are often discovered too late.

Installation and configuration of ZAP:

Download Link:

https://github.com/zaproxy/zaproxy/wiki/Downloads

Step1

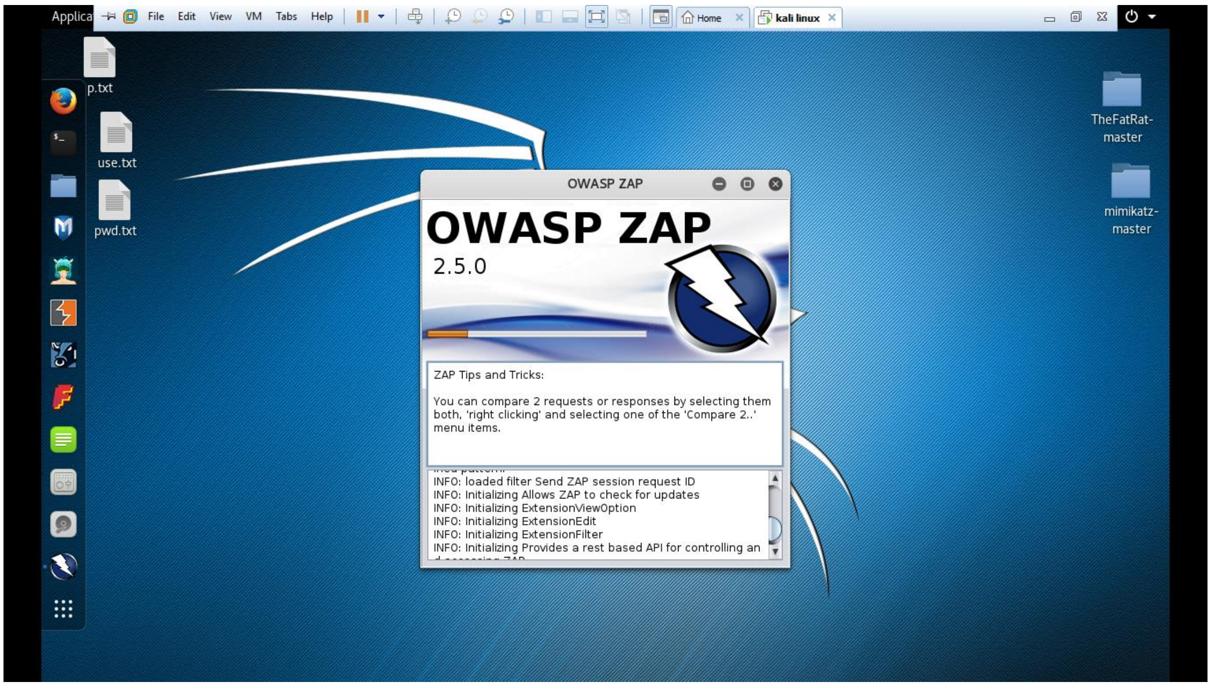
Adding a site to the testing scope

By telling ZAP what the target site is, ZAP can limit the scope of the scan and only scan the target site for vulnerabilities.

1. Open the web application that you want to test.

2. In Zap you will find your website/application displayed under sites.

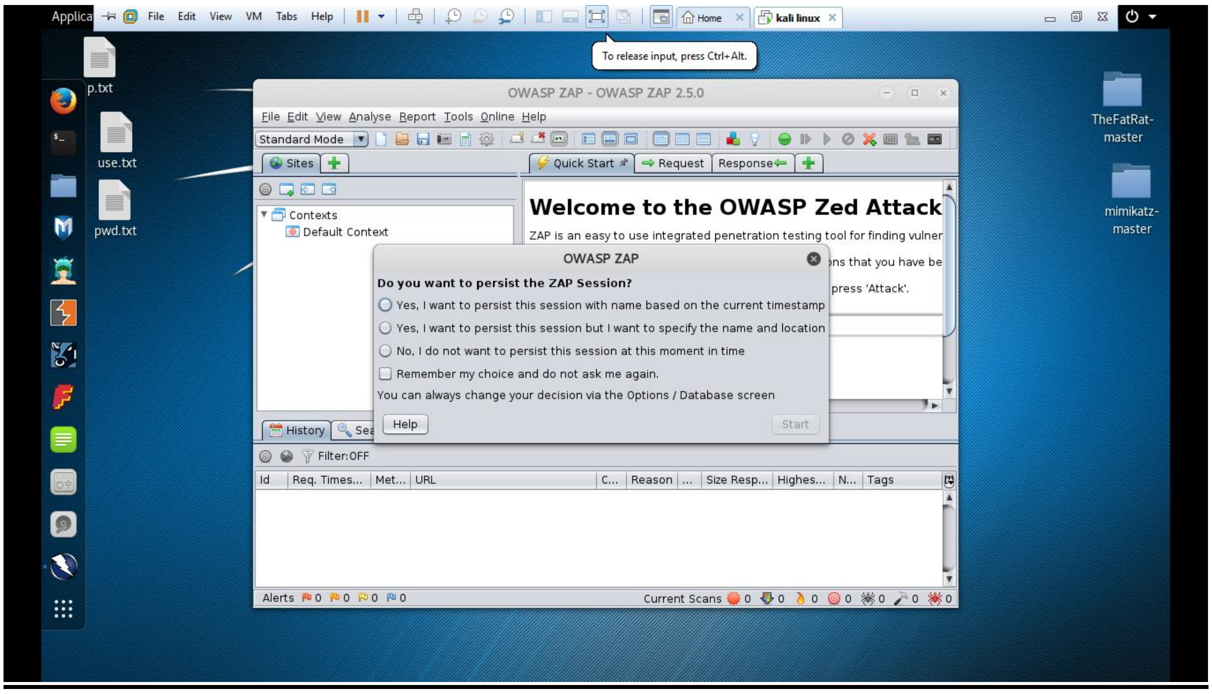
ZAP will spider that URL, then perform an active scan and display the results.



ZAP Tips and Tricks:

You can compare 2 requests or responses by selecting them both, 'right clicking' and selecting one of the 'Compare 2..' menu items.

```
INFO: loaded filter Send ZAP session request ID
INFO: Initializing Allows ZAP to check for updates
INFO: Initializing ExtensionViewOption
INFO: Initializing ExtensionEdit
INFO: Initializing ExtensionFilter
INFO: Initializing Provides a rest based API for controlling an
```


To release input, press Ctrl+Alt.
OWASP ZAP - OWASP ZAP 2.5.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
History
Filter:OFF
Id | Req. Times... | Met... | URL | C... | Reason | ... | Size Resp... | Highes... | N... | Tags
Alerts 0 0 0 0
Current Scans 0 0 0 0 0 0 0

Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulner

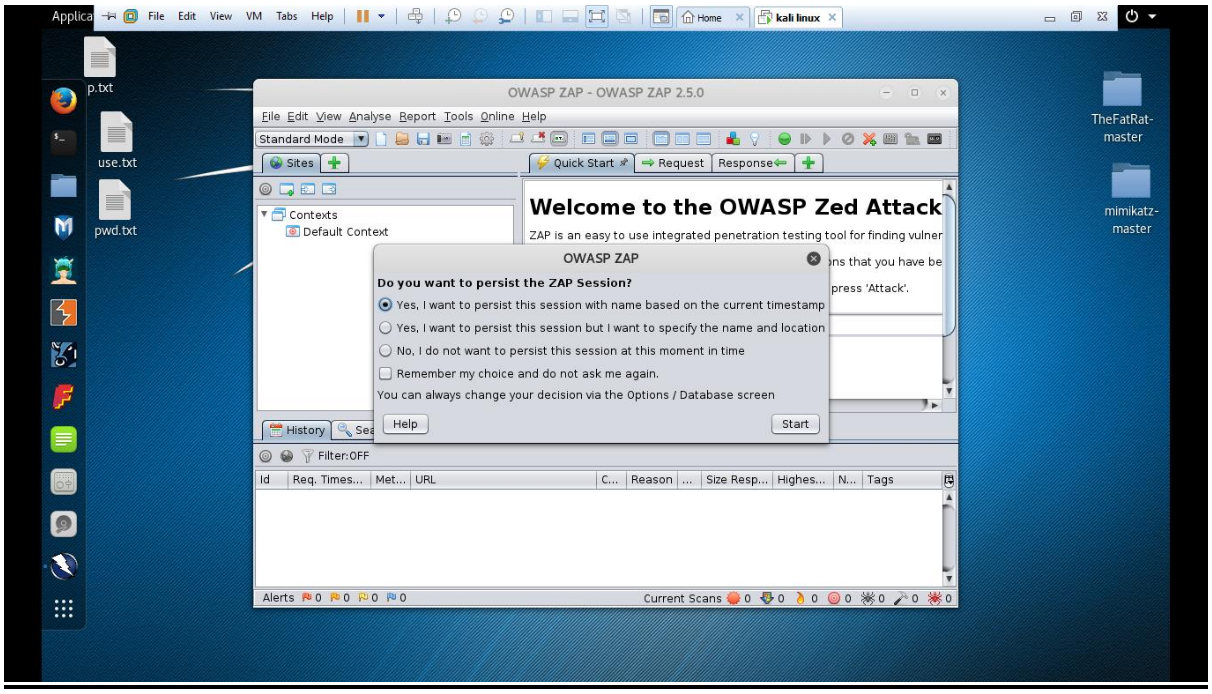
OWASP ZAP

Do you want to persist the ZAP Session?

- ○ Yes, I want to persist this session with name based on the current timestamp
- ○ Yes, I want to persist this session but I want to specify the name and location
- ○ No, I do not want to persist this session at this moment in time
- ☐ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

Help Start



Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulner

OWASP ZAP

Do you want to persist the ZAP Session?

[✓ Yes, I want to persist this session with name based on the current timestamp]
Yes, I want to persist this session but I want to specify the name and location
No, I do not want to persist this session at this moment in time

Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

Help Start

<u>Zap runs on proxy, to set up the proxy in ZAP:</u>

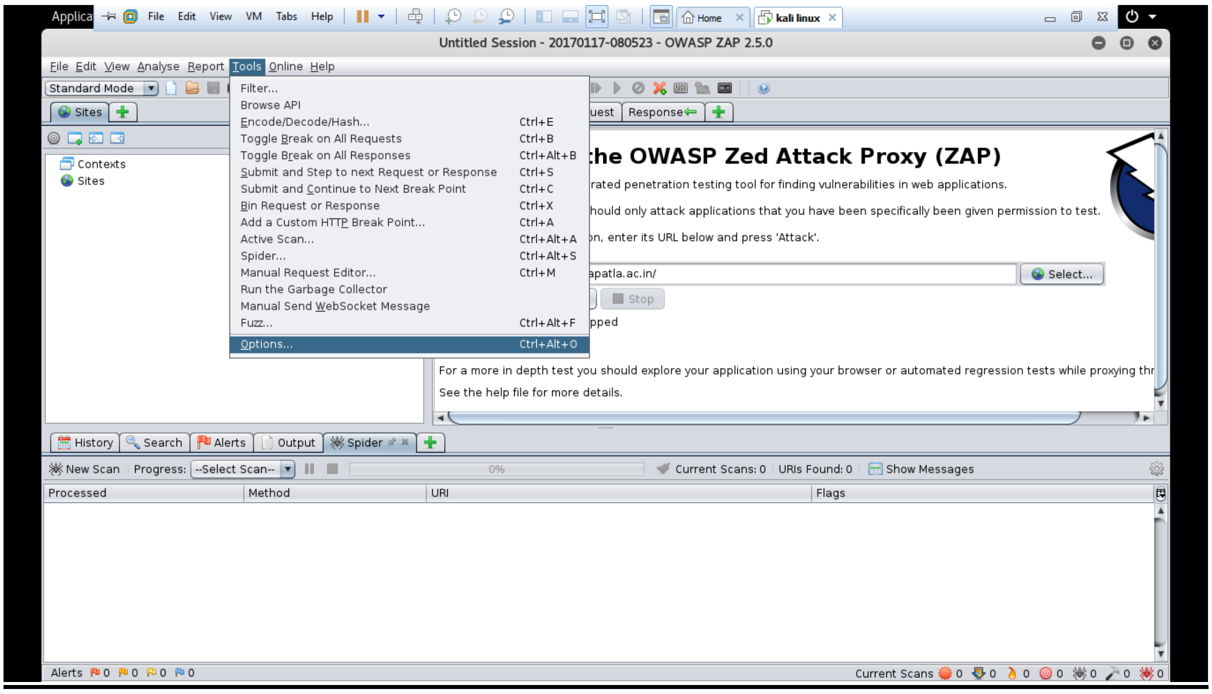
Close all active Firefox browser sessions

ZAP tool -> Tools Menu -> Options -> Local Proxy -> Change Address = 127.0.0.1 Port = 8080.

Mozilla browser -> Tools Menu -> Options -> Advanced tab -> Network -> Settings -> Select Manual Proxy configuration:- HTTP Proxy = 127.0.0.1 Port = 8080.

Now try to connect to your application using your browser.

If you can’t connect to it then check your proxy settings again. You will need to check your browser’s proxy settings, and ZAP’s proxy settings. It’s also worth checking that the application that you are trying to test is running!


Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

File Edit View Analyse Report Tools Online Help
Filter...
Browse API
Encode/Decode/Hash... Ctrl+E
Toggle Break on All Requests Ctrl+B
Toggle Break on All Responses Ctrl+Alt+B
Submit and Step to next Request or Response Ctrl+S
Submit and Continue to Next Break Point Ctrl+C
Bin Request or Response Ctrl+X
Add a Custom HTTP Break Point... Ctrl+A
Active Scan... Ctrl+Alt+A
Spider... Ctrl+Alt+S
Manual Request Editor... Ctrl+M
Run the Garbage Collector
Manual Send WebSocket Message
Fuzz... Ctrl+Alt+F
Options... Ctrl+Alt+O
Standard Mode
Sites
Contexts
Sites
History Search Alerts Output Spider
New Scan Progress: --Select Scan-- 0% Current Scans: 0 URIs Found: 0 Show Messages
Processed Method URI Flags
Alerts 0 0 0 0
Current Scans 0 0 0 0 0 0 0

the OWASP Zed Attack Proxy (ZAP)

rated penetration testing tool for finding vulnerabilities in web applications.

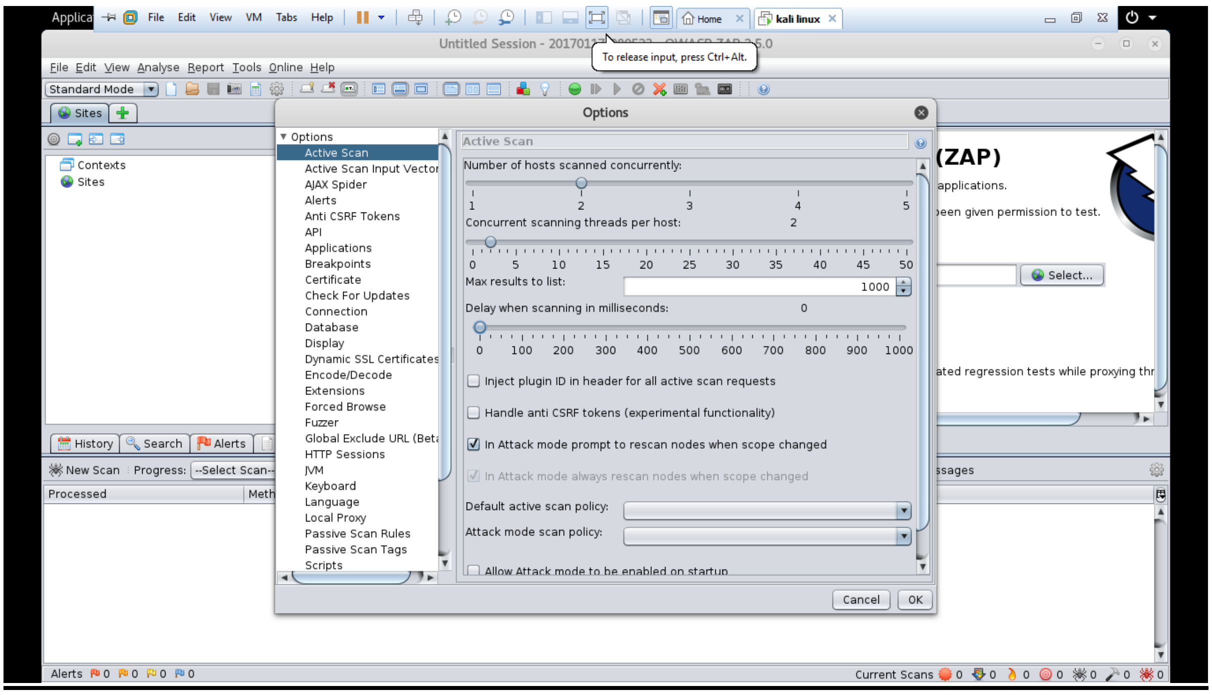
hould only attack applications that you have been specifically been given permission to test.

n, enter its URL below and press 'Attack'.

apatla.ac.in/

For a more in depth test you should explore your application using your browser or automated regression tests while proxying thr

See the help file for more details.


To release input, press Ctrl+Alt.

Active Scan

Number of hosts scanned concurrently: 1 2 3 4 5

Concurrent scanning threads per host: 2

0 5 10 15 20 25 30 35 40 45 50

Max results to list: 1000

Delay when scanning in milliseconds: 0

0 100 200 300 400 500 600 700 800 900 1000

☐ Inject plugin ID in header for all active scan requests

☐ Handle anti CSRF tokens (experimental functionality)

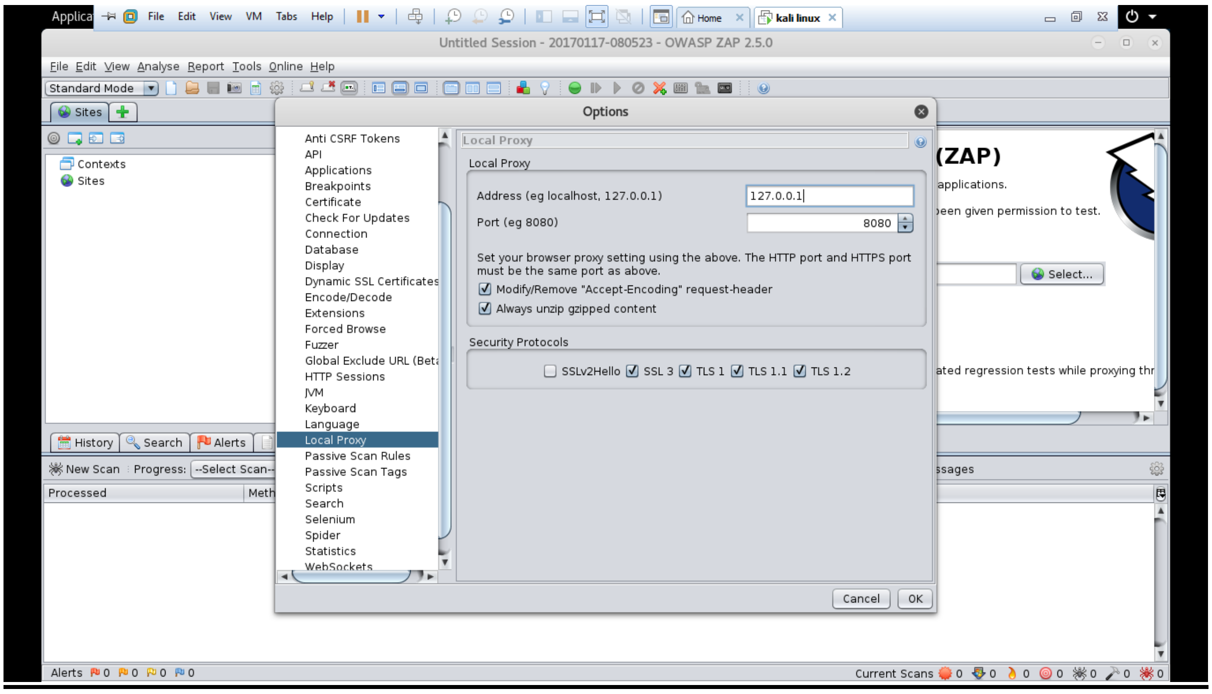
☑ In Attack mode prompt to rescan nodes when scope changed

☑ In Attack mode always rescan nodes when scope changed

Default active scan policy:

Attack mode scan policy:

☐ Allow Attack mode to be enabled on startup


Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

Options

Local Proxy

Address (eg localhost, 127.0.0.1): 127.0.0.1

Port (eg 8080): 8080

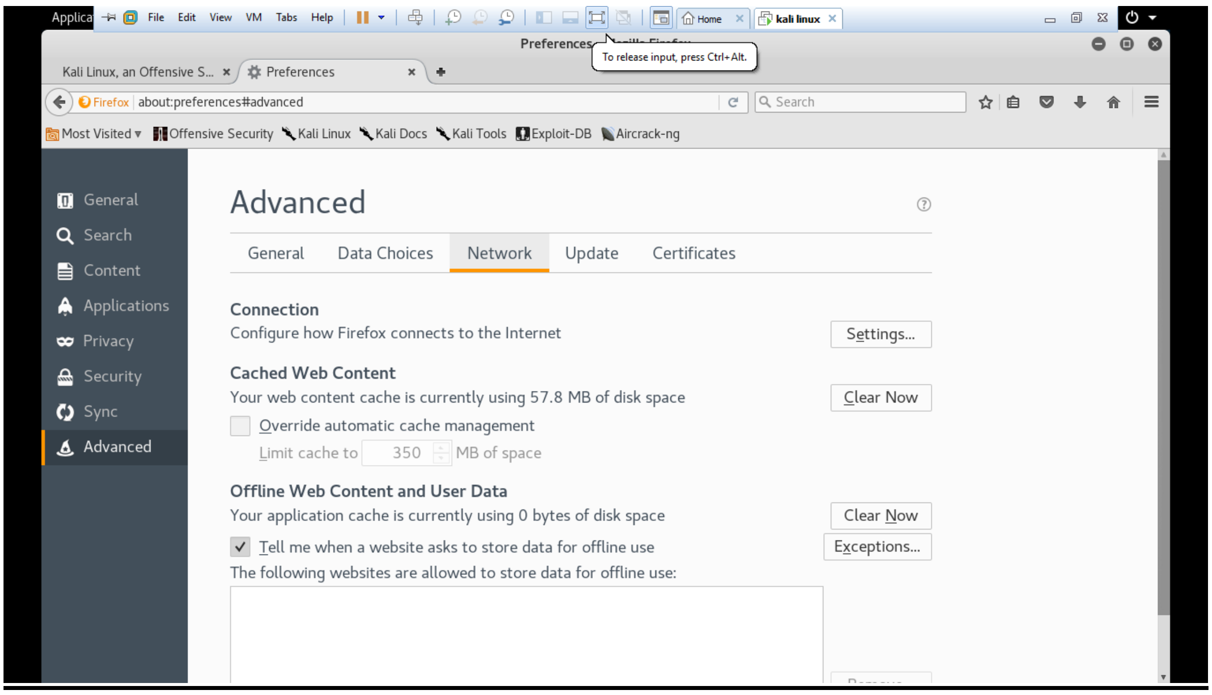
Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

[✓] Modify/Remove "Accept-Encoding" request-header

[✓] Always unzip gzipped content

Security Protocols

[ ] SSLv2Hello [✓] SSL 3 [✓] TLS 1 [✓] TLS 1.1 [✓] TLS 1.2


To release input, press Ctrl+Alt.

about:preferences#advanced

Advanced

General | Data Choices | Network | Update | Certificates

Connection

Configure how Firefox connects to the Internet — Settings...

Cached Web Content

Your web content cache is currently using 57.8 MB of disk space — Clear Now

[ ] Override automatic cache management

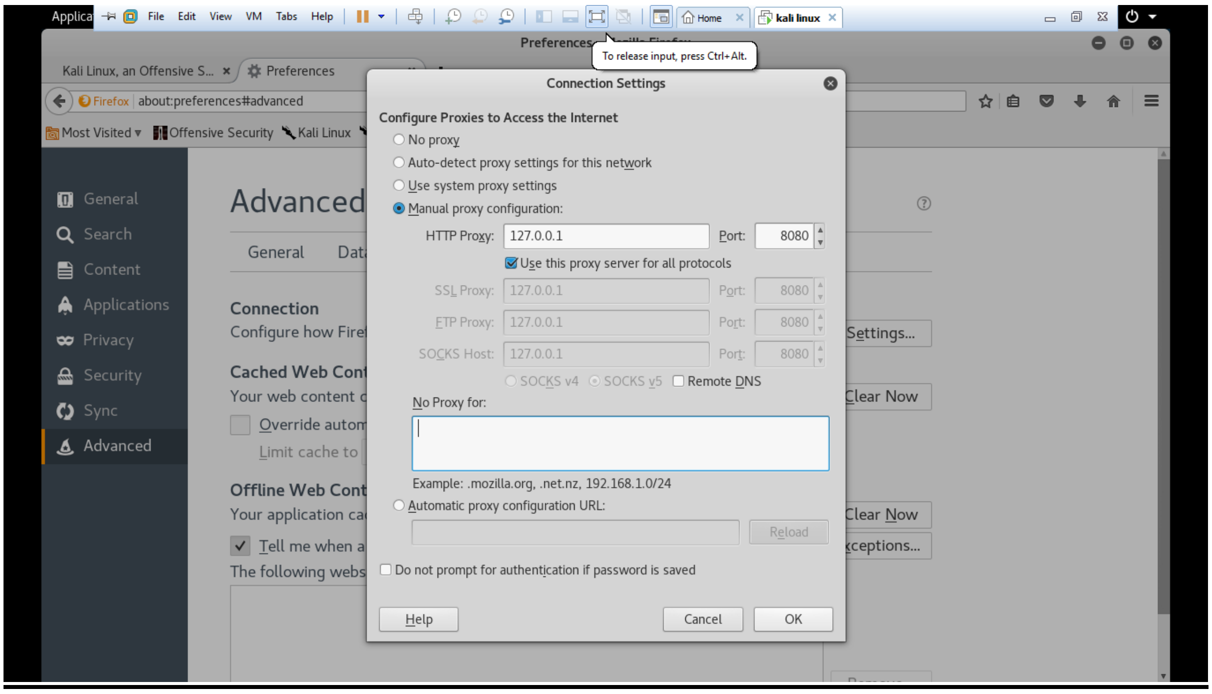
Limit cache to 350 MB of space

Offline Web Content and User Data

Your application cache is currently using 0 bytes of disk space — Clear Now

[✓] Tell me when a website asks to store data for offline use — Exceptions...

The following websites are allowed to store data for offline use:



Connection Settings

Configure Proxies to Access the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- [✓ Manual proxy configuration:]

HTTP Proxy: 127.0.0.1 Port: 8080

[✓] Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

SOCKS v4 SOCKS v5 Remote DNS

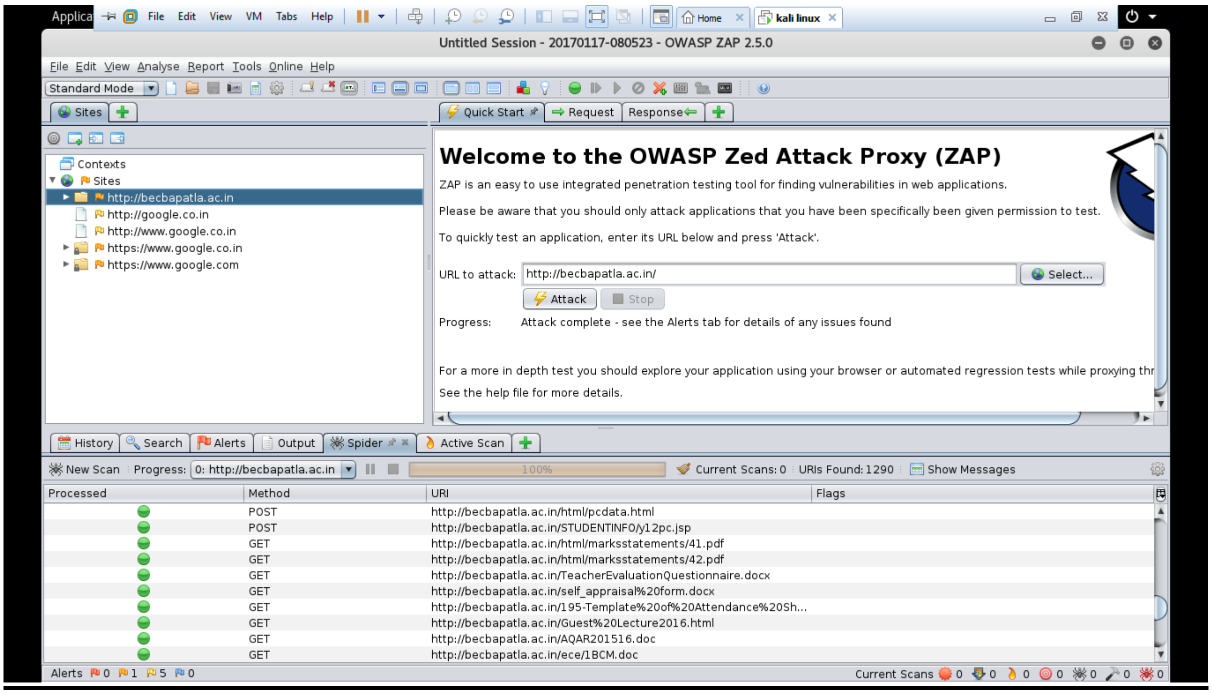
No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

- Automatic proxy configuration URL:

Do not prompt for authentication if password is saved

When you have successfully connected to your application you will see one or more lines in ZAP's Sites and History tabs.
Note that most of ZAP's tabs provide additional functionality that could be accessed via 'right click' menus.



Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

Sites:
- Contexts
- Sites
  - http://becbapatla.ac.in
  - http://google.co.in
  - http://www.google.co.in
  - https://www.google.co.in
  - https://www.google.com

Welcome to the OWASP Zed Attack Proxy (ZAP)

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

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

To quickly test an application, enter its URL below and press 'Attack'.

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

Progress: Attack complete - see the Alerts tab for details of any issues found

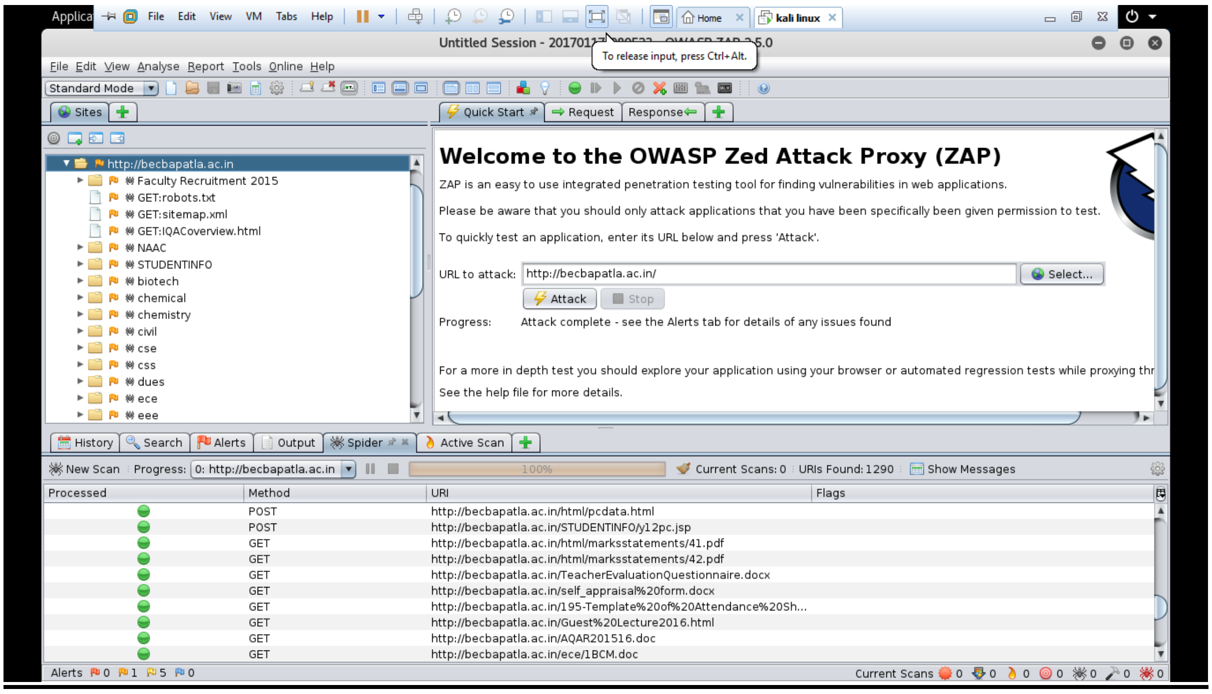
For a more in depth test you should explore your application using your browser or automated regression tests while proxying thr

See the help file for more details.

New Scan Progress: 0: http://becbapatla.ac.in 100% Current Scans: 0 URIs Found: 1290 Show Messages

Processed	Method	URI	Flags
🟢	POST	http://becbapatla.ac.in/html/pcdata.html	
🟢	POST	http://becbapatla.ac.in/STUDENTINFO/y12pc.jsp	
🟢	GET	http://becbapatla.ac.in/html/marksstatements/41.pdf	
🟢	GET	http://becbapatla.ac.in/html/marksstatements/42.pdf	
🟢	GET	http://becbapatla.ac.in/TeacherEvaluationQuestionnaire.docx	
🟢	GET	http://becbapatla.ac.in/self_appraisal%20form.docx	
🟢	GET	http://becbapatla.ac.in/195-Template%20of%20Attendance%20Sh...	
🟢	GET	http://becbapatla.ac.in/Guest%20Lecture2016.html	
🟢	GET	http://becbapatla.ac.in/AQAR201516.doc	
🟢	GET	http://becbapatla.ac.in/ece/1BCM.doc	

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0



Welcome to the OWASP Zed Attack Proxy (ZAP)

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

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

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://becbapatla.ac.in/ Select...

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

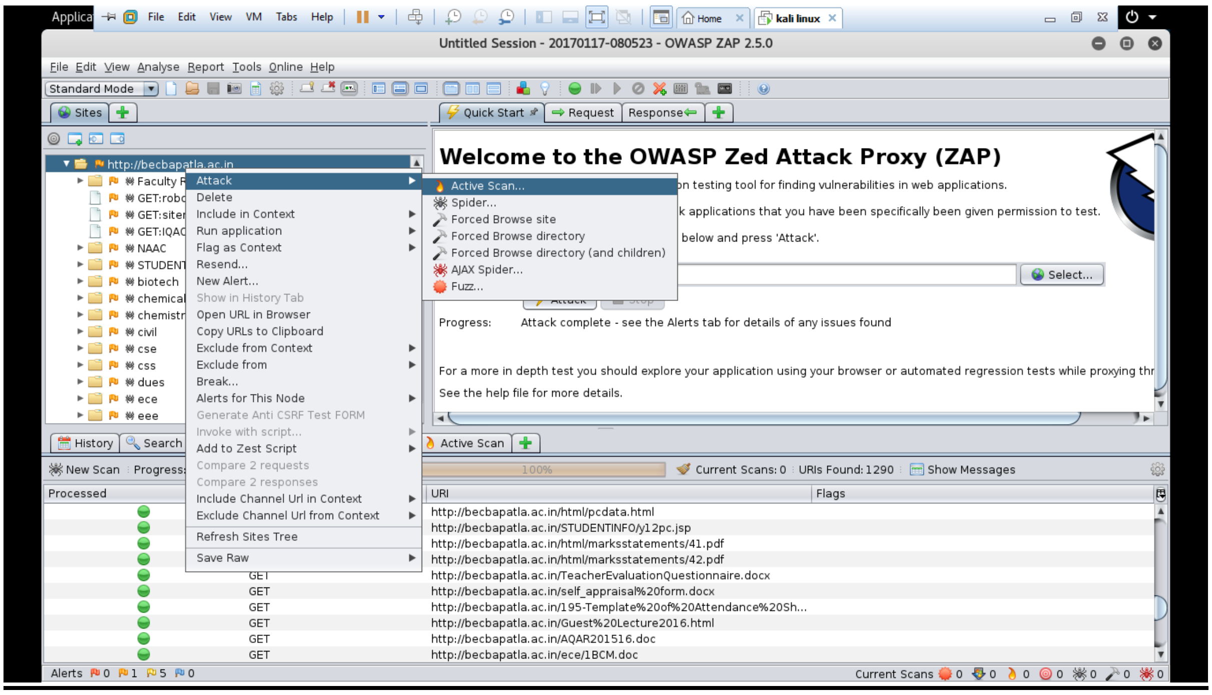
For a more in depth test you should explore your application using your browser or automated regression tests while proxying thr

See the help file for more details.

New Scan Progress: 0: http://becbapatla.ac.in 100% Current Scans: 0 URIs Found: 1290 Show Messages

Processed	Method	URI	Flags
●	POST	http://becbapatla.ac.in/html/pcdata.html	
●	POST	http://becbapatla.ac.in/STUDENTINFO/y12pc.jsp	
●	GET	http://becbapatla.ac.in/html/marksstatements/41.pdf	
●	GET	http://becbapatla.ac.in/html/marksstatements/42.pdf	
●	GET	http://becbapatla.ac.in/TeacherEvaluationQuestionnaire.docx	
●	GET	http://becbapatla.ac.in/self_appraisal%20form.docx	
●	GET	http://becbapatla.ac.in/195-Template%20of%20Attendance%20Sh...	
●	GET	http://becbapatla.ac.in/Guest%20Lecture2016.html	
●	GET	http://becbapatla.ac.in/AQAR201516.doc	
●	GET	http://becbapatla.ac.in/ece/1BCM.doc	

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0



Save the ZAP session

Once you have manually explored the application it would be a good time to save the ZAP session so that you can look at it again.

If your application has multiple roles then you should explore it with each role and save the sessions in separate files.

Generating a Report:

ZAP tool -> Report -> Generate HTML report (Any other options listed) -> Save and share the report.

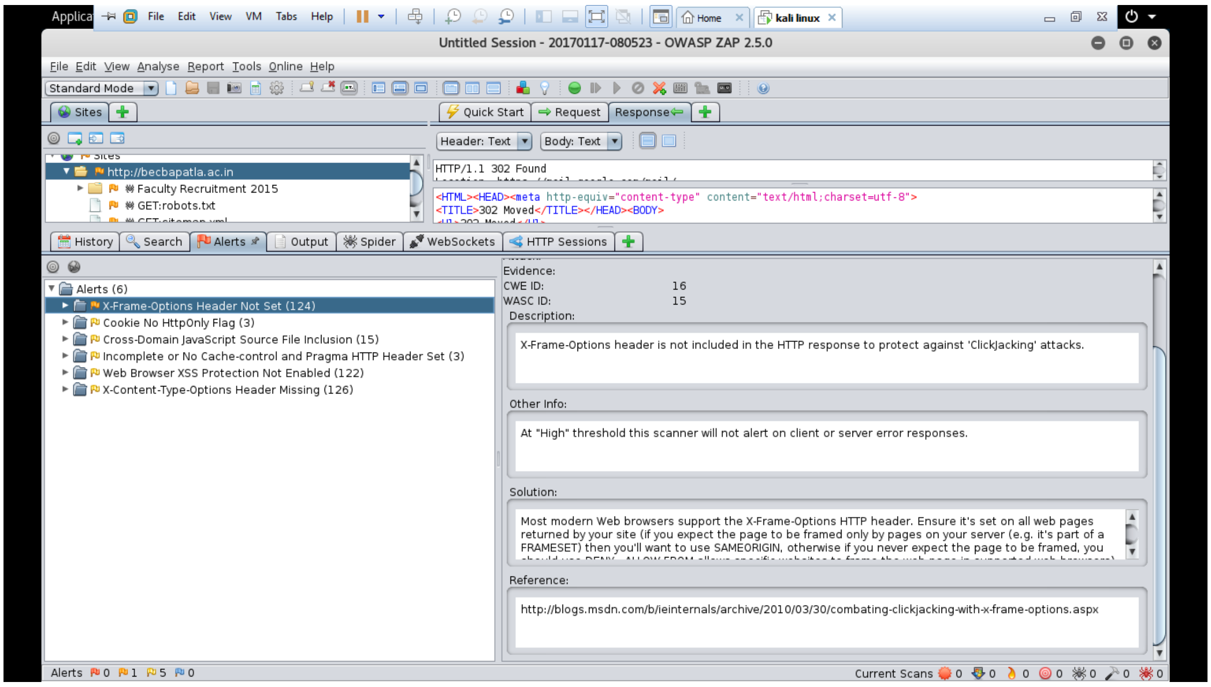
Authentication, session and User management using ZAP

1) Context: Represents a Web application
2) Session Management Method: How are the web Sessions identified by the server and handle requests

Example: cookie based using query parameters
3) Authentication Method: How is a new session established?
It could be either Form based authentication method, HTTP based or oath methods.
4) User Management: Handling users of web application that could be used for executing actions
Example: user name/password pair

Missing Parameters in the Web Application:

1). X-Frame-options Header Not Set



Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

```
HTTP/1.1 302 Found
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
```

Sites
- http://becbapatla.ac.in
  - Faculty Recruitment 2015
  - GET:robots.txt

Alerts (6)
- X-Frame-Options Header Not Set (124)
- Cookie No HttpOnly Flag (3)
- Cross-Domain JavaScript Source File Inclusion (15)
- Incomplete or No Cache-control and Pragma HTTP Header Set (3)
- Web Browser XSS Protection Not Enabled (122)
- X-Content-Type-Options Header Missing (126)

Evidence:
CWE ID: 16
WASC ID: 15

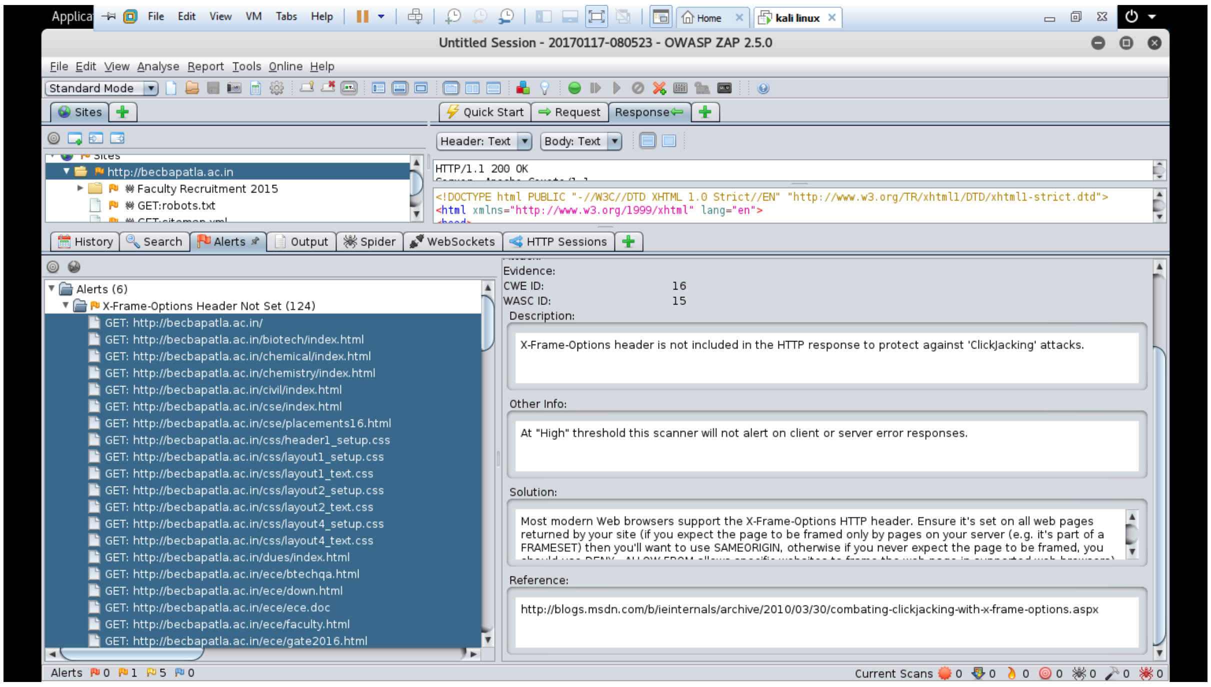
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Other Info:
At "High" threshold this scanner will not alert on client or server error responses.

Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you

Reference:
http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0



Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

```
HTTP/1.1 200 OK
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en">
```

Alerts (6)
- X-Frame-Options Header Not Set (124)
  - GET: http://becbapatla.ac.in/
  - GET: http://becbapatla.ac.in/biotech/index.html
  - GET: http://becbapatla.ac.in/chemical/index.html
  - GET: http://becbapatla.ac.in/chemistry/index.html
  - GET: http://becbapatla.ac.in/civil/index.html
  - GET: http://becbapatla.ac.in/cse/index.html
  - GET: http://becbapatla.ac.in/cse/placements16.html
  - GET: http://becbapatla.ac.in/css/header1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_text.css
  - GET: http://becbapatla.ac.in/css/layout2_setup.css
  - GET: http://becbapatla.ac.in/css/layout2_text.css
  - GET: http://becbapatla.ac.in/css/layout4_setup.css
  - GET: http://becbapatla.ac.in/css/layout4_text.css
  - GET: http://becbapatla.ac.in/dues/index.html
  - GET: http://becbapatla.ac.in/ece/btechqa.html
  - GET: http://becbapatla.ac.in/ece/down.html
  - GET: http://becbapatla.ac.in/ece/ece.doc
  - GET: http://becbapatla.ac.in/ece/faculty.html
  - GET: http://becbapatla.ac.in/ece/gate2016.html

Evidence:
CWE ID: 16
WASC ID: 15

Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

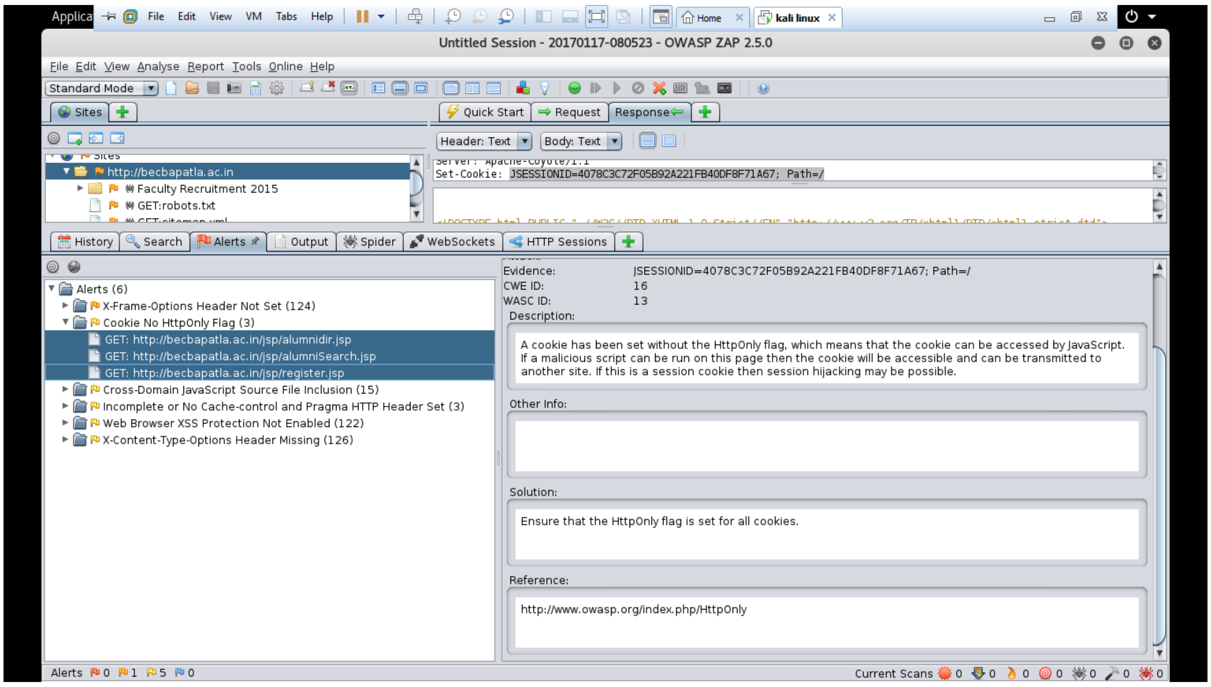
Other Info:
At "High" threshold this scanner will not alert on client or server error responses.

Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you

Reference:
http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0

2) Cookie No Http only Flag



```
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=4078C3C72F05B92A221FB400F8F71A67; Path=/
```

- http://becbapatla.ac.in
  - Faculty Recruitment 2015
  - GET:robots.txt

Alerts (6)
- X-Frame-Options Header Not Set (124)
- Cookie No HttpOnly Flag (3)
  - GET: http://becbapatla.ac.in/jsp/alumnidir.jsp
  - GET: http://becbapatla.ac.in/jsp/alumniSearch.jsp
  - GET: http://becbapatla.ac.in/jsp/register.jsp
- Cross-Domain JavaScript Source File Inclusion (15)
- Incomplete or No Cache-control and Pragma HTTP Header Set (3)
- Web Browser XSS Protection Not Enabled (122)
- X-Content-Type-Options Header Missing (126)

Evidence: JSESSIONID=4078C3C72F05B92A221FB40DF8F71A67; Path=/
CWE ID: 16
WASC ID: 13

Description:
A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

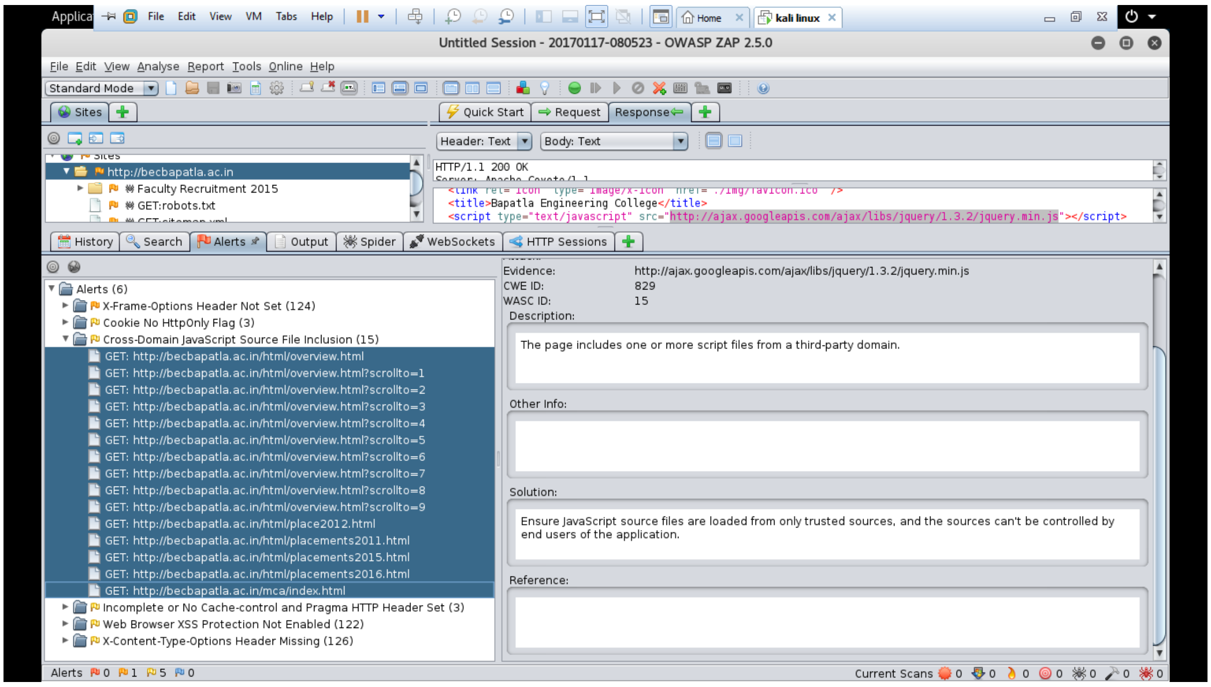
Other Info:

Solution:
Ensure that the HttpOnly flag is set for all cookies.

Reference:
http://www.owasp.org/index.php/HttpOnly

Alerts 0 1 5 0 — Current Scans 0 0 0 0 0 0 0

4).Cross Domain JavaScript Source File Inclusion.



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
<link rel="icon" type="image/x-icon" href="./img/favicon.ico" />
<title>Bapatla Engineering College</title>
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js"></script>
```

- http://becbapatla.ac.in
  - Faculty Recruitment 2015
  - GET:robots.txt

Alerts (6)
- X-Frame-Options Header Not Set (124)
- Cookie No HttpOnly Flag (3)
- Cross-Domain JavaScript Source File Inclusion (15)
  - GET: http://becbapatla.ac.in/html/overview.html
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=1
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=2
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=3
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=4
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=5
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=6
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=7
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=8
  - GET: http://becbapatla.ac.in/html/overview.html?scrollto=9
  - GET: http://becbapatla.ac.in/html/place2012.html
  - GET: http://becbapatla.ac.in/html/placements2011.html
  - GET: http://becbapatla.ac.in/html/placements2015.html
  - GET: http://becbapatla.ac.in/html/placements2016.html
  - GET: http://becbapatla.ac.in/mca/index.html
- Incomplete or No Cache-control and Pragma HTTP Header Set (3)
- Web Browser XSS Protection Not Enabled (122)
- X-Content-Type-Options Header Missing (126)

Evidence: http://ajax.googleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js
CWE ID: 829
WASC ID: 15

Description:
The page includes one or more script files from a third-party domain.

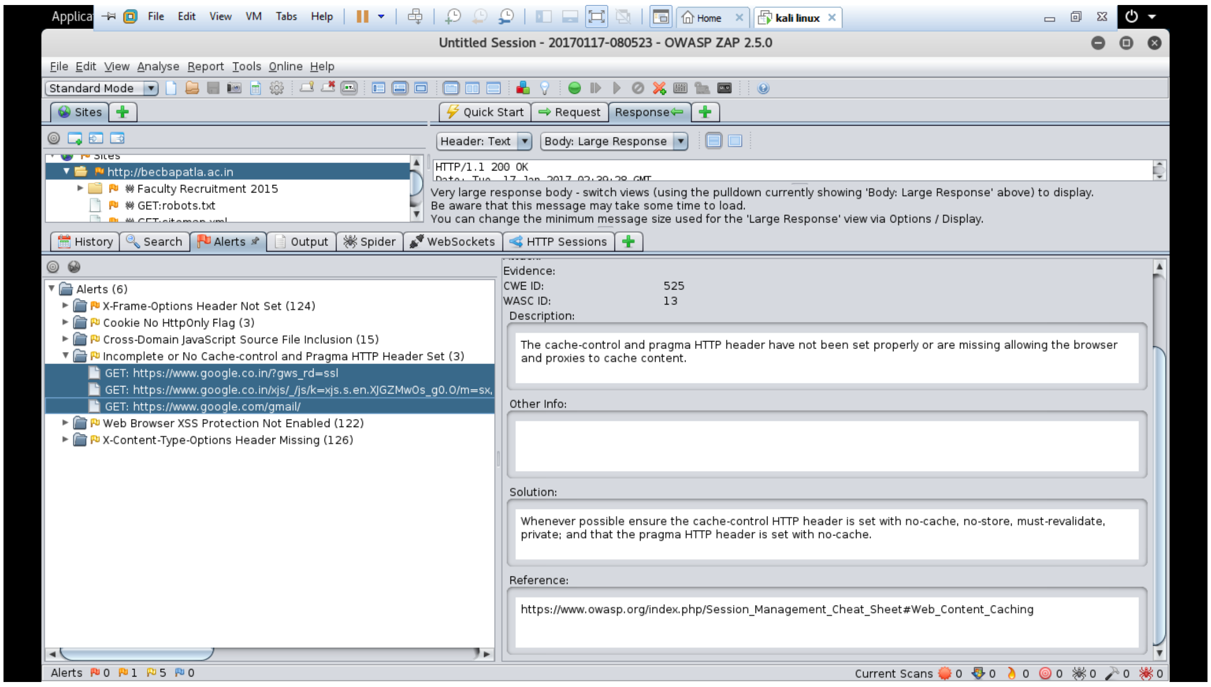
Other Info:

Solution:
Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Reference:

Alerts 0 1 5 0 — Current Scans 0 0 0 0 0 0 0

5).Incomplete or No Cache-Control and Program HTTP Header set



http://becbapatla.ac.in
Faculty Recruitment 2015
GET:robots.txt

```
HTTP/1.1 200 OK
```

Very large response body - switch views (using the pulldown currently showing 'Body: Large Response' above) to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the 'Large Response' view via Options / Display.

Alerts (6)
- X-Frame-Options Header Not Set (124)
- Cookie No HttpOnly Flag (3)
- Cross-Domain JavaScript Source File Inclusion (15)
- Incomplete or No Cache-control and Pragma HTTP Header Set (3)
  - GET: https://www.google.co.in/?gws_rd=ssl
  - GET: https://www.google.co.in/xjs/_/js/k=xjs.s.en.XJGZMwOs_g0.O/m=sx,
  - GET: https://www.google.com/gmail/
- Web Browser XSS Protection Not Enabled (122)
- X-Content-Type-Options Header Missing (126)

Evidence:
CWE ID: 525
WASC ID: 13

Description:
The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

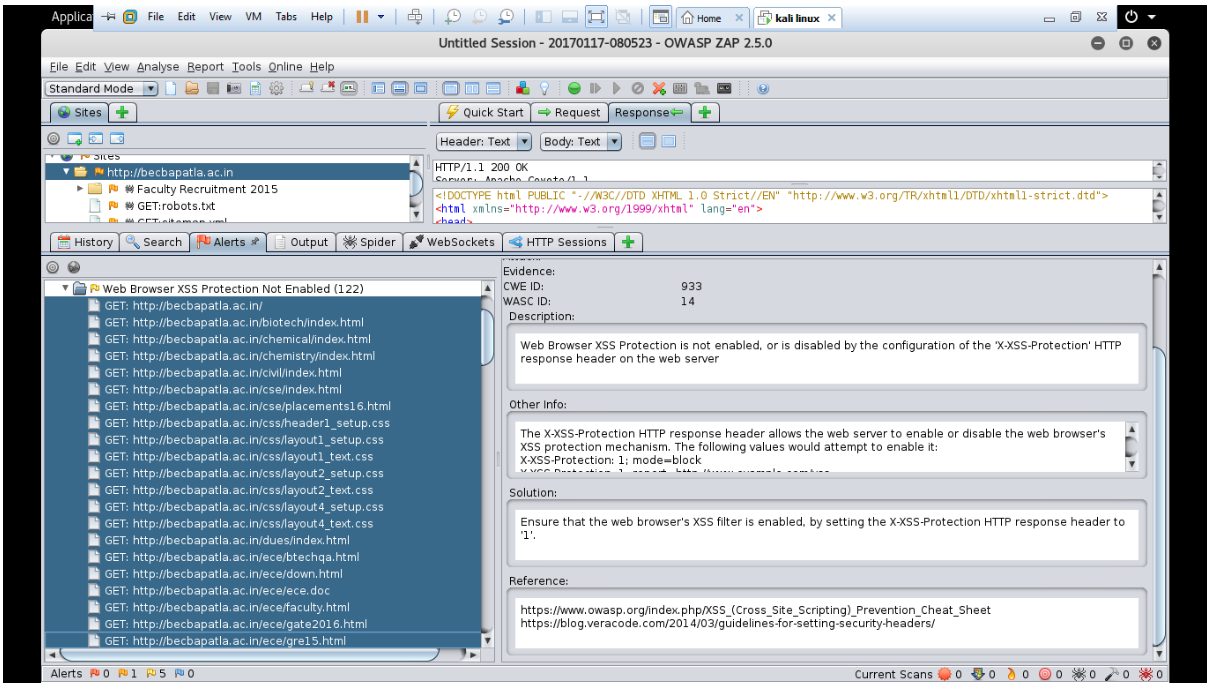
Other Info:

Solution:
Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate, private; and that the pragma HTTP header is set with no-cache.

Reference:
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0

6).Web Browser XSS Protection Not Enabled.



http://becbapatla.ac.in
Faculty Recruitment 2015
GET:robots.txt

```
HTTP/1.1 200 OK
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en">
```

- Web Browser XSS Protection Not Enabled (122)
  - GET: http://becbapatla.ac.in/
  - GET: http://becbapatla.ac.in/biotech/index.html
  - GET: http://becbapatla.ac.in/chemical/index.html
  - GET: http://becbapatla.ac.in/chemistry/index.html
  - GET: http://becbapatla.ac.in/civil/index.html
  - GET: http://becbapatla.ac.in/cse/index.html
  - GET: http://becbapatla.ac.in/cse/placements16.html
  - GET: http://becbapatla.ac.in/css/header1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_text.css
  - GET: http://becbapatla.ac.in/css/layout2_setup.css
  - GET: http://becbapatla.ac.in/css/layout2_text.css
  - GET: http://becbapatla.ac.in/css/layout4_setup.css
  - GET: http://becbapatla.ac.in/css/layout4_text.css
  - GET: http://becbapatla.ac.in/dues/index.html
  - GET: http://becbapatla.ac.in/ece/btechqa.html
  - GET: http://becbapatla.ac.in/ece/down.html
  - GET: http://becbapatla.ac.in/ece/ece.doc
  - GET: http://becbapatla.ac.in/ece/faculty.html
  - GET: http://becbapatla.ac.in/ece/gate2016.html
  - GET: http://becbapatla.ac.in/ece/gre15.html

Evidence:
CWE ID: 933
WASC ID: 14

Description:
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

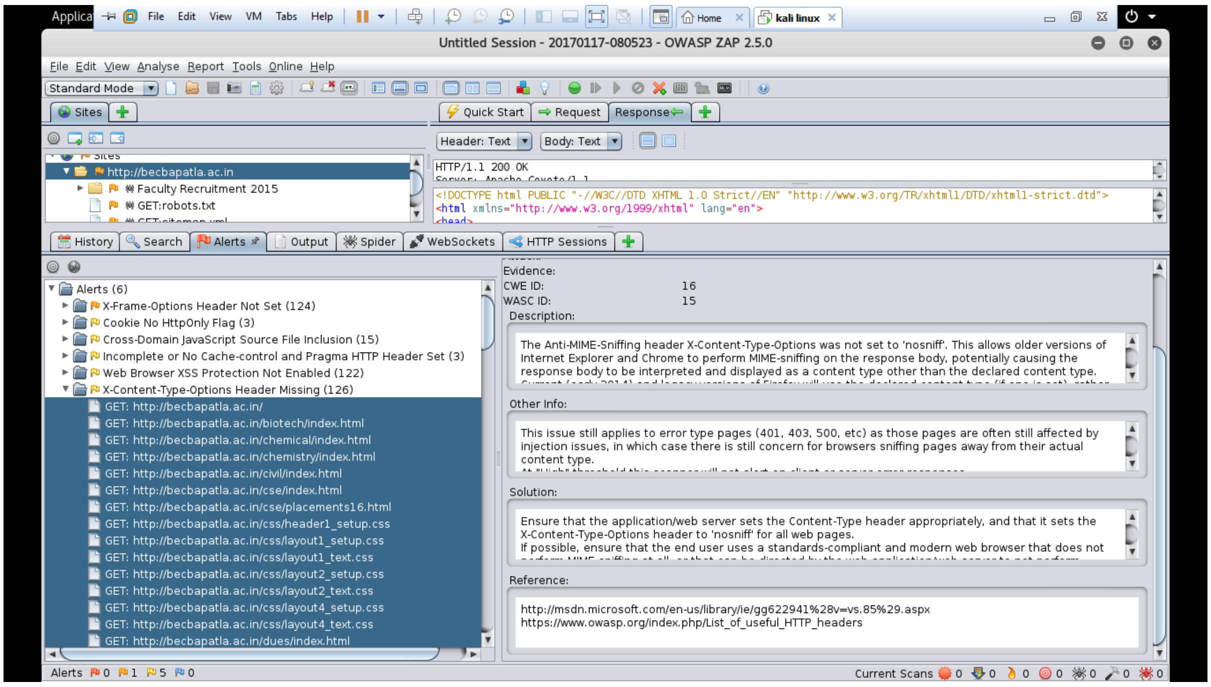
Other Info:
The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
X-XSS-Protection: 1; mode=block

Solution:
Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Reference:
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0

7).X-Content Type Options Headers Missing


Untitled Session - 20170117-080523 - OWASP ZAP 2.5.0

```
HTTP/1.1 200 OK
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en">
```

http://becbapatla.ac.in
- Faculty Recruitment 2015
- GET:robots.txt

Alerts (6)
- X-Frame-Options Header Not Set (124)
- Cookie No HttpOnly Flag (3)
- Cross-Domain JavaScript Source File Inclusion (15)
- Incomplete or No Cache-control and Pragma HTTP Header Set (3)
- Web Browser XSS Protection Not Enabled (122)
- X-Content-Type-Options Header Missing (126)
  - GET: http://becbapatla.ac.in/
  - GET: http://becbapatla.ac.in/biotech/index.html
  - GET: http://becbapatla.ac.in/chemical/index.html
  - GET: http://becbapatla.ac.in/chemistry/index.html
  - GET: http://becbapatla.ac.in/civil/index.html
  - GET: http://becbapatla.ac.in/cse/index.html
  - GET: http://becbapatla.ac.in/cse/placements16.html
  - GET: http://becbapatla.ac.in/css/header1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_setup.css
  - GET: http://becbapatla.ac.in/css/layout1_text.css
  - GET: http://becbapatla.ac.in/css/layout2_setup.css
  - GET: http://becbapatla.ac.in/css/layout2_text.css
  - GET: http://becbapatla.ac.in/css/layout4_setup.css
  - GET: http://becbapatla.ac.in/css/layout4_text.css
  - GET: http://becbapatla.ac.in/dues/index.html

Evidence:
CWE ID: 16
WASC ID: 15

Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.

Other Info:
This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

Solution:
Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not

Reference:
http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Alerts 0 1 5 0 Current Scans 0 0 0 0 0 0 0