DAY 2: Web Security Owasp

—Review Web Server Metadata files For Information leakage :

How to Test : Any actions can be performed with wget as well as curl.

DAST : (Dynamic Application Security Testing) : Zap and Burpsuite are the tools having checks or the parsing for the resources as part of spider/crawler functionality.

Robots :

Robots,Spider and Crawler retrieve the web pages and traverse hyperlinks to retrieve the further web content.

To retrieve the robots.txt from www.google.com using curl :

Command : curl –O –Ss https://www.google.com/robots.txt && head –n5 robots.txt

Meta Tags :

Meta tags is an HTML tag that provide information about a web page but it is not visible to users. Its placed inside html head tag.

Robots Meta Tag :

Robots meta tag tell search engines crawlers that they are allowed or not allowed to do that a specific web page.

Ex: <meta name="robots" content="noindex, nofollow"> , default values are index and follow

Comman robots meta tag values :

1)index – allowing index

2)no index – do not index page

3)follow – allowing follow links

4)no follow - do not follow links

Sitemap.xml :

Sitemap.xml is a file that provide the information about pages,videos and others files where these info is offered by site or application.

Ex : wget —no-verbose https://www.example.com/sitemap.xml && head –n8 sitemap.xml

Comman location :

Sitemap.xml , sitemap_index.xml , sitemap1.xml , sitemap-index.xml

Sometime sitemap contains :

/api/

/admin/

/internal/

/backup.zip

Security.txt :

security.txt is a file that tells security researchers how to report vulnerabilities to the website owner.

The file may be present at root web server or .well-known directory :

Ex: https://www.example.com/security.txt

OR

https://www.example.com/.well-known/security.txt

Tools :

Browser (View Source or Dev Tools functionality) , cURL , wget , Burp Suite , ZAP.