DAY 4 : Web Security Owasp

—Fingerprint Web Application Framework :

Test Objectives : Fingerprint the component used by the web application.There are several methods to identify frameworks and components :

- HTTP headers
- Cookies
- HTML source code
- Specific files and folders
- File extensions
- Error messages

1)HTTP Headers :

Most easiest way to identify framework is to look at X-Powered-By HTTP response header.Simplests way to identify web framework.But this methodology not work in all cases.

Tool : netcat

Command : nc target.com <port>

2)Cookies :

Most realible to identify web framework are framework-specific cookies.

```
GET /cake HTTP/1.1
Host: defcon-moscow.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: CAKEPHP=rm72kprivgmau5fmjdesbuqi71;
Connection: keep-alive
Cache-Control: max-age=0
```

CAKEPHP cookie are automatically been set, which gives information about which framework is used.

3)HTML source code :

This technique is on finding certain patterns in HTML page source code.One of the common markers is the HTML comment to discover the framework.

Such information is positioned at end <head> section of HTTP responses,<Meta> tags and at the end of the page.

4)Specific files and folders :

Every web application has folders and files structure on web server.In order to uncover them, There is a technique known as forcing Browsing and Dirbusting.

Dirbusting is brute-forcing a target with known folders and filenames and monitoring HTTP-responses to enumerate a server content.

Common Identifiers :

FRAMEWORKS	COOKIE NAME
Zope	Zope3
CakePHP	cakephp
Kohana	kohanasession
Laravel	Laravel_session
phpBB	Phpbb3_
WordPress	Wp-settings
1C-Bitrix	BITRIX_
AMPcms	AMP
DjangoCMS	django
DotNetNuke	DotNetNukeAnonymous
e107	e107_tz
EPiServer	EPiTrace,EPiServer
Graffiti CMS	graffitibot
Hotaru CMS	hotaru_mobile
ImpressCMS	ICMSession
Indico	MAKASESSION
InstantCMS	InstantCMS[Iogdate]
Kentico CMS	CMSPreferredCulture
MODx	SN4[12symb]
TYPO3	fe_typo_user
Dynamicweb	Dynamicweb

LEPTON	lep[some_numeric_value]+ sessionid
Wix	Domain=.wix.com
VIVVO	VivvoSessionID
Tiny File Manager	filemanager
Zenphoto	Zenphoto_auth

HTML Source Code :

Application	Keyword
WordPress	<meta name="generator" content="WordPress 3.9.2" />
phpBB	< body id="phpbb"
Mediawiki	<meta name="generator" content="Mediawiki 1.21.9" />
joomla	<meta name="generator" content="Joomla! - Open Source Content Management" />
Drupal	<meta name="Generator" content="Drupal 7 (https://drupal.org)" />
DotNetDuke	DNN Platform - https://www.dnnsoftware.com

General Markers :

- %framework_name%
- powered by
- built upon
- running

Specific Markers :

Framework	Keyword
Adobe ColdFusion	<!-- START headerTags.cfm
Microsoft ASP.NET	__VIEWSTATE
ZK	<!-- ZK
Business Catalyst	<!-- BC_OBNW -->
Indexhibit	ndxz-studio