ICTACADEMY®

TATA STRIVE | Right Skills Bright Future

Web Server and Application Security

Vulnerabilities in Web Server and Applications

March 2021

TATA TRUSTS

Ground Rules

1. For ease of conducting the session, we have disabled your microphones. Do keep your video turned on at all times.

2. Please raise any questions you may have through the chat.

3. Please confirm if you can see the presentation and the presenter clearly.

4. This is a 120-min long session. As we go through the session, I will take questions at the end of each concept and at the end of the session.

5. I will unmute the audio of participants volunteering for any activity.

Recap – M6 T1

Thus far, in the last topic you've learned about:

- Three Tier Architecture
- Components of Three-Tier Architecture
- Traffic flow between Three-Tier Architecture
- Basic DNS Flow

Agenda

In today’s session, you will learn about:

- Web application technologies
- Web server vulnerabilities
- Impact of web application vulnerabilities
- Why we need to protect web applications
- Case studies

Source: Freepik

What are Web Application Technologies?

Created by fae frey
from Noun Project

Few Years Back Vs. Today

FEW YEARS BACK

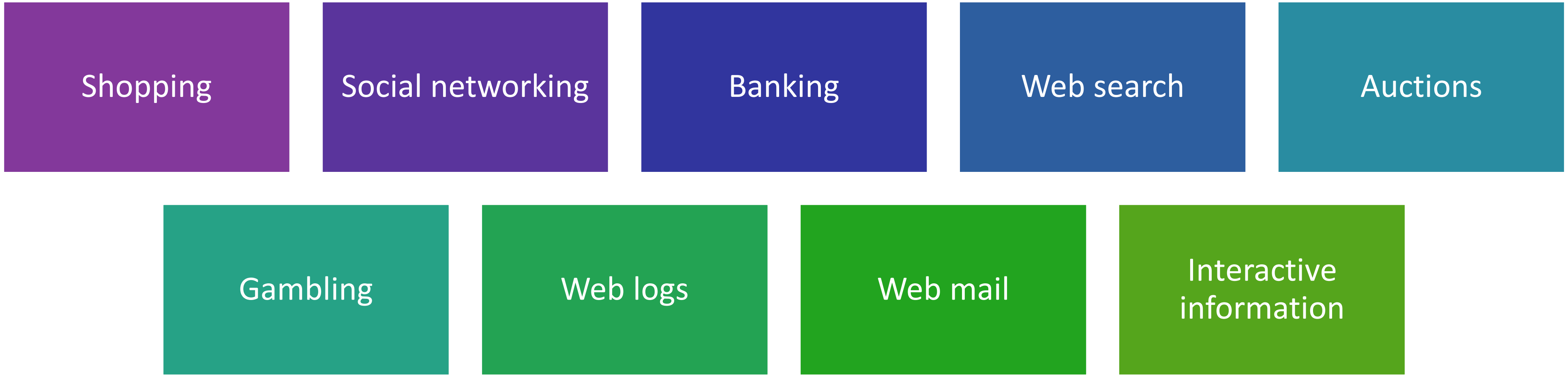
- The World Wide Web consisted only of web sites
- It contains static documents
- One-way flow from server to browser
- Security threats were related to vulnerabilities in web server software
- Information held on server was open to public view

TODAY

- Majority of sites on the web are applications
- Highly functional
- Two-way flow of information
- Content presented is generated dynamically
- Information processed is private and highly sensitive
- Security is a big issue

Introduction

- Web applications are dynamic web sites combined with server side programming
- It provides functionalities such as interacting with users, connecting to back-end databases, and generating results to browsers.
- It has been created to perform every function implemented online:



Shopping

Social networking

Banking

Web search

Auctions

Gambling

Web logs

Web mail

Interactive information

Activity

Name of the Activity

Fastest Finger First

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Fastest Finger First

How does Web Application differ from few years back to today?

Think-Tank

What are two types of Web Application Technologies?

Created by fae frey
from Noun Project

Web Application Technologies

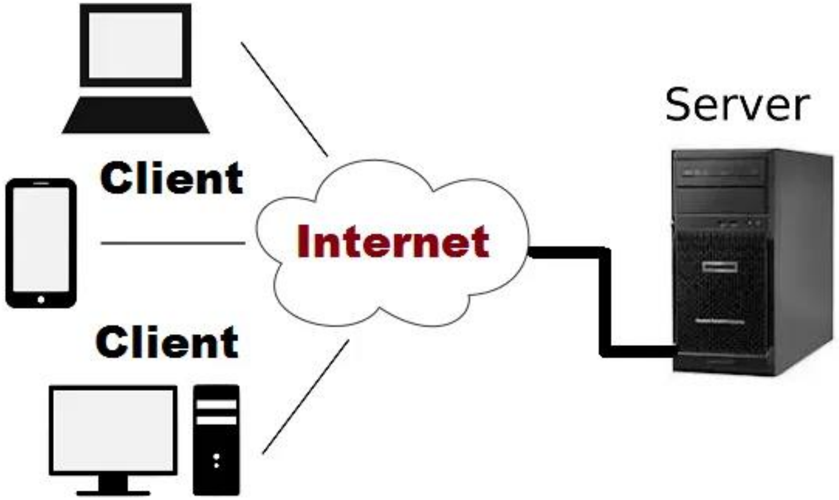
There are two main categories of coding, scripting and programming for creating Web Applications:

- Client Side Scripting / Coding
- Server Side Scripting / Coding

Created by fae frey from Noun Project

Client Server Architecture

- Client-server architecture is also called of the “Client/Server Network” or “Network computing Model“, because in this architecture all services and requests are spread over the network.
- Client-server architecture is a shared computer network architecture where several clients (remote system) send many requests and finally to obtained services from the centralized server machine (host system).



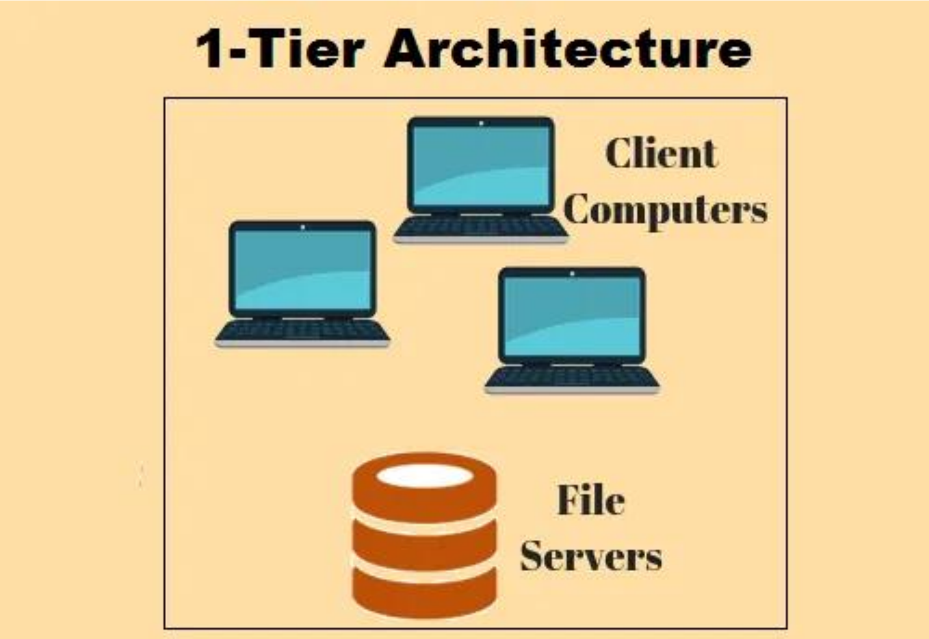
Types of Client Server Architecture

These are the different types of Client Server Architectures:

- 1-Tier Architecture
- 2-Tier Architecture
- 3-Tier Architecture
- N-Tier Architecture

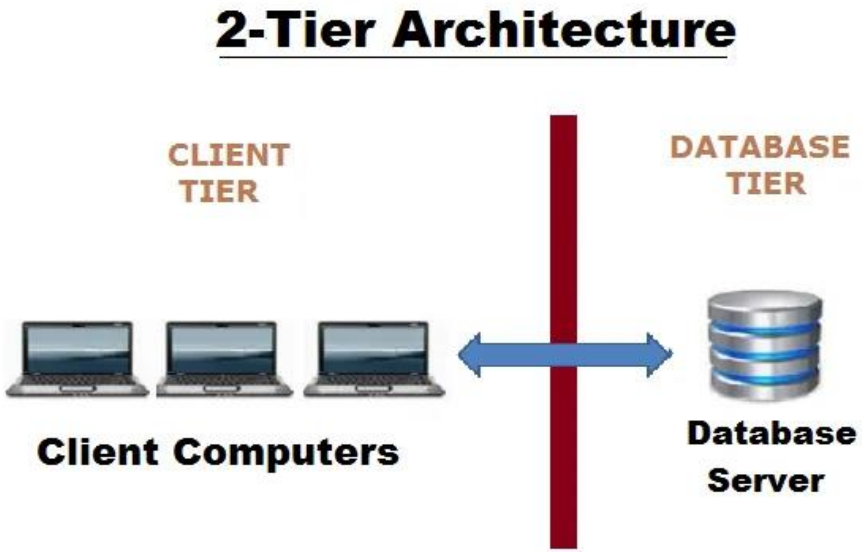
1-Tier Architecture

- In the 1-tier architecture, all client/server configuration setting, user interface environment, data logic, and marketing logic system are existed on the same system.
- This architecture also contain the different layers.



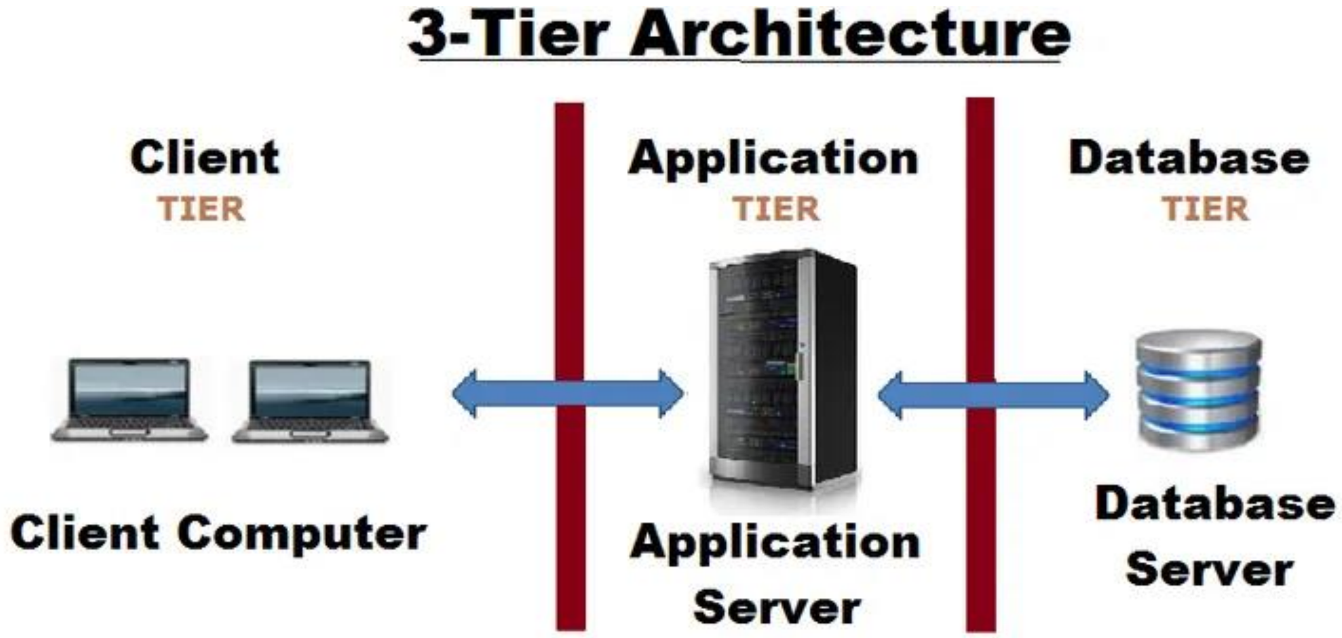
2-Tier Architecture

- In 2-tier architecture provides the best client/server environment that helps to store user interface on the client system and all database is saved on the server machine.
- Business logic and database logic are existed on the client otherwise server, but they are required to be maintained.



3-Tier Architecture

- In this 3-tier architecture, middleware is needed because if client machine sends the request to server machine then firstly this request is received by middle layer, and finally this request is obtained to server.



N-Tier Architecture

- This architecture is also known as the “Multitier Architecture”, so it is scaled form of 3-tier architecture. In this architecture, entire presentations, application processing, and data management functions are isolated from each other.
- It delivers the flexible and reusable applications and it is harder to implement because it uses the complex structure

Knowledge Check

Name of the Activity

Behind the Door Number

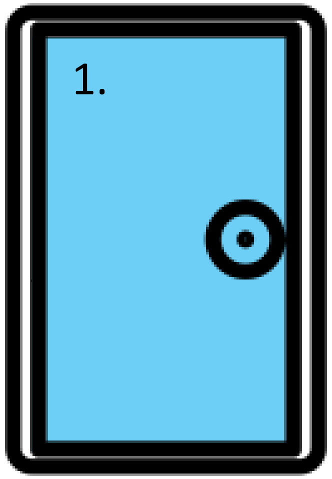
Instructions

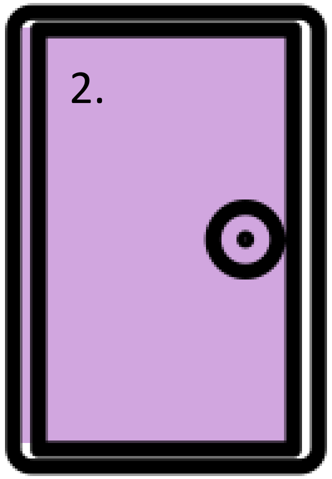
Mode: **In-session**

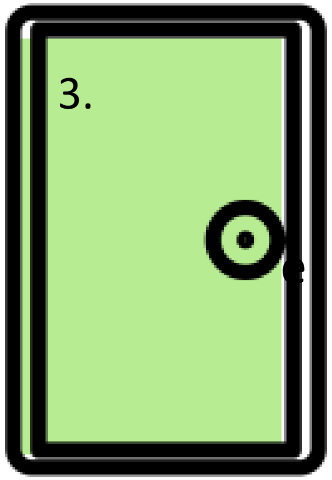
Duration: **5 minutes**

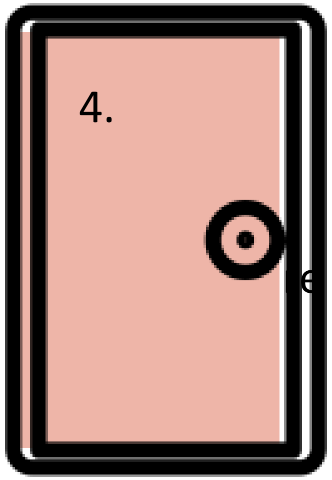
Materials Required: **None**

Knowledge Check – Behind the Door Number





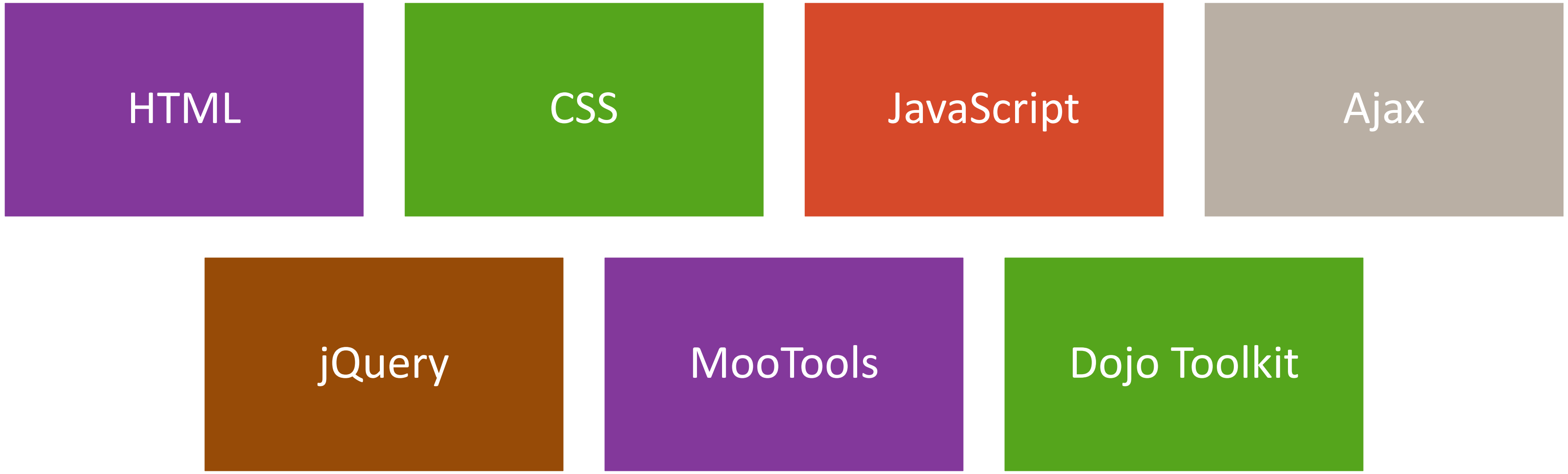




Source: Noun project

Client Side Scripting/Coding

- It is the type of code executed or interpreted by browsers
- It is viewable by any visitor to a site
- Common Client Side Scripting technologies:



HTML

CSS

JavaScript

Ajax

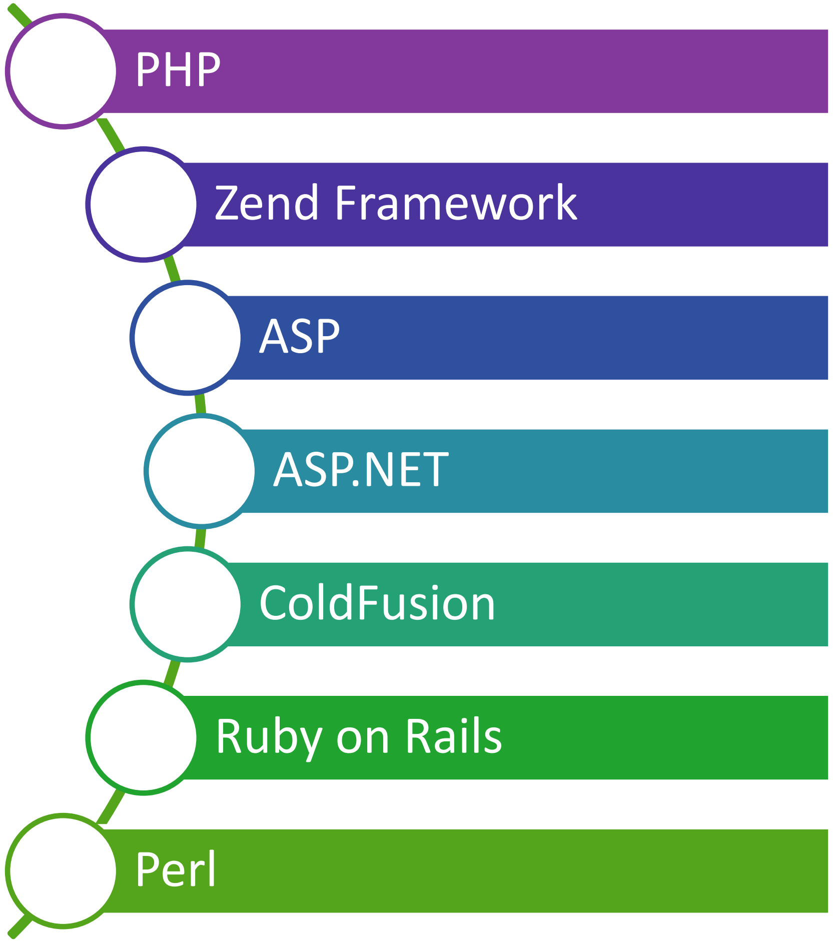
jQuery

MooTools

Dojo Toolkit

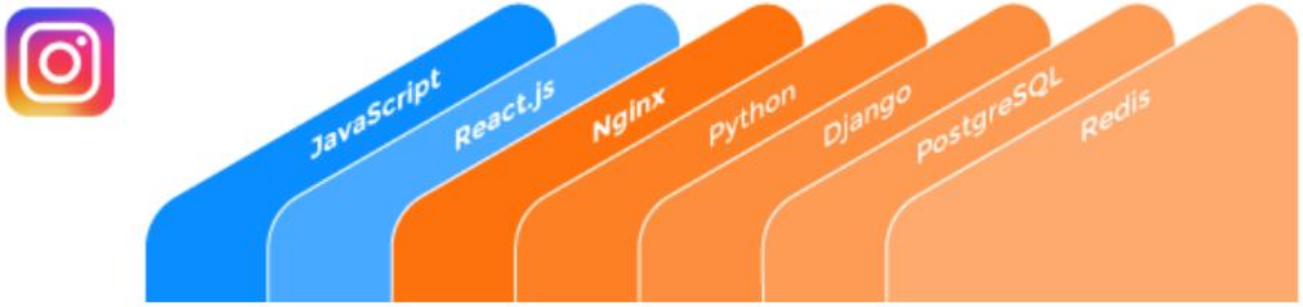
Server Side Scripting/Coding

- It is the type of code executed or interpreted by web server
- It is not viewable by any visitor or general public
- Common Server Side Scripting technologies:

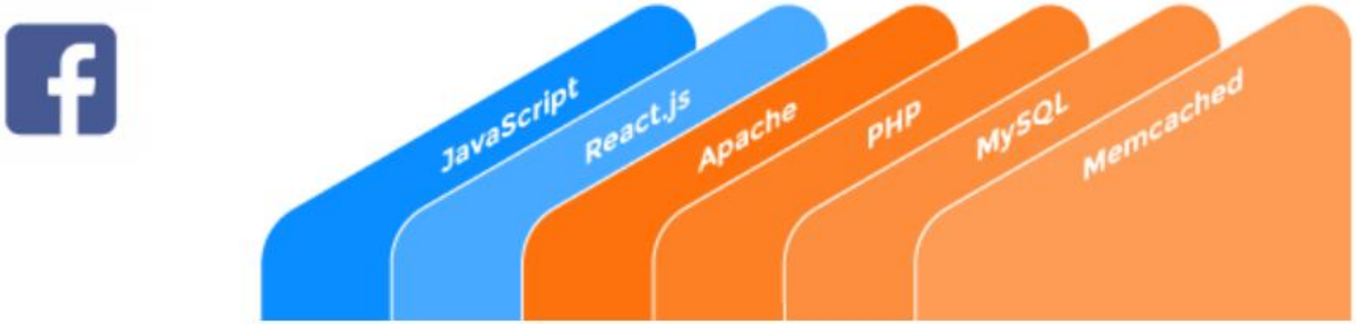


Technology Stacks Behind Successful Web Projects

- Instagram



- Facebook



Name of the Activity

Face off

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Face Off

Difference between
Client Side Scripting
and
Server Side Scripting

How to Analyze a Technology?

Created by fae frey
from Noun Project

Wappalyzer

- Powerful and useful add-on
- Extension is attached with Firefox and Chrome
- Detects

Content Management Systems

E-commerce Platform

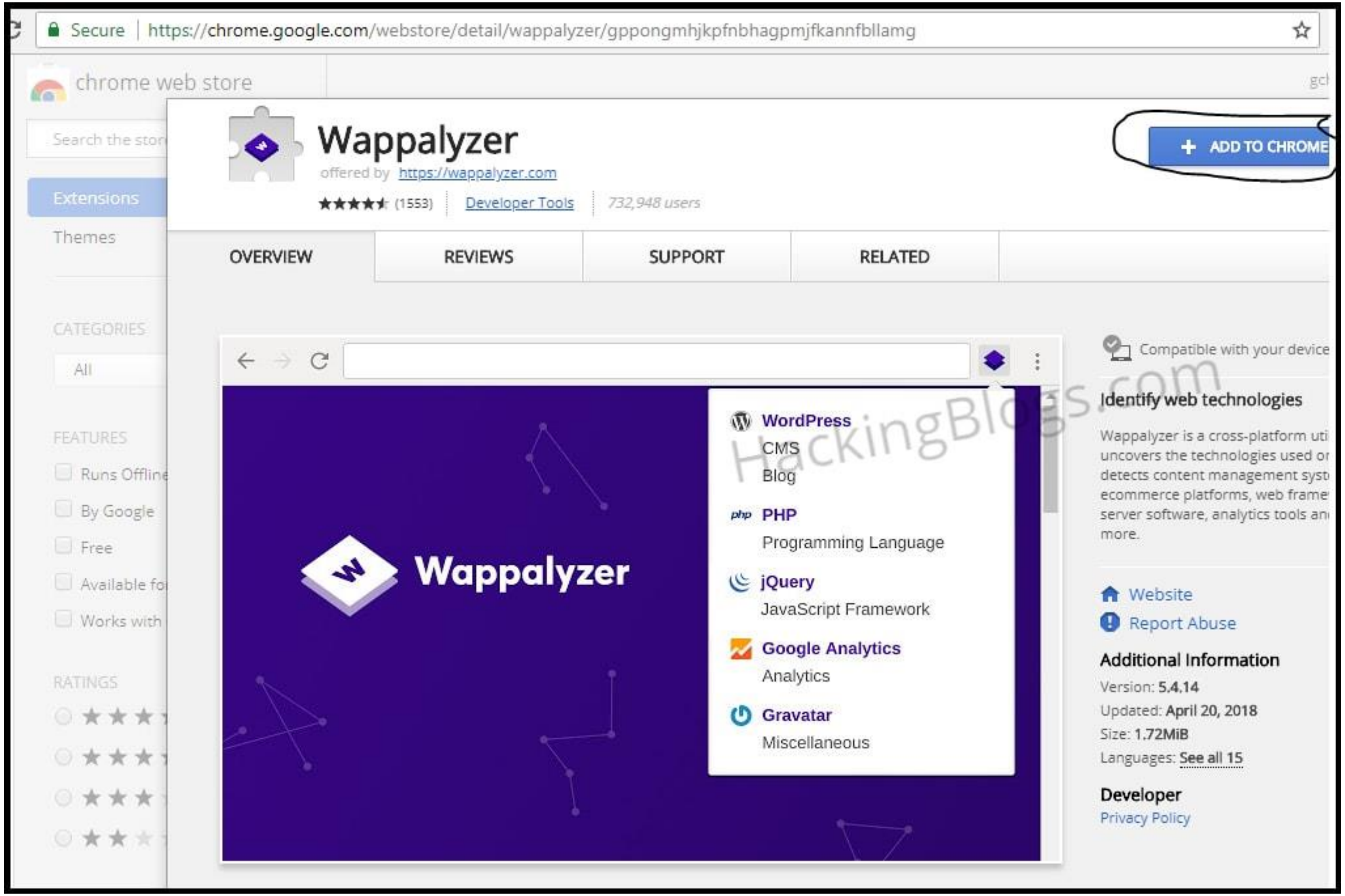
Web Frameworks

Server Software

Analytics Tools

Created by fae frey
from Noun Project

How to Use Wappalyzer



Secure | https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg

chrome web store

Search the stor

Extensions

Themes

CATEGORIES

All

FEATURES

□ Runs Offline
□ By Google
□ Free
□ Available fo
□ Works with

RATINGS

Wappalyzer

offered by https://wappalyzer.com

★★★★★ (1553) | Developer Tools | 732,948 users

+ ADD TO CHROME

OVERVIEW | REVIEWS | SUPPORT | RELATED

HackingBlogs.com

Compatible with your device

Identify web technologies

Wappalyzer is a cross-platform uti uncovers the technologies used or detects content management syst ecommerce platforms, web frame server software, analytics tools an more.

Website

Report Abuse

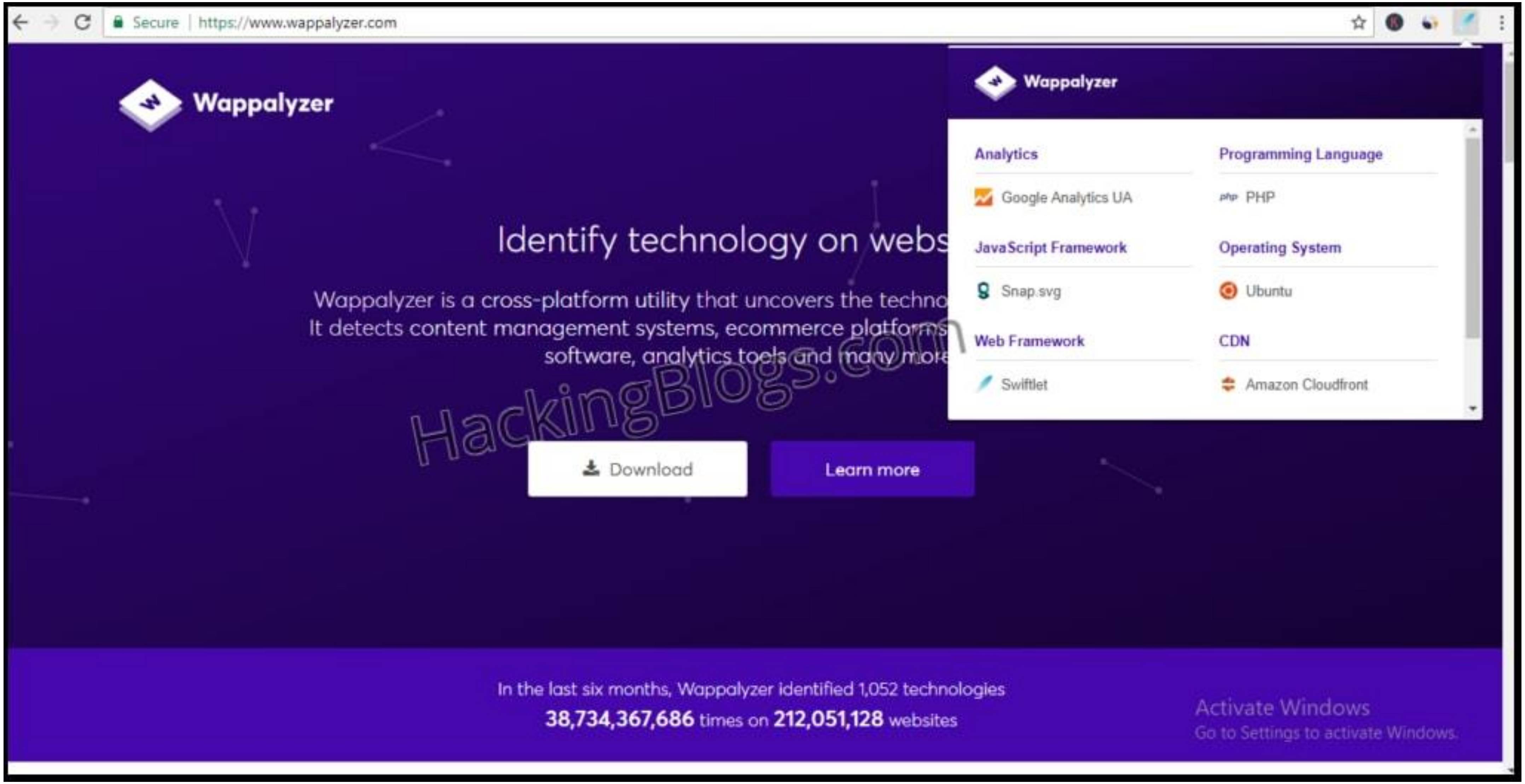
Additional Information

Version: 5.4.14
Updated: April 20, 2018
Size: 1.72MiB
Languages: See all 15

Developer

Privacy Policy

How to Use Wappalyzer



Secure | https://www.wappalyzer.com
Wappalyzer
Download
Learn more
HackingBlogs.com
Activate Windows
Go to Settings to activate Windows.

Identify technology on webs

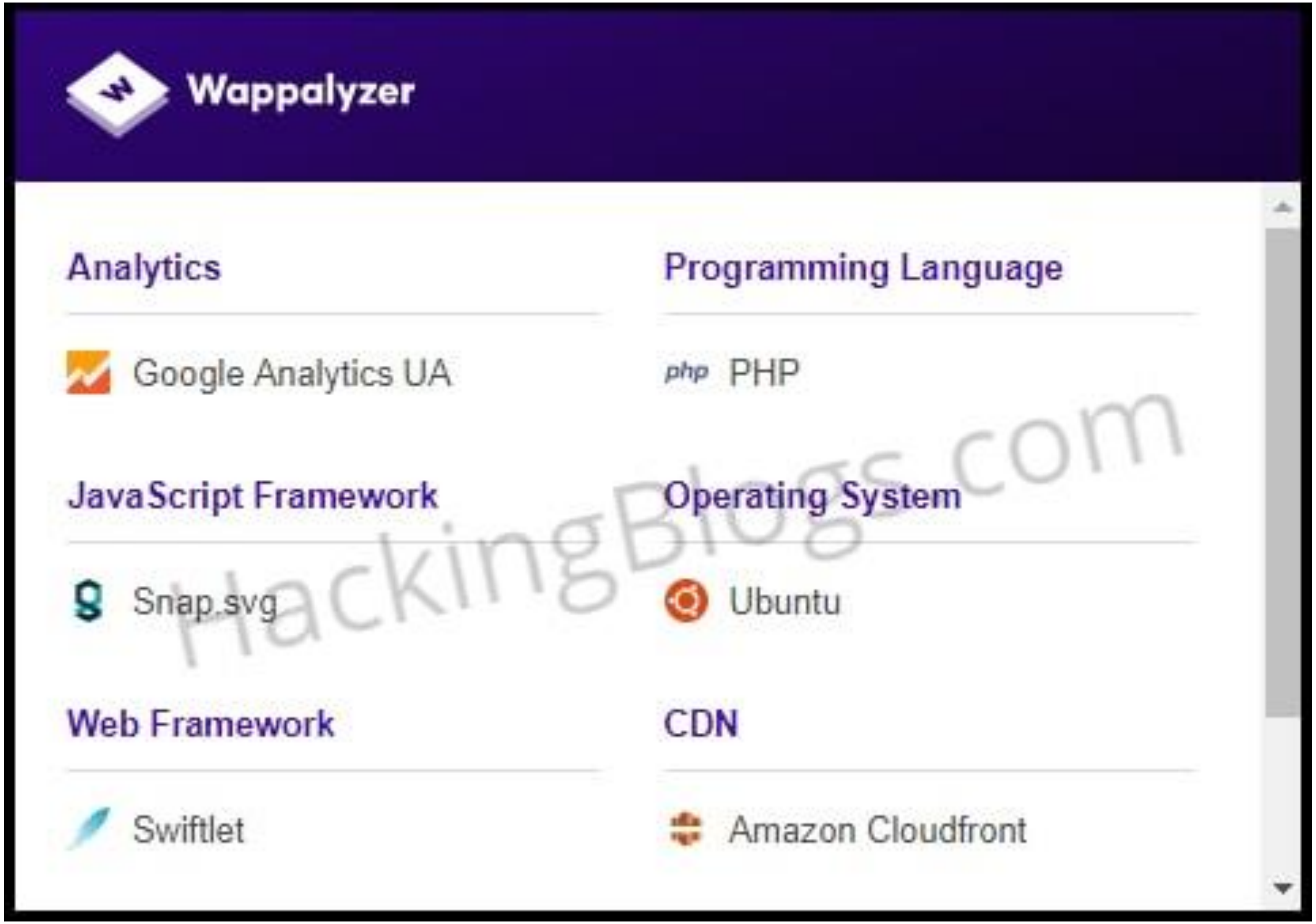
Wappalyzer is a cross-platform utility that uncovers the techno
It detects content management systems, ecommerce platforms
software, analytics tools and many more

In the last six months, Wappalyzer identified 1,052 technologies
38,734,367,686 times on 212,051,128 websites

Wappalyzer

Category	Technology
Analytics	Google Analytics UA
Programming Language	PHP
JavaScript Framework	Snap.svg
Operating System	Ubuntu
Web Framework	Swiftlet
CDN	Amazon Cloudfront

How to Use Wappalyzer



Wappalyzer

Analytics

Google Analytics UA

Programming Language

PHP

JavaScript Framework

Snap.svg

Operating System

Ubuntu

Web Framework

Swiftlet

CDN

Amazon Cloudfront

HackingBlogs.com

Think-Tank

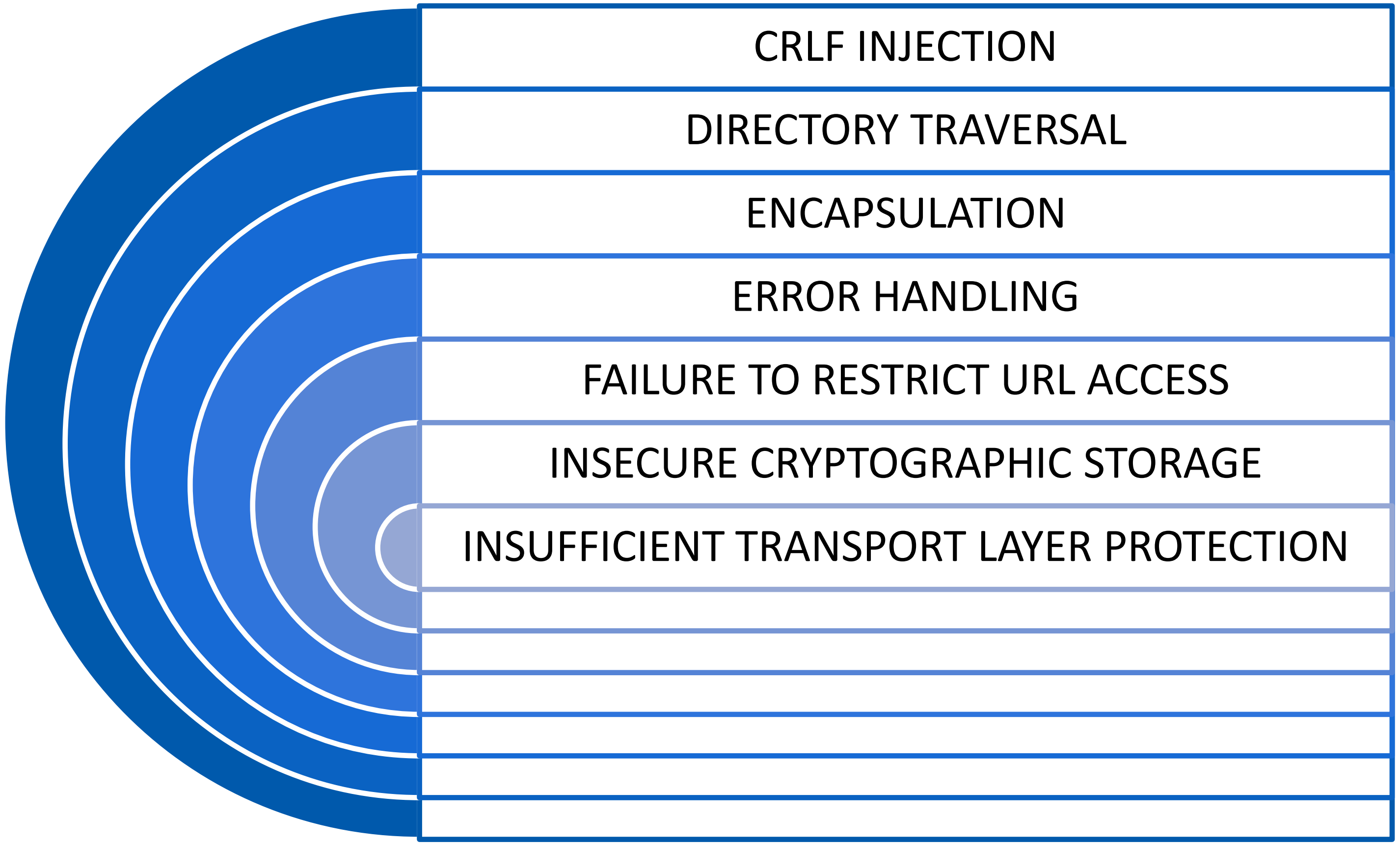
What are some Common Web Server Vulnerabilities?

Created by fae frey
from Noun Project

Common Web Server Vulnerabilities

- CROSS SITE SCRIPTING (XSS)
- SQL INJECTION (SQi)
- DENIAL-OF-SERVICE (DOS)
- MEMORY CORRUPTION
- BUFFER OVERFLOW
- CROSS-SITE REQUEST FORGERY (CSRF)
- DATA BREACH
- APPLICATION VULNERABILITIES
- CREDENTIALS MANAGEMENT

Common Web Server Vulnerabilities



CRLF INJECTION

DIRECTORY TRAVERSAL

ENCAPSULATION

ERROR HANDLING

FAILURE TO RESTRICT URL ACCESS

INSECURE CRYPTOGRAPHIC STORAGE

INSUFFICIENT TRANSPORT LAYER PROTECTION

Knowledge Check

Name of the Activity

Behind the Door Number

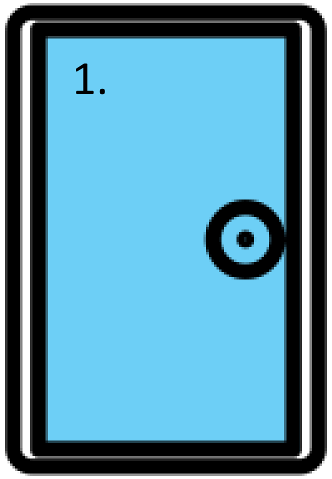
Instructions

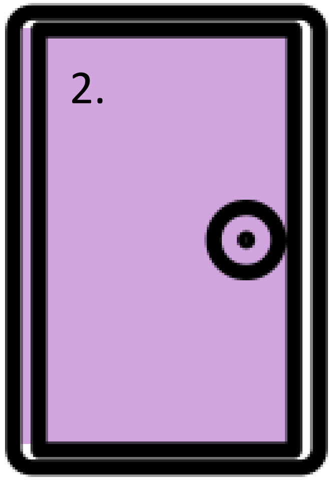
Mode: **In-session**

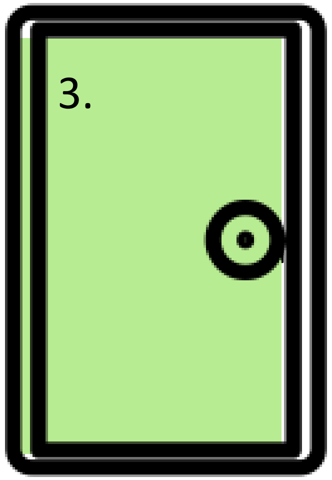
Duration: **5 minutes**

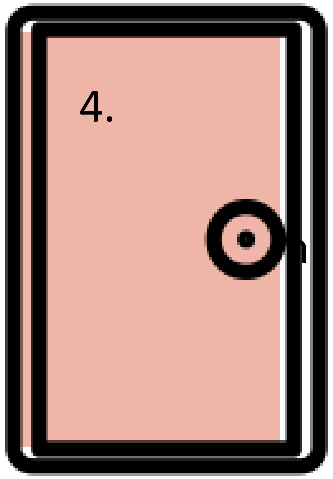
Materials Required: **None**

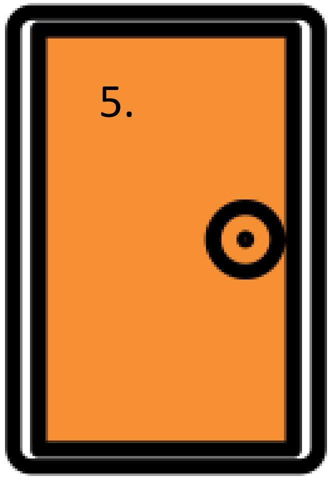
Knowledge Check – Behind the Door Number

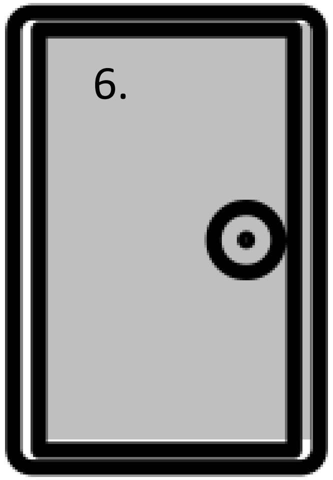


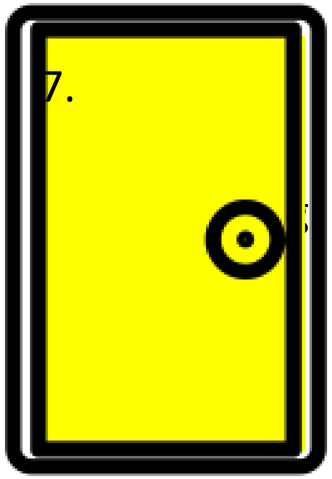












Source: Noun project

Name of the Activity

What does it Stand for?

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity

Abbreviation	What does it Stand for?
XSS	Cross Site Scripting
DoS	Denial-of-Service
CSRF	Cross-Site Request Forgery
CRLF	Carriage Return Line Feed
HTML	Hyper Text Mark-up Language
CSS	Cascading Style Sheets

Think-Tank

What is the Impact of Web Application Vulnerabilities?

Created by fae frey
from Noun Project

Impact of Web Application Vulnerabilities

- Attacks against web applications increased
- Biggest cause of data breaches
- 43% of breaches traced back to attacks against web applications
- 86% data breaches motivated by prospect of illicit financial gain,
- 67% breaches caused by credential theft, human error, or social engineering attacks
- 27% of malware incidents attributed to ransom-ware
- Analysis of 32,002 security incidents and 3,950 confirmed breaches from 81 contributors from 81 countries worldwide.

Created by fae frey
from Noun Project

Web App 'Front Doors' Under Attack

- 55% of attacks - combination of web application and application-specific attacks
- Majority of businesses use applications as front door
- Some not practicing basic security hygiene, threat actors are focus on vulnerabilities
- Attacks on content management systems account 20% of cyber-attacks
- 28% of attacks targeted technology platforms that support websites, such as ColdFusion and Apache Struts.

Created by fae frey from Noun Project

Data Breach I : Elara Claring

- Data breach exposed personal details
- More than 100,000 elderly patients
- Suffered unauthorized computer intrusion
- December 2020
- Data of 100,487 individuals compromised

Created by fae frey
from Noun Project

Data Breach II : Oxfam Australia

- Supporters' information "unlawfully accessed"
- January 20, 2021
- Engaged industry-leading forensic IT experts
- Information about supporters
- Data includes names, addresses, dates of birth, emails, phone numbers, gender, donation history
- Offered guidance about steps that they can take to protect their information

Created by fae frey
from Noun Project

Name of the Activity

Taboo

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Think-Tank

Why should we Protect Web Applications?

Created by fae frey
from Noun Project

Why Protect Web Applications?

- 30 000 to 50 000 websites hacked every day
- Importance of website security increasing rapidly
- Vital to protect website and data
- Hackers can use site to infect site visitors
- Customer loses trust, company reputation loss, end of the business

Created by fae frey from Noun Project

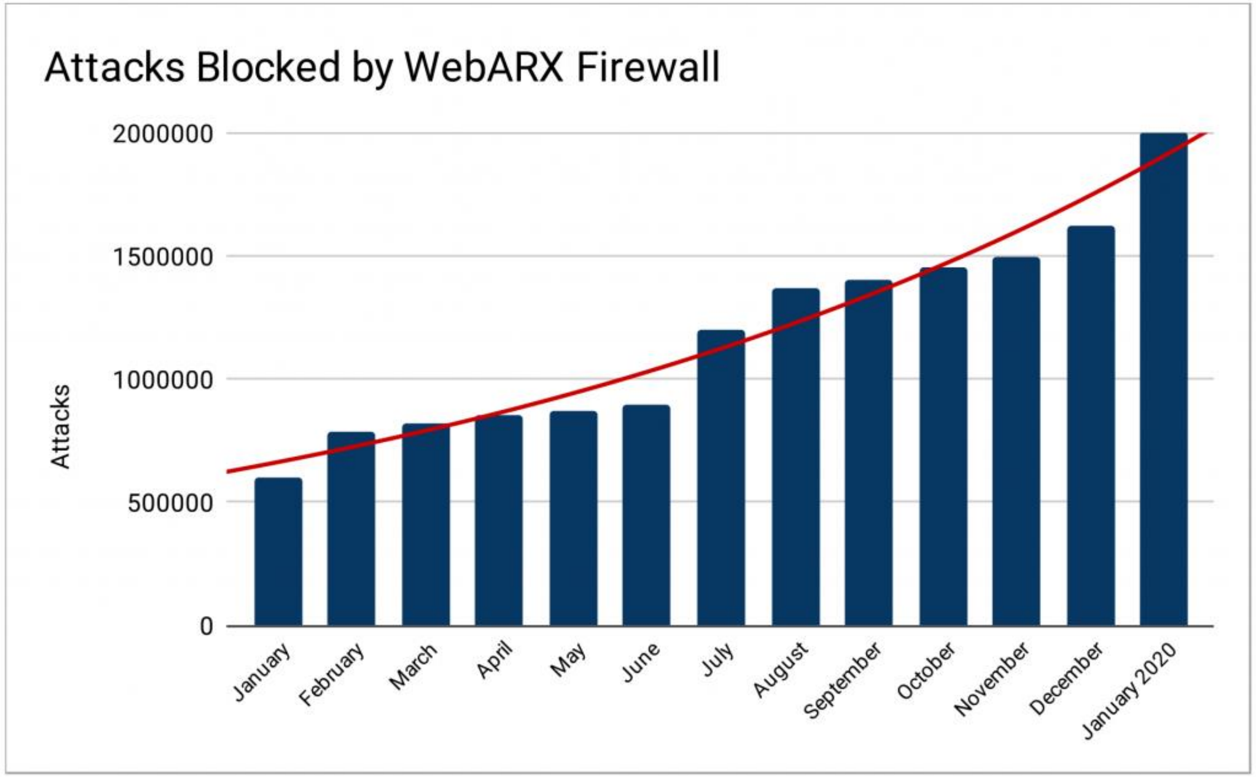
Hacked Websites Target Customers

- Malicious software is used to infect websites, gather data and hijack computer resources
- Site where attacker has gained access can be used to infect visitors
- Means site is not protected
- Done by automated hacking tools
- Hacked websites retarget potential customers

Created by fae frey
from Noun Project

Hacked Sites Rising Rapidly

- Attack every 39 seconds on the web
- Non-secure usernames and passwords give attackers more chance of success
- Attack does not always mean hacked



Business Reputation

- People rely on search engines when they want to reach information
- Search engine optimization is important
- Google and other search engines warn customers and restrict them from entering your website.
- Starting July 2018, website without SSL (HTTPS) marked as insecure
- 80% of hacked sites detected and removed from search results

Created by fae frey
from Noun Project

Learning from Mistakes

- 84% of websites contain vulnerabilities
- Prone to be infected
- Process of malware clean-up of a website is about knowing the vulnerabilities and knowing the way of a hackers mind
- Malware is hidden from the original files
- Expensive indeed
- Lost revenue and reputational damage takes time to recover from

Created by fae frey
from Noun Project

Website gets Blacklisted

- When a website is on blacklist, search engine is expelling a site from their list
- Website loses 95% of its organic traffic, which affects revenue
- Gets blacklisted when it contains something harmful to the user
- 2 approaches to recovering a hacked site:

Do it yourself

Find a trusted service provider

Created by fae frey
from Noun Project

Activity

Name of the Activity

Fastest Finger First

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Fastest Finger First

List the 5 reasons why we need to Protect Web Applications?

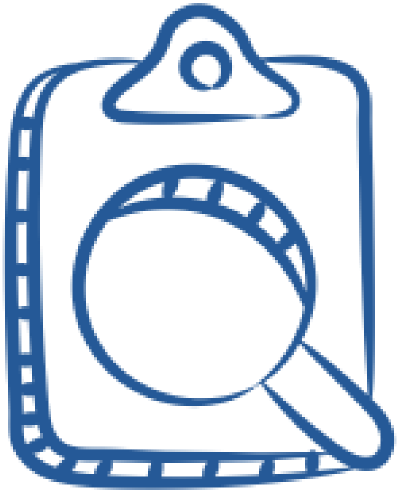
Think-Tank

What are some of the Biggest Data Breaches?

Created by fae frey
from Noun Project

Case Study I : Verifications.io

- **Date reported**: March 7, 2019
- **Impact**: 800 million to 2 billion records worldwide
- **Security failure**: No authentication required
- **Reported by**: Bob Diachenko



Created by fae frey
from Noun Project

Case Study II : First American Financial

- **Date reported**: May 25, 2019
- **Impact**: About 885 million files related to mortgage deals
- **Security failure**: Lack of authentication control
- **Reported by**: Brian Krebs

Created by fae frey
from Noun Project

Case Study III : Facebook

- **Date reported**: April 3, 2019
- **Impact**: More than 540 million records exposed
- **Security failure**: Publicly accessible server hosted by a third party
- **Reported by**: Upguard Cyber Risk

Created by fae frey
from Noun Project

He Who

Asks a Question

May Remain a Fool

For Five Minutes

But, He Who

Does Not Ask

Remains a Fool

Forever

Source: Freepik

Summary

In this session, you learnt about:

- Web application technologies
- Web server vulnerabilities
- Impact of web application vulnerabilities
- Why we need to protect web applications
- Case studies

What Next?

In this topic, you will further learn about:

- OWASP Top 10 Web Application Vulnerabilities
- SSL/TLS
- HTTP Request/Response
- HTTP Methods
- Setting up the Proxy Interception

Source: Pixabay

TATA STRIVE | Right Skills Bright Future

Skill Development Initiative of Tata Trusts

- www.tatastrive.com -