① words - mkce. ac. in Config - Webmail

06/04/24
Saturday

DAY - 6

Vulnerability Assessment (VA)

* Finding out potentiall weakness

HW
Hackthebox academy ⓧ

Risk matrix ⓧ

likelyhood - Possibility

(1) Asset discovery
(2) Vulnerability scanning
(3) Vulnerability assessment
(4) Vulnerability remediation

* CVSS Score must provided
* National vulnerability Database
→ Common vulnerability Scoring System (CVSS)

Low	0.9 - 3.9
medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Latest version CVSS V3

User Interaction → Passive
→ Active

People needed for attack

Vulnerability Scanners

↓ Manual Method

↓ Automatic

→ Pen test

{ AWS solution architect

{ Microsoft Central

① Policy - Controling what to be done

② Procedure - Step by step process for Policy

③ Standard - Quality

④ Regulations - Government (HIPPA)
(PCIDSS)
(GDPR)

IT - Password Policy

Regulation
↳ standard
↳ Procedure
↳ Policy

* False Positive - இல்லை ஆனால் இருக்கிறது

* False Negative -

* True Positive -

* True Negative - The vulnerability exists but not shown.

Vulnerability Scanner } Not AI trained

SAST Tools ⊗⊗

→ Static Application Security Testing (A

Vulnerability Assessment Methods

* Code Review

* Patch Management, Etc...

Penetration Testing ⊗ ⊗

(1) Information Gathering - Host, Router

(2) Scanning - versions,

(3) Gaining Access

(4) Maintaining Access - Persistant ⊗

(5) Clearing Tracks - Digital Foot prints

5 Phases

* Content management System

(1) Wordpress

Process

(1) Information gathering

(2) Threat modeling

(3) Vulnerability analysis

(4) Exploitation

(5) Post - Exploitation

(6) Reporting

Abstract
↓
Executive
summary

* Social
Engineering
↓

Types

(1) Physical

(2) Application

(3) Network

(4) IoT

Internal Penetration Testing - Limitation

External Penetration Testing - Only target is giv

* Zaproxy

```
Sudo apt install zaproxy
```

→ Store - Microsoft Store Snyk

Headless - Not opening browser but doing its work.

Use headless - reduce resource

Zaproxy - VA

- * Spider - makes Copy
- * Work on - 8080 (Port Conflict)
- * 1 - 1024 ports are reserved ports
- * ,

→ Private IP Disclosure

[Performance Improvement program]

Cloudflare

* Strict - Transport security Header not set without https - http can be used

→ EOL - End of Line

tenable

Nessus essential

↓

Uninstall

Install

→ By using BurpSuite find top 10 vulnerabilities [OWASP] (*) (x) [Interview]

* Top 10 - web Application Security Risks

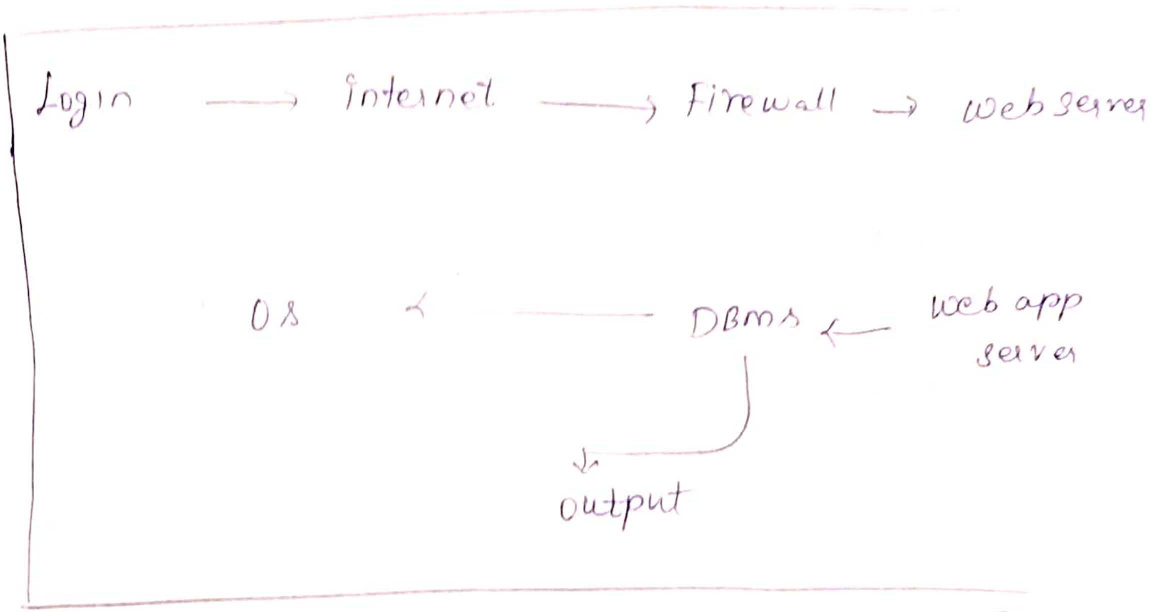
→ How to detect

→ How to prevent

CORS - CROSS ORIGIN RESOURCE

* using others website in another websites.

Web Application Firewall



→ SQL, injection.

Nitto
WPS

* Disabling password field

* Username only needed

Port
Swigger

<u>Can be done at</u>

* Where user input is got

<u>Detect</u>

* Single quote (or)
Double quote.

Authentication Vulnerability

→ ⊗⊗ Directory traversal

Cmd: pwd

Cmd: Cat /etc/passwd

→ Absolute Path
→ Relative Path

Cmd: where burpsuite

Cat ../../etc/passwd → Linux

Academy
↓
All labs

→ Path traversal payload

* put in intruder

① Authentication - username / Password

② Sql injection - Login bybass

→ Errobased Sql injection
→ Blinod
→ Boolean Based
→ Time Based

} 4 types of SQL injection

* SQL returns BOOLEAN Values so

admin' or 1=1

→ admin
→ ' OR 1=1--
" OR 1=1--

} universal username Password.

→ sql injection payload - data from github.

Login.php