

## Email Security

S/MIME

SPF

DKIM

DMARC

} Domain  
} TXT  
} Record

## DNS

find ip: `ipconfig /all` = DNS Server ip#

IBM YTB: What is DNSSEC (Domain Name System Security Extensions)?

DNSSEC:

- Authentication of DNS Data

- Protection Against DNS Spoofing
- Secure Email Routing
- Compliance & Data Integrity
- Trust chain Establishment
- Protection for IoT & Edge Devices
- Defense Against Cache Poisoning
- Support for secure web Browsing
- Improved Resilience in Zero Trust

Architectures

- Visibility for threat Hunting

- Topic 11B - Cloud & Web Application Security Concepts

DWASP - Open Web Application Security Projects



about 8 million  
2505/20/80  
111

William Prado  
08/05/2025  
Cloud & web App  
Sec Concepts

## Input Validation

Allow list ≡ white list

Deny list ≡ Black list

## YTB: Cookies: Part 2 - How secure cookies work

### Secure cookies:

Static - not running

Dynamic - running

Fuzzing - random ~~errors~~

Manual code review human analysis

### Incident Response

- Prepare / prevent

- Detect / Analyze

- Contain Eradicate & Recovery

- Feed BACK Document "lesson learned"

### CIRT / SOC

Framework "Blue Print"

<sup>mandatory</sup> ③ Procedure: "The how-to" step by step

<sup>mandatory</sup> ① Policy "The Law"

<sup>non mandatory</sup> ④ Guideline: "The advice" recommendations

<sup>mandatory</sup> ② Standard "The rule book"

Base Line "the floor"



- ① Static signature
- ② behavior ①
- ③ Heuristic multibehavior
- ④ Anomaly
- ⑤ Trend

## LockHeed-Martin Cyber Kill Chain Attack Framework

### Reconnaissance

1. Reconnaissance
2. weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Action on Objectives.