ngesec
lab & ngerumpi security

# CYBER SECURITY FOR STARTUP 1#

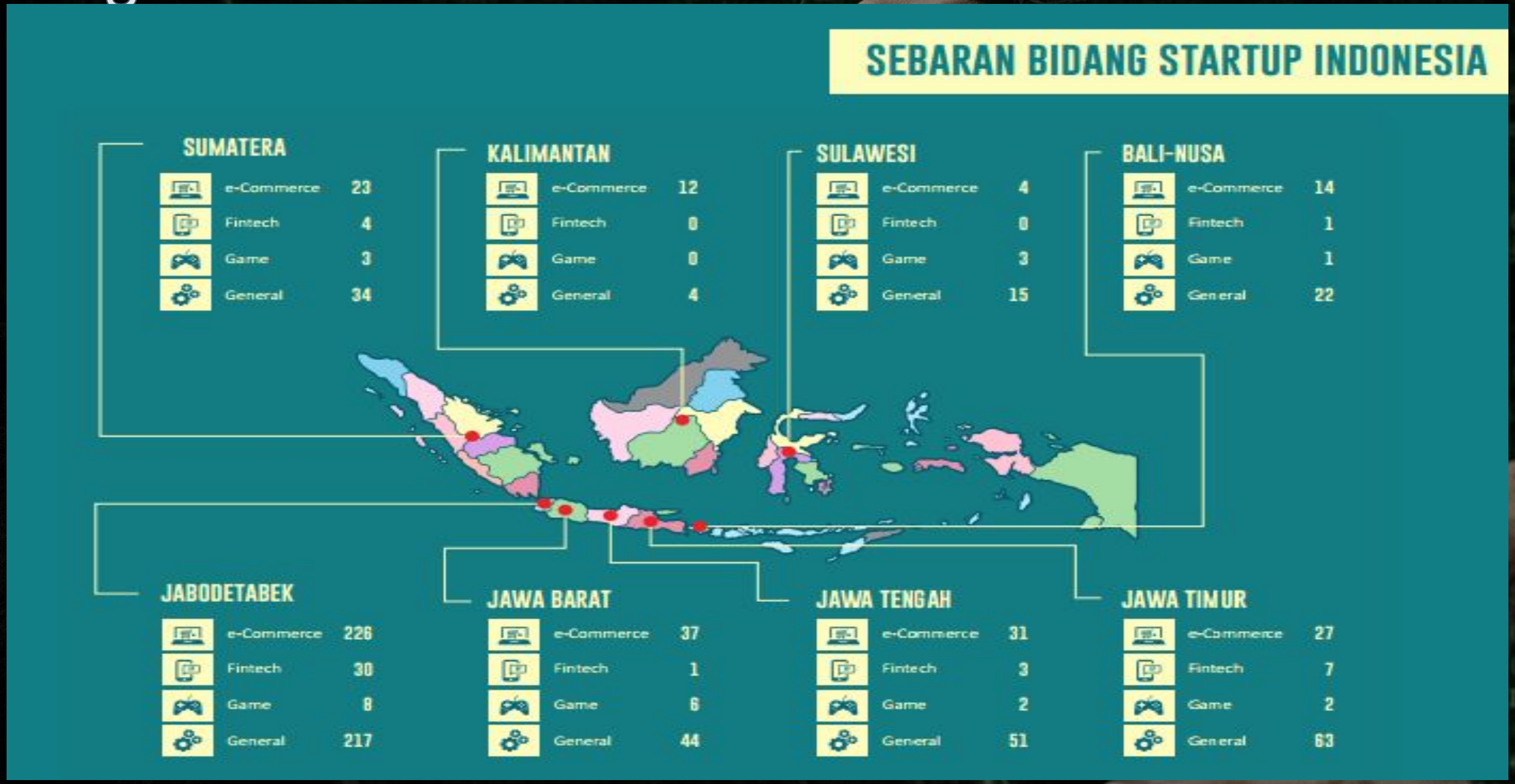
--- Febrian ---

Des 26, 2018

# About Me

- Cyber Security Activist
- System Administrator and Security Analyst at Shwetech Myanmar,Ltd
- Music Teacher at Dolce Music Class

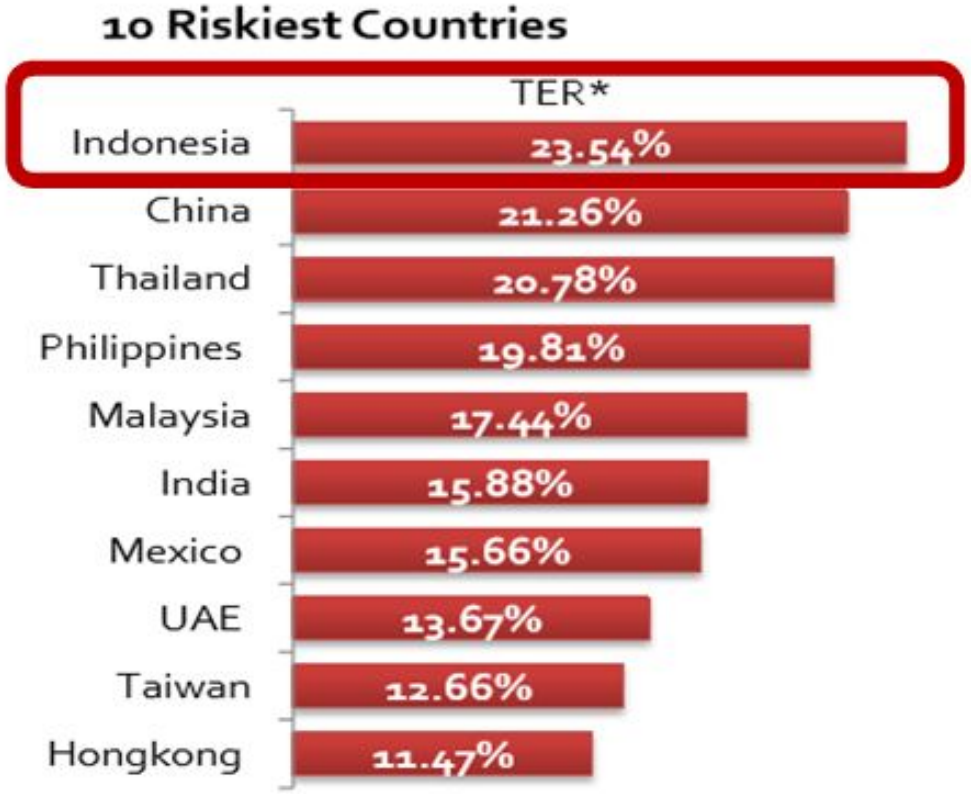
# Background 1#

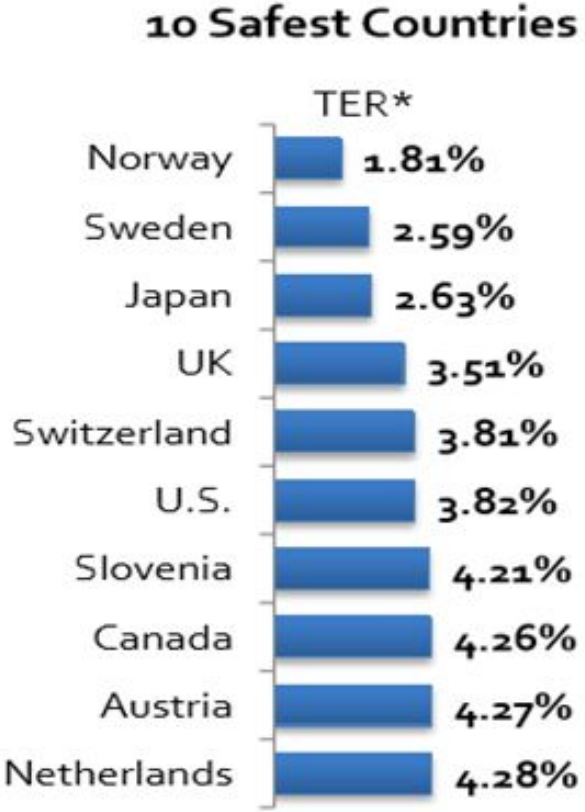



sumber : http://teknopreneur.com/2018/08/13/startup-e-commerce-menjamur-peran-medsos-jadi-tonggak-utama/

# Background 2#

## Indonesia Dianggap Sebagai Negara Paling Beresiko Mengalami Serangan IT Security




*Threat exposure rate (TER): diukur dari persentase PC yang terkena serangan malware, baik berhasil, maupun gagal, dalam periode 3 bulan

Sumber: Security threat report 2013, SophosLabs

# Background 3#

CNN Indonesia

Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya Hid

Teknologi > Berita Internet

## BSSN Catat 143 Juta Serangan Siber Pada Paruh Pertama 2018

CNN Indonesia | Selasa, 20/11/2018 21:42 WIB

Bagikan :

Ilustrasi serangan siber. (Foto: Istockphoto/ipopba

Jakarta, CNN Indonesia -- Badan Siber dan
hingga Juni 2018 terdapat 143,4 juta seran
frekuensi serangan itu bakal terus meningk

"Monitoring BSSN sepanjang bulan Januar
siber, ditambah 1.335 laporan kasus inside

CNN Indonesia

Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya Hi

Teknologi > Berita Internet

## Ransomware Masih Jadi Tren Serangan Siber

esia | Minggu, 19/08/2018 19:20 WIB

MARKET INVESTMENT NEWS ENTREPRENEUR SYARIAH FINTECH LIFESTYLE INS

CNBC Indonesia > Fintech > Berita Fintech

Perkembangan Teknologi

## Kejahatan Siber Merebak, RI Rugi Rp 478,8 Triliun

FINTECH - Roy Franedya, CNBC Indonesia | 24 May 2018 19:10

SHARE |

**Jakarta, CNBC Indonesia** - Kejahatan siber di Indonesia bisa menimbulkan kerugian
dari seluruh kateg

TEMPO.CO

FOKUS

HOME NASIONAL BISNIS METRO DUNIA BOLA CANTIK TEKNO OTOMOTIF FOTO VIDEO

HOME > BISNIS > BISNIS

## Kasus Voucher Bukalapak, Polisi: Tersangka Manipulasi Data

Reporter: Tempo.co
Editor: Martha Warta Silaban

Jumat, 21 Desember 2018 12:59 WIB

0 KOMENTAR 30 0 35


Di hari Belanja Online Nasional (Harbolnas)12.12 situs Bukalapak menawarkan sebuah mobil seharga Rp 12 ribu. 12 Desember 2018. TEMPO/Wawan Priyanto

# Why ???


When the development process is not in accordance with the principle "Secure Development LifeCycle" only prioritizes functionality and does not test the security level of the application

Weak level of information security awareness and lack of education about "Security Awareness"

The use of software and frameworks that do not update and use a firewall that is not optimal due to limited knowledge and skills

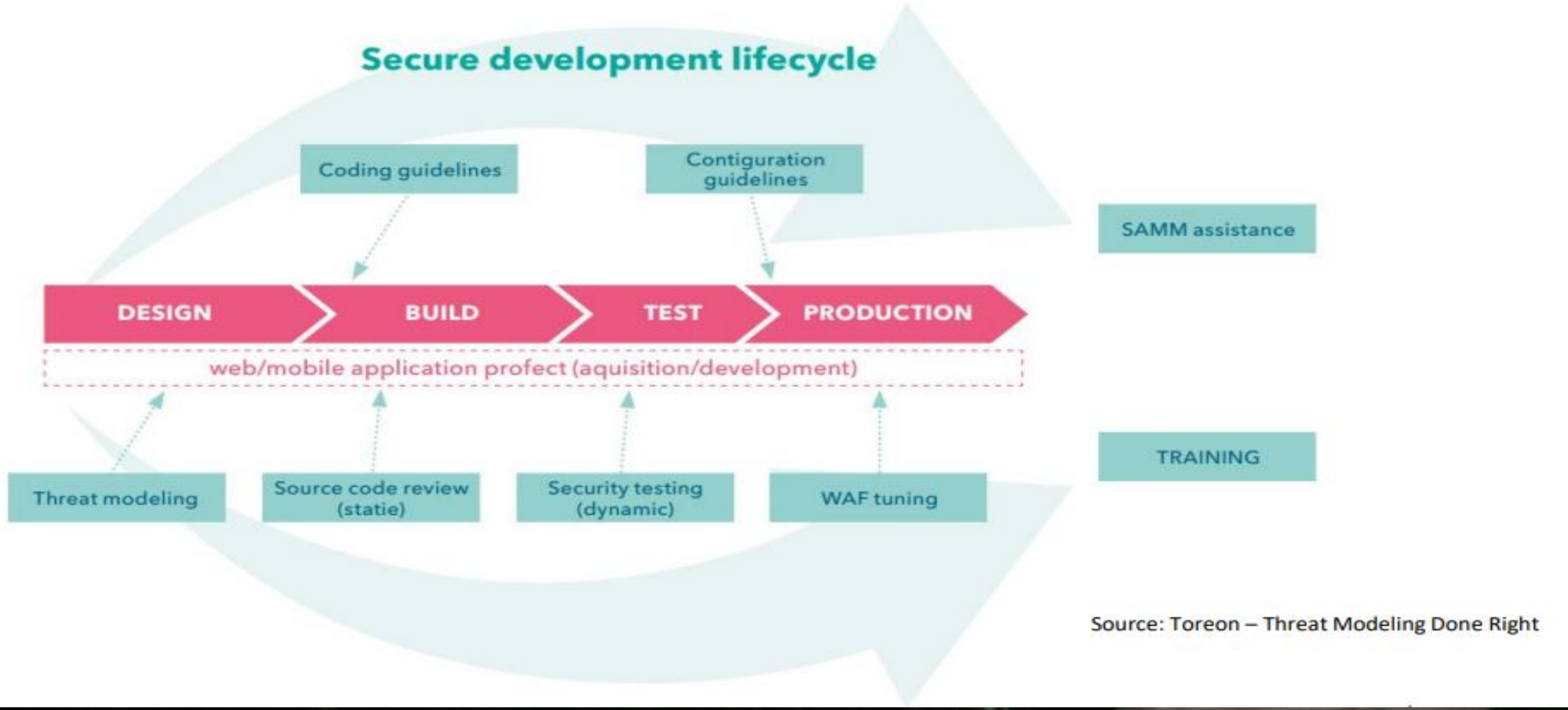
# Software Security And Risk principles Overview

- Different approach between development team and attacker

| Development Team | Attacker(s) |
| --- | --- |
| • Typically approaches an application based on what it is intended to do | • More interested in what an application can be made to do and operates on the principle that "any action not specifically denied, is allowed". |
| • Designing an application to perform specific tasks based on documented functional requirements and use cases. | • Intentionally making application in false condition |
| • Doing with Deadline Management | • Doing fun |

- To address this, some additional elements need to be integrated into the early stages of the software lifecycle.

# Secure Software Development LifeCycle



# Introduction of Vulnerabilities

Software security flaws can be introduced at any stage of the software development lifecycle, including:

- Not identifying security requirements up front
- Creating conceptual designs that have logic errors
- Using poor coding practices that introduce technical vulnerabilities
- Deploying the software improperly
- Introducing flaws during maintenance or updating

# Impact


| | | |
|---|---|---|
| 01 | **Data** | • Theft<br>• Manipulation<br>• Demage<br>• Financial Loss |
| 02 | **Server** | • The server is used as a proxy for cybercrime |
| 03 | **Ilegal Activities** | • Ilegal Access<br>• Spy<br>• Virus, Trojan, Backdoor, dll<br>• Terorisme |

# Web Security Myth

- Secure Socket Layer (SSL) will protect entire websites
- Firewall will secure you against attack
- No issues printed from Automatic Web Vulnerability Scanner
- Annual Vulnerability Assessment is enough
- Our developer has a good skill in programming
- ?

# Security Frameworks - Examples

# Security Frameworks - Examples

# Security Frameworks Recomendation

https://www.cisecurity.org/

**CIS Distribution :**


**CIS Product :**

| | |
|---|---|
| 01 | **CIS CONTROL**<br>To improve from the side of the organization. As a handle when organizations are confused about starting it. |
| 02 | **CIS BENCHMARK**<br>For technical guidance on servers, desktops, web servers, browsers, etc. CIS Benchmark is also used as a checklist when an organization conducts ISO 27001: 27003 certification. |

# Security Frameworks Recomendation

## CIS Benchmark And CIS CAT Tool (Examples)

### *3.2 Give the Apache User Account an Invalid Shell (Scored)*

- Level 1

**Description:**

The `apache` account must not be used as a regular login account, and should be assigned an invalid or `nologin` shell to ensure that the account cannot be used to login.

**Rationale:**

Service accounts such as the `apache` account represent a risk if they can be used to get a login shell to the system.

**Audit:**

Check the `apache` login shell in the `/etc/passwd` file:

```
# grep apache /etc/passwd
```

The `apache` account shell must be `/sbin/nologin` or `/dev/null` similar to the following:
`/etc/passwd:apache:x:48:48:Apache:/var/www:/sbin/nologin`

**Remediation:**

Change the `apache` account to use the `nologin` shell or an invalid shell such as `/dev/null`:

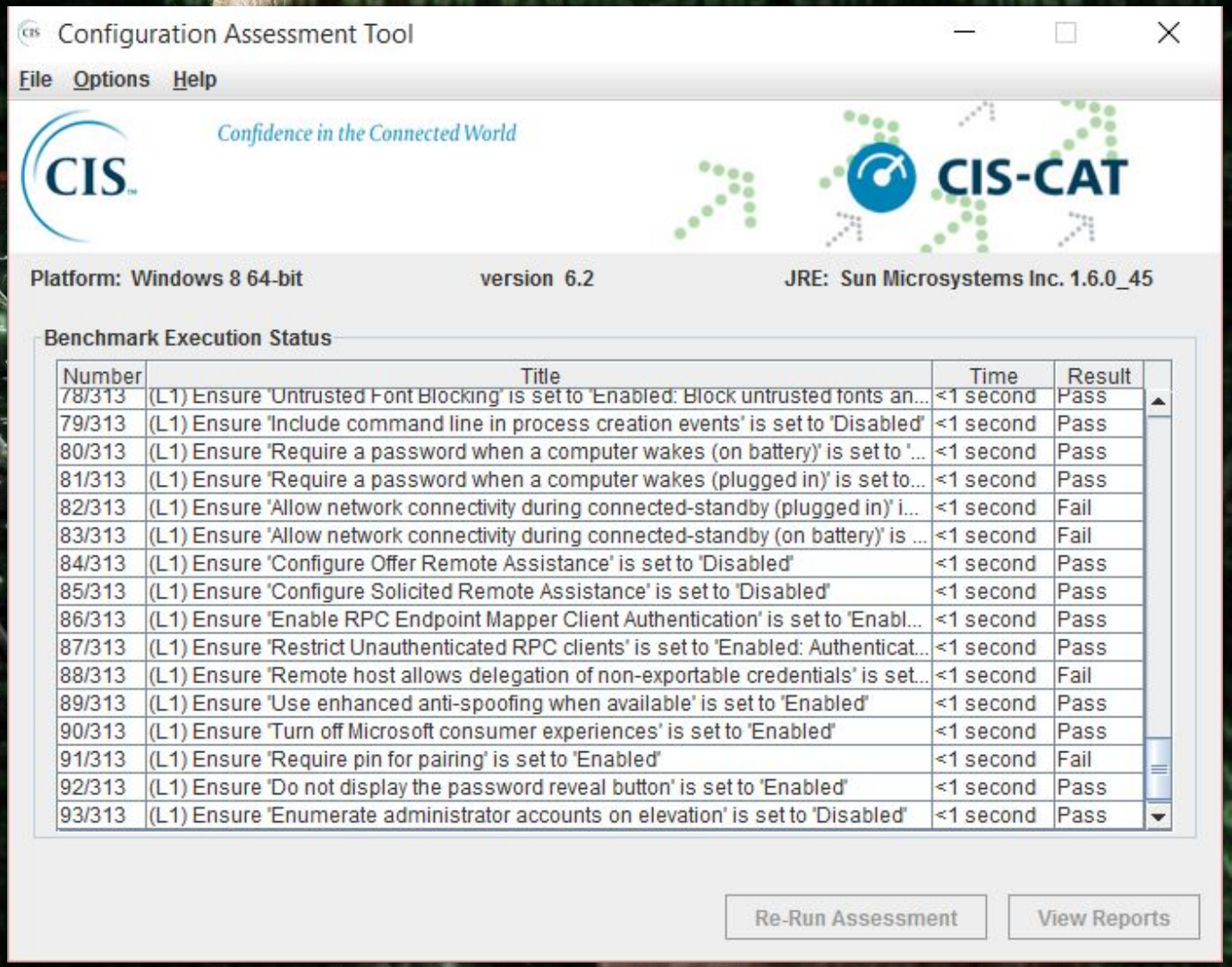
```
# chsh -s /sbin/nologin apache
```

**Default Value:**

The default Apache user account is `daemon`. The daemon account may have a valid login shell or a shell of `/sbin/nologin` depending on the operating system distribution version.

**CIS Controls:**

16 Account Monitoring and Control
Account Monitoring and Control



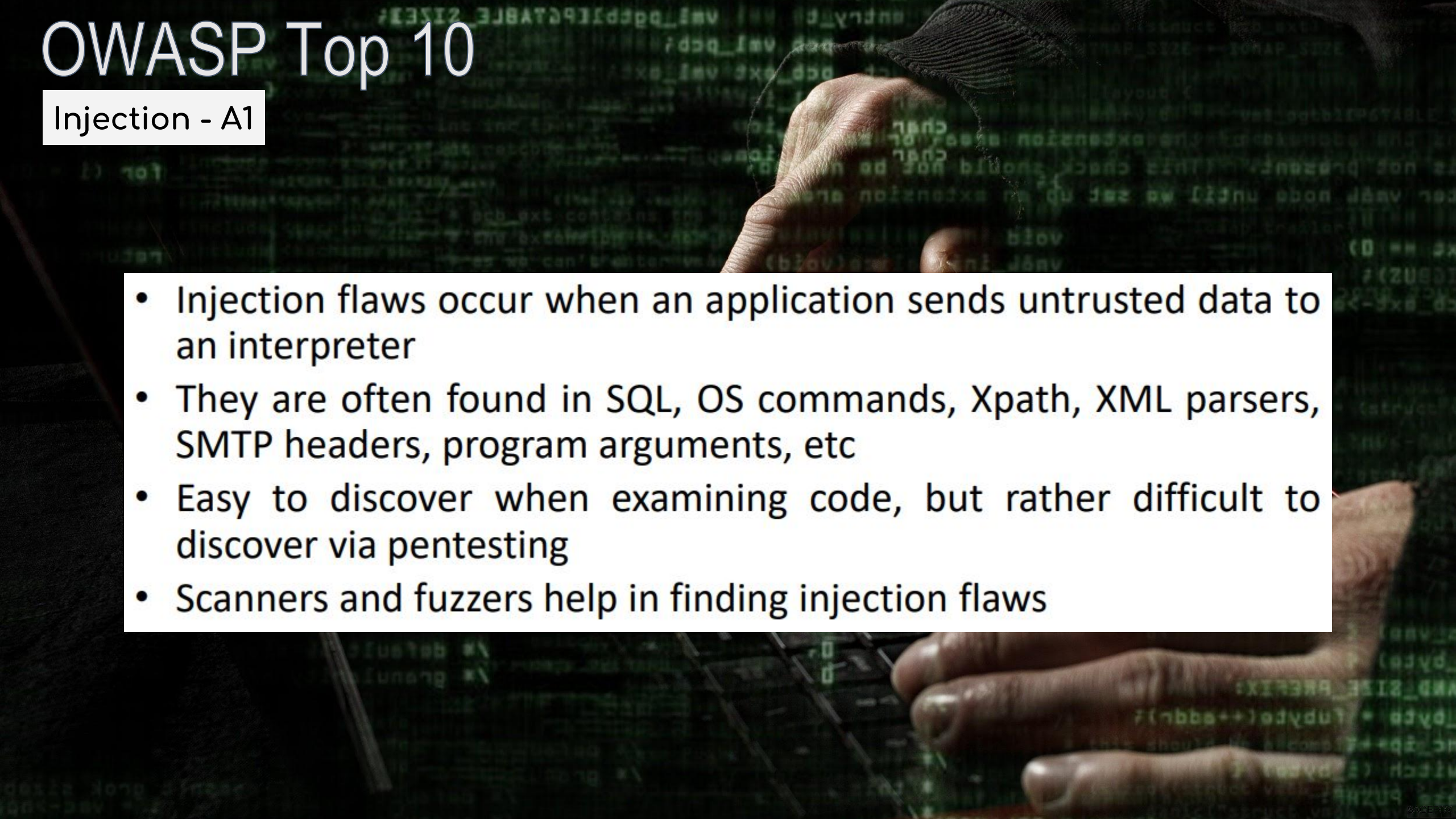
# The Open Web Application Security Project

## OWASP Top 10

| OWASP Top 10 - 2013 | → | OWASP Top 10 - 2017 |
|---|---|---|
| A1 – Injection | → | A1:2017-Injection |
| A2 – Broken Authentication and Session Management | → | A2:2017-Broken Authentication |
| A3 – Cross-Site Scripting (XSS) | ↘ | A3:2017-Sensitive Data Exposure |
| A4 – Insecure Direct Object References [Merged+A7] | U | A4:2017-XML External Entities (XXE) [NEW] |
| A5 – Security Misconfiguration | ↘ | A5:2017-Broken Access Control [Merged] |
| A6 – Sensitive Data Exposure | ↗ | A6:2017-Security Misconfiguration |
| A7 – Missing Function Level Access Contr [Merged+A4] | U | A7:2017-Cross-Site Scripting (XSS) |
| A8 – Cross-Site Request Forgery (CSRF) | ☒ | A8:2017-Insecure Deserialization [NEW, Community] |
| A9 – Using Components with Known Vulnerabilities | → | A9:2017-Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards | ☒ | A10:2017-Insufficient Logging&Monitoring [NEW,Comm.] |

# OWASP Top 10

## Injection - A1



- Injection flaws occur when an application sends untrusted data to an interpreter
- They are often found in SQL, OS commands, Xpath, XML parsers, SMTP headers, program arguments, etc
- Easy to discover when examining code, but rather difficult to discover via pentesting
- Scanners and fuzzers help in finding injection flaws

# OWASP Top 10

Injection - A1

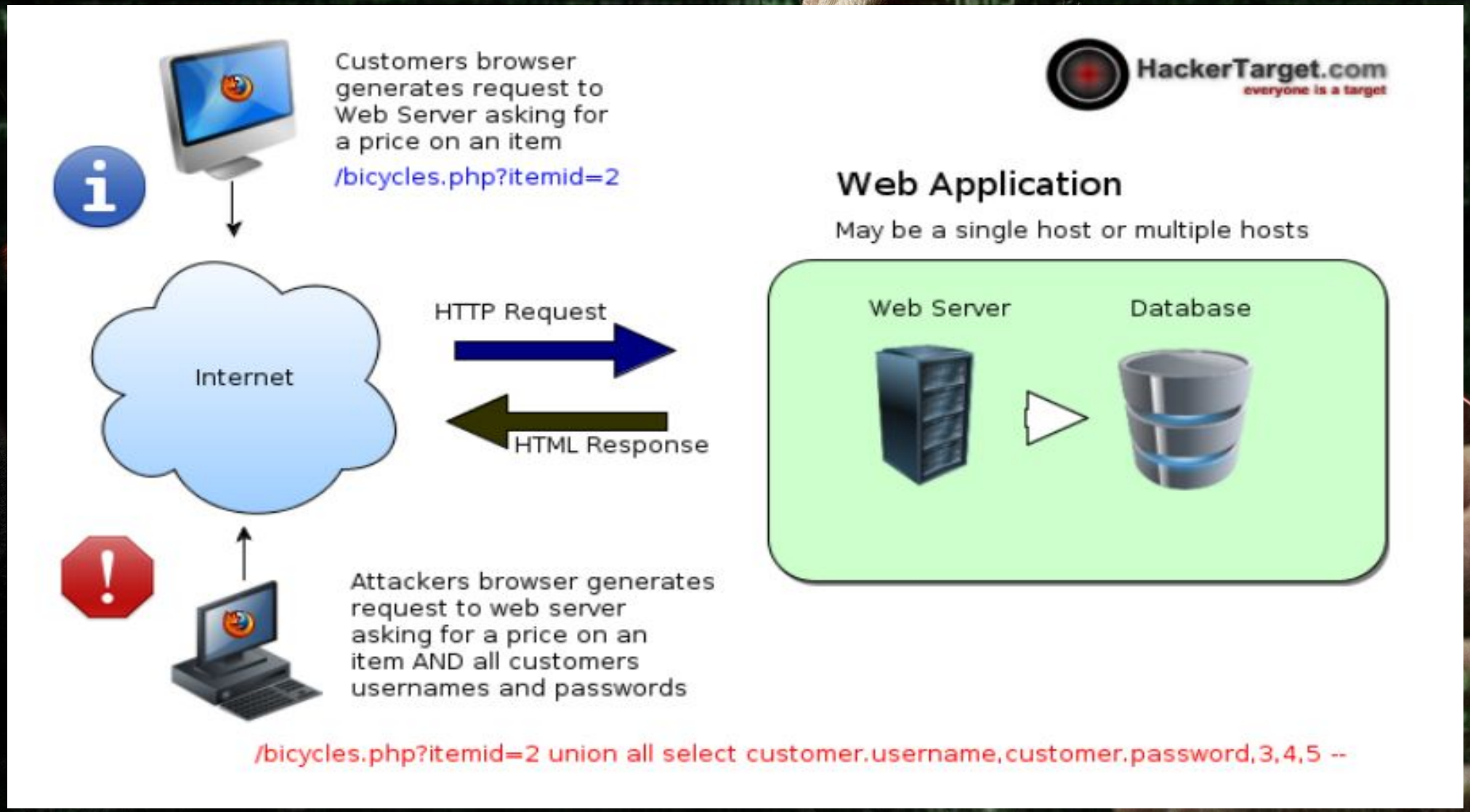
## SQL Injection

- SQL injection is an attack technique that exploits a security vulnerability occurring in the database layer of an application.

- Attackers use injections to obtain unauthorized access to the underlying data, structure, and DBMS.

# OWASP Top 10

## Injection - A1



# OWASP Top 10

Injection - A1

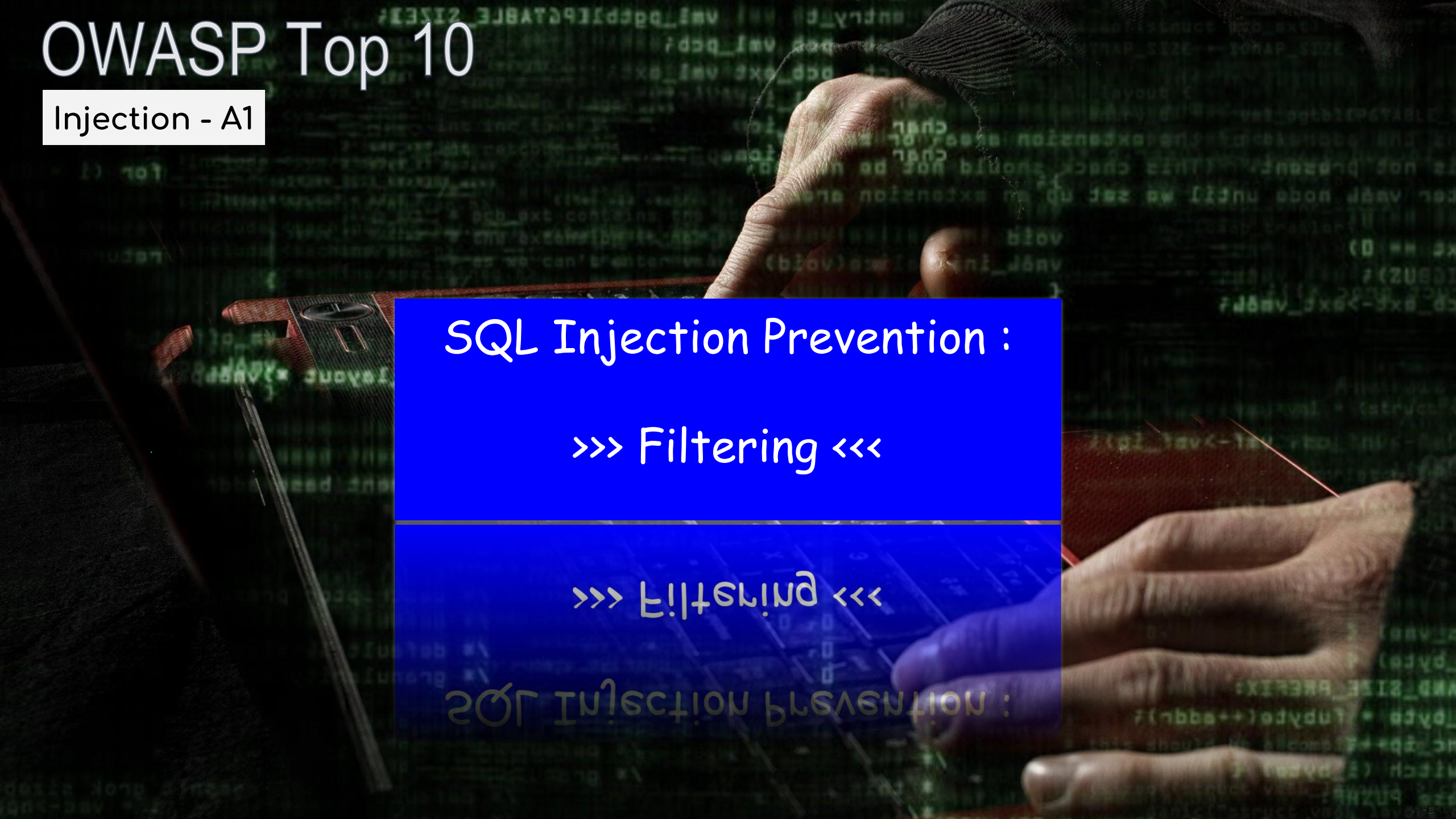
## SQL Injection – How it works?

- Attacker should be manipulate the URL with SQL command


- Sample Target:
  - http://target.local/news.php?id=99 [sql command]

# OWASP Top 10

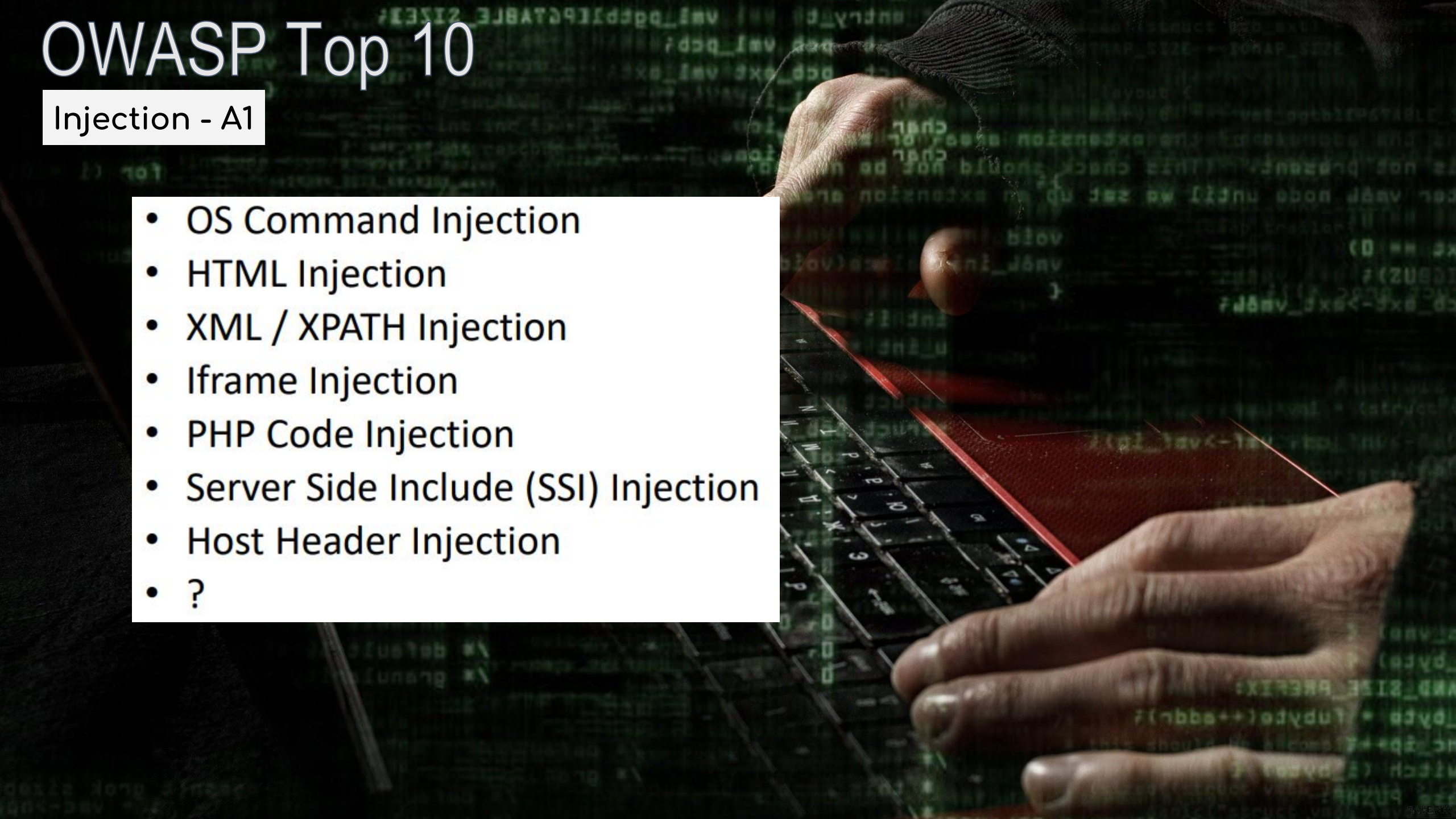
Injection - A1



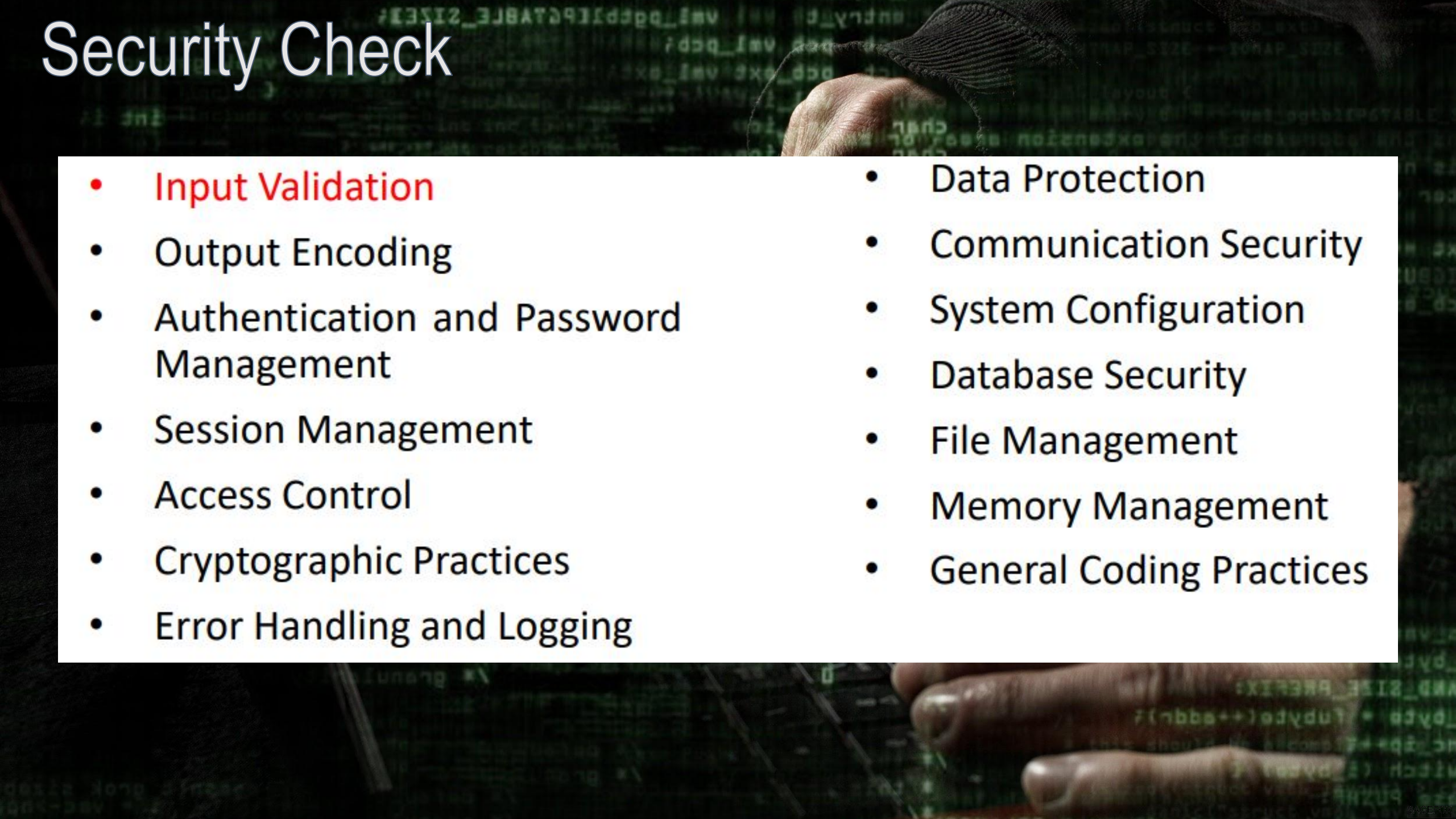
# OWASP Top 10

## Injection - A1

- OS Command Injection
- HTML Injection
- XML / XPATH Injection
- Iframe Injection
- PHP Code Injection
- Server Side Include (SSI) Injection
- Host Header Injection
- ?



# Security Check



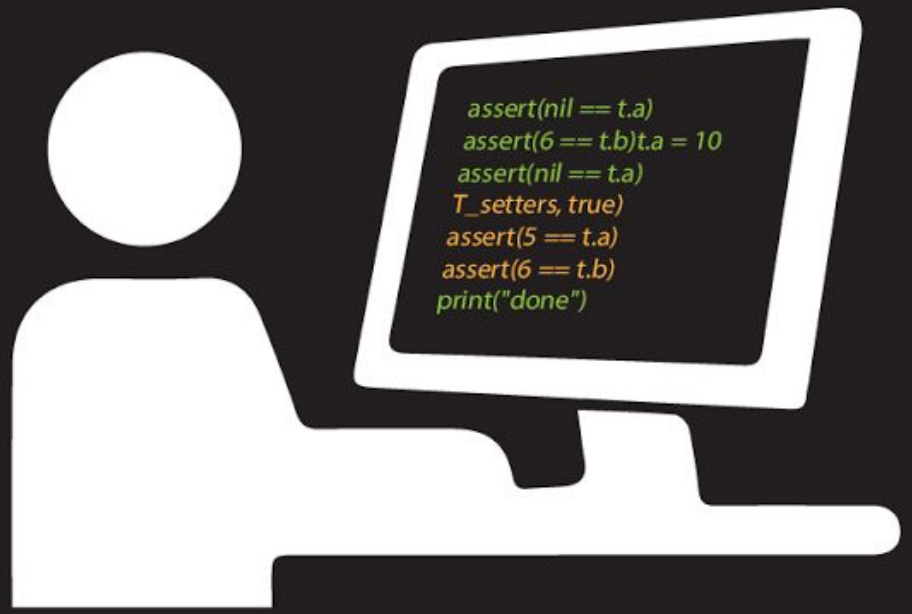
- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

# Security Test

## Penetration Testing

VS.

## Vulnerability Scanning




# Penetration Testing

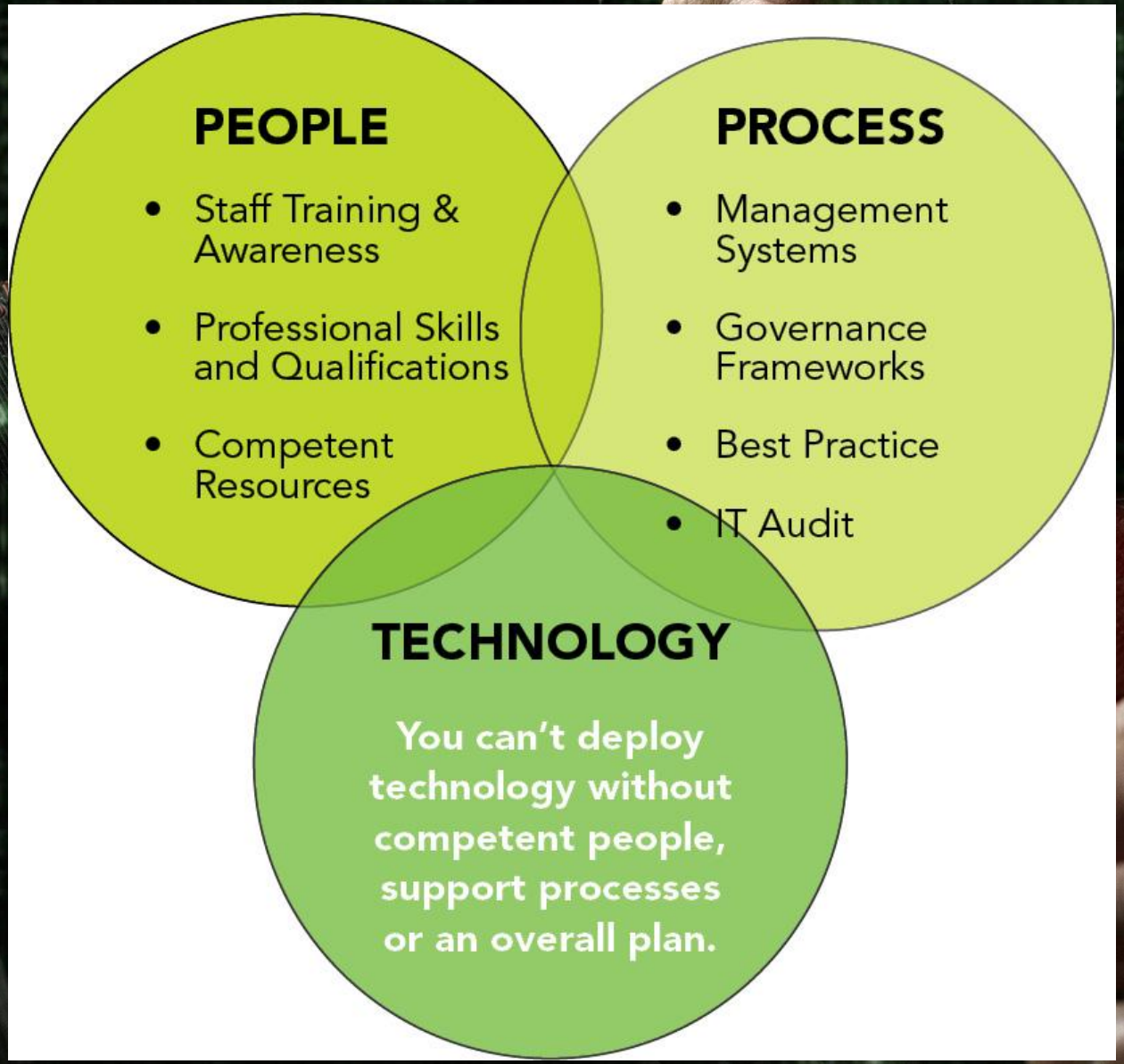
# Penetration Testing

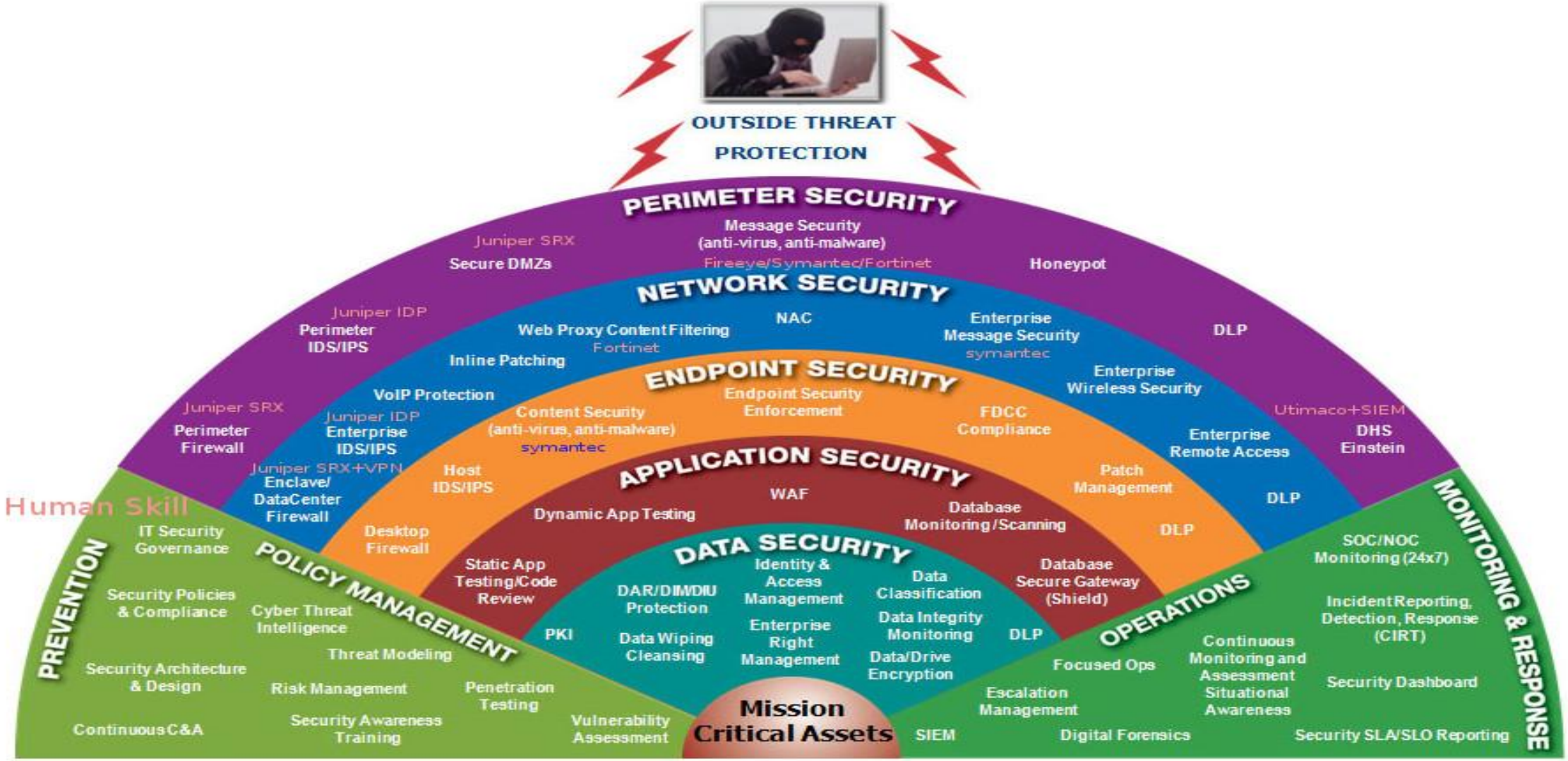
# Vulnerability Assessement

# Vulnerability Assessement


PENETRATION TESTING
≠
VULNERABILITY ASSESSEMENT

# Process In IT Security

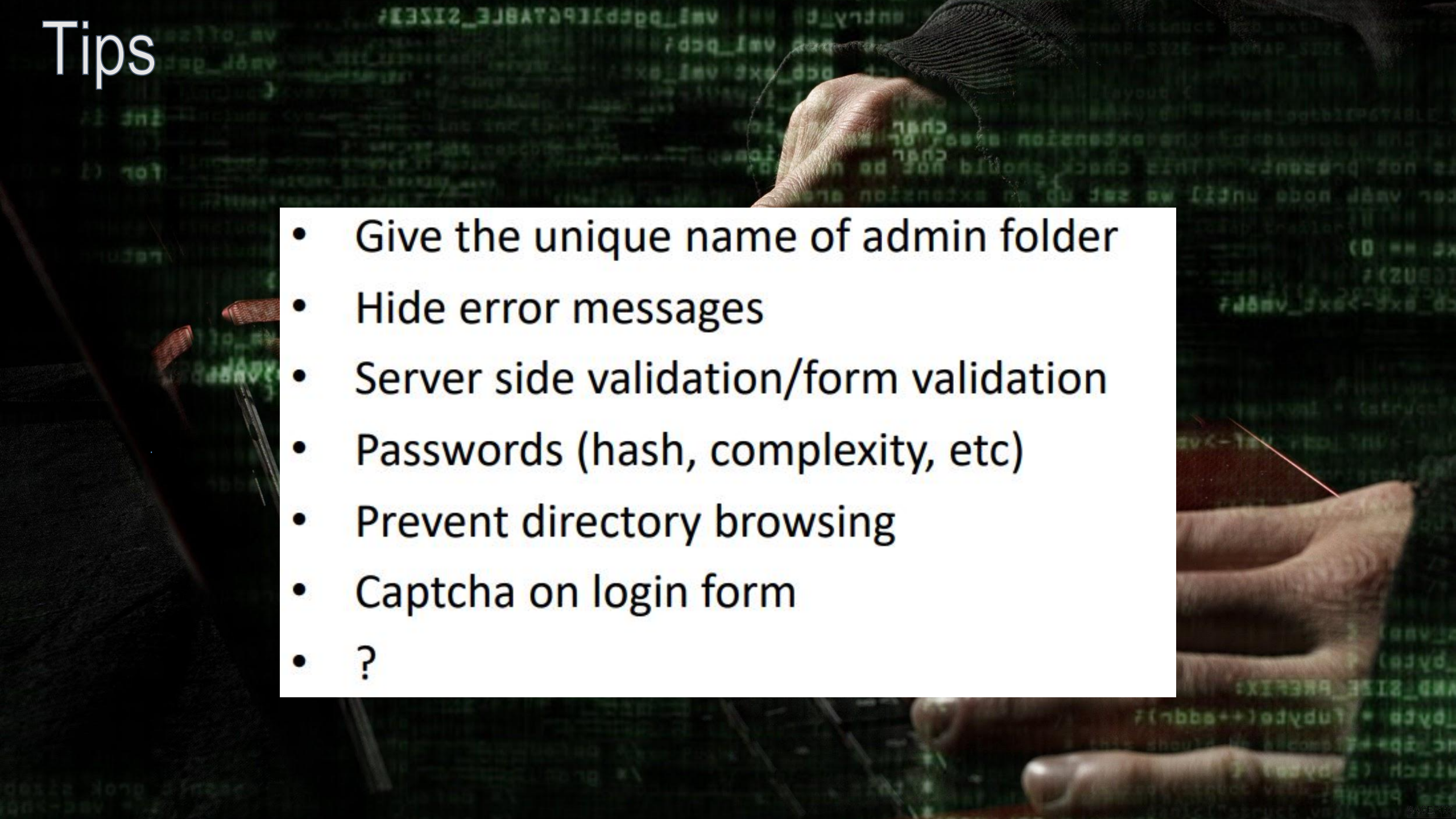





DLP = Data Lost Prevention

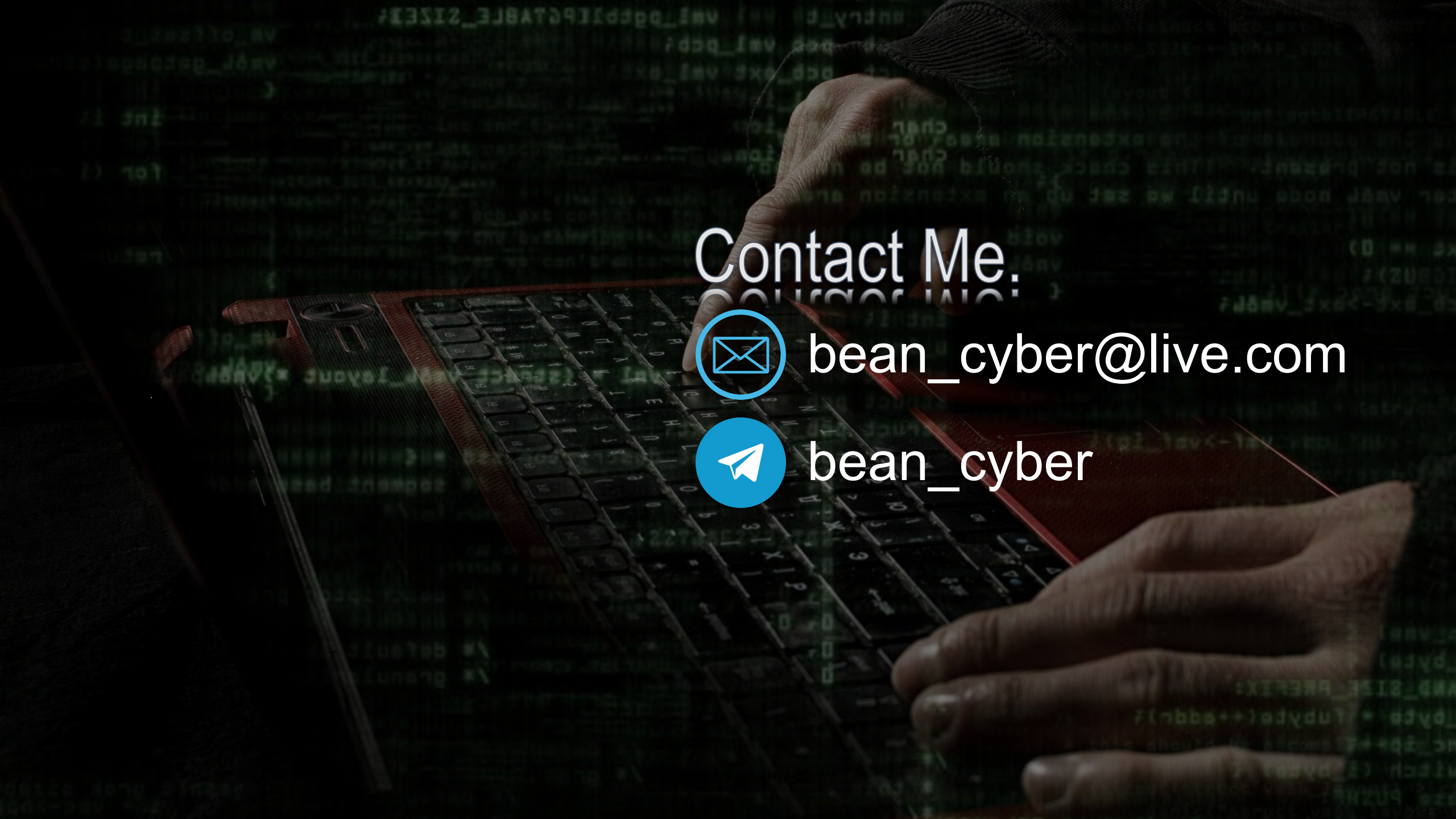
WAF =Web Application Firewall
DHS = Departement of Homland Security/US-Cert Program
C&A = Certification and Accreditation
PKI = Public Key Infrastucture
DAR = Data at Rest
DIM = Data in Motion
DIU = Data in Use
SLO = Service Level Objective
SIEM = Security Information and Event Management
FDCC = Federal Desktop Core Configuration

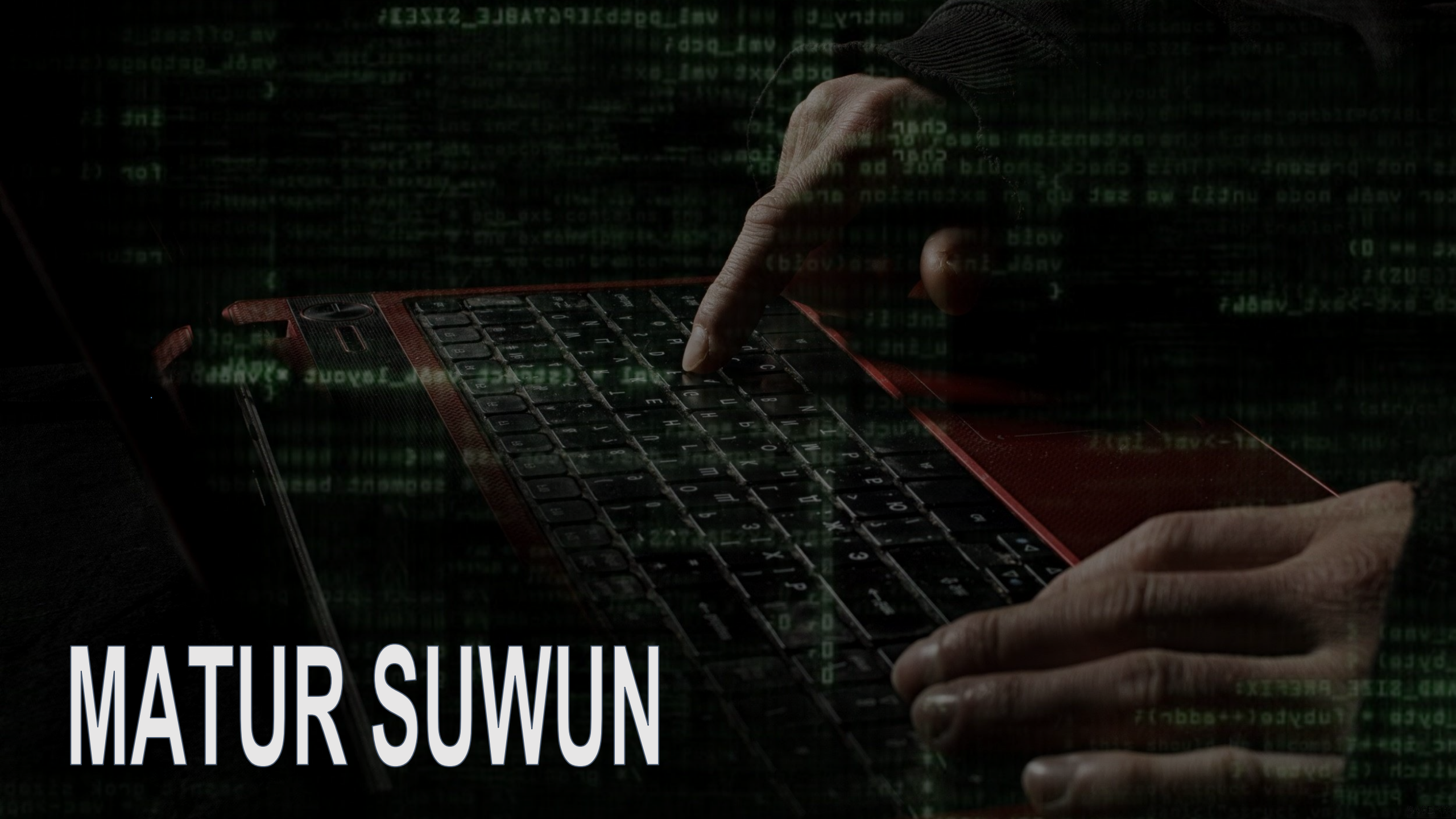
# Tips



- Give the unique name of admin folder
- Hide error messages
- Server side validation/form validation
- Passwords (hash, complexity, etc)
- Prevent directory browsing
- Captcha on login form
- ?

# Conclusion


Contact Me.
bean_cyber@live.com
bean_cyber


MATUR SUWUN


Q
A