

# Hackers & Hunters II

## هکرها و شکارچیان ۲

آشنایی با آسیب پذیری‌های برتر وب سایت‌ها  
*OWASP Top 10*

۱۴۰۳

کیان درفش‌دار



# فیلم خوش آمدگویی

۱۱:۰۰

آنچه گذشت ...

آسیب پذیری های برتر وب اپلیکیشن ها  
در سال ۲۰۲۱

بخش اول

مثال هایی از هر آسیب پذیری

بخش دوم

## آنترانک

ادامه مثال ها

بخش سوم

نکات مهم امنیتی در ساخت وب اپلیکیشن

بخش چهارم

خطرات امنیتی قابل توجه برای برنامه نویسان وب

بخش پنجم

پرسش و پاسخ

۱۲:۳۰



مروری بر قسمت اول

# شاخه‌های اصلی امنیت

## چرا زمینه‌های مختلفی در امنیت سایبری داریم؟

۶. استراتژی‌های دفاع در مقابل حمله  
(تشخیص و کاهش آسیب)

۷. تحقیق و توسعه  
(آسیب پذیری‌های جدید)

۸. آموزش و پرورش  
(آموزش‌های جدید و مدارک بیشتر)

۱. انواع مختلفی از تهدید‌ها و حملات  
(malware, phishing, social engineering, and etc.)

۲. توانایی‌های خاص  
(technical skills and knowledge)

۳. قانون‌گذاری و رعایت قوانین  
(HIPPA , PCI DSS)

۴. پیچیدگی تکنولوژی‌ها  
(IOT , mobile applications and etc.)

۵. مدیریت ریسک  
(بانک و مغازه فست‌فود)

# معیارها و سازمانهای جهانی امنیت

NIST

National Institute of Standards  
and Technology

PCI SSC

Payment Card Industry  
Security Standards Council

MITRE  
Corporation

CIA Triad

Confidentiality, Integrity, and  
Availability

CVSS

Common Vulnerability  
Scoring System

CVE

Common Vulnerabilities and  
Exposures



# زمینه های فعالیت

۱. تست نرم افزار
۲. تست وب اپلیکیشن
۳. تست موبایل اپلیکیشن
۴. امنیت شبکه
۵. برنامه های آزاد باگ بانگ
۶. تست بازی
۷. تیم قرمز، هک قانونمند
۸. امنیت سخت افزار

## STEP 01

Lorem ipsum dolor sit amet,  
consectetur adipiscing elit, sed  
do eiusmod tempor incididunt ut  
labore et dolore magna aliqua.



## STEP 02

Lorem ipsum dolor sit amet,  
consectetur adipiscing elit, sed  
do eiusmod tempor incididunt ut  
labore et dolore magna aliqua.



## STEP 03

Lorem ipsum dolor sit amet,  
consectetur adipiscing elit, sed  
do eiusmod tempor incididunt ut  
labore et dolore,

# نقشه راه

## STEP 04

Lorem ipsum dolor sit amet,  
consectetur adipiscing elit, sed  
do eiusmod tempor incididunt ut  
labore et dolore magna aliqua. Ut  
enim.



## STEP 05

Lorem ipsum dolor sit amet,  
consectetur adipiscing elit, sed  
do eiusmod tempor incididunt ut  
labore et dolore magna aliqua.



بخش اول

# آسیب پذیری‌های برتر وب اپلیکیشن‌ها در سال ۲۰۲۱



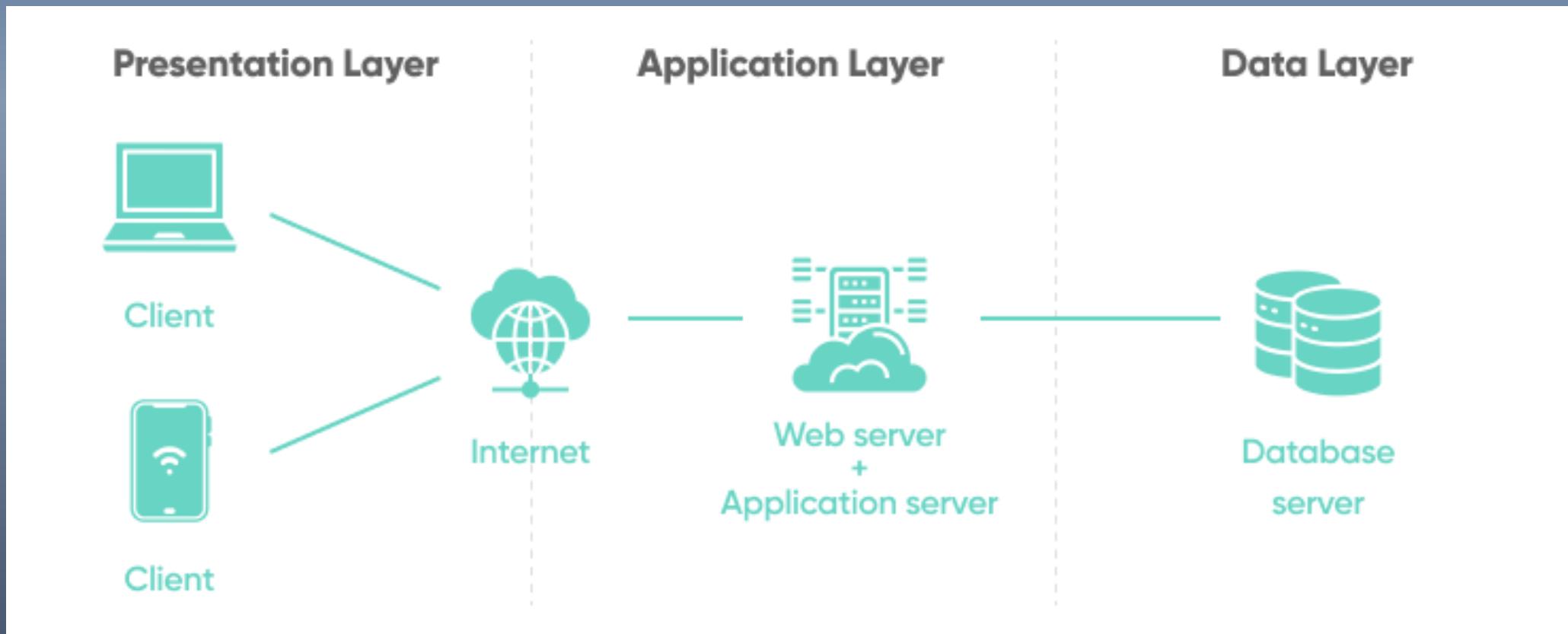
# OWASP Top 10

# چیست؟ OWASP

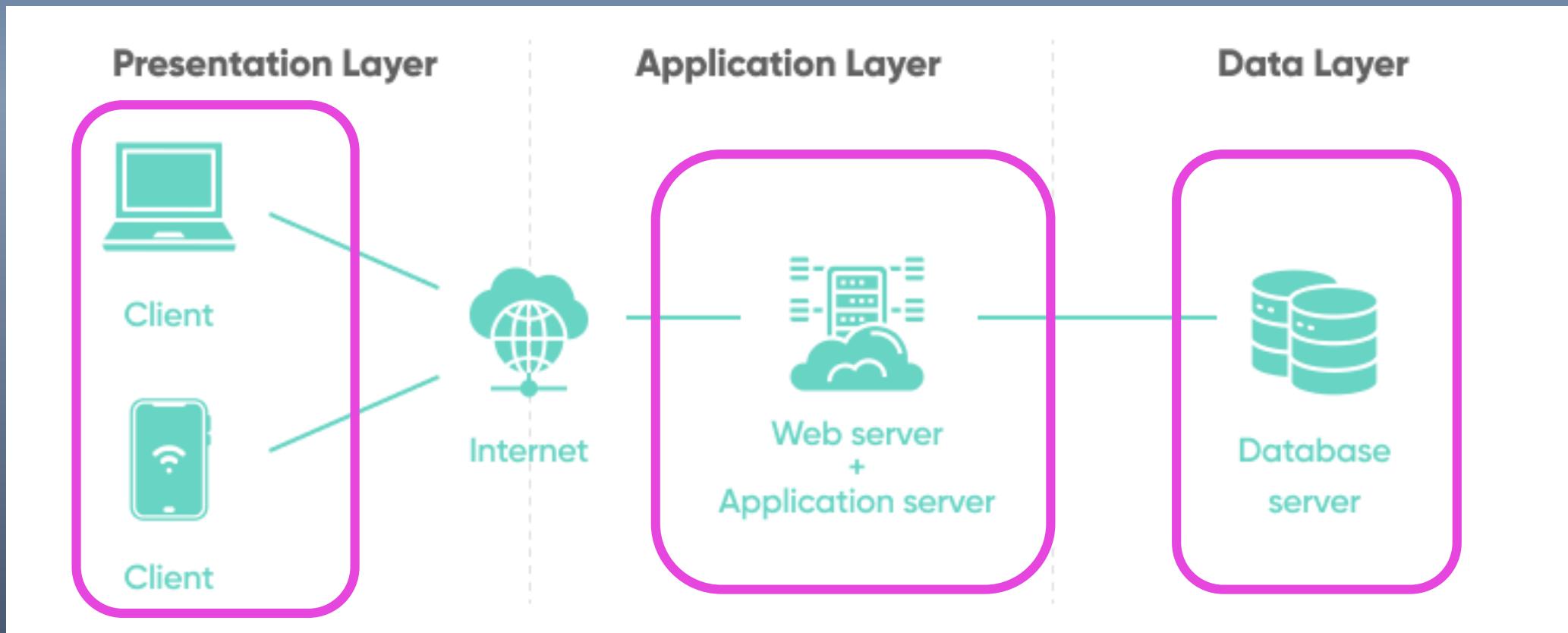
Open Web Application Security Project

- Nonprofit Organization
  - Provide freely available Resources, Tools, and Guidelines
  - most famous resource is the **OWASP Top 10**
- 
- ❖ OWASP's mission is to raise awareness about security vulnerabilities in web applications

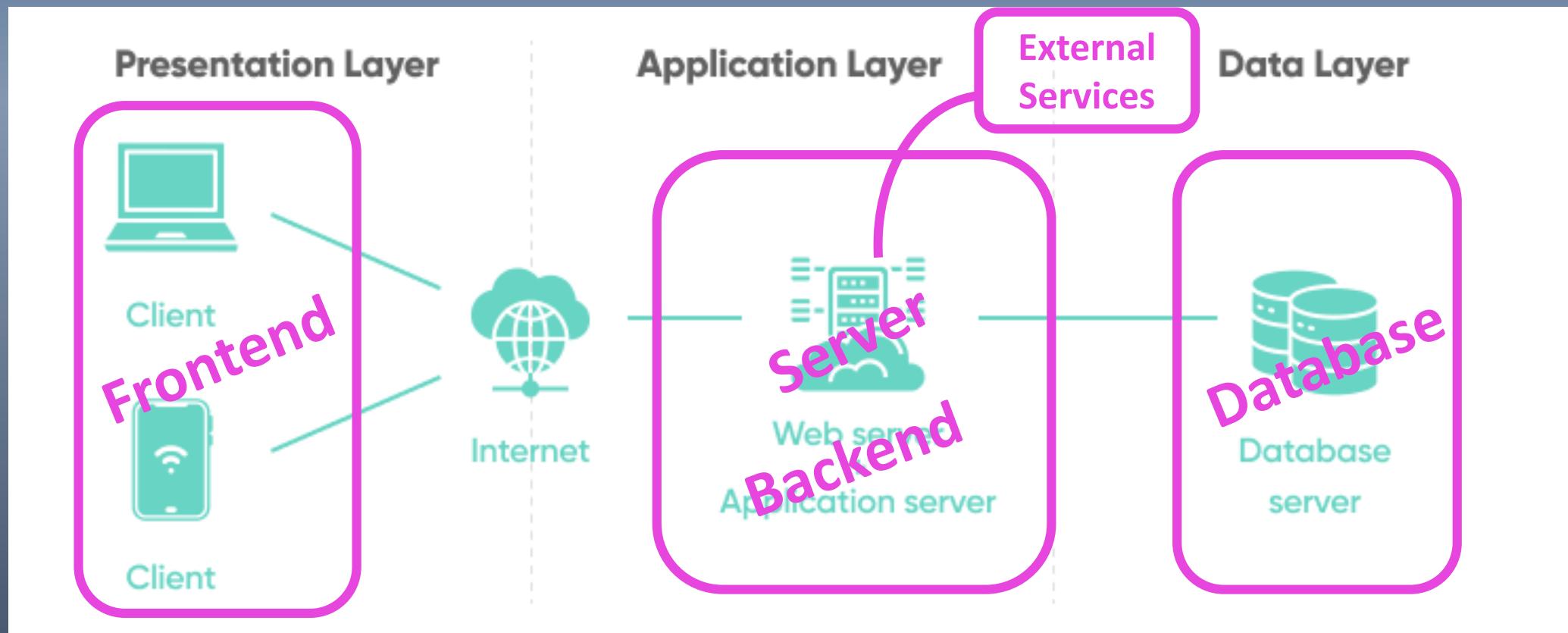
# Basic Web Application Schema



# Basic Web Application Schema



# Basic Web Application Schema



# Web Application Parts

## Frontend

User Interface (UI)

HTML

CSS

JavaScript & Frameworks

HTTP Requests

## Backend

Application Server  
(Node.js, Django, Flask, etc.)

Business Logic Layer  
(Authentication, etc.)

## Server

Web Server  
(Apache, nginx)

HTTP/HTTPS Handlers

## Database

Stores application  
data, queries, etc.

Relational Or NoSQL

## External Services & APIs

Third-party services for  
additional features

Payment Gateway  
Email Services  
Cloud Storage  
External APIs

# آسیب پذیری‌های برتر وب اپلیکیشن‌ها

## در سال ۲۰۲۱

2017

A01 Injection

A02 Broken Authentication

A03 Sensitive Data Exposure

A04 XML External Entities

A05 Broken Access Control

A06 Security Misconfiguration

A07 Cross Site Scripting

A08 Insecure Deserialization

A09 Using Components with Known Vulnerabilities

A10 Insufficient Logging & Monitoring

2021

▲ 4 A01 Broken Access Control

▲ 1 A02 Cryptographic Failures

▼ 2 A03 Injection

NEW A04 Insecure Design

▲ 1 A05 Security Misconfiguration

▲ 3 A06 Vulnerable and Outdated Components

▼ 5 A07 Identification and Authentication Failures

NEW A08 Software and Data Integrity Failures

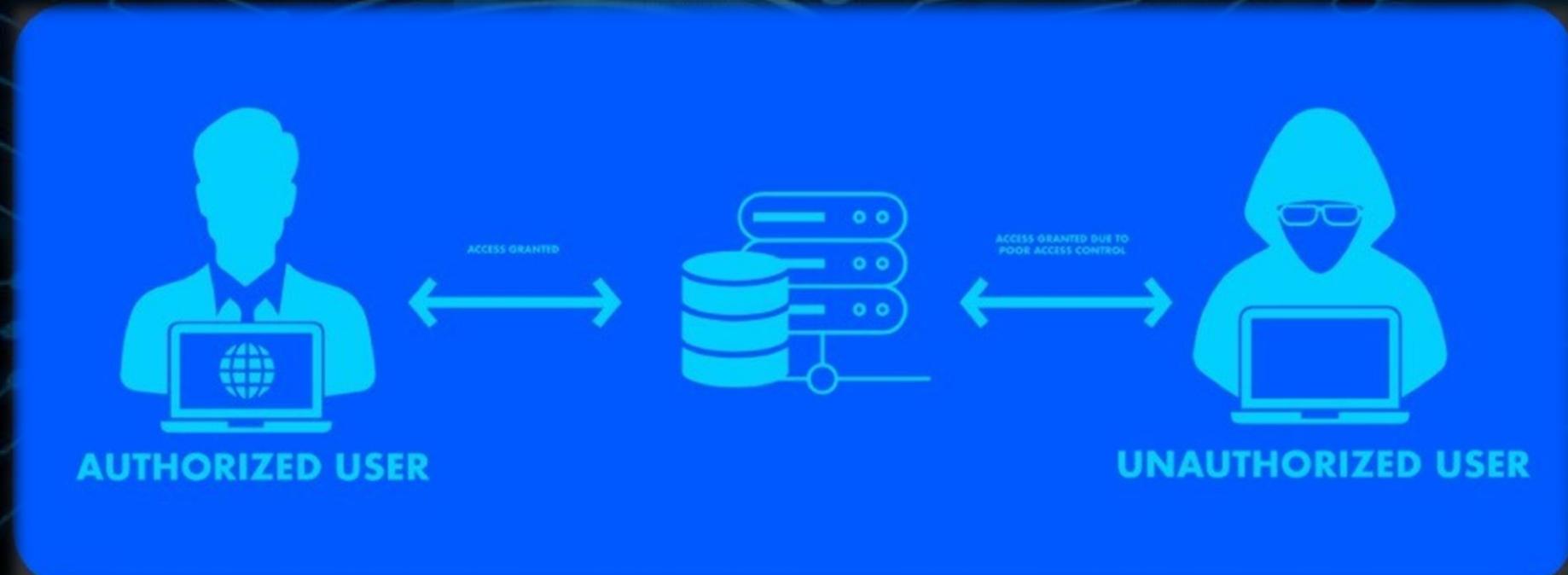
▲ 1 A09 Security Logging and Monitoring Failures

NEW A10 Server-Side Request Forgery

# First Bug

# Broken Access Control

OWASP Top 10



## Impact:

- Unauthorized access to sensitive data
- Privilege escalation
- Data manipulation and account takeovers

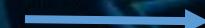
First Bug  
**Broken Access Control**

OWASP Top 10

<https://Example.tld/Login.php>



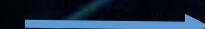
<https://Example.tld/Admin/Adduser.php>



**Admin can add User here**

**Without privilege:**

<https://Example.tld/Admin/Adduser.php>

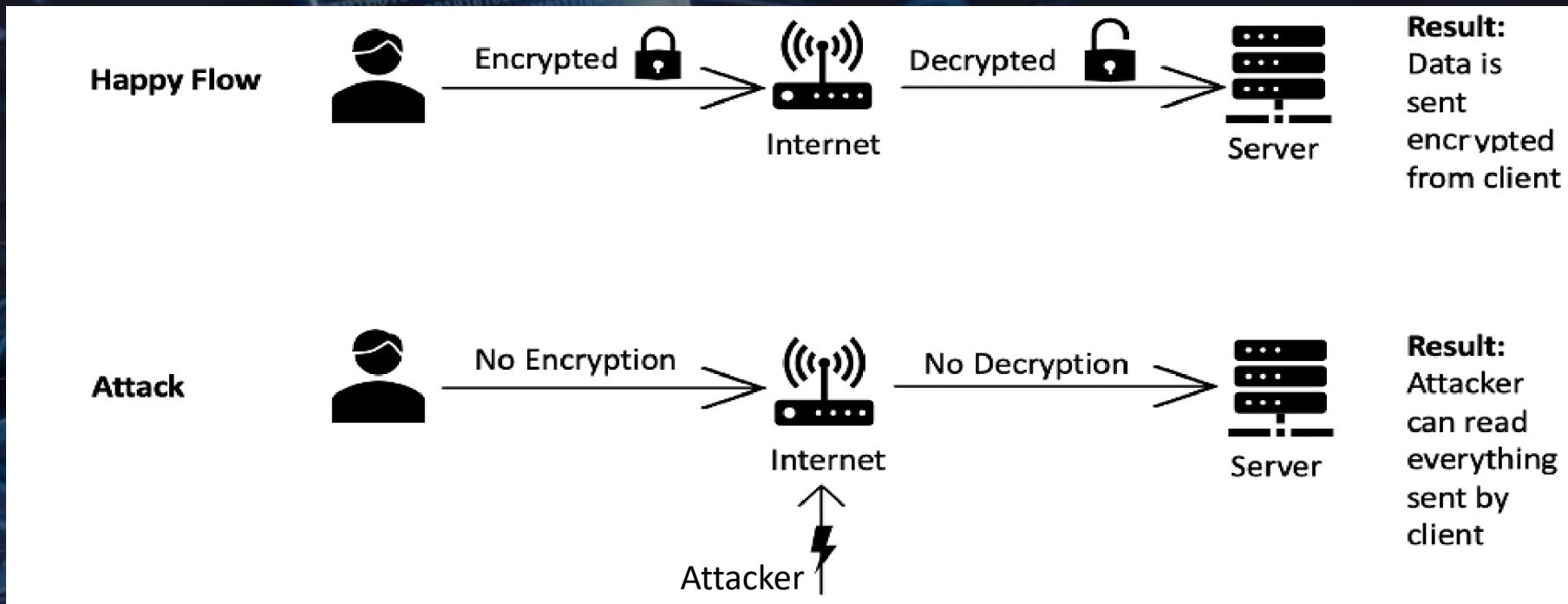


**Hacker can add User here**

## Second Bug

# Cryptographic Failures

OWASP Top 10



### Impact:

- Exposure of sensitive information (e.g., passwords, financial data)
- Data breaches and identity theft

Second Bug  
**Cryptographic Failures**

OWASP Top 10

**Database Table:**  
**Users**

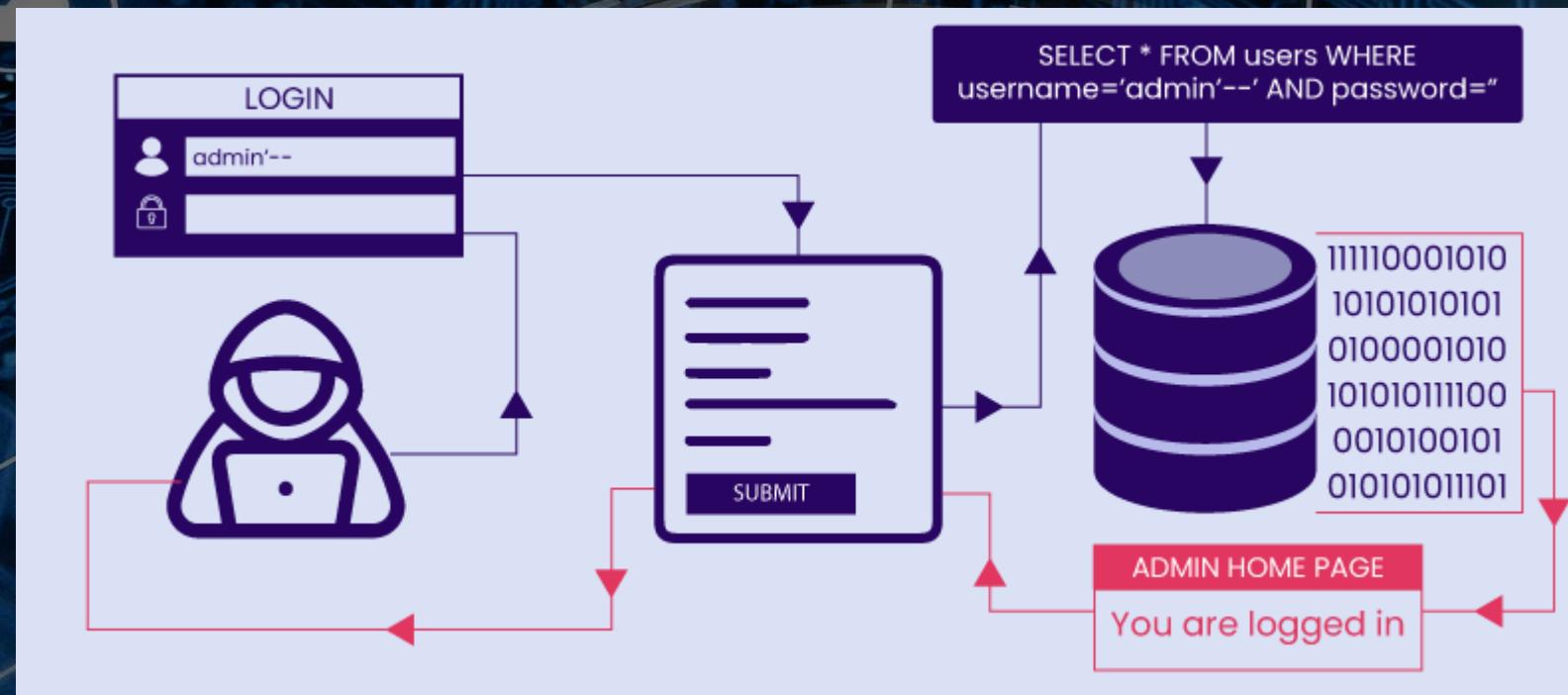
ID	Username	Password
1	Alice	password
2	Bob	qwerty

**Database Table:**  
**Users**

ID	Username	Password Hash
1	Alice	5f4dcc3b5aa765d61d8327deb882cf99 <sub>(md5)</sub>
2	Bob	b1b3773a05c0ed0176787a4f1574ff0075f7521e <sub>(sha1)</sub>

# Third Bug Injection

OWASP Top 10



## Impact:

- Data leakage and modification
- Unauthorized system access
- Potential complete server takeover

## Third Bug Injection

OWASP Top 10

Code and Input:

```
SELECT * FROM users WHERE  
username='$user' AND password='$pass'
```

*Our input:* admin'--

Output:

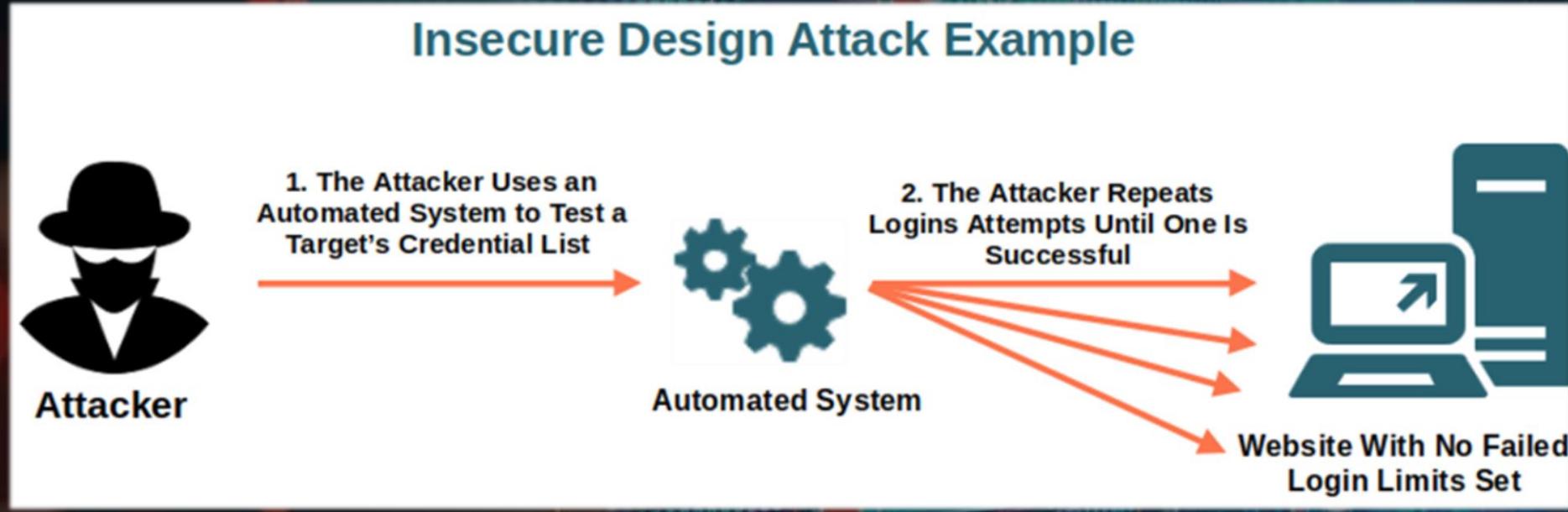
```
SELECT * FROM users WHERE  
username='admin'--' AND password=""
```

**Hacker Login as Admin User**

# Forth Bug

# Insecure Design

OWASP Top 10



## Impact:

- Inherent security weaknesses in architecture
- Hard-to-fix post-deployment vulnerabilities

# Forth Bug

## Insecure Design

OWASP Top 10

Simple Login form:

Log in

Username

Password

Log in

Remember me      [Forgot Password?](#)

[Create an Account](#)

Username and Password Input

Bruteforce or Spray:  
'admin' & '12345678'  
'admin' & '11111111'  
'admin' & 'PassW0rd'

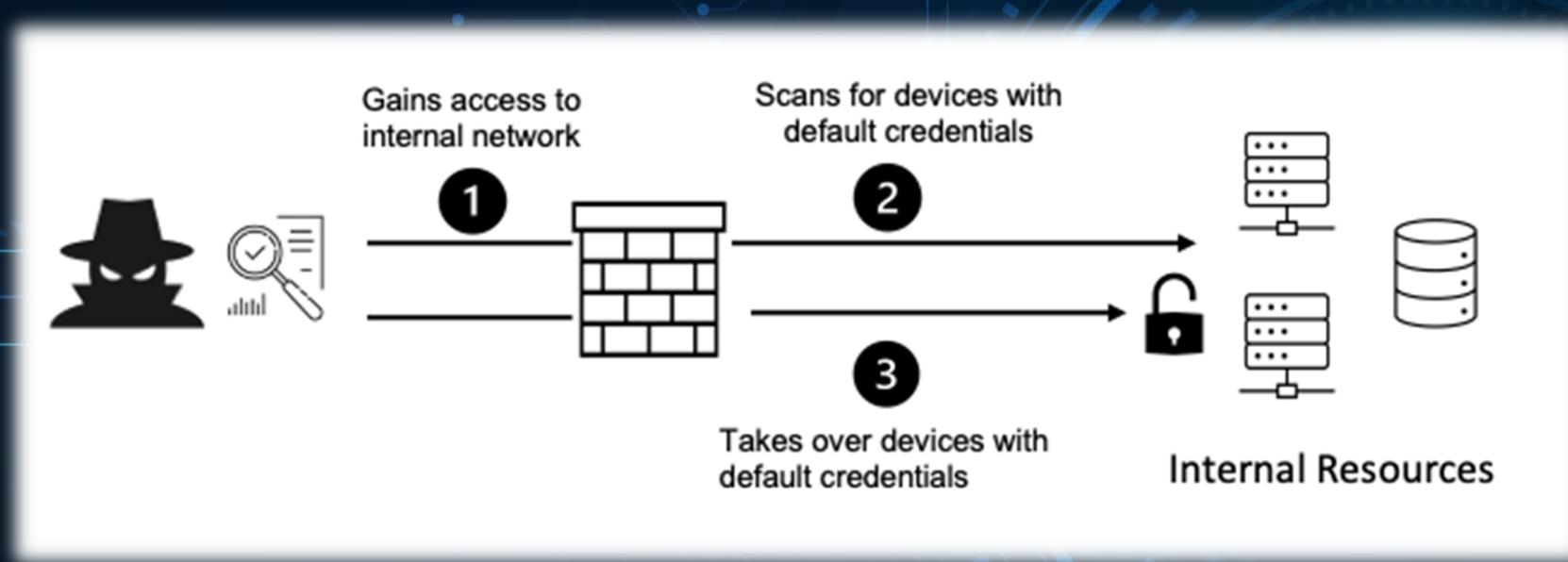
⋮  
⋮  
⋮  
⋮  
⋮

**'admin' & 'P@ssw0rd'**  
**Finally admin account takeover!**

# Fifth Bug

# Security Misconfiguration

OWASP Top 10



## Impact:

- Exposure of sensitive data
- Unauthorized access to systems
- Easy exploitation by hackers

Fifth Bug

# Security Misconfiguration

OWASP Top 10

server Login form:

**Server Login**

Username

Password

Log in

Remember me      [Forgot Password?](#)

Username and Password Input  
to go to the system panel

Try default username and password:  
'admin' & 'admin'  
'Administrator' & '12345678'

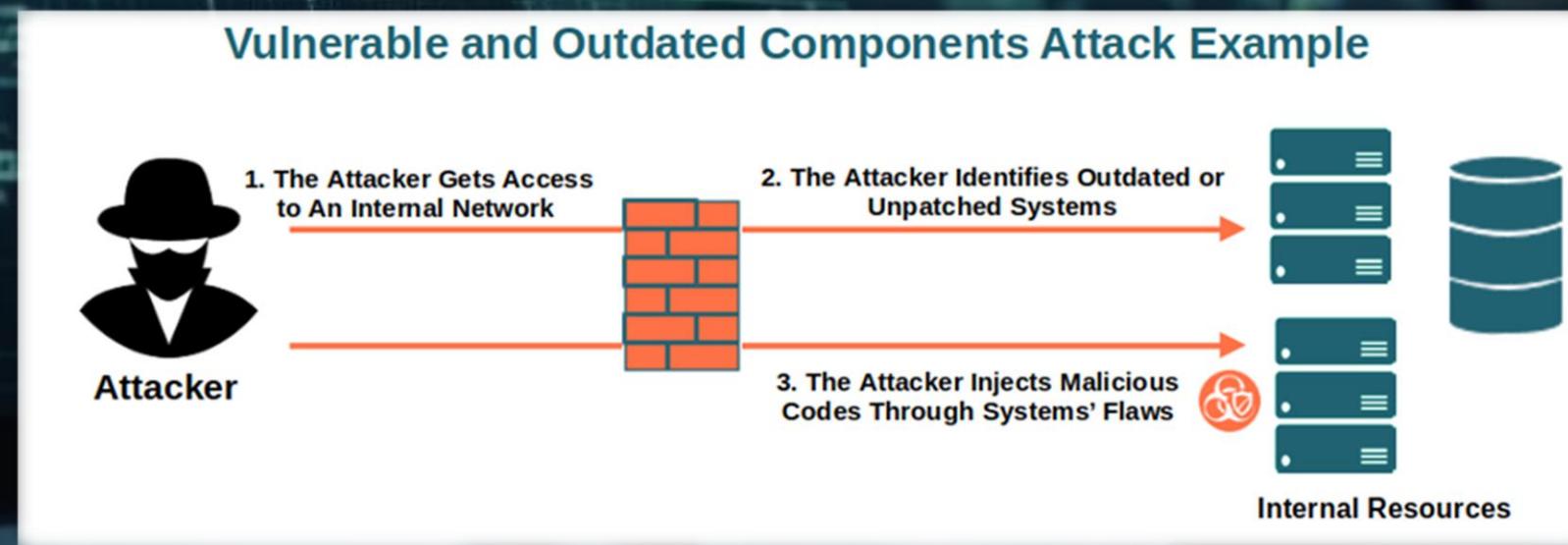


'test' & 'test'  
Finally system account takeover!

# Sixth Bug

## Vulnerable & Outdated Components

OWASP Top 10



### Impact:

- Exploitation of known vulnerabilities
- System compromise via third-party components

## Sixth Bug

# Vulnerable & Outdated Components

OWASP Top 10

website uses an old version  
of a WordPress plugin!



Attackers find a **known vulnerability**  
(like an **SQL injection** or **Remote Code  
Execution**) in the outdated plugin.

website uses an vulnerable  
version of a library!

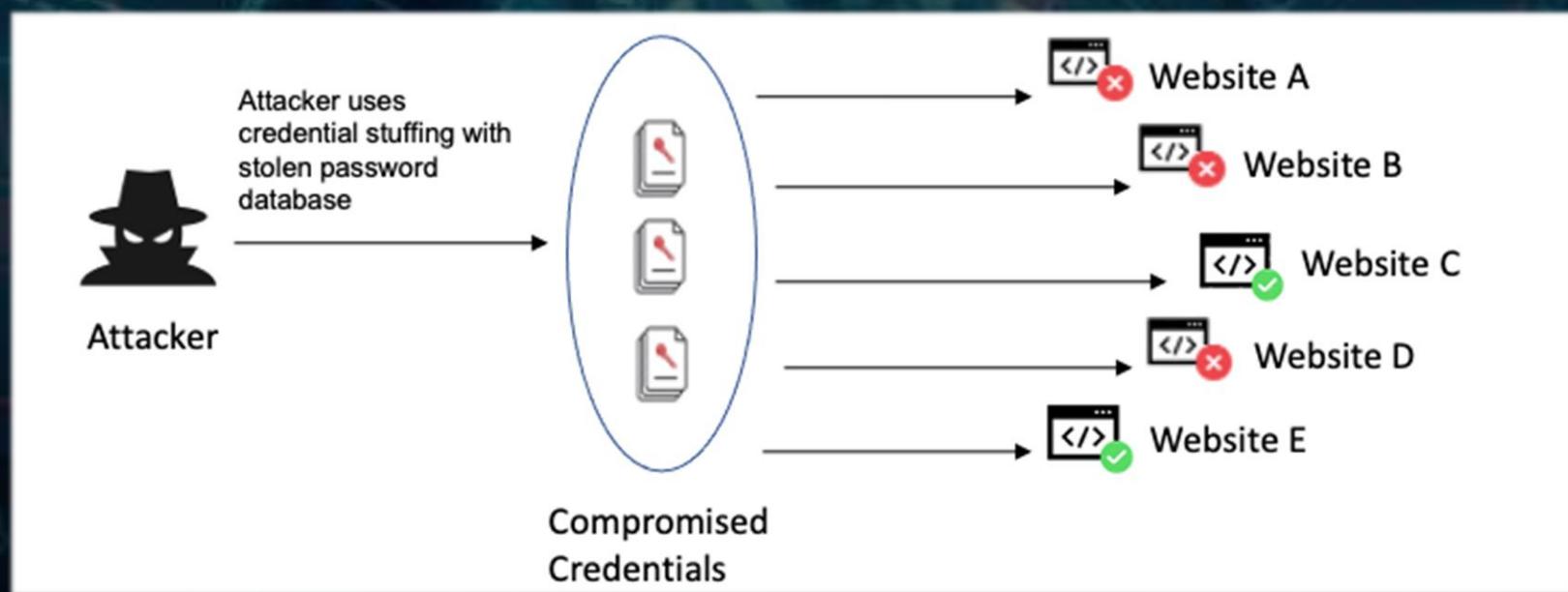


Attackers find a **known CVE** and use that  
to attack the vulnerable part of code.

# Seventh Bug

## Identification and Authentication Failures

OWASP Top 10



### Impact:

- Account takeovers
- Unauthorized access

## Seventh Bug

# Identification and Authentication Failures

OWASP Top 10

Use another email for  
forgot password!

[https://example.tld/logout?user=\\*\\*\\*](https://example.tld/logout?user=***)  
Logout from the account with an  
username.

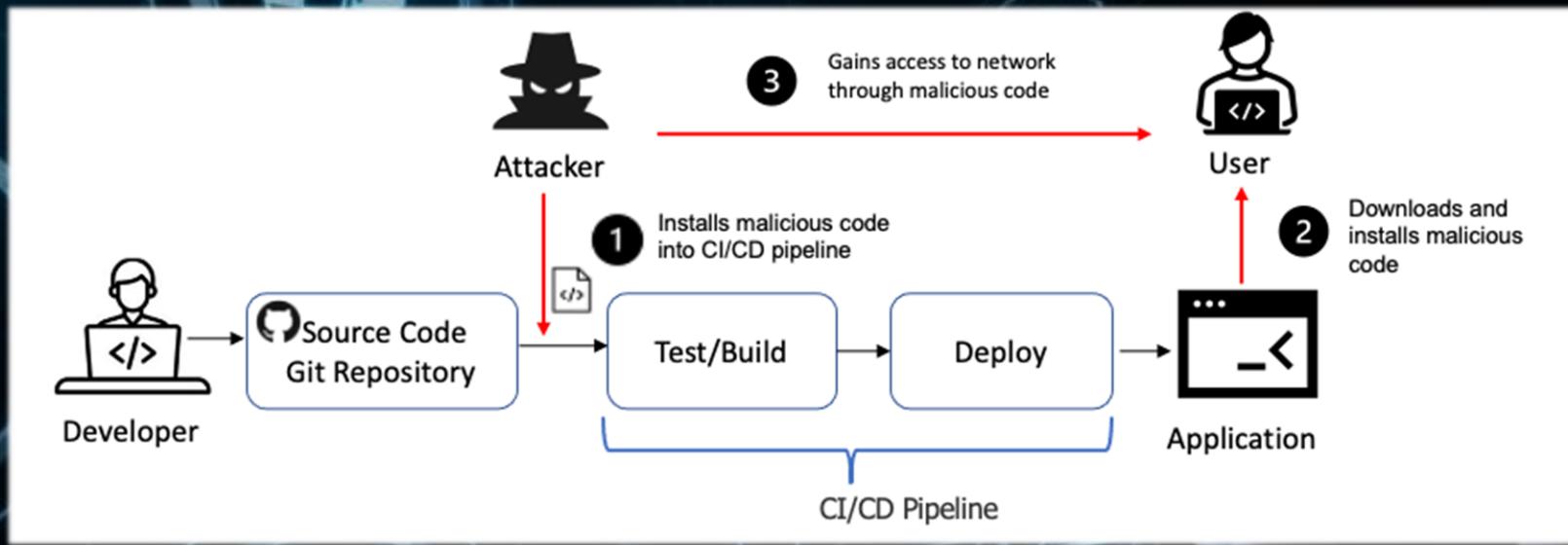
Hacker can send himself  
all usernames forgot  
password massage!

Hacker can logouts the  
users account!

# eighth Bug

## Software and Data Integrity Failures

OWASP Top 10



### Impact:

- Supply chain attacks
- Tampering with software updates

eighth Bug

## Software and Data Integrity Failures

OWASP Top 10

app downloads updates from an  
insecure HTTP link instead of HTTPS.

An **attacker** on the same network  
intercepts the connection and injects  
malicious code into the update.

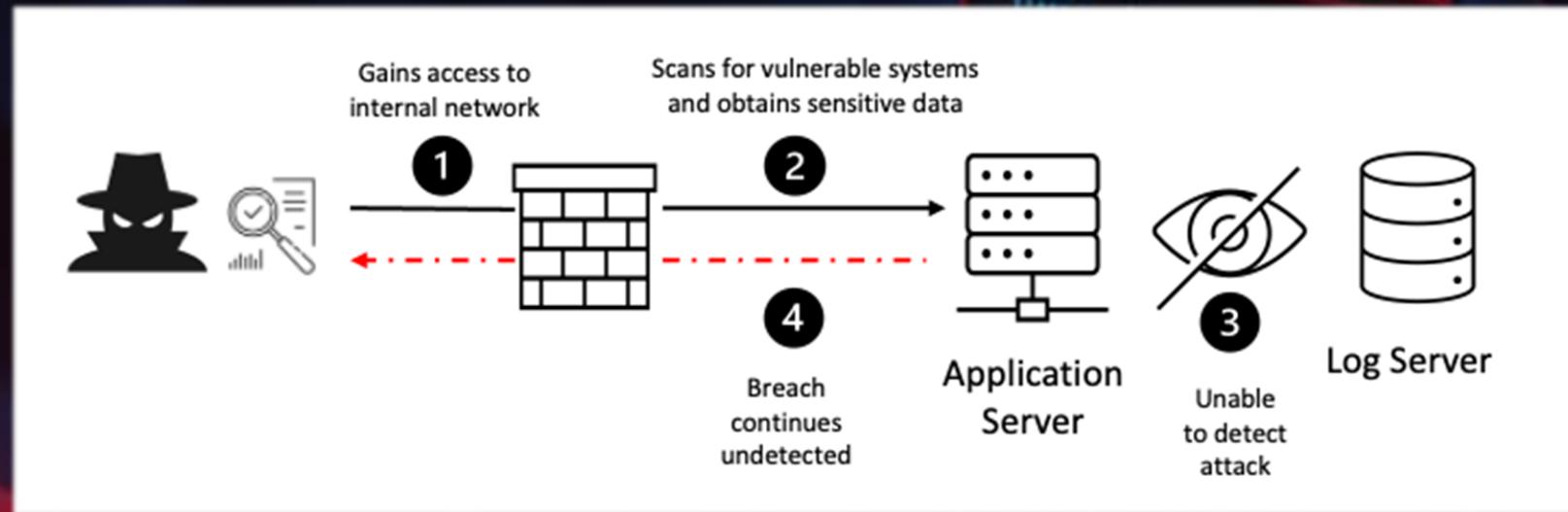
A web application stores user  
preferences in a serialized object.

An **attacker** modifies the  
serialized data to execute remote  
code or escalate privileges.

## ninth Bug

# Security Logging and Monitoring Failures

OWASP Top 10



## Impact:

- Delayed incident response
- Undetected data breaches

ninth Bug

## Security Logging and Monitoring Failures

OWASP Top 10

The site doesn't log the failed login attempts.

Web application doesn't log the malicious actions.

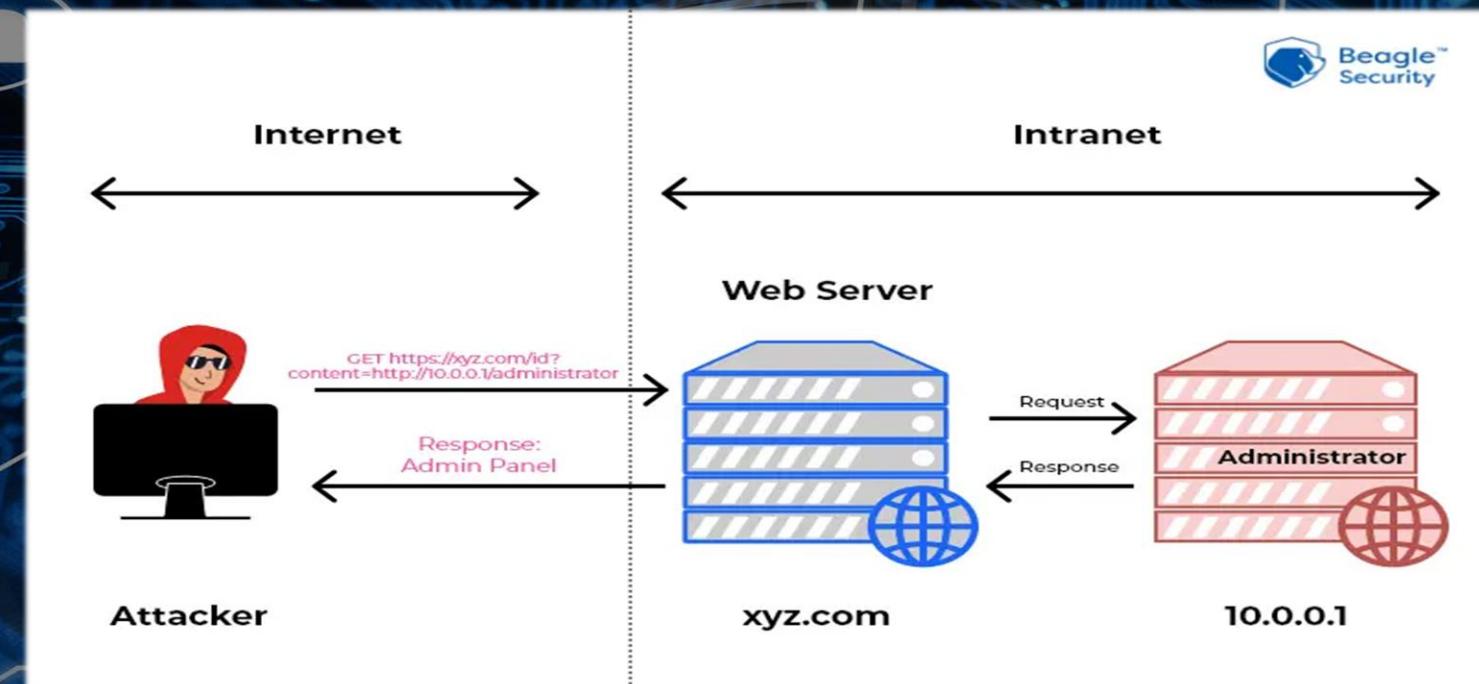
**attacker** if doing a bruteforce the Security team wont be noticed.

An **attacker** extracts and breach the data with no limits! (time, firewall, and etc.)

tenth Bug

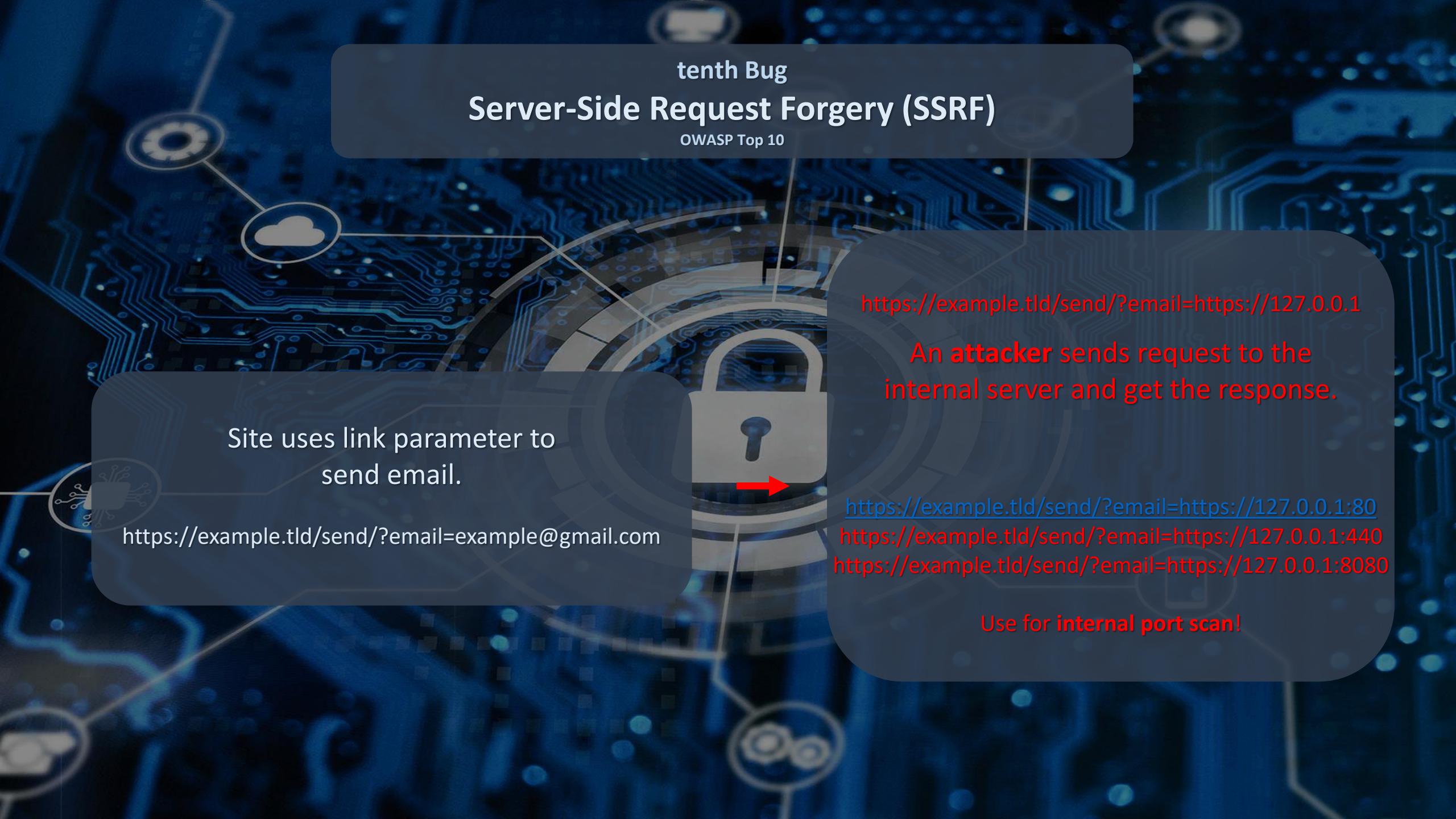
# Server-Side Request Forgery (SSRF)

OWASP Top 10



## Impact:

- Unauthorized access to internal systems
- Data exfiltration



# tenth Bug

## Server-Side Request Forgery (SSRF)

OWASP Top 10

Site uses link parameter to send email.

<https://example.tld/send/?email=example@gmail.com>

<https://example.tld/send/?email=https://127.0.0.1>

An **attacker** sends request to the internal server and get the response.

<https://example.tld/send/?email=https://127.0.0.1:80>

<https://example.tld/send/?email=https://127.0.0.1:440>

<https://example.tld/send/?email=https://127.0.0.1:8080>

Use for **internal port scan!**

بخش دوم

## نکات مهم امنیتی در ساخت وب اپلیکیشن



Web Application  
Security

# نکات مهم امنیتی در ساخت وب اپلیکیشن

1. Implement Strong Authentication & Authorization  
احراز هویت و مجوز

2. Protect Against Injection Attacks  
تزریق های مخرب

3. Secure Data with Proper Encryption  
امن سازی داده با رمزگاری خوب

4. Prevent Security Misconfigurations  
دوری از تنظیمات غلط امنیتی

5. Implement Secure Session Management  
پیاده سازی امن نشست کاربران

6. Protect APIs & Third-Party Integrations  
محافظت از بخش های لبه ای و جدا از سازمان

7. Monitor & Log Security Events  
مانیتور کردن و نگاشت لاگ فعالیت های امنیتی

8. Keep Dependencies and Software Updated  
نگهداری از بسته های الحقی و آپدیت نرم افزار ها

9. Protect Against Common Web Vulnerabilities  
محافظت در برابر آسیب پذیری های رایج

10. Secure Cloud & Deployment Configurations  
فضای ابری امن و تنظیمات پیاده سازی

## نکات مهم امنیتی در ساخت وب اپلیکیشن

### بخش اول

#### 1. Implement Strong Authentication & Authorization

احراز هویت و مجوز

##### 1. Use Multi-Factor Authentication (MFA)

احراز هویت چند عاملی

##### 2. Enforce Strong Password Policies

رمز گذاری قوی

##### 3. Use Role-Based Access Control (RBAC)

سطح دسترسی مبتنی بر نقش

##### 4. Avoid Hardcoded Credentials

جایگذاری دیتای معتبر

#### 2. Protect Against Injection Attacks

تزریق های مخرب

##### 1. Use Parameterized Queries & Prepared Statements

استفاده از پارامتر و گزاره های از قبل آماده

##### 2. Escape and Sanitize User Input

اعتبار سنجی ورودی کاربر

##### 3. Disable Direct Execution of User Input

جلوگیری از اجرای مستقیم ورودی کاربر

## نکات مهم امنیتی در ساخت وب اپلیکیشن

بخش دوم

### 3. Secure Data with Proper Encryption

امن سازی داده با رمزگاری خوب

### 1. Use HTTPS Everywhere

استفاده از https

### 2. Hash & Salt Passwords

هش و رمز کردن پسورد ها

### 3. Encrypt Sensitive Data at Rest & In Transit

رمزگاری داده های در حال انتقال

### 4. Prevent Security Misconfigurations

دوری از تنظیمات غلط امنیتی

### 1. Disable Debug Mode in Production

از کار آنداختن بخش های دیباگ

### 2. Use Secure Headers

پکت هدر های امن

### 3. Restrict Error Messages

جلوگیری از پیام خطای

## نکات مهم امنیتی در ساخت وب اپلیکیشن

بخش سوم

### 5. Implement Secure Session Management

پیاده سازی امن نشست کاربران

### 6. Protect APIs & Third-Party Integrations

محافظت از بخش های لبه‌ای و جدا از سازمان

#### 1. Use Secure & HttpOnly Cookies

استفاده از کوکی های امن

#### 2. Set Proper Session Expiry

تنظیم درست زمان از بین رفتن نشست

#### 3. Regenerate Session IDs

ساخت دوباره نشست در هر تغییر

#### 1. Use API Rate Limiting & Throttling

محدودیت نرخ ورودی ای پی آی

#### 2. Validate API Inputs

اعتبار سنجی ورودی های ای پی آی

#### 3. Use API Keys, OAuth, or JWTs

استفاده از کلید ها، احراز هویت یا jwt



## نکات مهم امنیتی در ساخت وب اپلیکیشن

### بخش چهارم

#### 7. Monitor & Log Security Events

مانیتور کردن و نگاشت لاغ فعالیت های امنیتی

#### 1. Implement Logging & Monitoring

مانیتور کردن و ثبت لاغ ها

#### 2. Enable Intrusion Detection Systems (IDS)

فعال سازی سیستم های تشخیص نفوذ

#### 3. Audit Logs Regularly

گزارش منظم لاغ ها

#### 8. Keep Dependencies and Software Updated

نگهداری از بسته های الحاقی و آپدیت نرم افزار ها

#### 1. Update Third-Party Libraries & Frameworks

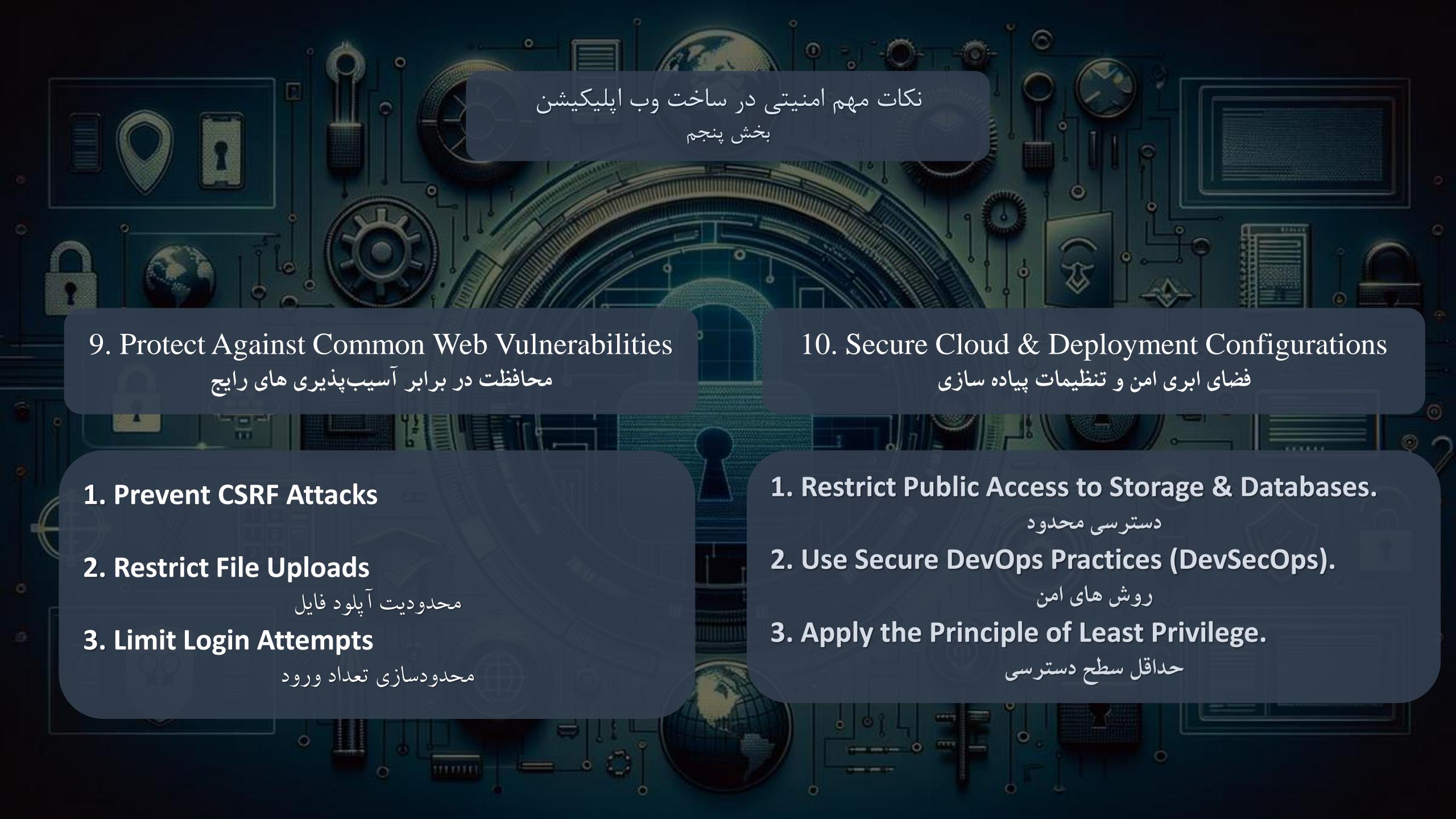
آپدیت کتابخانه ها و فریمورک ها

#### 2. Use Dependency Scanning Tools

استفاده از ابزار های اسکن وابستگی

#### 3. Remove Unused Features & Plugins

از بین بردن بخش های بی استفاده



## نکات مهم امنیتی در ساخت وب اپلیکیشن

### بخش پنجم

#### 9. Protect Against Common Web Vulnerabilities

##### محافظت در برابر آسیب‌پذیری‌های رایج

#### 10. Secure Cloud & Deployment Configurations

##### فضای ابری امن و تنظیمات پیاده‌سازی

#### 1. Prevent CSRF Attacks

#### 2. Restrict File Uploads

محدودیت آپلود فایل

#### 3. Limit Login Attempts

محدودسازی تعداد ورود

#### 1. Restrict Public Access to Storage & Databases.

دسترسی محدود

#### 2. Use Secure DevOps Practices (DevSecOps).

روش‌های امن

#### 3. Apply the Principle of Least Privilege.

حداقل سطح دسترسی

### بخش سوم

## خطرات امنیتی قابل توجه برای برنامه نویسان وب



## 1. Injection Attacks: (SQLi, XSS, Command Injection, etc.)

Unvalidated user input

## 2. Broken Authentication & Session Management

steal credentials, hijack sessions, or bypass login protections

## 3. Broken Access Control

gain access to restricted data or admin functionalities

## 4. Cryptographic Failures (Data Exposure)

Storing passwords in plain text or using weak encryption

## 5. Security Misconfigurations

Default settings, exposed error messages, open ports, and unnecessary features

## 6. Using Vulnerable & Outdated Components

### 7. Cross-Site Scripting (XSS)

inject malicious JavaScript into web pages, stealing user data or executing unauthorized actions.

## 8. Insecure APIs

data leaks and unauthorized access

## 9. Server-Side Request Forgery (SSRF)

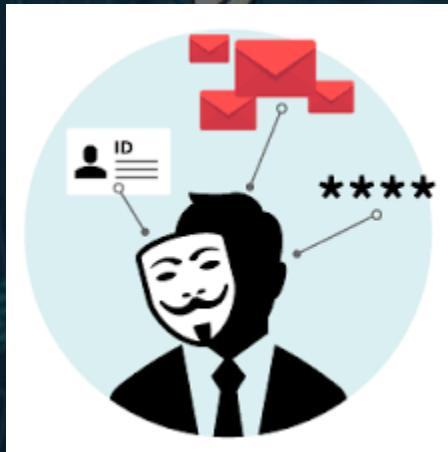
Make web application to request to internal services, exposing sensitive data.

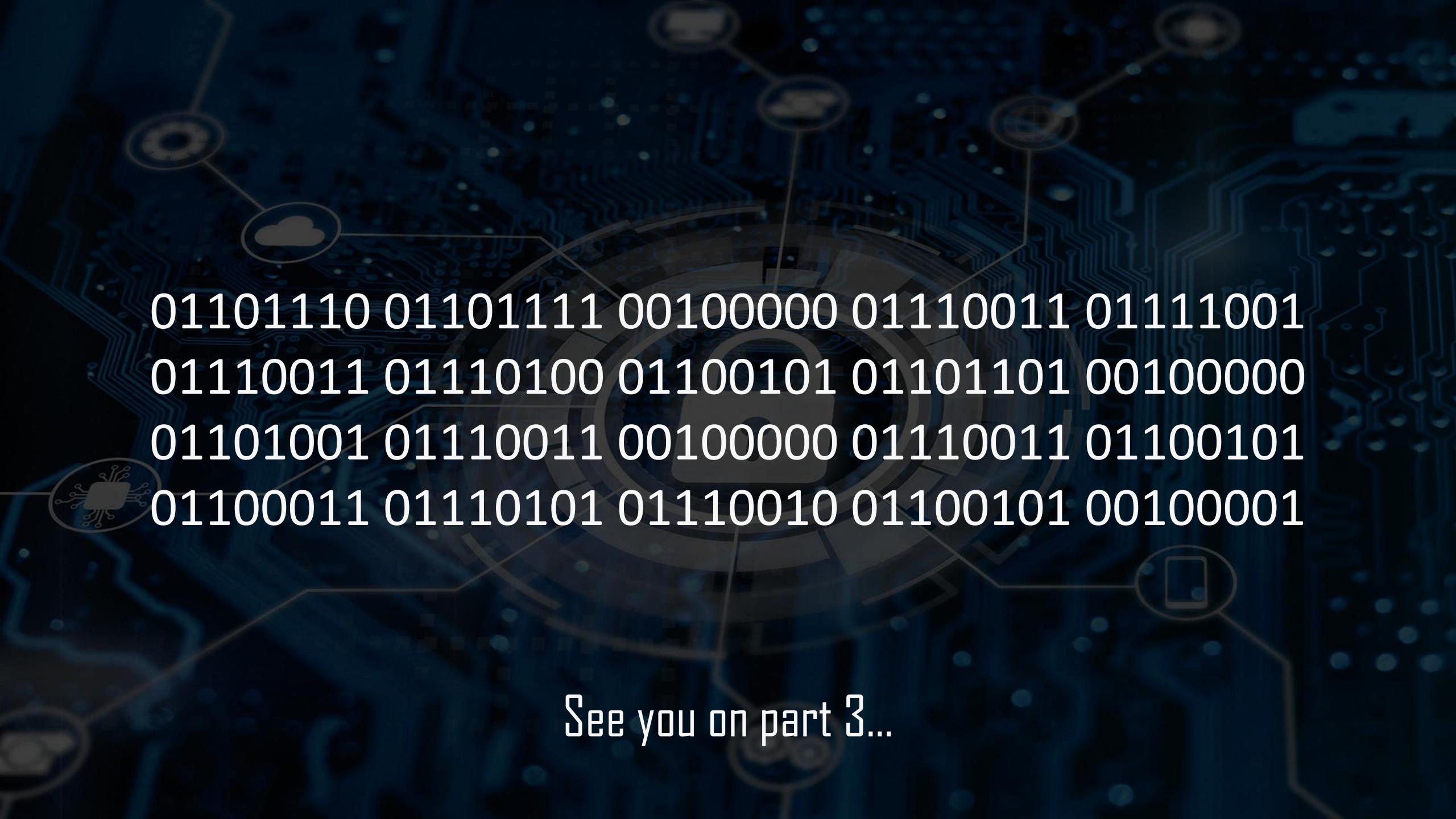
## 10. Insufficient Logging & Monitoring

Attackers can operate unnoticed

خطرات امنیتی قابل توجه برای برنامه نویسان وب

# Cyber Security





01101110 01101111 00100000 0110011 01111001  
01110011 01110100 01100101 01101101 00100000  
01101001 01110011 00100000 01110011 01100101  
01100011 01110101 01110010 01100101 00100001

See you on part 3...