DAVID GROUP CYBERSECURITY COMPLIANCE STANDARDS

Safeguard the Systems, Data and Sensitive Information

2024

DavidGroup®

DIREKTORAT JENDERAL
KEKAYAAN INTELEKTUAL
KEMENTERIAN HUKUM & HAM R.I.

davidgroup.co.id

1. FOREWORD

DAVID GROUP Cybersecurity Compliance Standards is Compliance Standards that have been prepared to provide a set of guidelines and requirements to ensure that organizations implement effective cybersecurity measures to protect their systems, data, and sensitive information. These Compliance Standards encompass a comprehensive approach to information security, covering a wide spectrum of cybersecurity domains. From data protection and access controls to threat detection and incident response, these standards address various crucial aspects of safeguarding digital assets.

The requirements outlined in these Compliance Standards are general and intended to be applicable to all types of organizations, regardless of their type, size, or nature. The standards are designed to be applied with flexibility to ensure seamless integration with existing operations. By providing a strong framework, these Compliance Standards assist organizations in achieving and maintaining compliance with relevant cybersecurity regulations, industry best practices, and international standards.

This Cybersecurity Compliance Standards is evidence of DAVID GROUP's commitment to providing the services and solutions needed by organizations to navigate the complex cybersecurity landscape. By implementing these standards, it not only enhances the cybersecurity posture of organizations but also contributes to collective efforts to strengthen the digital world against threats.

- **Security Testing Table**

No.	SECURITY TESTING
1	Database Injection
2	Cross Site Scripting (XSS)
3	Server-side Request Forgery (SSRF)
4	XML External Entity (XXE)
5	Insecure Direct Object Reference (IDOR)
6	Local File Inclusion (LFI)
7	Remote File Inclusion (RFI)
8	Misconfiguration Detection
9	Data Breach Protection
10	Privilege Escalation
11	Cross-site Request Forgery (CSRF)
12	Server-side Remote Code Execution (RCE)
13	Server-side Template Injection (SSTI)
14	Local File Disclosure (LFD)
15	Session and User Hijacking Protection
16	TLS Pinning
17	Clickjacking Protection
18	Brute Force Protection
19	Bad Bot Scrapper
20	0-day Exploits

2. X-DAVIDGROUP-GUARD

DAVID GROUP proudly announces the latest addition to its lineup of cybersecurity solutions name: X-DAVIDGROUP-GUARD. In a commitment to providing the best protection for digital assets, X-DAVIDGROUP-GUARD is a specially formulated product designed to enhance the security of servers and web applications.

In today's rapidly evolving digital landscape, the need for robust cybersecurity measures has become more critical than ever before. Cyber threats in the online world are growing increasingly sophisticated, targeting vulnerabilities in servers and web applications to gain unauthorized access, steal sensitive data, and disrupt online services. X-DAVIDGROUP-GUARD has been developed with these challenges in mind, offering a comprehensive and proactive approach to safeguarding online assets.

- **Specially designed to work on multi-platform programming languages:**

Language	Java
	JSF/EL (JavaServer Faces)
	PHP (Hypertext Preprocessor)
	ASP (Active Server Pages .NET)
	Perl
	Python

- **X-DAVIDGROUP-GUARD works well with multiple web servers:**

Session Cookie	LiteSpeed Enterprise/OpenLiteSpeed
	Apache
	Nginx
	Apache Tomcat
	IIS (Internet Information Services)
	Lighttpd
	Oracle HTTP Server
	Domain/Sub

X-DAVIDGROUP-GUARD has several values that are functional according to the needs and the level of security standardization that you want to implement. Some of the values of X-DAVIDGROUP-GUARD are: Pinning, Intermittent, David Group Trusted Seal, and Enforce.

In general, X-DAVIDGROUP-GUARD takes full responsibility for the sectors that will be explained next.

2.1 Session Cookie

It is a type of attack when an unauthorized person intercepts and takes over an active session between a user and an application/website. During a regular online session, such as logging into an account or accessing a secure website, the server creates a session to maintain the user's status and identity.

Session Cookie	Partitioned
	Prefix
	Secure
	HttpOnly
	SameSite
	Max-Age
	Path
	Domain/Sub

2.2 Source Pinning

Source Pinning is a security mechanism designed to enhance the security of web applications and prevent certain types of attacks, such as Man-in-the-Middle (MitM) attacks. It involves associating specific cryptographic identities with resources or web applications, ensuring that only resources from trusted sources are loaded and executed by the user's browser.

Source Pinning	JS (JavaScript)
	CSS (Cascading Style Sheets)
	Images
	Documents

2.3 SQL Injection

SQL Injection is a type of security vulnerability that occurs when a web application or database fails to properly validate user-provided input before incorporating it into an SQL statement. SQL Injection attacks allow attackers to inject or manipulate SQL statements executed by the database, potentially leading to unauthorized access, disclosure of sensitive data, or even data destruction.

SQL Injection (MySQL, Oracle, Microsoft SQL Server, PostgreSQL, SQLite, Sybase, MongoDB)	Boolean-Based Blind
	Error-Based
	Union Query-Based
	Stacked Queries
	Time-Based Blind
	Inline Queries

2.4 XML External Entity (XXE) Injection

XML External Entity Injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with the processing of XML data in an application. This type of attack often enables the attacker to view files on the application server's file system and interact with any backend or external system accessible by the application itself.

XML External Entity (XXE) Injection	XXE Attacks Via File Upload
	XInclude Attacks
	XXE Attacks Via Modified Content Type

2.5 Privilege Escalation

Privilege Escalation is a cyberattack aimed at gaining unauthorized access to rights, permissions, ownership, or other privileges beyond what is assigned to an identity, account, user, or machine. This attack can involve threat actors from external or internal sources. Privilege Escalation consists of two types: Horizontal Privilege Escalation and Vertical Privilege Escalation.

Privilege Escalation	Horizontal Privilege Escalation
	Vertical Privilege Escalation

2.6 Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attack is a type of injection where malicious scripts are injected into a harmless and trusted website.

Cross Site Scripting (XSS)	Reflected XSS
	Stored (Persistent) XSS
	DOM (Document Object Model) XSS
	Self XSS Chain

2.7 Server-Side Request Forgery (SSRF)

Server-Side Request Forgery (SSRF) attacks involve an attacker exploiting server functionality to access or modify resources. Attackers target applications that support importing data from URLs or allow them to read data from URLs. URLs can be manipulated, either by replacing them with new ones or by tampering with the URL path traversal.

2.8 Remote Code Execution (RCE)

Remote Code Execution (RCE) is a vulnerability that allows an attacker to execute arbitrary code in the programming language in which the developer wrote the application. The term "remote" means that the attacker can do this from a location different from the system running the application. Remote code execution is also known as code injection and remote code evaluation.

2.9 Local File Inclusion (LFI)

Appears when an application uses data that a user can control to access files and directories on an application server or other back-end file system in an unsafe manner. By sending specially crafted input, an attacker can cause arbitrary content to be read from or written to anywhere in the file system. This often allows attackers to read sensitive information from the server, or overwrite sensitive files, which can ultimately result in command execution on the server.

2.10 Remote File Inclusion (RFI)

Remote File Inclusion (RFI) is an attack that targets vulnerabilities in web applications that dynamically reference external scripts. The attacker's goal is to exploit the referencing function within the application to upload malicious software (e.g., backdoor shells) from a remote URL located in a different domain. Consequences of a successful RFI attack include information theft, compromised servers, and website takeover that allows content modification.

2.11 Insecure Direct Object References (IDOR)

Insecure Direct Object References (IDOR) is a type of security vulnerability that occurs when an application allows unauthorized access to resources or data by not properly validating and controlling user input. This vulnerability can arise when an application references objects such as files, database records, or URLs without proper checks, allowing attackers to manipulate input and access resources they should not be authorized to access.

2.12 Bad Bots

An example of this is when a bot crawler indexes a page on a website containing someone's sensitive data. Bad Bot Scrapers are very dangerous because attackers do not need authentication to access this data (indexed by search engines).

Bad Bots	Automated Scanner
	Unwanted Search Engine Indexing
	Spoof Agents

2.13 Default Configuration/Misconfiguration

Configuration errors occur when security options are not specified in a maximal way, or when services are deployed with insecure default settings. This can happen in any computer system, software applications, as well as cloud infrastructure and networks.

Default Configuration/Misconfiguration	Outdated 3rd Parties
	Vulnerable Template Framework
	Trivial/Obvius Configurations
	Outdated Version

2.14 TLS Security

HTTP Strict Transport Security (HSTS) is a policy mechanism that helps protect websites from man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. It allows a web server to declare that web browsers should interact automatically using only HTTPS connections, providing Transport Layer Security (TLS/SSL).

The HSTS policy is communicated by the server to the user agent through an HTTP response header field called Strict-Transport-Security. The HSTS policy specifies a period of time during which the user should only access the server securely.

TLS Security	Invalid Chain Certificate (Incomplete)
	HTTP Strict Transport Security (HSTS/Preload)
	TLS 1.3/1.2/1.1/1.0 (compatibility)
	Redirection Mechanism

2.15 Brute-Forcing

A brute force attack is an attack that involves repeated, sequential attempts to try various password combinations in order to breach a website. Attackers do this by using bots they deploy on other computers to increase the computing power needed to execute such an attack.

Brute-Forcing	Filename Bruteforcing
	ID Value Bruteforcing
	User/pass Bruteforcing

2.16 Web Shell Exploitation

Web shell exploitation is a cybersecurity threat in which attackers upload or inject malicious scripts, often referred to as "web shells," into vulnerable web servers to gain unauthorized access and control over the server and its underlying systems. Web shells provide attackers with a remote interface to execute commands, manipulate files, and carry out various malicious activities within the compromised server.

Web Shell Exploitation	Web Shell via File Upload
	Web Shell via Command OS Injections
	Web Shell via SQL Injections

2.17 Distributed Denial of Services (DDoS)

A type of cyberattack in which multiple computers or devices that have been configured are used to overwhelm a target system, network, or website with a very large amount of traffic. This traffic flood exceeds the target system's capacity, causing it to become slow, unresponsive, or even damaged.

Distributed Denial of Services (DDoS)	Layer 3 DDoS (TCP/IP)
	Layer 7 DDoS (Application)

2.18 Insecure Infrastructures

Insecure Infrastructures	Vulnerable Hosting/Cloud Environment
	DNS Hijacking
	CNAME Manipulation
	IPv4/IPv6 open ports
	Multiple Host Listener

2.19 Deep Inspection

Deep Inspection	Monitoring dan Log Evaluation
	Code Inspection
	Suspicious Files/Sources
	Folder Permissions
	Security Policy

3. CONCLUSION

DAVID GROUP Cybersecurity Compliance Standards is aimed at promoting internationally standardized domestic innovations and supporting efforts to boost the use of domestic products (P3DN) and technological advancement. DAVID GROUP is committed to actively participating in and supporting the P3DN Program to enhance the competitiveness and productivity of the domestic industry. With the presence of these Compliance Standards, it helps meet regulatory requirements, reduce cyber risks, and establish a strong cybersecurity position.