G-PRIVACY 2023

2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

사이버공격의 주요 원인, SW보안취약점에 대한 근본 해결책 제시

(주)하로스

사이버 공격의 주요 원인

01
취약한 시스템 및 소프트웨어

02
인적 요인

03
미흡한 보안 정책 및 절차

04
공격 기술의 발전

05
내부 위협

취약한 애플리케이션

01 NTT Application Security 에서 테스트한 2021년 전체 사이트의 50%가 하나 이상의 심각한 취약성을 갖고 있음 (NTT Application Security Report)

02 18,000 건의 보안 사고 중 60% 이상이 웹어플리케이션의 취약점과 관련있음. (Verizon's 2022 Data Breach Investigations report)

03 2020년에 3700만 개 이상의 레코드가 도난당했으며 웹 애플리케이션이 침해의 39%를 차지

애플리케이션 보안 취약점 공격이 많은 이유

인터넷에 연결된 많은 웹 어플리케이션

웹 어플리케이션의 복잡성

웹 어플리케이션의 업데이트 미비

미처리된 입력 값 검증

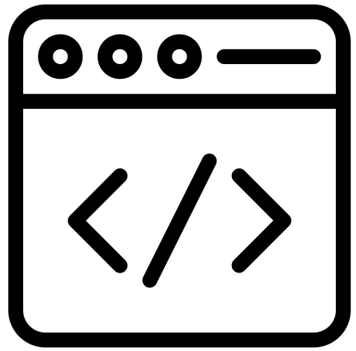
인증 및 권한 부여의 미비

애플리케이션 취약점 보완 방안

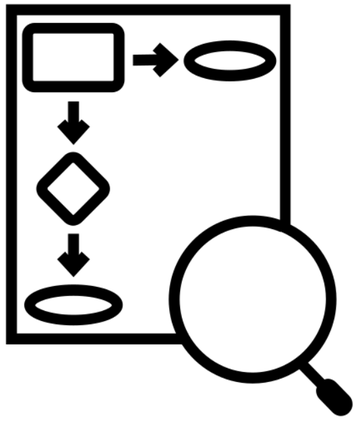
- 취약점 평가 및 분석
- 패치 및 업데이트
- 시큐어 코딩 적용
- 보안 개발 생명 주기(SSDLC) 도입
- 인증 및 권한 관리 강화
- 로깅 및 모니터링
- 사용자 교육 및 인식

정적 분석 도구

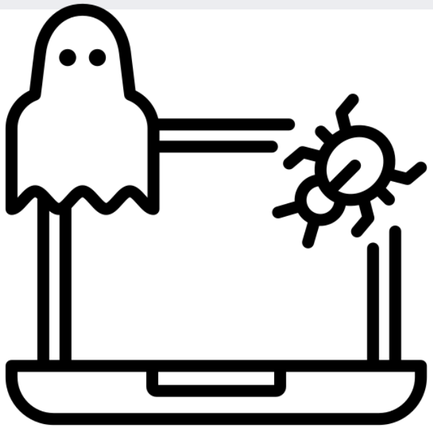
01 코드 분석



02 데이터 흐름 분석



03 취약점 검사

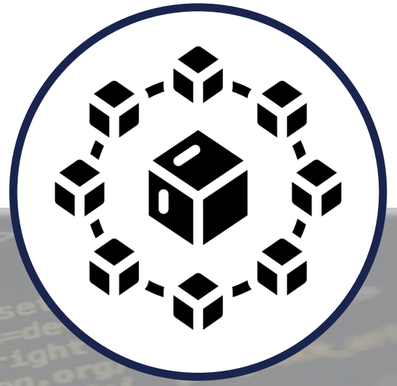


04 보고서 작성

개발 방법의 변화

스프링
프레임워크

스프링부트



마이크로서비스
아키텍처

Restful
API

클라우드 기반
개발

프레임워크와 정적분석도구

01 프레임워크 활용으로 쉽고 빠르게 개발

02 프레임워크를 제대로 이해하지 못하고
사용하는 개발자 증가

03 정적분석도구는 프레임워크나 라이브러리의
취약점을 효과적으로 검출

정적분석도구에서의 Source와 Sink

Source

데이터가 **유입**되는 곳

Sink

데이터가 **유출**되는 곳

라이브러리와 정적분석 도구

Source

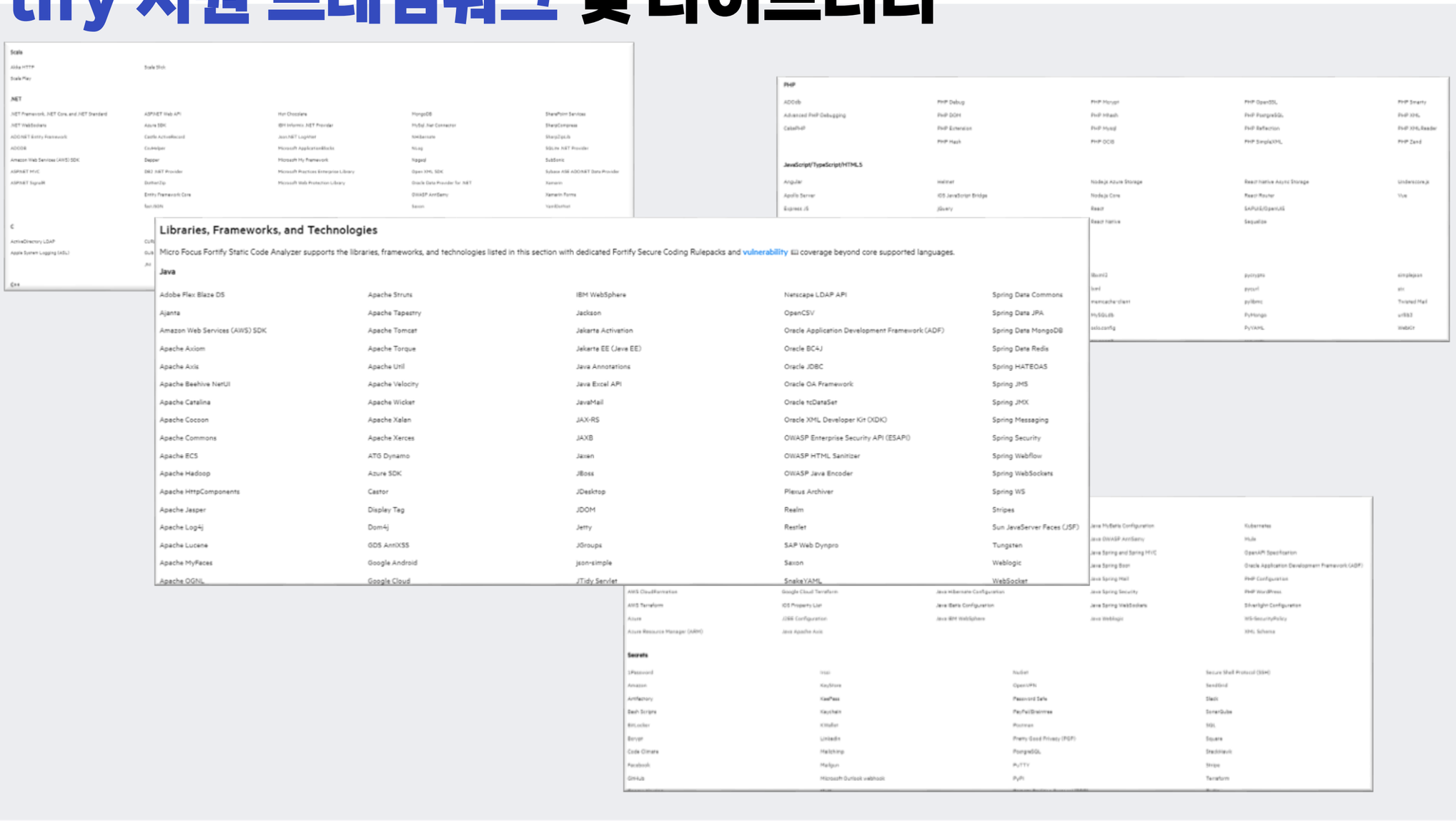
라이브러리의 **입력값**

Sink

라이브러리의 **출력값**

정적분석도구에서는
라이브러리의 **Source**와 **Sink** 정보를 제공해야 함.

Fortify 지원 프레임워크 및 라이브러리



Scala

Akka HTTP
Scala Slick
Scala Play

.NET

.NET Framework, .NET Core, and .NET Standard
ADP.NET Web API
Hot Chocolate
MongoDB
SharePoint Services
.NET WebSockets
Azure SDK
IBM Informix .NET Provider
MySql.Net Connector
SharpCompress
ADO.NET Entity Framework
Castle ActiveRecord
Json.NET Loginter
NHibernate
SharpSpLib
ADODB
CsvHelper
Microsoft ApplicationBlocks
NLog
SQLite .NET Provider
Amazon Web Services (AWS) SDK
Dapper
Microsoft My Framework
Nlogid
SubSonic
ASP.NET MVC
DB2 .NET Provider
Microsoft Practices Enterprise Library
Open XML SDK
Sybase ASE ADO.NET Data Provider
ASP.NET SignalR
DotNetZip
Microsoft Web Protection Library
Oracle Data Provider for .NET
Xamarin
Entity Framework Core
OWASP AntiSamy
Xamarin Forms
fast JSON
Saxon
YamlDotNet

C

ActiveDirectory LDAP
CURL
Apple System Logging (ASL)
GLib
Jni

C++

PHP

ADOdb
PHP Debug
PHP Mongo
PHP OpenSSL
PHP Smarty
Advanced PHP Debugging
PHP DOM
PHP Mssql
PHP PostgreSQL
PHP XML
CakePHP
PHP Extension
PHP Mysql
PHP Reflection
PHP XMLReader
PHP Hack
PHP OCI8
PHP SimpleXML
PHP Zend

JavaScript/TypeScript/HTML5

Angular
Helmet
Nodejs Azure Storage
React Native Async Storage
Underscore.js
Apollo Server
IOS JavaScript Bridge
Nodejs Core
React Router
Vue
Express JS
JQuery
React
SAPUI5/OpenUI5
React Native
Sequelize

libxml2
pycrypto
simplejson
lxml
pycurl
stc
memcache client
pylibmc
Twisted Mail
MySQLdb
PyMongo
urllib3
psloconfig
PyYAML
WebStr

Libraries, Frameworks, and Technologies

Micro Focus Fortify Static Code Analyzer supports the libraries, frameworks, and technologies listed in this section with dedicated Fortify Secure Coding Rulepacks and vulnerability coverage beyond core supported languages.

Java

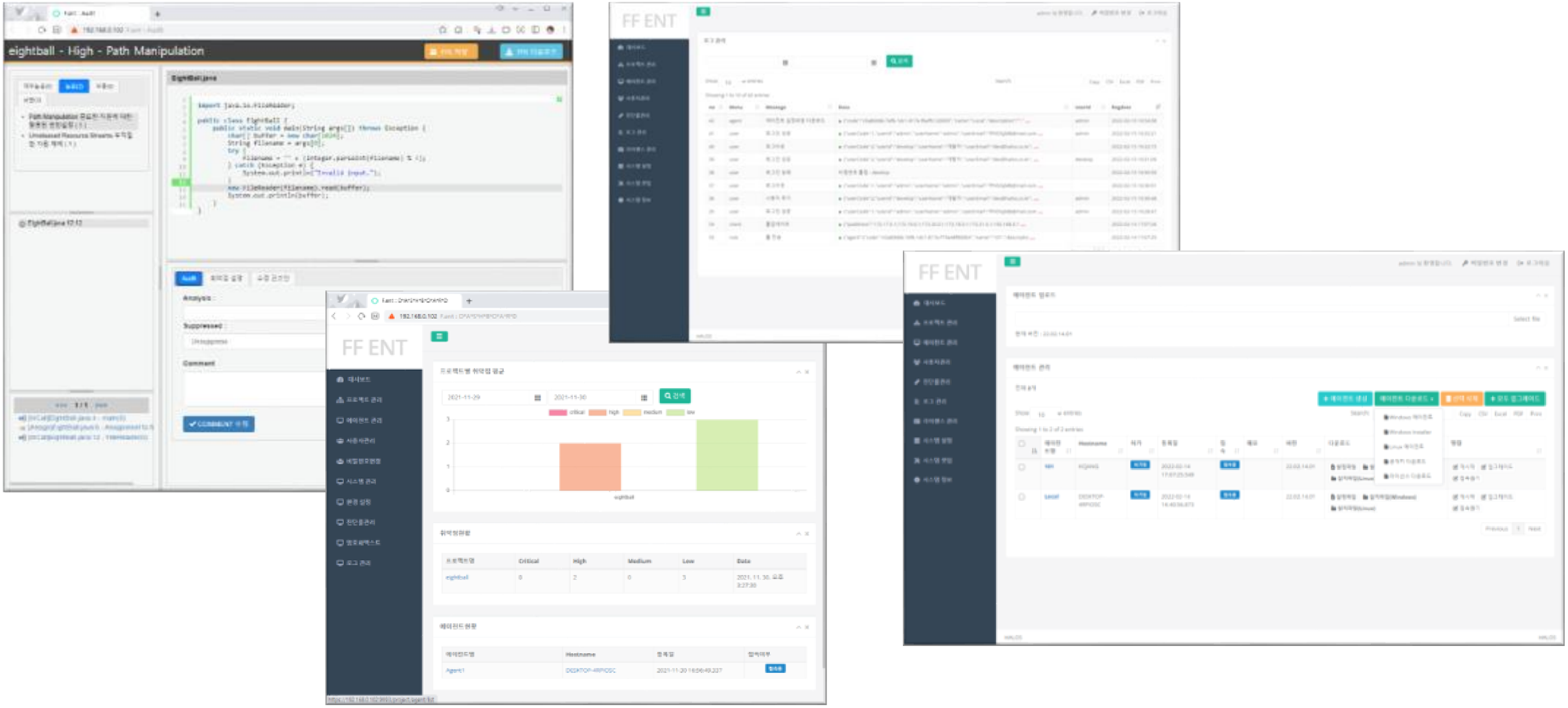
Adobe Flex Blaze DS	Apache Struts	IBM WebSphere	Netscape LDAP API	Spring Data Commons
Ajanta	Apache Tapestry	Jackson	OpenCSV	Spring Data JPA
Amazon Web Services (AWS) SDK	Apache Tomcat	Jakarta Activation	Oracle Application Development Framework (ADF)	Spring Data MongoDB
Apache Axiom	Apache Torque	Jakarta EE (Java EE)	Oracle BC4J	Spring Data Redis
Apache Axis	Apache Util	Java Annotations	Oracle JDBC	Spring HATEOAS
Apache Beehive NetUI	Apache Velocity	Java Excel API	Oracle OA Framework	Spring JMS
Apache Catalina	Apache Wicket	JavaMail	Oracle rcDataSet	Spring JMX
Apache Cocoon	Apache Xalan	JAX-RS	Oracle XML Developer Kit (XDK)	Spring Messaging
Apache Commons	Apache Xerces	JAXB	OWASP Enterprise Security API (ESAPI)	Spring Security
Apache EC5	ATG Dynamo	Jaxen	OWASP HTML Sanitizer	Spring Webflow
Apache Hadoop	Azure SDK	JBoss	OWASP Java Encoder	Spring WebSockets
Apache HttpComponents	Castor	JDesktop	Plexus Archiver	Spring WS
Apache Jasper	Display Tag	JDOM	Realm	Stripes
Apache Log4j	Dom4j	Jetty	Restlet	Sun JavaServer Faces (JSF)
Apache Lucene	GDS AntiXSS	JGroups	SAP Web Dynpro	Tungsten
Apache MyFaces	Google Android	json-simple	Saxon	Weblogic
Apache OGNL	Google Cloud	JTidy Servlet	SnakeYAML	WebSocket

AWS CloudFormation
Google Cloud Terraform
Java Hibernate Configuration
Java MyBatis Configuration
Kubernetes
AWS Terraform
IOS Property List
Java iBatis Configuration
Hyb
Azure
J2EE Configuration
Java IBM WebSphere
Java OWASP AntiSamy
OpenAPI Specification
Azure Resource Manager (ARM)
Java Apache Axis
Java Spring and Spring MVC
Oracle Application Development Framework (ADF)
Java Spring Boot
PHP Configuration
Java Spring Mail
PHP WordPress
Java Spring Security
Silverlight Configuration
Java Spring WebSockets
WS-SecurityPolicy
Java Weblogic
XML Schema

Secrets

1Password
Hiki
Nuget
Secure Shell Protocol (SSH)
Amazon
KeyStore
OpenVPN
SendGrid
Artifactory
KeePass
Password Safe
Slack
Bash Scripts
Keychain
PayPal/Braintree
SonarQube
BitLocker
Kitsafer
Postman
SQL
Bevyr
LinkedIn
Pretty Good Privacy (PGP)
Square
Code Climate
Mailchimp
PostgreSQL
StackHawk
Facebook
Mailgun
PuTTY
Stripe
GitHub
Microsoft Outlook webhook
PyPi
Terraform

Fortify Enterprise



정보보호제품 성능평가 인증

KISA-SCA-2022-001

KISA

정보보호제품 성능평가 결과 확인서

신청기관명 : ㈜하로스
대 표 자 명 : 장 기 창
주 소 : 서울특별시 서초구 강남대로39길 15-3, 3층 401호(서초동, 보전빌딩)

1. 제품 유형 : 소스코드 보안약점 분석도구
2. 제품명 및 모델명 : Fortify Enterprise v3.1 (Windows)
3. 소프트웨어/펌웨어 버전 : 운영체제 Windows 11 Pro 64 bit
4. 성능평가 기준 : 소스코드 보안약점 분석도구 성능평가 절차서 V2.0 (2021.11.30)
5. 성능평가기관명 : ㈜한국정보보안기술원
6. 유효기간 : 2022년 12월 22일 ~ 2027년 12월 21일

위 제품은 정보보호산업의 진흥에 관한 법률 제17조 및 동법 시행령 제10조의 정보보호제품 성능평가 기준에 따라 성능평가를 수행하였음을 확인합니다.

2022년 12월 22일

한국인터넷진흥원장

KISA-SCA-2022-002

KISA

정보보호제품 성능평가 결과 확인서

신청기관명 : ㈜하로스
대 표 자 명 : 장 기 창
주 소 : 서울특별시 서초구 강남대로39길 15-3, 3층 401호(서초동, 보전빌딩)

1. 제품 유형 : 소스코드 보안약점 분석도구
2. 제품명 및 모델명 : Fortify Enterprise v3.1 (Linux)
3. 소프트웨어/펌웨어 버전 : 운영체제 Ubuntu 20.04.1 LTS 64 bit
   커 널 5.15.0-43
4. 성능평가 기준 : 소스코드 보안약점 분석도구 성능평가 절차서 V2.0 (2021.11.30)
5. 성능평가기관명 : ㈜한국정보보안기술원
6. 유효기간 : 2022년 12월 22일 ~ 2027년 12월 21일

위 제품은 정보보호산업의 진흥에 관한 법률 제17조 및 동법 시행령 제10조의 정보보호제품 성능평가 기준에 따라 성능평가를 수행하였음을 확인합니다.

2022년 12월 22일

한국인터넷진흥원장

Thank you