# vulnerability\_patterns.py

vulnerability\_patterns = {

"Broken Access Control": r"HttpServlet(Request|Response)|HttpSession|ServletContext|ServletRequest|ServletResponse|Filter(Chain|Config)|ServletConfig|\.(get|set|add|send|invalidate|doFilter|log|encode|getResource|getRealPath|getServlet|getContext|get(Major|Minor)Version|get(ServerInfo|NamedDispatcher|ServletRegistration|VirtualServerName))",

"Cryptographic Failures": r"^(?:java\.security\.MessageDigest|crypto\.Cipher|crypto\.KeyGenerator|crypto\.KeyAgreement|crypto\.Mac|crypto\.SecretKeyFactory|crypto\.spec\.DESKeySpec|crypto\.spec\.DESedeKeySpec|crypto\.spec\.PBEKeySpec|crypto\.spec\.SecretKeySpec|security\.KeyPairGenerator|security\.KeyFactory|security\.KeyPair|security\.Signature|security\.SecureRandom|security\.cert\.CertificateFactory|security\.cert\.X509Certificate|security\.cert\.Certificate|security\.spec\.AlgorithmParameterSpec|security\.spec\.DSAParameterSpec|security\.spec\.ECGenParameterSpec|security\.spec\.ECParameterSpec|security\.spec\.ECPrivateKeySpec|security\.spec\.ECPublicKeySpec|security\.spec\.KeySpec|security\.spec\.MGF1ParameterSpec|security\.spec\.PKCS8EncodedKeySpec|security\.spec\.RSAKeyGenParameterSpec|security\.spec\.RSAPrivateCrtKeySpec|security\.spec\.RSAPrivateKeySpec|security\.spec\.RSAPublicKeySpec|security\.spec\.X509EncodedKeySpec|security\.KeyStore|security\.SignedObject|security\.UnresolvedPermission|security\.Principal|security\.Policy|security\.Permission|security\.CodeSource|security\.Provider|security\.Security|security\.SecureClassLoader|security\.AlgorithmConstraints|security\.AlgorithmParameterGenerator|security\.DomainCombiner|security\.Identity|security\.IdentityScope|security\.Key|security\.KeyManagementException|security\.KeyStoreException)$",

"Injection": r"^(sql\.(Statement|PreparedStatement|CallableStatement|ResultSet)|util\.regex\.Pattern|util\.Scanner|lang\.Runtime\.exec\(\)|lang\.ProcessBuilder|lang\.Process|lang\.String\.format\(\)|lang\.System\.getenv\(\)|xml\.parsers\.SAXParser|beanutils\.BeanUtils\.setProperty\(\)|org\.apache\.commons\.collections4\.Transformer|org\.apache\.commons\.collections4\.functors\.InvokerTransformer|org\.apache\.commons\.collections4\.functors\.InstantiateTransformer|org\.apache\.commons\.dbcp\.BasicDataSource|org\.apache\.commons\.fileupload\.FileUpload|org\.apache\.commons\.fileupload\.servlet\.ServletFileUpload|org\.apache\.commons\.httpclient\.HttpClient|org\.apache\.commons\.httpclient\.methods\.PostMethod|org\.apache\.commons\.httpclient\.methods\.GetMethod|org\.apache\.commons\.httpclient\.NameValuePair|org\.apache\.commons\.lang\.StringEscapeUtils|org\.apache\.commons\.logging\.Log|org\.apache\.commons\.logging\.LogFactory|org\.apache\.commons\.net\.ftp\.FTPClient|org\.apache\.commons\.net\.ftp\.FTP|org\.apache\.commons\.pool\.impl\.GenericObjectPool|org\.apache\.commons\.pool\.impl\.StackKeyedObjectPool|log4j\.Logger|log4j\.Category|log4j\.Priority|lucene\.analysis\.Analyzer|lucene\.queryParser\.QueryParser|lucene\.search\.Searcher|lucene\.search\.IndexSearcher|lucene\.search\.highlight\.Highlighter|lucene\.util\.Version|runtime\.ProcessGroovyMethods\.execute\(\)|runtime\.ProcessGroovyMethods\.executeProcess\(\)|runtime\.RuntimeInvoker|runtime\.SqlGroovyMethods|runtime\.dgmimpl\.arrays\.IntegerArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.ShortArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.FloatArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.DoubleArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.LongArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.CharacterArrayGetAtMetaMethod|runtime\.dgmimpl\.arrays\.BooleanArrayGetAtMetaMethod)$",

"Insecure Design": r"^(net\.Socket|net\.ServerSocket|net\.URL|net\.URLConnection|net\.URLStreamHandler|net\.ProxySelector|net\.Authenticator|nio\.channels\.SocketChannel|nio\.channels\.ServerSocketChannel|nio\.file\.Files|nio\.file\.Path|nio\.file\.Paths|nio\.file\.attribute\.BasicFileAttributes|nio\.file\.attribute\.PosixFileAttributes|nio\.file\.attribute\.PosixFilePermission|nio\.file\.attribute\.PosixFilePermissions|util\.zip\.ZipEntry|util\.zip\.ZipInputStream|util\.zip\.ZipOutputStream|util\.zip\.ZipFile|util\.Timer|util\.TimerTask|util\.Properties|util\.prefs\.Preferences|util\.regex\.Matcher|util\.regex\.Pattern|util\.logging\.Logger|naming\.InitialContext|naming\.directory\.DirContext|net\.ssl\.SSLContext|net\.ssl\.SSLSocket|net\.ssl\.SSLSocketFactory|security\.auth\.Subject|security\.auth\.callback\.CallbackHandler|security\.auth\.login\.LoginContext|security\.auth\.x500\.X500Principal|servlet\.http\.Cookie|servlet\.http\.HttpServletRequest|servlet\.http\.HttpServletResponse|servlet\.http\.HttpSession|swing\.JFrame|swing\.JDialog|swing\.JOptionPane|swing\.JPanel|swing\.JTextField|xml\.XMLConstants|xml\.parsers\.DocumentBuilderFactory|xml\.transform\.TransformerFactory|xml\.validation\.SchemaFactory|w3c\.dom\.Document)$",

"Security Misconfiguration": r"^(util\.logging\.FileHandler|util\.logging\.SocketHandler|util\.logging\.StreamHandler|util\.logging\.ConsoleHandler|util\.logging\.Logger|net\.ssl\.SSLServerSocket|net\.ssl\.SSLSocket|net\.ssl\.SSLSession|net\.ssl\.X509TrustManager|crypto\.Cipher|crypto\.SecretKeyFactory|crypto\.spec\.SecretKeySpec|security\.auth\.login\.Configuration|security\.auth\.Subject|security\.auth\.callback\.CallbackHandler|security\.auth\.x500\.X500Principal|servlet\.http\.Cookie|servlet\.http\.HttpServletRequest|servlet\.http\.HttpServletResponse|servlet\.http\.HttpSession|servlet\.Filter|servlet\.Servlet|servlet\.ServletContext|servlet\.ServletRequest|servlet\.ServletResponse|servlet\.http\.HttpRequest|servlet\.http\.HttpResponse|xml\.parsers\.DocumentBuilder|xml\.validation\.Validator|xml\.validation\.SchemaFactory|xml\.transform\.TransformerFactory|management\.MBeanServer|management\.remote\.JMXConnector|management\.remote\.JMXConnectorServer|security\.Key|security\.KeyStore|security\.cert\.Certificate|security\.cert\.CertificateFactory|security\.cert\.X509Certificate|security\.MessageDigest|security\.SecureRandom|security\.Provider|security\.Security|net\.InetAddress|net\.InetSocketAddress|net\.ServerSocket|net\.Socket|net\.SocketAddress|net\.URL|net\.URLConnection)$",

"Vulnerable and Outdated Components": r"^(collections\.map\.LazyMap|fileupload\.FileItemFactory|io\.FileUtils|lang\.StringEscapeUtils|lang3\.ArrayUtils|lang3\.StringUtils|logging\.LogFactory|http\.client\.HttpClient|http\.client\.methods\.HttpRequestBase|http\.conn\.ssl\.SSLConnectionSocketFactory|http\.impl\.client\.CloseableHttpClient|http\.impl\.conn\.PoolingHttpClientConnectionManager|struts2\.dispatcher\.Dispatcher|struts2\.views\.freemarker\.FreemarkerResult|runtime\.ConvertedClosure|runtime\.MethodClosure|jackson\.map\.ObjectMapper|jackson\.JsonFactory|jackson\.JsonParser|jackson\.JsonGenerator|jackson\.map\.DeserializationConfig|jackson\.map\.SerializationConfig|jettison\.json\.JSONObject|xfire\.XFireFactory|xfire\.client\.XFireProxyFactory|xfire\.util\.Base64|hibernate\.SessionFactory|hibernate\.validator\.internal\.engine\.ConfigurationImpl|jboss\.logging\.Logger|joda\.time\.DateTime|joda\.time\.Duration|joda\.time\.format\.DateTimeFormat|joda\.time\.format\.DateTimeFormatter|springframework\.beans\.factory\.BeanFactory|springframework\.context\.support\.ClassPathXmlApplicationContext|springframework\.jdbc\.core\.JdbcTemplate|springframework\.orm\.hibernate3\.HibernateTransactionManager|springframework\.orm\.hibernate3\.LocalSessionFactoryBean|springframework\.security\.authentication\.AuthenticationManager|springframework\.security\.core\.userdetails\.UserDetailsService|springframework\.security\.crypto\.password\.PasswordEncoder|springframework\.web\.context\.ContextLoaderListener|springframework\.web\.context\.support\.XmlWebApplicationContext|springframework\.web\.filter\.CharacterEncodingFilter|springframework\.web\.servlet\.DispatcherServlet|springframework\.web\.servlet\.mvc\.Controller|springframework\.web\.servlet\.view\.InternalResourceViewResolver|springframework\.web\.util\.UriComponentsBuilder|xml\.sax\.XMLReader|xml\.sax\.helpers\.XMLFilterImpl)$",

"Identification & Authentication Failures": r"^(servlet\.http\.HttpServletRequest\.(getRemoteUser|getHeader|getAuthType)|servlet\.http\.HttpSession\.(setAttribute|getAttribute|invalidate|setMaxInactiveInterval)|security\.auth\.(Subject\.(doAs|getSubject)|login\.LoginContext|callback\.(CallbackHandler|NameCallback|PasswordCallback|UnsupportedCallbackException)|spi\.LoginModule)|security\.cert\.(X509Certificate|CertificateFactory|CertificateEncodingException|CertificateParsingException|X509Certificate2)|crypto\.(Cipher|KeyGenerator|SecretKey|spec\.(SecretKeySpec|PKCS8EncodedKeySpec|X509EncodedKeySpec)|Mac)|security\.(MessageDigest|SecureRandom|KeyPairGenerator|KeyStore)|net\.(Authenticator\.setDefault|URL\.openConnection|HttpURLConnection|URLConnection\.(setDoOutput|getOutputStream|setDoInput|getInputStream))|util\.(Base64\.encodeToString|UUID\.randomUUID)|codec\.(digest\.DigestUtils|binary\.(Base64|Hex)))$",

"Software and data Integrity Failures": r"^(io\.File|nio\.file\.Files|nio\.file\.Path|util\.zip\.ZipInputStream|util\.zip\.ZipOutputStream|util\.zip\.ZipEntry|io\.FileOutputStream|io\.FileInputStream|io\.ObjectOutputStream|io\.ObjectInputStream|io\.InputStream|io\.OutputStream|io\.ByteArrayInputStream|io\.ByteArrayOutputStream|util\.jar\.JarFile|util\.jar\.JarInputStream|util\.jar\.JarOutputStream|util\.jar\.JarEntry|util\.logging\.Logger|util\.logging\.FileHandler|util\.logging\.ConsoleHandler|util\.logging\.Handler|util\.logging\.Level|util\.Properties|lang\.System\.setProperty\(\)|lang\.Runtime\.exec\(\)|lang\.ProcessBuilder|lang\.ProcessBuilder\.command\(\)|lang\.ProcessBuilder\.directory\(\)|lang\.ProcessBuilder\.environment\(\)|lang\.Process\.waitFor\(\)|lang\.reflect\.Method|lang\.reflect\.Constructor|lang\.reflect\.Field|lang\.Class\.getDeclaredMethod\(\)|lang\.Class\.getDeclaredConstructor\(\)|lang\.Class\.getDeclaredField\(\)|lang\.ClassLoader\.defineClass\(\)|lang\.invoke\.MethodHandle|lang\.invoke\.MethodHandles|lang\.invoke\.MethodHandles\.Lookup|net\.Socket|net\.ServerSocket|net\.ssl\.SSLServerSocket|net\.ssl\.SSLSocket|xml\.parsers\.DocumentBuilderFactory|xml\.parsers\.DocumentBuilder|xml\.transform\.TransformerFactory|xml\.transform\.Transformer|xml\.transform\.stream\.StreamResult)$",

"Security Logging and Monitoring Failures": r"^(util\.logging\.(Logger|FileHandler|ConsoleHandler|Handler|Level|LogManager|LogRecord)|apache\.log4j\.(Logger|FileAppender|ConsoleAppender|Appender|Level|spi\.LoggingEvent)|apache\.commons\.logging\.(Log|LogFactory)|slf4j\.(Logger|LoggerFactory)|servlet\.ServletContext\.log\(\)|servlet\.http\.HttpServletRequest\.getRequestURI\(\)|servlet\.http\.HttpServletRequest\.getParameter\(\)|javax\.servlet\.http\.HttpServletRequest\.getHeader\(\)|servlet\.http\.HttpSession\.getAttribute\(\)|servlet\.http\.HttpSession\.getId\(\)|servlet\.http\.HttpSession\.getLastAccessedTime\(\)|servlet\.http\.HttpSession\.setMaxInactiveInterval\(\)|security\.auth\.login\.LoginContext|security\.auth\.callback\.CallbackHandler|security\.auth\.message\.MessageInfo|security\.auth\.message\.MessagePolicy|security\.auth\.Subject|net\.(Socket|ServerSocket|URL|URI|URLConnection|ProxySelector|Proxy|InetAddress|NetworkInterface|DatagramSocket|DatagramPacket|MulticastSocket|ServerSocketChannel|SocketChannel)|sql\.(Connection|Statement|PreparedStatement|ResultSet|DatabaseMetaData))$",

"Server-Side Request Forgery": r"^(net\.URL\.openStream\(\)|net\.URL\.openConnection\(\)|net\.HttpURLConnection|net\.Socket|net\.URLDecoder\.decode\(\)|net\.URLEncoder\.encode\(\)|net\.URI\.create\(\)|net\.InetAddress\.getAllByName\(\)|net\.ProxySelector|net\.Proxy|net\.InetSocketAddress|net\.DatagramSocket|net\.DatagramPacket|net\.MulticastSocket|net\.ServerSocketChannel|net\.SocketChannel|net\.NetworkInterface|net\.URLClassLoader|sql\.Connection|sql\.Statement|sql\.PreparedStatement|sql\.ResultSet|xml\.parsers\.DocumentBuilderFactory|xml\.transform\.TransformerFactory|xml\.transform\.Transformer|xml\.transform\.stream\.StreamResult|xml\.transform\.dom\.DOMSource|xml\.parsers\.SAXParser|xml\.parsers\.SAXParserFactory|xml\.validation\.SchemaFactory|xml\.validation\.Validator|xml\.xpath\.XPathFactory|xml\.xpath\.XPath|xml\.xpath\.XPathExpression|xml\.xpath\.XPathConstants|xml\.bind\.JAXBContext|xml\.bind\.Marshaller|xml\.bind\.Unmarshaller|httpclient\.HttpClient|httpclient\.HttpMethod|httpclient\.methods\.GetMethod|httpclient\.methods\.PostMethod|httpclient\.methods\.HeadMethod|httpclient\.methods\.PutMethod|httpclient\.methods\.DeleteMethod|httpclient\.methods\.OptionsMethod|httpclient\.methods\.TraceMethod|httpclient\.NameValuePair|httpclient\.HttpState|httpclient\.HostConfiguration)$",

}

**Validator:**

https://www.101computing.net/bracket-validator/

--------------------------Broken Access Control----------------------------

HttpServletRequest.getRequestURI()

HttpServletRequest.getRequestURL()

HttpServletRequest.getMethod()

HttpServletRequest.getQueryString()

HttpServletRequest.getParameter()

HttpServletRequest.getHeader()

HttpSession.getAttribute()

HttpSession.setAttribute()

HttpSession.invalidate()

ServletContext.getAttribute()

ServletContext.setAttribute()

ServletContext.log()

ServletRequest.getAttribute()

ServletRequest.setAttribute()

ServletRequest.getRemoteAddr()

ServletRequest.getRemoteHost()

ServletRequest.getRemoteUser()

ServletRequest.getRequestedSessionId()

ServletRequest.getScheme()

ServletRequest.getServerName()

ServletRequest.getServerPort()

ServletRequest.getParameter()

ServletRequest.getParameterMap()

ServletRequest.getParameterValues()

HttpServletResponse.setHeader()

HttpServletResponse.addHeader()

HttpServletResponse.sendError()

HttpServletResponse.sendRedirect()

HttpServletResponse.setStatus()

FilterChain.doFilter()

FilterConfig.getInitParameter()

FilterConfig.getServletContext()

ServletConfig.getInitParameter()

ServletContext.getInitParameter()

ServletContext.getResource()

ServletContext.getResourceAsStream()

ServletContext.getRealPath()

ServletContext.getServlet()

ServletContext.getServletNames()

ServletContext.getServlets()

ServletContext.getContext()

ServletContext.getContextPath()

ServletContext.getMajorVersion()

ServletContext.getMinorVersion()

ServletContext.getServerInfo()

ServletContext.getNamedDispatcher()

ServletContext.getServletRegistration()

ServletContext.getServletRegistrations()

ServletContext.getVirtualServerName()

ServletResponse.encodeURL()

---------------------- Cryptographic Failures--------------

security.MessageDigest

crypto.Cipher

crypto.KeyGenerator

crypto.KeyAgreement

crypto.Mac

crypto.SecretKeyFactory

crypto.spec.DESKeySpec

crypto.spec.DESedeKeySpec

crypto.spec.PBEKeySpec

crypto.spec.SecretKeySpec

security.KeyPairGenerator

security.KeyFactory

security.KeyPair

security.Signature

security.SecureRandom

security.cert.CertificateFactory

security.cert.X509Certificate

security.cert.Certificate

security.spec.AlgorithmParameterSpec

security.spec.DSAParameterSpec

security.spec.ECGenParameterSpec

security.spec.ECParameterSpec

security.spec.ECPrivateKeySpec

security.spec.ECPublicKeySpec

security.spec.KeySpec

security.spec.MGF1ParameterSpec

security.spec.PKCS8EncodedKeySpec

security.spec.RSAKeyGenParameterSpec

security.spec.RSAPrivateCrtKeySpec

security.spec.RSAPrivateKeySpec

security.spec.RSAPublicKeySpec

security.spec.X509EncodedKeySpec

security.KeyStore

security.SignedObject

security.UnresolvedPermission

security.Principal

security.Policy

security.Permission

security.CodeSource

security.Provider

security.Security

security.SecureClassLoader

security.AlgorithmConstraints

security.AlgorithmParameterGenerator

security.DomainCombiner

security.Identity

security.IdentityScope

security.Key

security.KeyManagementException

security.KeyStoreException

----------------- Injection --------------------

sql.Statement

sql.PreparedStatement

sql.CallableStatement

sql.ResultSet

util.regex.Pattern

util.Scanner

lang.Runtime.exec()

lang.ProcessBuilder

lang.Process

lang.String.format()

lang.System.getenv()

xml.parsers.SAXParser

beanutils.BeanUtils.setProperty()

org.apache.commons.collections4.Transformer

org.apache.commons.collections4.functors.InvokerTransformer

org.apache.commons.collections4.functors.InstantiateTransformer

org.apache.commons.dbcp.BasicDataSource

org.apache.commons.fileupload.FileUpload

org.apache.commons.fileupload.servlet.ServletFileUpload

org.apache.commons.httpclient.HttpClient

org.apache.commons.httpclient.methods.PostMethod

org.apache.commons.httpclient.methods.GetMethod

org.apache.commons.httpclient.NameValuePair

org.apache.commons.lang.StringEscapeUtils

org.apache.commons.logging.Log

org.apache.commons.logging.LogFactory

org.apache.commons.net.ftp.FTPClient

org.apache.commons.net.ftp.FTP

org.apache.commons.pool.impl.GenericObjectPool

org.apache.commons.pool.impl.StackKeyedObjectPool

log4j.Logger

log4j.Category

log4j.Priority

lucene.analysis.Analyzer

lucene.queryParser.QueryParser

lucene.search.Searcher

lucene.search.IndexSearcher

lucene.search.highlight.Highlighter

lucene.util.Version

runtime.ProcessGroovyMethods.execute()

runtime.ProcessGroovyMethods.executeProcess()

runtime.RuntimeInvoker

runtime.SqlGroovyMethods

runtime.dgmimpl.arrays.IntegerArrayGetAtMetaMethod

runtime.dgmimpl.arrays.ShortArrayGetAtMetaMethod

runtime.dgmimpl.arrays.FloatArrayGetAtMetaMethod

runtime.dgmimpl.arrays.DoubleArrayGetAtMetaMethod

runtime.dgmimpl.arrays.LongArrayGetAtMetaMethod

runtime.dgmimpl.arrays.CharacterArrayGetAtMetaMethod

runtime.dgmimpl.arrays.BooleanArrayGetAtMetaMethod

--------------------------Insecure Design---------------

net.Socket

net.ServerSocket

net.URL

net.URLConnection

net.URLStreamHandler

net.ProxySelector

net.Authenticator

nio.channels.SocketChannel

nio.channels.ServerSocketChannel

nio.file.Files

nio.file.Path

nio.file.Paths

nio.file.attribute.BasicFileAttributes

nio.file.attribute.PosixFileAttributes

nio.file.attribute.PosixFilePermission

nio.file.attribute.PosixFilePermissions

util.zip.ZipEntry

util.zip.ZipInputStream

util.zip.ZipOutputStream

util.zip.ZipFile

util.Timer

util.TimerTask

util.Properties

util.prefs.Preferences

util.regex.Matcher

util.regex.Pattern

util.logging.Logger

naming.InitialContext

naming.directory.DirContext

net.ssl.SSLContext

net.ssl.SSLSocket

net.ssl.SSLSocketFactory

security.auth.Subject

security.auth.callback.CallbackHandler

security.auth.login.LoginContext

security.auth.x500.X500Principal

servlet.http.Cookie

servlet.http.HttpServletRequest

servlet.http.HttpServletResponse

servlet.http.HttpSession

swing.JFrame

swing.JDialog

swing.JOptionPane

swing.JPanel

swing.JTextField

xml.XMLConstants

xml.parsers.DocumentBuilderFactory

xml.transform.TransformerFactory

xml.validation.SchemaFactory

w3c.dom.Document

---------------------------------------Security Misconfiguration-----------

util.logging.FileHandler

util.logging.SocketHandler

util.logging.StreamHandler

util.logging.ConsoleHandler

util.logging.Logger

net.ssl.SSLServerSocket

net.ssl.SSLSocket

net.ssl.SSLSession

net.ssl.X509TrustManager

crypto.Cipher

crypto.SecretKeyFactory

crypto.spec.SecretKeySpec

security.auth.login.Configuration

security.auth.Subject

security.auth.callback.CallbackHandler

security.auth.x500.X500Principal

servlet.http.Cookie

servlet.http.HttpServletRequest

servlet.http.HttpServletResponse

servlet.http.HttpSession

servlet.Filter

servlet.Servlet

servlet.ServletContext

servlet.ServletRequest

servlet.ServletResponse

servlet.http.HttpRequest

servlet.http.HttpResponse

xml.parsers.DocumentBuilder

xml.validation.Validator

xml.validation.SchemaFactory

xml.transform.TransformerFactory

management.MBeanServer

management.remote.JMXConnector

management.remote.JMXConnectorServer

security.Key

security.KeyStore

security.cert.Certificate

security.cert.CertificateFactory

security.cert.X509Certificate

security.MessageDigest

security.SecureRandom

security.Provider

security.Security

net.InetAddress

net.InetSocketAddress

net.ServerSocket

net.Socket

net.SocketAddress

net.URL

net.URLConnection

-------------Vulnerable and Outdated Components-----------

collections.map.LazyMap

fileupload.FileItemFactory

io.FileUtils

lang.StringEscapeUtils

lang3.ArrayUtils

lang3.StringUtils

logging.LogFactory

http.client.HttpClient

http.client.methods.HttpRequestBase

http.conn.ssl.SSLConnectionSocketFactory

http.impl.client.CloseableHttpClient

http.impl.conn.PoolingHttpClientConnectionManager

struts2.dispatcher.Dispatcher

struts2.views.freemarker.FreemarkerResult

runtime.ConvertedClosure

runtime.MethodClosure

jackson.map.ObjectMapper

jackson.JsonFactory

jackson.JsonParser

jackson.JsonGenerator

jackson.map.DeserializationConfig

jackson.map.SerializationConfig

jettison.json.JSONObject

xfire.XFireFactory

xfire.client.XFireProxyFactory

xfire.util.Base64

hibernate.SessionFactory

hibernate.validator.internal.engine.ConfigurationImpl

jboss.logging.Logger

joda.time.DateTime

joda.time.Duration

joda.time.format.DateTimeFormat

joda.time.format.DateTimeFormatter

springframework.beans.factory.BeanFactory

springframework.context.support.ClassPathXmlApplicationContext

springframework.jdbc.core.JdbcTemplate

springframework.orm.hibernate3.HibernateTransactionManager

springframework.orm.hibernate3.LocalSessionFactoryBean

springframework.security.authentication.AuthenticationManager

springframework.security.core.userdetails.UserDetailsService

springframework.security.crypto.password.PasswordEncoder

springframework.web.context.ContextLoaderListener

springframework.web.context.support.XmlWebApplicationContext

springframework.web.filter.CharacterEncodingFilter

springframework.web.servlet.DispatcherServlet

springframework.web.servlet.mvc.Controller

springframework.web.servlet.view.InternalResourceViewResolver

springframework.web.util.UriComponentsBuilder

xml.sax.XMLReader

xml.sax.helpers.XMLFilterImpl

---------------------------Identification and Authentication Failures------------

servlet.http.HttpServletRequest.getRemoteUser()

servlet.http.HttpServletRequest.getHeader()

servlet.http.HttpServletRequest.getAuthType()

servlet.http.HttpSession.setAttribute()

servlet.http.HttpSession.getAttribute()

servlet.http.HttpSession.invalidate()

servlet.http.HttpSession.setMaxInactiveInterval()

security.auth.Subject.doAs()

security.auth.Subject.getSubject()

security.auth.login.LoginContext

security.auth.callback.CallbackHandler

security.auth.callback.NameCallback

security.auth.callback.PasswordCallback

security.auth.callback.UnsupportedCallbackException

security.auth.spi.LoginModule

security.cert.X509Certificate

crypto.Cipher

crypto.KeyGenerator

crypto.SecretKey

crypto.spec.SecretKeySpec

crypto.Mac

security.MessageDigest

security.SecureRandom

security.KeyPairGenerator

security.KeyStore

security.cert.Certificate

security.cert.CertificateFactory

security.cert.CertificateEncodingException

security.cert.CertificateParsingException

security.cert.X509Certificate

security.cert.X509Certificate2

security.interfaces.RSAPublicKey

security.interfaces.RSAPrivateKey

security.spec.KeySpec

security.spec.PKCS8EncodedKeySpec

security.spec.X509EncodedKeySpec

net.Authenticator.setDefault()

net.URL.openConnection()

net.HttpURLConnection

net.URLConnection.setDoOutput()

net.URLConnection.getOutputStream()

net.URLConnection.setDoInput()

net.URLConnection.getInputStream()

net.URLDecoder.decode()

net.URLEncoder.encode()

util.Base64.encodeToString()

util.UUID.randomUUID()

codec.digest.DigestUtils

codec.binary.Base64

codec.binary.Hex

--------------------------Software and Data Integrity Failures-------------

io.File

nio.file.Files

nio.file.Path

util.zip.ZipInputStream

util.zip.ZipOutputStream

util.zip.ZipEntry

io.FileOutputStream

io.FileInputStream

io.ObjectOutputStream

io.ObjectInputStream

io.InputStream

io.OutputStream

io.ByteArrayInputStream

io.ByteArrayOutputStream

util.jar.JarFile

util.jar.JarInputStream

util.jar.JarOutputStream

util.jar.JarEntry

util.logging.Logger

util.logging.FileHandler

util.logging.ConsoleHandler

util.logging.Handler

util.logging.Level

util.Properties

lang.System.setProperty()

lang.Runtime.exec()

lang.ProcessBuilder

lang.ProcessBuilder.command()

lang.ProcessBuilder.directory()

lang.ProcessBuilder.environment()

lang.Process.waitFor()

lang.reflect.Method

lang.reflect.Constructor

lang.reflect.Field

lang.Class.getDeclaredMethod()

lang.Class.getDeclaredConstructor()

lang.Class.getDeclaredField()

lang.ClassLoader.defineClass()

lang.invoke.MethodHandle

lang.invoke.MethodHandles

lang.invoke.MethodHandles.Lookup

net.Socket

net.ServerSocket

net.ssl.SSLServerSocket

net.ssl.SSLSocket

xml.parsers.DocumentBuilderFactory

xml.parsers.DocumentBuilder

xml.transform.TransformerFactory

xml.transform.Transformer

xml.transform.stream.StreamResult

-------------------Security Logging and Monitoring Failures--------------

util.logging.Logger

util.logging.FileHandler

util.logging.ConsoleHandler

util.logging.Handler

util.logging.Level

util.logging.LogManager

util.logging.LogRecord

apache.log4j.Logger

apache.log4j.FileAppender

apache.log4j.ConsoleAppender

apache.log4j.Appender

apache.log4j.Level

apache.log4j.spi.LoggingEvent

apache.commons.logging.Log

apache.commons.logging.LogFactory

slf4j.Logger

slf4j.LoggerFactory

servlet.ServletContext.log()

servlet.http.HttpServletRequest.getRequestURI()

servlet.http.HttpServletRequest.getParameter()

javax.servlet.http.HttpServletRequest.getHeader()

servlet.http.HttpSession.getAttribute()

servlet.http.HttpSession.getId()

servlet.http.HttpSession.getLastAccessedTime()

servlet.http.HttpSession.setMaxInactiveInterval()

security.auth.login.LoginContext

security.auth.callback.CallbackHandler

security.auth.message.MessageInfo

security.auth.message.MessagePolicy

security.auth.Subject

net.Socket

net.ServerSocket

net.URL

net.URI

net.URLConnection

net.ProxySelector

net.Proxy

net.InetAddress

net.NetworkInterface

net.DatagramSocket

net.DatagramPacket

net.MulticastSocket

net.ServerSocketChannel

net.SocketChannel

sql.Connection

sql.Statement

sql.PreparedStatement

sql.ResultSet

sql.DatabaseMetaData

-----------------------Server-Side Request Forgery------------

net.URL.openStream()

net.URL.openConnection()

net.HttpURLConnection

net.Socket

net.URLDecoder.decode()

net.URLEncoder.encode()

net.URI.create()

net.InetAddress.getAllByName()

net.ProxySelector

net.Proxy

net.InetSocketAddress

net.DatagramSocket

net.DatagramPacket

net.MulticastSocket

net.ServerSocketChannel

net.SocketChannel

net.NetworkInterface

net.URLClassLoader

sql.Connection

sql.Statement

sql.PreparedStatement

sql.ResultSet

xml.parsers.DocumentBuilderFactory

xml.transform.TransformerFactory

xml.transform.Transformer

xml.transform.stream.StreamResult

xml.transform.dom.DOMSource

xml.parsers.SAXParser

xml.parsers.SAXParserFactory

xml.validation.SchemaFactory

xml.validation.Validator

xml.xpath.XPathFactory

xml.xpath.XPath

xml.xpath.XPathExpression

xml.xpath.XPathConstants

xml.bind.JAXBContext

xml.bind.Marshaller

xml.bind.Unmarshaller

httpclient.HttpClient

httpclient.HttpMethod

httpclient.methods.GetMethod

httpclient.methods.PostMethod

httpclient.methods.HeadMethod

httpclient.methods.PutMethod

httpclient.methods.DeleteMethod

httpclient.methods.OptionsMethod

httpclient.methods.TraceMethod

httpclient.NameValuePair

httpclient.HttpState

httpclient.HostConfiguration

1. r"getRequestURI|getRequestURL|getMethod|getQueryString|getParameter|getHeader|getAttribute|setAttribute|invalidate|getAttribute|setAttribute|log|getAttribute|setAttribute|getRemoteAddr|getRemoteHost|getRemoteUser|getRequestedSessionId|getScheme|getServerName|getServerPort|getParameter|getParameterMap|getParameterValues|setHeader|addHeader|sendError|sendRedirect|setStatus|doFilter|getInitParameter|getServletContext|getInitParameter|getInitParameter|getResource|getResourceAsStream|getRealPath|getServlet|getServletNames|getServlets|getContext|getContextPath|getMajorVersion|getMinorVersion|getServerInfo|getNamedDispatcher|getServletRegistration|getServletRegistrations|getVirtualServerName|encodeURL"
2. r"MessageDigest|Cipher|KeyGenerator|KeyAgreement|Mac|SecretKeyFactory|DESKeySpec|DESedeKeySpec|PBEKeySpec|SecretKeySpec|KeyPairGenerator|KeyFactory|KeyPair|Signature|SecureRandom|CertificateFactory|X509Certificate|Certificate|AlgorithmParameterSpec|DSAParameterSpec|ECGenParameterSpec|ECParameterSpec|ECPrivateKeySpec|ECPublicKeySpec|KeySpec|MGF1ParameterSpec|PKCS8EncodedKeySpec|RSAKeyGenParameterSpec|RSAPrivateCrtKeySpec|RSAPrivateKeySpec|RSAPublicKeySpec|X509EncodedKeySpec|KeyStore|SignedObject|UnresolvedPermission|Principal|Policy|Permission|CodeSource|Provider|Security|SecureClassLoader|AlgorithmConstraints|AlgorithmParameterGenerator|DomainCombiner|Identity|IdentityScope|Key|KeyManagementException|KeyStoreException"
3. r"Statement|PreparedStatement|CallableStatement|ResultSet|Pattern|Scanner|ProcessBuilder|Process|SAXParser|Transformer|InvokerTransformer|InstantiateTransformer|BasicDataSource|FileUpload|ServletFileUpload|HttpClient|PostMethod|GetMethod|NameValuePair|StringEscapeUtils|Log|LogFactory|FTPClient|FTP|GenericObjectPool|StackKeyedObjectPool|Logger|Category|Priority|Analyzer|QueryParser|Searcher|IndexSearcher|Highlighter|Version|RuntimeInvoker|SqlGroovyMethods|IntegerArrayGetAtMetaMethod|ShortArrayGetAtMetaMethod|FloatArrayGetAtMetaMethod|DoubleArrayGetAtMetaMethod|LongArrayGetAtMetaMethod|CharacterArrayGetAtMetaMethod|BooleanArrayGetAtMetaMethod"
4. r"Socket|ServerSocket|URL|URLConnection|URLStreamHandler|ProxySelector|Authenticator|SocketChannel|ServerSocketChannel|Files|Path|Paths|BasicFileAttributes|PosixFileAttributes|PosixFilePermission|PosixFilePermissions|ZipEntry|ZipInputStream|ZipOutputStream|ZipFile|Timer|TimerTask|Properties|Preferences|Matcher|Pattern|Logger|InitialContext|DirContext|SSLContext|SSLSocket|SSLSocketFactory|Subject|CallbackHandler|LoginContext|X500Principal|Cookie|HttpServletRequest|HttpServletResponse|HttpSession|JFrame|JDialog|JOptionPane|JPanel|JTextField|XMLConstants|DocumentBuilderFactory|TransformerFactory|SchemaFactory|Document"
5. r"FileHandler|SocketHandler|StreamHandler|ConsoleHandler|Logger|SSLServerSocket|SSLSocket|SSLSession|X509TrustManager|Cipher|SecretKeyFactory|SecretKeySpec|Configuration|Subject|CallbackHandler|X500Principal|Cookie|HttpServletRequest|HttpServletResponse|HttpSession|Filter|Servlet|ServletContext|ServletRequest|ServletResponse|HttpRequest|HttpResponse|DocumentBuilder|Validator|SchemaFactory|TransformerFactory|MBeanServer|JMXConnector|JMXConnectorServer|Key|KeyStore|Certificate|CertificateFactory|X509Certificate|MessageDigest|SecureRandom|Provider|Security|InetAddress|InetSocketAddress|ServerSocket|Socket|SocketAddress|URL|URLConnection"
6. r"LazyMap|FileItemFactory|FileUtils|StringEscapeUtils|ArrayUtils|StringUtils|LogFactory|HttpClient|HttpRequestBase|SSLConnectionSocketFactory|CloseableHttpClient|PoolingHttpClientConnectionManager|Dispatcher|FreemarkerResult|ConvertedClosure|MethodClosure|ObjectMapper|JsonFactory|JsonParser|JsonGenerator|DeserializationConfig|SerializationConfig|JSONObject|XFireFactory|XFireProxyFactory|Base64|SessionFactory|ConfigurationImpl|Logger|DateTime|Duration|DateTimeFormat|DateTimeFormatter|BeanFactory|ClassPathXmlApplicationContext|JdbcTemplate|HibernateTransactionManager|LocalSessionFactoryBean|AuthenticationManager|UserDetailsService|PasswordEncoder|ContextLoaderListener|XmlWebApplicationContext|CharacterEncodingFilter|DispatcherServlet|Controller|InternalResourceViewResolver|UriComponentsBuilder|XMLReader|XMLFilterImpl"
7. r"LoginContext|CallbackHandler|NameCallback|PasswordCallback|UnsupportedCallbackException|LoginModule|X509Certificate|Cipher|KeyGenerator|SecretKey|SecretKeySpec|Mac|MessageDigest|SecureRandom|KeyPairGenerator|KeyStore|Certificate|CertificateFactory|CertificateEncodingException|CertificateParsingException|X509Certificate|X509Certificate2|RSAPublicKey|RSAPrivateKey|KeySpec|PKCS8EncodedKeySpec|X509EncodedKeySpec|HttpURLConnection|DigestUtils|Base64|Hex"
8. r"File|Files|Path|ZipInputStream|ZipOutputStream|ZipEntry|FileOutputStream|FileInputStream|ObjectOutputStream|ObjectInputStream|InputStream|OutputStream|ByteArrayInputStream|ByteArrayOutputStream|JarFile|JarInputStream|JarOutputStream|JarEntry|Logger|FileHandler|ConsoleHandler|Handler|Level|Properties|ProcessBuilder|Method|Constructor|Field|MethodHandle|MethodHandles|Lookup|Socket|ServerSocket|SSLServerSocket|SSLSocket|DocumentBuilderFactory|DocumentBuilder|TransformerFactory|Transformer|StreamResult"
9. r"Logger|FileHandler|ConsoleHandler|Handler|Level|LogManager|LogRecord|Logger|FileAppender|ConsoleAppender|Appender|Level|LoggingEvent|Log|LogFactory|Logger|LoggerFactory|LoginContext|CallbackHandler|MessageInfo|MessagePolicy|Subject|Socket|ServerSocket|URL|URI|URLConnection|ProxySelector|Proxy|InetAddress|NetworkInterface|DatagramSocket|DatagramPacket|MulticastSocket|ServerSocketChannel|SocketChannel|InetSocketAddress|Connection|Statement|PreparedStatement|ResultSet|DatabaseMetaData"
10. r"HttpURLConnection|Socket|ProxySelector|Proxy|InetSocketAddress|DatagramSocket|DatagramPacket|MulticastSocket|ServerSocketChannel|SocketChannel|NetworkInterface|URLClassLoader|Connection|Statement|PreparedStatement|ResultSet|DocumentBuilderFactory|TransformerFactory|Transformer|StreamResult|DOMSource|SAXParser|SAXParserFactory|SchemaFactory|Validator|XPathFactory|XPath|XPathExpression|XPathConstants|JAXBContext|Marshaller|Unmarshaller|HttpClient|HttpMethod|GetMethod|PostMethod|HeadMethod|PutMethod|DeleteMethod|OptionsMethod|TraceMethod|NameValuePair|HttpState|HostConfiguration"