1.0	2019-08-24			

▪

2.1 Web

2.1.1 SQL

SQL
SQL SQL
SQL
SQL SQL

2.1.2 XSS

(Cross Site Scripting) (Cascading Style Sheets, CSS)
XSS Web Script
Web Script
XSS
DOM Cookies

2.1.3 XML XXE

XXE Injection XML External Entity Injection, XML
行 XML1.0 里 ,XML
(entity) ,
“ ” , XML

2.1.4 CSRF

CSRF Cross-Site Request Forgery

CSRF

2.1.5 SSRF

SSRF(Server-Side Request Forgery:)

SSRF

SSRF

URL

2.1.6

Web javascript

jsp asp php aspx

2.1.7

(..\ ../)

2.1.8

../ ..

2.1.9 .svn/.git

.svn/.git

(svn git)

2.1.10

2.1.11 CRLF

CRLF “HTTP ”
HTTP
(\r\n) HTTP web

2.1.12

2.1.13 URL

URL Web URL URL
URL URL URL

2.1.14 Json

Json Json
URL
Javscript Hook Json

2.1.15

Ewebeditor FCKeditor Ueditor JQuery

2.1.16 /

/ PHP PHP

php

2.1.17

2.1.18 Struts2

Struts2 Strut2

OGNL OGNL

2.1.19 Spring

Spring Spring
Spring

2.1.20 “X-XSS-Protection”

“X-XSS-Protection” “ ”
web IE 8+ Chrome 4+

2.1.21 flash

flash flash player
crossdomain.xml ,

allow-access-from domain * flash

2.1.22 HTML CSRF

CSRF XSRF

html Web

CSRF

CSRF Web

2.1.23 HTTP

http http

2.1.24 GET

GET URL

2.1.25 X-Frame-Options Header

iframe

iframe iframe

iframe

X-Frame-Options HTTP “frame” “iframe”

2.1.26

(..\

../)

2.1.27

2.1.28 HTTPONLY

Cookie JSESSIONID HttpOnly
Cookie

2.1.29 X-Forwarded-For

2.1.31 HTTP Methods

HTTP PUT/DELETE/MOVE/COPY/TRACE,

2.1.32

2.2

2.2.1

2.2.2 telnet

Telnet

1 sniffer

2

3

4

2.3

2.3.1

2.3.2

2.3.3

“

”

2.3.4

2.3.5

2.3.6

Session ID

Session ID URL URL

Session ID

2.3.7

2.3.8

2.3.9

2.3.10

-
-
-

1.

1

1

“ x = ”

/

1

1

( )

2.

1

URL

3.

JavaScript

2.3.11

“ ”

2.3.12 Flash

Flash

2.4

2.4.1

2.4.2

2.4.3 Jboss

Jboss Commoncollections.jar

2.4.4 Websphere

Websphere Commoncollections.jar

2.4.5 Jenkins

Jenkins Commoncollections.jar

2.4.6 JBoss

Jboss
EJBInvokerServlet JMXInvokerServlet
WAR

2.4.7 Webloigc

Weblogic Commoncollections.jar

2.4.8 Apache Tomcat session

Apache Tomcat ”/examples” session
(/examples/servlets/servlet/SessionExample) session
session session

2.5

2.5.1

2.5.2

DNS

DNS DNS

IP

2.5.3 Redis

Redis Redis

Redis

SSH

2.5.4 MongoDB

MongoDB MongoDB

MongoDB MongoDB

2.5.5

2.5.6

2.5.7

2.5.8

2.5.9

EternalBlue SMB

WannaCry

2.5.10 mssql

SQL Server TCP-1433 UDP-1434 1433 SQL Server
1434 SQL Server TCP/IP

2.5.11 windows

windows

2.5.12

2.5.13