1.由于涉及的操作系统、JAVA版本、Web服务器、加密机和浏览器较多，为了提高测试效率，采取交叉测试，目前优先测试以下组合：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 操作系统 | JAVA版本 | Web服务器 | 加密机 | 浏览器 |
| Redhat 6.5（64位） | 8（64位） | Tomcat（8.5） | 得安 | Firefox |
| 8（32位） | Tomcat(9)  Weblogic 11g （10.3.6） |
| Redhat 7.5（64位） | 7（64位） | Tomcat（7） | 得安  江南天安 | Chrome  IE |
| centos 7（32位） | 7（32位） | Tomcat（8.0） | 得安  普华 | IE  Chrome  Firefox |
| 8（32位） | Wildfly（12） |
| Windows Server 2012 R2 | 8（32位） | Tomcat（9）  Wildfly（12） | 得安  普华 | IE  Chrome Firefox |
| Windows Server 2016 | 7（64位） | Tomcat（8.5）  Weblogic 12c（12）  Weblogic 11g （10.3.6） | 得安  江南天安 | IE  Chrome |

2.密码套件测试列表：

|  |  |  |
| --- | --- | --- |
| SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA |  |  |
| TLS\_ECDHE\_RSA\_\*\*\* |  |  |
| TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA |  |  |
| TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA |  |  |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA |  |  |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA |  | AES\_256 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |  |  |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 |  | AES\_256 |
| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | AES\_GCM |  |
| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | AES\_GCM | AES\_256 |
| TLS\_ECDHE\_ECDSA\_\*\*\* |  |  |
| TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA |  |  |
| TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA |  |  |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA |  |  |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA |  | AES\_256 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 |  |  |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 |  | AES\_256 |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | AES\_GCM |  |
| TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | AES\_GCM | AES\_256 |