Stack：先进后出

|  |  |
| --- | --- |
| Payload1 | |
| \0 | Strlen就读到0 |
| \xff  \xff  \xff  \xff  \xff  \xff  \xff | 最大的数值（类似ffH）\xff  直到把第八个位置占领了，即buf[7]是个很大的数目 |

|  |  |
| --- | --- |
| Payload2 | |
| 4 | 写的长度 |
| Write\_got | 写的内容 |
| 1 | 写的地址 |
| Main | 执行完后返回 |
| Write\_plt | 执行write |
| Aaaaaaaa…  （0xe7+4） | 栈溢出用于覆盖返回地址 |

|  |  |
| --- | --- |
| Payload3 | |
|  |  |
| binsh |  |
| 1 | 栈对齐 |
| System\_addr |  |
| aaa | 溢出 |