1. sql注入，缓冲区溢出
2. select \* from users where id =1 and/or 1
3. select \* from users where id =1 and 0
4. Select \* from users where id=2 order by 4
5. Select \* from users where id=2 union select 1,2,@@version（user()） order by 1(注意字段个数，结果显示位置可不同)
6. 技巧：cheat sheet、sqlmap
7. Samy蠕虫
8. Beef
9. Console.log(document.cookie)
10. Date +%s | md5sum
11. dom操作
12. Security content automation protocol

自动化扫描工具（验证漏洞存在性）

描述性语言.

1. 分页

\*select \*from users limit 10;

1. single page application
2. 消除风险付出成本
3. php文件包含