1、安装熊海cms的注意事项：

php版本选择5.x

mysql的配置文件my.ini中加上

sql-mode="NO\_AUTO\_CREATE\_USER,NO\_ENGINE\_SUBSTITUTION"

2、安装bluecms的注意事项

php版本选择5.x

安装路径为:域名/uploads/install，安装成功后会跳转到错误页，然后访问：域名/uploads即可

3、常用的xss的payload

<img/src=x>

<svg/onload=alert(1)>

<script>alert(1)</script>等等

4、sql注入，观察url，是否可能带有查询数据库的参数，常用的sql注入命令

报错注入(updatexml(1,concat(0x7e,(select database()),0x7e),1))

判断是否有注入点：and 1=1 ，and 1=2

判断字段数order by 1 等等

5、存在xss漏洞，如何获取管理员的信息，比如cookie，可借助

xss免费平台https://xss8.cc

1. 注册xss免费平台后登陆
2. 创建项目，如bluecms
3. 创建项目后配置代码，选择超强默认模块、基础默认模块，点击配置
4. 点击查看代码，可以看到可以输入的payload
5. 点击项目即可看到获取到的cookie

(6)eg：比如前台注册了一个会员，会员资料中写入了payload，当用管理员登录后台后，打开这个会员的信息，改payload执行，即可获取到管理员的cookie

6、sqlmap工具的使用，该工具可以自动检测是否有sql注入

安装sqlmap

<https://blog.csdn.net/zhongcui8067/article/details/80439934>

如何使用

Pikachu的使用案例<https://www.cnblogs.com/Hunter-01001100/p/11341671.html>