# 二 网络安全实验

1. **实验（分为三个难度）**
2. Command Injection，设定DVWA Security(Low and Medium)------------------2分
3. SQL Injection，设定DVWA Security(Low and Medium)---------------------------1.5分
4. XSS(Stored)，设定DVWA Security(Low and Medium)-----------------------------1.5分

**二、实验目的与要求**

1. 掌握Web漏洞中的命令执行漏洞的形成原理，攻击方法及防御方法。

2. 掌握Web漏洞中的SQL注入漏洞的形成原理，攻击方法及防御方法。

3. 掌握Web漏洞中的XSS漏洞的形成原理，攻击方法及防御方法。

**三、实验环境**

DWVA漏洞实验靶场

Chrome浏览器

**完成对应难度实验即可得对应分数，附录提供了部分网上参考资料。**

**需提交实验报告，实验报告模板已提供。**

**附录：**

**DVWA靶场搭建参考资料：**

https://blog.csdn.net/u013541325/article/details/109323067

https://blog.csdn.net/qq\_45756971/article/details/110001169

**实验参考资料：**

**Command Injection:**

https://www.huaweicloud.com/articles/dc426ba453c835489efdf0a949085033.html

https://www.freebuf.com/articles/web/253231.html

https://www.youtube.com/watch?v=WiqRvlN\_UIU

**SQL Injection:**

https://blog.csdn.net/lady\_killer9/article/details/108983997

<https://levelup.gitconnected.com/ethical-hacking-part-1-owasp-top-10-and-dvwa-3f2d55580ba8>

https://www.youtube.com/watch?v=5bj1pFmyyBA

**XSS(Stored):**

https://www.huaweicloud.com/articles/5a3df7a2d31f711ff69e428dcafabacf.html

https://www.fatalerrors.org/a/dvwa-customs-guide-xss-stored.html

https://levelup.gitconnected.com/ethical-hacking-part-1-owasp-top-10-and-dvwa-3f2d55580ba8

https://www.youtube.com/watch?v=P1I9UGpGdrU

**DVWA靶场登录**

打开浏览器后，在地址栏中输入实验平台的网址，登录的默认用户名是admin，默认密码是password。



图1.1 登录实验平台

首次进入实验平台需要点击Create/Reset Database，初始化数据库。

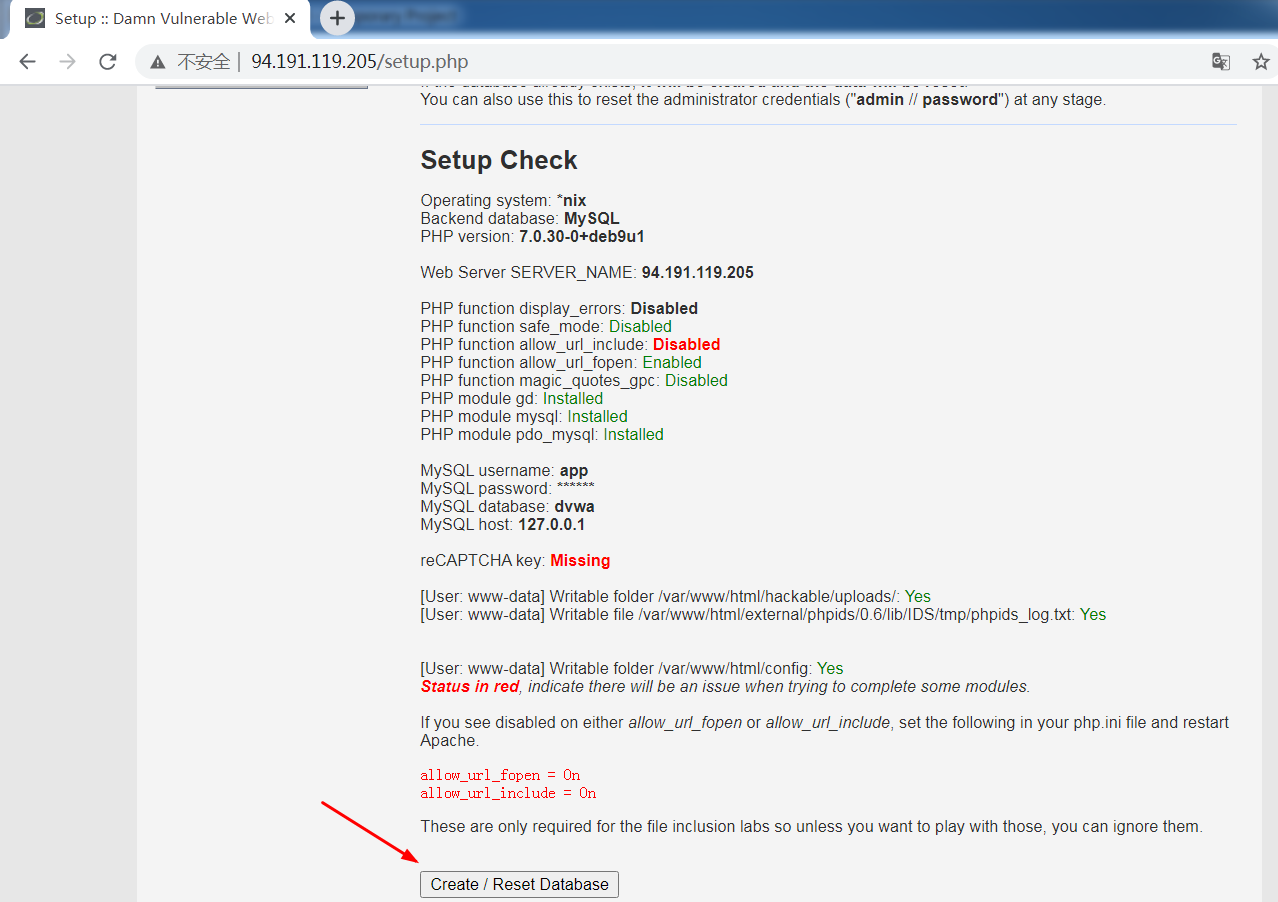


图1.2 实验平台初始化数据库

再次登录后，进入实验平台的主界面。

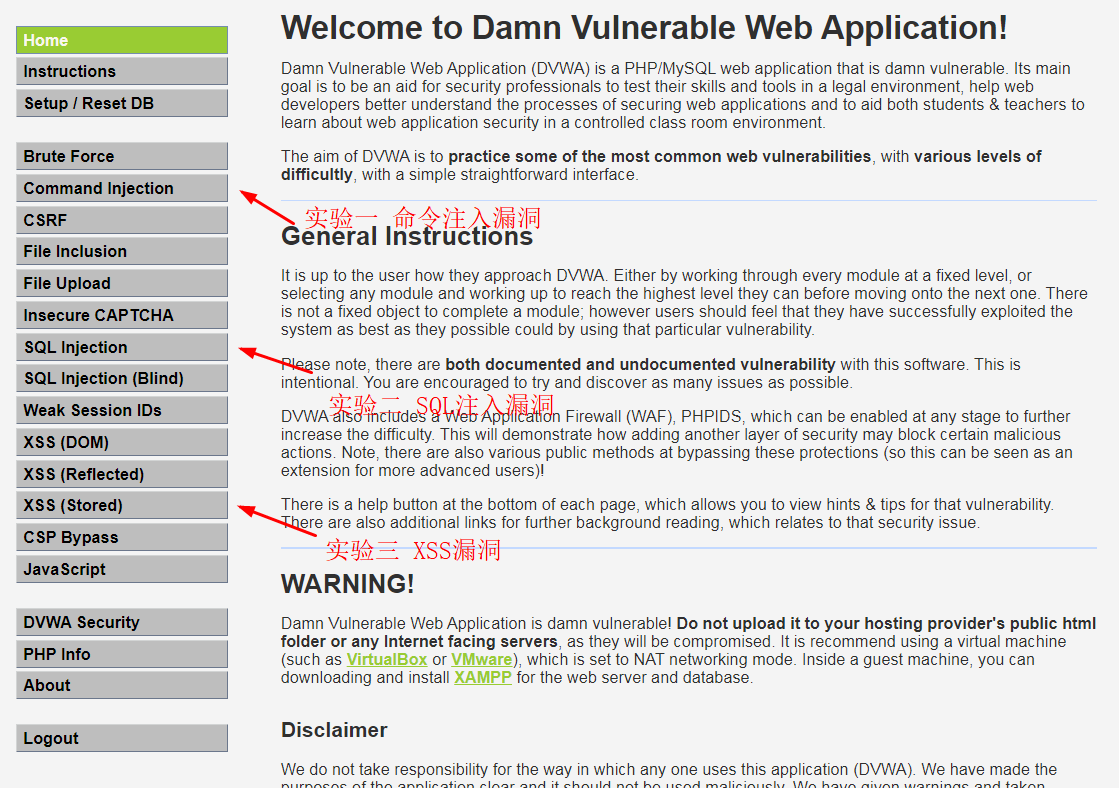


图1.3 实验平台主页面

点击DVWA Security，进入Security Level安全等级设置页面，可以调整难度。

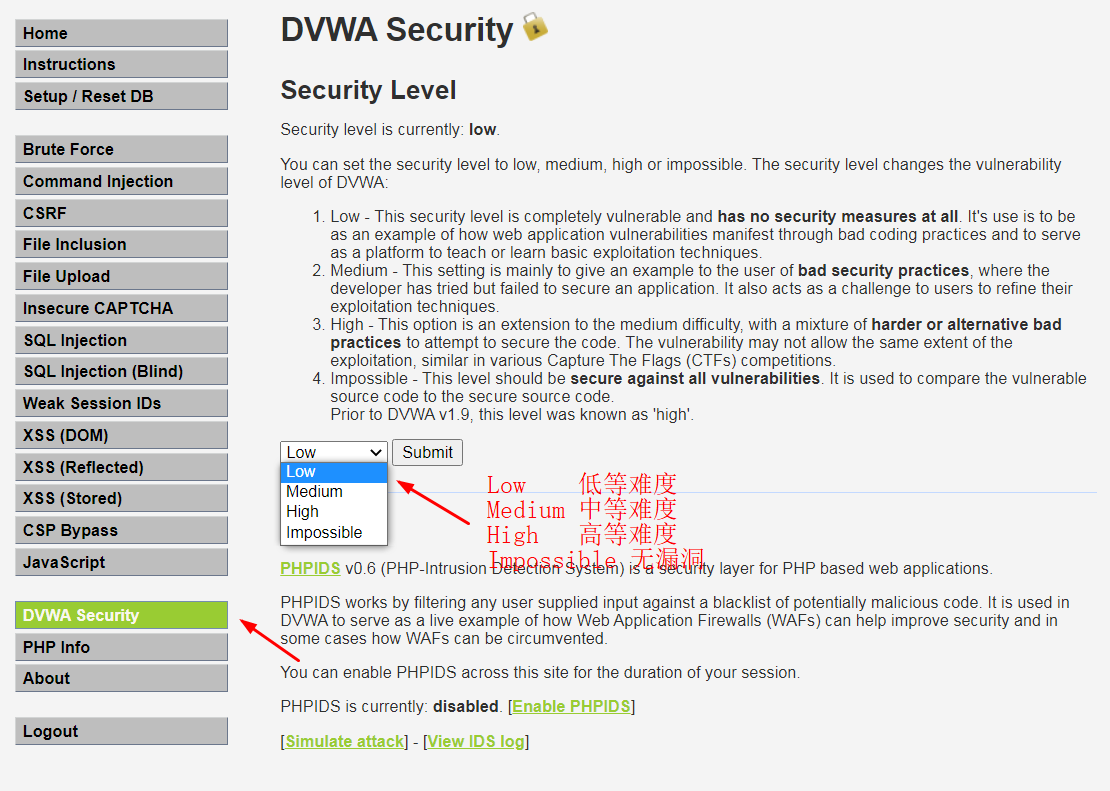


图1.4 实验平台难度调整页面