1. 下载实验素材包

在浏览器中输入地址[http://101.132.145.237:15513](http://101.132.145.237:15513/)

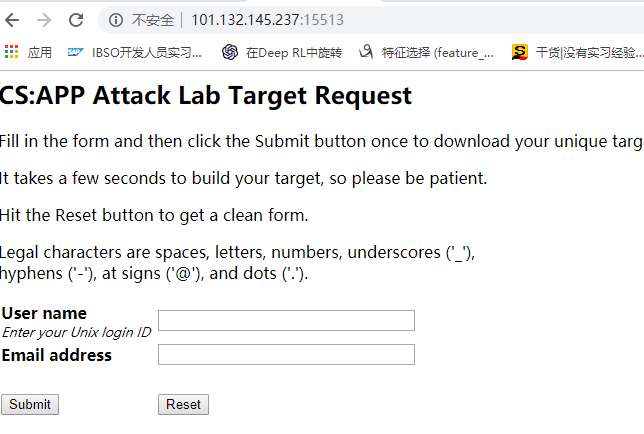
将看到如下图所示。

User name请输入你的学号

Email address输入你的邮箱

然后点击submit下载实验素材包

每个同学的素材包不一样，请不要相互复制使用，很有可能被判0分



1. 查看成绩请前往<http://101.132.145.237:15513/scoreboard>
2. 实验内容及要求如attacklab.pdf所示。

第一部分：代码注入攻击，针对ctarget文件

Level１

在这个等级中，我们不需要注入任何攻击代码，只需要更改getbuf函数的返回地址执行指定的函数touch1（该函数已经存在于程序中）

Level 2

这个等级中我们同样需要跳转到指定的函数touch2

Level 3

该等级同样让我们跳转到touch3函数中

第二部分：返回导向编程攻击，针对rtarget

Level 2

目的与之前的Level 2相同，我们需要为rdi赋上cookie值，再跳转到touch2函数执行

Level 3

攻击目标与之前的Level 3相同，需要将rdi指向cookie的字符串表示的首地址。

1. 温馨提示

gdb里面成功，单独运行失败

需要这条命令sudo echo 0 > /proc/sys/kernel/randomize\_va\_space