**题目信息：**

**题目名称：**EnAdminNo

**旗帜名称：**EAN

**题目描述：**挖掘并利用靶机中的sql注入漏洞、bjyadmin框架漏洞获取目标主机权限，修改主页。

**靶机环境：**Win10 虚拟机，默认安装配置，系统补丁安装至最新。安装运行biyadmin框架（服务端口80，使用www-data权限启动）。靶机配置出站规则，禁止主动访问其他机器。

**附件信息：**附件中包含最新版本的biyadmin源代码、sql注入题目说明。

**展示环境拓扑：**交换机连接选手攻击机和展示机，展示机使用VMware（最新版）运行靶机，靶机通过桥接方式连接到网络。

**验证过程：**选手携带自己的攻击机上台展示题解。选手使用攻击机利用靶机中的sql注入漏洞获取bjyadmin框架路径，进一步利用bjyadmin框架漏洞，修改其bjyadmin管理后台主页/index.php/Admin/Nav/index为如下页面：

|  |
| --- |
| <html><br><br><br><h1 style="font-size:100px;color:red;" align="center">Hacked by "teamname"</h1></html> |

其中teamname请更换为本战队名。操作人员使用展示机浏览器确认页面正确修改后判定成功。

**注意事项：**上台展示题解的时候注意关闭exp的调试信息。

**展示时操作人员操作步骤：**

1. 恢复虚拟机快照到初始状态；
2. 检查虚拟机IP，协助选手连通网络；
3. 等待选手攻击；
4. 确认攻击效果；
5. 在规定时间内可以配合选手重启题目（重置快照）；
6. 攻击成功或超时后：关闭虚拟机、恢复虚拟机快照到初始状态。