记录第一次AWDplus线下--“陇警杯”

原创

墨子辰 于 2021-05-16 22:52:03 发布 2420 收藏 11
分类专栏： 线下比赛记录 文章标签： 安全 渗透测试 网络安全 信息安全

本文链接：https://blog.csdn.net/qq_43277152/article/details/116904048

题比赛介绍

AWDplus和AWD有很大的区别，类似于CTF。只是赛题只有web+pwn，除了正常的打出flag还加上了题目修复。

攻击于防御介绍

1、攻击于防御环节采用动态攻防兼备的比赛模式，综合考核参赛战队的漏洞发现、漏洞挖掘、漏洞修复以及即时策略能力。

2、战队得分：攻防部分积分为攻击得分和防御得分的总分，成功利用漏洞获得flag并提交成功就会再积分轮次内获得该题的攻击分，成功修补漏洞并通过平台check，在积分轮次内就会获得该题的防御分。服务器异常时会被扣分。

3、某参赛队的题目服务器出现异常导致无法进行攻击时，该队伍可点击“重置攻击靶机”按钮进行重置，注意没题重置赛题次数。

4、防御修补：选手可在平台下载题目附件包，包内包含部分或完整的题目源码等文件。选手在本地尝试修补成功后，通过ftp存在修补包（报名xxx.tar.gz，包内需要包含一个update.sh的可执行文件），ftp存在修补包后在界面对应对应题目框内点击申请判定按钮，平台会将修复包上传到防御环境解压并执行update.sh文件，执行平台的check和exp。

5、防御状态判定：check失败则判定防御异常，每轮会扣除200分；check成功、exp成功则判定防御失败，不扣分；check成功、exp失败则判定防御成功，每轮改题目不再失分，且获得防御得分。

6、若某参赛队的题目check判定异常时，该队伍可点击“一键恢复正常”按钮，可消除当前check异常状态，该轮次分值统计时，将不会扣除此次异常分值，注意每题恢复次数。

积分规则

1、所有战队Awdplus的起始分数为5000分，轮次时间为20分钟一轮，每轮比赛题目积分随攻防格局变化而变化，每轮次内有效的攻击和防御都会分别计分。

2、选手攻击自己的靶机，提交正确的flag后，每一轮平台会自动帮助本队攻击其他战队，获取积分，获取的积分为动态分数。

3、选手上传题目修补包后经平台验证成功后，会获取改题目的防御分，题目每轮次防御分值也随题目难度和成功防御队伍数而动态变化。因修补失败造成的题目服务异常，会被扣分。

4、若战队可以为所有的题目提供成功防守且无服务异常，就不会失分。

5、上传防御包导致服务器异常，每轮每题会扣除200分，直到修补成功或修补失败为止，也可以点击“一键恢复正常”恢复服务状态（需要扣去1次恢复次数）。

6、题目攻防得分值随解题队伍数动态衰减。

题目链接

注：题目只有源码，部分题目需要自己搭建数据库等。

链接：AWDplus 比赛题目
提取码：geze

网抑云音乐防御：

```
function waf($str){
        return !preg_match("/\'|http|\"|\`|cookie/", $str);
}

function fetch_data($num){
        $arr = $this->get_all_data();
        $res = array();
        foreach ($arr as $a) {
                if ($a['songID'] == $num){
                        $res[] = $a;
                }
        }
        return ($res);
}
```


首先，这是一个Xss题目。我们找到源码发现waf过滤http、cookie。xss最好的防守方式就是过滤掉<、>、javascript或者直接html实体化编码。这里将尖括号过滤掉成功防守。

```
class DB{

        function waf($str){
                return !preg_match("/\'|http|\"|\`|>|<|cookie/", $str);
        }
```

login_as_admin

这是一个sql盲注的题目，对于sql注入的题，我们只要找到sql语句，过滤掉单引号或者双引号可以防守绝大部分题目。如果还不行，可过滤其它字符，如：select、ascii、or、and、in等等字符。(这里就不一一列举了，只要把sql的语句过滤差不多，就能防守)

```
require_once 'libs/mysql_config.php';
require_once 'libs/flag.php';

function sqlWaf($s)
{
    if (preg_match('/sqlmap/i', $_SERVER['HTTP_USER_AGENT']))
        die;

    $filter = '/xml|extractvalue|regexp|copy|read|file|create|grand|dir|insert|link|server|drop|=|>|<|;|\"|\^|\||\ /i';
    if (preg_match($filter,$s))
        return False;
    return True;
}

function alertMes($mes,$url){
    echo "<script>alert('{$mes}');location.href='{$url}';</script>";
    die;
}
```


这是sqlwaf过滤的字符。

```
if (isset($_POST['username']) && isset($_POST['password'])) {

    $username = strval($_POST['username']);
    $password = strval($_POST['password']);

    if ($username !== 'admin')
    {
        alertMes("you must be admin" ,"./index.php");
    }

    if ( !sqlWaf($password) )
        alertMes('damn hacker' ,"./index.php");

    $password = preg_replace('/select/i', '', $password);

    $sql = "SELECT * FROM users WHERE username='${username}' AND password= '${password}'";
    echo "<!-- " . $sql . "--> ";

    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        $row = $result->fetch_assoc();
        if ( $row['username'] === 'admin' && $row['password'] )
        {
            if ($row['password'] == $password)
            {
                alertMes("Login success:".$FLAG ,"./index.php");
            } else {
                alertMes("Sorry, I haven't let you login" ,"./index.php");
```


上面是查询语句，可以看见username password 都是单引号闭合，也就是说我们只要过滤用户输入的单引号即可避免sql语句报错的问题。也就没办法执行后面输入的sql语句。

```
$filter = '/xml|extractvalue|regexp|copy|read|file|create|grand|dir|insert|link|server|drop|=|>|<|;|\"|\^|\||\
/i';
```

但是我们发现这里的过滤是用单引号来标注的，我们无法在里面闭合单引号。所以我们需要改为：

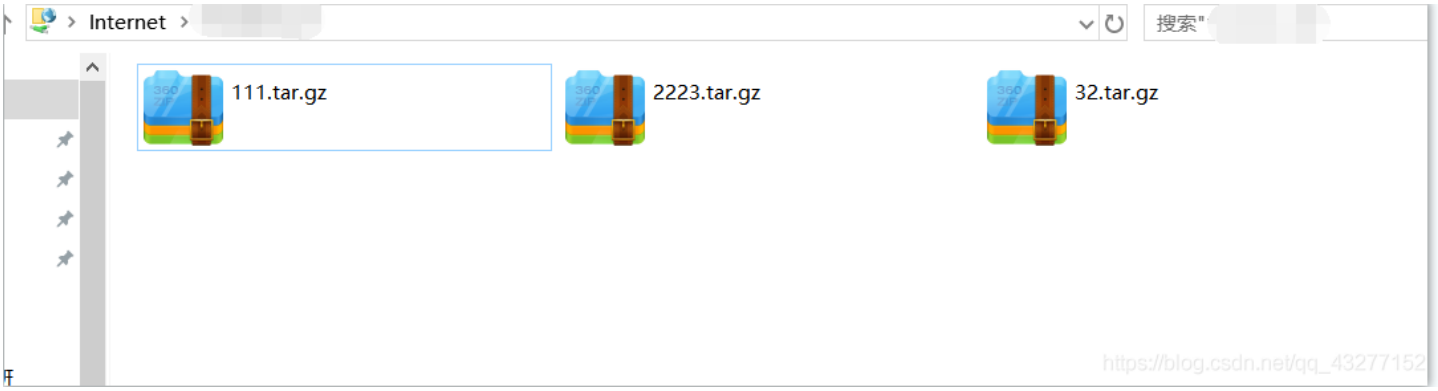
```
$filter = "/xml|extractvalue|regexp|copy|read|file|create|grand|dir|insert|link|server|drop|=|>|<|;|select|union|flag|ascii|subm|right|\'|\^|\||\ /i";
```

自此我们大概了解awdplus玩法了。

接下来就是需要上传修复包的问题了。

上传包需要xx.tar.gz格式文件。

里面包含修改的文件，update.sh可执行文件。（其目的就是执行.sh去替换掉原来环境里面的文件）



ftp连接指定服务器，上传我们修复包。

申请判定后，有显示结果。

如果服务器异常，一定 在本轮次里面恢复环境，要不然进入下一轮后会被扣分。前提是你还有恢复环境的次数。

OK，希望我的记录对你下一次比赛有帮助。