一个完整的渗透测试报道需要很多条件构成

但不同于安全审计 审计是对方公司将源代码交给你

渗透测试报道就是 多角度渗透授权站点 提供的测试报道

一般用于 公司刚上线的站点

出自：[www.91ri.org](http://www.91ri.org) （帮朋友仓促写的，某怪 别怪我是宣传。。。）

作者：kn1f3

邮箱：681796@qq.com

一：授权

以下是授权的站点：<http://www.gXXX.com/> （那里有什么授权，只是模拟下）

授权站点只给了一个站点。。。

二：渗透流程

1：任意文件下载漏洞

2：sql注入漏洞

3：任意文件上传漏洞

4：脚本文件危害

以下是漏洞方面：

因为这个是非常简短的测试报道 ，懒得写格式了 排版很麻烦

漏洞方面就给予一个

漏洞出现在

**/www/hstml/board/lib/down.php 文件 上**

****

**漏洞源代码：**

<?

if(is\_file("../system/db/$db/data/$fname")) {

include "../../DCadmin/system/connect.php";

include "../../DCadmin/dbconn.php";

$ItsTN = $db;

$sql = "select download,file from $ItsTN where uid=$number";

$result = mysql\_query($sql);

$row = mysql\_fetch\_array($result);

$files = explode("-", $row[file]);

$downs = explode("-", $row[downroad]);

for($i=0;$i<sizeof($files);$i++) {

if($files[$i]==$fname) {

if($i==0) {

$tempdown .= strval(intval($downs[$i])+1);

} else {

$tempdown .= "-".strval(intval($downs[$i])+1);

}

} else {

if($i==0) {

$tempdown .= $downs[$i];

} else {

$tempdown .= "-".$downs[$i];

}

}

} // for($i=0;$i<sizeof($files);$i++) 끝

$dosql = "update $ItsTN set download='$tempdown' where uid=$number";

$doresult = mysql\_query($dosql);

$filename = $fname;

$filetype = $ftype;

$filesize = $fsize;

$file\_path = "../system/db/$db/data/".$filename;

$fname = str\_replace($number."\_","",$filename);

// 20040605 수정 - by qoren

if(strstr($HTTP\_USER\_AGENT, "MSIE 5.5")) {

header("Content-Type:application/unknown");

header("Content-Disposition:filename=$fname");

header("Content-Transfer-Encoding: binary");

header("Pragma: no-cache");

header("Expires: 0");

}

else {

Header("Content-type: application/unknown");

Header("Content-Disposition: attachment; filename=$fname");

Header("Content-Description: PHP3 Generated Data");

header("Pragma: no-cache");

header("Expires: 0");

}

//. Header("Content-Disposition:attachment;filename=$fname");

//. Header("Content-Transfer-Encoding:binary");

//. Header("Pragma:no-cache");

//. Header("Expires:0");

//. fpassthru($fp)

//. fclose($fp);

// echo $filename.'<br>';

// echo $filesize.'<br>';

// echo $filetype.'<br>';

// echo $file\_path.'<br>';

// echo $fname.'<br>';

// echo "c";

if (is\_file("$file\_path")) {

$fp = fopen("$file\_path", "rb");

if (!fpassthru($fp))

fclose($fp);

}

// 수정 끝

} else {

echo "<script>alert('파일이 존재 하지 않아서 다운받으실 수 없습니다');history.go(-1);</script>";

exit;

}

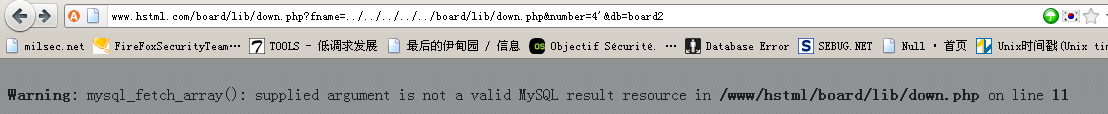
?>

可以看见 $fname 变量可控 造成了 任意文件下载漏洞

更为可笑的事 居然还带入了 sql 查询

通过操控 $number

导致 mysql 注入漏洞



漏洞证明：

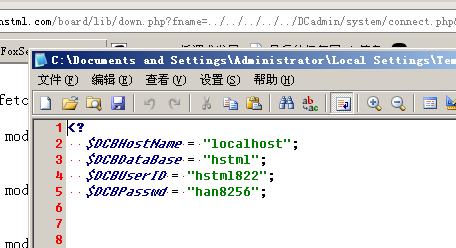
Current User: hstml822@localhost

Sql Version: 4.0.27-log

漏洞的危害性 高

通过任意文件下载漏洞

我们下载到了他的数据库连接串



$DCBHostName = "localhost";

$DCBDataBase = "hstml";

$DCBUserID = "hxxx";

$DCBPasswd = "haxxx";

通过有关文件下载

找到后台地址

<http://www.xxxxxx.com/super/index.php>

<tr><form name="sFm" action="alogin\_ok.php" method="post" onSubmit="return alogin\_ck();">

<td>

<table cellpadding=0 cellspacing=0 border=0>

<tr valign=top>

<td width=100><img src="img/login\_id.gif" width=100 height=25></td>

<td width=115><input type="text" name="admin\_id" size=15 maxlength=20 class="inpt" autocomplete="off"></td>

</tr>

<tr>

<td colspan=2><img src="img/blank.gif" width="1" height="5"></td>

</tr>

<tr valign=top>

<td><img src="img/login\_pass.gif" width="100" height="25"></td>

<td><input type="password" name="admin\_pwd" size=15 maxlength=20 class="inpt" autocomplete="off"></td>

</tr

Post提交给 alogin\_ok.php 文件

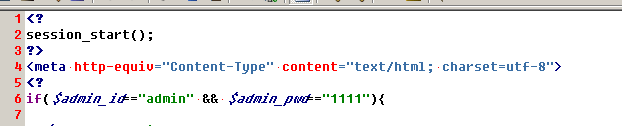
通过下载后台验证文件 进入后台

账号密码 储存在 后台验证文件中

证明：

Admin

1111



“话说回来 ，棒子密码 十个有九个都是 1111 我擦你妹”

进入后台后 查看了 后台上传文件

利用任意下载文件查看了 路径

/DCShop/system/Cates2/



尼玛 不仅是任意下载 还尼玛的任意上传啊 棒子国度 你伤不起啊。。。

成功了拿到web权限



渗透测试报道 一般对 一个大型网络 和 数据库 的一些渗透

找出各种漏洞 已经检测各种有危害性的东西

最重要的 还有内网之间的联系 数据库之间的安全

等等 所以 渗透测试报道 基本上 是有很大的篇幅

这边只是给新手学习下 顶多就算一篇 入侵文章吧

另附：渗透测试报道格式一枚

**目录**

[1. 概述 4](#_Toc29255)

[1.1. 工作说明 4](#_Toc16658)

[1.2. 渗透范围 4](#_Toc10541)

[2. 渗透测试步骤 4](#_Toc18773)

[2.1. 渗透测试流程 4](#_Toc7585)

[2.2. 信息收集阶段 5](#_Toc2022)

[2.3. 信息分析阶段 5](#_Toc17228)

[2.4. 模拟测试阶段 5](#_Toc21348)

[2.5. 测试结果记录 6](#_Toc2417)

[3. 风险状况概述 6](#_Toc27839)

[3.1. xxxxx.com 6](#_Toc18722)

[3.2. xxxxxxx.cn 8](#_Toc7423)

[4. 漏洞总结和建议 13](#_Toc12938)

[4.2. 安全建议 14](#_Toc6647)

1. 概述
   1. 工作说明

XXXX科技股份有限公司授权XXXX - 对如下地址：xxxxx.cn及子域名进行渗透测试。

XXXX科技股份有限公司的渗透测试工作开始于200x年xx月xx日至xx月xx日，所有的渗透工作过程都是测试人员以黑盒形式 。

* 1. 渗透范围

渗透测试涉及的范围仅限于XXXX科技股份有限公司提供域名及子域名进行渗透测试，不包含该应用系统服务器中其他的网站的渗透。不对任何超于授权范围内的网站进行评估。