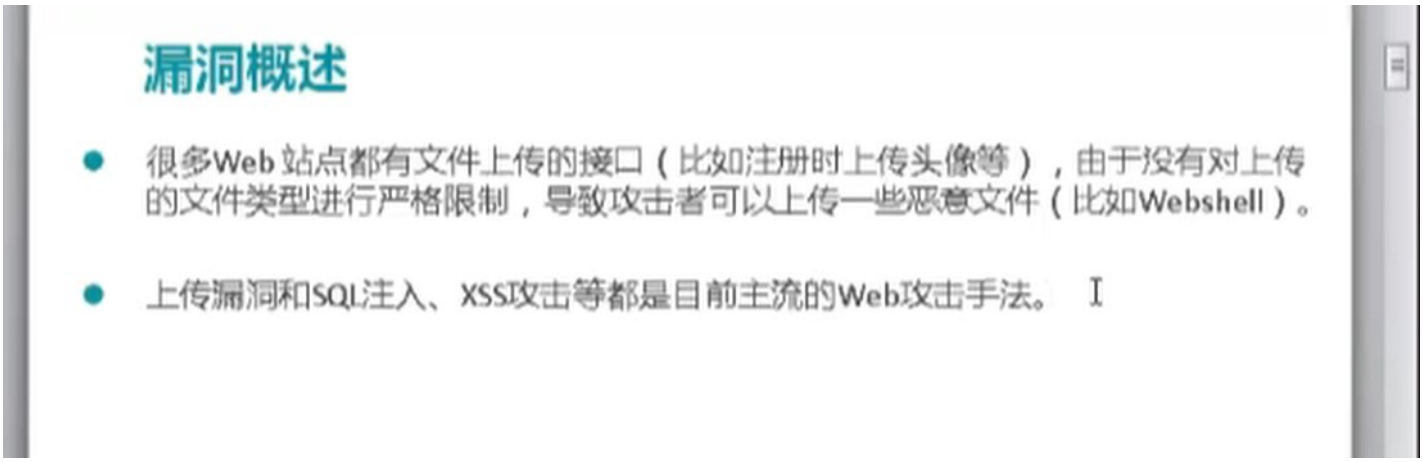
定义




```php
<?php
   if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";//这个变量保存的是上
            $target_path = $target_path . basename( $_FILES['uploaded']['name']);//这里

            if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {//

                echo '<pre>';
                echo 'Your image was not uploaded.';
                echo '</pre>';

              } else {

                echo '<pre>';
                echo $target_path . ' succesfully uploaded!';
                echo '</pre>';

            }

        }
?>
```

代码分析

$_FILES变量专门用于获取上传文件的各种信息。

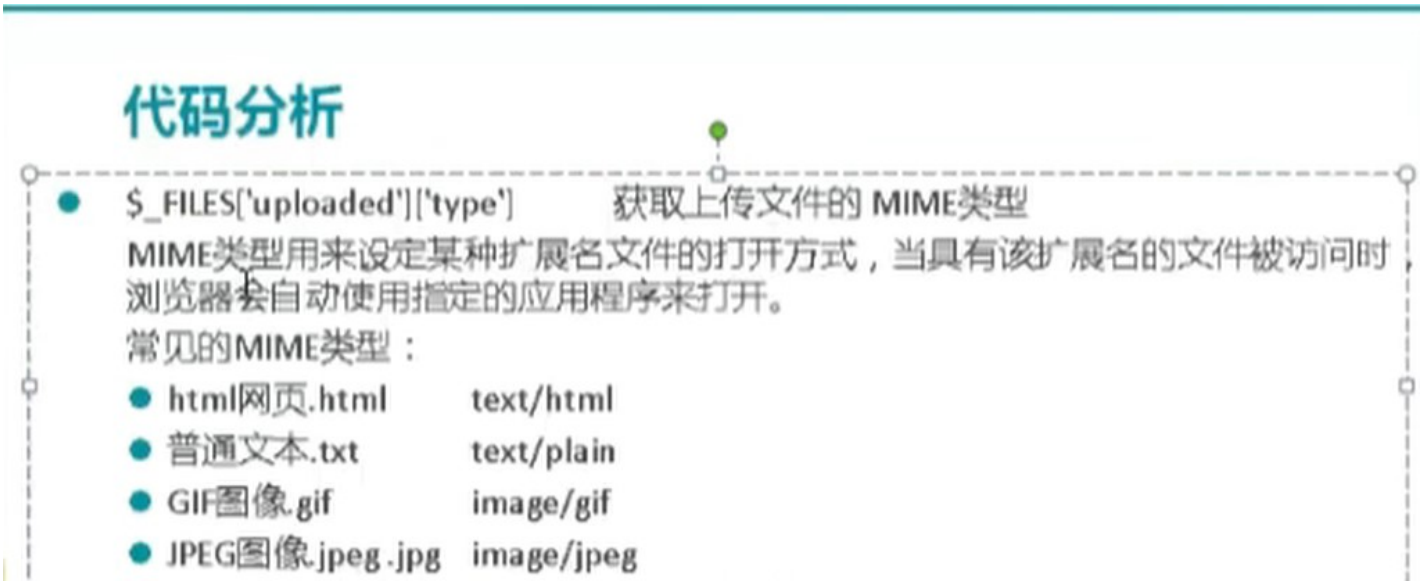
- $_FILES['uploaded']['name']，获取客户端文件的原名称；
- $_FILES['uploaded']['tmp_name']"，获取文件被上传后在服务端存储的临时文件名。

- $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
  指定文件上传路径为 "网站根目录/hackable/uploads"
- $target_path = $target_path . basename($_FILES['uploaded']['name']);
  指定上传之后的文件名及保存路径

中级

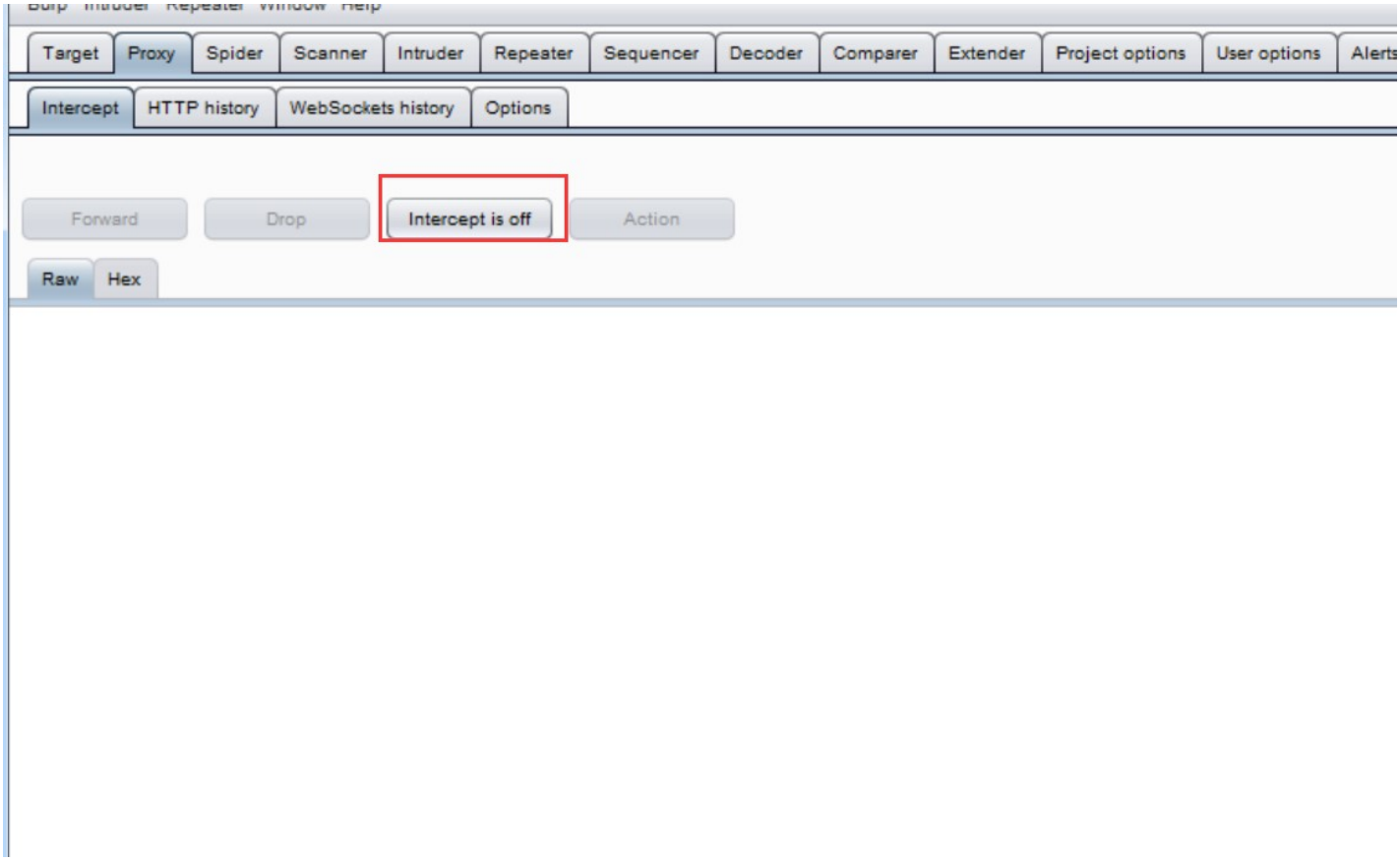
```php
<?php
   if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename($_FILES['uploaded']['name']);
            $uploaded_name = $_FILES['uploaded']['name'];
            $uploaded_type = $_FILES['uploaded']['type'];
            $uploaded_size = $_FILES['uploaded']['size'];

            if (($uploaded_type == "image/jpeg") && ($uploaded_size < 100000)){


                if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)

                    echo '<pre>';
                    echo 'Your image was not uploaded.';
                    echo '</pre>';

                  } else {

                    echo '<pre>';
                    echo $target_path . ' succesfully uploaded!';
                    echo '</pre>';

                    }
            }
            else{
```

```
28                 echo '<pre>Your image was not uploaded.</pre>';
29             }
30         }
31 ?>
```

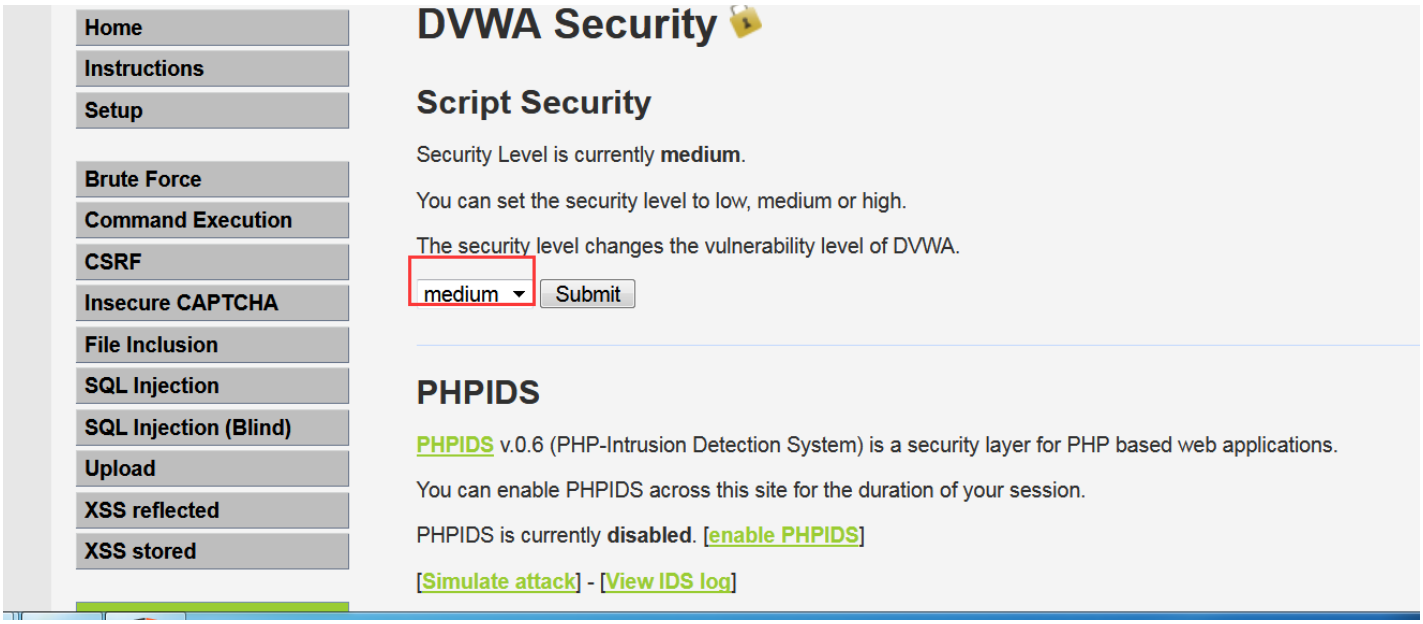


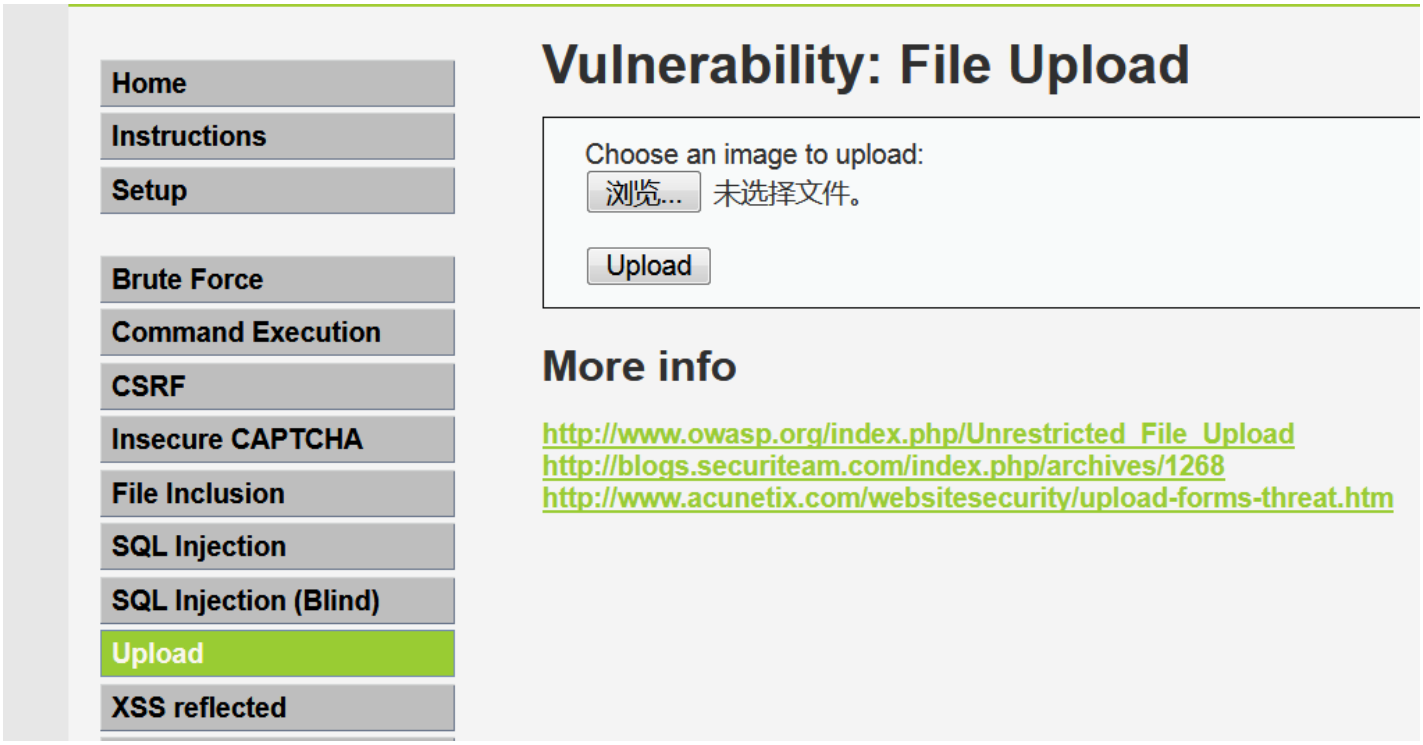
一个例子

设置代理

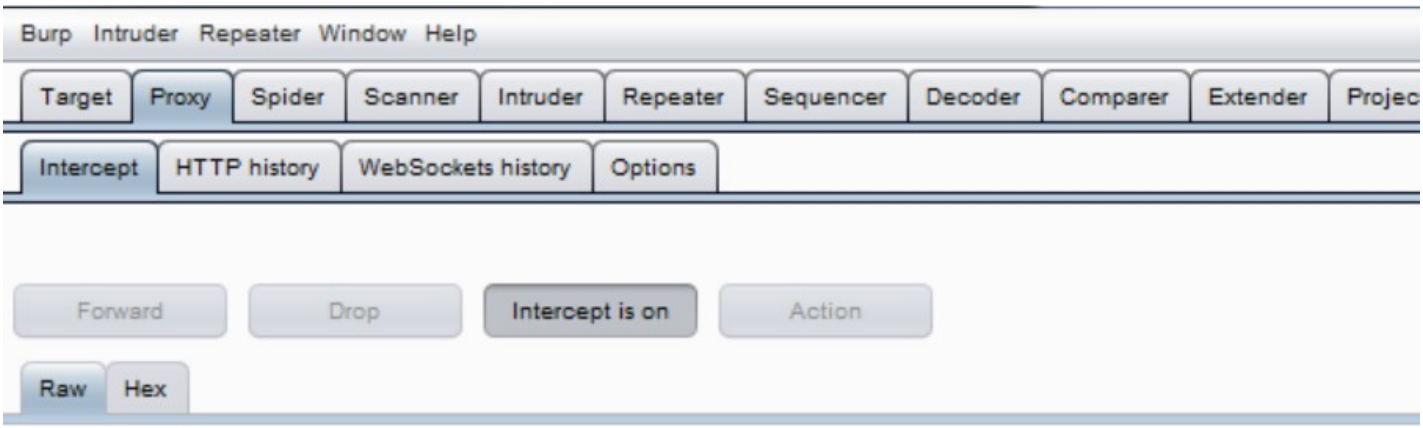

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is off
Action
Raw
Hex

设置为中级：

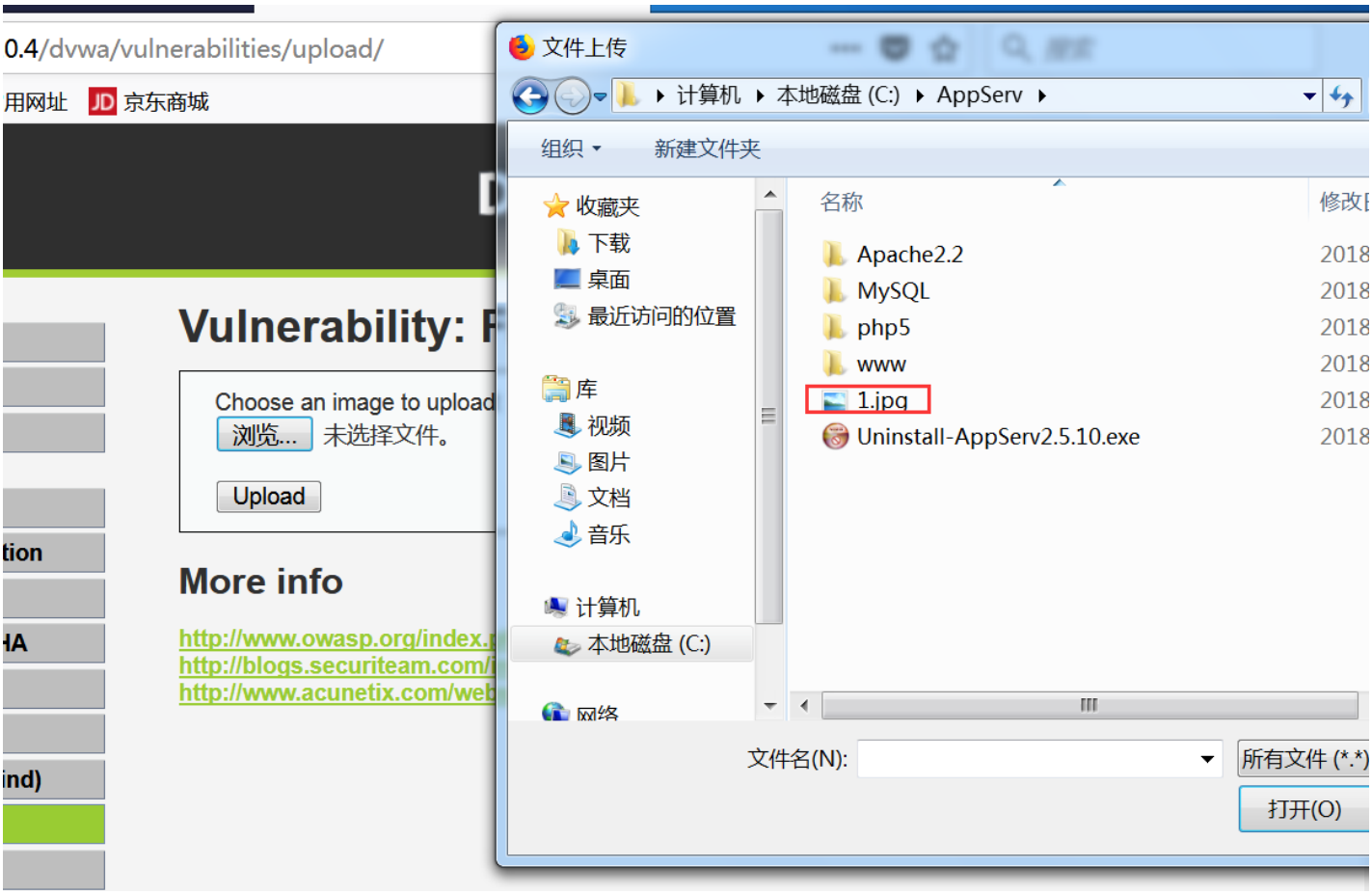

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Script Security
Security Level is currently medium.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
medium
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]


Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
Vulnerability: File Upload
Choose an image to upload:
浏览...
未选择文件。
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

打开拦截:

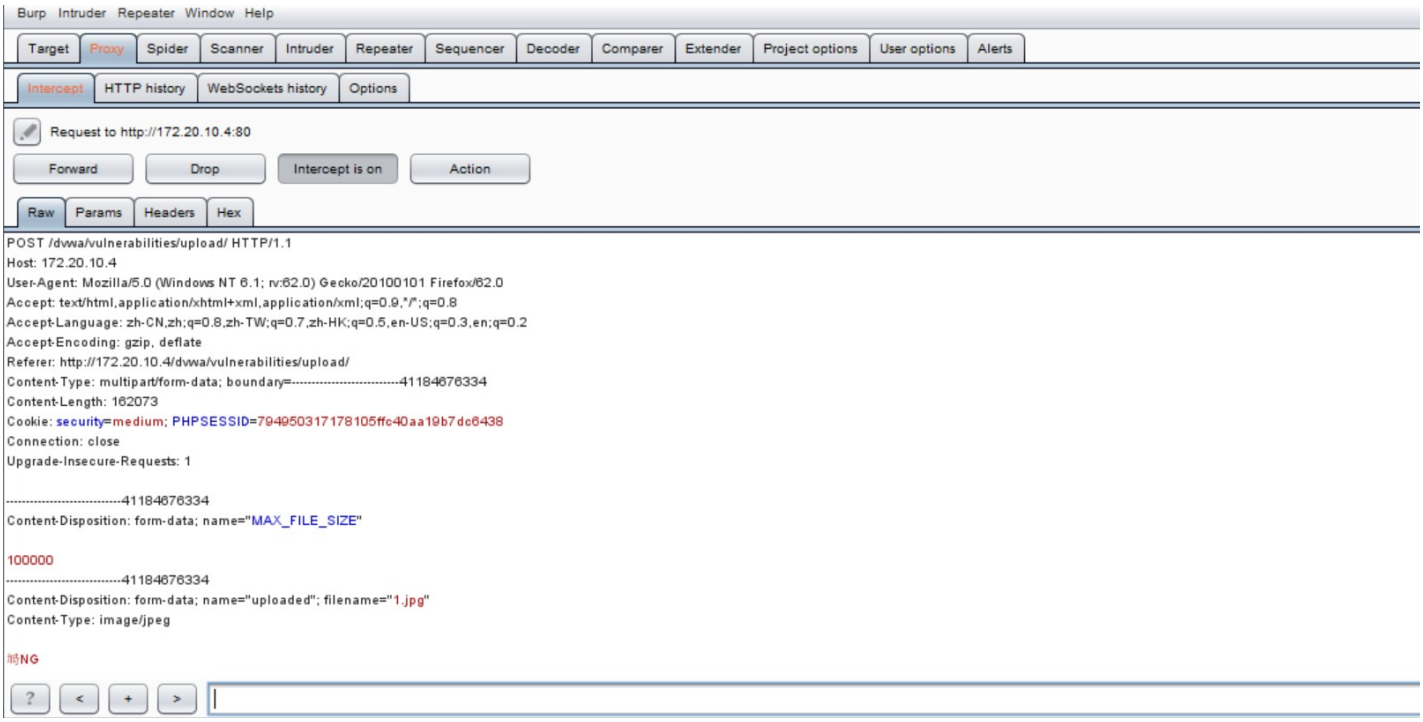

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Hex

上传:


0.4/dvwa/vulnerabilities/upload/
用网址
京东商城
Vulnerability: F
Choose an image to upload
浏览...
未选择文件。
Upload
More info
http://www.owasp.org/index.
http://blogs.securiteam.com/
http://www.acunetix.com/web
文件上传
计算机 ▸ 本地磁盘 (C:) ▸ AppServ ▸
组织
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
网络
名称
修改日
Apache2.2 2018
MySQL 2018
php5 2018
www 2018
1.jpg 2018
Uninstall-AppServ2.5.10.exe 2018
文件名(N):
所有文件 (*.*)
打开(O)


最常访问
火狐官方站点
新手上路
常用网址
京东商城
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
Vulnerability: File Upload
Choose an image to upload:
浏览...
1.jpg
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268

可以看到:

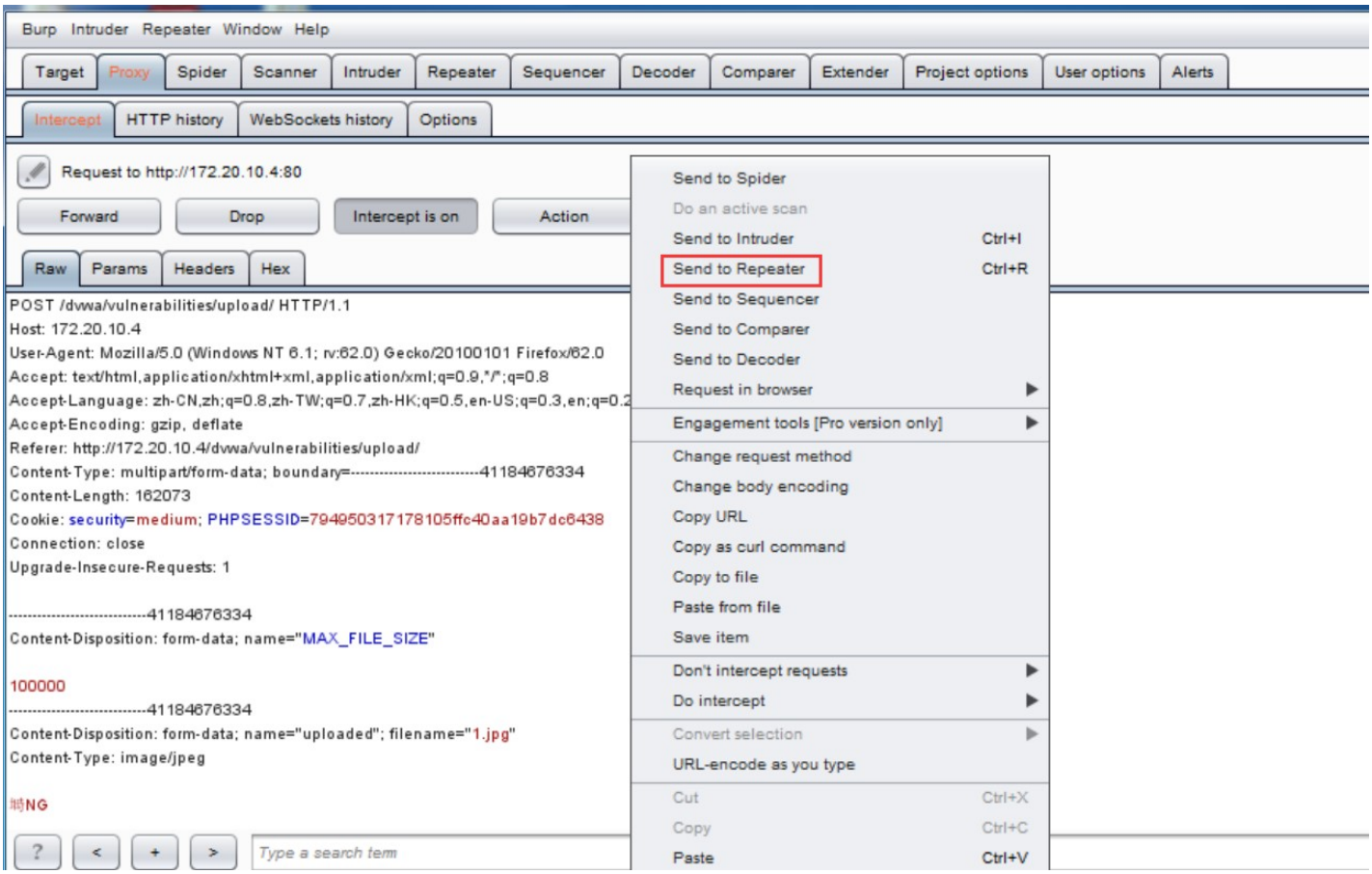


host:就是访问的目标网站;

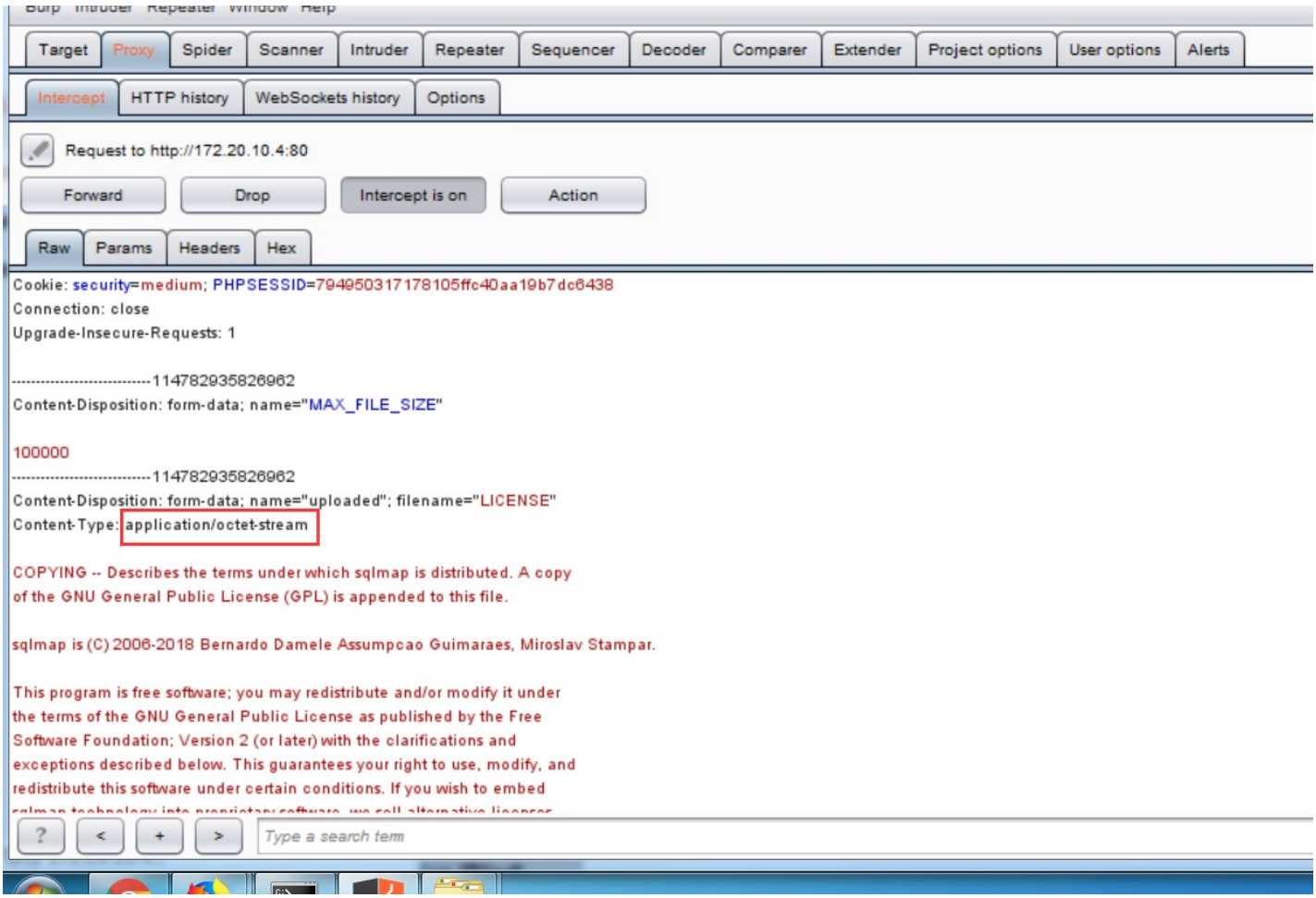
referer:是访问目标站点之前的那个url;

这里的content-type就是mil类型;刚才的那个$_FileS获取的就是这个;

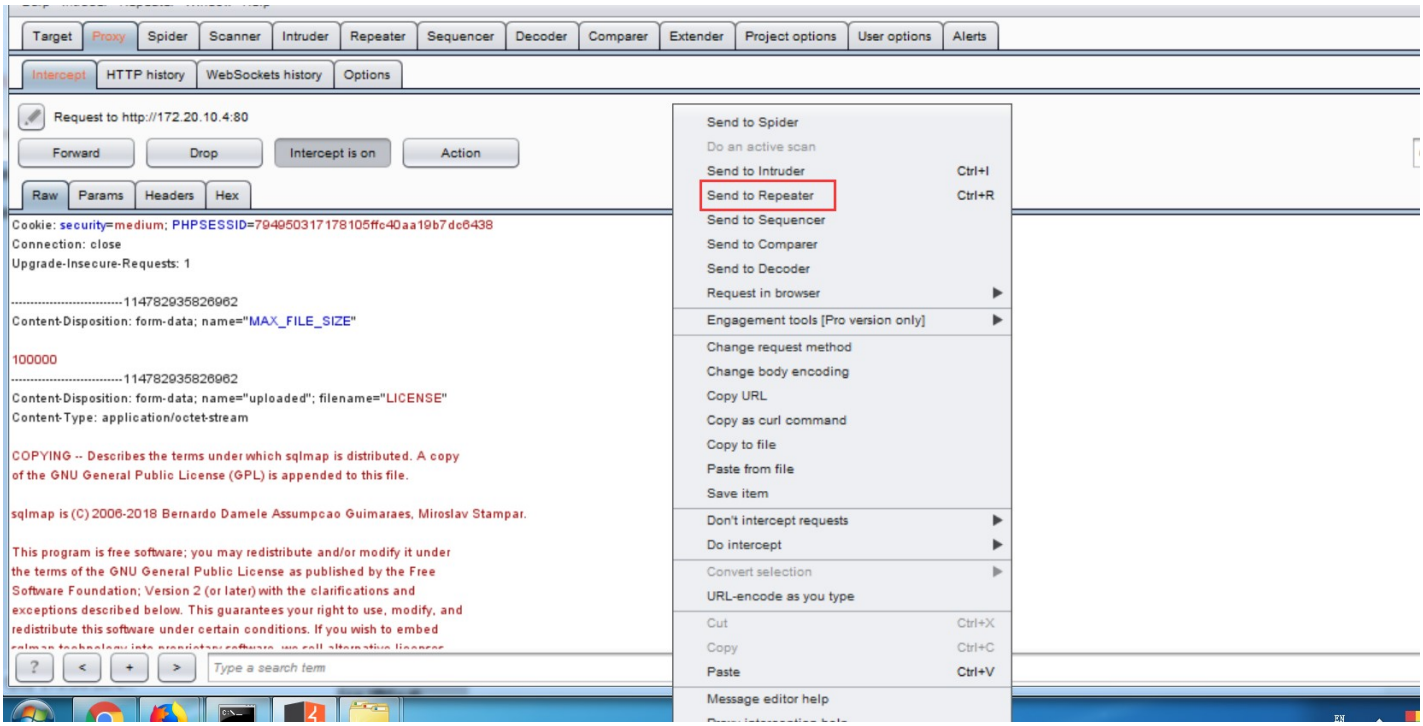
为了绕过(如果不是image/jpeg类型),可以右击-->send to repeater;



下面这个上传的不是image/jpeg这个类型:



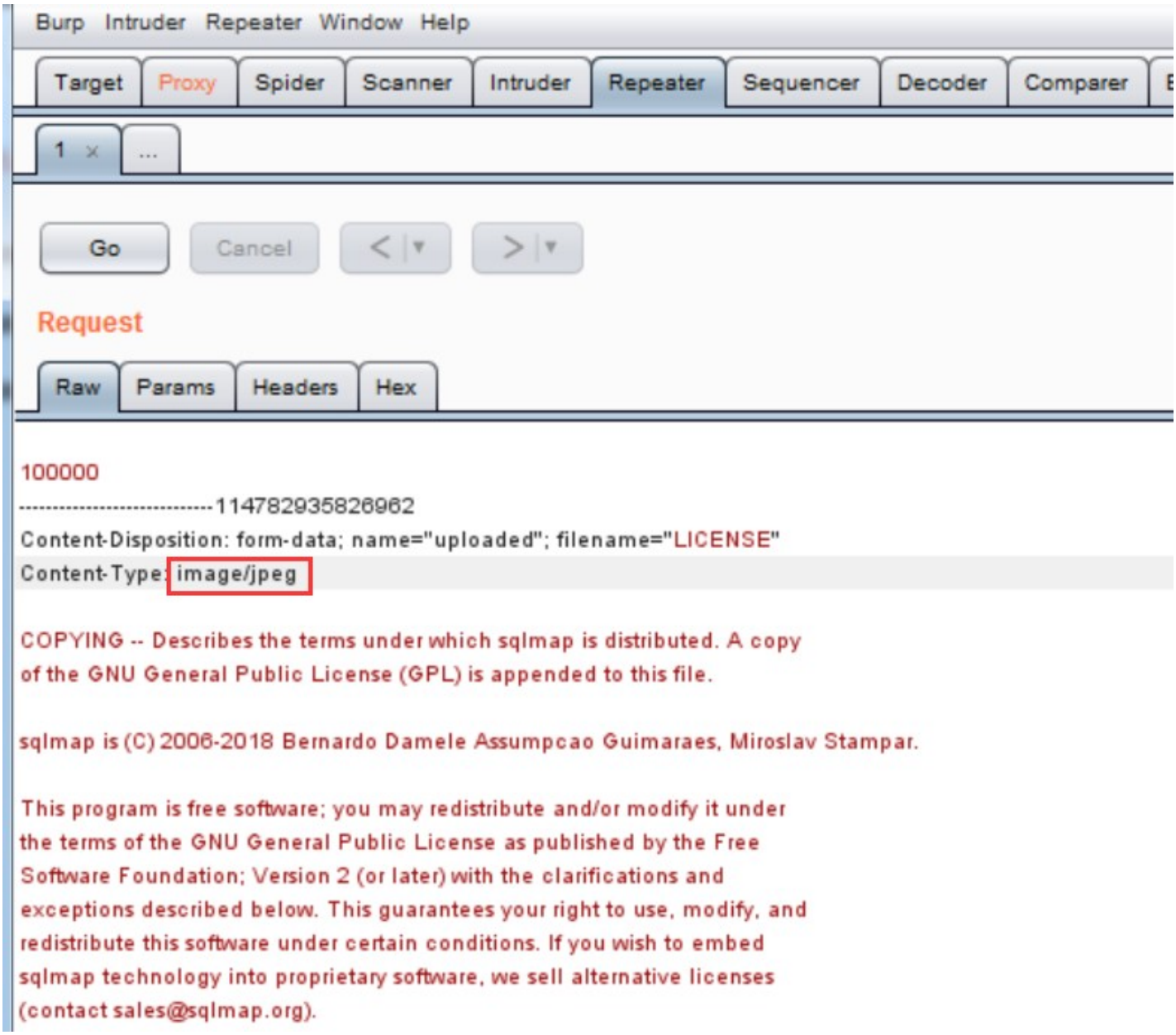
send to repeater：



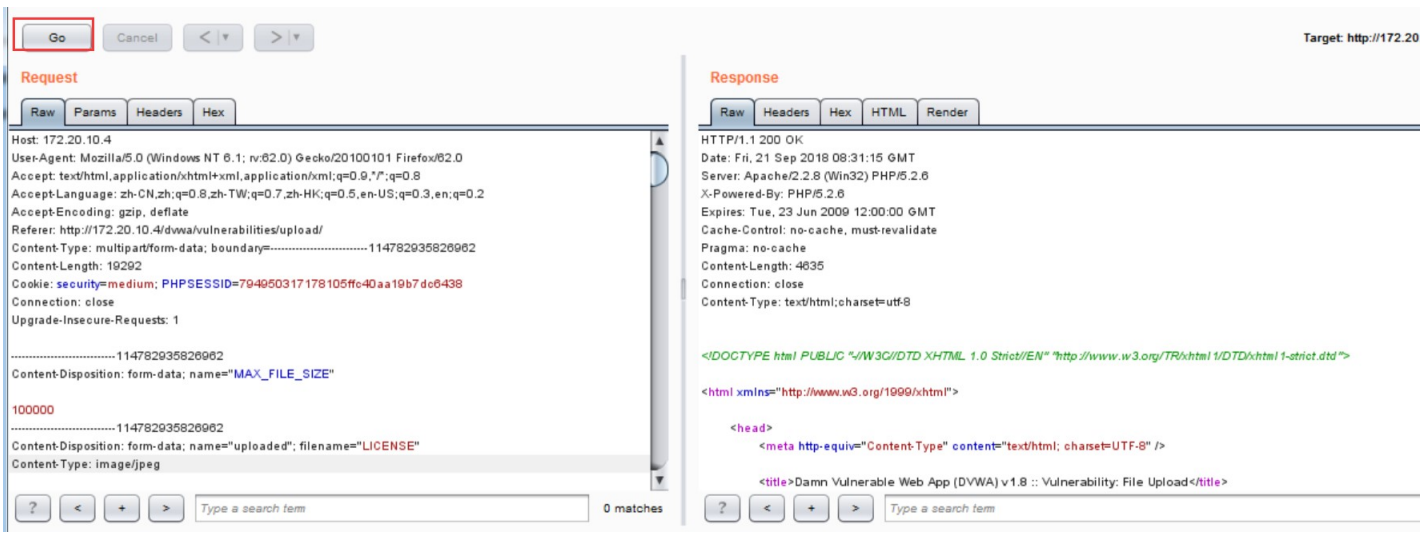
repeater这个模块适合改包！！！

intruder适合暴力破解！

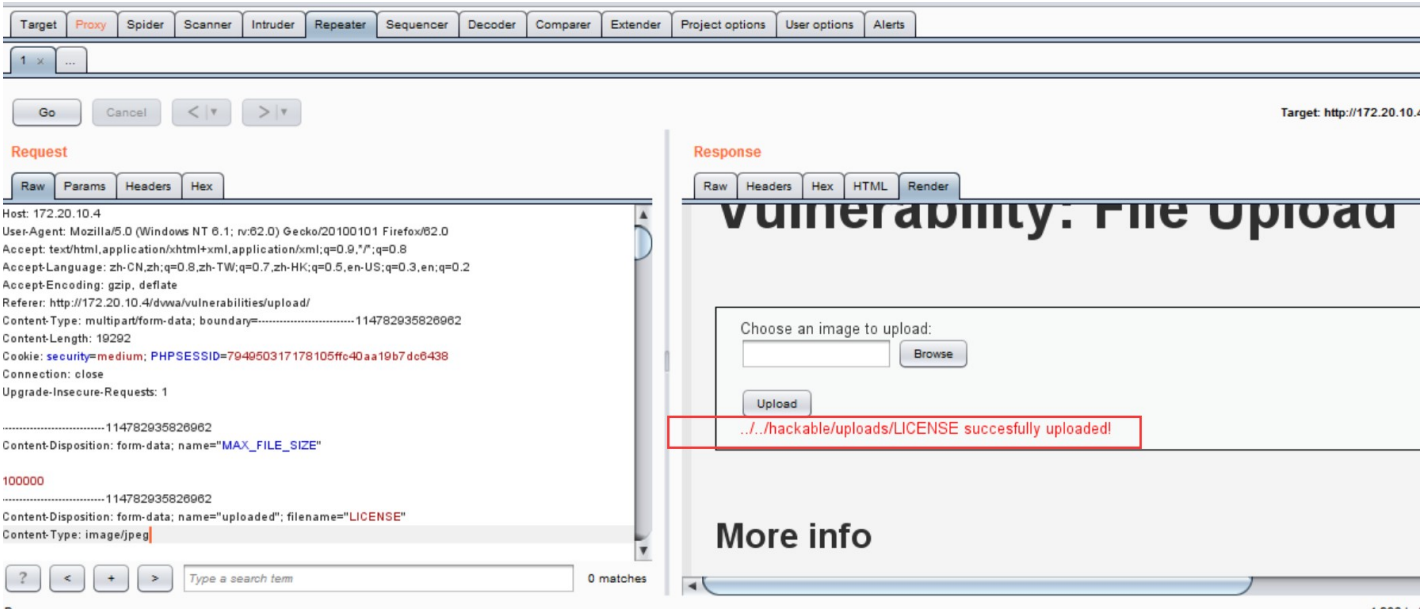
改包:


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
1 ...
Go Cancel
Request
Raw Params Headers Hex
100000
----------114782935826962
Content-Disposition: form-data; name="uploaded"; filename="LICENSE"
Content-Type: image/jpeg
COPYING -- Describes the terms under which sqlmap is distributed. A copy
of the GNU General Public License (GPL) is appended to this file.
sqlmap is (C) 2006-2018 Bernardo Damele Assumpcao Guimaraes, Miroslav Stampar.
This program is free software; you may redistribute and/or modify it under
the terms of the GNU General Public License as published by the Free
Software Foundation; Version 2 (or later) with the clarifications and
exceptions described below. This guarantees your right to use, modify, and
redistribute this software under certain conditions. If you wish to embed
sqlmap technology into proprietary software, we sell alternative licenses
(contact sales@sqlmap.org).

go一下:


Go Cancel
Target: http://172.20
Request
Raw Params Headers Hex
Host: 172.20.10.4
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.20.10.4/dvwa/vulnerabilities/upload/
Content-Type: multipart/form-data; boundary=----------114782935826962
Content-Length: 19292
Cookie: security=medium; PHPSESSID=794950317178105ffc40aa19b7dc6438
Connection: close
Upgrade-Insecure-Requests: 1
----------114782935826962
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
----------114782935826962
Content-Disposition: form-data; name="uploaded"; filename="LICENSE"
Content-Type: image/jpeg
Type a search term
0 matches
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 21 Sep 2018 08:31:15 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 4635
Connection: close
Content-Type: text/html;charset=utf-8
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Damn Vulnerable Web App (DVWA) v1.8 :: Vulnerability: File Upload</title>
Type a search term

绕过成功:



高级:

```php
 <?php
if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename($_FILES['uploaded']['name']);
            $uploaded_name = $_FILES['uploaded']['name'];
            $uploaded_ext = substr($uploaded_name, strrpos($uploaded_name, '.') + 1);
            $uploaded_size = $_FILES['uploaded']['size'];

            if (($uploaded_ext == "jpg" || $uploaded_ext == "JPG" || $uploaded_ext ==


                if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)

                    echo '<pre>';
                    echo 'Your image was not uploaded.';
                    echo '</pre>';

                  } else {

                    echo '<pre>';
                    echo $target_path . ' succesfully uploaded!';
                    echo '</pre>';

                    }
            }

            else{
```

```
29
30                  echo '<pre>';
31                  echo 'Your image was not uploaded.';
32                  echo '</pre>';
33
34              }
35          }
36
37  ?>
38
```