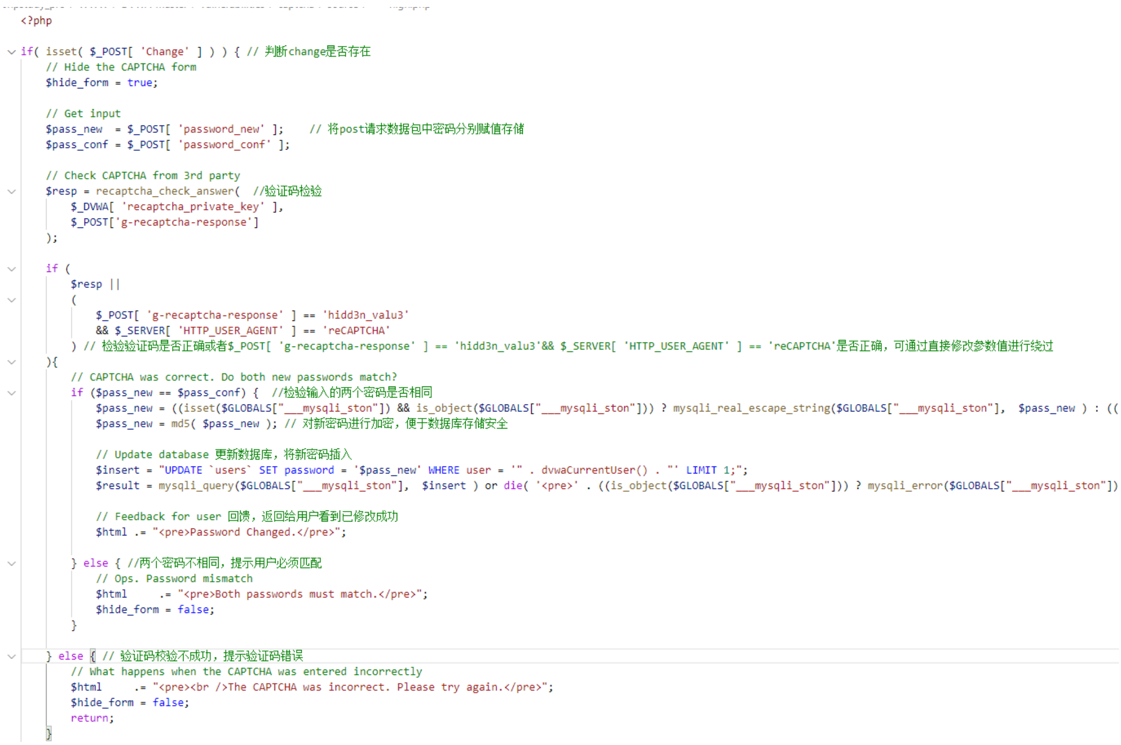
20200805信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/5 11:36	**更新时间:**	2020/8/5 17:59
作者:	820410740@qq.com		
URL:	about:blank		

对DVWA captcha php代码低中高三个级别进行代码分析
（主要逻辑 主要判断方法 如何判断代码最后是否成功）

高级别

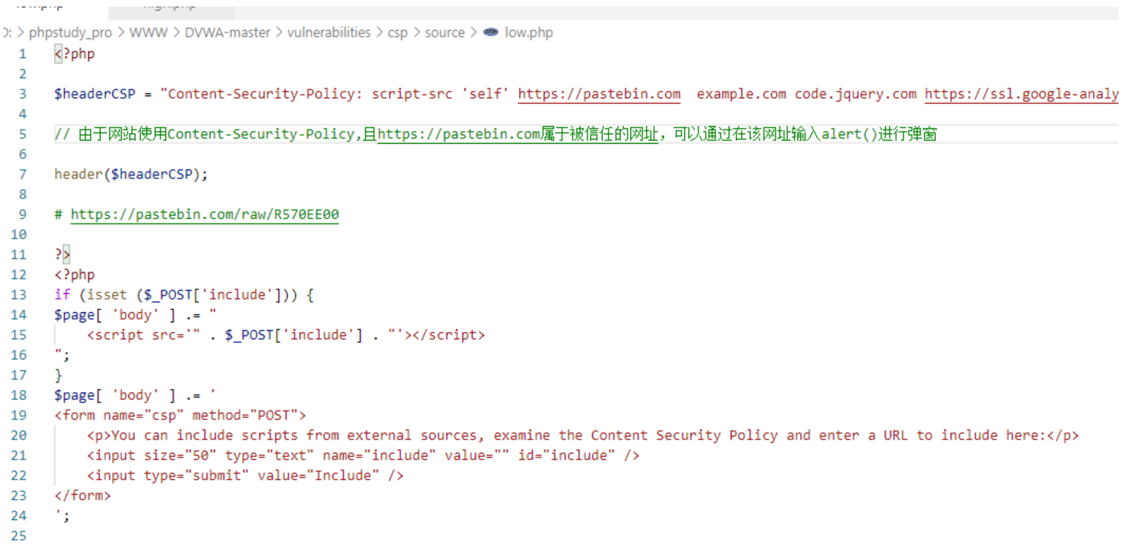


```php
<?php

if( isset( $_POST[ 'Change' ] ) ) { // 判断change是否存在
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new  = $_POST[ 'password_new' ];    // 将post请求数据包中密码分别赋值存储
    $pass_conf = $_POST[ 'password_conf' ];

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

    if (
        $resp ||
        (
            $_POST[ 'g-recaptcha-response' ] == 'hidd3n_valu3'
            && $_SERVER[ 'HTTP_USER_AGENT' ] == 'reCAPTCHA'
        ) // 检验验证码是否正确或者$_POST[ 'g-recaptcha-response' ] == 'hidd3n_valu3'&& $_SERVER[ 'HTTP_USER_AGENT' ] == 'reCAPTCHA'是否正确，可通过直接修改参数值进行绕过
    ){
        // CAPTCHA was correct. Do both new passwords match?
        if ($pass_new == $pass_conf) {  //检验输入的两个密码是否相同
            $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $pass_new ) : ((
            $pass_new = md5( $pass_new ); // 对新密码进行加密，便于数据库存储安全

            // Update database 更新数据库，将新密码插入
            $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "' LIMIT 1;";
            $result = mysqli_query($GLOBALS["___mysqli_ston"],  $insert ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"])

            // Feedback for user 回馈，返回给用户看到已修改成功
            $html .= "<pre>Password Changed.</pre>";

        } else { //两个密码不相同，提示用户必须匹配
            // Ops. Password mismatch
            $html     .= "<pre>Both passwords must match.</pre>";
            $hide_form = false;
        }

    } else { // 验证码校验不成功，提示验证码错误
        // What happens when the CAPTCHA was entered incorrectly
        $html     .= "<pre><br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }
```

pikachu第一关的代码分析

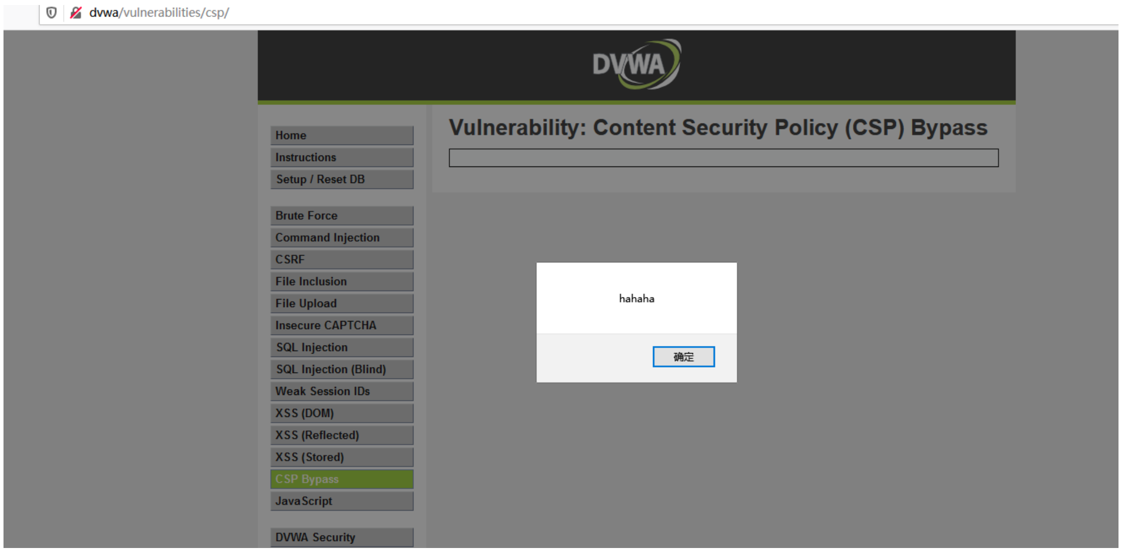
https://cloud.tencent.com/developer/section/1189876

csp-bypass low



phpstudy_pro > WWW > DVWA-master > vulnerabilities > csp > source > low.php

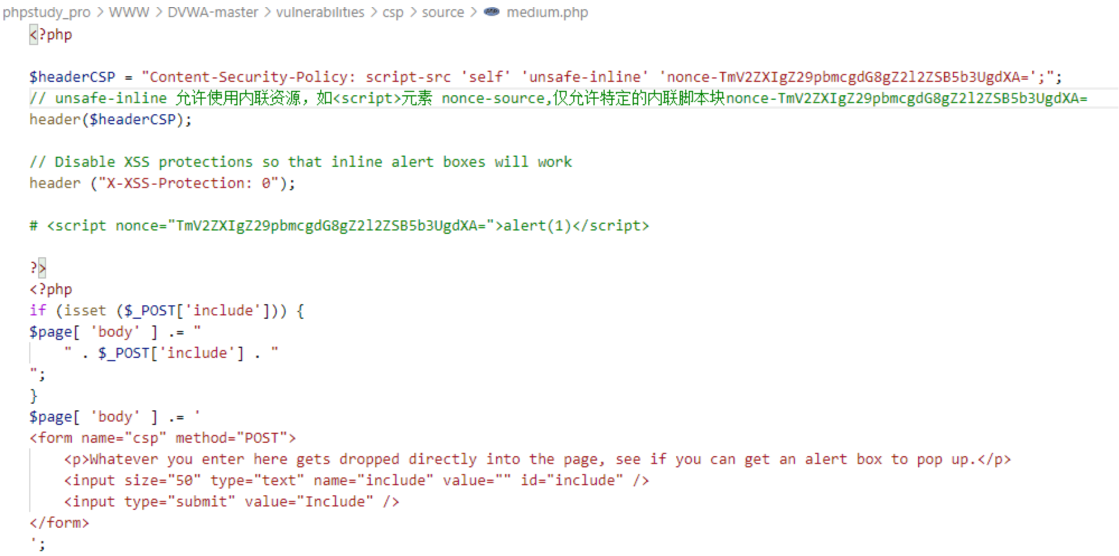
```
<?php

$headerCSP = "Content-Security-Policy: script-src 'self' https://pastebin.com  example.com code.jquery.com https://ssl.google-analy

// 由于网站使用Content-Security-Policy,且https://pastebin.com属于被信任的网址，可以通过在该网址输入alert()进行弹窗

header($headerCSP);

# https://pastebin.com/raw/R570EE00

?>
<?php
if (isset ($_POST['include'])) {
$page[ 'body' ] .= "
    <script src='" . $_POST['include'] . "'></script>
";
}
$page[ 'body' ] .= '
<form name="csp" method="POST">
    <p>You can include scripts from external sources, examine the Content Security Policy and enter a URL to include here:</p>
    <input size="50" type="text" name="include" value="" id="include" />
    <input type="submit" value="Include" />
</form>
';

```



Vulnerability: Content Security Policy (CSP) Bypass

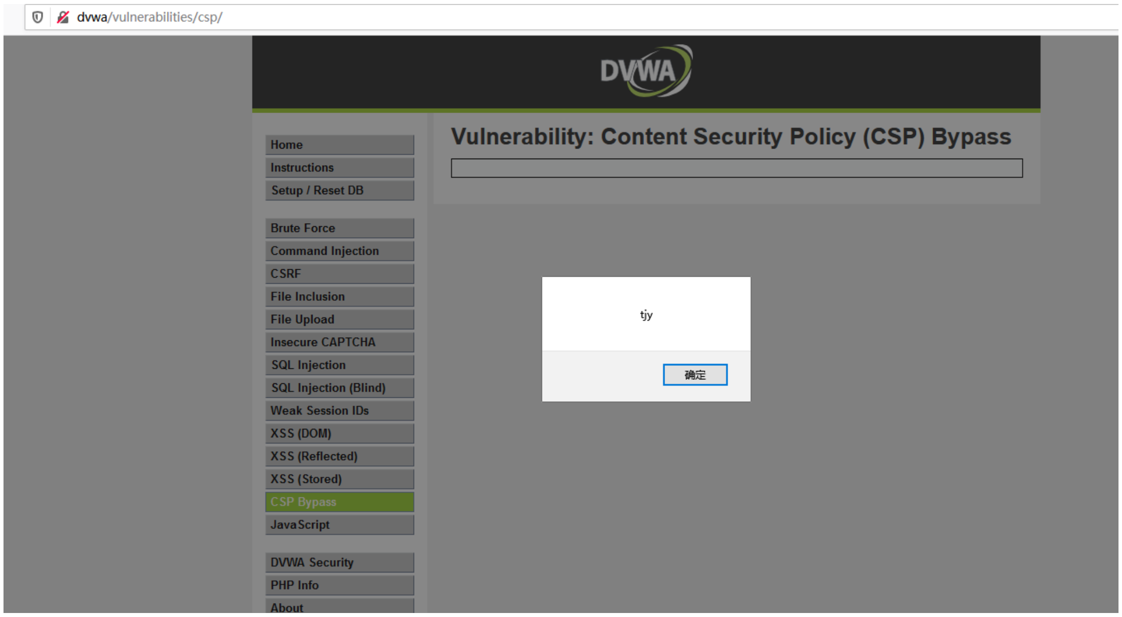
hahaha

csp-bypass medium



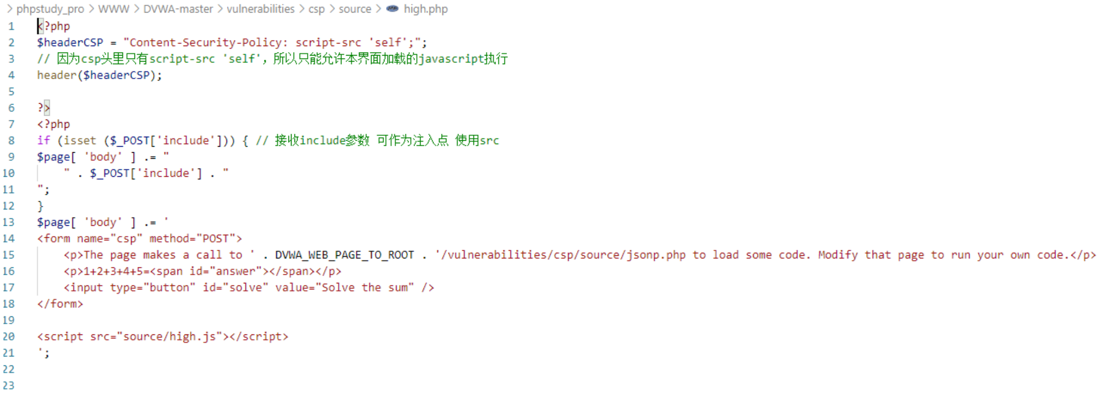
phpstudy_pro > WWW > DVWA-master > vulnerabilities > csp > source > medium.php

```
<?php

$headerCSP = "Content-Security-Policy: script-src 'self' 'unsafe-inline' 'nonce-TmV2ZXIgZ29pbmcgdG8gZ2l2ZSB5b3UgdXA=';";
// unsafe-inline 允许使用内联资源，如<script>元素 nonce-source,仅允许特定的内联脚本块nonce-TmV2ZXIgZ29pbmcgdG8gZ2l2ZSB5b3UgdXA=
header($headerCSP);

// Disable XSS protections so that inline alert boxes will work
header ("X-XSS-Protection: 0");

# <script nonce="TmV2ZXIgZ29pbmcgdG8gZ2l2ZSB5b3UgdXA=">alert(1)</script>

?>
<?php
if (isset ($_POST['include'])) {
$page[ 'body' ] .= "
    " . $_POST['include'] . "
";
}
$page[ 'body' ] .= '
<form name="csp" method="POST">
    <p>Whatever you enter here gets dropped directly into the page, see if you can get an alert box to pop up.</p>
    <input size="50" type="text" name="include" value="" id="include" />
    <input type="submit" value="Include" />
</form>
';
```

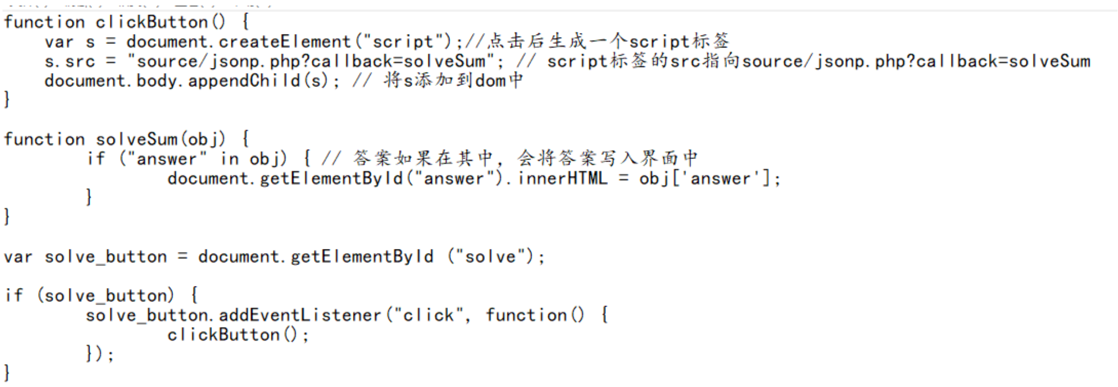


Vulnerability: Content Security Policy (CSP) Bypass

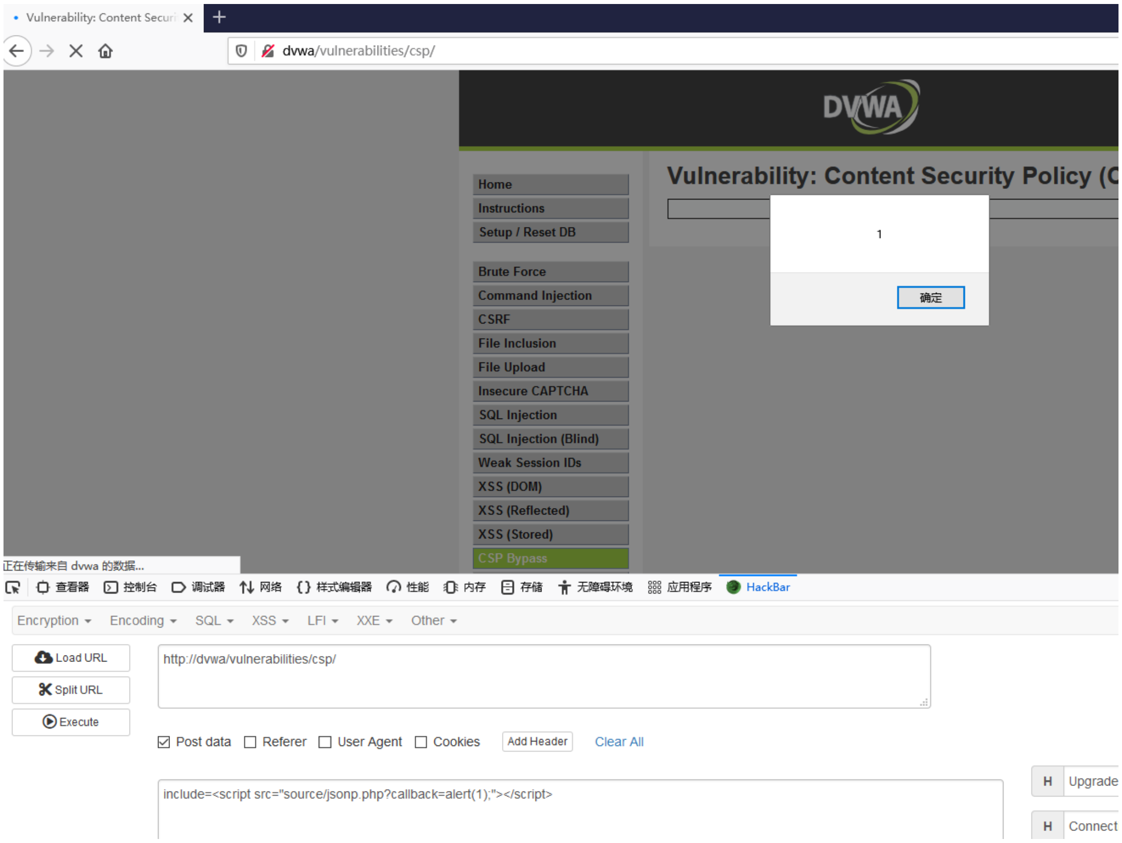
csp-bypass high


> phpstudy_pro > WWW > DVWA-master > vulnerabilities > csp > source > high.php

```
<?php
$headerCSP = "Content-Security-Policy: script-src 'self';";
// 因为csp头里只有script-src 'self'，所以只能允许本界面加载的javascript执行
header($headerCSP);

?>
<?php
if (isset ($_POST['include'])) { // 接收include参数 可作为注入点 使用src
$page[ 'body' ] .= "
    " . $_POST['include'] . "
";
}
$page[ 'body' ] .= '
<form name="csp" method="POST">
    <p>The page makes a call to ' . DVWA_WEB_PAGE_TO_ROOT . '/vulnerabilities/csp/source/jsonp.php to load some code. Modify that page to run your own code.</p>
    <p>1+2+3+4+5=<span id="answer"></span></p>
    <input type="button" id="solve" value="Solve the sum" />
</form>

<script src="source/high.js"></script>
';


```



```
function clickButton() {
    var s = document.createElement("script");//点击后生成一个script标签
    s.src = "source/jsonp.php?callback=solveSum"; // script标签的src指向source/jsonp.php?callback=solveSum
    document.body.appendChild(s); // 将s添加到dom中
}

function solveSum(obj) {
        if ("answer" in obj) { // 答案如果在其中, 会将答案写入界面中
                document.getElementById("answer").innerHTML = obj['answer'];
        }
}

var solve_button = document.getElementById ("solve");

if (solve_button) {
        solve_button.addEventListener("click", function() {
                clickButton();
        });
}
```



Vulnerability: Content Security Policy (C

1

确定

http://dvwa/vulnerabilities/csp/

☑ Post data □ Referer □ User Agent □ Cookies

```
include=<script src="source/jsonp.php?callback=alert(1);"></script>
```