代码里的黄金屋

智盟启明　　袁畅

关于我

- 程序猿

PHP

JAVA

Chora

- 白帽子

渗透测试

代码审计

文盲的自学经历

- 自己所谓的代码审计之初体验（瞎找） 10年

常用语法、函数不懂百度谷歌【Oask（asp） hdwiki(php) 】

- 自己所谓的代码审计再体验（比对着书瞎找）12年

常用语法、函数已百度谷歌的记得一大半

黑客手册、暗组工具包，精通脚本黑客全本（代码审计）

多多返利 B2BBuiler 杰奇等

- 进军乌云娱乐圈（入门真正的代码审计）13年

任务：每个月至少分析两套程序，每个月至少3个高危漏洞

- 不断学习，不断总结、改进自己的审计方法 14年

推荐的学习过程

- 语言基础知识（ php基本语法、函数，mysql 基本操作

  【参考资料a、c】
- 常见漏洞类型（SQL注入、文件包含等）

  【参考资料1、3、4】
- 从易到难的实践（看明白是一回事儿，会操作是一会儿事儿，懂原理是一件事儿）
- 语言进阶（php核心技术、正则表达式、设计模式等，mysql大多数操作）

  【参考资料b、c】
- 创新（新的方法、新的思路）

多看、多想、多写

参考资料：	
1、https://code.google.com/p/pasc2at/wiki/SimplifiedChinese	见[Heige_高级PHP代码审核技术.pdf]
2、http://zone.wooyun.org/content/11669	见[LaiX_PHP安全代码审计手册.txt]
3、http://static.wooyun.org/upload/image/201503/2015031611341847544.png	见[BMa_代码审计图.png]
4、http://drops.wooyun.org/papers/4544	见[' 雨。_论PHP常见的漏洞.mht]
http://drops.wooyun.org/?s=%E4%BB%A3%E7%A0%81%E5%AE%A1%E8%AE%A1&submit=%E6%90%9C%E7%B4%A2	
http://zone.wooyun.org/zone/SCA	
http://www.wooyun.org/bug.php?action=list&type=9	
a、《细说PHP》、《PHP和MySQL Web开发》	
b、《php核心技术与最佳实践》、《PHP精粹》	
c、《mysql_manual_zh.chm》《php_enhanced_zh.chm》	

读书的重要性

摘自mysql参考手册select语法：

```
SELECT
    [ALL | DISTINCT | DISTINCTROW ]
      [HIGH_PRIORITY]
      [STRAIGHT_JOIN]
      [SQL_SMALL_RESULT] [SQL_BIG_RESULT] [SQL_BUFFER_RESULT]
      [SQL_CACHE | SQL_NO_CACHE] [SQL_CALC_FOUND_ROWS]
    select_expr [, select_expr ...]
    [FROM table_references
    [WHERE where_condition]
    [GROUP BY {col_name | expr | position}
      [ASC | DESC], ... [WITH ROLLUP]]
    [HAVING where_condition]
    [ORDER BY {col_name | expr | position}
      [ASC | DESC], ...]
    [LIMIT {[offset,] row_count | row_count OFFSET offset}]
    [PROCEDURE procedure_name(argument_list)]
    [INTO OUTFILE 'file_name' export_options
      | INTO DUMPFILE 'file_name'
      | INTO var_name [, var_name]]
    [FOR UPDATE | LOCK IN SHARE MODE]]
```

- order by inject
- group by inject
- Limit x inject
- having inject
- into [out|dump]file inject

- [group|order] by x [asc|desc] inject
- [group|order] by x,inject [asc|desc] inject
- [!=order by] limit x[,x] inject(union select)
- order by x [asc|desc] limit x[,x] procedure analyse(inject,1) 详见[注释]
- having inject(类似于where,区别在于where字句在聚合前先筛选记录,而having是聚合后筛选)
- into [out|dump]file inject

显错注入：

procedure analyse(updatexml(1,concat(0x7c,version(),0x7c),1),1)

延时注入：

procedure analyse(updatexml(1,concat(0x7c,if(1=1,BENCHMARK(5000000,md5(1)),null),0x7c),1),1)

注释：

- 原文： https://rateip.com/blog/sql-injections-in-mysql-limit-clause/
- 译文： http://zone.wooyun.org/content/18220
- 感谢五道口杀气的翻译，以及分享。

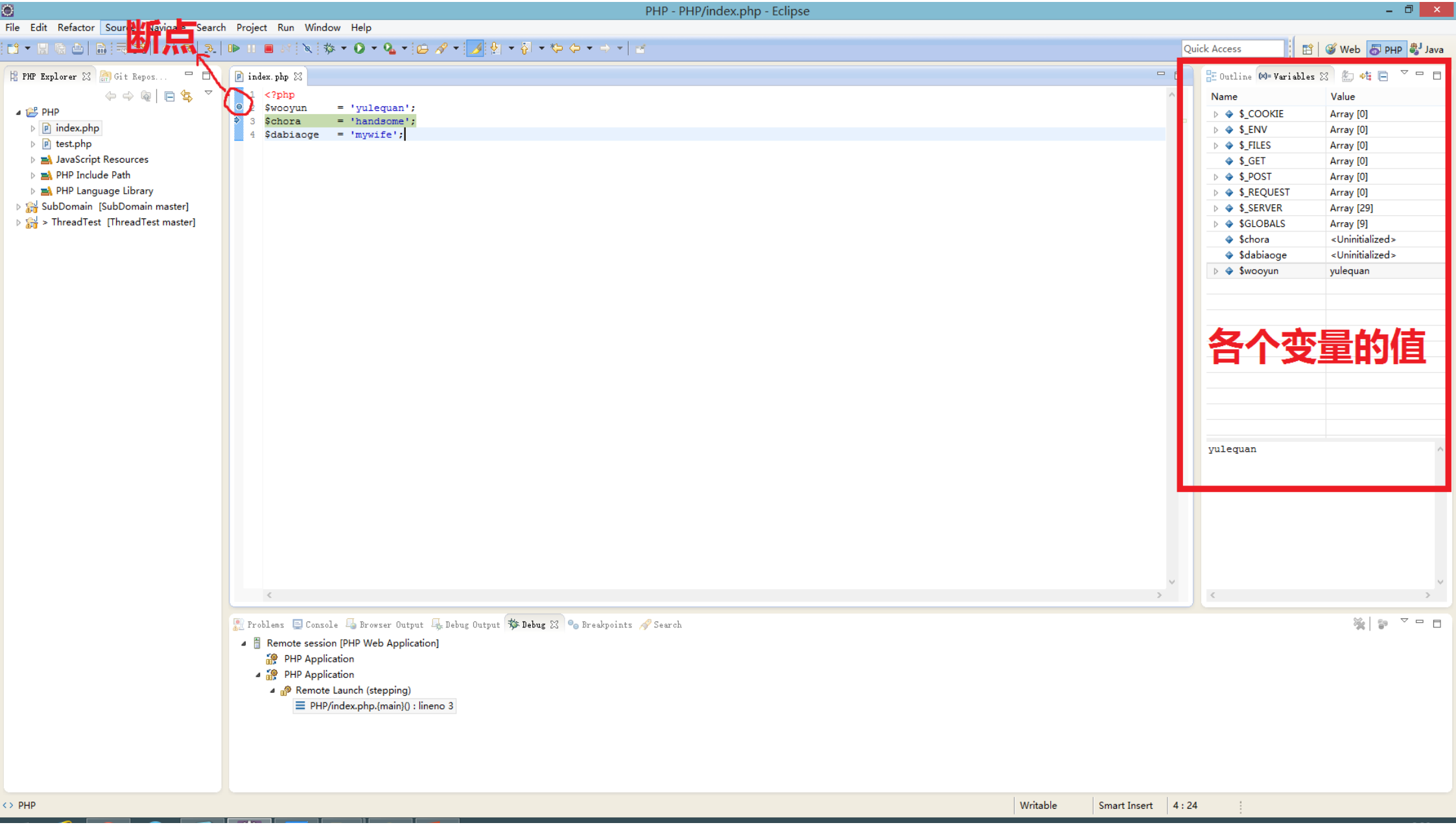
代码审计方式：

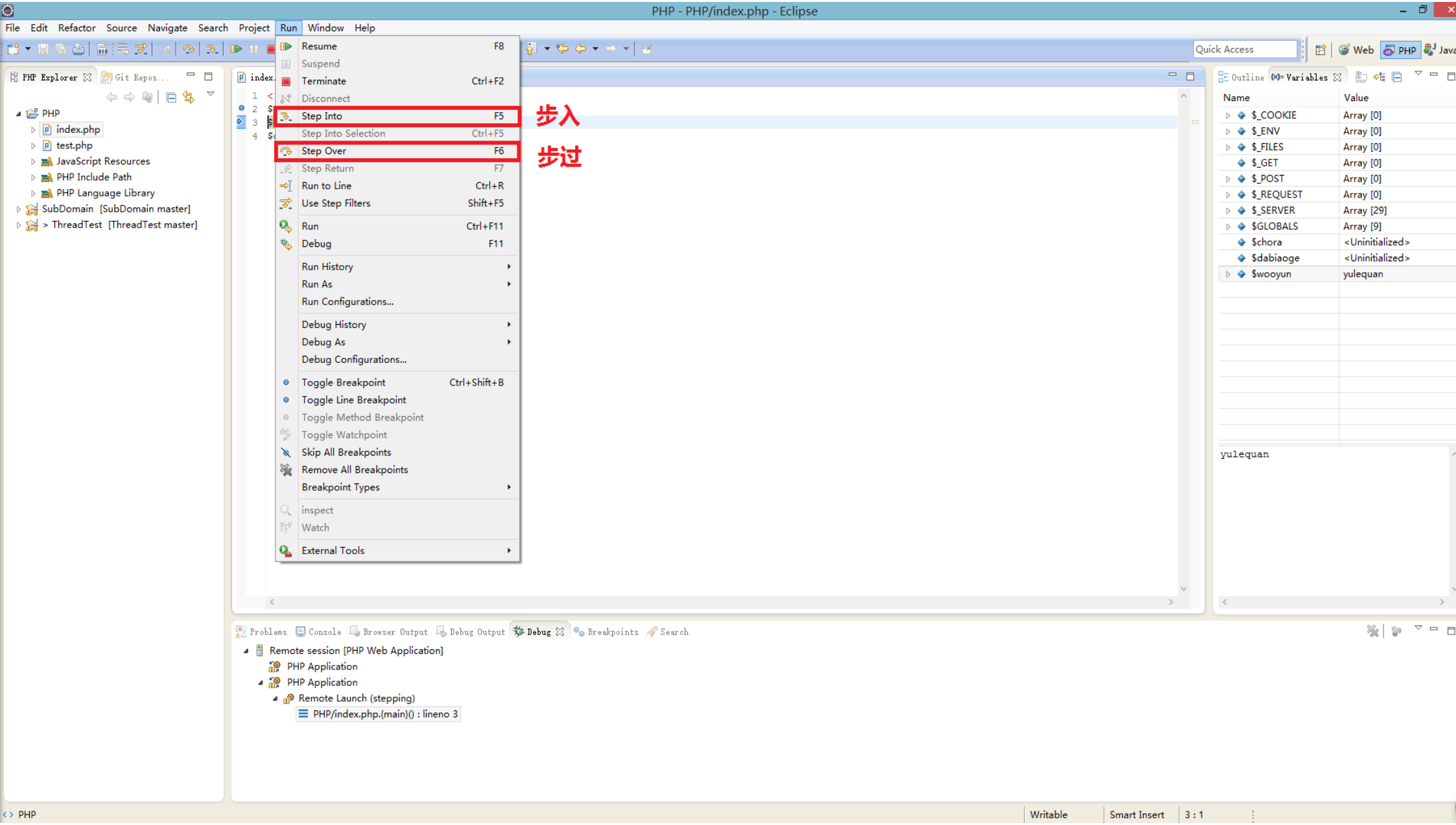
- 核心思想

一切输入都是有害的，以理解运行机制为主，搜索关键词为辅，进行可控变量的跟踪。

关键词【见参考资料2】

- 静态分析
- 动态调试
- 自动化审计


PHP - PHP/index.php - Eclipse
File Edit Refactor Source Navigate Search Project Run Window Help
断点
Quick Access
Web PHP Java
PHP Explorer
Git Repos...
PHP
index.php
test.php
JavaScript Resources
PHP Include Path
PHP Language Library
SubDomain [SubDomain master]
> ThreadTest [ThreadTest master]
index.php
1 <?php
2 $wooyun = 'yulequan';
3 $chora = 'handsome';
4 $dabiaoge = 'mywife';
Outline
Variables
Name
Value
$_COOKIE
Array [0]
$_ENV
Array [0]
$_FILES
Array [0]
$_GET
Array [0]
$_POST
Array [0]
$_REQUEST
Array [0]
$_SERVER
Array [29]
$GLOBALS
Array [9]
$chora
<Uninitialized>
$dabiaoge
<Uninitialized>
$wooyun
yulequan
各个变量的值
yulequan
Problems
Console
Browser Output
Debug Output
Debug
Breakpoints
Search
Remote session [PHP Web Application]
PHP Application
PHP Application
Remote Launch (stepping)
PHP/index.php.(main)() : lineno 3
PHP
Writable
Smart Insert
4 : 24


PHP - PHP/index.php - Eclipse
File Edit Refactor Source Navigate Search Project Run Window Help
Resume F8
Suspend
Terminate Ctrl+F2
Disconnect
Step Into F5
Step Into Selection Ctrl+F5
Step Over F6
Step Return F7
Run to Line Ctrl+R
Use Step Filters Shift+F5
Run Ctrl+F11
Debug F11
Run History
Run As
Run Configurations...
Debug History
Debug As
Debug Configurations...
Toggle Breakpoint Ctrl+Shift+B
Toggle Line Breakpoint
Toggle Method Breakpoint
Toggle Watchpoint
Skip All Breakpoints
Remove All Breakpoints
Breakpoint Types
inspect
Watch
External Tools
步入
步过
PHP Explorer
index.php
test.php
JavaScript Resources
PHP Include Path
PHP Language Library
SubDomain [SubDomain master]
> ThreadTest [ThreadTest master]
Outline
Variables
Name
Value
$_COOKIE Array [0]
$_ENV Array [0]
$_FILES Array [0]
$_GET Array [0]
$_POST Array [0]
$_REQUEST Array [0]
$_SERVER Array [29]
$GLOBALS Array [9]
$chora <Uninitialized>
$dabiaoge <Uninitialized>
$wooyun yulequan
yulequan
Problems Console Browser Output Debug Output Debug Breakpoints Search
Remote session [PHP Web Application]
PHP Application
PHP Application
Remote Launch (stepping)
PHP/index.php.{main}() : lineno 3
PHP
Writable
Smart Insert
3 : 1

准备阶段

- 开启mysql日志记录功能，以及准备好数据库审计软件实实时记录数据库数据库活动。

如：BareTailRro。

- 即可静态分析又可动态调试的审计工具。

如：Eclipse+PDT+Xdebug

- 需要审计的源码所对应环境。

如：Apache+PHP+Mysql

审计过程

- 静态分析核心文件，了解运行机制。

如：是否有安全防护类或者函数、是否使用框架（如果使用了框架且有安全防护，测试重心则偏向于非框架的内容以及逻辑方面的问题）、Web入口点对应的文件等。

- 搜索敏感关键词，追踪可控变量引入攻击代码。

如：内置读写删执行等敏感函数【见参考资料2】、被重写的函数、敏感信息表段（涉及会员数据、金额等）、存在漏洞的自写函数或类等。例：$page=max($page,1)

- 动态调试较为复杂的逻辑，结合静态分析准确发现漏洞点。

如：动态调试算法、动态调试多变量多组的运算与赋值，不用修改代码echo或者exit查看输出等。

审计结束

- 根据发现的漏洞写出EXP
- 使用动态调试验证流程确保准确
- 在本地以外的多个环境验证EXP
- 确认漏洞

案例一：某科技高危漏洞影响用户安全

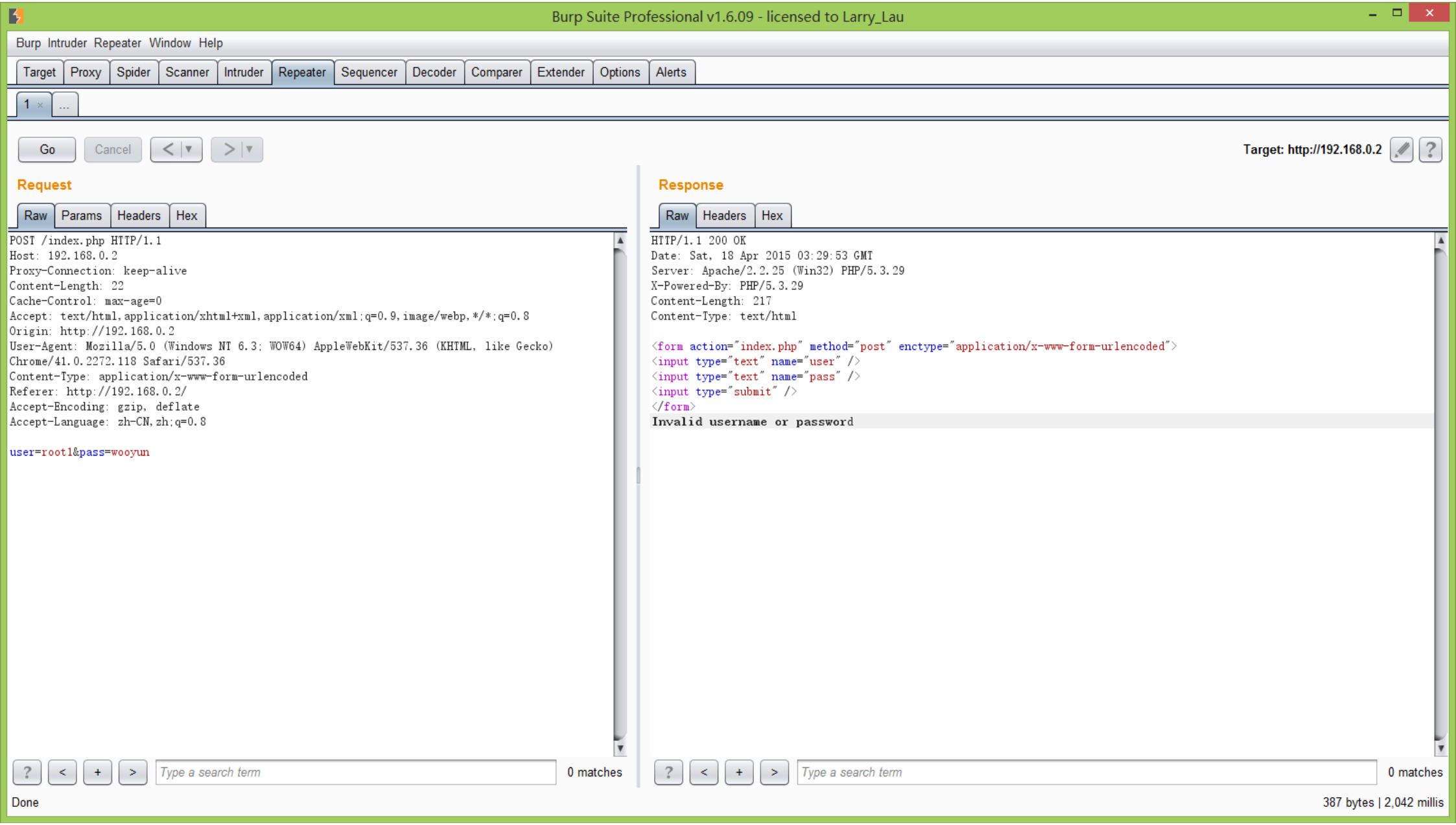
```
$file = $_FILES['avatar'];
$type = $file['type'];
$tmp  = $file['tmp_name'];
$name = $file['name'];
$ext  = strrchr($name,'.');
$data = file_get_contents($tmp);
if($type == "image/gif" || $type == "image/jpeg" || $type == "image/png"
&& !preg_match('~<\?php~',$data))
{
    echo 'Upload file success!';
} else {
    echo 'Upload file type error!';
}
```

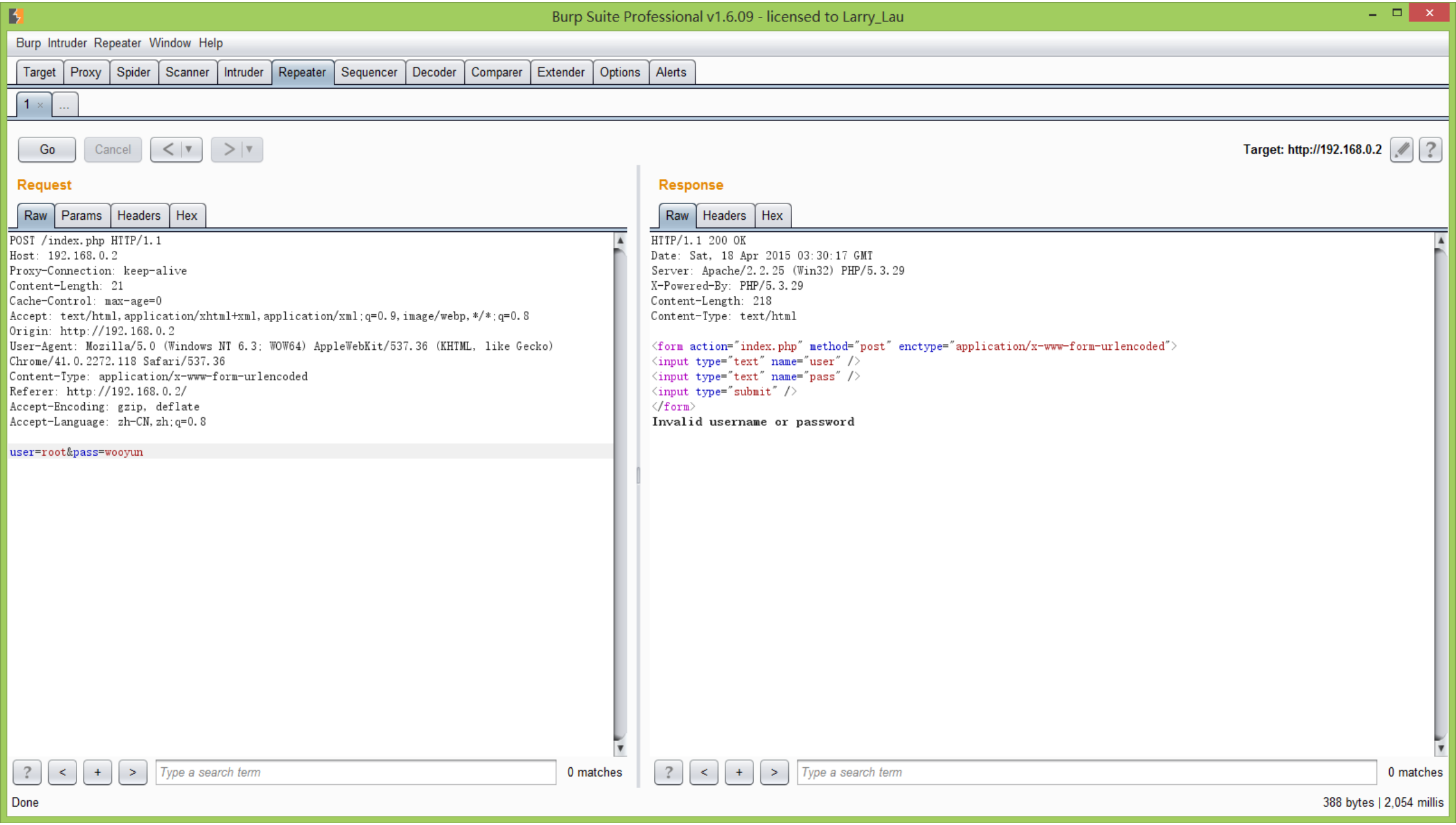
实例二：某集团逻辑漏洞影响内网安全

```
$query = mysql_query("select user,pass from admin where user='$user'");
$data = mysql_fetch_assoc($query);
if($data)
{
        if($data['pass'] == $pass)
        {
                echo ‘Login success.';
        } else
        {
                echo 'Password wrong.';
        }
} else {
        echo 'Username does not exist.';
}
```

延伸:注意执行时间、响应包是否相同

```
$query = mysql_query("select user,pass from admin where user='$user'");
$data = mysql_fetch_assoc($query);
if($data)
{
	if($data['pass'] == $pass)
	{
		echo 'Login success';
	} else
	{
		echo 'Invalid username or password ';
	}
} else {
	echo 'Invalid username or password';
}
```


Burp Suite Professional v1.6.09 - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel
Target: http://192.168.0.2
Request
Raw Params Headers Hex
POST /index.php HTTP/1.1
Host: 192.168.0.2
Proxy-Connection: keep-alive
Content-Length: 22
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://192.168.0.2
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.118 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.0.2/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
user=root1&pass=wooyun
Type a search term
0 matches
Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Sat, 18 Apr 2015 03:29:53 GMT
Server: Apache/2.2.25 (Win32) PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 217
Content-Type: text/html
<form action="index.php" method="post" enctype="application/x-www-form-urlencoded">
<input type="text" name="user" />
<input type="text" name="pass" />
<input type="submit" />
</form>
Invalid username or password
Type a search term
0 matches
Done
387 bytes | 2,042 millis


Burp Suite Professional v1.6.09 - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel
Target: http://192.168.0.2
Request
Raw Params Headers Hex
POST /index.php HTTP/1.1
Host: 192.168.0.2
Proxy-Connection: keep-alive
Content-Length: 21
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://192.168.0.2
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.118 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.0.2/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
user=root&pass=wooyun
Type a search term
0 matches
Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Sat, 18 Apr 2015 03:30:17 GMT
Server: Apache/2.2.25 (Win32) PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 218
Content-Type: text/html
<form action="index.php" method="post" enctype="application/x-www-form-urlencoded">
<input type="text" name="user" />
<input type="text" name="pass" />
<input type="submit" />
</form>
Invalid username or password
Type a search term
0 matches
Done
388 bytes | 2,054 millis

实例三：某金融集团另类任意充值漏洞

```
$total_money = 0.02;
$amount = isset($_POST['amount'])?floatval($_POST['amount']):0.00; //$amount=0.005
if($total_money > 0.00 && $amount > 0.00)
{
        $total_money  = round($total_money-$amount);//$total_money=0.02-0.005=0.015≈0.02
        $freeze_money = round($amount);//$freeze_money=0.005≈0.01
} else {
        echo 'error';
}
$tx = 'fail';
if($tx == 'fail')
{
        $total_money = $total_money + $freeze_money;//$total_money=0.02+0.01=0.03
}
```

设计原则

- 简单易懂
- 最小特权
- 拒绝信任
- 验证输入
- 净化输出
- 故障处理
- 统一编码

谢谢观看！