PHP代码的安全审查

汤青松

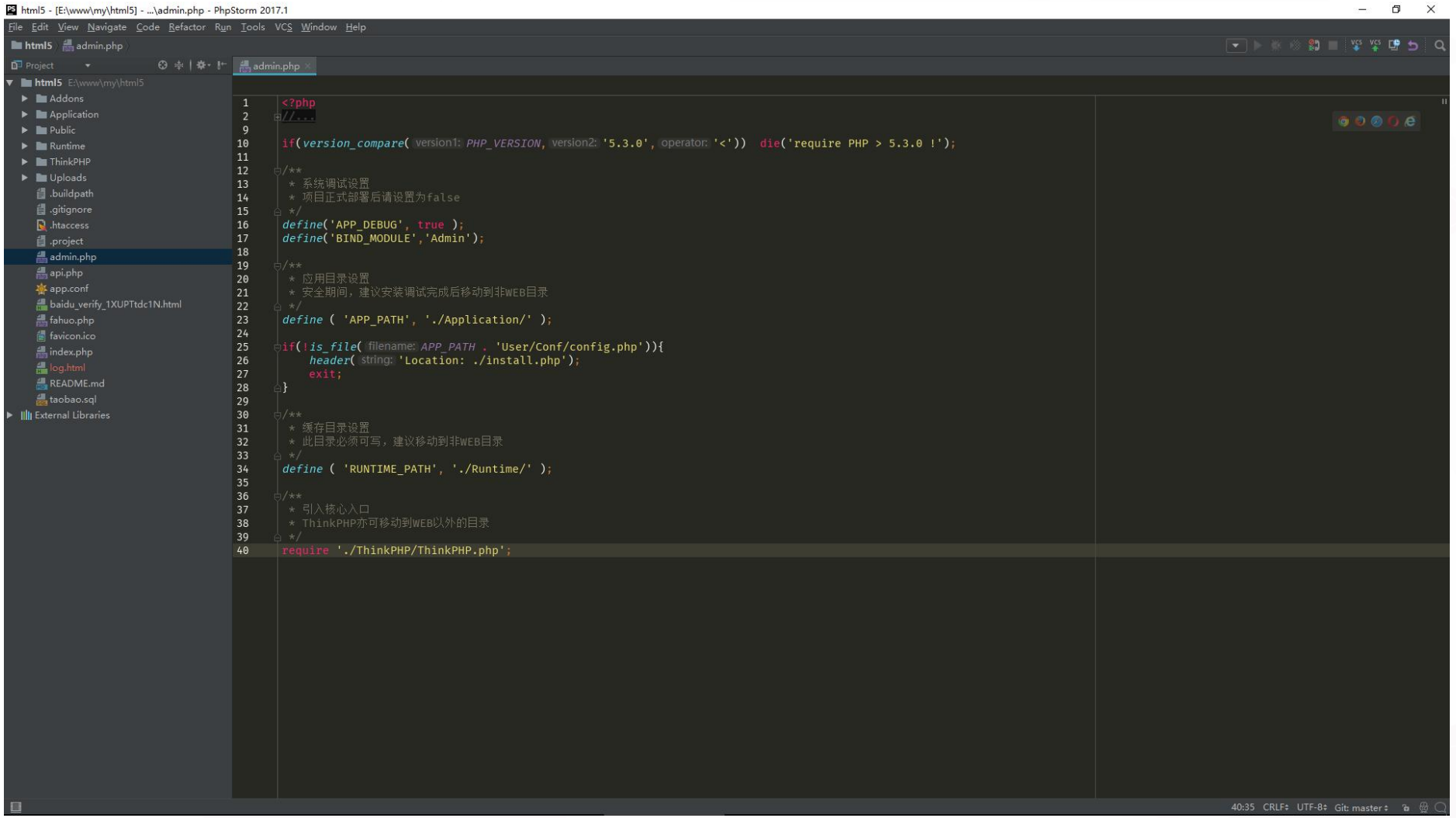
内容大纲

1. 代码审计辅助工具
2. 常规漏洞挖掘
3. 逻辑漏洞挖掘

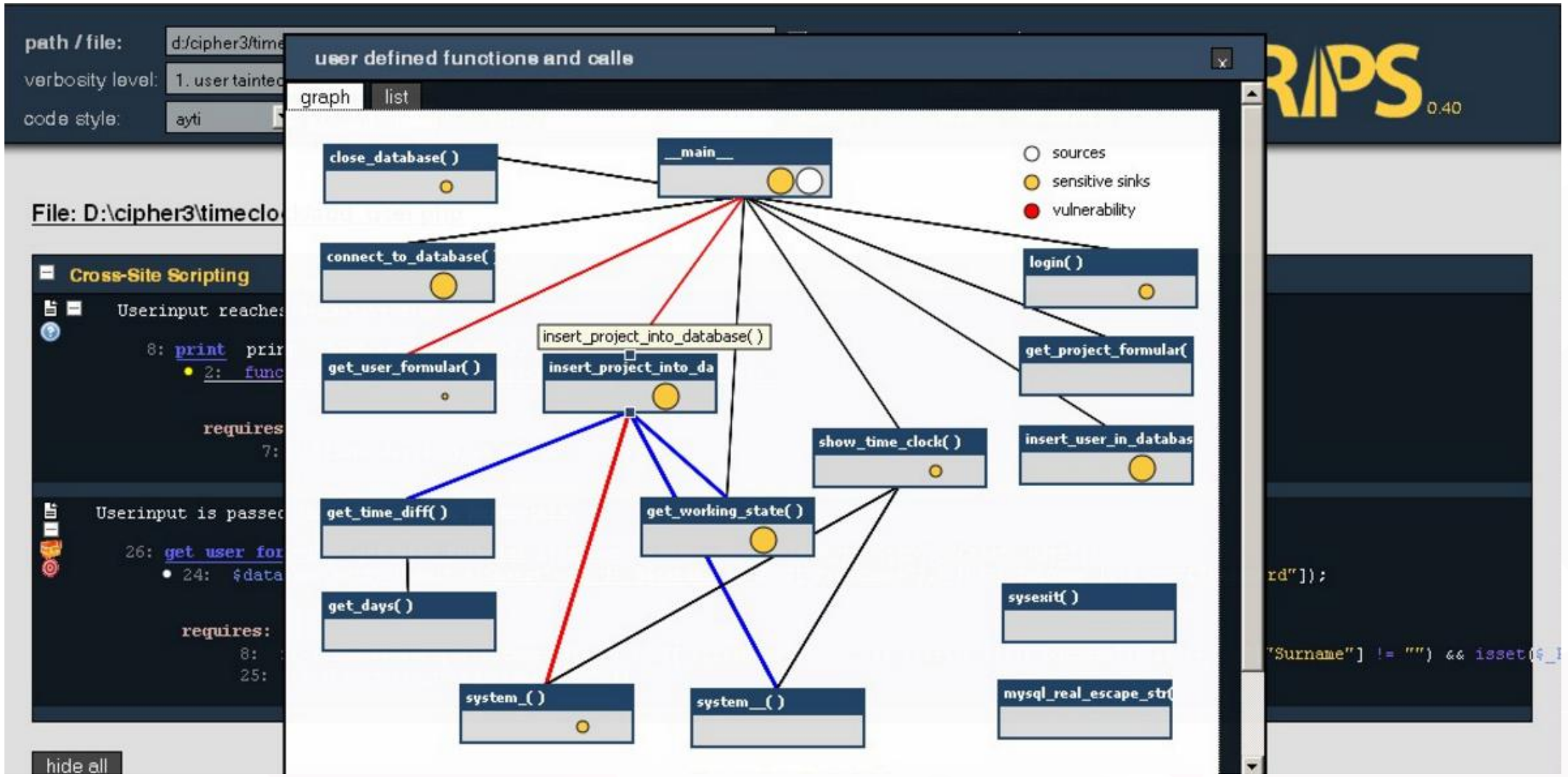
代码审计辅助工具

- 1. phpstorm 代码编辑器
- 2. PHP代码审计系统—RIPS
- 3. seay 源代码审计系统

phpstorm 代码编辑器



PHP代码审计系统—RIPS



seay 源代码审计系统

SQL注入漏洞

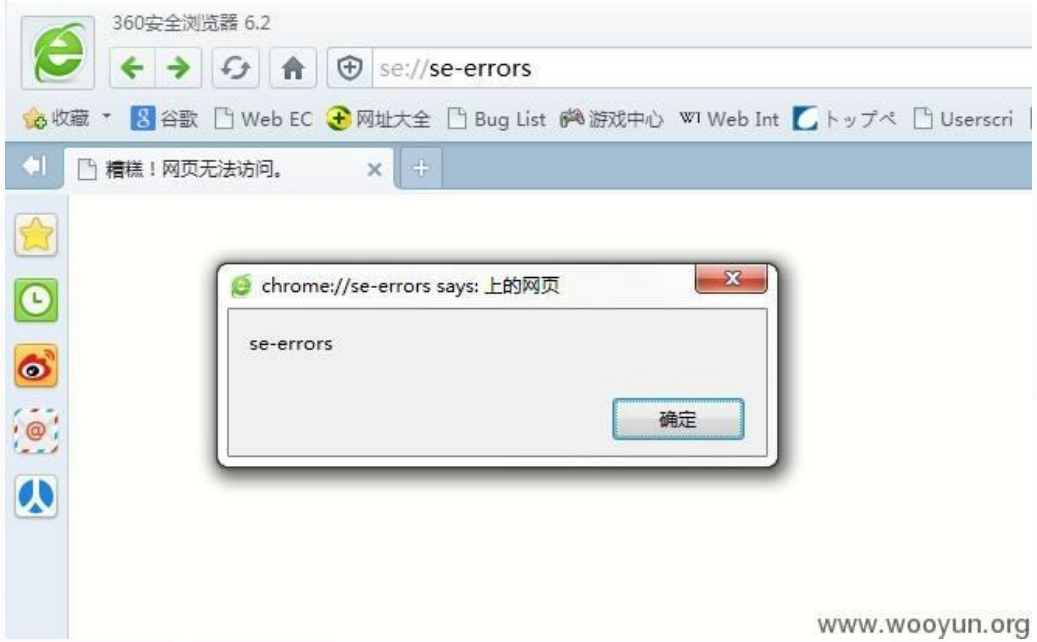
- 1. 挖掘经验
  - 寻找裸写SQL
  - 寻找$_GET、$_POST、$_COOKIE

- 2. 漏洞防范
  - 参数过滤
  - 使用PDO

XSS漏洞

- 1. 挖掘经验
  - 寻找搜索、存储后可以可以展示的位置
  - 寻找$_GET、$_POST、$_COOKIE

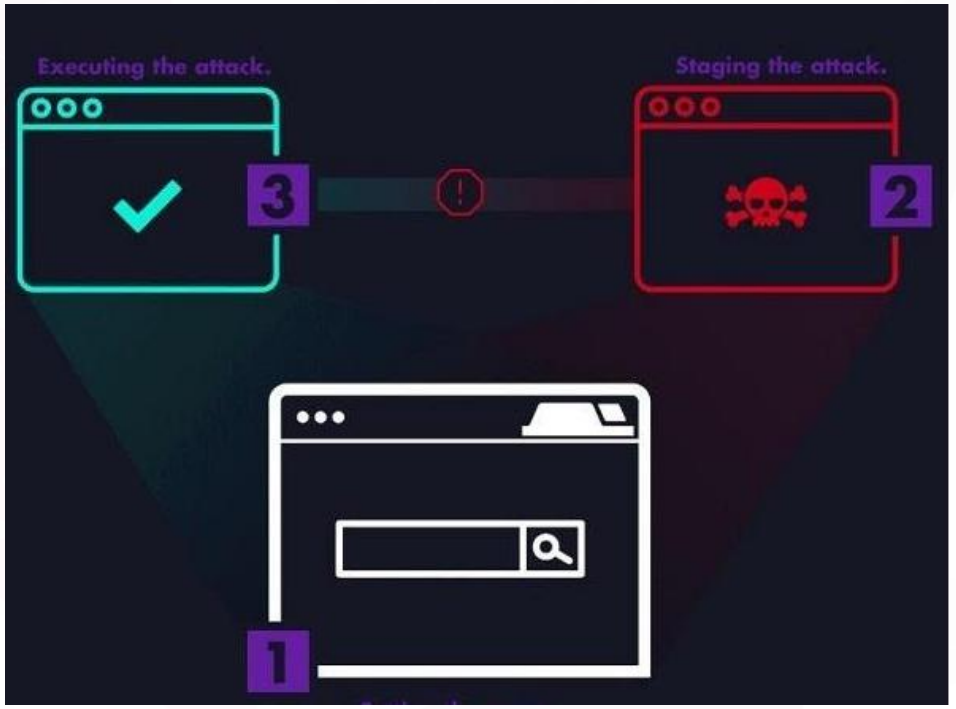
- 2. 漏洞防范
  - 代码转义



CSRF漏洞审计

- 1. 挖掘经验
  - 打开动态页面，看看有没有token验证
  - 不加referer访问，如果返回数据一致，说明有漏洞

- 2. 漏洞防范
  - 图片验证码验证
  - token验证



常规漏洞审计总结

- 1. 常规漏洞特点
- 2. 防范方案

1. 常规漏洞特点

- 1. 参数没有过滤
- 2. 没有对参数验证来源

2.常规漏洞防范方案

- 1. taint PHP安全扩展
- 2. ngx_lua_waf nginx安全扩展

taint PHP安全扩展

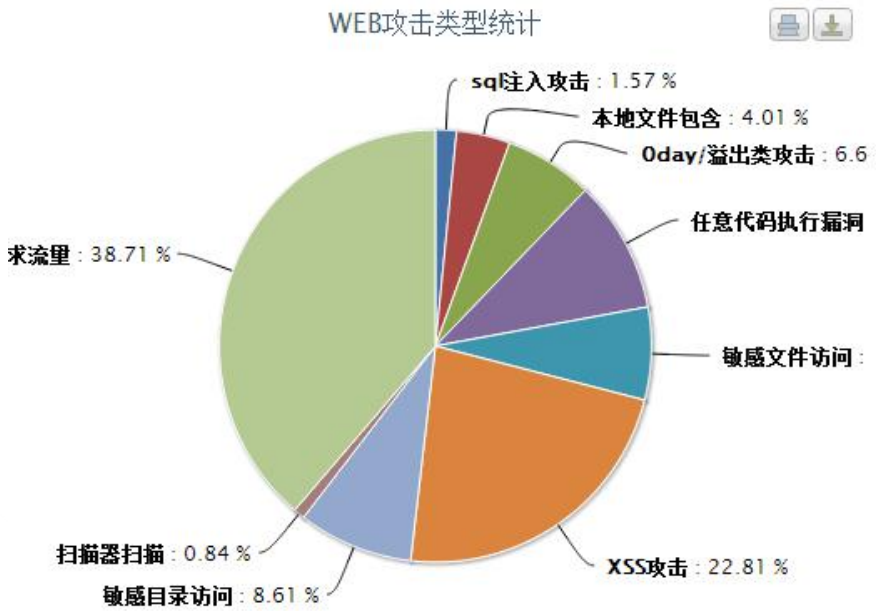
```php
<?php
 $a = $_GET['a'];

 $file_name = '/tmp' .  $a;
 $output    = "Welcome, {$a} !!!";
 $var       = "output";
 $sql       = "Select *  from " . $a;
 $sql      .= "ooxx";

 echo $output;
//Warning: main(): Attempt to echo a strin    ch might be tainted in xxx.php on line x

 print $$var;
//Warning: main(): Attempt to print a string which might be tainted  in xxx.php on line x

 include($file_name);
//Warning: include() [function.include]: File path contains data that might be tainted in xxx.php on x

 mysql_query($sql);
//Warning: mysql_query() [function.mysql-query]: First argument contains data that might be tainted in xxx.php on line x
?>
```

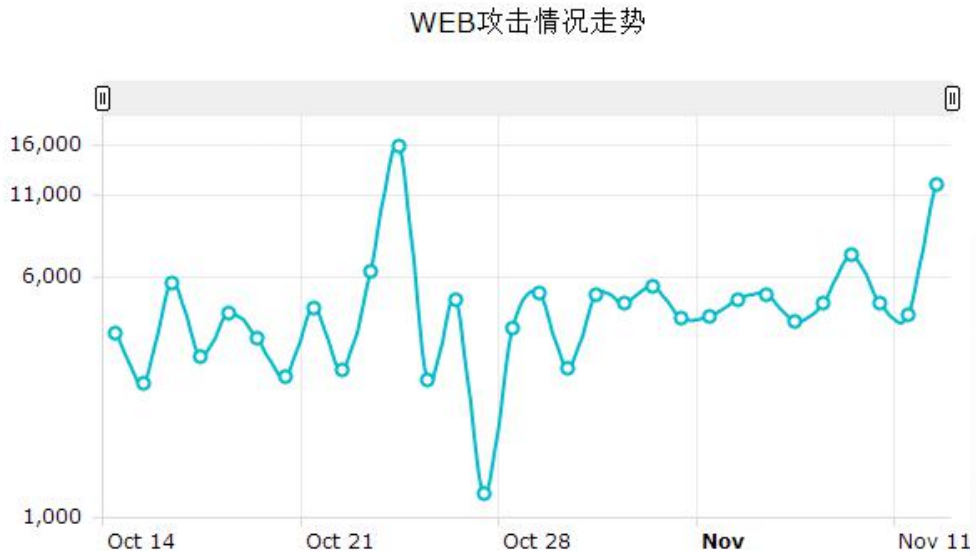
在一些关键函数或语句(echo, print, system, exec)

没有经过转义, 安全过滤处理，就使用来自$_GET,

$_POST或者$_COOKIE的数据,Taint会提示Warning

ngx_lua_waf nginx安全扩展





概况统计

已拦截180672次web攻击	攻击者IP地址个

攻击行为统计

SQL注入2837条	文件包含7238条	任意代码执行17869条
命令执行11988条	XSS攻击41216条	目录探测15554条
敏感文件12509条	扫描器扫描1516条	异常请求69945条

WeChat: songboy8888

Email:soupqingsong@foxmail.com