
Think
ThinkInLAMP.com
PHPCon 2015
北京站

PHP 安全编程

by

陈　峰　卫

Email:　chenfwvip@foxmail.com

Company:　Knownsec

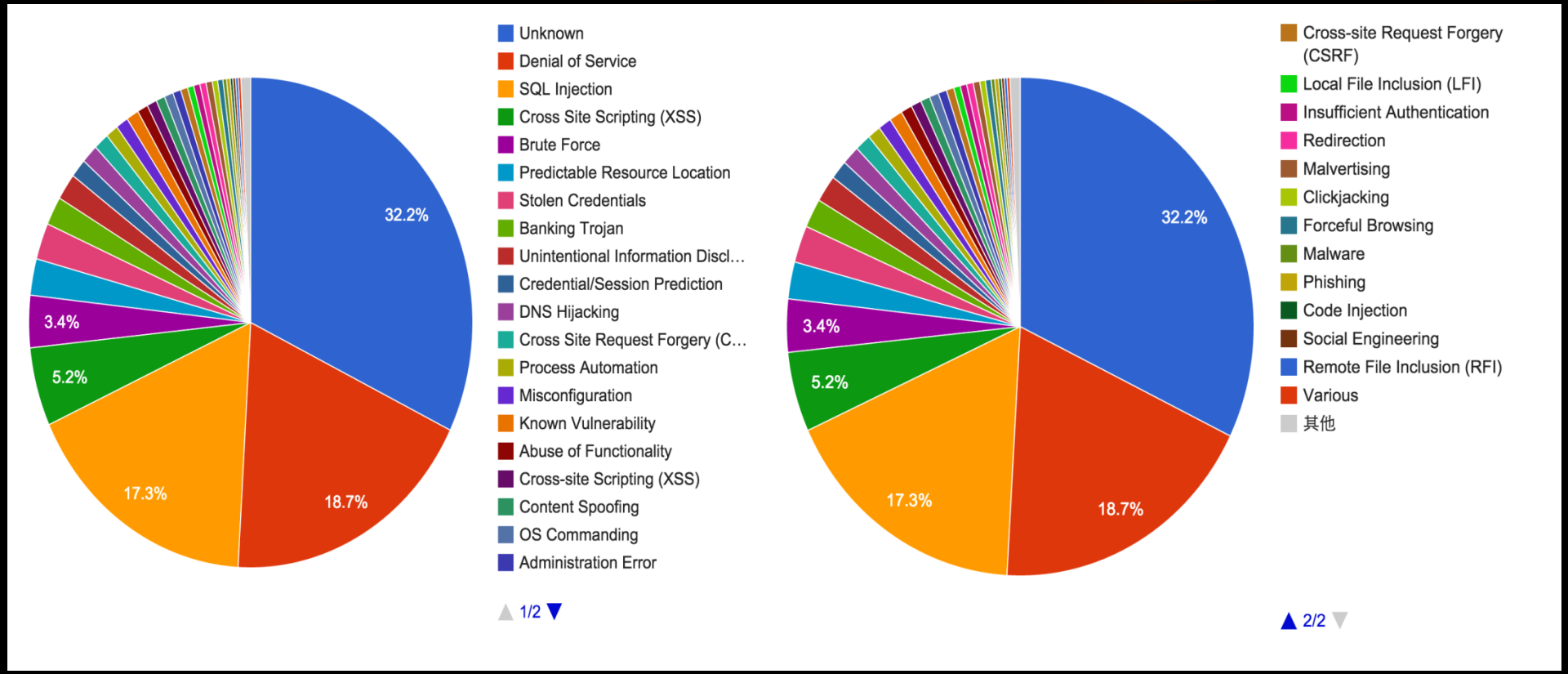
Blog:　http://www.php101.cn

大纲

- Web安全概况
- 常见漏洞类型及其防御
- 配置安全
- 其他防御方法

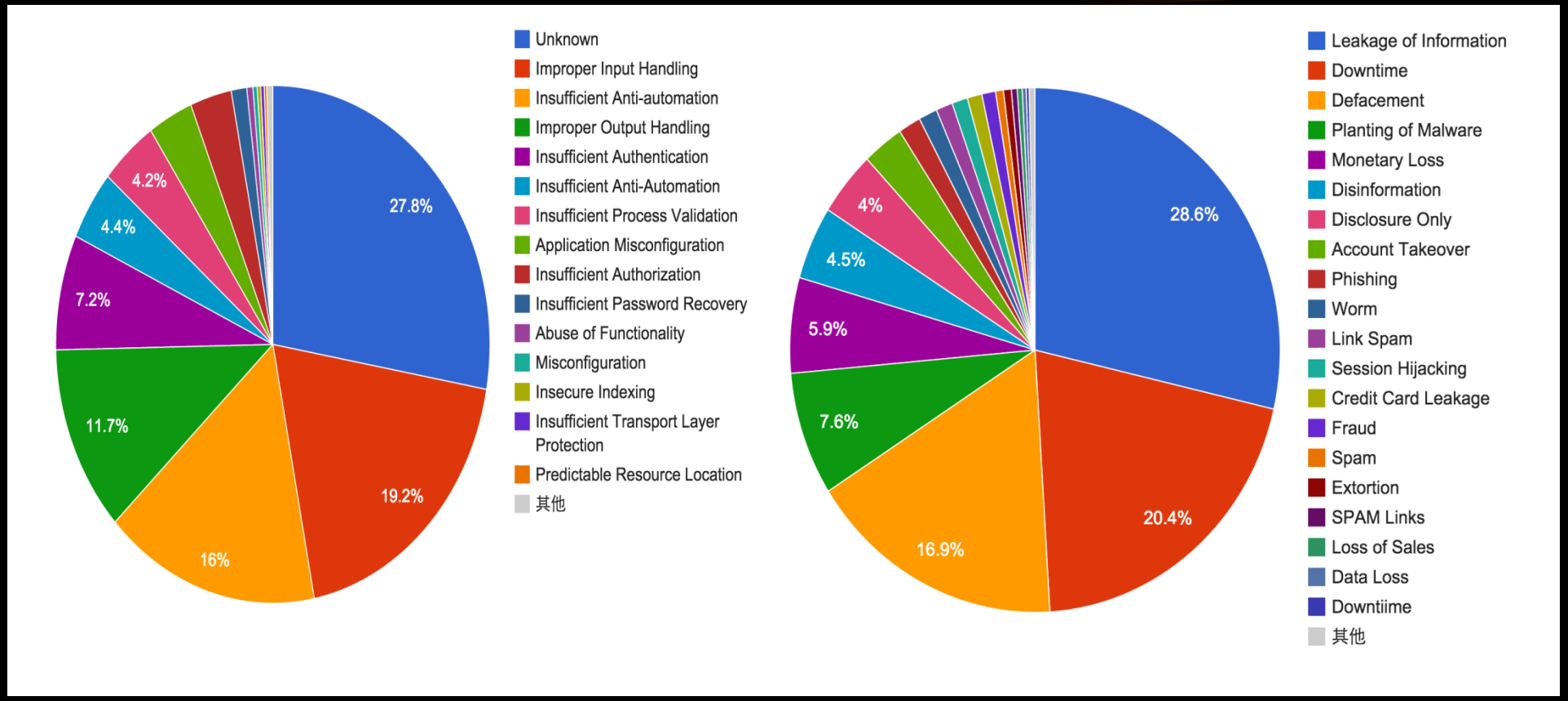
Web安全概况

Top Attack Methods



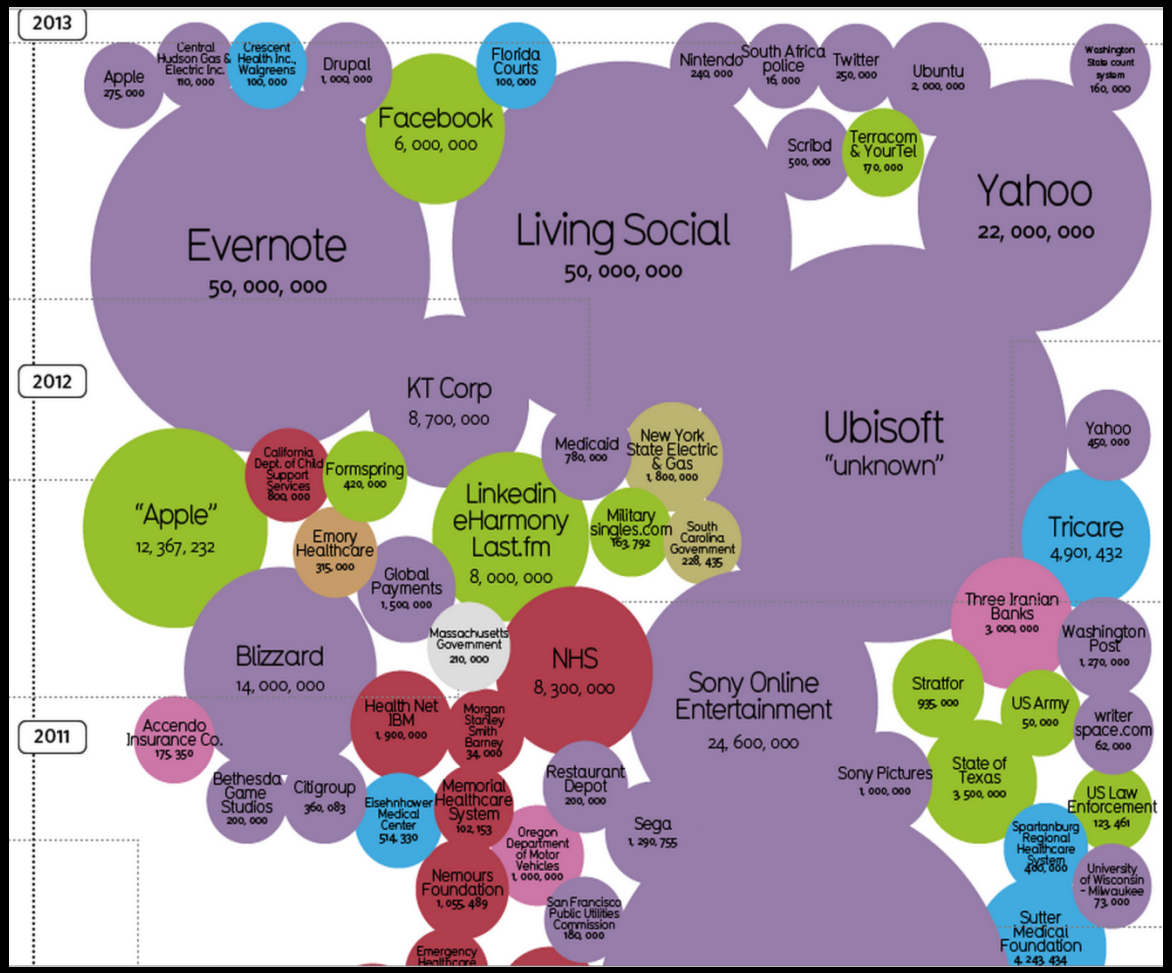
Web安全概况

Top Application Weaknesses



Top Impacts/Outcomes

Web安全概况



从2012年到2013年，
大约有140,621,000
的数据泄露。
如左图所示，
Yahoo，ubuntu，
evernote，
Ubisoft，CSDN
有没有哪个让你留下了
深刻印象呢？

SQL注入

SQL注入类型

- Union Based
  - Interger Based
  - String Based
- Error Based
  - Error Based
  - Double Query
- Blind SQL injection
  - Time based
  - Boolean Based

SQL注入分类

- Inband
- Out-of-Band
- Inferential

SQL注入

SQL注入示例：

```
$sql="SELECT * FROM users WHERE id='$id' LIMIT
 0,1";
$result=mysql_query($sql);
$row = mysql_fetch_array($result);
if($row){
     echo '<font size="5"color="#FFFF00">';
     echo 'You are in..........';
     echo "<br>";
     echo "</font>";
 }else {
     echo '<font size="5" color="#FFFF00">';
     //echo 'You are in..........';  // boolean
 based
     //print_r(mysql_error());    // error based
     //echo "You have an error in your SQL syntax";
     echo "</br></font>";
     echo '<font color= "#0000ff" font size= 3>';

     }
}
```

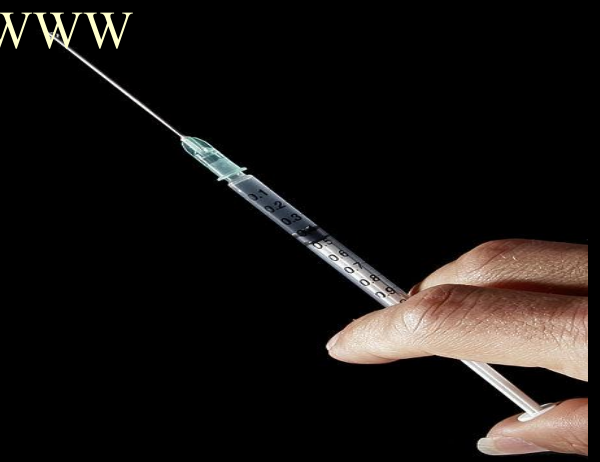
SQL注入

SQL注入防御

- magic_quotes_gpc
  - 版本:5.3(过期) 5.4(移除)
  - $_SERVER、getenv()、输入输出流、SQL中的in/limit/order/...
- 使用预处理语句
  - PDO
  - MySQLi
- 转义/过滤
  - intval()
  - mysql_real_escape_string()

  (合理使用过滤)

WWW



再谈SQL注入

- 正确的过滤
- 使用合理的字符集
- 宽字节注入
  - 受字符集影响
  - 示例代码:

```
// username=%df%27%20or%201=1%20limit%202,1%23

$username = $_GET['username'];
$username =
    mysql_real_escape_string($username);
$sql = "SELECT * FROM users WHERE
    username='$username'";
```

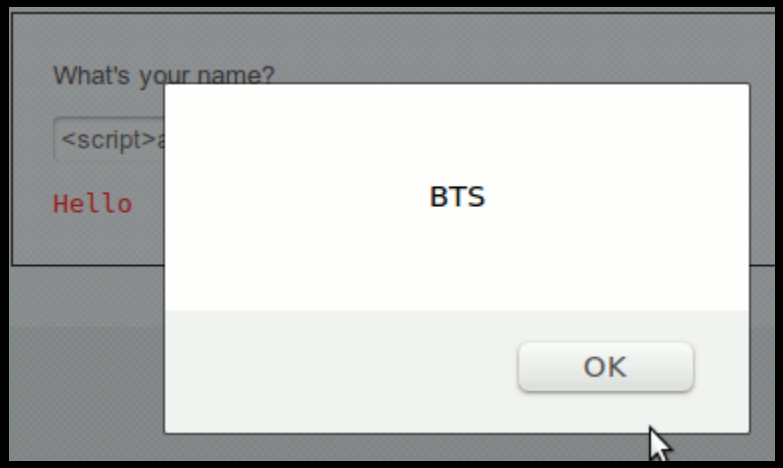
XSS(跨站脚本攻击)

XSS类型

- 反射型(Reflected)
- 存储型(Stored)
- DOM型
- 其他类型
  - 突变型(Mutation XSS)
  - 通用型(UXSS)
  - Flash XSS
  - UTF-7 XSS
  - MHTML XSS
  - CSS XSS
  - VBScript XSS

XSS（跨站脚本攻击）

XSS示例：



XSS(跨站脚本攻击)

XSS的注入点

- HTML元素

  ```
  <div>userInput</div>
  ```

- 元素属性值

  ```
  <input value="userInput">
  ```

- URL查询

  ```
  http://example.com/
  ?parameter=userInput
  ```

- CSS属性值

  ```
  CSS value
  ```

- JavaScript变量

  ```
  var name = "userInput";
  ```

XSS(跨站脚本攻击)

XSS危害

- 窃取Cookie
- Keylogging
- Phishing(钓鱼)
- Dos攻击
- 其他

XSS(跨站脚本攻击)

XSS防御

- 转义/编码
  - htmlspecialchars()
- 过滤
  - strip_tags()
- CSP(Content Security Policy)
- 第三方库
  - HTMLPurifier
  - htmLawed
  - Zend_Filter_Input

会话(session)攻击

会话攻击概述

HTTP协议是无状态的，因此有了会话

对攻击者而言，会话攻击中最重要的部分是获取会话标识符，获取会话标识符主要有三种途径：

- 预测
- 捕获
- 固化

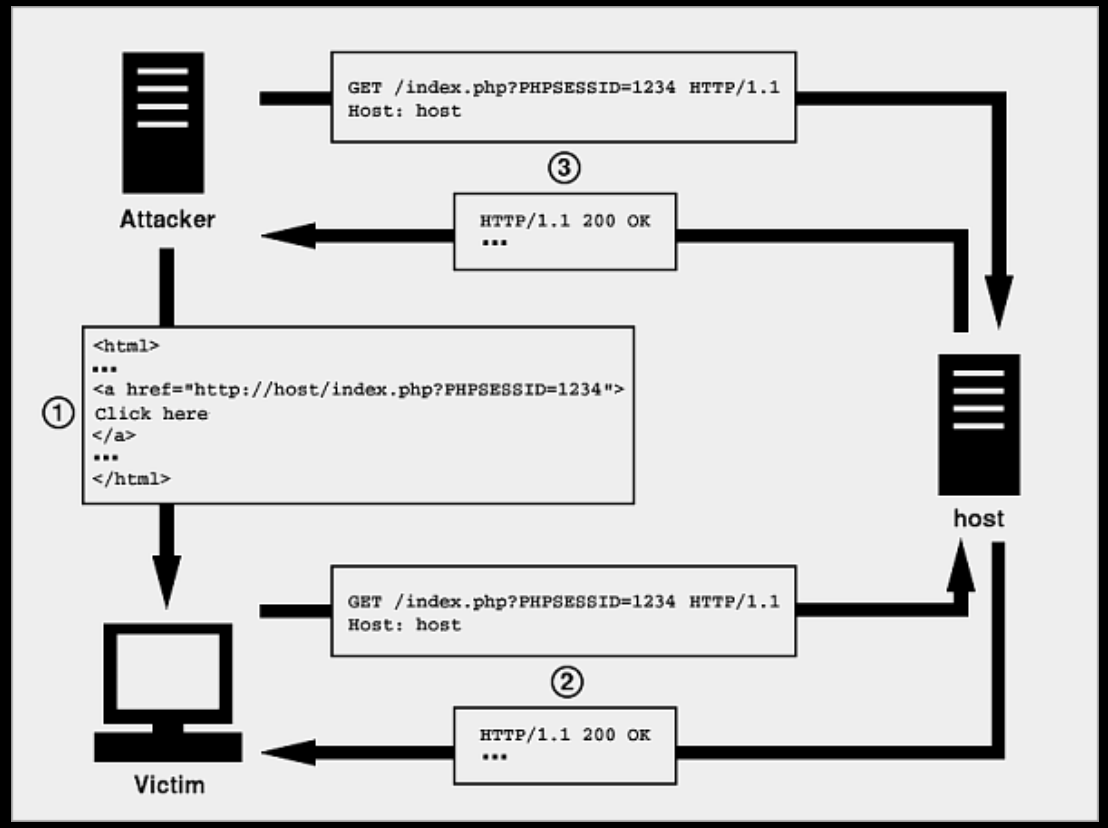
会话(session)攻击

会话攻击类型

- 会话固化
- 会话劫持
- 会话毒化(注入)

会话(session)攻击

会话固化攻击示意



会话(session)攻击

会话劫持

- XSS
- 嗅探
- 中间人攻击

会话毒化

- Cookie注入

会话(session)攻击

会话攻击防御

- session_regenerate_id();
- 二级令牌
- 检测UA和用户IP

File Inclusion(文件包含)

文件包含漏洞类型

- 本地文件包含(LFI)
- 远程文件包含(RFI)

相关函数

- include(),include_once()
- require(),require_once()

File Inclusion(文件包含)

文件包含漏洞示例

```
$filename = $_GET["file"];

Include($_SERVER["DOCUMENT_ROOT"]."/".
    $filename.".php");

// 利用
index.php?file=../../../../../../../../../..
  /etc/passwd

php://input

截断 %00、?(伪截断)
```

File Inclusion(文件包含)

文件包含漏洞防御

– 白名单

```
$page_files=array( 'about'=>'about.html',
                   'photos'=>'photos.html',
                   'contact'=>'contact.html',
                   'home'=>'home.html'
                 );
if (in_array($_GET['page'],array_keys($page_files))) {
      include $page_files[$_GET['page']];
 } else {
      include $page_files['home'];
}
```

– 其他防御手段

- PHP配置
- 服务器配置

聊一聊Nullbyte

Nullbyte

- NULL是控制字符，值为0
- 字符集中的NULL
  - unicode:\u0000
- C语言中的NULL

```
char string[4];
int main() {
  string[0] = 'f';
  string[1] = 'o';
  string[2] = 'o';
  string[3] = '\0';
}
```

%00
Null Byte Design

聊一聊Nullbyte

ＰＨＰ中的ＮＵＬＬ

```
<?php
$input = "foo\0bar";
if ($input == "foo") echo "$input is
    'foo'\n";
else echo "$input is not 'foo'\n";
echo "including " . $input . ".php\n";
include ($input . ".php");
?>
```

```
foobar is not 'foo'
including foobar.php
PHP Warning:  include(foo): failed to open
    stream: No such file or directory in
  /var/www/html/nullbyte.php on line 9
```

%00
Null Byte Design

聊一聊Nullbyte

ＰＨＰ中受影响的函数

copy(),is_file(),file_put_contents(),
file(),glob(),is_dir(),file_exists(),
fileatime(), filectime(),
filegroup(), fileinode(),
filemtime(), fileowner(),
fileperms(), filesize(), filetype(),
fopen(), is_executable(), is_link(),
is_readable(), is_writable(),
lchgrp(), lchown(), link(),
linkinfo(), lstat(), mkdir(),
pathinfo(), popen(), readfile(),
realpath(), rename(), rmdir(),
stat(), symlink(), touch(),

%00
Null Byte Design

聊一聊Nullbyte

ＮＵＬＬｂｙｔｅ防御

- 替换

```
$input = str_replace(chr(0), '',
 $input);
```

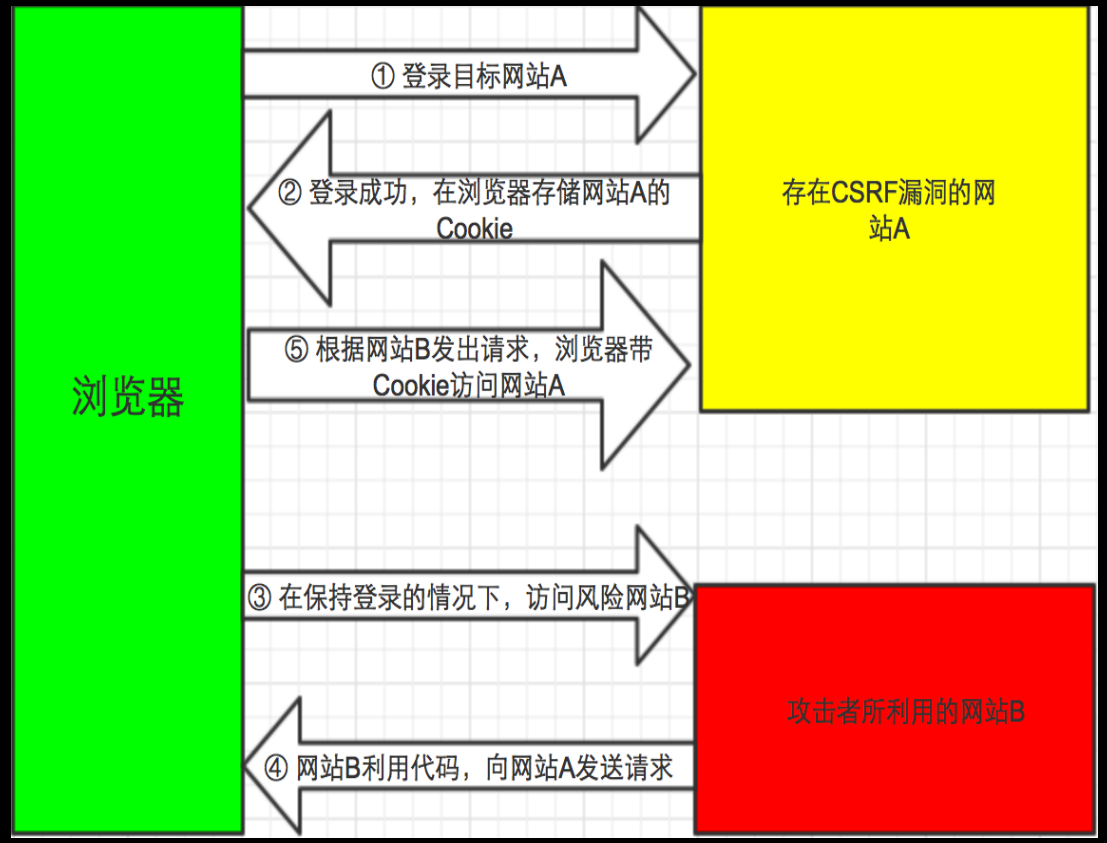
- 白名单
- 升级PHP版本

https://bugs.php.net/bug.php?id=39863

%00
Null Byte Design

CSRF(跨站请求伪造)

CSRF原理：



CSRF

Cross Site Request Forgery.

CSRF(跨站请求伪造)

CSRF代码示例

```
<script type="text/javascript">
    function steal(){
          iframe = document.frames["steal"];
      iframe.document.Submit("transfer");
  }
</script>
<body onload="steal()">
  <iframe name="steal" display="none">
     <form method="POST" name="transfer"
     action="http://www.myBank.com/Transfer.php">
         <input type="hidden" name="toBankId"
    value="11">
         <input type="hidden" name="money"
    value="1000">
       </form>
  </iframe>
```

CSRF(跨站请求伪造)

CSRF漏洞防御

- Cookie Hashing
- 验证码
- One-Time Tokens

CSRF

Cross Site Request Forgery.

Command Execution(命令执行)

命令执行相关函数

- exec
- passthru
- shell_exec
- system

> os command

Command Execution(命令执行)

命令执行代码示例

```
$status = $_GET['status'];
$ns  = $_GET['ns'];
$host   = $_GET['host'];
$query_type    = $_GET['query_type'];
$ip     = $_SERVER['REMOTE_ADDR'];
$self   = $_SERVER['PHP_SELF'];
system ("dig @$ns $host $query_type");

// demo
ns=whoami&host=sirgod.net&query_type=NS&stat
  us=digging
```

> os command

Command Execution(命令执行)

命令执行防御

- 避免用户输入
- 转义
  - escapeshellarg
  - escapeshellcmd

Code Execution(代码执行)

代码执行总结

- eval()
- preg_replace($pattern ,$replacement,$subject)
- dynamic variable(动态变量)
- create_function
- 其他
  - ob_start()
  - unserialize()
  - array_map()

Code Execution(代码执行)

代码执行示例

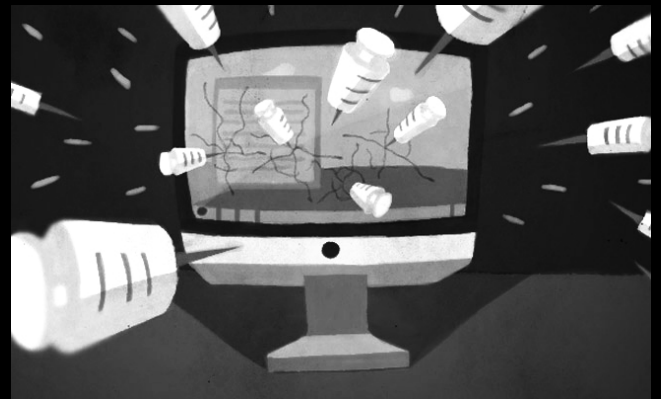
```
$code=$_GET['code'];
eval($code);
```

```
echo $regexp = $_GET['reg'];
$var = '<php>phpinfo()</php>';
preg_replace("/<php>(.*?
  )$regexp", '\\1', $var);
```

Code Execution(代码执行)

代码执行防御

- 禁用";"
- 过滤特殊字符"or"
- 使用白名单



其他漏洞

其他漏洞

- 逻辑漏洞
- 目录遍历
- 文件上传
- 会话劫持
- LDAP注入
- http拆分
- ....

PHP安全配置

PHP安全配置

PHP有大约283个配置项，安全相关的配置项大概有27项，常见的有：

allow_url_fopen

enable_dl

disable_functions

display_errors

expose_php

allow_url_include

file_uploads

open_basedir

.....

PHP漏洞防御

PHP漏洞防御:

- 知己知彼
  - 代码审计
  - 漏洞扫描
- WAF
  - Mod_security
  - suhosin

Questions…????

Thank You !!