安全沙龍

逐鹿

第一期：研发安全

如何建立有效的安全开发机制，保障应用的安全性，防止业务带病上线？

逐鹿

企业安全开发实践

止介 <feei@feei.cn>

目录

CONTENTS

01 开发安全思路

02 安全意识培训

03 安全开发组件

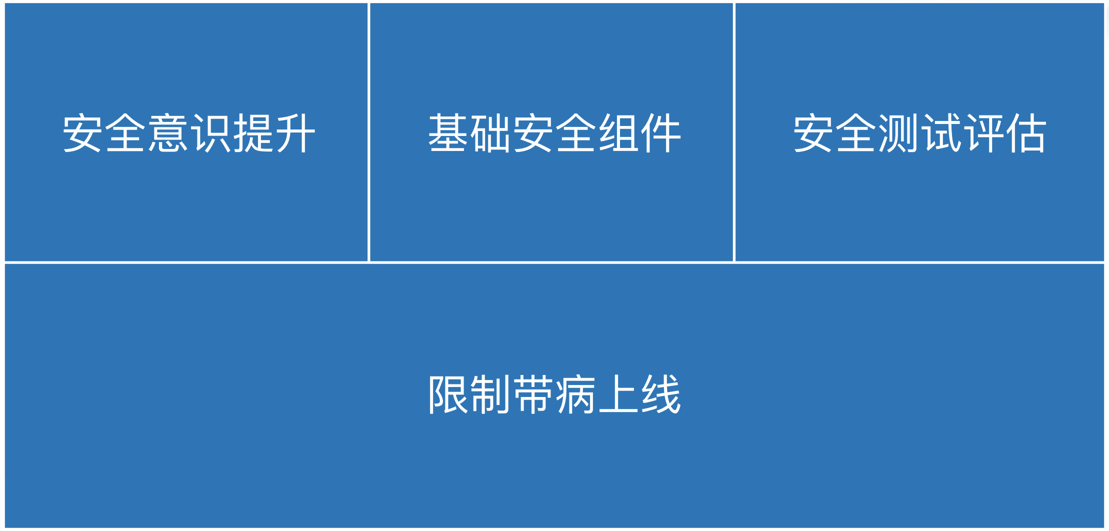
04 安全评估测试

05 限制带病上线

逐鹿

安全沙龍

开发安全思路



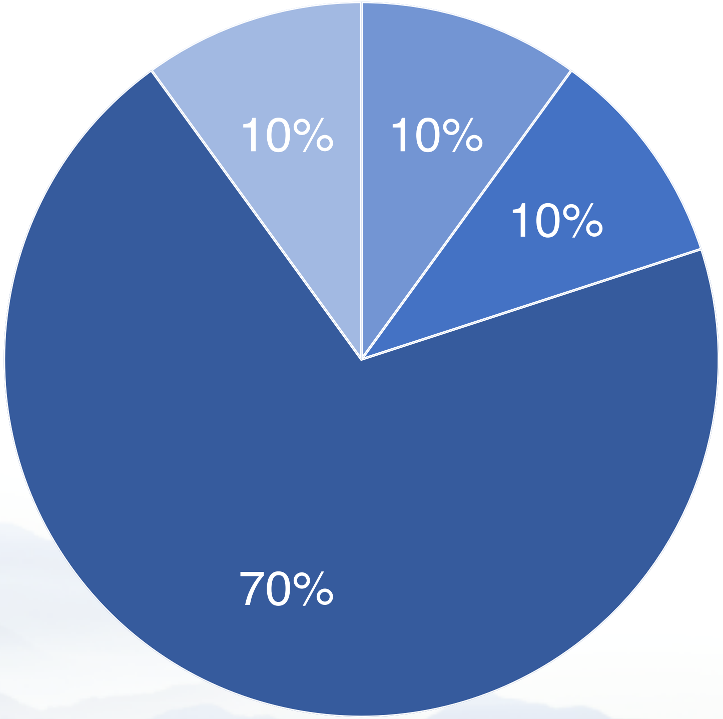
安全意识提升

基础安全组件

安全测试评估

限制带病上线

安全意识培训 - 背景



一点都不清楚
（10%）

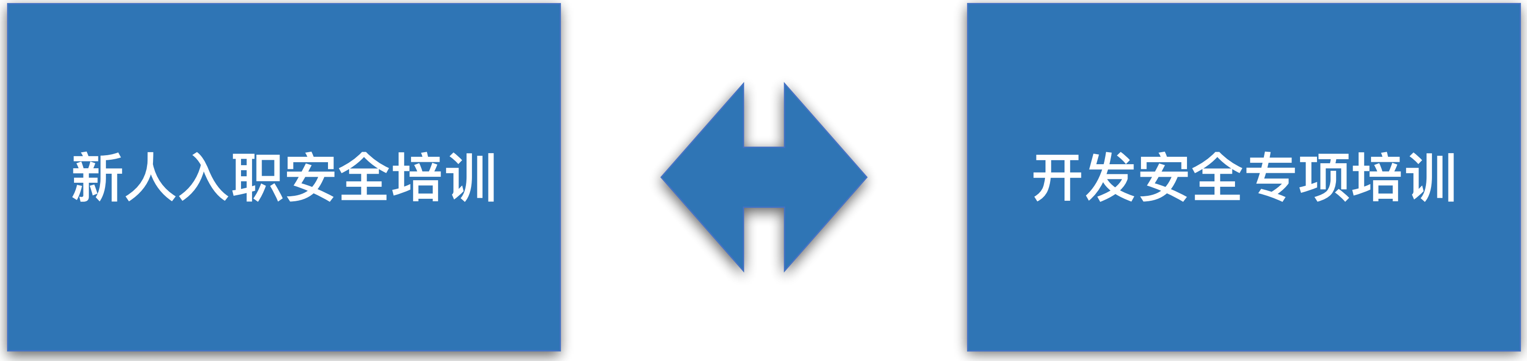
知道一点点
（70%）

很多都知道但不了解细节
（10%）

知道利用方法且会修复
（10%）

逐鹿
安全沙龍

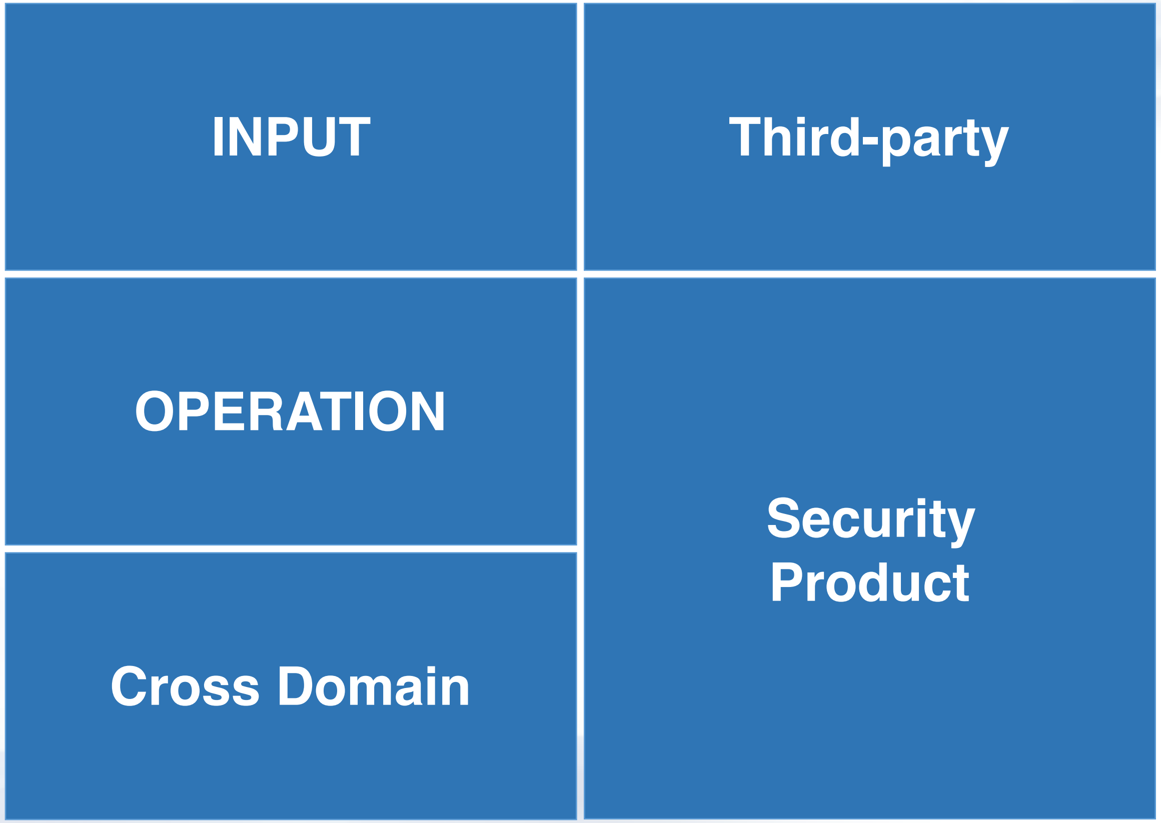
安全意识培训 - 培训



新人入职安全培训

开发安全专项培训

安全开发 - Frame



INPUT

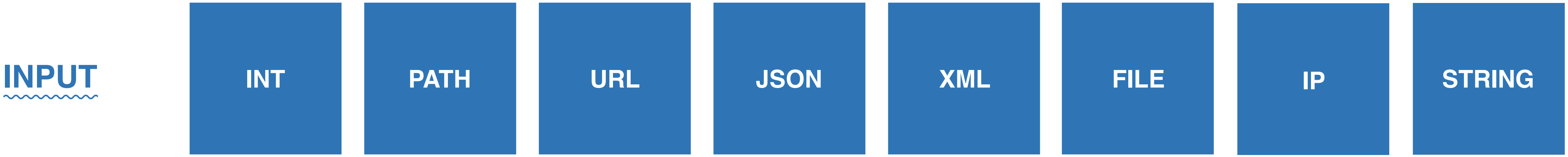
Third-party

OPERATION

Security Product

Cross Domain

安全开发 - INPUT



INPUT

INT

PATH

URL

JSON

XML

FILE

IP

STRING

安全开发 - VULNERABILITY

INPUT	INT	PATH	URL	JSON	XML	FILE	IP	STRING
VUL	SQL INJECTION	UNAUTH DOWNLOAD	UNAUTH REDIRECT /SSRF	Unserialize	XXE	UNAUTH UPLOAD	AUTH BYPASS	XSS

安全开发 - REPAIR

INPUT	INT	PATH	URL	JSON	XML	FILE	IP	STRING
VUL	SQL INJECTION	UNAUTH DOWNLOAD	UNAUTH REDIRECT /SSRF	Unserialize	XXE	UNAUTH UPLOAD	AUTH BYPASS	XSS
REPAIR	Mybatis	MAP	WHITELIST URL/ REQUEST SERVICE	Unserialize	DDD(True)	CDN/ OSS	REAL-IP	ENCODE

安全沙龍

安全开发 - CASE SQL INJECTION(Mybatis)

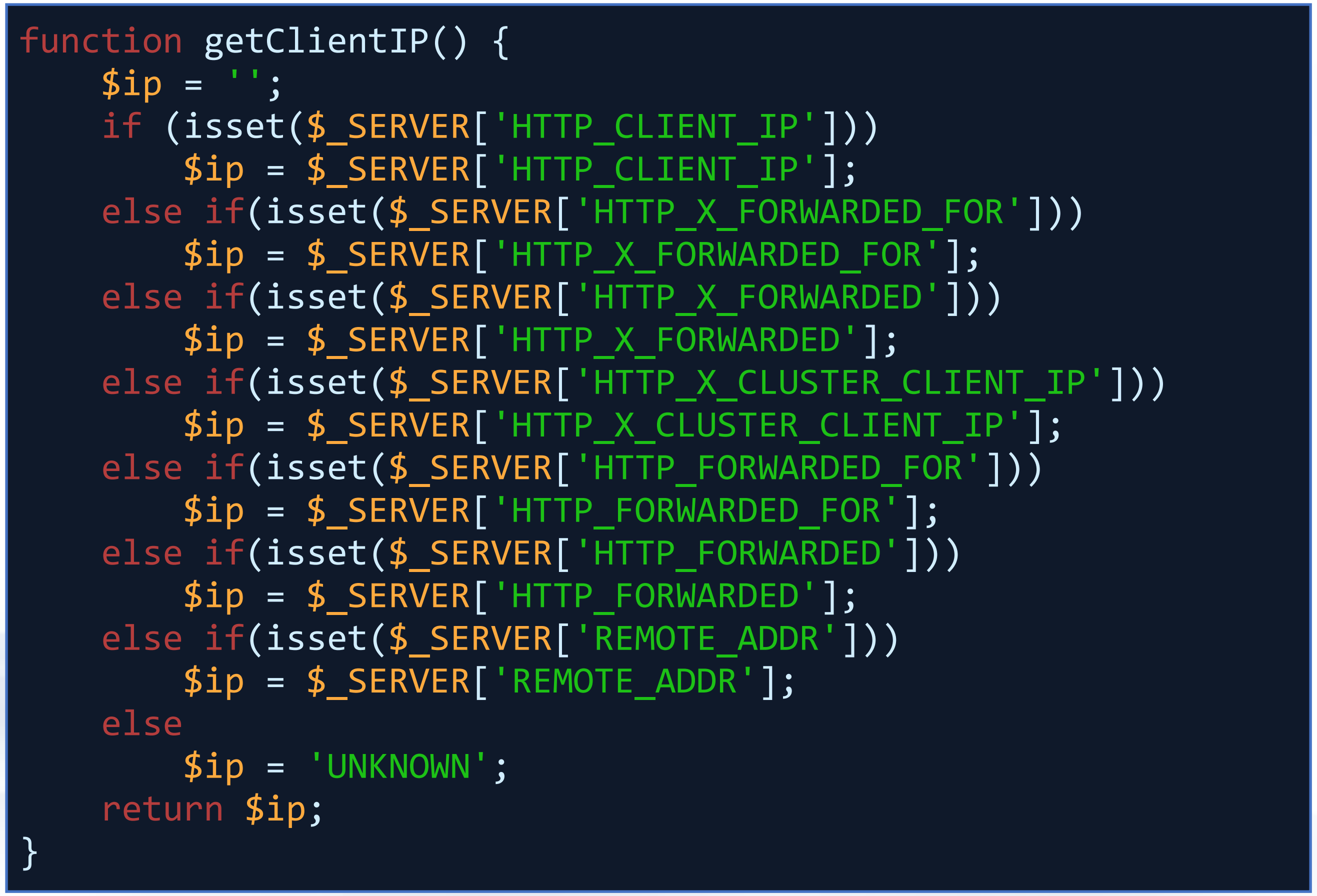
#

```
<select id="getPerson" parameterType=“int" resultType="org.application.vo.Person">
SELECT * FROM PERSON WHERE ID = #{id}
</select>
```

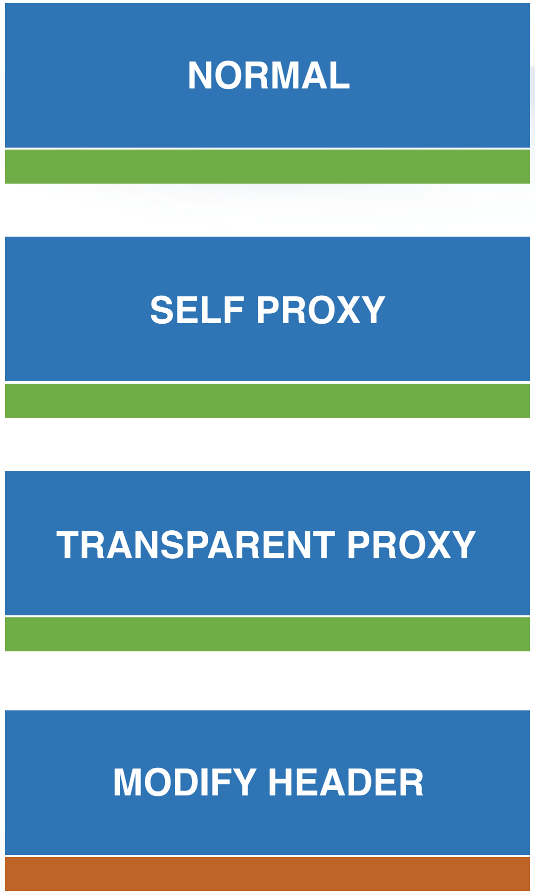
$

```
<select id="getPerson" parameterType="string"
resultType="org.application.vo.Person">
SELECT * FROM PERSON WHERE NAME = #{name} AND PHONE LIKE '${phone}';
</select>
```

安全开发 - CASE IP(Auth Bypass)



```php
function getClientIP() {
    $ip = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ip = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_X_CLUSTER_CLIENT_IP']))
        $ip = $_SERVER['HTTP_X_CLUSTER_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ip = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ip = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = 'UNKNOWN';
    return $ip;
}
```



NORMAL

SELF PROXY

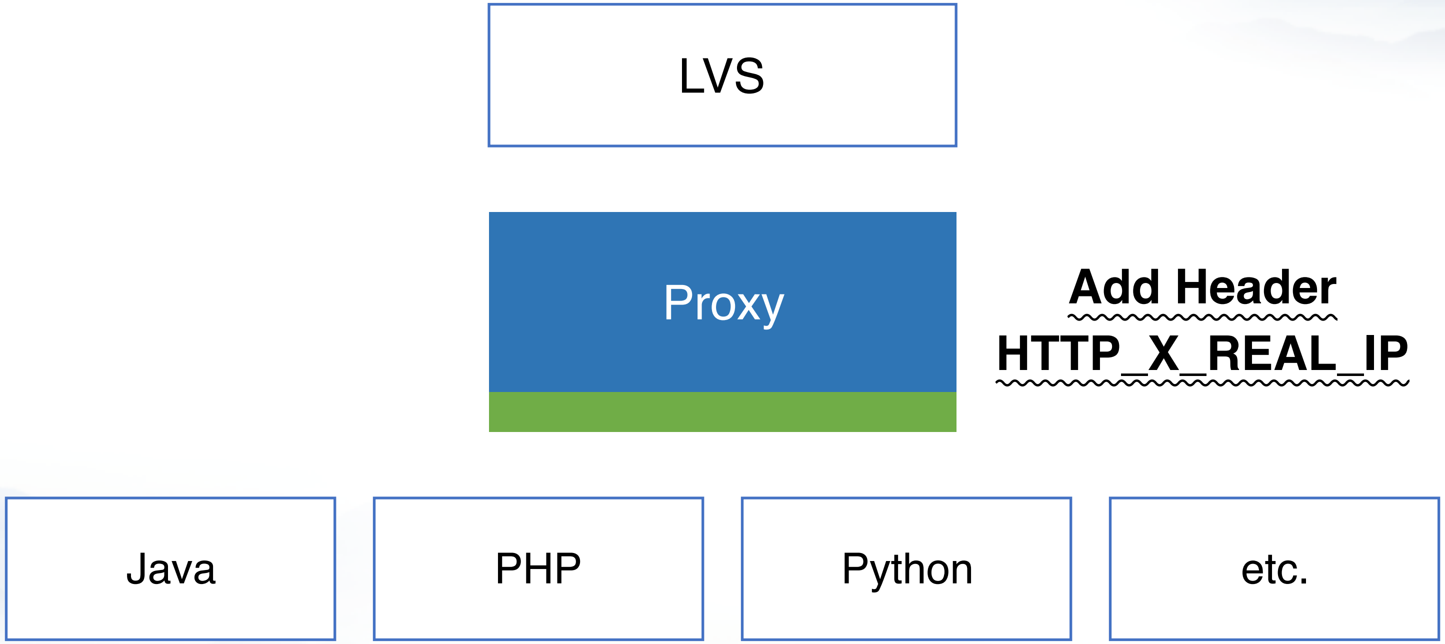
TRANSPARENT PROXY

MODIFY HEADER

安全开发 - CASE IP(Auth Bypass)

Normal	Transparent Proxy	Anonymous Proxy	High Anonymous Proxy
REMOTE_ADDR 🟩	REMOTE_ADDR 🟧	REMOTE_ADDR 🟩	REMOTE_ADDR 🟩
HTTP_VIA 🟧	HTTP_VIA 🟧	HTTP_VIA 🟧	HTTP_VIA 🟧
HTTP_X_FORWARDED_FOR 🟧	HTTP_X_FORWARDED_FOR 🟩	HTTP_X_FORWARDED_FOR 🟧	HTTP_X_FORWARDED_FOR 🟧

安全开发 - CASE IP(Auth Bypass)



Add Header
HTTP_X_REAL_IP

安全开发 - CASE URL(Unauth Redirect)

CONTAINS

```
if url.contains("mogujie.com") {
    return true;
}
```

attack.com/#mogujie.com
attack.com?mogujie.com

GET HOST + EQUALS

```
URL u = new URL(url);
String host = u.getHost().toLowerCase();
String domain = InternetDomainName.from(host).topPrivateDomain().toString();
if domain.equals('mogujie.com'){
    return true;
}
```

安全开发 - CASE URL(SSRF)

PROTOCOL
HTTP[S]

FOLLOW REDIRECT
OFF

WHITELIST URL
ON

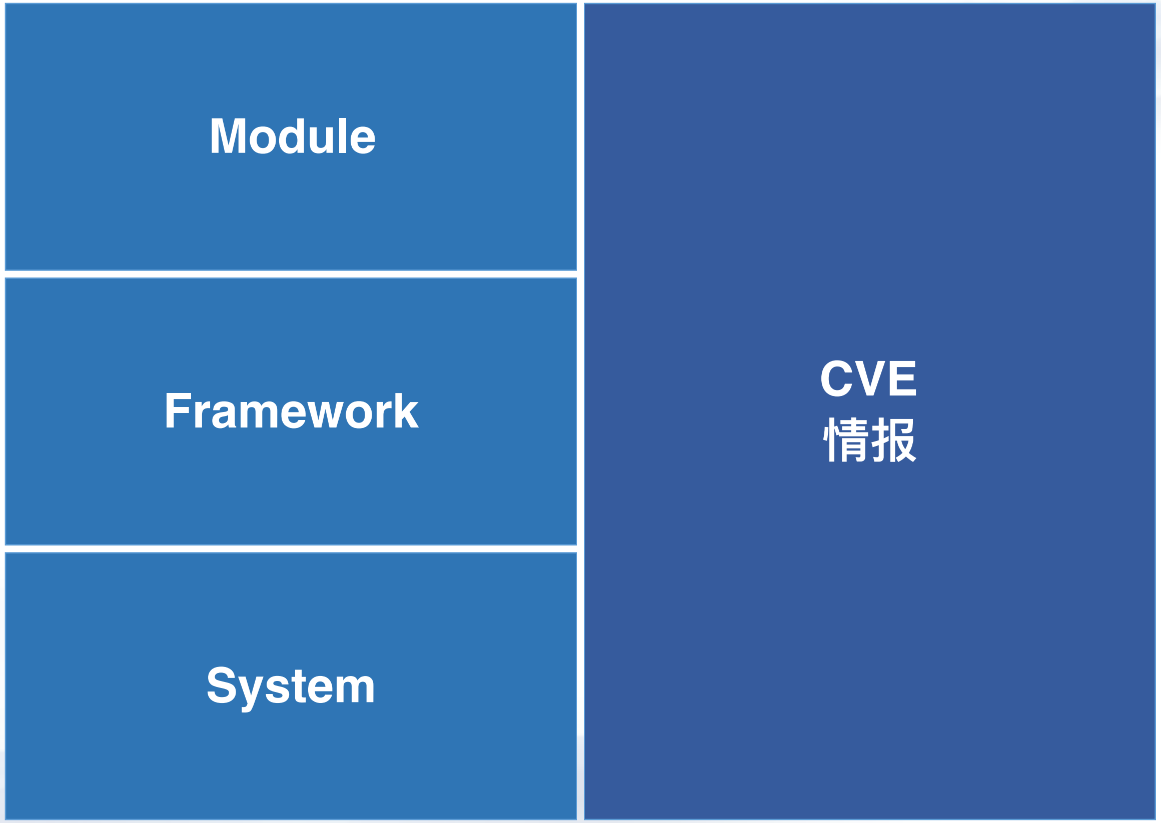
安全开发 - OPERATION

FRONT	Network	Backend
CSRF	Rate	Unauthorized
Token	WAF	Penetration

安全开发 - CROSS DOMAIN

JSONP	CORS
JSONP Hijack	ACAR Hijack
JSONP Token	Whitelist

安全开发 - THIRD-PARTY DEPENDENT



Module

Framework

System

CVE
情报

安全开发组件 - 基础安全产品服务

验证码

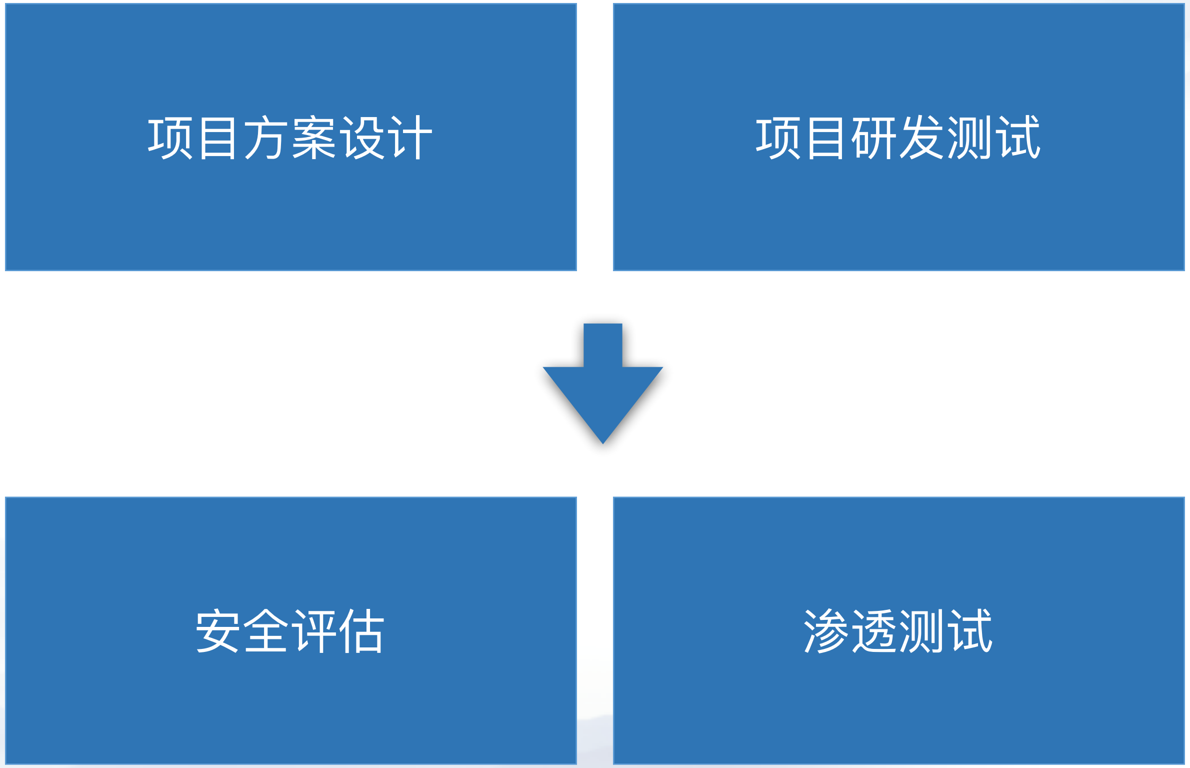
数字证书

反垃圾

设备指纹

…

安全评估测试 - 业务生命全流程



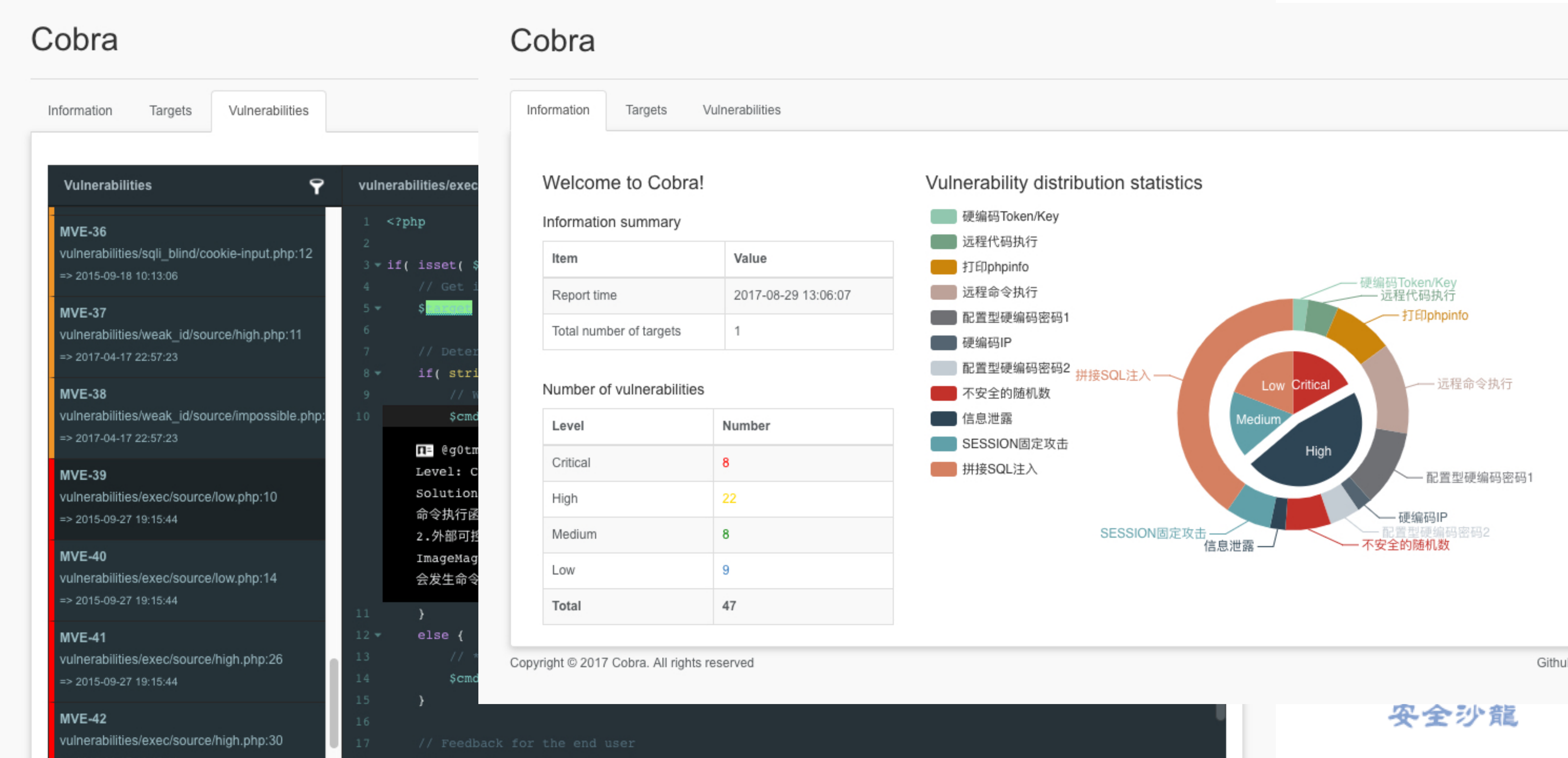
项目方案设计

项目研发测试

安全评估

渗透测试

限制带病上线 - 白盒代码安全检查



Cobra

Information　Targets　Vulnerabilities

Vulnerabilities

MVE-36
vulnerabilities/sqli_blind/cookie-input.php:12
=> 2015-09-18 10:13:06

MVE-37
vulnerabilities/weak_id/source/high.php:11
=> 2017-04-17 22:57:23

MVE-38
vulnerabilities/weak_id/source/impossible.php:
=> 2017-04-17 22:57:23

MVE-39
vulnerabilities/exec/source/low.php:10
=> 2015-09-27 19:15:44

MVE-40
vulnerabilities/exec/source/low.php:14
=> 2015-09-27 19:15:44

MVE-41
vulnerabilities/exec/source/high.php:26
=> 2015-09-27 19:15:44

MVE-42
vulnerabilities/exec/source/high.php:30

vulnerabilities/exec

```
<?php

if( isset( $
    // Get i
    $target

    // Deter
    if( stri
        // W
        $cmd
      @g0tm
      Level: C
      Solution
      命令执行函
      2.外部可控
      ImageMag
      会发生命令
    }
    else {
        // *
        $cmd
    }

    // Feedback for the end user
```

Cobra

Information　Targets　Vulnerabilities

Welcome to Cobra!

Information summary

Item	Value
Report time	2017-08-29 13:06:07
Total number of targets	1

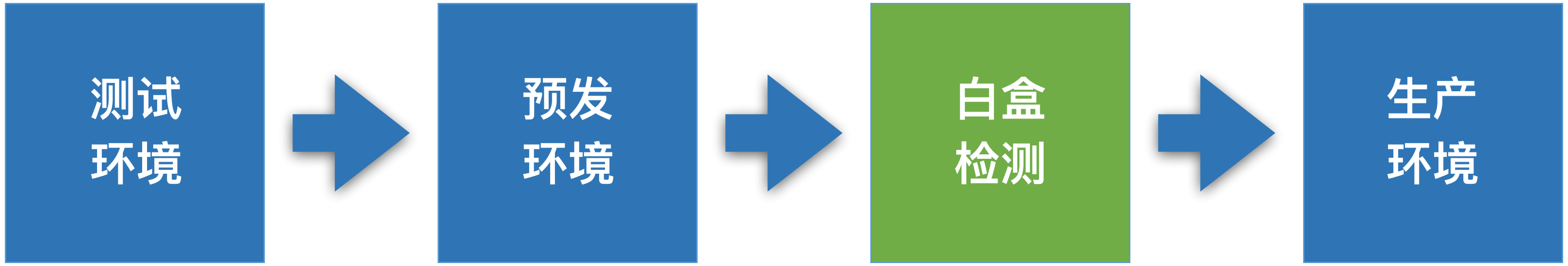
Number of vulnerabilities

Level	Number
Critical	8
High	22
Medium	8
Low	9
Total	**47**

Vulnerability distribution statistics

Githu

限制带病上线 - 发布系统卡口


测试环境

预发环境

白盒检测

生产环境

逆袭

安全沙龙

第一期：研发安全

[如何建立有效的安全开发机制，
保障应用的安全性，防止业务带病上线？]

感谢各位