

Onboard security in software companies 软件企业的安全之道

Wenjun Wang(王文君) Hewlett Packard Enterprise software security lead

Self introduction

- –Hewlett Packard Enterprise software security lead, responsible for BU security with \$1B revenue
- -10+ years enterprise software then security
- -CSSLP & CISSP
- -Co-author Web应用安全威胁与防治





王文君 李建蒙 编著





Vulnerabilities

Remote file downloading

搜索关键字: 任意文件下载 (共 1090 条纪录) 将未公开漏洞纳入搜索结果

上海青橙漏洞礼包(目录遍历/任意文件下载/敏感信息泄露/SQL注入等/已getshell)

RT...用的是泛微OA code 区域1: 目录遍历http://ftp.qingcheng...任意文件下载http://ftp.qingcheng.com/weaver/weaver.email.FileDownloadLocation?download=1&fileid=1 code 区域4: ge tshell 看了这个构造表单提交直接getshell无需登录 WooYun: 泛微某系统漏洞集合(不拿shell不是合格的白帽子) http://ftp.qingcheng.com/tools/SWFUpload/upload.jsp code 区域<form method='post' action='http://ftp.qingcheng.com/tools/SWFUpload/upload.jsp' enctype="multipart/form-data" > <...

提交日期: 2016-03-29 作者: 黑色键盘>

西安电子科技大学某分站一处任意文件下载

由于一个<mark>任意文件下载</mark>的漏洞导致用户验证代码泄露,构造出了普通用户到管理员的提权方法…由于一个<mark>任意文件下载</mark>的漏洞导致用户验证代码泄露,构造出了普通用户到管理员的提权方法,<mark>任意文件下载</mark>漏洞在这里: http://photo.xidian.edu.cn/download.asp?file=xxx 看到登录页面是admin_login.asp,下载下来看看 在这里它指向了Admin_ChkLogin.asp应该是验证成功后跳转到Admin_Index.asp,这里重点关注一下Admin_ChkLogin.asp ...

提交日期: 2016-03-28 作者: chengable

找小工Blind XXE案例

找小工Blind XXE案例,可<mark>任意文件下载</mark>。...问题主要发生在http://blog.gongren8.com/。使用了Z-blog,该系统存在Blind XEE问题。 00x01 在自己的主机上面添加接收文件,命令为get. php,代码如下 code 区域<?php file_put_contents('01.txt', \$_GET['xxe_local']); ?> 00x02 定义xml文件,文件名为xxe.xml,代码如下 code 区域<!ENTITY % info SYSTEM "php://filter/read-convert.base64-encode/resource=file:///c:/win...

提交日期: 2016-03-21 作者: 路人甲

長華電材股份有限公司任意文件下载

rt...目标:http://**.***.*** 构造 code 区域http://**.**.***.**/download.php?file=../includes/config_inc.php 数据库配置文件 code 区域http://**.***.***/download.php?file=../includes/config_inc.php 数据库密码泄露 code 区域error..<?php \$db_server = "localhost"; \$db_user = "CWEI"; // \$db_password = "Jessica"; -- Modified by Frank 2014/08/25, security issue. \$db_password = "muWTs qMsHD7L9SUK"; ...

提交日期: 2016-03-12 作者: 路人甲

Hewlett Packard Enterprise

Adhoc solution

What should do



漏洞概要

The fact

缺陷编号: WooYun-2016-189556

漏洞标题: 上海青橙漏洞礼包(目录遍历/任意文件下载/敏感信息泄露/SQL注入等/已getshell)

相关厂商: 上海青橙漏洞作者: 黑色键盘、

提交时间: 2016-03-29 11:24 公开时间: 2016-04-03 11:30 漏洞类型: 系统/服务运维配置不当

危害等级: 高 自评Rank: 20

漏洞状态: 漏洞已经通知厂商但是厂商忽略漏洞

漏洞来源: http://www.wooyun.org , 如有疑问或需要帮助请联系 help@wooyun.org

Tags标签: 目录遍历 敏感信息泄露 webserver服务配置不当

分享漏洞: 🚼 分享到 🔀 🚮 🔆 😰

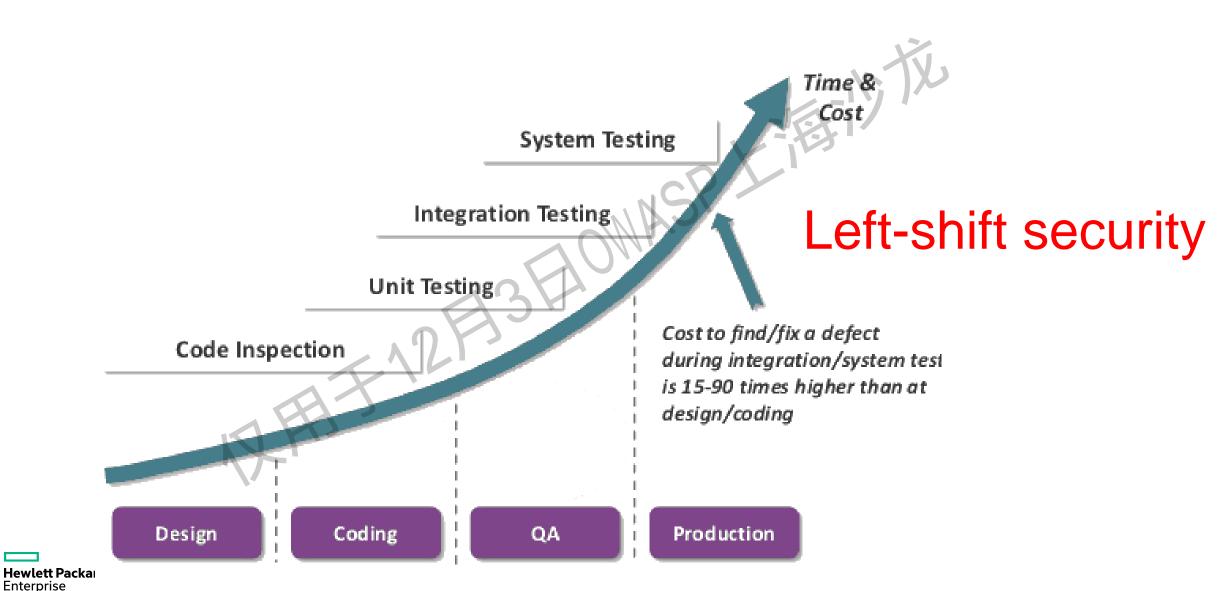
漏洞详情

Vendor ignores the vulnerability, then disclose publicly

披露状态:

2016-04-03: 厂商已经主动忽略漏洞,细节向公众公开

Cost to fix these issues



RnD's voice to security

Revenue driven

Legacy

I'm a developer

Security scanner

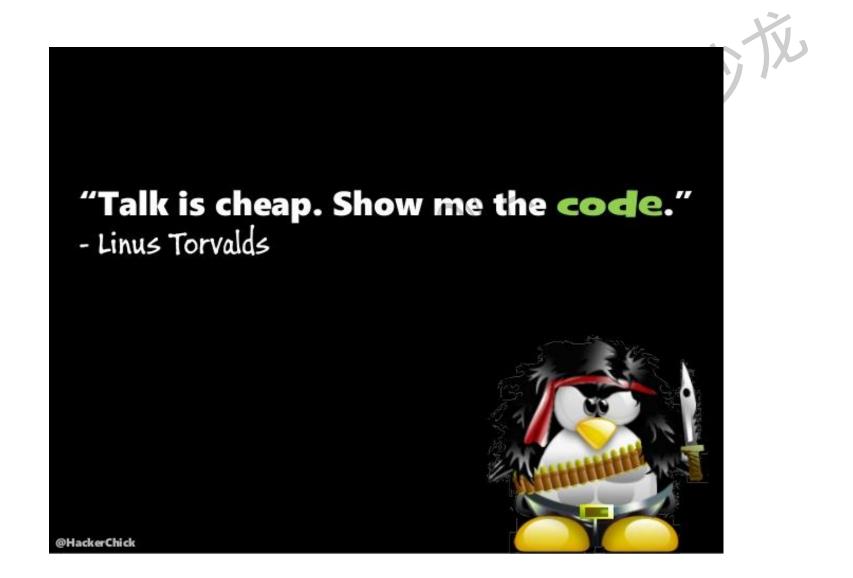


RnD's impression to security guys





RnD's expectation to security guys





Security guys' challenge

Product team



Security architect



Hewlett Packard Enterprise

Security as a quick start





1. Create security bug type

Security bug

- Severity
- Impact
- Released version

Verify success

- Meet release criteria
- Mitigation is provided

Damage

Reproducibility

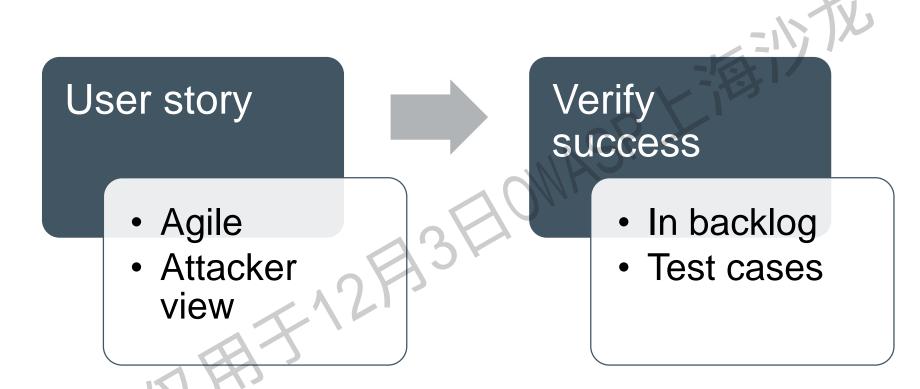
Exploitability

Affected users

Discoverability



2. Security user story



"As an [operator], I want to [do something] so that I can [derive a benefit]"

"As an [attacker], I want to [do something] so that I can [damage the system]"



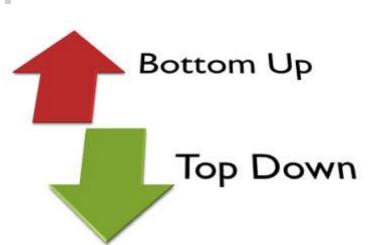
3. Security dashboard

Dashboard

- Aggregation
- Drill down

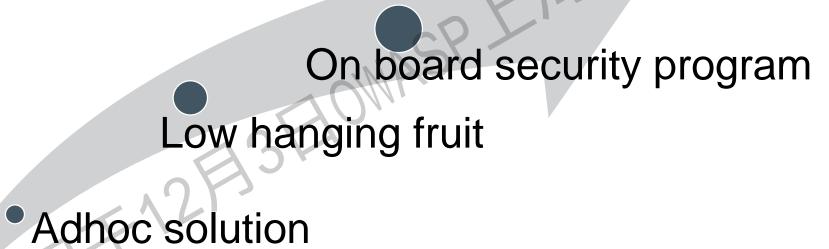
Verify success

- Stakeholders are aware
- Business decision





So evolve





Security program

- 1. Security awareness training
- 2. Security release criteria
- 3. Threat modeling and security design review
- 4. Security assessment
- 5. Risk response



Security awareness training

Diversity

- Management
- Dev
- QA



Options

- Instructor based
- Web based
- Event



Security release criteria

Risk

- DREAD
- CVSS3

Criteria

- Threshold
- Business balance



Threat modeling and security design review

Threat

- Threat list
- Refresh list

Review

- Security pattern
- Security user story



Security assessment

Automatic

- Static
- Dynamic

Manually

- Check list
- Pen test



Risk response

Pre-event

- 3rd party lib scan
- Subscription



Post-event

- Action plan
- Risk tracker



Apply what you learnt today

3 days

 Know security methodology in this document

3 weeks

 Handle low hanging fruit in your company

3 months

Start

 onboarding
 security
 program



To be continued



```
type="color" default="#204063" value="#204063">
<Variable name="blog"
                               "cription="Blog Title Color"
     type="color"
                                    e="#eef6fe">
                 .ult="#eef6fe
<Variable name
                                      cription="Blog Description Color"
     type="c stTitleColor" descri "cef6fe">
                                         Post Title Color"
<Variable na
             default="#477fba" val
     type=
                                        77fba">
            lateHeader BUG" descr
<Variable n
                                          "Date Header Color"
             default="#8facc8" valu acc8">
     type=
<Variable n
                                         on="Sidebar Title Color"
             debarHeaderColor" de
                                         809fbd">
     type=
               -fault="#809fbd" v
<Variable n
                                      ="Link Color"
                  inkColor" de
                                     ="#4386ce">
                                 " description="Visited Link Color"
                        ...2402a5" value="#2462a5">
                        "Color" description="Sidebar Link Color"
                          199be2" value="#599be2">
                         edLinkColor"
                        isited Link Color"
                       "#3372b6" value="#3372b6">
```



Hewlett PackardEnterprise

Thank you