



网络钓鱼防范： 钓鱼网站，钓鱼 邮件的防控

01

钓鱼网站防范

01

钓鱼邮件防范



扫码试看/订阅

《Web 安全攻防实战》视频课程

01 钓鱼网站防范



钓鱼网站



在网站安全建设越发完整的情况下，攻击者针对网站直接的入侵变得越发困难，把目光放在了网站用户或管理员身上。



钓鱼网站

▲ 不安全 | 192.168.1.23/login

Geekbang
极客邦科技

+86 ▾

11111111111

.....

👁

[忘记密码?](#)

登录

[免密登录](#)

第三方账号登录

👤

👤

👤

极客邦企业账号已上线, 来为团队买单,
[立即注册](#) →

© 2018 Geekbang Technology Ltd. All rights reserved

域名伪装:

域名折扣限时抢

geeekbang

.com

查询

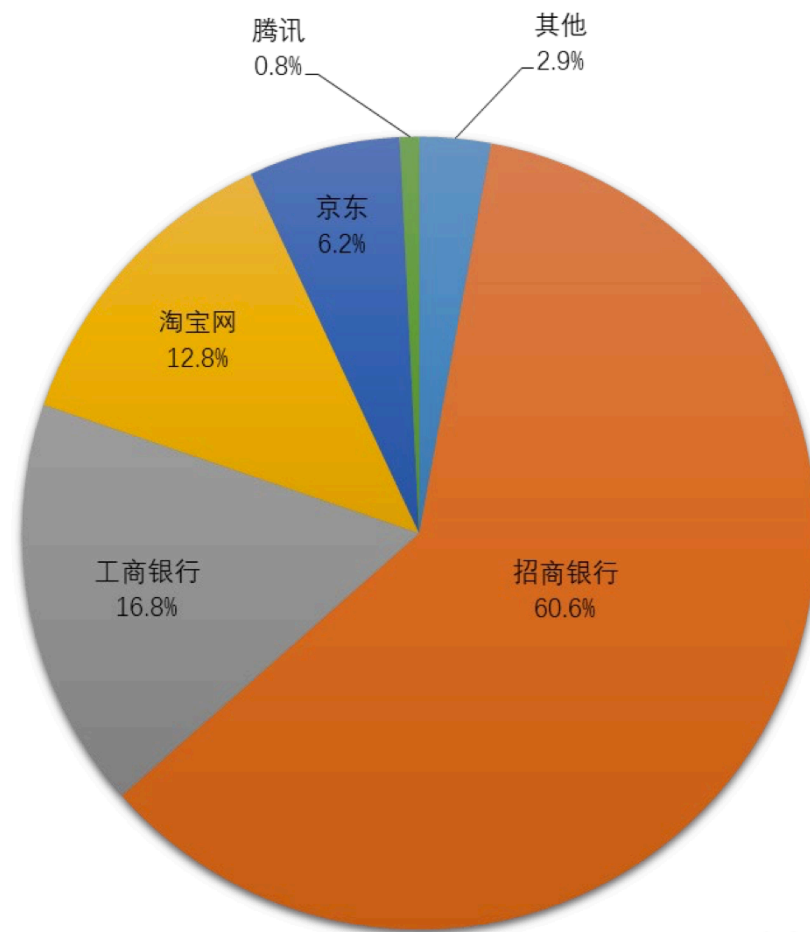
geeekbang .com

32元/首年 59元

[一键购买>](#)



钓鱼网站







2020年8月

图 3 钓鱼网站仿冒对象情况

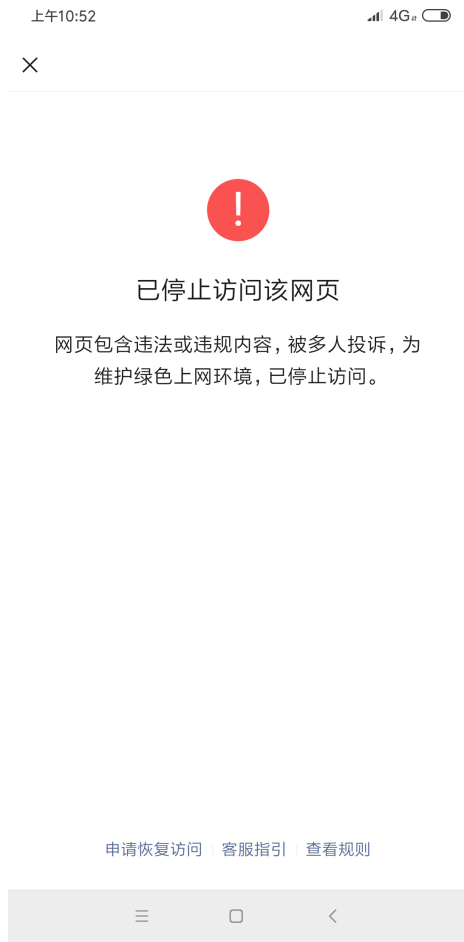


钓鱼网站防范

-  控制钓鱼网站传播途径。
-  用户教育。
-  关停站点。
-  自动化识别钓鱼网站。



控制钓鱼网站传播途径



- 通过 QQ、阿里旺旺、微信等客户端聊天工具传播钓鱼网站链接。
- 在搜索引擎，中小网站投放广告，吸引用户点击钓鱼网站。
- 通过微博，推特传播钓鱼网站。
- 结合钓鱼邮件使接受用户点击。



用户教育

- 使用户知道点击什么样的链接是相对安全的。
- 对于浏览器提示不安全的链接，不点击或不输入账号密码。
- 不要相信陌生人的说辞。

您用的是啥浏览器，我这里没有报网站的安全问题，你直接登录就可以了，没事的，如果你不相信，要不我把这个官方浏览器发给你，你试试就知道了？

网站=钓鱼网站

官方浏览器=病毒木马



关停站点



- DNS 运营商



- 云服务提供商



- 中国反钓鱼网站联盟（cn 域名）





自动化识别

钓鱼网站相比真实网站，在技术力和信息备案有差别，导致了功能缺陷，可用于自动化识别，如：

- 多次刷新页面。验证码不变。
- URL 异常
- 网站的备案信息
- 支付方式
- 网页链接

02 钓鱼邮件防范



钓鱼邮件

真实的钓鱼邮件，并不是错漏百出，除了恶意链接本身，它的真实度还原相当高。





钓鱼邮件防范

1. 公私邮箱要分离
2. 注意邮件的异常情况，如：
 - 乱码
 - 发件人异常
 - 日期异常
 - 异常链接
3. 不要使用公共场所的网络设备执行敏感操作



怎样建立安全
开发流程

01

安全开发流程

01 安全开发流程



安全开发

安全开发生命周期（SDL）包含一系列具有安全保证和合规性要求的实践。SDL 通过减少软件漏洞的数量和降低漏洞严重性，同时降低开发成本，帮助开发人员构建更安全的软件。



提供安全培训



定义安全需求



Provide Training

Ensure everyone understands security best practices.

Define Security Requirements

Continually update security requirements to reflect changes in functionality and to the regulatory and threat landscape.



定义指标和合规性报告



Define Metrics and Compliance Reporting

Identify the minimum acceptable levels of security quality and how engineering teams will be held accountable.

威胁建模



Perform Threat Modeling

Use threat modeling to identify security vulnerabilities, determine risk, and identify mitigations.



建立设计需求



Establish Design Requirements

Define standard security features that all engineers should use.



定义和使用的加密标准



Define and Use Cryptography Standards

Ensure the right cryptographic solutions are used to protect data.





管理使用第三方组件的安全风险

使用得到授权的工具



Manage the Security Risk of Using Third-Party Components

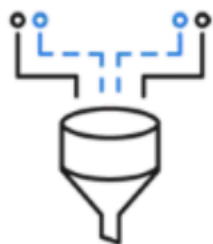
Keep an inventory of third-party components and create a plan to evaluate reported vulnerabilities.

Use Approved Tools

Define and publish a list of approved tools and their associated security checks.



静态代码分析



Perform Static Analysis Security Testing (SAST)

Analyze source code before compiling to validate the use of secure coding policies.



动态代码分析

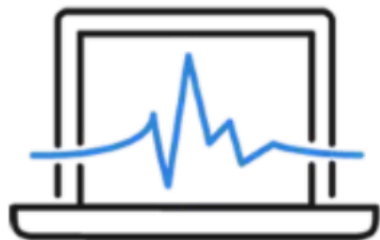


Perform Dynamic Analysis Security Testing (DAST)

Perform run-time verification of fully compiled software to test security of fully integrated and running code.



渗透测试



Perform Penetration Testing

Uncover potential vulnerabilities resulting from coding errors, system configuration faults, or other operational deployment weaknesses.

建立标准事件响应流程



Establish a Standard Incident Response Process

Prepare an Incident Response Plan to address new threats that can emerge over time.



扫码试看/订阅

《Web 安全攻防实战》视频课程