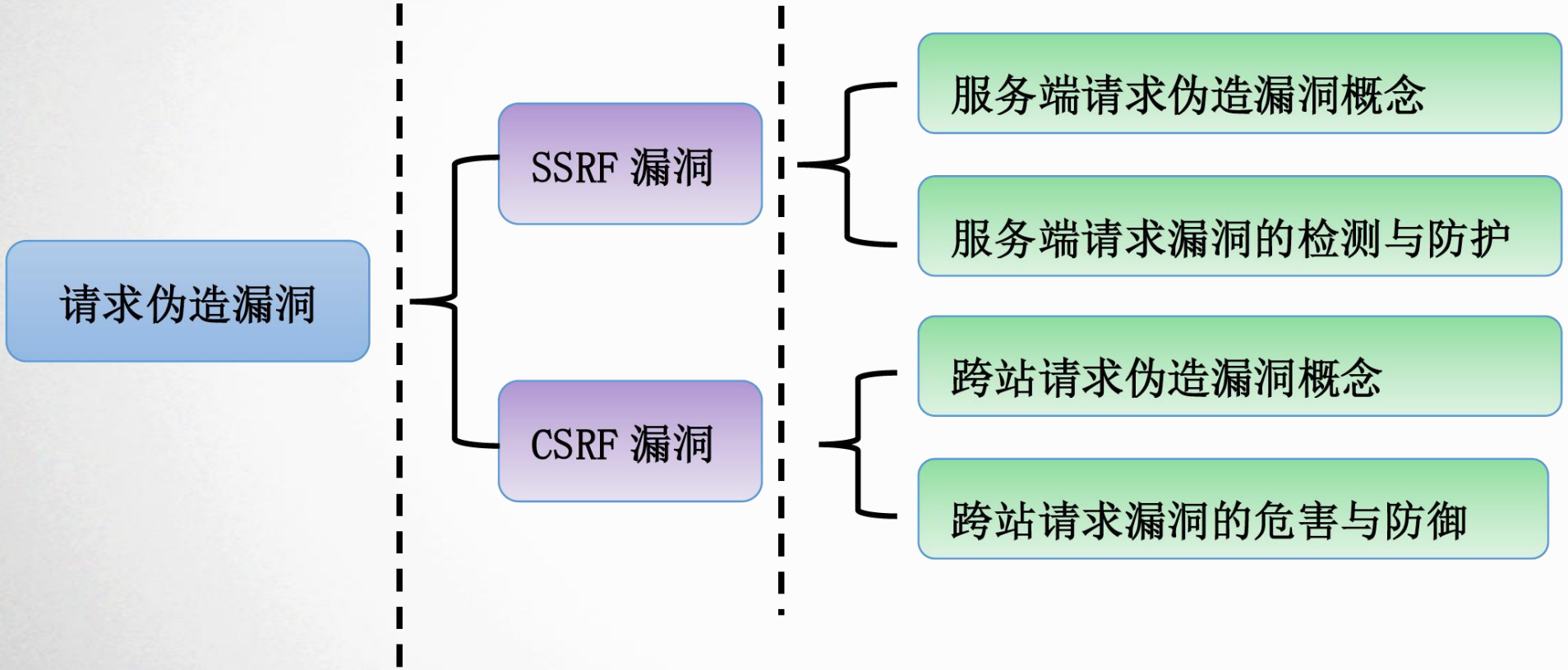
培训教育
Training Services

CISP-PTE

Web 安全基础(4) – 请求伪造漏洞

主讲：

请求伪造漏洞



SSRF漏洞

SSRF漏洞

- 通过本知识域，我们会：
  - 服务器请求伪造漏洞概念
    - 了解什么是SSRF漏洞
    - 了解利用SSRF漏洞进行端口探测的方法
  - 服务器请求伪造漏洞的检测与防护
    - 掌握SSRF漏洞的检测方法
    - 了解SSRF漏洞的修复方法

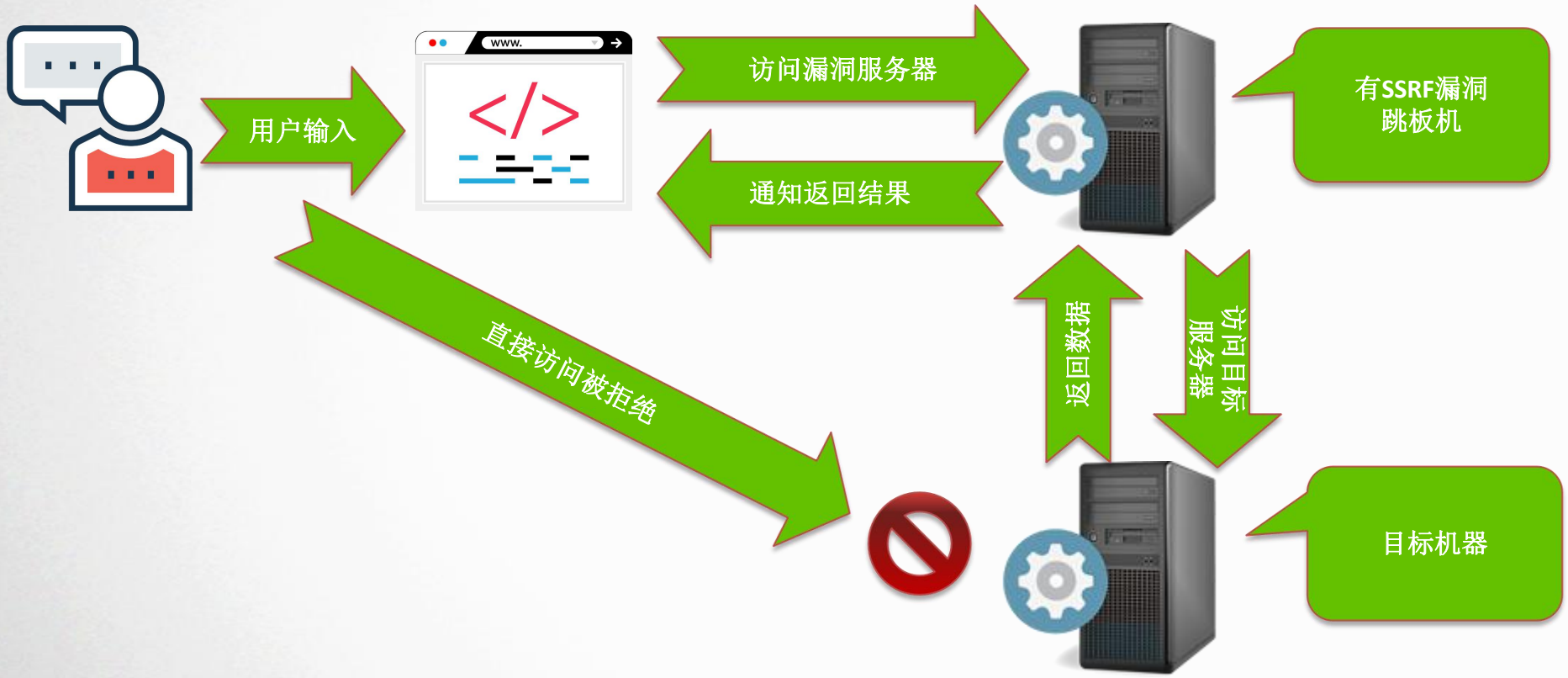
服务器请求伪造漏洞概念

- 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞
- 一般情况下，SSRF攻击的目标是从外网无法访问的内部系统
- 可以对外网、内网、本地进行端口扫描，某些情况下端口的Banner会回显出来（比如3306的）
- 使用file:///协议读取本地文件

SSRF漏洞出现的原因

- 很多web应用都提供了从其他的服务器上获取数据的功能。使用用户指定的URL，web应用可以获取图片，下载文件，读取文件内容等。这个功能如果被恶意使用，可以利用存在缺陷的web应用作为**代理**攻击远程和本地的服务器。当攻击者提供的是一个企业私网IP时，服务器可能会访问对应网址当前后把结果返回
- 如果应用程序对用户提供的URL和远端服务器返回的信息没有进行合适的验证和过滤，就可能存在这种服务端请求伪造的缺陷。Google,Facebook,Adobe,baidu,tencent等知名公司都被发现过这种漏洞。攻击者利用ssrf可以实现的攻击主要为绕过网络限制攻击企业内网

服务器请求伪造漏洞概念图



SSRF漏洞攻击方式

- 攻击者利用ssrf可以实现的攻击主要有5种：
  - 信息收集：可以对外网、服务器所在内网、本地进行端口扫描，获取一些服务的banner信息;
  - 信息收集：对内网web应用进行指纹识别，通过访问默认文件实现;
  - 执行指令：攻击内外网的web应用，主要是使用get参数就可以实现的攻击（比如struts2，sqli等）；
  - 执行指令（溢出）：攻击运行在内网或本地的应用程序（比如溢出）；
  - 信息收集：利用file协议读取本地文件等。

SSRF漏洞产生的原因

- 以下业务场景容易出现这种漏洞：
  - 应用从用户指定的url获取图片。然后把它用一个随即文件名保存在硬盘上，并展示给用户
  - 应用获取用户制定url的数据（文件或者html）。这个函数会使用socket跟服务器建立tcp连接，传输原始数据
  - 应用根据用户提供的URL，抓取用户的web站点，并且自动生成移动wap站
  - 应用提供测速功能，能够根据用户提供的URL，访问目标站点，以获取其在对应经纬度的访问速度

如何利用SSRF漏洞进行端口探测

- URL里包含端口：
  - http://192.168.1.64/ssrf2.php?url=http://192.168.1.64:22
- 返回值：
  - SSH-2.0-OpenSSH_6.6.1 Protocol mismatch

SSRF漏洞检测方法

- PHP
  - file_get_contents()
    fsockopen()
    curl_exec()
    以上三个函数使用不当会造成SSRF漏洞
    大部分 PHP 并不会开启 fopen 的 gopher wrapper
    file_get_contents 的 gopher 协议不能 URLencode
    file_get_contents 关于 Gopher 的 302 跳转有 bug，导致利用失败
    curl/libcurl 7.43 上 gopher 协议存在 bug（截断），经测试 7.49 可用
    curl_exec() //默认不跟踪跳转，
    file_get_contents() // file_get_contents支持php://input协议

SSRF漏洞检测方法（续）

- JSP
  - 以下几种类引用不当会造成SSRF，需要进行检测
    Request类，URL类的openStream，HttpClient类，URLConnection和HttpURLConnection类，

SSRF漏洞检测方法（续）

- 绕过方法（需要检测）
  - 添加端口号
  - 短网址绕过
  - 指向任意IP的域名xip.io
    - 10.0.0.1.xip.io resolves to 10.0.0.1
    - www.10.0.0.1.xip.io resolves to 10.0.0.1
    - mysite.10.0.0.1.xip.io resolves to 10.0.0.1
    - foo.bar.10.0.0.1.xip.io resolves to 10.0.0.1
  - IP限制绕过
  - 十进制转换 八进制转换 十六进制转换 不同进制组合转换
  - 协议限制绕过

SSRF漏洞修复方法

- 过滤返回信息，验证远程服务器对请求的响应是比较容易的方法
  - 如果web应用是去获取某一种类型的文件，那么在把返回结果展示给用户之前先验证返回的信息是否符合标准
- 统一错误信息，避免用户可以根据错误信息来判断远端服务器的端口状态。
- 限制请求的端口为http常用的端口，比如,80,443,8080,8090
- 黑名单内网IP，避免应用被用来获取内网数据，攻击内网。
- 禁用不需要的协议，仅仅允许http和https请求。

CSRF漏洞

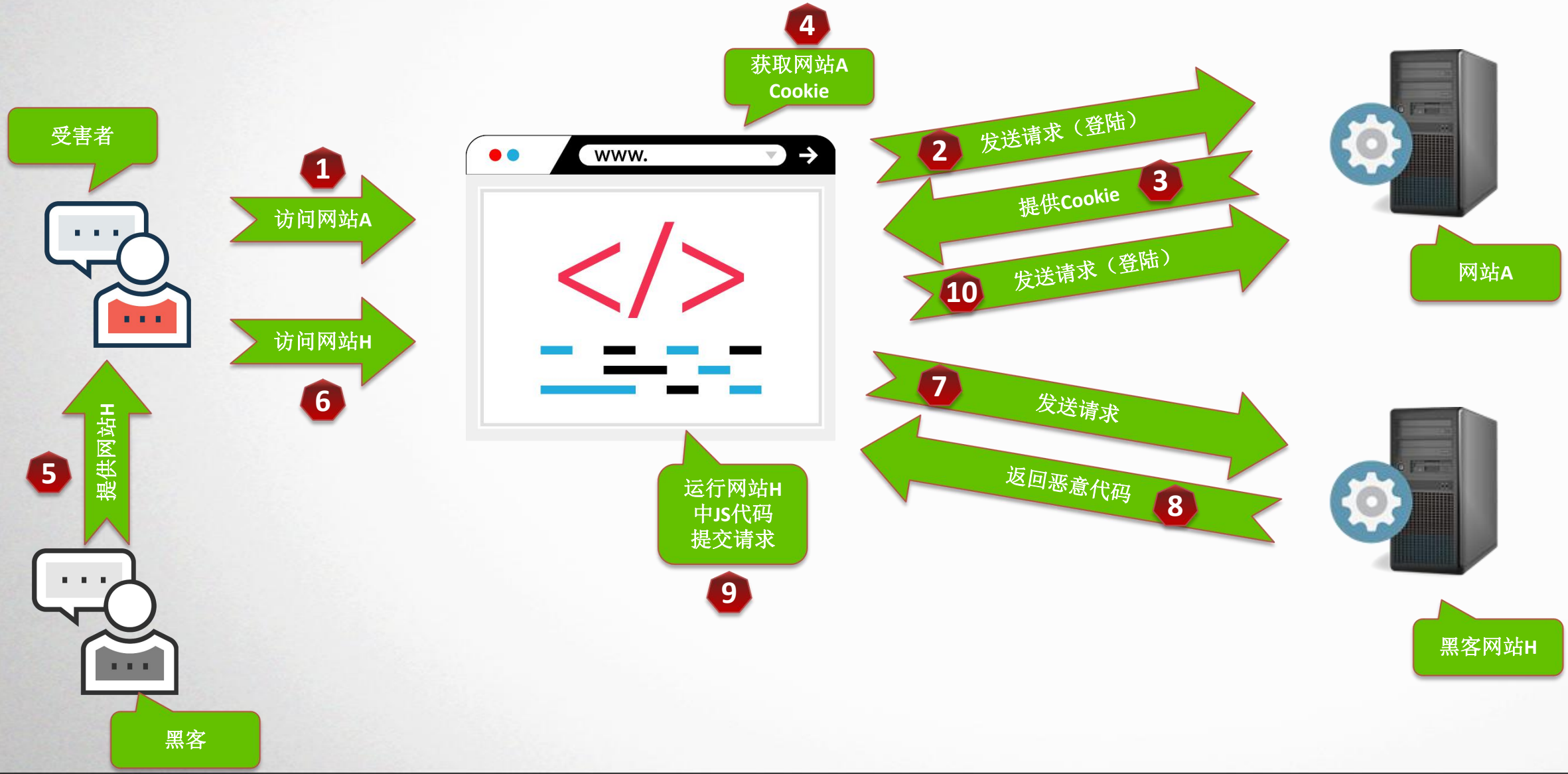
SSRF漏洞

- 通过本知识域，我们会：
  - 跨站请求伪造漏洞的原理
    - 了解CSRF漏洞产生的原因
    - 理解CSRF漏洞的原理
  - 跨站请求伪造漏洞的危害与防御
    - 了解CSRF漏洞与XSS漏洞的区别
    - 掌握CSRF漏洞的挖掘和修复方

CSRF概念

- CSRF 的全称是Cross-site request forgery，即跨站请求伪造，我们可以简单的理解这种漏洞为，攻击者利用被攻击者的身份发起了某些被攻击者原本不知情的网络请求。包括以被攻击者的身 份发布一条微博，以被攻击者的身份发布一条留言，以被攻击者的身份关注某个用户的微博等。
- CSRF能够做的事情包括
  - 以你名义发送邮件
  - 发消息
  - 盗取你的账号
  - 购买商品
  - 虚拟货币转账

CSRF原理图



CSRF漏洞产生的原理说明

- 跟其它漏洞不同，此类漏洞需要特定的条件。
  - 受害者必须登陆过网站（或者有权限）
  - 攻击者（或黑客）提供的恶意链接受害者必须打开
  - 网站除了验证Cookie，没有特殊验证方法
- 满足上面条件时，会利用到CSRF漏洞。