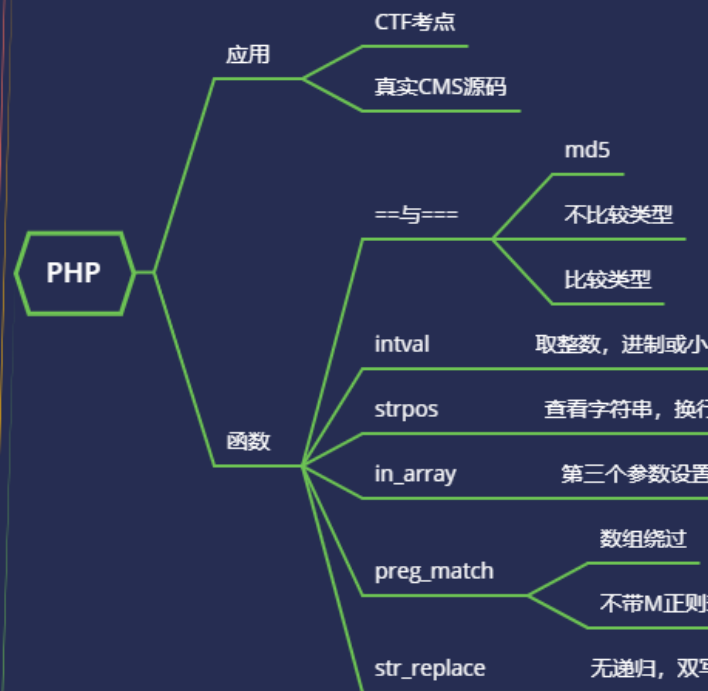
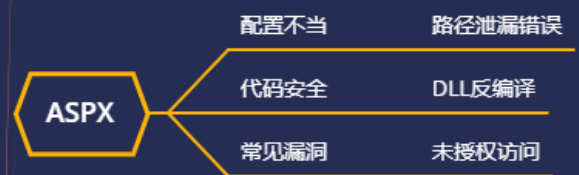


WEB 攻防-通用漏洞&XSS 跨站
&MXSS&UXSS&FlashXSS&PDFXSS



#知识点:

1、XSS 跨站-原理&攻击&分类等

2、XSS 跨站-MXSS&UXSS&FlashXss&PDFXSS 等

1、原理

指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。通过在用户端注入恶意的可执行脚本，若服务器对用户的输入不进行处理或处理不严，则浏览器就会直接执行用户注入的脚本。

-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

关键词、标签、说明

文件上传

2、分类

反射型（非持久型）

存储型（持久型）

DOM 型

mXSS (突变型 XSS)

UXSS（通用型 xss）

Flash XSS

UTF-7 XSS

MHTML XSS

CSS XSS

VBScript XSS

3、危害

网络钓鱼，包括获取各类用户账号；

窃取用户 cookies 资料，从而获取用户隐私信息，或利用用户身份对网站执行操作；

劫持用户（浏览器）会话，从而执行任意操作，例如非法转账、发表日志、邮件等；

强制弹出广告页面、刷流量等；

网页挂马；

进行恶意操作，如任意篡改页面信息、删除文章等；

进行大量的客户端攻击，如 ddos 等。

演示案例：

- UXSS-Edge&CVE-2021-34506
 - FlashXSS-PHPWind&SWF 反编译
 - PDFXSS-PDF 动作添加&文件上传
-
-

#MXSS: <https://www.fooying.com/the-art-of-xss-1-introduction/>

#UXSS 全称 Universal Cross-Site Scripting

UXSS 是利用浏览器或者浏览器扩展漏洞来制造产生 xss 并执行代码的一种攻击类型。

MICROSOFT EDGE uXSS CVE-2021-34506

Edge 浏览器翻译功能导致 JS 语句被调用执行

<https://www.bilibili.com/video/BV1fX4y1c7rX>

#Flashxss-swf 引用 js 的 xss

JPEXS Free Flash Decompiler

phpwind SWF 反编译 Flashxss

ExternalInterface.call 执行 JS 代码

Payload:

```
/res/js/dev/util_libs/jPlayer/Jplayer.swf?jQuery=alert(1))}catch(e){}//
```

#PDFXSS-上传后直链触发

- 1、创建 PDF，加入动作 JS
- 2、通过文件上传获取直链
- 3、直链地址访问后被触发

涉及资源：

补充：[涉及录像课件资源软件包资料等下载地址](#)
