WEB 渗透入门——XSS

XSS 简介

XSS 攻击就是在网站中嵌入客户端恶意脚本代码 ,这些脚本代码一般是通过【JavaScript】来写的。一般来说，一旦出现 XSS 注入漏洞，那么就可以 通过这个漏洞执行我想要执行的【JavaScript】脚本代码。所以要深入 XSS 攻击，首先要做到的精通【JavaScript】。

简单的 XSS 攻击

首先放一段在简单的【index.php】代码。

```php
<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){
  $isempty = true;
} else {
  echo '<pre>';
  echo 'Hello ' . $_GET['name'];
  echo '</pre>';
}
```

实现功能：输入名字，输出【hello 名字】

我们来看看实际的效果

我们输入【xiaobai】，回显【hello xiaobai】

这段代码是没有对用户的输入进行任何过滤的，所以我们可以轻松的构造【JavaScript】代码来进行攻击。下面介绍最最简单经典的【JavaScript】的 XSS 攻击代码。

】这对脚本标签，实现【alert】弹窗警报。

通过成功弹窗，就可以证实【JavaScript】代码顺利执行，存在【XSS】漏洞。

XSS 危害

XSS 漏洞基本上是通过执行【JavaScript】脚本代码来实现的，那么【JavaScript】到底能有多大的威力呢？

获取用户的 cookie 信息。如果被获取到的是管理员的用户信息，那么这个危害性和通过 SQL 注入直接【get shell】是没有区别的，就是说整个网站就已经被拿下了。

获取到用户的 cookie 值，就是相当于【攻击者】可以以【该用户】的身份进行后面的所有操作，可能会涉及到【盗取银行账户】、【修改密码】、【转账】、【参与 Ddos 攻击】等等。

导航到恶意网站。比如说你在浏览某个网站的时候，突然弹窗出来说“请移步到我们的新网站：www.XSShacker.com”，然后你没有怀疑的就点进去了，那么恭喜你，你是中招了。假如这个链接是指向一个恶意的脚本文件，那么攻击者还可能可以有后续操作。

XSS 分类

XSS 大致可以分为【反射型 XSS】、【存储型 XSS】和【DOM 型 XSS】。其中【DOM 型 XSS】涉及到标签节点，节点树等内容，一言半语无法解释清楚，故不展开介绍。下面介绍一下【反射型】和【存储型】。

反射型 XSS

反射型 XSS，就是当攻击者使用【XSS 代码】攻击的时候，服务端处理数据后，会马上返回这段【XSS 代码】请求的数据到浏览器，浏览器解析后造成【XSS 漏洞】。上面【简单的 XSS 攻击】就是一个反射型 XSS。

可能有的人会不以为意，其实介绍的只是最最简单的一个【XSS 攻击】，实际上，可以通过【反射型 XSS】实现获取用户的【cookie】信息，并伪造成用户成功登陆某网站获取敏感信息。

存储型 XSS

存储型 XSS 是最危险的一种【跨站脚本】。【存储型 XSS】不像【反射型】和【DOM 型】那样需要用户手动去触发，它是存储在服务器的某个地方，当用户访问特地的页面的时候，就会自动的执行。【存储型 XSS】具有很高的隐蔽性和危害性