HACKTHEBOX

ATTACKING AUTHENTICATION MECHANISMS

CHEAT SHEET

Attack	Description
JWT	
`Missing Signature Verification`	Can freely make any changes to the JWT token
`None Algorithm Attack`	Use 'none' as 'alg' in the JWT header, and empty signature after last.
`Weak Secret`	Brute force token secure with `~/go/bin/gojwtcrack -t tokens.txt -d /usr/share/wordlists/rockyou.txt`
`Insecure KID Parameter Processing`	Try command injection in the `kid` field in the JWT header, like `"kid": "\"'(){}[]&;/'(}{'£%^"`
OAuth	
`redirect_uri Misconfiguration`	Change `/?redirect=` to our IP and use the link in phishing to capture tokens
`Brute Forcing Weak Access Tokens`	Brute force token secure with a python script to obtain authenticated token
SAML	
`Weak Public/Private Keys`	Use public key/cert with OSINT to find respective private key/cert, then use them to modify requests and obtain access as another user

Attack	Description
No Signature Verification	Use any signature to modify requests and obtain access as another user
Signature Stripping Attack	Use empty signature values to modify requests and obtain access as another user

HTB ACADEMY CHEATSHEET