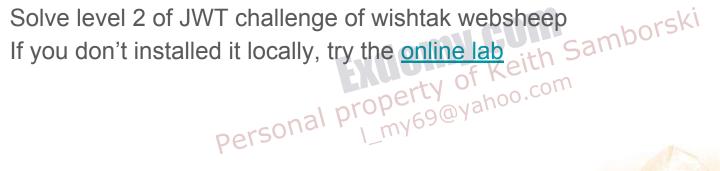
Exilemy Com samborski Web Service Attacks

JSON Web Token



JSON Web Token

- Solve level 2 of JWT challenge of wishtak websheep





JSON Web Token - Solution

- As mentioned in the lesson hint, we must try fuzzing the application and the only place we can supply our inputs is in the Login Form
- Try logging in with both valid and invalid credentials, can you see some kind of flaw/pattern?
- Notice the JWT_HMAC_SECRET in error details when you enter invalid credentials
 - Using this secret key you can sign any JWT token for any user you want (you can also find out the token structure using given credentials (foobar:123456))

```
Verrors: [{type: "technical-error",...}]}
Verrors: [{type: "technical-error",...}]
V0: {type: "technical-error",...}
V0: {type: "technical-error",...}
Venvironment: {npm_config_cache_lock_stale: "60000", npm_config_ham_it_up: "", npm_config_legacy_bundling: "",...}
HOME: "/root"
HOSTNAME: "24b262674aac"
INIT_CND: "/wishtack-websheep"
JAVA_HOME: "/jdkl.6.0_45"
JWT_HMAC_SECRET: "MY_INSECURE_JWT_HMAC_SECRET"
NODE: "/usr/bin/node"
OLDPWD: "/wsbGoat-OMASP_Standard-5.3_RC1"
PATH: "/usr/lib/node modules/npm/node_modules/npm-lifecycle/node-gyp-bin:/wishtack-websheep/node_modules/.bin:/
PMD: "/wishtack-websheep"
SHLVL: ""
SHOW_SOLUTION: "true"
```



JSON Web Token - Solution - Contd.

You can find the solution written in Javascript here:

http://lab.awh.exdemy.com/websheep/jwt/v2/solution







ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com