EXPLOITING VERSION CONTROL SYSTEMS

PILLAGING FOR FUN AND PROFIT

BY

ANANT SHRIVASTAVA

ANANT SHRIVASTAVA

- Information Security Consultant
- Admin - Dev - Security
- null + OWASP + G4H
- http://anantshri.info and @anantshri
- Trainer : Blackhat USA, NullCon, g0s, c0c0n, RootConf
- Speaker : Nullcon, c0c0n, ClubHack, RootConf

WHAT IS VCS

- Version Control System
- The hip / developers way of deploying code
- Supports **Auto-Deployment on commit**

WHY EXPLOIT

- Coz its fun
- Its like a golden ticket
- Auto-deployment if available makes it more hip.

VCS 101

Type	FOLDER
GIT	.git
SVN	.svn
Mercurial	.hg

PREDICATABLE FILES

- .git/HEAD
- .hg/requires
- .bzr/README

ROBOTS.TXT OF VCS

.gitignore

TOOLS

1. SVN-extractor (Only SVN) (on top coz i wrote it)
2. DVCS-pillage (lacks SVN support)
3. dvcs-ripper (alternative implementation covers svn too)

DEMO TIME

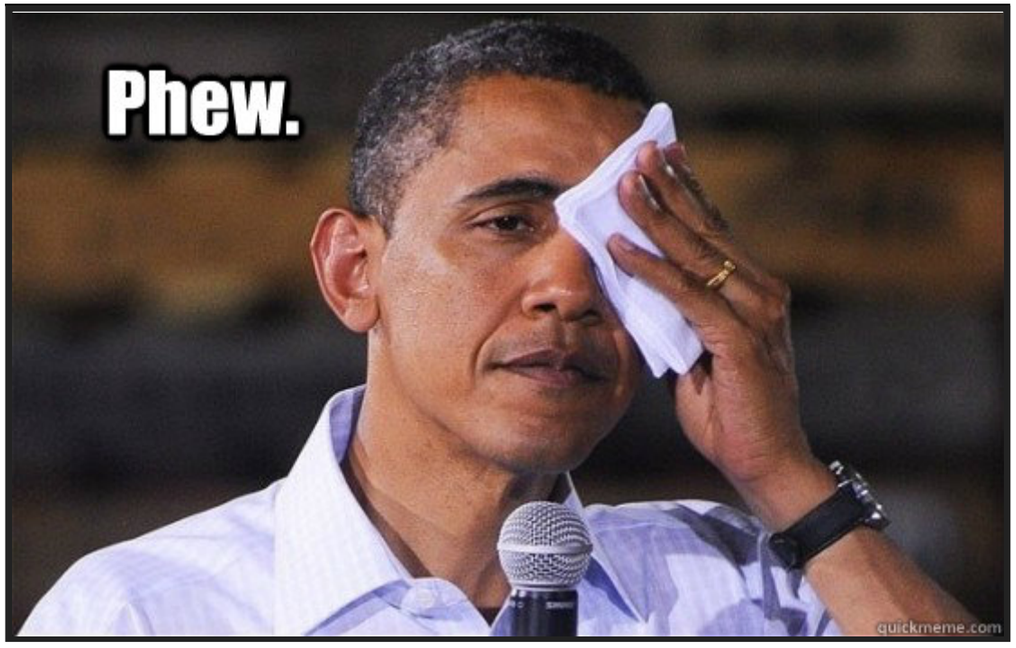
NOTE: ALL DEMO's are prepared while in sleep deprived state.

DIRECTORY LISTING ENABLED

DIRECTORY LISTING DISABLED

SVN

PHEW DEMO DONE



QUICK CHECKS

```
while read p;
do
  echo "Input: "$p
  echo "CHECK: SVN entries http"
  curl -I http://$p/.svn/entries
  echo "CHECK: SVN entries https"
  curl -k -I https://$p/.svn/entries
  echo "CHECK: SVN wcdb"
  curl -I http://$p/.svn/wc.db
  echo "CHECK: SVN wcdb https"
  curl -k -I https://$p/.svn/wc.db
done<$1
```

ANY QUESTIONS

ANANT SHRIVASTAVA

- Information Security Consultant
- Admin - Dev - Security
- null + OWASP + G4H
- http://anantshri.info and @anantshri
- Trainer : Blackhat USA, NullCon, g0s, c0c0n, RootConf
- Speaker : Nullcon, c0c0n, ClubHack, RootConf