

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Secure Coding Practices

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Hello, I'm a disclaimer slide. I'm here to tell you that trademarks, copyrights and other legal things are the property of their respective owners.

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Hello, I'm another disclaimer slide. This one tells you that this is not an exhaustive discourse on security practices. It's difficult to do that in one hour.

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

¿Quién es Kenneth?

QA

Development Project Manager

Forum: [cpanelkenneth](#)

IRC: [escherlat](#)

# Secure Coding Practices

OCTOBER 4TH-6TH, 2010

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

**Security is not a feature**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Least Privilege

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Separation of Privilege

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Simplicity**

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

"Debugging is twice as hard as writing the code in the first place. Therefore, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it." – Brian W. Kernighan

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Test your Assumptions**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Least Privilege
- Separation of Privilege
- Simplicity
- Test your Assumptions

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# PRIVILEGES

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Defined by:

- Who You Are (UID)
- Who You Are Associated With (GIDs)

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Determines access permissions and  
privileges

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Processes add to the fun

- Effective ID
- Real ID
- Saved ID

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Reference: man 7 credentials

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Effective ID

Used by the kernel to determine the permissions that the process will have

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Real ID

ID of the User or Process that created  
this process

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Saved ID

Used in set-user-ID and set-group-ID programs to save a copy of the corresponding effective IDs that were set when the program was executed

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## **Supplemental Groups**

Used for permission checks

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Often Abbreviated:

EUID, RUID, SUID, EGID, RGID, SGID

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# EXAMPLES

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Non-privileged (/bin/lS)

EUID = kpower

RUID = kpower

SUID = kpower

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Privileged executable (/usr/bin/passwd):

EUID = root

RUID = kpower

SUID = root

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Dropping Privileges

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

perl

RUID = \$<      RGID = \$(

EUID = \$>      EGID = \$)

SUID = ??      SGID = ??

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting Values

RUID (\$<): 0

EUID (\$>): 0

Set RUID to 501

RUID (\$<): 501

EUID (\$>): 0

Set EUID to 501

RUID (\$<): 501

EUID (\$>): 501

Set RUID to 0

RUID (\$<): 501

EUID (\$>): 501

Set EUID to 0

RUID (\$<): 501

EUID (\$>): 0

Set RUID to 0

RUID (\$<): 0

EUID (\$>): 0

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting Values

RUID (\$<): 0

EUID (\$>): 0

Set EUID = RUID = 501

RUID (\$<): 501

EUID (\$>): 501

Set RUID to 0

RUID (\$<): 501

EUID (\$>): 501

Set EUID to 0

RUID (\$<): 501

EUID (\$>): 0

Set RUID to 0

RUID (\$<): 0

EUID (\$>): 0

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting Values

RUID (\$<): 0

EUID (\$>): 0

Set RUID = EUID = 501

RUID (\$<): 501

EUID (\$>): 501

Set RUID to 0

RUID (\$<): 501

EUID (\$>): 501

Set EUID to 0

RUID (\$<): 501

EUID (\$>): 501

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- perl 5.8, 5.12
- Linux
- FreeBSD tells a different story

## Test Your Assumptions

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Proc::UID

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting Values

SUID :0

RUID (\$<): 0

EUID (\$>): 0

Set RUID to 501

SUID :0

RUID (\$<): 501

EUID (\$>): 0

Set EUID to 501

SUID :0

RUID (\$<): 501

EUID (\$>): 501

Set EUID to 0

SUID :0

RUID (\$<): 501

EUID (\$>): 0

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting Values

SUID :0

RUID (\$<): 0

EUID (\$>): 0

Set RUID = EUID = 501

SUID :501

RUID (\$<): 501

EUID (\$>): 501

Set RUID to 0

SUID :501

RUID (\$<): 501

EUID (\$>): 501

Set EUID to 0

SUID :501

RUID (\$<): 501

EUID (\$>): 501

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Cpanel::AccessIds::runasuser

Cpanel::AccessIds::SetUids::setuids

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

PHP

EUID = posix\_seteuid, posix\_geteuid

RUID = posix\_setuid, posix\_getuid

SUID = ??

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Don't confuse with  
getmyuid, getmygid

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting values

EUID: 0

RUID: 0

Set EUID to 505

EUID: 505

RUID: 0

Set UID to 505

EUID: 505

RUID: 0

Set EUID to 0

EUID: 0

RUID: 0

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Starting values

EUID: 0

RUID: 0

Set UID to 505

EUID: 505

RUID: 505

Set UID to 0

EUID: 505

RUID: 505

Set EUID to 0

EUID: 505

RUID: 505

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- PHP 5.2.9, 5.3.3
- Linux (CentOS 5)

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- perl

Proc::UID

Cpanel::AccessIds::runasuser

Cpanel::AccessIds::SetUids::setuids

- PHP

posix\_

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Fork**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Beware that which follows

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Not Environmentally Friendly

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Perl
  - PERL5LIB
  - PERLIB
    - Allows loading User modules first

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Perl
- PERL5OPT
- Allows providing command line parameters to perl interpreter

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- PHP
- PHPRC
  - Specifies directory to search for php.ini
- PHP\_INI\_SCAN\_DIR
  - Other directories to search for php.ini

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Scrub Environment

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- perl
  - %ENV
  - Cpanel::Env::cleanenv

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- PHP
- `getenv`, `setenv`

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# ESCALATION

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- setuid?

```
chmod +s script_name
```

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Why is this a bad idea?

```
chmod +s `which perl`
```

```
chmod +s `which php`
```

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

setuid binary

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- `/usr/local/cpanel/src/wrap/wrap.c`

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Privileges
  - Drop ASAP
  - Clean your Environment
  - Control Escalation

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Handling Files

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

```
# perl
if( ! -e 'file_name' ){
    open( my $fh, '>', 'file_name' )...
}

# PHP
if( file_exists( 'file_name' ) === FALSE ){
    $fh = fopen( 'file_name', 'w+' )...
}
```

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

```
# perl
if( ! -e 'file_name' && open( my $fh, '>', 'file_name' ) ){...
}

# PHP
if( file_exists( 'file_name' ) === FALSE && $fh = fopen( 'file_name',
'w+' ) ){...
}
```

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

```
# perl
sysopen( my $fh, 'file_name', &Fcntl::O_WRONLY | &Fcntl::O_CREAT |
&Fcntl::O_NOFOLLOW | &Fcntl::O_EXCL | &Fcntl::O_TRUNC, 0600 );

# similar for read
sysopen( my $fh, 'file_name', $Fcntl::O_RDONLY | &Fcntl::O_NOFOLLOW );
```

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

```
# PHP  
my $fh = fopen( 'file_name', 'x' );  
# mode x: O_EXCL|O_CREAT
```

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

What about chmod?

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Direct IO PECL Extension

```
dio_open( file_name, O_CREAT | O_EXCL | O_WRONLY, 0600 );
```

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- All file and directory manipulations are subject to time slicing

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Possible Attacks
  - write: clobber file
  - read: information disclosure
  - chmod, chown: give access

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Atomicity
- Least Privilege

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Beware that which the user controls

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Is root ownership a safeguard?

```
# ls -la
total 12
drwxr-xr-x  3 user  users 4096 Nov 10 21:58 .
drwxr-xr-x 40 user  users 4096 Nov 10 21:57 ..
drwx----- 2 root  root  4096 Nov 10 21:57 control
-rw----- 1 root  root    0 Nov 10 21:58 settings
```

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Files may be:
  - Renamed
  - Deleted

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- Directories may be:
  - Renamed
  - Deleted, if empty

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## Separation of Privilege

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Don't blindly change ownership or  
permissions

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- As root:
- `chown -R user:user /home/user`

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Scenario

-----

```
[root@squash ~]# ls -l /etc/shadow
-rw----- 1 root root 0 Jun 3 07:30 /etc/shadow
```

```
[whoanel@squash ~]$ ln /etc/shadow public_html/favorite_book_list.txt
[whoanel@squash ~]$ ls -l public_html/favorite_book_list.txt
-rw----- 2 root root 905995 May 14 09:49 public_html/
favorite_book_list.txt
```

```
[root@squash ~]# chown -R whoanel:whoanel /home/whoanel
[root@squash ~]# ls -l /etc/shadow
-rw-r--r-- 2 whoanel whoanel 0 Jun 3 07:35 /etc/shadow
```

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# REFERENCES

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

<http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html>

<http://www.kernel.org/doc/man-pages/online/pages/man7/credentials.7.html>