

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](#)

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Security is not a feature

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

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

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

Processes add to the fun

- Effective ID
- Real ID
- Saved ID

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

[http://www.kernel.org/doc/man-pages/
online/pages/man7/credentials.7.html](http://www.kernel.org/doc/man-pages/online/pages/man7/credentials.7.html)

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

PHP

EUID = posix_seteuid, posix_geteuid

RUID = posix_setuid, posix_getuid

SUID = ??

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

EXAMPLES

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Perl

```
$< = 501;
```

```
$> = 501;
```

PHP

```
posix_seteuid( 501 );
```

```
posix_setuid( 501 );
```

Did we drop privileges?

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

PERL

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

PHP

Starting values

EUID: 0

RUID: 0

Set EUID to 501

EUID: 501

RUID: 0

Set UID to 501

EUID: 501

RUID: 0

Set EUID to 0

EUID: 0

RUID: 0

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Temporary vs. Permanent

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

PERL

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

PHP

Starting values

EUID: 0

RUID: 0

Set UID to 501

EUID: 501

RUID: 501

Set UID to 0

EUID: 501

RUID: 501

Set EUID to 0

EUID: 501

RUID: 501

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- perl 5.8, 5.12
- Linux (CentOS 5)
- FreeBSD tells a different story

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- PHP 5.2.9, 5.3.3
- Linux (CentOS 5)
- FreeBSD the same

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Proc::UID

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Interface that is easy to understand

- `drop_uid_perm`, `drop_gid_perm`
- `drop_uid_temp`, `drop_gid_temp`
- `restore_uid`, `restore_gid`

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

Drops privileges temporarily

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

ESCALATION

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Separation of Privilege

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

setuid?

```
chmod +s script_name
```

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

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

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

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

`chmod +s `which perl``

`chmod +s `which php``

Why is this a bad idea?

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

- Simple, clear channel
- Whitelist
- Audit log
- Access Controls

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

Privileges

- Clear interface when dropping
- Know implementation differences
- Simple channel for 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

Subject to Race Condition

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

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

Put important information where the user
does not control it

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

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

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

¿Questions?