

Owning Stuff With Format Strings

deanx

utline

vhat are they

yang what are they syntax

Owning Stuff With Format Strings

deanx

Intercon II

13th June 2008



Owning Stuff With Format Strings

deanx

outline

what are the

yang
what are they

- 1 yin
 - what are they
 - syntax
- 2 yang
 - what are they
 - syntax



Owning Stuff With Format Strings

deanx

outlin

outiin

what are they

syntax

yang what are they Format strings are a way of secifying the format when data is outputted

deanx



Owning Stuff With Format Strings

deanx

outlin

outilli

yın . . .

what are they syntax

yang

what are they syntax Format strings are a way of secifying the format when data is outputted

dave is 20



Owning Stuff With Format Strings

deanx

utline

outiiii

yın

what are they

syntax

what are they syntax Format strings are a way of secifying the format when data is outputted

- dave is 20
- %s is %d

deanx



Owning Stuff With Format Strings

deanx

utlin

.

what are they

syntax

yang what are they syntax Format strings are a way of secifying the format when data is outputted

- dave is 20
- %s is %d
- printf(" %s is %d", name, age)



Owning Stuff With Format Strings

deanx

......

outiin

what are t

syntax

what are the

These are used to format the output of variables



Owning Stuff With Format Strings

deanx

. . . .

outline

what are the syntax

syntax

what are the

These are used to format the output of variables

■ %d - int



Owning Stuff With Format Strings

deanx

utlin

outlin

what are th

syntax

yang what are they syntax These are used to format the output of variables

- %d int
- %f float



Owning Stuff With Format Strings

deanx

syntax

These are used to format the output of variables

- %d int
- %f float
- %u unsigned int

deanx



Owning Stuff With Format Strings

deanx

outlin

.

what are the

yang

what are they syntax These are used to format the output of variables

- %d int
- %f float
- %u unsigned int
- %x hex representation of an int



Owning Stuff With Format Strings

deanx

syntax

These are used to format the output of variables

- %d int
- %f float
- %u unsigned int
- %x hex representation of an int
- %s string (prints till \x00)



Owning Stuff With Format Strings

deanx

.....

outlin

vin

what are th

what are the



Owning Stuff With Format Strings

deanx

utlin

outlin

yin

what are the syntax

what are they

Used to more specifically control how variables are represented

■ %.5f - 3.14159



Owning Stuff With Format Strings

deanx

outlin

vin

what are the syntax

yang what are they

- %.5f 3.14159
- %#x 0xdeadbeaf



Owning Stuff With Format Strings

deanx

outlin

what are the

syntax yang

what are they syntax

- %.5f 3.14159
- %#x 0xdeadbeaf
- %4u xxxx4



Owning Stuff With Format Strings

deanx

outline

.

what are th

yang what are they

- %.5f 3.14159
- %#x 0xdeadbeaf
- %4u xxxx4
- %hx beaf



Owning Stuff With Format Strings

deanx

syntax

Used to more specifically control how variables are represented

- %.5f 3.14159
- %#x 0xdeadbeaf
- %4u xxxx4
- %hx beaf
- %hhx af

deanx



Owning Stuff With Format Strings

deanx

utlin

outilli

yIII ...bat asa t

syntax

what are the

dave is 20, dave is male



Owning Stuff With Format Strings

deanx

syntax

- dave is 20, dave is male
- %s is %d, %s is %s

deanx



Owning Stuff With Format Strings

deanx

outline

what are the syntax

yang what are they

- dave is 20, dave is male
- %s is %d, %s is %s
- printf(" %s is %d, %s is %s",name, age, name, sex)



Owning Stuff With Format Strings

deanx

outlin

what are the syntax

yang what are they dave is 20, dave is male

■ %s is %d, %s is %s

printf(" %s is %d, %s is %s",name, age, name, sex)

■ %1\$s



Owning Stuff With Format Strings

deanx

outline

vin

what are the syntax

yang

what are they syntax

- dave is 20, dave is male
- %s is %d, %s is %s
- printf(" %s is %d, %s is %s",name, age, name, sex)
- %1\$s
- printf(" %s is %d, %1\$s is %s",name, age, sex)



Owning Stuff With Format Strings

deanx

outline

outiin

vhat are the

yang what are they



Owning Stuff With Format Strings

deanx

outlin

vin

what are the

what are they

They can be misused if programmers forget about them

dave



Owning Stuff With Format Strings

deanx

outlin

yin

/nat are tney yntax

what are they svntax

- dave
- printf(name)



Owning Stuff With Format Strings

deanx

outlin

yin

syntax

what are they

- dave
- printf(name)
- **■** %s



Owning Stuff With Format Strings

deanx

outlin

yin

vhat are they vntax

yang what are they

- dave
- printf(name)
- %s
- demo



Owning Stuff With Format Strings

deanx

outline

vin

what are the syntax

yang what are the syntax



Owning Stuff With Format Strings

deanx

. . .

utline

what are the

yang what are the syntax ■ %×



Owning Stuff With Format Strings

deanx

outline

044....0

what are the

yang what are they syntax

- %×



Owning Stuff With Format Strings

deanx

outlin

yin

iat are they ntax

what are the

- %x
- - aloadofcrap



Owning Stuff With Format Strings

deanx

outlin

yin

what are the

yang what are they syntax ■ %×

 $\bullet \circ_0 \times \circ$

aloadofcrap

■ aaaa-%x%x%x%x%x%x%x%x%x%x%x%x



Owning Stuff With Format Strings

deanx

outlin

yin

at are they tax

yang what are they syntax ■ %x

aloadofcrap

■ aaaa-%x%x%x%x%x%x%x%x%x%x%x%x

aaaa-aloadofcrap61616161morecrap



Owning Stuff With Format Strings

deanx

outlin

yin

vhat are they yntax

yang what are they syntax

- %×
- - aloadofcrap
- aaaa-%x%x%x%x%x%x%x%x%x%x%x%x
 - aaaa-aloadofcrap61616161morecrap
- aaaa-%8\$#x



Owning Stuff With Format Strings

deanx

outlin

yin

≀hat are they yntax

yang what are they syntax

- %×
- - aloadofcrap
- aaaa-%x%x%x%x%x%x%x%x%x%x
 - aaaa-aloadofcrap61616161morecrap
- aaaa-%8\$#x
 - aaaa-0x61616161



reading memory

Owning Stuff With Format Strings

deanx

outlin

yin

vhat are they yntax

/ang

what are they syntax

- %×
- - aloadofcrap
- aaaa-%x%x%x%x%x%x%x%x%x%x%x
 - aaaa-aloadofcrap61616161morecrap
- aaaa-%8\$#x
 - aaaa-0×61616161
- demo



Owning Stuff With Format Strings

deanx

deanx



Owning Stuff With Format Strings

deanx

outlin

what are tl

yang what are the syntax ■ Introducing %n



Owning Stuff With Format Strings

deanx

outlin

.

what are th

syntax

yang what are they syntax

■ Introducing %n

%n will write the number of bytes written to the pointer location specified



Owning Stuff With Format Strings

deanx

syntax

- Introducing %n
 - %n will write the number of bytes written to the pointer location specified
- dave has 4 characters in his name

deanx



Owning Stuff With Format Strings

deanx

outlin

vin

what are the

syntax vang

yang what are they syntax

- Introducing %n
 - %n will write the number of bytes written to the pointer location specified
- dave has 4 characters in his name
- printf("%s%n has %d characters in his name", name, &chars, chars)



Owning Stuff With Format Strings

deanx

outlin

yin

what are they syntax

yang what are they syntay

- Introducing %n
 - %n will write the number of bytes written to the pointer location specified
- dave has 4 characters in his name
- printf("%s%n has %d characters in his name", name, &chars, chars)
- printf("%s%x has %d characters in his name", name, &chars, chars)



Owning Stuff With Format Strings

deanx

outlin

yin

vhat are they syntax

yang what are they

- Introducing %n
 - %n will write the number of bytes written to the pointer location specified
- dave has 4 characters in his name
- printf("%s%n has %d characters in his name", name, &chars, chars)
- printf("%s%x has %d characters in his name", name, &chars, chars)
- demo



Owning Stuff With Format Strings

deanx

. . . .

outiin

what are

yang

what are the syntax



Owning Stuff With Format Strings

deanx

utline

Dutime

hat are the

yang

yang what are the syntax We want to overwrite 0xdeadbeef with 0x90909090

We push 0xdeadbeef onto the stack as the first part of our FS



Owning Stuff With Format Strings

deanx

outline

hat are the vntax

yang what are the syntax

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde



Owning Stuff With Format Strings

deanx

outline

what are the

yang what are they

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen



Owning Stuff With Format Strings

deanx

utline

hat are the yntax

yang what are they syntax

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or



Owning Stuff With Format Strings

deanx

outline

what are the

yang what are they

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or
- we use %hn or %hhn so we can write it in 2 or 1 byte sections



Owning Stuff With Format Strings

deanx

outline

vhat are they vntax

yang what are they syntay

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or
- we use %hn or %hhn so we can write it in 2 or 1 byte sections
- Lets choose %hn, so 2 byte chunks.



Owning Stuff With Format Strings

deanx

outlin

vhat are they syntax

yang what are they syntay

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or
- we use %hn or %hhn so we can write it in 2 or 1 byte sections
- Lets choose %hn, so 2 byte chunks.
- So now we write



Owning Stuff With Format Strings

deanx

outline

outilli

what are the

yang what are they syntax

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or
- we use %hn or %hhn so we can write it in 2 or 1 byte sections
- Lets choose %hn, so 2 byte chunks.
- So now we write
 - 9090h (370008) to 0xdeadbeef



Owning Stuff With Format Strings

deanx

outlin

vhat are they

yang what are they We want to overwrite 0xdeadbeef with 0x90909090

- We push 0xdeadbeef onto the stack as the first part of our FS
 - \xef\xbe\xad\xde
- We have now written 4 chars to the screen
- So we know need to write another (90909090h-4) or
- we use %hn or %hhn so we can write it in 2 or 1 byte sections
- Lets choose %hn, so 2 byte chunks.
- So now we write
 - 9090h (370008) to 0xdeadbeef
 - 9090h (370008) to 0xdeadbef1

deanx



Owning Stuff With Format Strings

deanx

outlin

yin

hat are the ntax

yang what are the syntax We have a stack-pop length of 8 using 2x2 byte writes

■ Push the addresses to the stack



Owning Stuff With Format Strings

deanx

...tlin

vin

what are the

yang what are they syntax

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde



Owning Stuff With Format Strings

deanx

autlin

outlin

what are the

yang what are they syntax

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde
- So now we have written 8 bytes so only another 37000 to go



Owning Stuff With Format Strings

deanx

autlin

hat are they

yang what are they

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde
- So now we have written 8 bytes so only another 37000 to go
 - %37000u simple



Owning Stuff With Format Strings

deanx

...tlin

what are they

yang

yang what are they syntax

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde
- So now we have written 8 bytes so only another 37000 to go
 - %37000u simple
- \xef\xbe\xad\xde\xf1\xbe\xad\xde%37000u



Owning Stuff With Format Strings

deanx

autlin

041111

what are the

syntax

yang what are they syntax

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde
- So now we have written 8 bytes so only another 37000 to go
 - %37000u simple
- \xef\xbe\xad\xde\xf1\xbe\xad\xde%37000u
- now we use %8\$hn and %9\$hn to write the data



Owning Stuff With Format Strings

deanx

autlin

outill

what are they

yang what are they

- Push the addresses to the stack
 - \xef\xbe\xad\xde\xf1\xbe\xad\xde
- So now we have written 8 bytes so only another 37000 to go
 - %37000u simple
- \xef\xbe\xad\xde\xf1\xbe\xad\xde%37000u
- now we use %8\$hn and %9\$hn to write the data



Owning Stuff With Format Strings

deanx

outlin

outim

what are th

syntax

yang what are the syntax ■ very simple example



Owning Stuff With Format Strings

deanx

syntax

- very simple example
 - no nx
 - no ramdomised stack

deanx



Owning Stuff With Format Strings

deanx

outlin

0.....

what are the

yang what are they syntax

- very simple example
 - no nx
 - no ramdomised stack
- execute shell code from our buffer



Owning Stuff With Format Strings

deanx

outlin

vin

what are the

yang what are they syntax

- very simple example
 - no nx
 - no ramdomised stack
- execute shell code from our buffer
- overwrite \$eip with location of shell code



Owning Stuff With Format Strings

deanx

outlin

yin . . .

syntax

yang what are they syntax

- very simple example
 - no nx
 - no ramdomised stack
- execute shell code from our buffer
- overwrite \$eip with location of shell code
- demo

deanx