

# My Handle

Or, how /<-r33t Handles  
are the shiznit!

**What the hell?**

# Who am I?

- ✘ I)ruid
- ✘ Founder, Computer Academic Underground
- ✘ Co-Founder, Austin Hackers Association (AHA!)
- ✘ Employed in Security Research for TippingPoint, a Division of 3Com



# Origin

- ⌘ ~1990 I needed a handle for an “underground” BBS
- ⌘ Was reading *The Sword of Shannara* by Terry Brooks
- ⌘ Favorite Character was Allanon, a Druid
- ⌘ “Druid” was too common
- ⌘ Modified the character representation by replacing “**D**” with “**I}**”



# What's so r33t about my handle?

 One simple character: ‘)’



# Case Studies

All of these are real and resulted  
from normal use of my handle

# Google

☒ Target: Google Book Search

☒ Input: Search Query

☒ Impact: Identified a deficiency

☒ Cause: Old, worn books caused the OCR to mis-recognize “D” as “I)”



# BlackHat USA 2006

- Target: BlackHat USA 2006 Registration Desk (web?) form
- Input: Registrant Name (or handle)
- Impact: Registration form submission fails with error.
- Cause: Malformed SQL syntax (potential SQL injection!)





# ShmooCon 2006 Hacker Arcade

- ☒ Target: Hacker Arcade game “Slash’Em”
- ☒ Input: Character Name
- ☒ Impact: Game application exits, drops to system shell
- ☒ Cause: User input wasn’t sanitized before being used



# Webs 1.x, 2.x

- ☒ Target: Countless web applications
- ☒ Input: Usually a web form
- ☒ Impact: Usually an SQL error, sometimes an internal server error
- ☒ Cause: WebApp developers not restricting or sanitizing input



# Using Your Handle to Perform Inherent Fault Injection

Why not fuzz *all* the time?

# Properties of a /<-r33t Handle

☒ Funny characters!

☒ Unmatched grouping:

☒ Parenthesis: ( or )

☒ Brackets: [ or ]

☒ Angle Brackets: < or >

☒ Braces: { or }

☒ Quotations: " or '

☒ Delimiter characters:

☒ Colon: :

☒ Semi-colon: ;

☒ Commas: ,

☒ Underscore: \_

☒ Shell Metacharacters:

☒ Exclamation Point: !

☒ Slashes: \ or /

☒ Dollar Sign: \$

☒ Ampersand: &

☒ Math Characters:

☒ Multiplication: \*

☒ Addition: +

☒ Subtraction: -















☒ Power: ^

☒ Modulus: %











# High Impact Letters

## Uppercase:

-  A: /.\, /- \
-  D: |), |), |), |), |}, etc.
-  H: |-, \-, /-
-  I: |
-  J: . \_ /
-  K: /< or |< or \<
-  M: / \ or | \
-  L: | \_ or \ \_
-  X: ><
-  V: V
-  N: | | or / \
-  O: ()
-  U: | |
-  W: V V or | \ |

## Lowercase:

-  h: |-,
-  i: |, !
-  k: /< or |< or \<
-  l: |
-  o: ()
-  v: V
-  w: V V or | \ |
-  x: ><



# Examples:

☒ intropy: !ntr()p!zz|e

☒ HD Moore: ]-[ ]) |V|oore

☒ gammah: G/-\|V||V|/-\|-|

☒ nummish: ^Nu^^^Is\-\

☒ Johnny: .\_/( )|-,^/My

☒ Lupin III: |\_up!n ]|[



# What to do?

- ☒ Change your fucking handles!
- ☒ Nah, not really, I just thought this was funny...



**I'm out, bitchezz!**