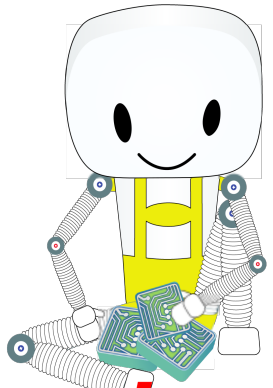
From Gaming to Hacking the Planet

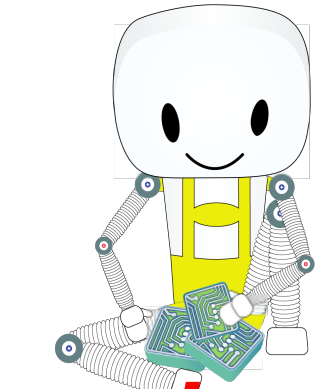
Chris “Lopi” Spehn



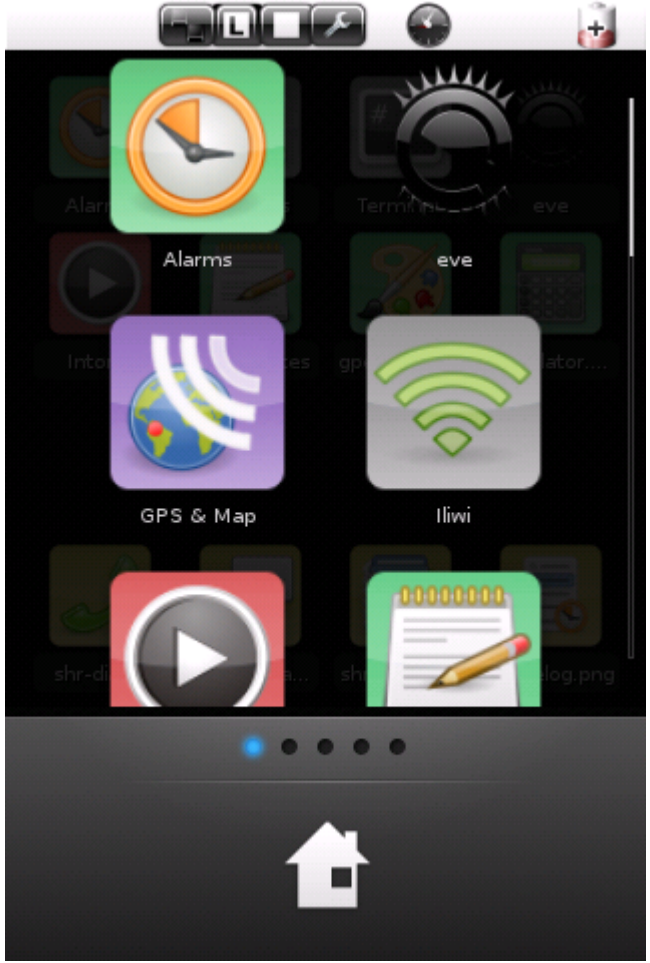
HAK4KiDZ

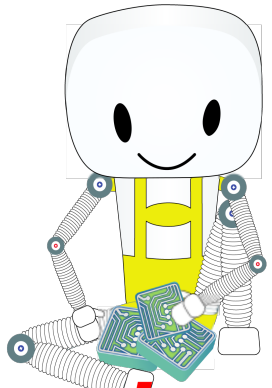
Who Am I?

- Gamer
  - Diablo II
  - DotA Allstars
    - Evil Geniuses
- Hacker
  - Red Team Love
  - CTF Advocate
  - iDroid Project / iX Project
    - OpenEmbedded / OpenMoko




Alarms
Settings
Terminal
eve
Intone
opimd-notes
gpe-sketch...
calculator....
shr-dialer
shr-messa...
shr-contacts
phonelog.png

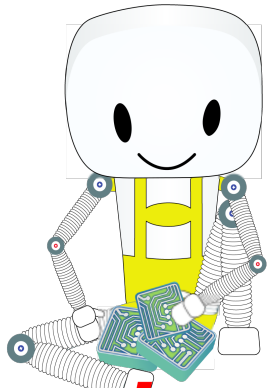

Alarms
eve
GPS & Map
Iliwi



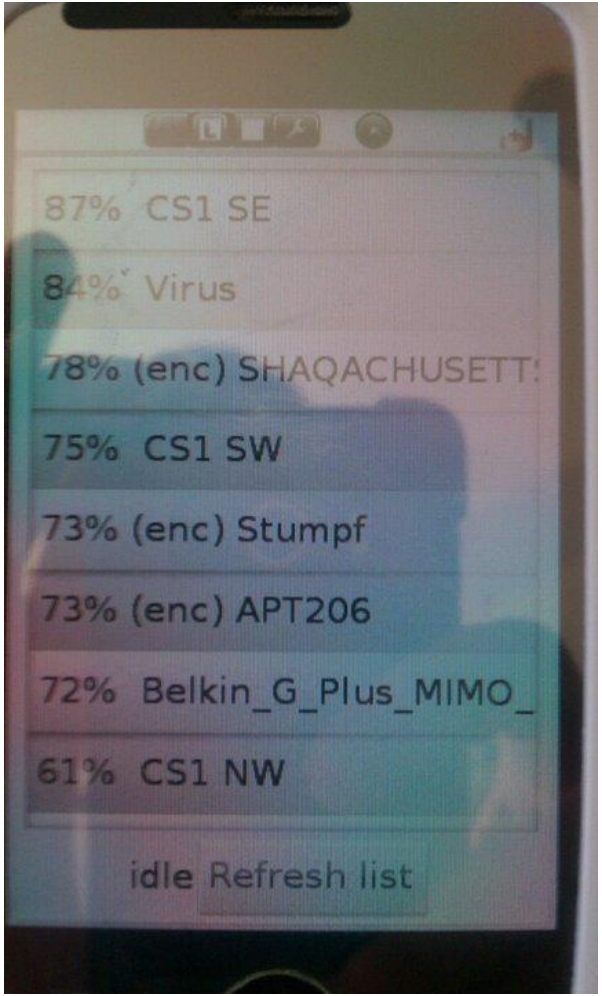
HAK4KiDZ

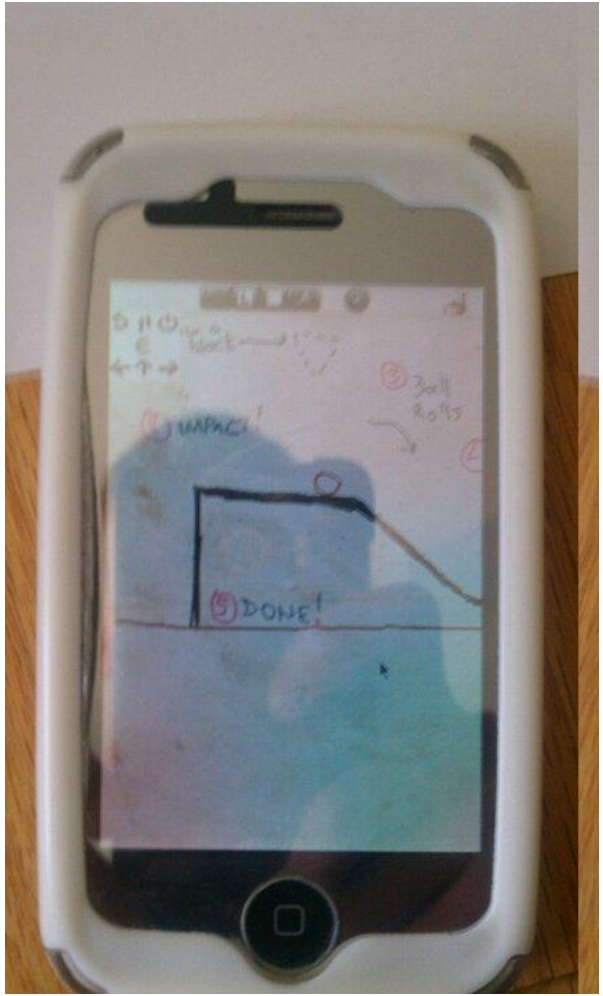

19:21
29.4.2011
default
SHR

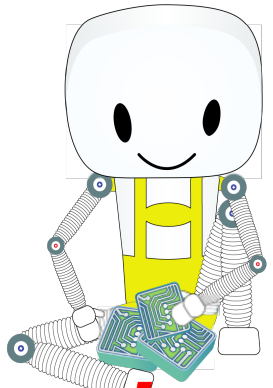

911
1
2
ABC
3
DEF
4
GHI
5
JKL
6
MNO
7
PQRS
8
TUV
9
WXYZ
*
0
#
Call
More
Close



HAK4KiDZ


87% CS1 SE
84% Virus
78% (enc) SHAQACHUSETT!
75% CS1 SW
73% (enc) Stumpf
73% (enc) APT206
72% Belkin_G_Plus_MIMO_
61% CS1 NW
idle Refresh list

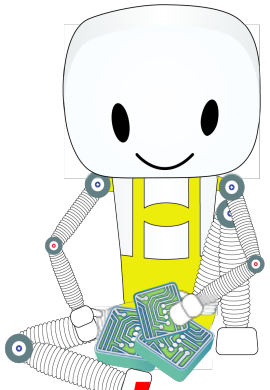

DONE!



HAK4KIDZ

Goal

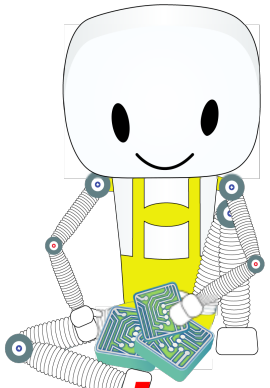
- Teach a methodology to hack the planet.
  - Hack to learn, not learn to hack.



HAK4KiDZ

Road to Pro Gaming

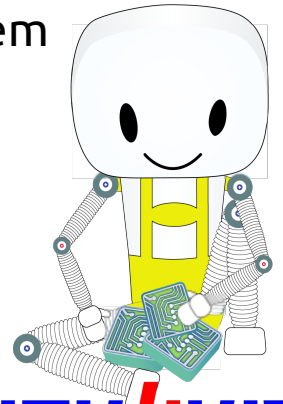
- Megaman
- Diablo II
  - palapk
  - amapk
- DotA
  - Dreamhack
  - ESWC Masters



HAK4KiDZ

Diablo II: Charsi Dupe

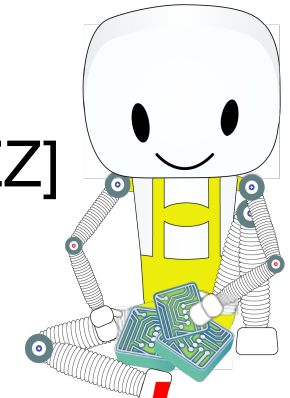
1. Player acquires the (reusable) sequence for the part of the imbue quest that drops the item.
2. Player finds the id of the item he wishes to dupe by simply dropping it on the ground and sniffing the event.
3. Player sends the known sequence to charsi substituting the id with the id of the item to dupe.
4. Player can send this over and over rapidly cloning the single item



HAK4KiDZ

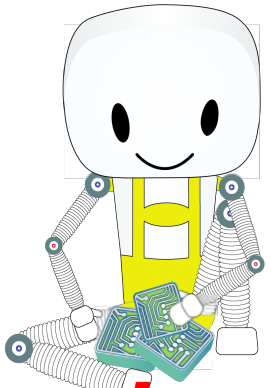
Diablo II: Charsi Dupe (cont.)

1. Find Charsi
   a. 13 01 00 00 00 [XX XX XX XX]
2. Pickup Item
   a. 19 [ZZ ZZ ZZ ZZ]
3. Tell Charsi to imbue the item
   a. 38[00 00 00 00][XX XX XX XX][ZZ ZZ ZZ ZZ]
4. Repeat
   a. Profit



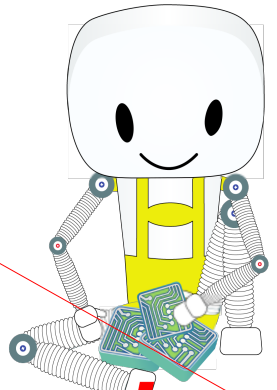
HAK4KiDZ

Diablo II: Charsi Dupe (cont.)



HAK4KIDZ

DotA



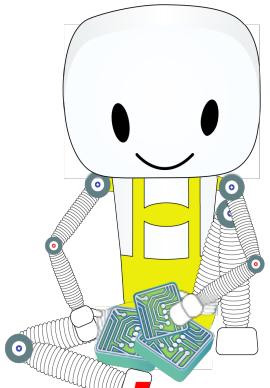
HAK4KiDZ


STRENGTH
AGILITY
INTELLIGENCE


Quests (F9)
Menu (F10)
Allies
Log (F12)
500
0
0
No Upkeep
Shade
Muerto viv.
Armor:
Invulnerable
250 / 250
Status:

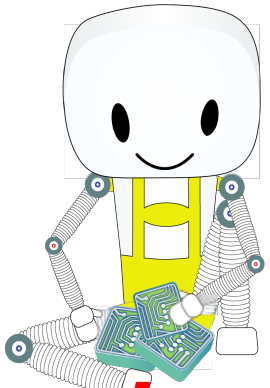

Quests (F9)
Menu (F10)
Allies
Log (F12)
500
0
0
No Upkeep
Shade
Muerto viv.
Armor:
Invulnerable
250 / 250
Status:

DotA: Creep Blocking



HAK4KIDZ

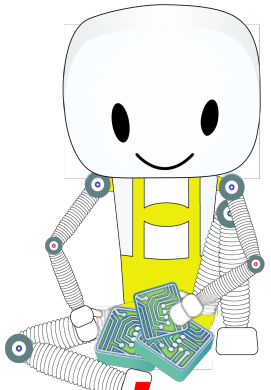
DotA: Creep Blocking Part Two



HAK4KiDZ

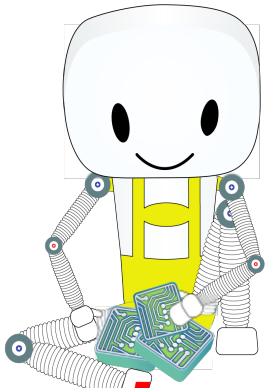
Methodology

What do we know?



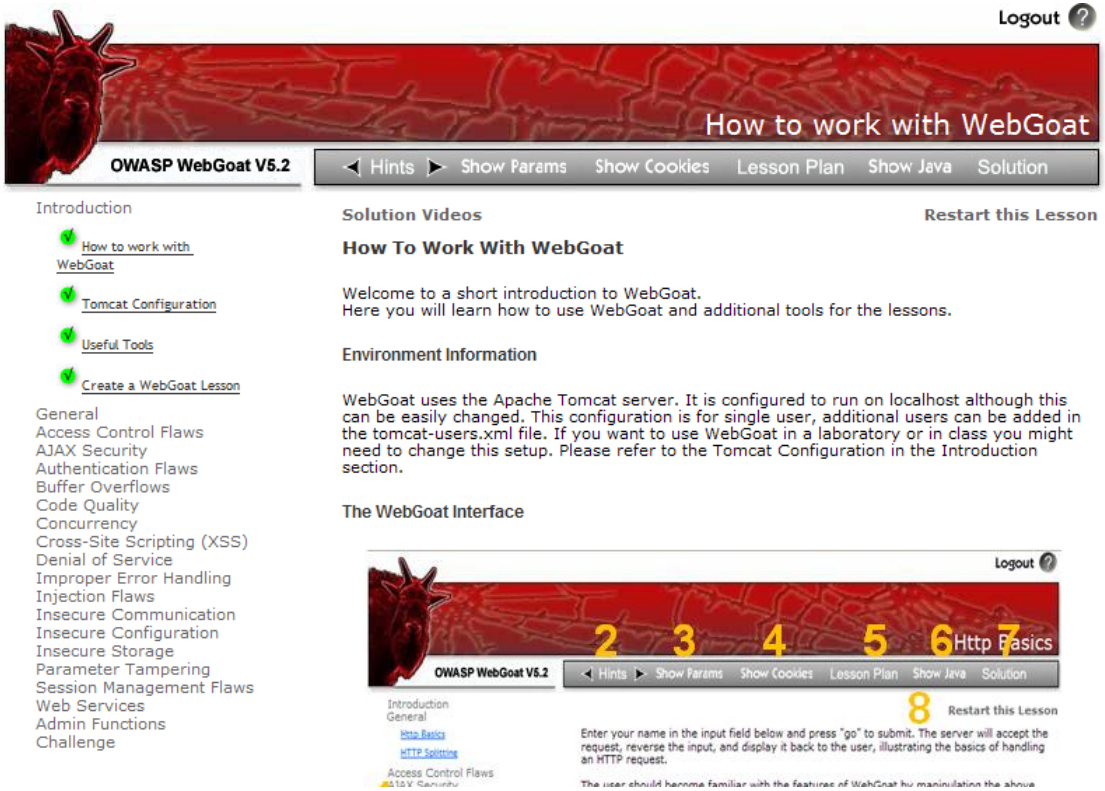
HAK4KiDZ

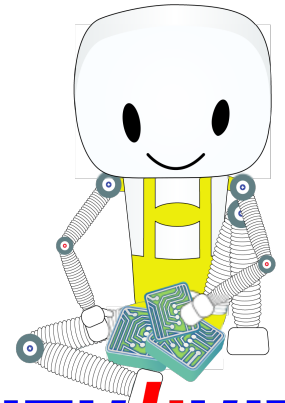
Megaman



HAK4KiDZ

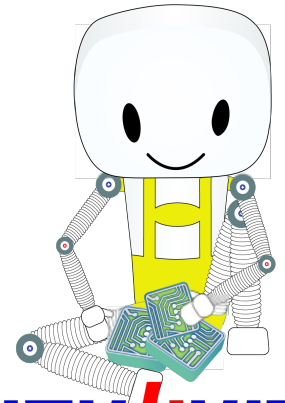
Web Application





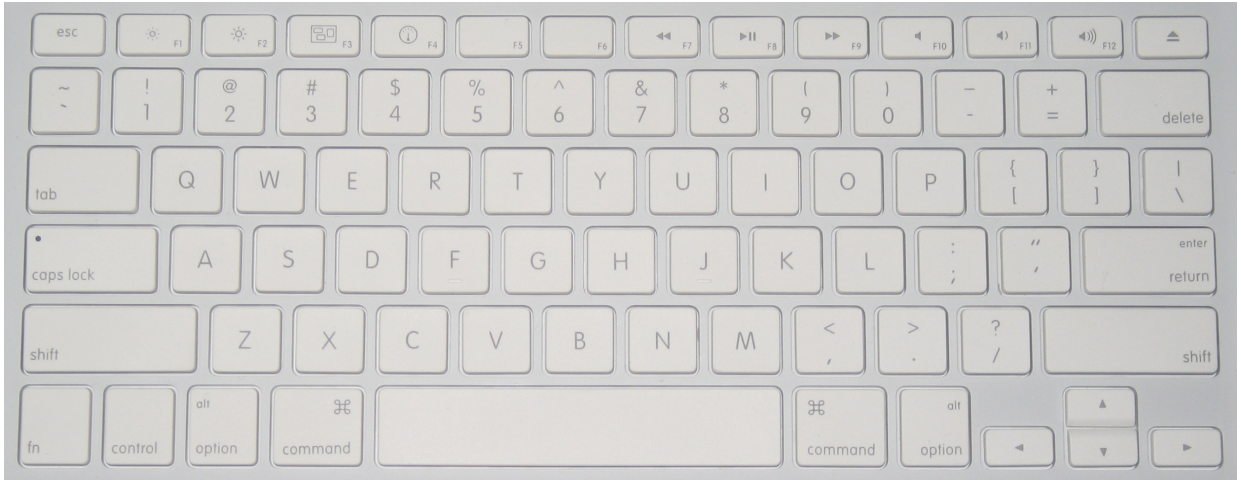
HAK4KIDZ

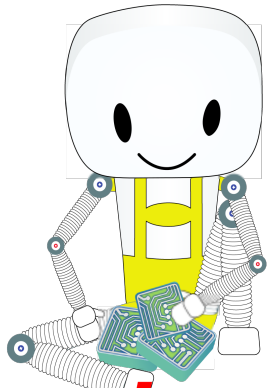
Megaman Input



HAK4KiDZ

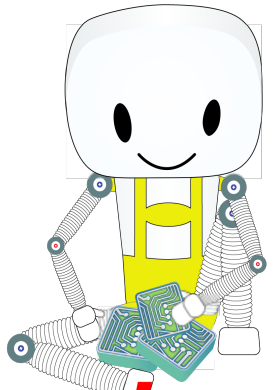
Web Application Input





HAK4KiDZ

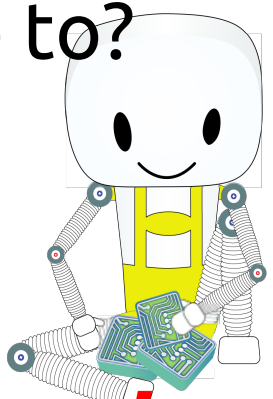
MegaMan Boss Fight



HAK4KiDZ

MegaMan Methodology

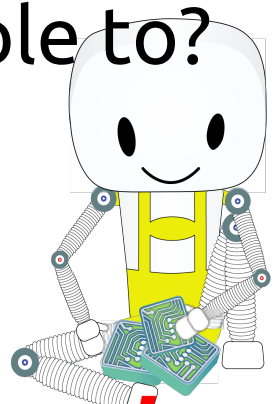
- What is our input?
- What can we do with the NES Controller?
- How does the boss work?
- Which weapon is the boss vulnerable to?



HAK4KiDZ

Web Application Methodology

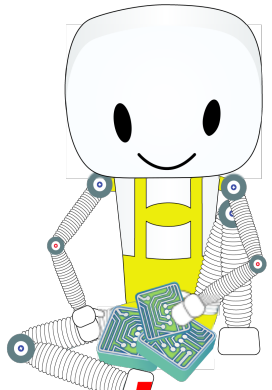
- What is our input?
- What can we do with the keyboard?
- How does the web application work?
- What is the web application vulnerable to?



HAK4KiDZ

Learning about Web Applications

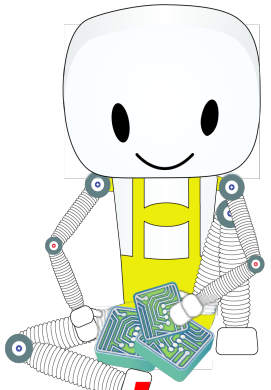
DEMO



HAK4KIDZ

Build your own Web Application

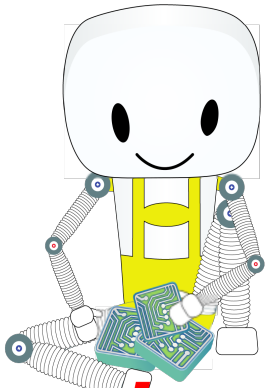
- http://learnpythonthehardway.org/
- http://learncodethehardway.org/



HAK4KiDZ

Go Hack Some Stuff

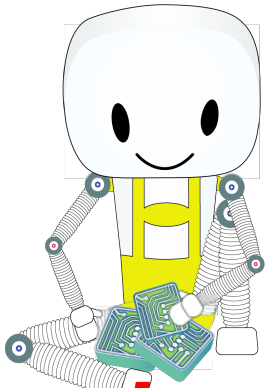
- OWASP Broken Web Application Project
- Mutillidae



HAK4KiDZ

What did we learn?

Ask yourself what you know, and take it one step at a time. Be curious. Think different.



HAK4KiDZ

Questions?

Thanks for coming!

www.lopisec.com

@_Lopi_ on Twitter