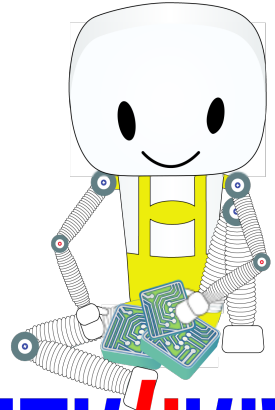


From Gaming to Hacking the Planet

Chris “Lopi” Spehn



HAK4KIDZ

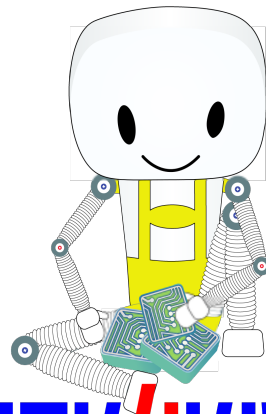
Who Am I?

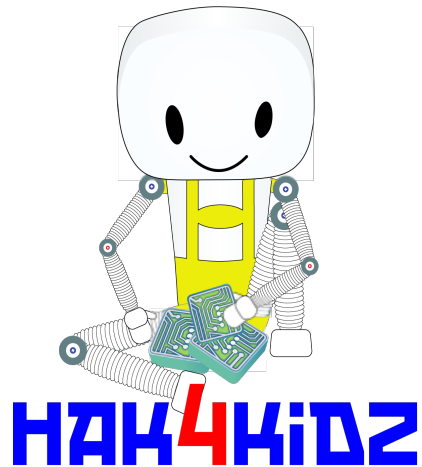
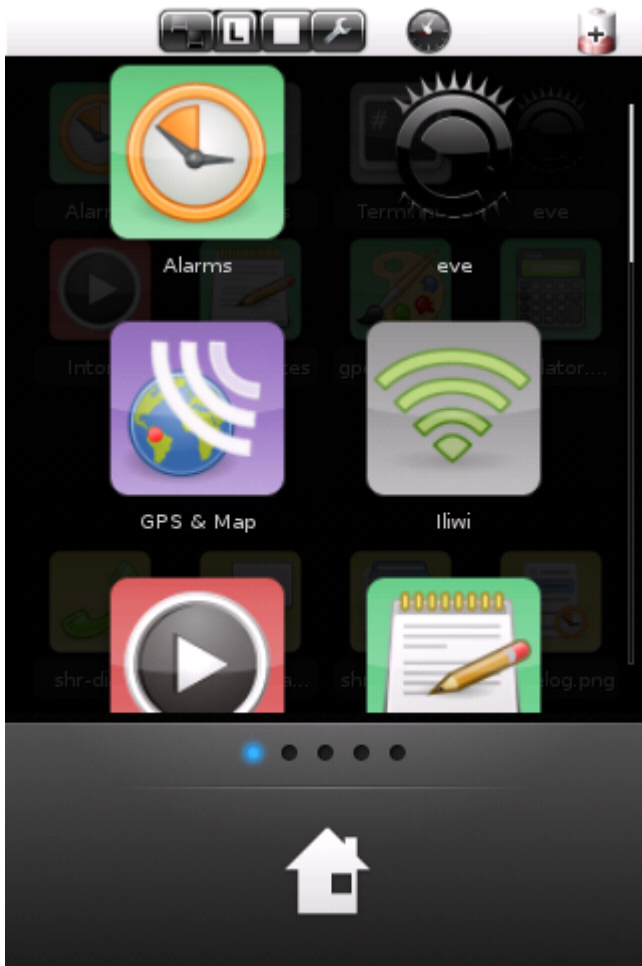
- Gamer

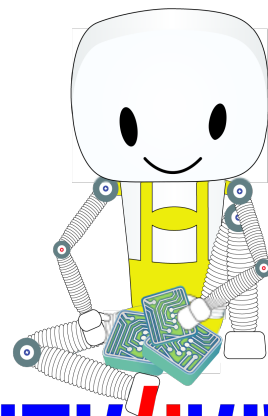
- Diablo II
- DotA Allstars
 - [Evil Geniuses](#)

- Hacker

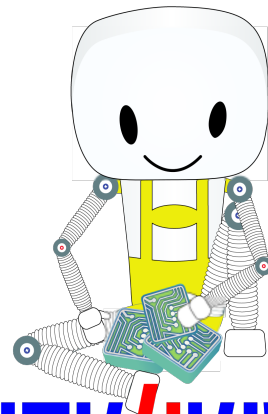
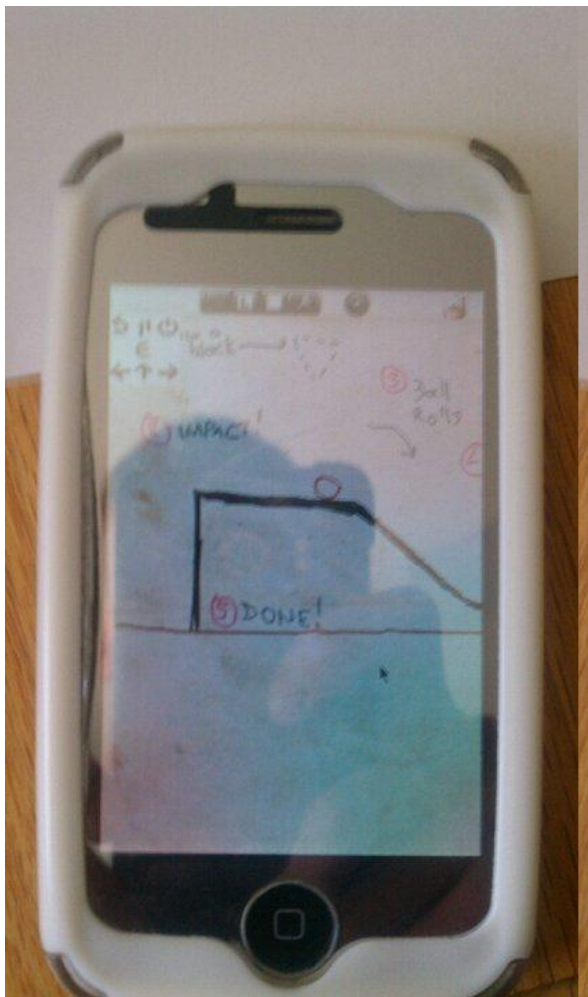
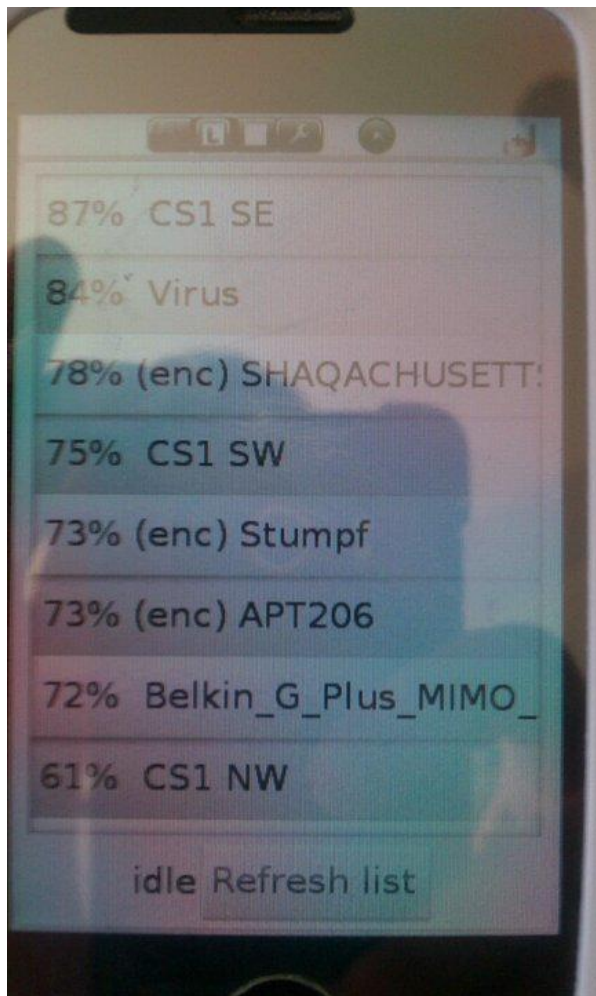
- Red Team Love
- CTF Advocate
- iDroid Project / iX Project
 - OpenEmbedded / OpenMoko







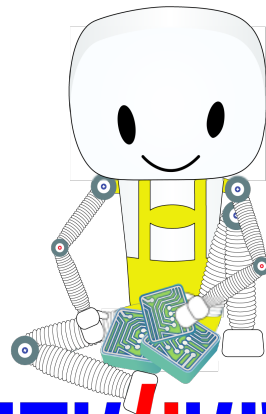
HAK4KIDZ



HAK4KIDZ

Goal

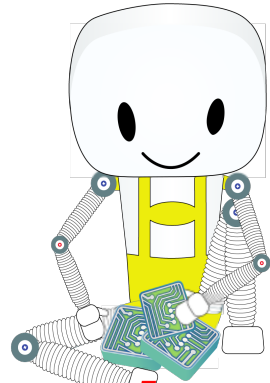
- Teach a methodology to hack the planet.
 - Hack to learn, not learn to hack.



HAK4KIDZ

Road to Pro Gaming

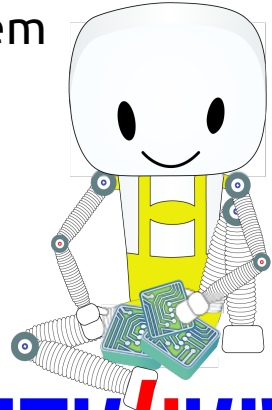
- Megaman
- Diablo II
 - palapk
 - amapk
- DotA
 - Dreamhack
 - ESWC Masters



HAK4KIDZ

Diablo II: Charsi Dupe

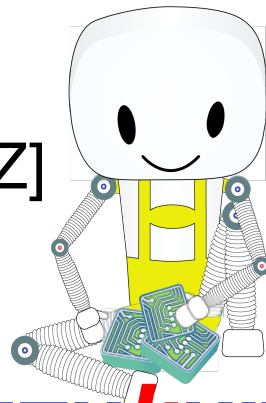
1. Player acquires the (reusable) sequence for the part of the imbue quest that drops the item.
2. Player finds the id of the item he wishes to dupe by simply dropping it on the ground and sniffing the event.
3. Player sends the known sequence to charsi substituting the id with the id of the item to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



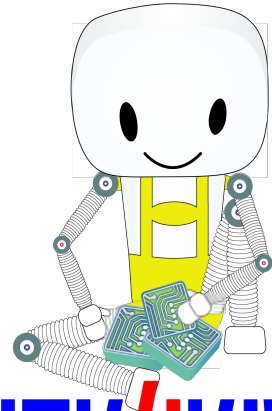
HAK4KIDZ

Diablo II: Charsi Dupe (cont.)

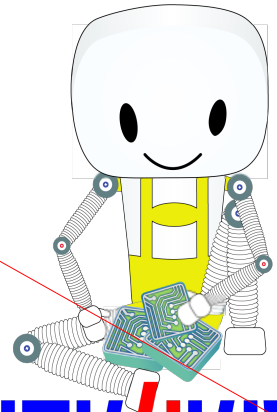
1. Find Charsi
 - a. 13 01 00 00 00 [XX XX XX XX]
2. Pickup Item
 - a. 19 [ZZ ZZ ZZ ZZ]
3. Tell Charsi to imbue the item
 - a. 38[00 00 00 00][XX XX XX XX][ZZ ZZ ZZ ZZ]
4. Repeat
 - a. Profit



Diablo II: Charsi Dupe (cont.)



DotA



HAK4KIDZ



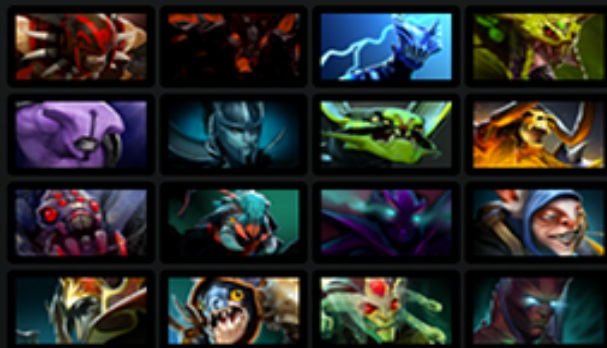
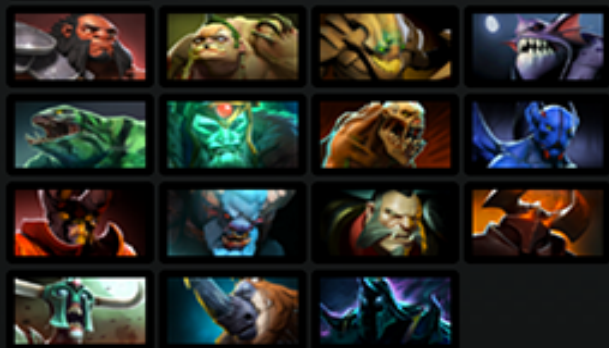
STRENGTH



AGILITY



INTELLIGENCE





Shade

Muerto viv.

Armor:
Invulnerable

Status:




250 / 250

Shade
Muerto viv.

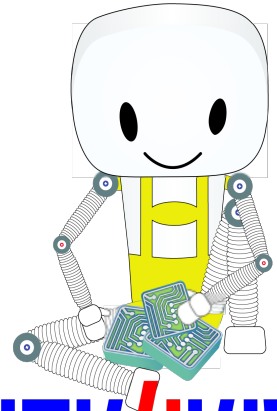
 Armor:
Invulnerable

Status:



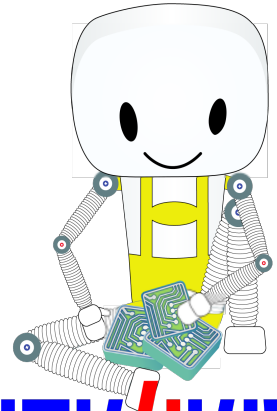
			
			
			

DotA: Creep Blocking



HAK4KIDZ

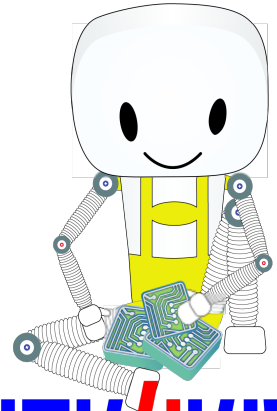
DotA: Creep Blocking Part Two



HAK4KIDZ

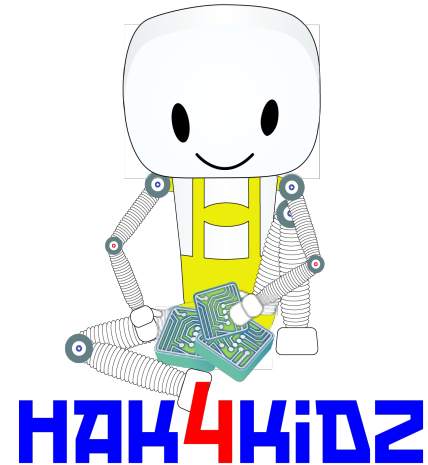
Methodology

What do we know?

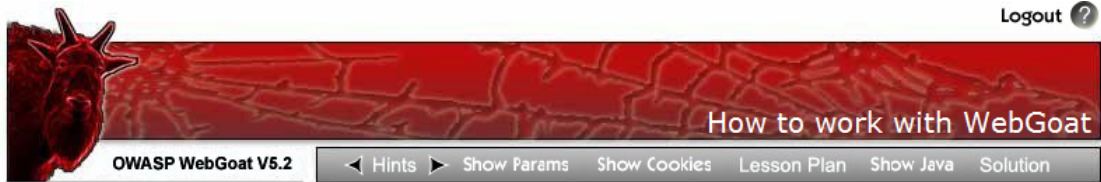


HAK4KIDZ

Megaman



Web Application



Introduction

- ✓ [How to work with WebGoat](#)
- ✓ [Tomcat Configuration](#)
- ✓ [Useful Tools](#)
- ✓ [Create a WebGoat Lesson](#)

General

- Access Control Flaws
- AJAX Security
- Authentication Flaws
- Buffer Overflows
- Code Quality
- Concurrency
- Cross-Site Scripting (XSS)
- Denial of Service
- Improper Error Handling
- Injection Flaws
- Insecure Communication
- Insecure Configuration
- Insecure Storage
- Parameter Tampering
- Session Management Flaws
- Web Services
- Admin Functions
- Challenge

Solution Videos

[Restart this Lesson](#)

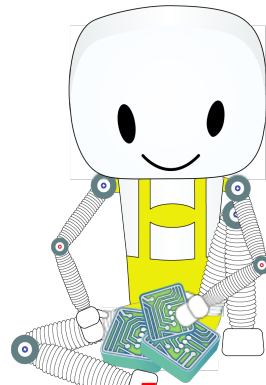
How To Work With WebGoat

Welcome to a short introduction to WebGoat.
Here you will learn how to use WebGoat and additional tools for the lessons.

Environment Information

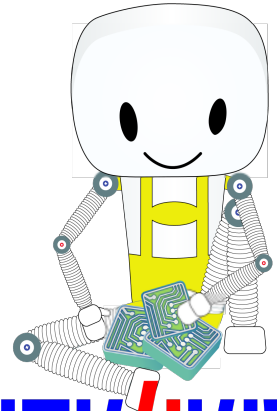
WebGoat uses the Apache Tomcat server. It is configured to run on localhost although this can be easily changed. This configuration is for single user, additional users can be added in the tomcat-users.xml file. If you want to use WebGoat in a laboratory or in class you might need to change this setup. Please refer to the Tomcat Configuration in the Introduction section.

The WebGoat Interface



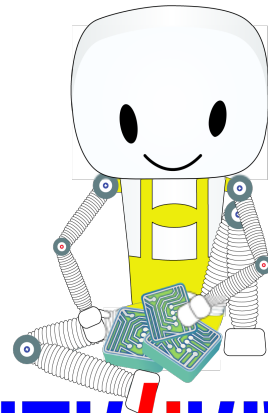
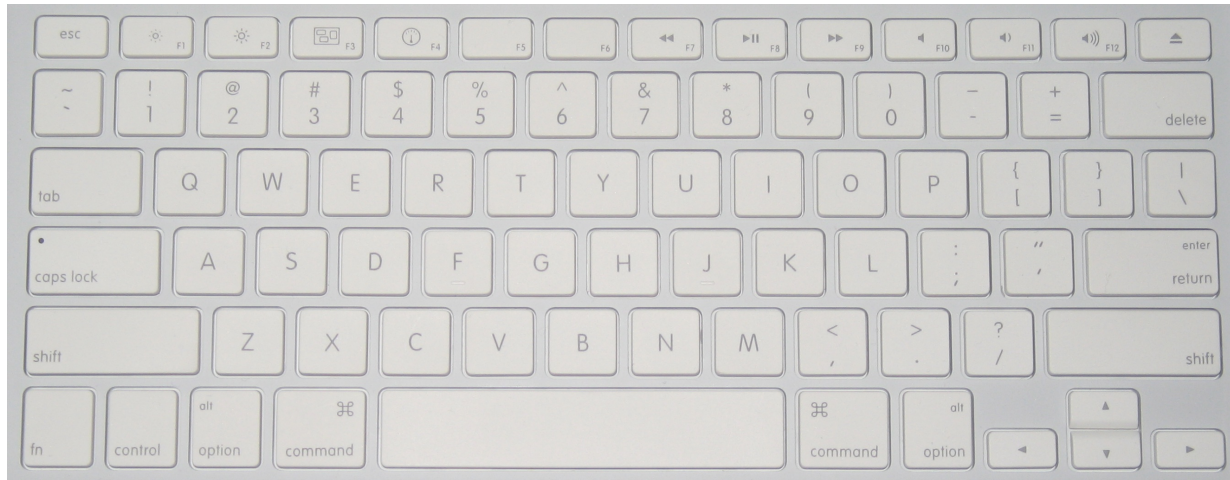
HAK4KIDZ

Megaman Input



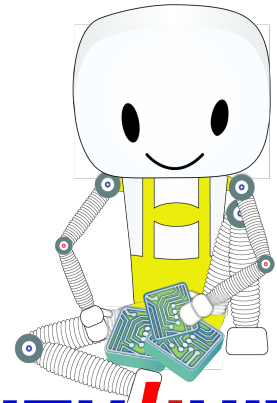
HAK4KIDZ

Web Application Input



HAK4KIDZ

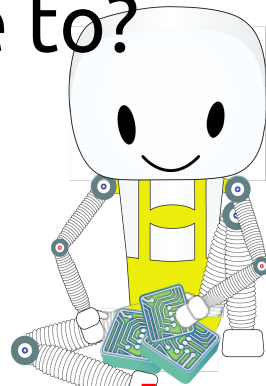
MegaMan Boss Fight



HAK4KIDZ

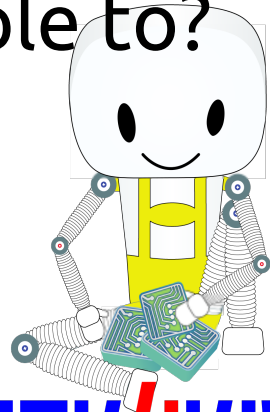
MegaMan Methodology

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



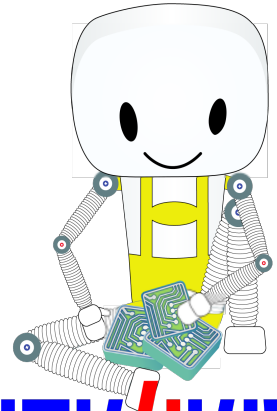
Web Application Methodology

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



Learning about Web Applications

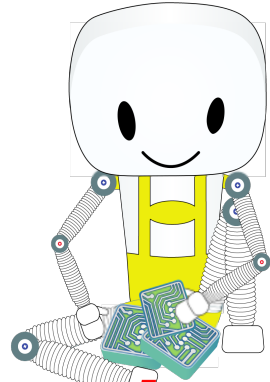
DEMO



HAK4KIDZ

Build your own Web Application

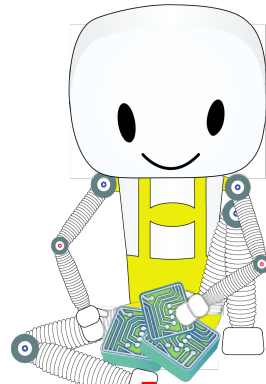
- <http://learnpythonthehardway.org/>
- <http://learncodethehardway.org/>



HAK4KIDZ

Go Hack Some Stuff

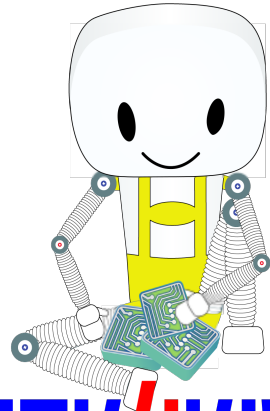
- [OWASP Broken Web Application Project](#)
- [Mutillidae](#)



HAK4KIDZ

What did we learn?

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



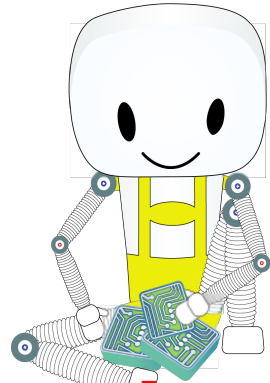
HAK4KIDZ

Questions?

Thanks for coming!

www.lopisek.com

@_Lopi_ on Twitter



HAK4KIDZ