Hack to the future

Marinus Kuivenhoven
Senior Security Specialist

#hitb2012ams
Commodore 64
Commodore 1541 floppy drive
Copy protection

• Difference in resources to buy and use vs. copy and use
Copy protection C64 #1

• Bad Sector (1983)
Copy protection reboot

- Xbox 360 (2005)
Copy protection C64 #2

• Gap Bytes (1985)
Copy protection reboot

• PC games with SafeDisc (2002 - ....)
Copy protection C64 #3

• Trackallignment (1987)
Copy protection reboot

- PlayStation 2 (2000)
  - Afwijkende ruimte tussen blocks
So..

We don’t learn from other people mistakes
The ‘F’-test

An infection is the invasion of body tissues by disease-causing microorganisms, their multiplication and the reaction of body tissues to these microorganisms and the toxins that they produce. Hosts normally fight infections themselves via their immune system.

Assignment:
Count the number of times the character 'F' appears on this slide. Write it on a paper, put your fingers up or yell the amount. Don’t cheat and count it in one go.
Phone + Freak = Phreak

"Joybubbles" & "Captain Crunch"
Bluebox (1960)

Phone → Switch 1 → Phone ∴ Free phonenumber

Phone ← Switch 2
Bluebox (1960)

Phone → 2600hz whistle → Switch 1

Phone ← Switch 2
Trygve Reenskaug

- DBO, MVC, OO, UML, etc.
Front-end:
USERNAME: [PERSONA]
PASSWORD: [SECRET12]

Back-end:
Is access the account permitted when:
the username is 'PERSONA'
en
the password is 'SECRET12';
Front-end:
USERNAME: [PERSONA]
PASSWORD: [IDUNNO or 1=1]

Back-end:
Is access to the account permitted when:
the username is 'PERSOONA'
and
the password is IDUNNO or 1=1;

1 Request with data

Browser

3 New page

Webserver

2 Generates page
Cross-site scripting (1996)

1. Request with data + code
2. Generate page with the code
3. New page
4. Show pagina and execute code
Cause

Phone \[\rightarrow\] Switch

Application \[\rightarrow\] Database

Application \[\rightarrow\] Browser

Voice + Tones

Query + Data

Content + Javascript
Cause

Phone → Voice + Tones → Switch
Application → Query + Data → Database
Application → Content + Javascript → Browser
Presentator → Text + Assignment → Audience
The interpreter can’t distinguish between data and logic.
Out of band communication - Telefoon

Phone

Voice

Switch 1

Voice

Tones

Phone

Voice

Switch 2
Out of band communication - Database

Client → Application

Data

Application → Database

Data

Query
1: stmt = ‘select something from table where column =‘ + variable;

2: stmt = ‘select something from table where column = ?‘;
Bind(1,variable);

1: var: a, -> hash = 0cc175b9c0f1b6a831c399e269772661
var: b, -> hash = 92eb5ffee6ae2fec3ad71c777531578f

2: var: a, then hash = 4a8a08f09d37b73795649038408b5f33
var: b, then hash = 4a8a08f09d37b73795649038408b5f33
Out of band communication - Browser

HTTP only has in band communication

1 Request with code

Browser

→

Webserver

←

3 New page

2 Generate page with code
Focus on incidents..
specific a blacklist of incidenten

- OWASP top 10
  - Injection
  - Cross-Site Scripting (XSS)
  - Broken Authentication and Session Management
  - Insecure Direct Object References
  - Cross-Site Request Forgery (CSRF)

- SANS CWE/25
  - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
  - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
  - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
  - Unrestricted Upload of File with Dangerous Type
  - Cross-Site Request Forgery (CSRF)
  - URL Redirection to Untrusted Site ('Open Redirect')

- WASC 24+2
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - SSI Injection
  - SQL Injection
  - XPath Injection
  - XQuery Injection
Principe

Client → Data → Logica → Interpreter

Client → Contextsafe data + Logica → Interpreter
Listerine
Thus..

We have the right ideas
We know the solutions

We just use them in the wrong way
And present them in the wrong way

We can learn from history how to this right
More on this stuff

C64:
Michael Steil / c64.org
Nate / root.org

XSS/SQL/Injection flaws:
www.owasp.org

Engressia/Draper/Semmelweis/Lister:
www.wikipedia.org
staat voor resultaat