Seguridad Web:
Ataques a la lógica de negocio

Miguel Ángel Hernández Ruiz

Agenda

1| **MOTIVACIÓN**
2| UNA HISTORIA DE HACKING
3| LO QUE ESTAMOS BUSCANDO
4| UNA APROXIMACIÓN METODOLÓGICA
5| LA TIENDA
6| CASOS DE ABUSO DESDE 0
7| CONCLUSIONES

Motivación

January 12, 2007 12:15 PM PST

Macworld crack (passes, hacke

By Joris Evers
Staff Writer, CNET News

Alongside the VIPs and pe hacker claims he also got p Jobs' speech at the Macwo this week.

A security weakness in the event's Web ente the e claim Macv the J spee

Security Advisory - VirtueMart Extension for Joomla!

By Marc-Alexandre Montp

If you're using the popular Virtue ds), you should update right away. During a routine aud could be used by a malicious us access, the attacker has full con

execution, (save/modif basically all

KrebsonSecurity

16 White-Hat Hacker Schools Security Pro School

MAY 14

A Bug in Bug Tracker "Bugzilla" exposes Private Bugs

by Sabari Selvan on Tuesday, October 07, 2014 |

Vulnerability researchers at Check Point Software Technologies reported the bug to Mozilla that allows anyone to register with email address of the targeted domain (for example, admin@mozilla.com) and bypass email validation.

Researcher exploited the vulnerability and managed to create administrator accounts for the Mozilla.org, Mozilla.com and Bugzilla.org.

Gervase Markham from Mozilla wrote a detailed technical post. The attack method appears to be "***HTTP Parameter Pollution(HPP)***" technique.

was visiting the site to pay his and was getting ready to fork

ould skip the payment he checkout page to a produced an email

a tenth of the done this 4 and the credit

07-19-2013, 11:09 AM

samkgood
Junior Member

Website Shopping Cart Manipulatio

My question involves collection proceedin

A customer of our website found a trick t actual cost. We did not notice the mistake times before. He owes $322 for the items card company and there is nothing they c

#1

Join Date: Jul 2013
Posts: 2

Bugzilla

Agenda

1| Motivación
2| Una historia de Hacking
3| Lo que estamos buscando
4| Una aproximación metodológica
5| La tienda
6| Casos de Abuso desde 0
7| Conclusiones

Una historia de hacking:
Los personajes

Nombre: Paul
Edad: 27
Trab: Developer

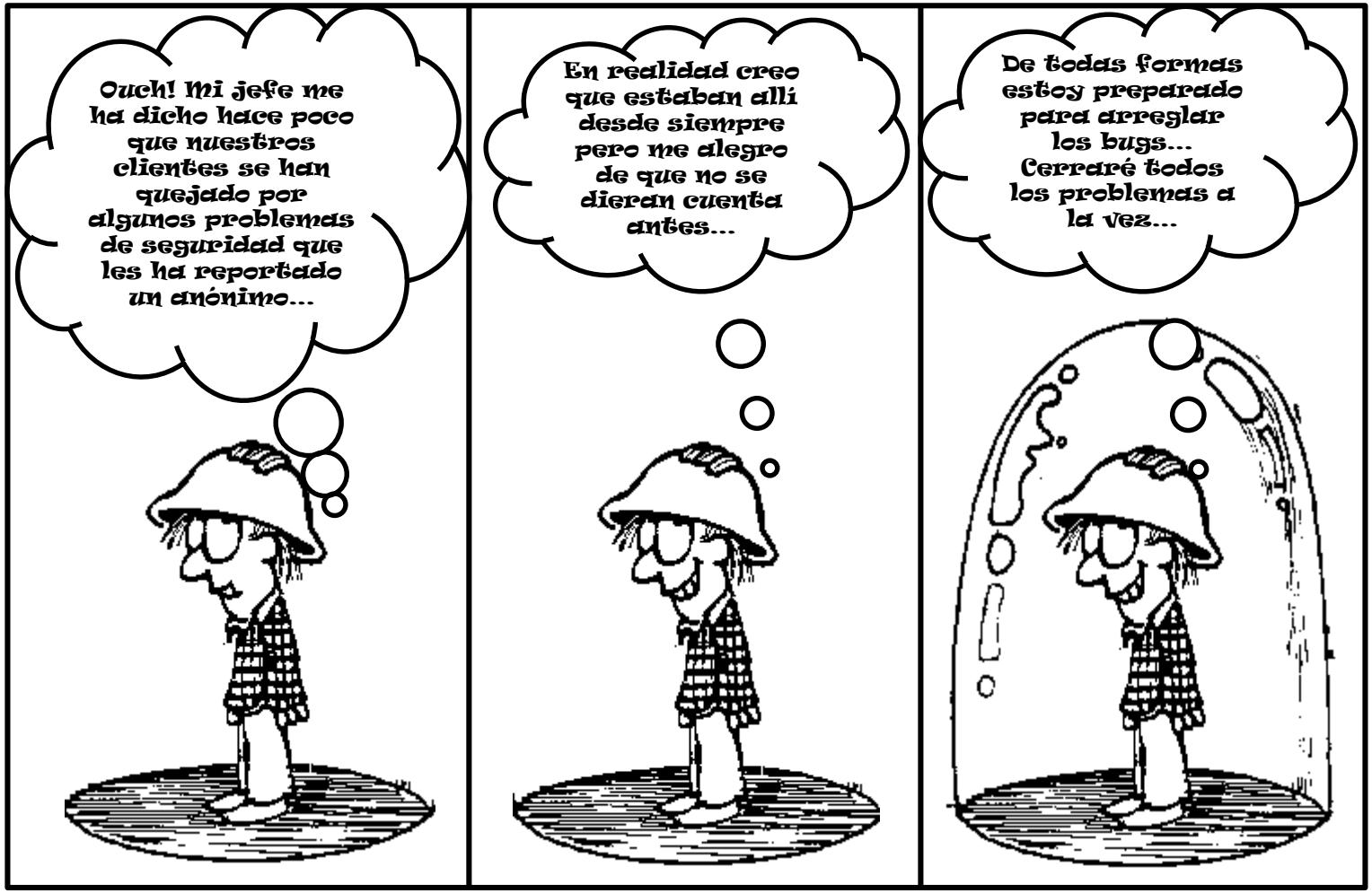
Paul trabaja como IT Engineer para una empresa que proporciona una solución de carro de la compra a gran cantidad de clientes. Nunca le ha prestado atención a la seguridad; su jefe tampoco…

Nombre: Mike
Edad: 22
Trabajo: Ninguno

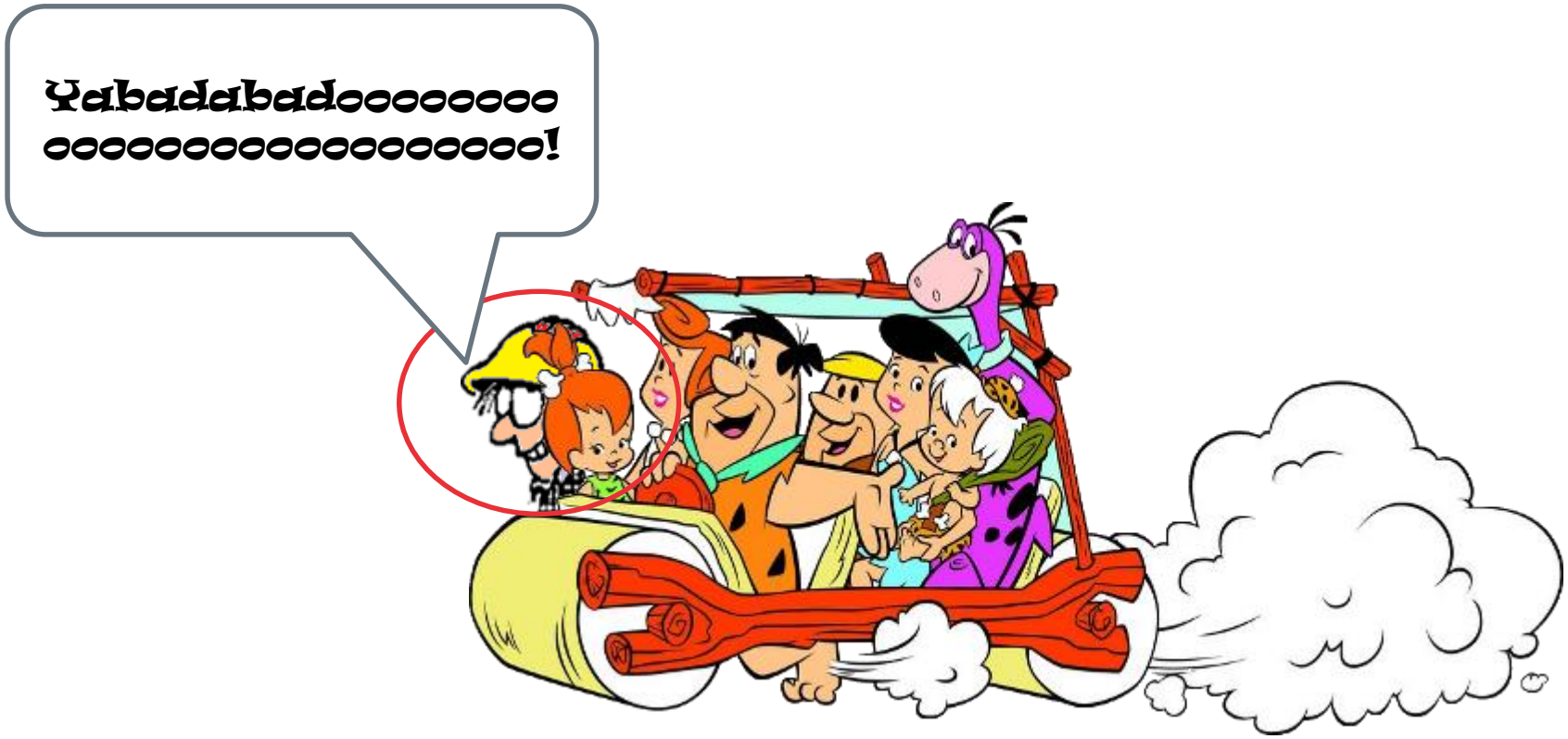
Mike es un estudiante de universidad con demasiado tiempo libre. Es un apasionado de la seguridad al que le encanta encontrar vulnerabilidades en las aplicaciones web. Es muy consciente de lo que implica la seguridad…

Exención de Responsabilidad:
He encontrado ambas imágenes en Internet sin aparentes derechos de copia. Si alguien encontrase las mismas con dichos derechos ruego me lo comunique para proceder en consecuencia.

Una historia de hacking:
El problema



Rep. Gráfica de la App de Pol



Una historia de hacking – La solución

Session Hijacking

Session Fixation

SQLi

Buffer Overflow

XSS

Insecure Direct Object Reference

HTMLi

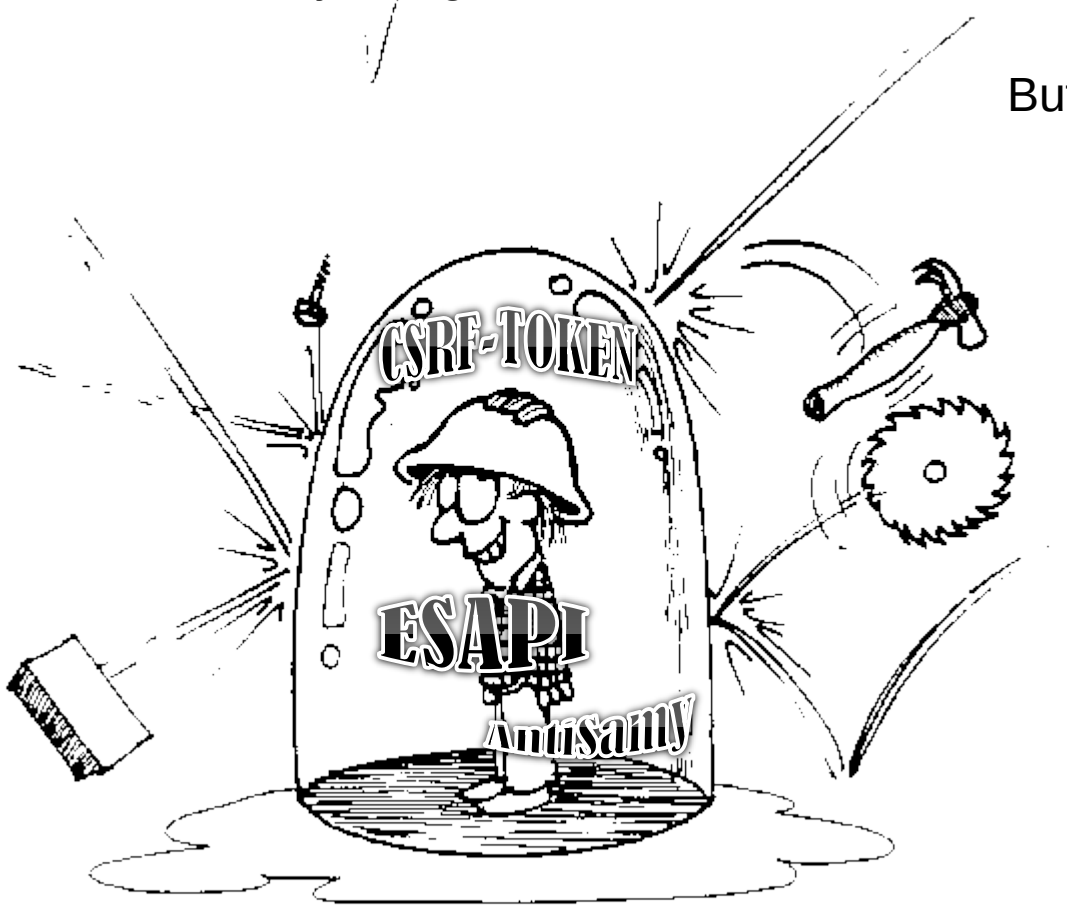
Non-validated Redirects

CSRF

XXE

Server Side Inclusion

LFI / RFI



Rep. Gráfica de la nueva App de Pol

Una historia de hacking:
El contraataque

Una historia de hacking:
¡Owned!

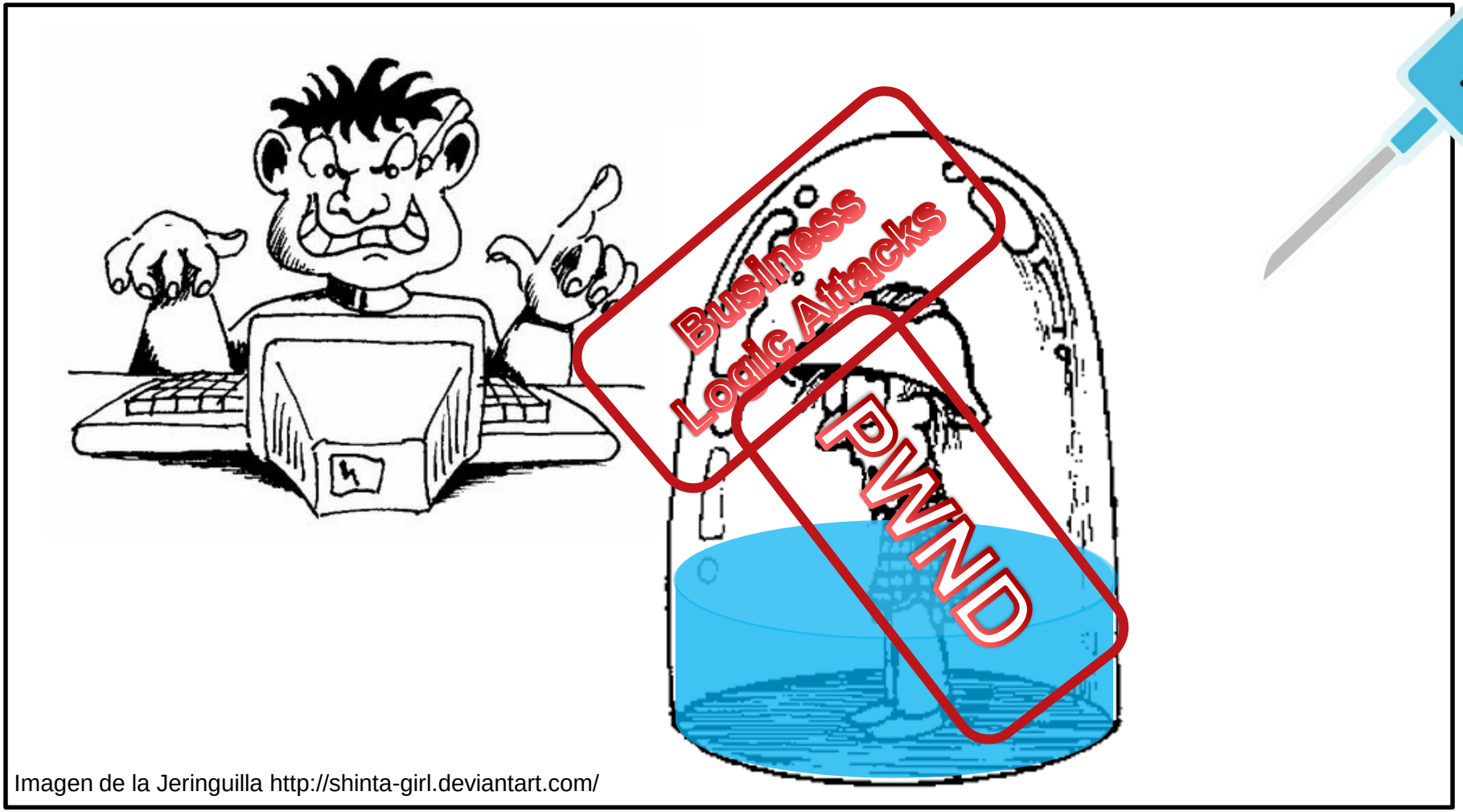


Imagen de la Jeringuilla http://shinta-girl.deviantart.com/

Agenda

1| MOTIVACIÓN
2| UNA HISTORIA DE HACKING
3| LO QUE ESTAMOS BUSCANDO
4| UNA APROXIMACIÓN METODOLÓGICA
5| LA TIENDA
6| CASOS DE ABUSO DESDE 0
7| CONCLUSIONES

Lo que estamos buscando:
La diferencia

La lógica de negocio de la aplicación debe probarse desde una perspectiva de seguridad

Lo que estamos buscando:
Casos de Uso vs Casos de Abuso

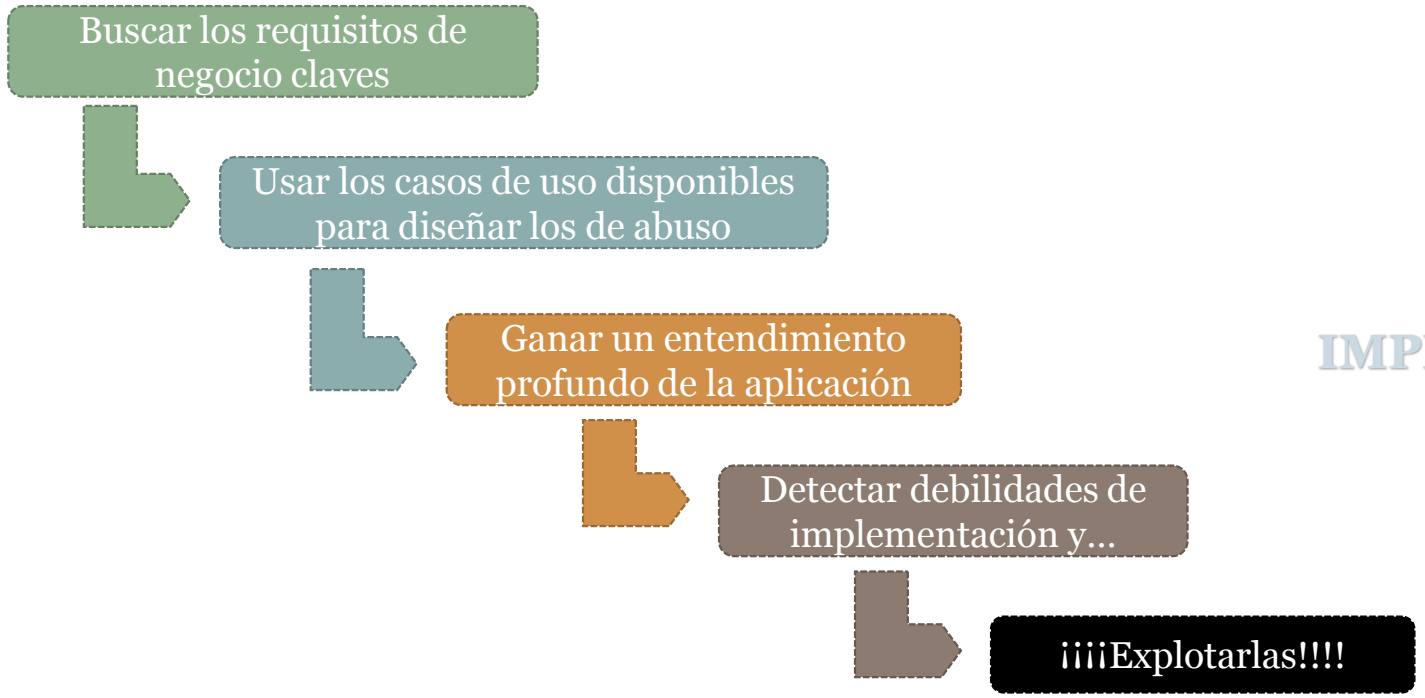
- Casos de Uso
  - Un **CASO DE USO** es una lista de pasos, típicamente definida como interacciones entre un role y un sistema para conseguir un objetivo
  - Son básicamente escenarios estructurados donde se detalle un comportamiento normal durante el uso de una aplicación o software
  - Un caso de uso no es sólo un diagrama ni tampoco suele ser sólo texto. Es una mezcla de ambas cosas donde se detalla gráficamente una secuencia de acciones y se expone en modo texto junto a su objetivo , el contexto, una descripción de los actores, etc…

- Casos de Abuso
  - Un **CASO DE ABUSO** es un tipo de interacción completa entre un sistema y uno o más actores donde el resultado de la interacción resulta perjudicial para el sistema, uno de los actores o uno de los terceros implicados por el sistema
  - Los casos de abuso se suelen crear en conjunción con casos de uso (siempre que estén disponibles), pero haciendo uso de documentos separados
  - No existe terminología o símbolos especiales introducidos para los casos de abuso

Agenda

1| Motivación
2| Una historia de Hacking
3| Lo que estamos buscando
4| Una aproximación metodológica
5| La tienda
6| Casos de Abuso desde 0
7| Conclusiones

La escalera hacia el Bug



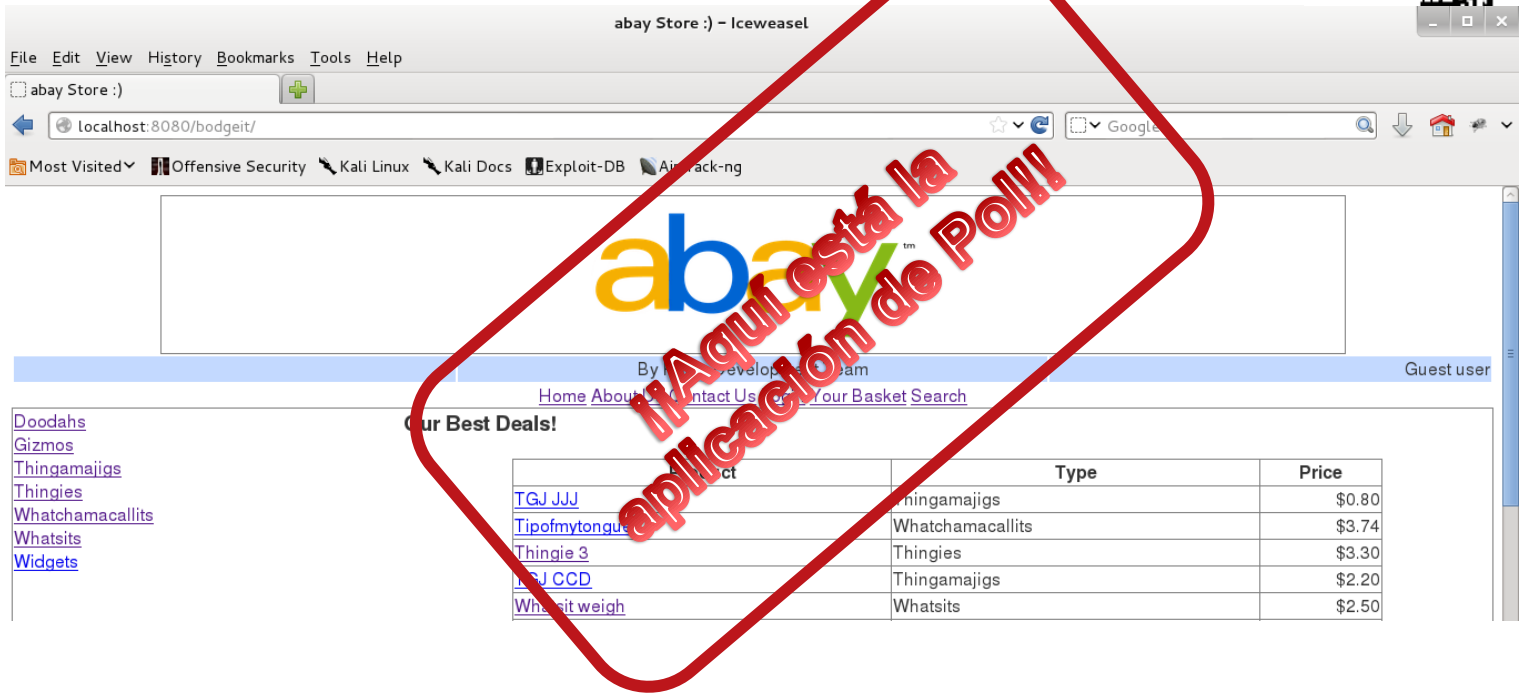
LA ESCALERA HACIA EL BUG

Agenda

1| MOTIVACIÓN
2| UNA HISTORIA DE HACKING
3| LO QUE ESTAMOS BUSCANDO
4| UNA APROXIMACIÓN METODOLÓGICA
5| LA TIENDA
6| CASOS DE ABUSO DESDE 0
7| CONCLUSIONES

La Tienda:

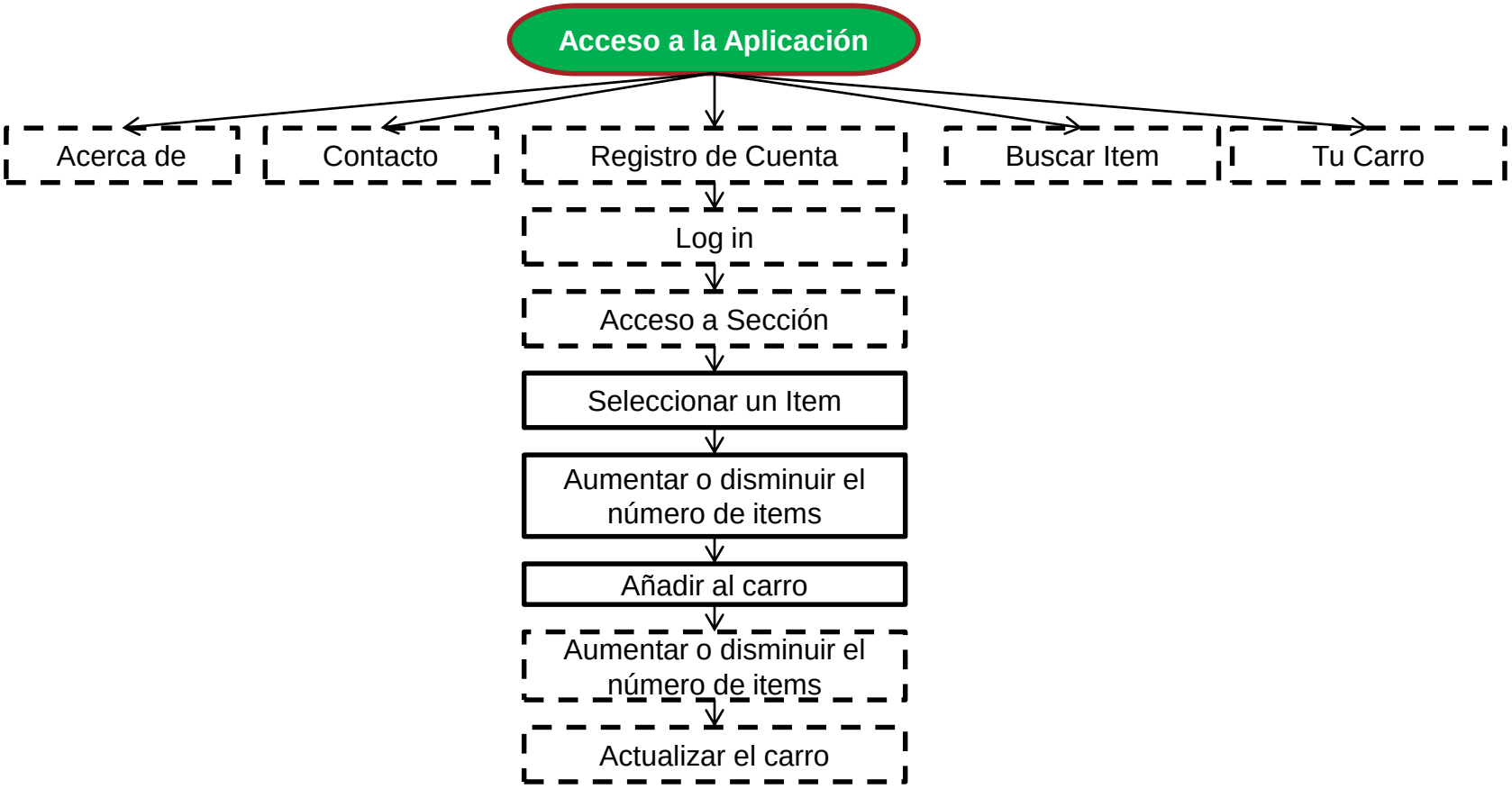
abay (La aplicación de Pol)



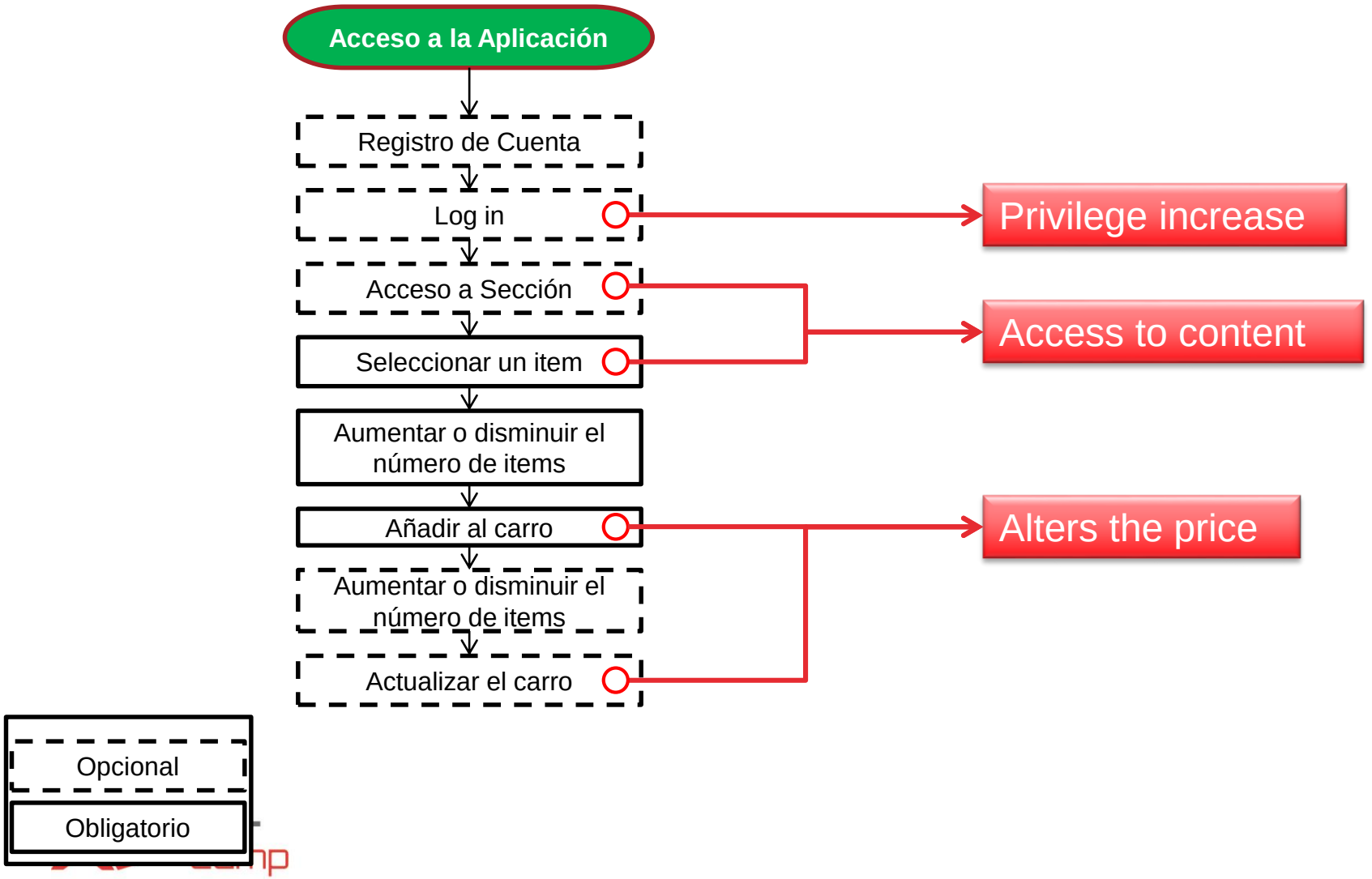
Agenda

1| MOTIVACIÓN
2| UNA HISTORIA DE HACKING
3| LO QUE ESTAMOS BUSCANDO
4| UNA APROXIMACIÓN METODOLÓGICA
5| LA TIENDA
6| CASOS DE ABUSO DESDE 0
7| CONCLUSIONES

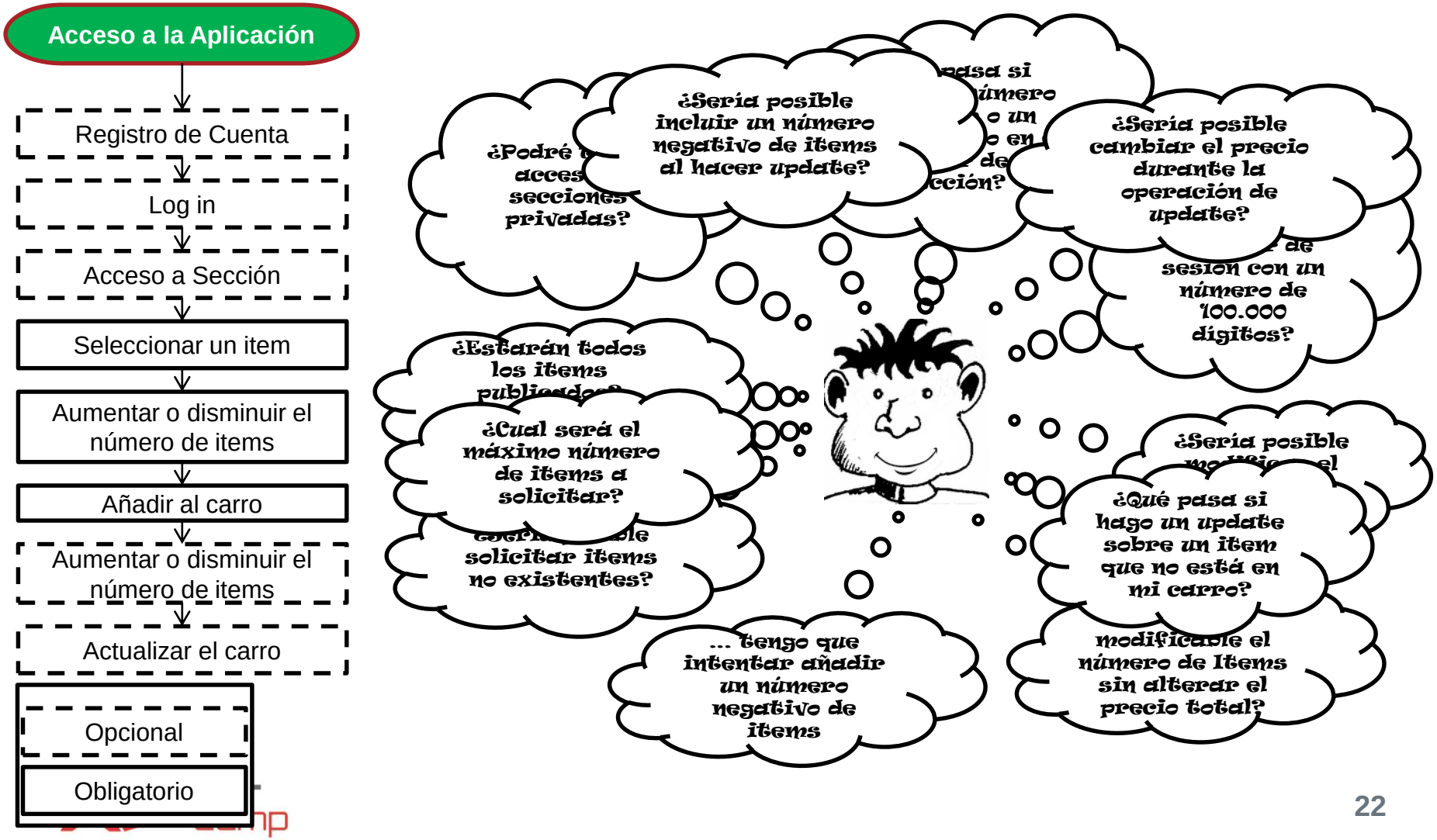
Casos de abuso desde cero:
El workflow



Casos de abuso desde cero:
Los puntos clave

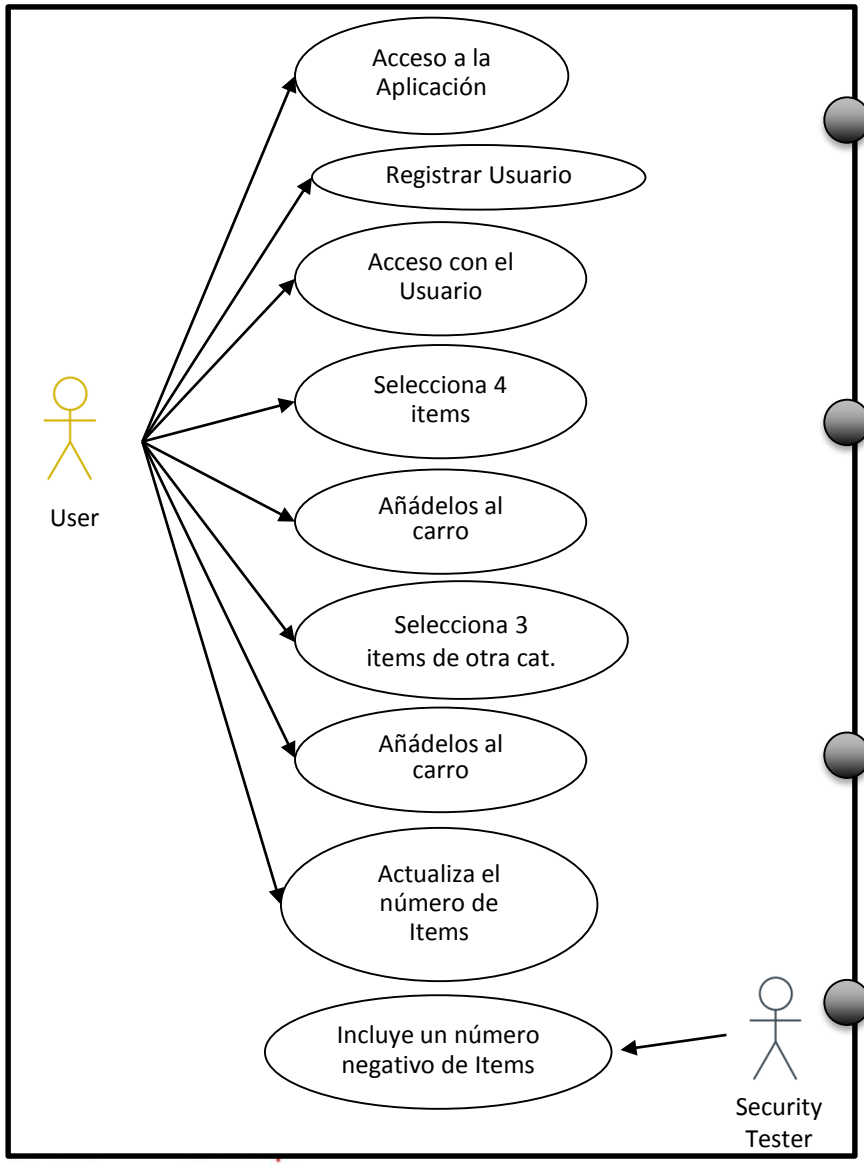


Casos de abuso desde cero:
El pensamiento negativo



Casos de abuso desde cero:

El caso de Abuso



Objetivo

Ganar un mayor nivel de confianza en el tratamiento del número de items en el lado del servidor

Precondiciones

- Todos los módulos necesarios de la aplicación han sido desplegados
- Deben existir como mínimo dos categorías dadas de alta en el entorno de pruebas
- Una de las categorías tiene que disponer de 4 items y otra de 3 como mínimo

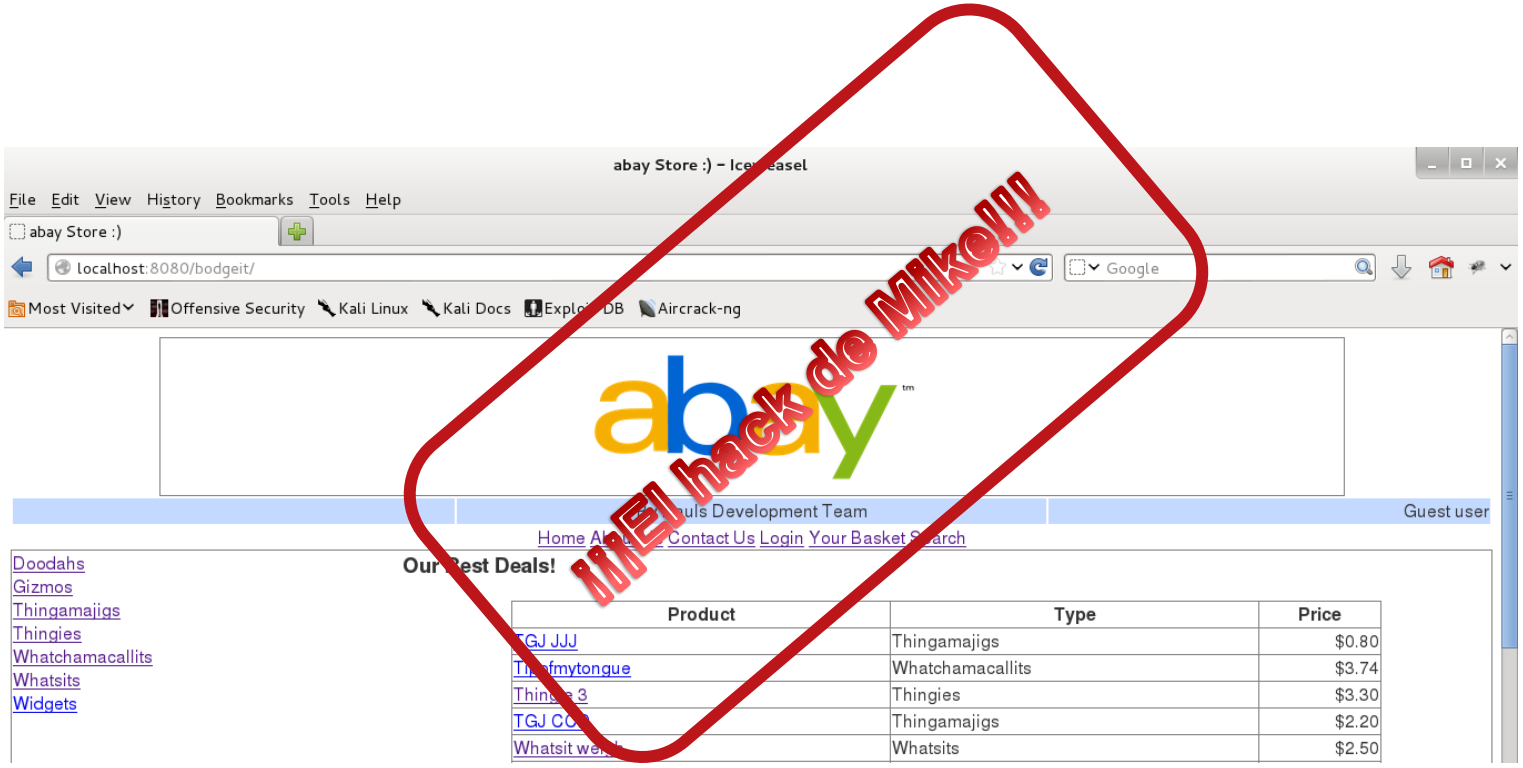
Actores

- Usuario: agente que realiza acciones comunes sobre el sistema
- Tester de Seguridad: agente que causará un comportamiento anómalo

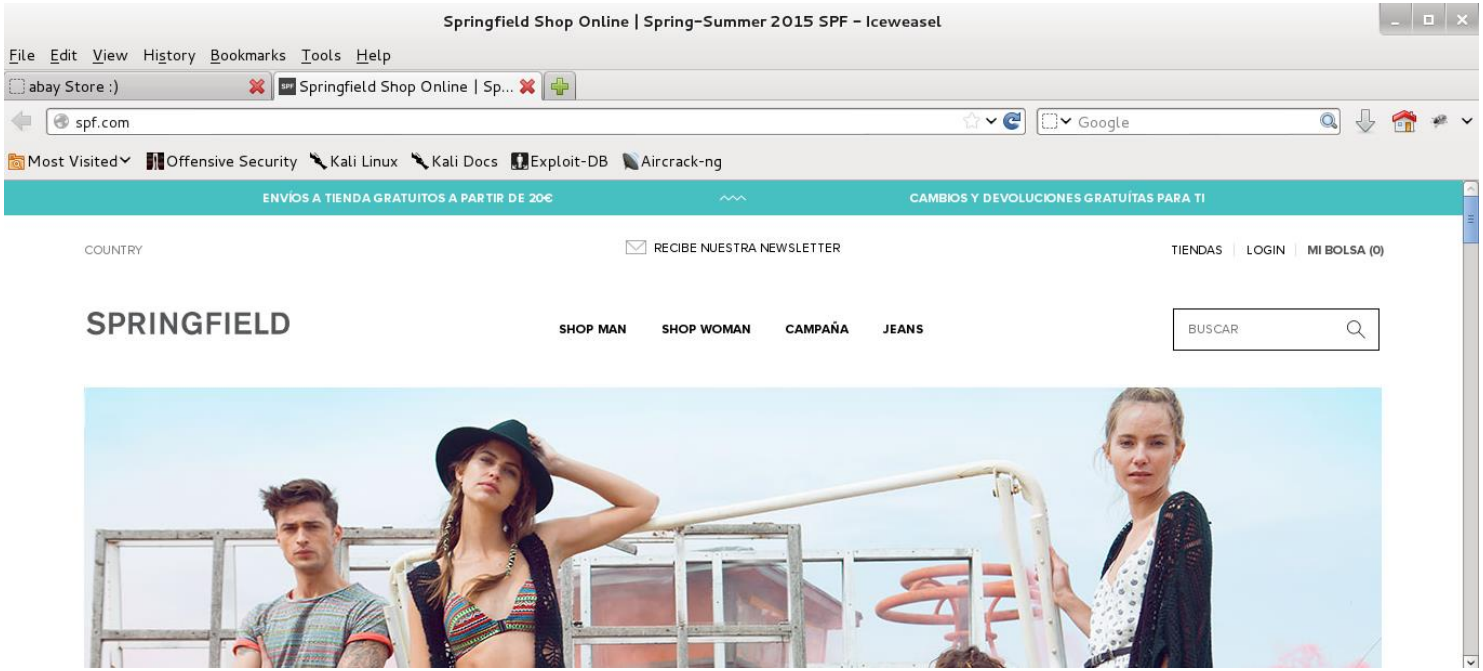
Descripción

- Accede al sistema a través de la dirección http://www...
- Registra un nuevo usuario: haz clic sobre la entrada…
- …

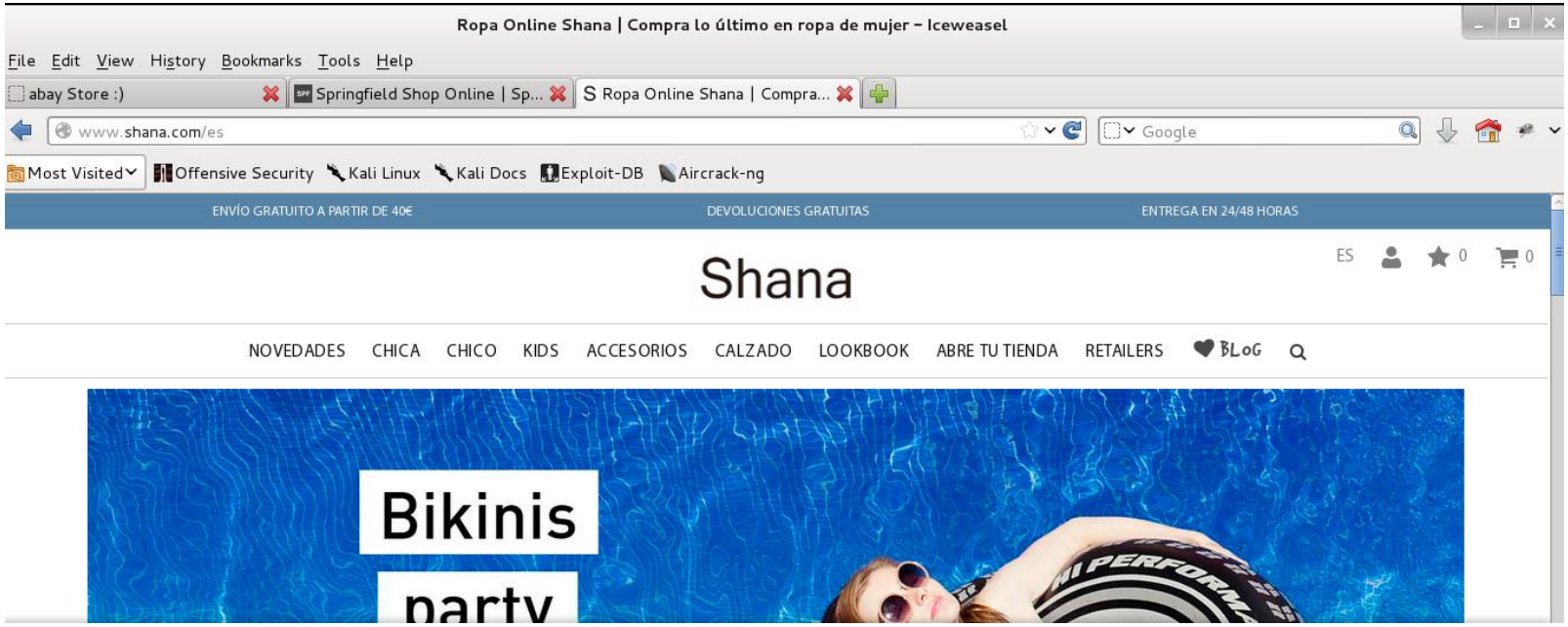
Casos de abuso desde cero:
El hack



Atacando el sistema de stock



Atacando la lógica de negocio “for fun and profit”



Agenda

1| Motivación
2| Una historia de Hacking
3| Lo que estamos buscando
4| Una aproximación metodológica
5| La tienda
6| Casos de Abuso desde 0
7| Conclusiones

Conclusiones

- **Iluminan un área oscura de la seguridad que es fuente de bugs**
- **Refuerzan la seguridad de la aplicación**
- **Incrementan la confianza de los clientes en la seguridad de la aplicación**
- **Se incluye un pensamiento negativo en el proceso de testing**
- **Se dispondrá de un repositorio mayoritariamente reutilizable de casos de abuso por aplicación**
- **Ningún dispositivo de seguridad perimetral te protegerá contra este tipo de ataques…**

…Los Casos de Abuso son Necesarios

Referencias

- **OWASP Business Logic Cheat sheet; *OWASP Foundation; 2014***
  - https://www.owasp.org/index.php/Business_Logic_Security_Cheat_Sheet
- **Common weakness Enumeration; *Business Logic Errors; 2014***
  - http://cwe.mitre.org/data/definitions/840.html
- **Ten Business Logic Attack Vectors: Business Logic Bypass & More; *NTObjectives; 2012***
  - http://www.ntobjectives.com/research/web-application-security-white-papers/business-logic-attack-vectors-white-paper/
- **How to Prevent Business Flaws Vulnerabilities in Web Applications; Marco Morana; 2011**
  - http://es.slideshare.net/marco_morana/issa-louisville-2010morana
- **Seven Business Logic Flaws that Put your Website at Risk; *Jeremiah Grossman; October 2007***
  - https://www.whitehatsec.com/assets/WP_bizlogic092407.pdf

Referencias

- **White-Hat Hacker Schools Security Pro School; Bryan Kerbs; 2014**
  - http://krebsonsecurity.com/2014/05/white-hat-hacker-schools-security-pro-school/
- **Defying Logic - Business Logic Testing with Automation; Rafal Los & Prajakta Jagdale; 2011**
  - http://es.slideshare.net/RafalLos/defying-logic-business-logic-testing-with-automation
- **Bugs in your shopping cart: A Taxonomy; Giri Vijayaraghavan et al; 2002**
  - http://www.testingeducation.org/articles/BISC_Final.pdf
- **A Bug in Bug Tracker "Bugzilla"; Sabari Selvan; 2014**
  - http://www.ehackingnews.com/2014/10/http-parameter-pollution-bugzilla-vulnerability.html
- **Website Shopping Cart Manipulation Caused Product to be Shipped Below Retail Price; anonymous; 2013**
  - http://www.expertlaw.com/forums/showthread.php?t=161561
- **Security Advisory – VirtueMart Extension for Joomla!; Marc-Alexandre Montpas; 2014**
  - http://blog.sucuri.net/2014/09/security-advisory-virtuemart-for-joomla.html

Preguntas y Respuestas

¡Hasta la Próxima!

Miguel Ángel Hernández Ruiz
Security Consultant & Web Application Pentester

Miguel Angel Hernández es IT Security Consultant & WA Pentester en la empresa Sopra Group. Actualmente se encuentra desarrollando su actividad profesional entre la consultoría y las pruebas de seguridad para clientes de ámbito internacional. Atesora más de 9 años de experiencia repartidos entre investigación, consultoría y pruebas durante los cuáles ha obtenido las certificaciones internacionalmente reconocidas CEH, CISA, CISM, ISTQB-f, ITIL-f e IRCA LA 27001

Datos de Contacto

Miguel Angel Hernández Ruiz

Miguel-angel.hernandez@sopra.com / hernandezrma@gmail.com

sopra

cyber camp

https://cybercamp.es **#CyberCamp15** **@CyberCampEs**

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD