WebApp Penetration Testing

A gentle introduction

Ruben Recabarren
CISSP-ISSAP, GSE, CyberGuardian (red team)

Consultor de Seguridad Informática

http://latinsec.blogspot.com

@latinsec

¿Quien soy?

Ruben Recabarren

- Consultor ITSec por 10+ años
- Especialista en pruebas de penetración.
- Criptografía, protocolos de comunicación segura.
- CISSP, CISSP-ISSAP, GIAC - GSEC, GCIA, GCIH, GWAPT, GPEN, GAWN, GCFA, Cyber Guardian (red team),

Agenda

Pruebas de penetración para aplicaciones web

- ¿Qué son?
- ¿Qué **NO** son?
- ¿Para qué?
- Vulnerabilidades obvias pero catastróficas.
- Vulnerabilidades NO-obvias pero igualmente catastróficas.

¿Qué son?

Pruebas de penetración para aplicaciones web

- Evaluación enfocada a aplicaciones web.
- Evaluación desde el punto de vista de un atacante real.
- Mucho más que dialogos de “alerta” y listas de vulnerabilidades.
- Innovación, desarrollo de técnicas más alla de las empleadas usualmente.

¿Qué NO son?

Pruebas de penetración para aplicaciones web

- No es un "sondeo" de vulnerabilidades.
- No es una "auditoría."
- No es la ejecución de un scanner automatizado.
- No es un método para la generación de: Miedo-Incertidumbre-Duda.

¿Para qué?

Pruebas de penetración para aplicaciones web

- Numerosas alternativas.
- ¿Para saber si pueden “hackearme”?
- Estimación verdadera del impacto de la explotación de la vulnerabilidad.
- Utilización eficiente de los recursos destinados a la remediación.
- ISO, ITIL, PCI, SOX, HIPAA, etc no son suficientes.

Vuln's Obvias

Protección del lado del cliente

- "Esta función no está permitida"
- Botón derecho "deshabilitado"
- Protección del "Source Code" de la página web.
- "Client-side scripting" - JavaScript.
- ¿Cómo se evaden estos mecanismos?
- ¿Cual es el impacto?

Vuln's Obvias

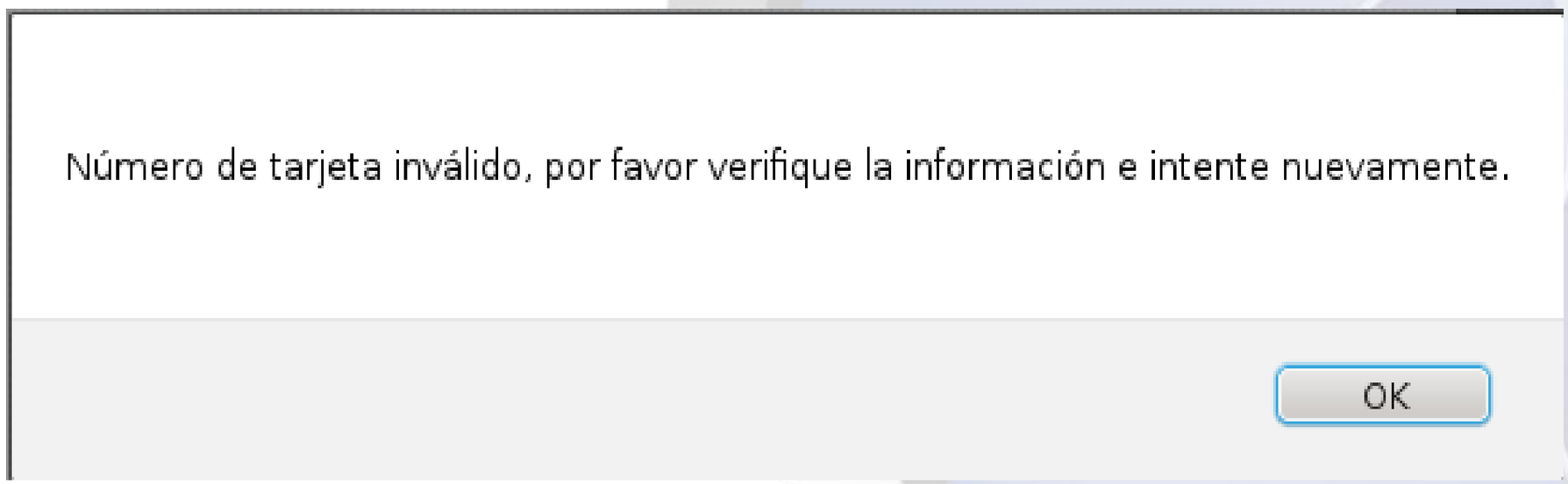
Password Guessing – Password Cracking

- WARGAMES - 1983
- Puede ser lame, pero todavía muy efectivo.
- Vuln subyacente: no hay control sobre los queries.
- ¿Cómo se llevan a cabo estos ataques?
- ¿Cual es el impacto?

Vuln's Obvias

USERNAME Guessing

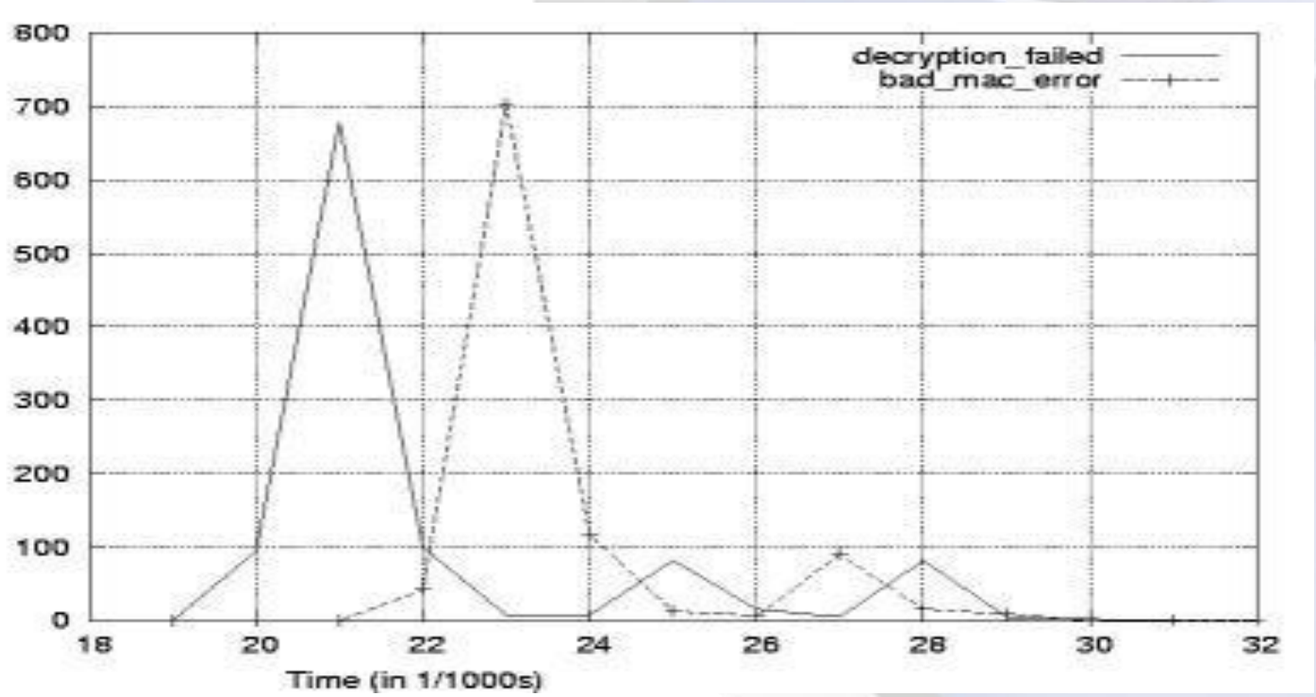
- Probablemente más viejo que 1983.
- Sólo recientemente recibiendo atención.
- Vuln subyacente: situación de “oráculo”



Vuln's Obvias

USERNAME Guessing

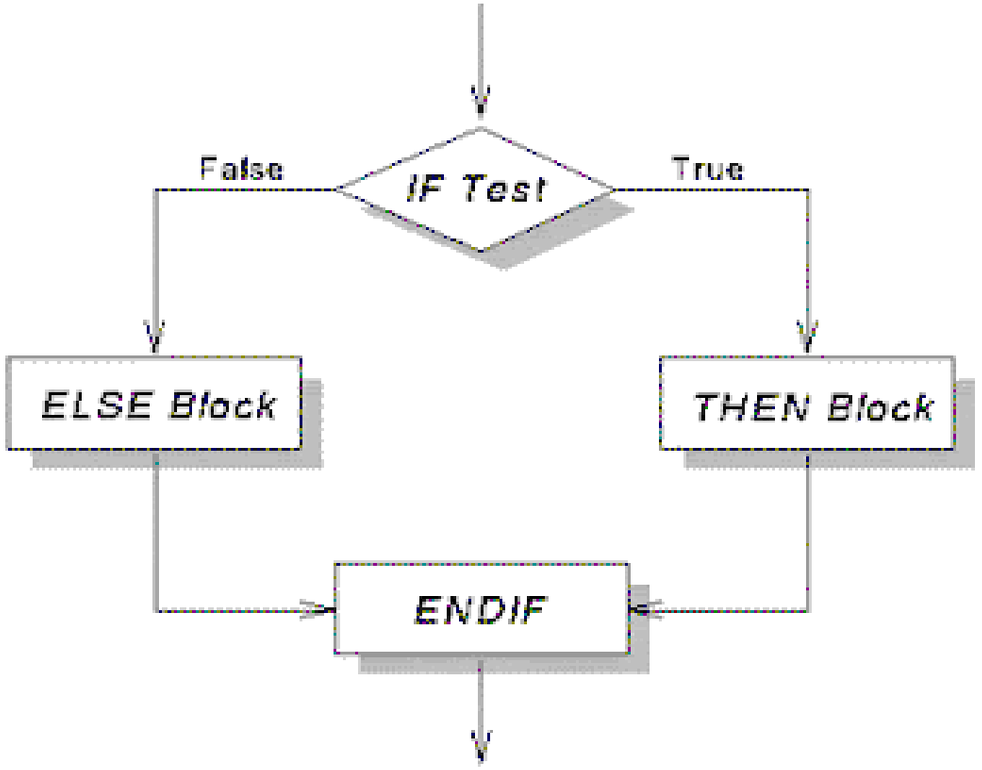
- No es necesario un mensaje explícito.
- Las diferencias pueden ser sutiles.
- Se abre la puerta para “timing attacks”



Vuln's Obvias

USERNAME Guessing

- ¿Cómo se llevan a cabo estos ataques?
  - HINT: Lenguajes de scripting



Condimentos base:

- Un loop
- un if-then-else

Salsa secreta:

- Multi-threading

1
2

Vuln's Obvias

USERNAME Guessing

- ¿Cúal es el impacto?
- Mecanismo alterno para obtener credenciales de acceso
- Posibilidad de ataques de denegación de servicio.
- Un grandísimo “etc”.

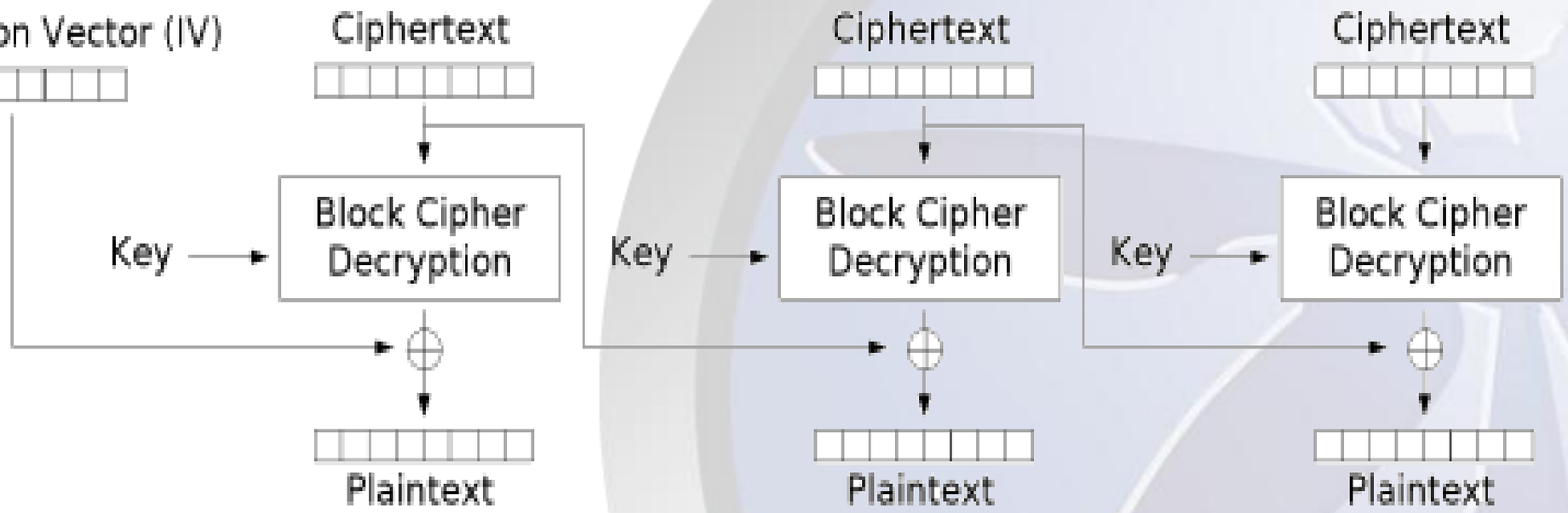
Vuln's NO Obvias

Padding Oracle Attacks

- Idea original de Vaudenay – 2002.
- Ataque práctico sobre cookies http encriptadas por frameworks: Java Server Faces, Ruby on Rails y ASP.NET.
- Popularizados por Juliano Rizzo y Thai Duong 2010-2011.
- Vuln subyacente: situación de “oráculo”

Encripción CBC

CBC – Cypher Block Chaining - Decryption.



Cipher Block Chaining (CBC) mode decryption

Fuente: Wikipedia.org

Padding

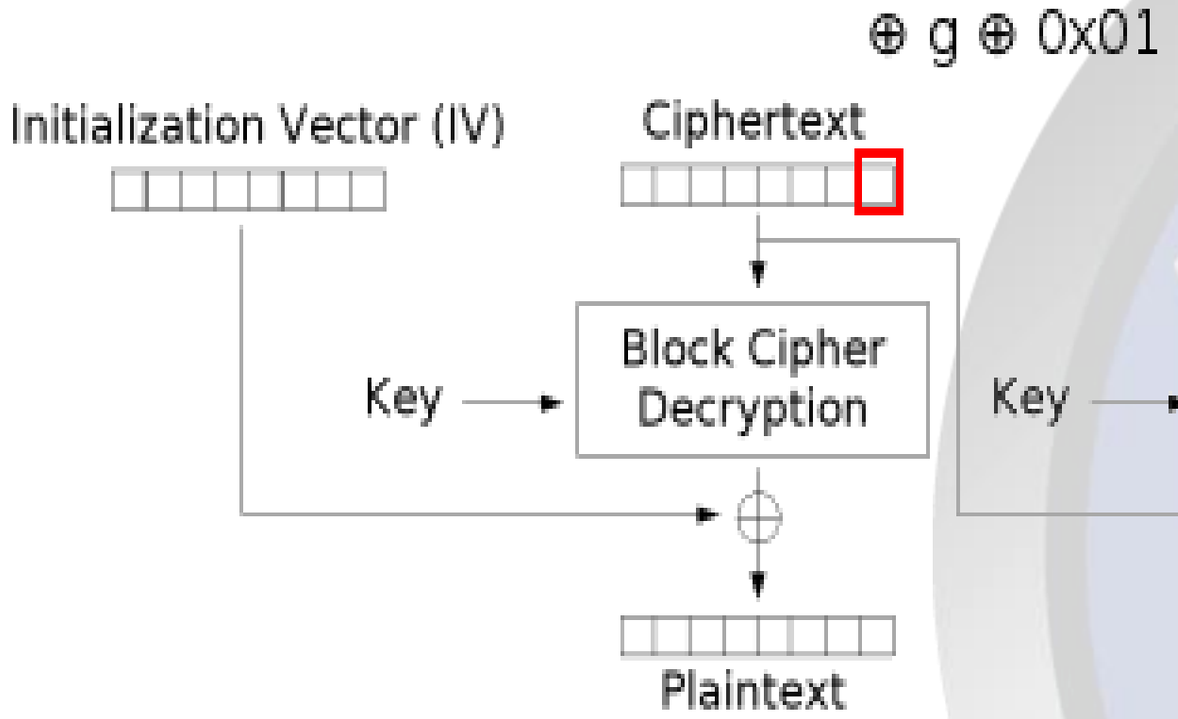
PKCS #5 - Padding

	BLOCK #1								BLOCK #2							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Ex 1	F	I	G													
Ex 1 (Padded)	F	I	G	0x05	0x05	0x05	0x05	0x05								
Ex 2	B	A	N	A	N	A										
Ex 2 (Padded)	B	A	N	A	N	A	0x02	0x02								
Ex 3	A	V	O	C	A	D	O									
Ex 3 (Padded)	A	V	O	C	A	D	O	0x01								
Ex 4	P	L	A	N	T	A	I	N								
Ex 4 (Padded)	P	L	A	N	T	A	I	N	0x08	0x08	0x08	0x08	0x08	0x08	0x08	0x08
Ex 5	P	A	S	S	I	O	N	F	R	U	I	T				
Ex 5 (Padded)	P	A	S	S	I	O	N	F	R	U	I	T	0x04	0x04	0x04	0x04

Fuente: gdssecurity.com

Padding Oracle

Using a CBC padding oracle



si last-byte = g:
=> Valid Pad

de lo contrario:
=> Invalid Padding

= last-byte ⊕ g ⊕ 0x01

Padding Oracle

¿Cómo se explotan estas vulnerabilidades?

- Presencia del oráculo:
- Un poquito más complicado que un loop y un if-then-else.
- Detección del tamaño del bloque.
- Múltiples herramientas para explotar aplicaciones/situaciones específicas.
- Muchísimas aplicaciones esperando que alguien les contruya un exploit.

Padding Oracle

¿Cual es el impacto?

- VIDEOS

Resumen & Conclusiones

Resumen

- Mecanismos de seguridad del lado del cliente.
- Otorgar demasiada información al atacante.
- Esto es sólo el comienzo.

¿ Preguntas ?

- http://latinsec.blogspot.com
- @latinsec
- recabarren@gmail.com