Trucos para jugar con la criptografía en el desarrollo

Lic. Cristian Borghello, CISSP - MVP
www.segu-info.com.ar
info@segu-info.com.ar
@SeguInfo

WWW.SEGU.INFO
SEGURIDAD DE LA INFORMACION

¿Para qué sirve la Criptografía?

- Confidencialidad, guardar un secreto
- Integridad
- Autenticidad
- Disponibilidad… casi nada*

(*) Existe el algoritmo de secreto compartido de Blakely-Shamir

En 1883 **August Kerckhoff** dijo que:

Sólo la clave debe ser secreta

El algoritmo debe ser público

La fortaleza del sistema depende de la clave


¿Y PARA QUE SE PUEDE USAR ESTO?
NO SABEMOS, LO QUE HACEMOS ES INVESTIGACION BASICA
QUE BONITO, NOSOTROS NOS MATAMOS EMPUJANDO PIEDRAS Y ARRASTRANDO ANIMALES SALVAJES, MIENTRAS LOS SEÑORES SE ENTRETIENEN HACIENDO COSAS QUE NO SIRVEN PARA NADA
TROLEK 2011

Algoritmo de Cifrado

- Cifra texto plano usando una/dos clave/s
- Descifra texto cifrado usando las claves

```
e_AES(“OWASP”, clave) → U2FsdGVkX1+8Dk81eLz80gfrHzxDumxhS
d_AES(“U2FsdGVkX1+8Dk81eLz80gfrHzxDumxhS”, clave) → OWASP
```

Algoritmo de Hashing

- Función de una vía
- Genera una cadena de longitud constante a partir de una cadena de longitud variable
- Sin inversa*

```
e_MD5(password) → 5f4dcc3b5aa765d61d8327deb882cf99
d_MD5(5f4dcc3b5aa765d61d8327deb882cf99) → Fuerza Bruta
```

(*) No existe un proceso matemático para obtener la inversa

WHAT
★ the ★
FUCK
IS THIS SHIT

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

NUNCA

Inventar tus propios algoritmos

TECNOLOGÍA | Dice haber creado un sistema de criptografía 'indescifrable'

Un físico reta a los 'hackers'

Generación de números aleatorios

La criptografía está basada en la generación de números aleatorios (PRNG). Una vulnerabilidad en PRNG consiste en utilizar algoritmos de mala calidad y/o predecibles

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Generación de números aleatorios

Precaución

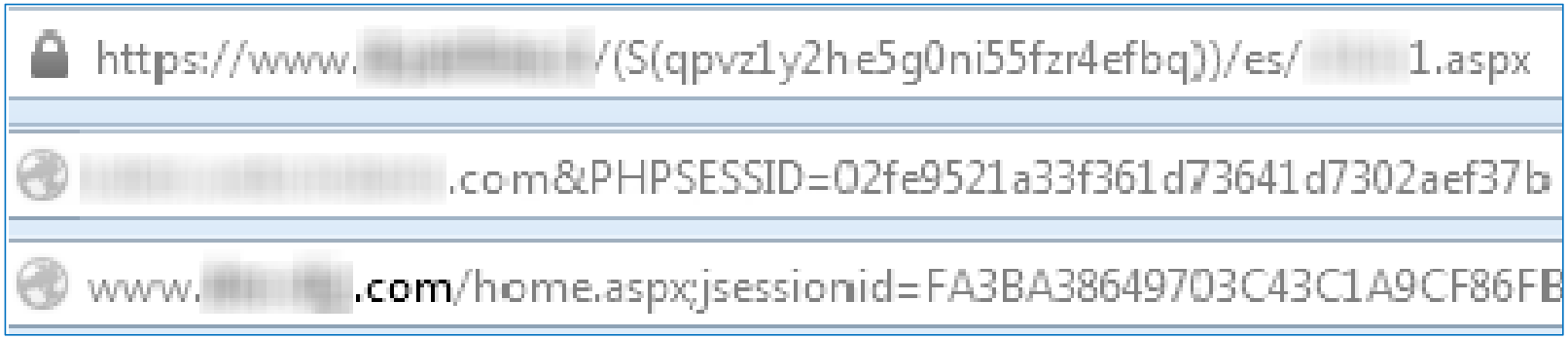
Esta función no genera valores criptográficos fiables por lo que no debería usarse para propósitos criptográficos. Si fuera necesario un valor criptográfico seguro, considérese usar openssl_random_pseudo_bytes() en su lugar.

```
php.rnd()
java.util.Random() (año 2006)
WEP (año 2000)
RC4 en TLS (hace dos semana)
BSDNET (SSH/SSL) (hace una semana)
```

http://php.net/manual/es/function.rand.php
http://php.net/manual/es/function.mt-rand.php
http://en.wikipedia.org/wiki/Random_number_generator_attack
http://blog.segu-info.com.ar/2013/03/ataque-alfbpps-tls-cuanta-vida-le-queda.html
http://blog.segu-info.com.ar/2013/02/ssl-y-tls-en-peligro-lucky-thirteen.html

Sesiones predecibles

- Una *Session_ID* debe tener al menos 128 bits (16 bytes) para evitar que sea predecible
- La sesión **no** debe almacenar información sensible (~~o debe estar cifrada~~) y debe ser almacenada en el servidor
- Utilizar *Session-Less*



Session Prediction

Las aplicaciones vulnerables generan credenciales predecibles

```
Host: http://www.foo.bar
User-Agent: Mozilla/5.0
Cookie: ID=usuario1segu-info
```

```
Host: http://www.foo.bar
User-Agent: Mozilla/5.0
Cookie: ID=usuario2segu-info
```

Se debería generar una sesión no predecible, mediante el uso de *hash* y variables no repetibles (ej. *timestamp*)

```
Host: http://www.foo.bar
User-Agent: Mozilla/5.0
Cookie: ID=2074c519d665f5cf9eb3c52abd97865223f65b70
```

```
SHA1: usuarioXsegu-info20110810120945-ClaveSecreta
```

Redirección abierta

Evitar redirecciones abiertas

- Listas blancas de direcciones permitidas
- Permitir sólo URL locales
- Cifrar la URL destino

```
e_AES(“http://segu.info”, “secreto”) →
        U2FsdGVkX1KGbecRMEplX8

www.test.com/?url=U2FsdGVkX1KGbecRMEplX8
```

Seguridad por oscuridad

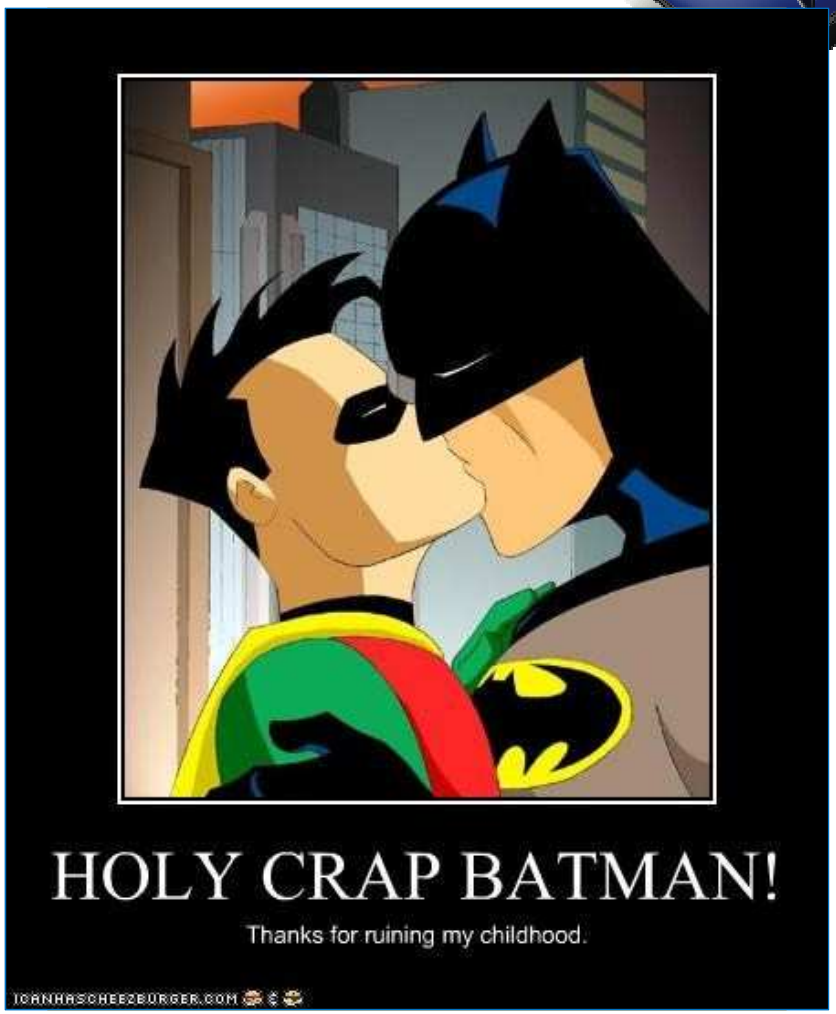
Un sistema ~~puede tener~~ tiene vulnerabilidades pero sus diseñadores creen que, debido al secreto que se mantiene, son muy difíciles de encontrar y hay pocas probabilidades de descubrirlos

¡Han pasado más de 2000 años!

```
########################################
#      [ - Owned and Exposed - ]       #
# Brought to you by the D33Ds Company  #
#                                      #
# Target: <censored>.yahoo.com         #
```

```
000001e471fb782ebaeb9f3f1160cc5f1beba90d
000001e4d1e7329207f085bf782a88830a0b8f55
000001e428686e60caab8f44cc9307cd279273c9
000001e459b5ea677576f9f26dc97f4dabbf9f6e
000001e4043adc807345dcf220110d1662925c76
000001e40cf723b9393d301ad524c7b682fa7604
000001e4c9b93f3f0682250b6cf8331b7ee68fd8
000001e41112b96f0c14bd8fcec238f37fbd5f91
000001e40e9fc0ae5e1b5749b7fed8ecf6f41930
000001e47b41f184c708c24c174bbaba40fe9efc
000001e45e683a5887a4d916a822c389aafd4d3c
000001e4e03d1752f522d0aa58c455a6e88cd645
000001e454544bb1d9ee938c25f7fa2ec7356361
```

```
14:timarms[redacted]@gmail.com:tagoogle
16:curran[redacted]il.com:giants
17:tckirk([redacted].com:chapman
```



SHA1("password") → 5baa6**1e4c9b93f3f0682250b6cf8331b7ee68fd8**

HMAC

- **HMAC (Hash-based Message Authentication Code):** generar un valor (MAC) en base a un Hash cifrado con una clave secreta (conocida como **Salt**)
- Utilizado para verificar la integridad (*hash*) y autenticidad (cifrado) del mensaje

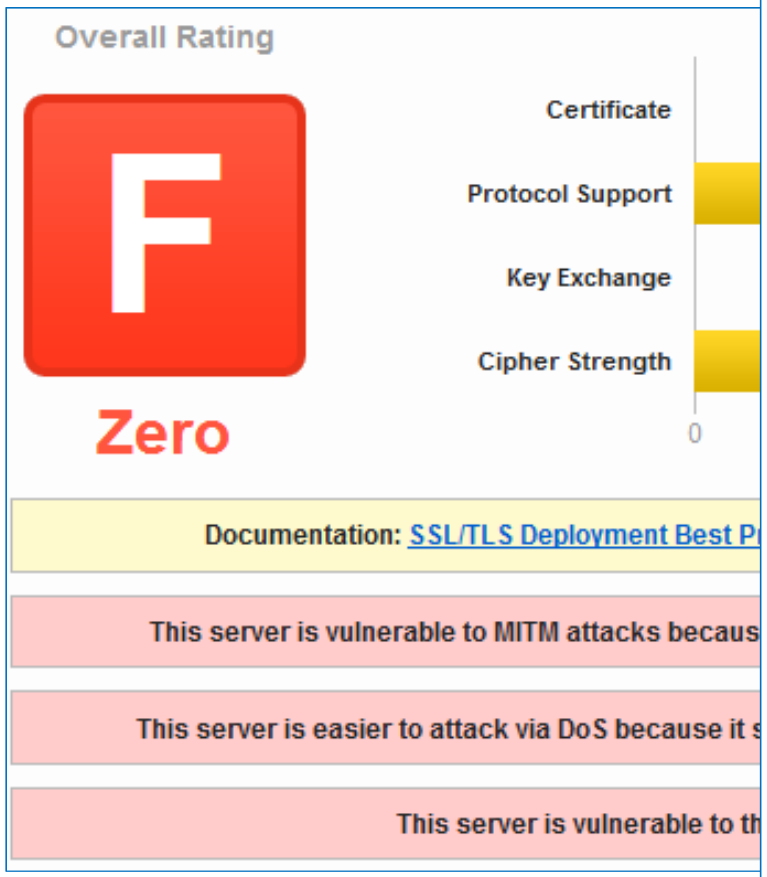
Mensaje	MD5	SHA1
password	5f4dcc3b5aa765d61d8327deb882cf99	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

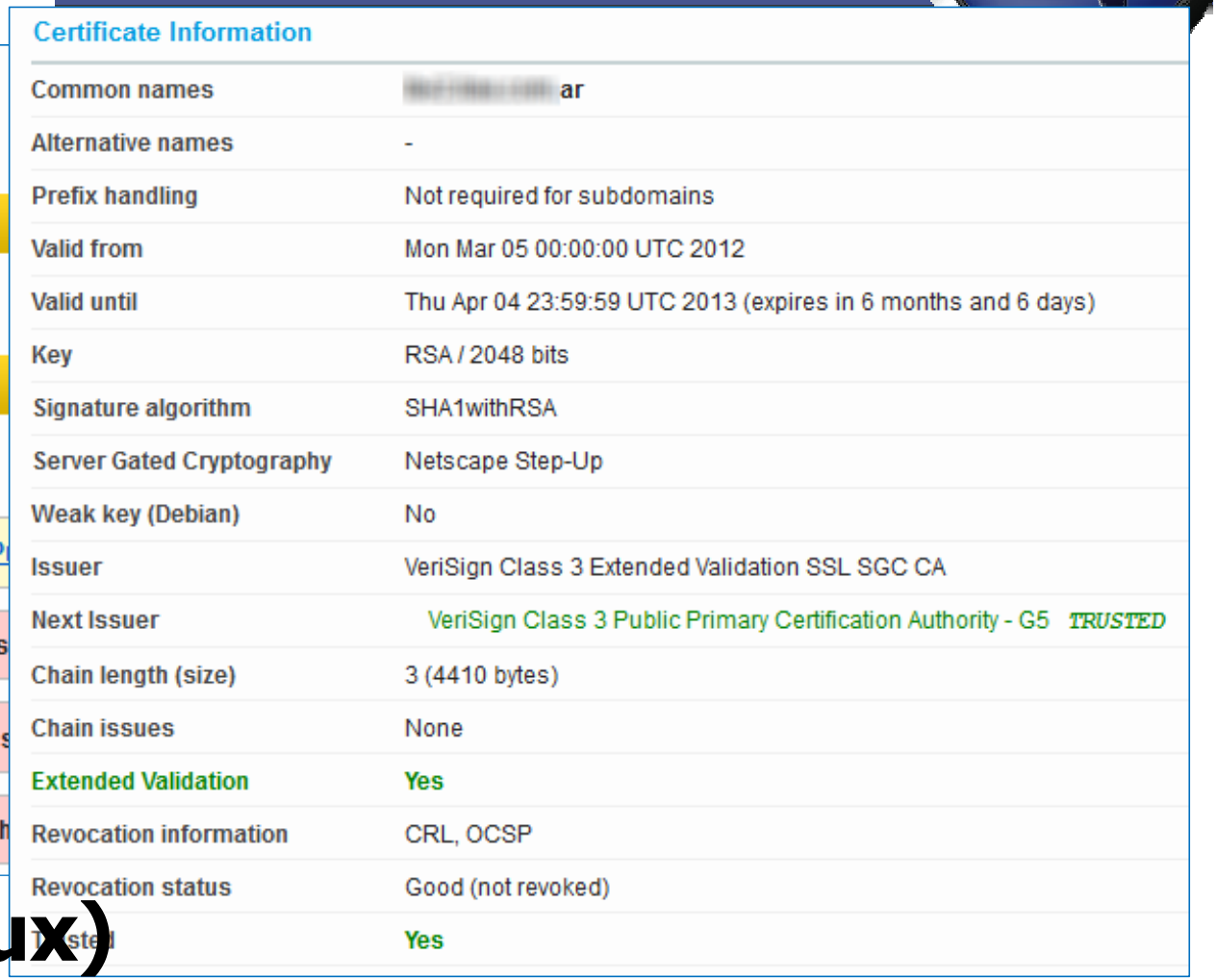
Mensaje	HMAC-MD5	HMAC-SHA1	SALT
password	5f4dcc3b5aa765d61d8327deb882cf99	**7DB5EEFE8BD10447855265E8EACB6F0BFDC59CFC**	rnd(1)
password	45f29dcc3d4aa7785d61d5323adf82c5	**34FD02E4C516DE4760BACDB86FDDBC1DBC22B524**	rnd(2)

Protección insuficiente en la capa de transporte

- La aplicación no utiliza SSL para las páginas que requieren autenticación o transmisión de datos sensibles
- Se transmiten *cookies* por canales inseguros
- Se utilizan protocolos no seguros o débiles
- La aplicación utiliza un certificado SSL configurado incorrectamente, vencido o revocado. Al mostrarse la advertencia los usuarios la ignoran

Análisis de certificados





Certificate Information	
Common names	[redacted]ar
Alternative names	-
Prefix handling	Not required for subdomains
Valid from	Mon Mar 05 00:00:00 UTC 2012
Valid until	Thu Apr 04 23:59:59 UTC 2013 (expires in 6 months and 6 days)
Key	RSA / 2048 bits
Signature algorithm	SHA1withRSA
Server Gated Cryptography	Netscape Step-Up
Weak key (Debian)	No
Issuer	VeriSign Class 3 Extended Validation SSL SGC CA
Next Issuer	VeriSign Class 3 Public Primary Certification Authority - G5 *TRUSTED*
Chain length (size)	3 (4410 bytes)
Chain issues	None
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
[illegible]	Yes

Herramientas (Linux)

```
sslyze.py --tlsv1 mail.google.com
sslscan --no-failed mail.google.com
testssl.sh -a mail.google.com
openssl s_client -no_tls1 -connect www.google.com:443
```

https://www.ssllabs.com/ssltest/analyze.html

https://www.owasp.org/index.php/Testing_for_SSL-TLS_%28OWASP-CM-001%29

Esta conexión no es de confianza

Ha solicitado a Firefox que conecte de forma segura a **www1.masterconsultas.com.ar**, pero no podemos confirmar que su conexión sea segura.

Normalmente, cuando se trata de conectar de forma segura, los sitios presentan un identificación confiable para probar que está dirigiéndose al lugar correcto. Sin embargo, la identidad de este sitio no puede verificarse.

¿Qué debería hacer?

Si usualmente se conecta a este sitio sin problemas, este error podría significar que alguien está tratando de imitar ese sitio y no debería continuar.

¡Sáquenme de aquí!

Detalles técnicos

Un error ocurrió durante una conexión a www1.masterconsultas.com.ar porque usa un certificado de seguridad no válido.

El certificado ha expirado el 04/03/2013 08:59 p.m.. La fecha actual es 08/03/2013 05:19 p.n

(Código de error: sec_error_expired_certificate)

Comprendo los riesgos

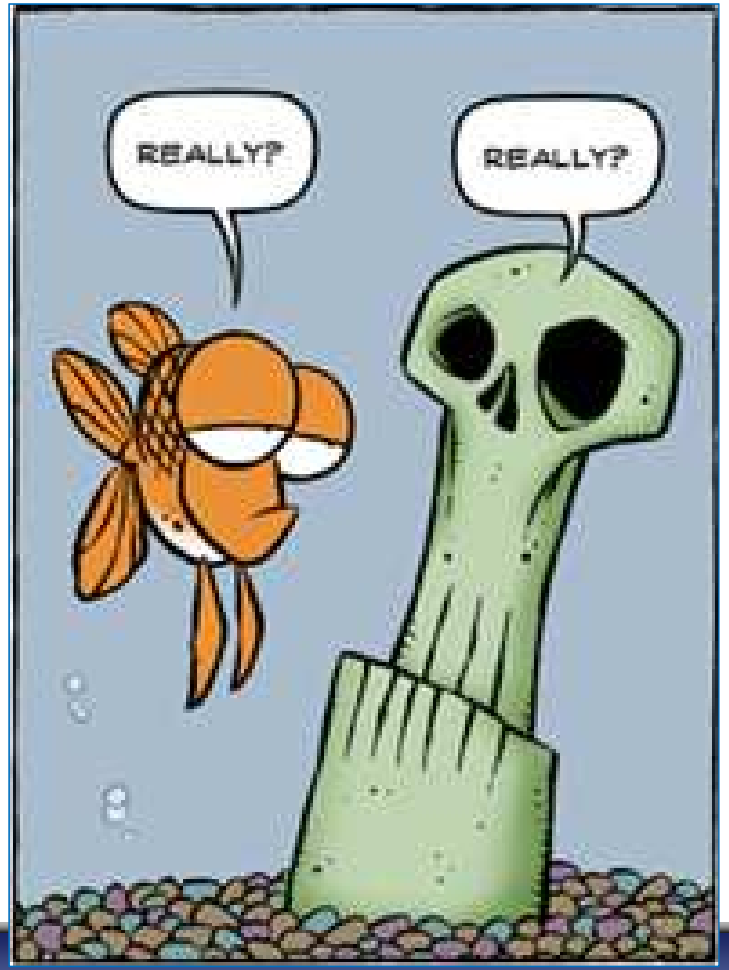
Recomendaciones

1. Cifrar datos sensibles (en almacenamiento, tráfico y backups)
2. NO Usar algoritmos propios (seguridad por oscuridad) No cree sus propios algoritmos
3. NO utilizar algoritmos antiguos o con probadas vulnerabilidades (ej. MD5)
4. NO al *Hardcoding* de claves en el código fuente o almacenar las claves en forma insegura
5. Sólo almacenar la información necesaria

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Recomendaciones

6. NO almacenar las claves en texto plano
7. NO Utilizar cifrado de dos vías en contraseñas (utilice *Hashing + Salt / HMAC*)



Tenias que hacer una cosa…

Lic. Cristian Borghello, CISSP - MVP
www.segu-info.com.ar
info@segu-info.com.ar
@SeguInfo