





OWASP

The Open Web Application Security Project

Gastón Toth

- Licenciado en Computación
- Certified Ethical Hacker
- CISSP
- Pentester
- OWASP Patagonia Chapter Leader



gaston.toth@owasp.org



[@OWASP_Patagonia](https://twitter.com/OWASP_Patagonia)



OWASP

The Open Web Application Security Project

WEBAPP LITTLE MISTAKES...

...BIG PROBLEMS!!!



OWASP

The Open Web Application Security Project

¿Por qué esta charla?

- Porque OWASP tiene que ver con aplicaciones web, no?
- Porque cada vez mas organizaciones exponen sus servicios a través de portales web
- Para concientizar y no subestimar ninguna falla por mas pequeña que parezca



OWASP

The Open Web Application Security Project

¿Por qué el nombre de esta charla?

“Pequeños” problemas pueden dar lugar al compromiso de un sistema grande.



OWASP

The Open Web Application Security Project

No se debe dejar afuera ningún aspecto

- Capacitación a usuarios (muuuy importante)
- Diseño y desarrollo seguro
- Mantener los sistemas actualizados
- Asistir a las charlas de OWASP => esto es lo más importante :)



OWASP

The Open Web Application Security Project

Algunos comentarios que me ha tocado escuchar...

“...El tema de la seguridad es algo simple, total corrés un script y listo...”

“...nosotros focalizamos nuestra energía en un login seguro...”

“...ese es un sistema de pruebas, no importa la seguridad...”

“...a quien le va a interesar meterse en nuestra página?”



OWASP

The Open Web Application Security Project

Bueno, muchas palabras...
veamos algunos ejemplos de sitios reales



OWASP

The Open Web Application Security Project

Sitio web para reservas de hotel

← ⓘ http://[REDACTED] ↻ 🚚 🌐 🔍 Buscar ☆ 📅 ⬇️ 🏠 📍 »

Forma de Pago 💰

Tarjeta:	Número	Vencimiento		Cod Seg
<input checked="" type="radio"/> <input type="text" value="VISA"/>	<input type="text"/>	<input type="text" value="mm"/>	<input type="text" value="/ aa"/>	<input type="text"/>

Seleccione su Tarjeta de Crédito.

primer síntoma: no se usa HTTPS



OWASP

The Open Web Application Security Project

Segundo y casi definitivo síntoma:

```
ERROR [REDACTED][MySQL][ODBC 5.1 Driver]  
[mysqld-5.6.17-log]You have an error in  
your SQL syntax; check the manual that  
corresponds to your MySQL server
```

Inyección SQL



OWASP

The Open Web Application Security Project

Y ya que estamos...

A screenshot of a web browser window showing a login form. The address bar at the top displays 'http://www.' followed by a blurred URL. The login form itself has a white background and contains the following elements: a label 'Nombre de Usuario:' followed by a red person icon and a text input field; a label 'Contraseña:' followed by a yellow padlock icon and a yellow text input field; a checkbox labeled 'Recordar Usuario.' which is checked; and two buttons at the bottom, 'Aceptar' and 'Cancelar', both with a grey gradient.

... acceso al portal de administración de reservas (sin https y con inyección SQL)



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

En el sitio del desarrollador...

Seguro

Moderno

Simple

Eficiente

Tu sitio de reservas online

- * Seguro
- * Moderno
- * Simple
- * Eficiente





OWASP

The Open Web Application Security Project

Y el problema no afecta sólo a un hotel

HOME

EMPRESA

PRODUCTOS

CLIENTES

CONTACTO

...varios clientes → muchas reservas → muchos números de tarjeta!!!





OWASP

The Open Web Application Security Project

Otro ejemplo...

Banca electrónica

... pero acá estas cosas no creo que pasen ¿o si?



OWASP

The Open Web Application Security Project

Login seguro con utilización de tokens



Utilización de Viewstate MAC



Elegir la cuenta bancaria por parámetro

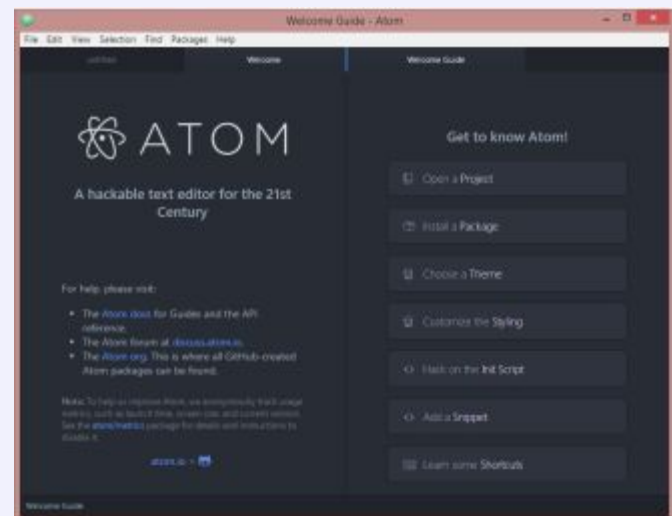
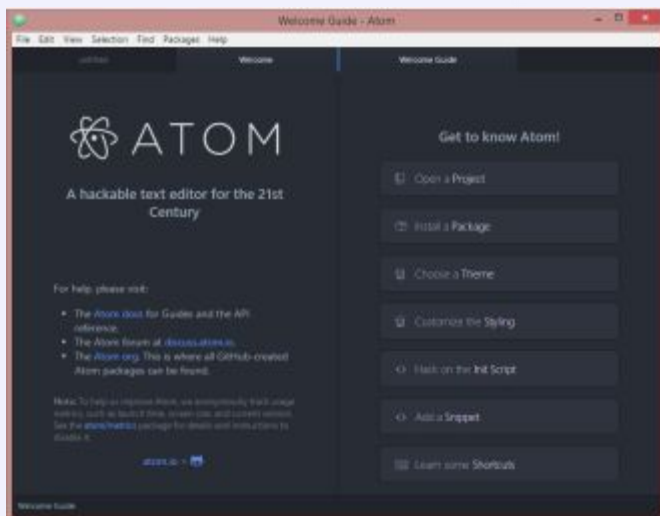
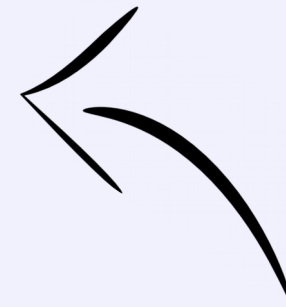




OWASP

The Open Web Application Security Project

Github + AtomConfig





OWASP

The Open Web Application Security Project

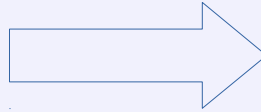
Sitio de compras



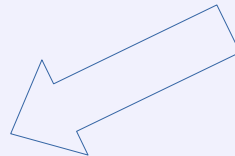
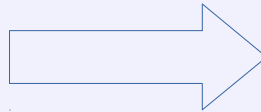
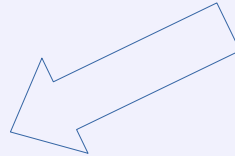
Sitio de compras (cont.)



Encontramos una forma de subir una webshell



No lo consideramos grave porque es todo solo lectura, menos ese directorio en particular, que es para eso.





OWASP

The Open Web Application Security Project

Sitio de compras (cont.)

Para comprobar que sí era de alto impacto se armó un script que simulaba el proceso de pago copiando el código fuente original (usando claves y datos originales). Y se realizaron transacciones (compras) válidas salteando la etapa del pago.



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

Demo...

www.empresa.com