



# CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

# 2<sup>do</sup> Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09  
2021

011011 10000  
100010110 0

0 0

1

00001  
00 10 1  
10100  
000 0  
11010 1

10110 1  
0 0001

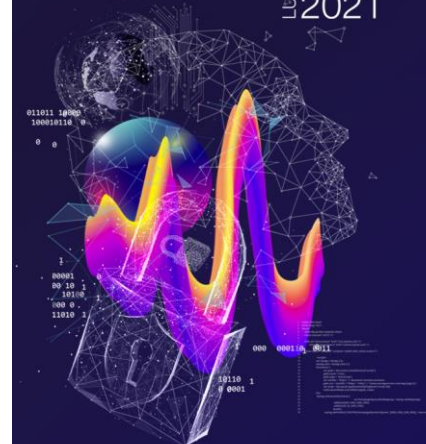
000 000110 0011

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>perfect solution</title>
5 <meta charset="utf-8" />
6 <link rel="stylesheet" href="css/mysite.com"/>
7 <div id="connect" href="http://www.mysite.com"/>
8 </div>
9 </head>
10 <body>
11 <div id="connect" content="width:60, initial scale:1">
12
13 <script>
14 var mytag = mytag || {};
15 mytag.cmd = mytag.cmd || [];
16 (function() {
17   var gads = document.createElement("script");
18   gads.async = true;
19   gads.src = "http://";
20   gads.src = (isSSL? "https": "http") + "://www.mytag.com/tag.js?pt=2";
21   var node = document.getElementsByTagName("script")[0];
22   node.parentNode.insertBefore(gads, node);
23
24   mytag.cmd.push(function() {
25     var homepageSquareSizeMapping = mytag.sizeMapping();
26     addSize(195, 290, [200, 200]);
27     addSize(0, 0, [200, 290]);
28     build();
29     mytag.defineSize("1023782/homepageDynamicSquare", [200, 290, [200, 200], "reserved-div 1");
30

```

# Seguridad en sitios web (introducción teórica)



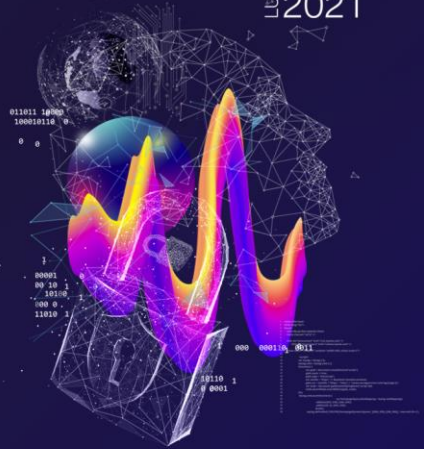
TÉRMINO	EXPLICACIÓN
Amenaza	Un peligro potencial de un activo, como los datos o la red.
Vulnerabilidad	Una debilidad o falla en un sistema o en su diseño que podría ser aprovechada por una amenaza.
Incidente	Uno o varios eventos que ocurren de forma inesperada y/o no deseada, que pueden afectar el normal funcionamiento de una organización, debido a la pérdida, modificación o uso indebido de información o recurso afectando la triada de seguridad.
Impacto	El daño potencial que puede causar una amenaza si logra afectar a la organización.
Riesgo	Probabilidad x Impacto

# ¿Qué es la seguridad web?

- Es una rama de la seguridad informática que se encarga específicamente de la seguridad de sitios web, aplicaciones web y servicios web.
- Es la práctica de proteger sitios web del acceso, uso, modificación, destrucción o interrupción no autorizados
- La seguridad de las aplicaciones web es fundamental para proteger los datos, los clientes y las organizaciones del robo de datos, las interrupciones en la continuidad de los negocios u otras consecuencias perjudiciales del delito cibernético.
- Además, se puede ver amenazada la seguridad de la infraestructura a través de un ataque a un sitio web.

2<sup>do</sup> Seminario de  
Ciberseguridad  
para funcionarios  
públicos

LUNES 23/09  
2021



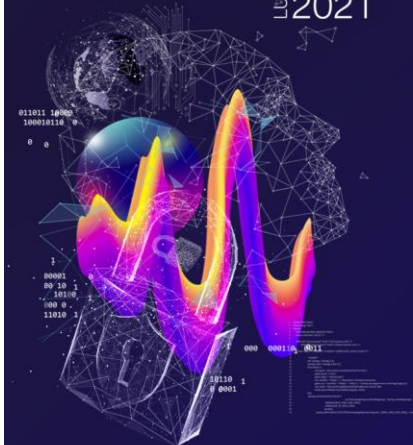
# ¿Por qué es importante la seguridad web?

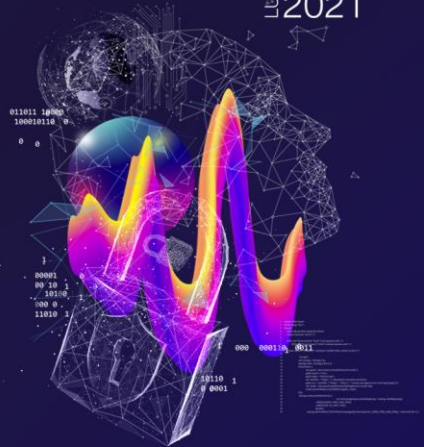
Hoy por hoy gran parte de nuestro día a día gira en torno a aplicaciones. De ver películas a organizar nuestra vida laboral, pedir comida a la casa o usar el banco.

Cuando algo se vuelve popular y en muchos casos imprescindible, se transforma al mismo tiempo en un imán para los delincuentes, que se aprovechan de las fallas de diseño y vulnerabilidades en las API y las widgets, el código abierto y los controles de acceso, entre otras, para acceder a nuestra información confidencial, secuestrar nuestros datos, robarnos, extorsionarnos, o aún peor.

Ataques comunes contra las aplicaciones web incluyen:

- Fuerza bruta
- Inyección SQL
- Cross-site scripting
- Envenenamiento de cookies
- Ataques del tipo «Man in the middle» (MITM) y del tipo «Man in the browser» (MITB)
- Divulgación de datos confidenciales
- Secuestro de sesión

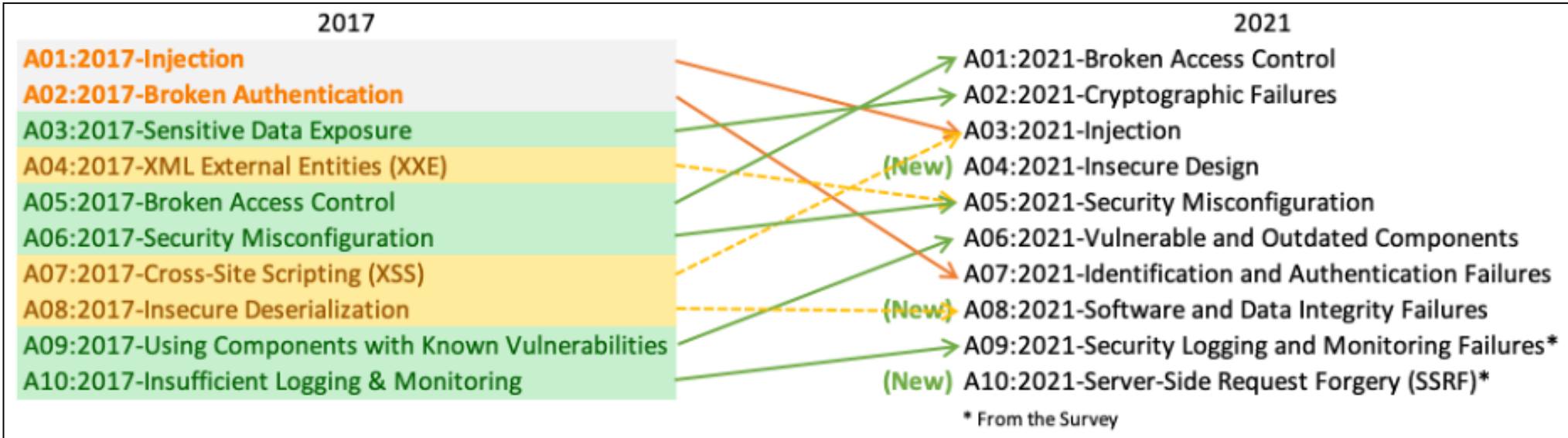
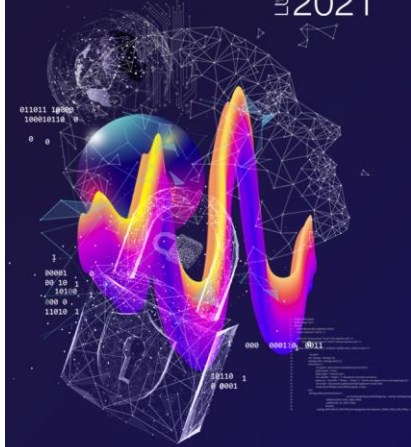


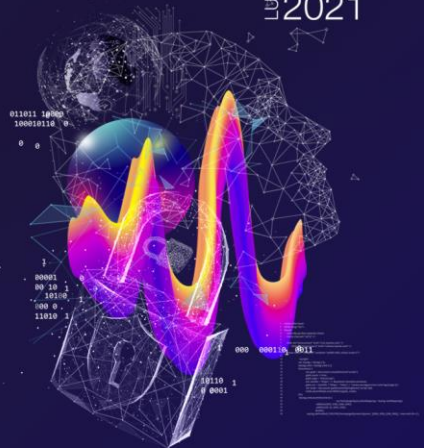


# Estándares de clasificación y valoración de vulnerabilidades

- OWASP (Open Web Application Security Project, en inglés ‘Proyecto abierto de seguridad de aplicaciones web’) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- CVE (Common Vulnerabilities and Exposures, “Vulnerabilidades y exposiciones comunes”): La misión del Programa CVE es identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente.
- CWE (Common Weakness Enumeration, “Enumeración de debilidades comunes”) es una lista de tipos comunes de debilidades de software y hardware que tienen ramificaciones de seguridad.

# OWASP TOP 10





# Herramientas por fases

## Reconocimiento:

- WHOIS
- Dig
- dnsrecon
- Nslookup
- Buscadores
- RRSS
- Shodan
- Foca
- theHarvester
- Maltego
- Recon-ng
- **Whatweb**
- **Amass**
- nmap
- Test SSL
- **Sublist3r**
- **Wpscan**
- JoomScan

## Mapeo de la Aplicación Web:

- Fuzzing
- Information Leak
- **ZAP**
- Burp Suite
- Dirbuster
- **Dirsearch**

## Análisis de Vulnerabilidades:

- **Nikto**
- **ZAP**
- Burp Suite
- Hydra
- XSSer
- XSScrapy
- xssniper

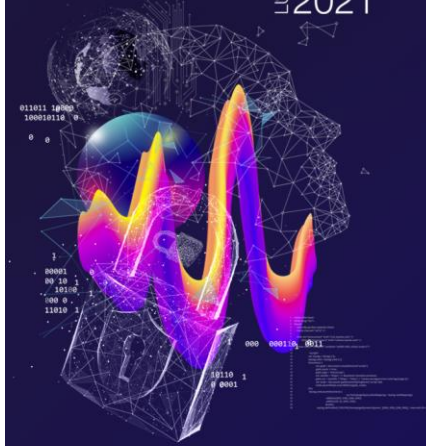
## Explotar Vulnerabilidades:

- Sqlmap
- BeEF
- W3af



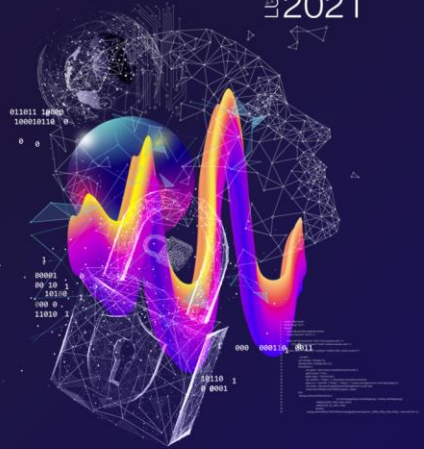
# Recomendaciones.

- Almacena y muestra sólo los datos que sea necesario.
- Usar soluciones de cifrado actualizadas.
- Solicitar una autenticación adecuada.
- Considerar la autenticación de dos factores.
- Ejecutar parches para solucionar vulnerabilidades.
- Contar con soluciones eficaces de desarrollo de software.
- Usar una gestión de contraseñas fomentando las contraseñas fuertes y que se cambien con regularidad.
- Desinfectar todos los datos originados por el usuario antes de ser mostrados en el explorador.
- Configurar tu servidor web para usar HTTPS y HTTP Strict Transport Security (HSTS).
- Usar herramientas de escaneo de vulnerabilidades para realizar pruebas automáticas de seguridad en tu sitio y pruebas manuales.



2<sup>do</sup> Seminario de  
Ciberseguridad  
para funcionarios  
públicos

LUNES 23/09  
2021



# Recomendaciones.

Se puede mejorar la seguridad de las aplicaciones web implementando soluciones de protección contra ataques DDoS, a la capa de aplicación y al DNS:

- WAF
- Mitigación DDoS
- Seguridad DNS
- MFA
- Cookies

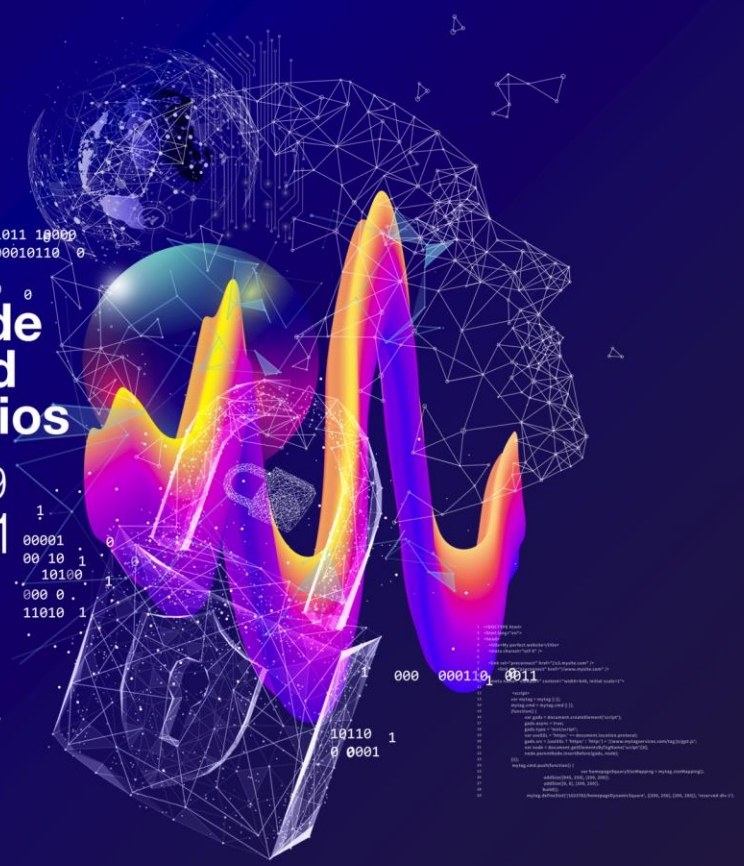
# 2<sup>do</sup> Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09  
2021

011011 10000  
100010110 0

1  
00001  
00 10 1  
10100  
000 0  
11010 1

10110 1  
0 0001



CSIRT  
<https://www.csirt.gob.cl/>

Teatinos 92 piso 6  
Santiago, Chile