



HTTP DATA INTEGRITY VALIDATOR

Garantiza la seguridad de tus aplicaciones web



El 95% de las aplicaciones web son vulnerables

Según el 75% de los ataques realizados en la actualidad se realizan en las aplicaciones web, debido a la mejora de la seguridad a nivel red y sistemas operativos. En consecuencia, se considera que el 95% de las aplicaciones web son **vulnerables** a algún tipo de ataque:

- > Cross-Site Scripting (80%).
- > SQL Injection (62%).
- > Parameter- Tampering (60%).

HDIV garantiza la seguridad de las aplicaciones web

Gran parte de las vulnerabilidades de nivel aplicación **pueden ser solucionadas con una correcta programación** de las aplicaciones web.

Para ello es necesario securizar cada una de las peticiones que se realiza contra las aplicaciones realizando una correcta validación de entrada.

Teniendo en cuenta que dentro de una aplicación pueden existir cientos de tipos de peticiones, el margen de riesgo existente es extremadamente alto.

Por ello se requiere utilizar soluciones software adecuadas, como **HDIV**, que solucionen de forma automática las necesidades de seguridad, eliminando el margen de error humano que existe en todas las aplicaciones.

Transparente al programador

HDIV securiza las aplicaciones web de forma transparente al programador. Gracias a que se trata de una **extensión de los principales frameworks web**, concretamente **Struts 1, Struts 2, Spring MVC y JSF**, que respeta todos los interfaces definidos por los mismos, no es necesario modificar el código fuente de las aplicaciones, siendo aplicable de forma declarativa vía configuración. Esta propiedad es especialmente importante para aquellas aplicaciones previamente desarrolladas y que requieran de un sistema que garantice su seguridad.

HDIV extiende el comportamiento de los principales frameworks web modificando parte del HTML generado por la aplicación para posteriormente poder validar las peticiones enviadas por el cliente.

Registro de ataques

HDIV genera **logs** con los ataques contra las aplicaciones posibilitando conocer el nivel de riesgo de las mismas incluyendo la petición, la IP, el tipo de ataque e incluso la identidad del usuario de aplicación que ha realizado el ataque en aquellas zonas en las que se exige autenticación.

```
[type of attack]; [action]; [parameter]; [value]; [userLocalIP]; [IP]; [userId]
```

