SQL Injection y archivo peligroso en Demokratian

mar 05 mayo 2020 ofensiva #auditar software sqli demokratian

Demokratian es una aplicación web para realizar votaciones de forma sencilla y segura. Es software libre y puede ser utilizada sin mucho nivel técnico. Está escrita en PHP y que utiliza una base de datos MySQL.

Por casualidades encontré el software demokratian en unas votaciones en las que participé. Al participar me entró la curiosidad y realizando algunas pruebas encontré estas 2 vulnerabildades.

Hay que decir que el desarrollador, al contactar con el, arreglo el bug bastante rápido.

Info del Software

- Nombre: Demokratian
- Repositorio: https://bitbucket.org/csalgadow/demokratian_votaciones
- Web: http://demokratian.org/

Vulnerabilidades

Bien, aquí están dos los vulnerabilidades que encontré y que fueron reportadas y solucionadas por el desarrollador Carlos Salgado.

SQL Injection

- URL: basicos_php/genera_select.php
- Parametro: id_provincia
- Método: GET
- Autenticación: No requerido.
- Modo: Remoto
- POC: http://example.com/basicos_php/genera_select.php?id_provincia=-1%20union%20all%20select%201,2,3,4,database()
- Parche: https://bitbucket.org/csalgadow/demokratian_votaciones/commits/b56c48b519fc52efa65404c312ea9bbde320e3fa

Como podemos ver la vulnerabilidad es bastante grave. Ya que es posible descargar los datos de los votantes. La vulnerabilidad tiene parche y es posible aplicarlo descargando la versión master o aplicando la siguiente modificación en el código:

basicos_php/genera_select.php

```
#$id_provincia = fn_filtro($con, $_GET['id_provincia']);
$id_provincia = fn_filtro_numerico($con, $_GET['id_provincia']);
```

Broken Authentication

- URL: install/install3.php
- Autenticación: No requerido.
- Modo: Remoto
- POC: http://example.com/install/install3.php
- Parche: https://bitbucket.org/csalgadow/demokratian_votaciones/commits/0d073ee461edd5f42528d41e00bf0a7b22e86bb3

Esta vulnerabilidad se debe a que los administradores de sistemas se dejan el fichero después de la instalación y es posible hacer un usuario con rol de administrador de forma transparente y ganando control total sobre la aplicación. En las nuevas versiones este fichero es borrado una vez se ha instalada la aplicación.