



**Tecnológico  
de Monterrey**

## **Informe de Recomendaciones de las Pruebas de Penetración (PENTEST)**

**Informe Preliminar de las pruebas de Penetración a la  
Infraestructura Tecnológica del Programa Resultados Electorales  
Preliminares (PREP) del IEE Sinaloa**

### **Descripción breve**

Este documento describe los resultados preliminares de las pruebas de penetración (PENTEST) que se ejecutará al sistema del PREP

**Roberto Luis Iriarte / Raime Alejandro Bustos**

roberto@iriarte.net

raime.bustos@tec.mx

**Jesús R. González / Juan Arturo Nolazco**

jrgonza@gmail.com

jnolazco@itesm.mx

### Índice

1 Resumen Ejecutivo	2
2 Alcance	3
3 Resultado de las pruebas	4
4 Recomendaciones Generales	5

Versión	Fecha	Descripción
1.0		Reporte inicial de resultados del plan de Penetración (PENTEST) de la infraestructura tecnológica del sistema de información preliminar de resultados electorales (PREP) del <b>IEE Sinaloa</b>
1.1	16/May/2021	Revisión general

Dictamen elaborado por:

MSc. Jesús Raúl González Hernández en coordinación con el Dr. Juan Arturo Nolasco, Ing. Roberto Luis Iriarte Pablos y MSE Raime Alejandro Bustos Gardea.

### 1 Resumen Ejecutivo

En base a las pruebas realizadas en el plan de pruebas de penetración de infraestructura tecnológica del PREP del **IEE Sinaloa**, se encuentran detalladas en la siguiente tabla de resumen ejecutivo:

Vulnerabilidad (CVSS)	Explotable (SI/NO)	¿Explotación exitosa?	Servidor / URL afectada	Comentario
CVE-2014-0226	SI <sup>1</sup>	No	prepsinaloa.info 10.3.0.224 10.3.0.222	Se recomienda actualizar la versión del Apache Web Server a la última disponible por el fabricante
CVE-2021-31618	SI <sup>2</sup>	No	prepsinaloa.info 10.3.0.224 10.3.0.222	Se recomienda actualizar la versión del Apache Web Server a la última disponible por el fabricante. Vulnerabilidad publicada el 3 de junio del 2021
CVE-2014-0231	No		prepsinaloa.info 10.3.0.224 10.3.0.222	Escáner no reportó exploits disponibles
CVE-2016-8743	No		prepsinaloa.info 10.3.0.224 10.3.0.222	Escáner no reportó exploits disponibles
CVE-2017-3169	No		prepsinaloa.info 10.3.0.224 10.3.0.222	Escáner no reportó exploits disponibles
CVE-2019-0217	No		prepsinaloa.info 10.3.0.224 10.3.0.222	Escáner no reportó exploits disponibles
CVE2016-0734	No		prepsinaloa.info 10.3.0.224 10.3.0.222	Escáner no reportó exploits disponibles

El detalle de pruebas así como el escenario bajo el cual se realizaron los escaneos, se encuentra detallado en el plan de pruebas de penetración (PENTEST).

<sup>1</sup> <https://www.cvedetails.com/cve/CVE-2014-0226/>

<sup>2</sup> <https://www.cybersecurity-help.cz/vdb/SB2021060320>

## 2 Alcance

El alcance de las pruebas de penetración contempla la siguiente lista de activos de la infraestructura tecnológica del PREP de la **IEE Sinaloa**.

Activo (IP)	Servicios
prepsinaloa.info	PREP Sinaloa
10.3.0.224	webserver PREP
10.3.0.221	Base de datos MySQL
10.3.0.222	Web Server interno Central PREP

A estos activos se les encontró las siguientes vulnerabilidades que de acuerdo a su clasificación CVSS son potencialmente explotables.

Vulnerabilidad (CVSS)	Descripción	Explotable (SI/NO)
CVE-2014-0231	mod_cgid denial of service	No
CVE-2016-8743	important: Apache HTTP Request Parsing Whitespace Defects	No
CVE-2017-3169	important: mod_ssl Null Pointer Dereference	No
CVE-2019-0217	important: mod_auth_digest access control bypass	No
	TLS Version 1.0 Protocol Detection	No
CVE2016-0734	Web Application Potentially Vulnerable to Clickjacking	No
CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server	Si
CVE-2021-31618	The vulnerability exists due to a NULL pointer dereference error in mod_http2 in Apache HTTP server	Si

### 3 Resultado de las pruebas

El resultado que se da de las pruebas que se tuvo en cada uno de los escenarios descritos en el plan de pruebas de penetración a la infraestructura tecnológica del **IEE Sinaloa** se describe en esta sección.

En el caso de la vulnerabilidad alta, se revisó la arquitectura y se evaluó que dado los elementos de mitigación que tienen con WAF de Cloudflare cuentan con protección para este tipo de ataques.

### 4 Recomendaciones Generales

Las recomendaciones que se hacen sobre los hallazgos que se hicieron en las pruebas de penetración a la infraestructura tecnológica del **IEE Sinaloa**:

En los servidores de PREP Sinaloa se utiliza Apache Web Server v2.4.6, del cual presenta 42 vulnerabilidades<sup>3</sup>, de las cuales 6 se consideran como importantes. Se recomienda actualizar el servicio a la última versión disponible por por The Apache Software Foundation, Apache Web Server v2.4.48

Deshabilitar en los web servers los protocolos inseguros TLS 1.0 y 1.1 ya que el primero es vulnerable y el segundo ya no es soportado.

Evitar accesos a los servidores con la cuenta de administrador root, primero realizar el login con cuenta personalizada y, si se requiere, ya hacerse root dentro del servidor.

Instalar el parche<sup>4</sup> para el módulo openssl del sistema operativo CentOS 7.9.2009

---

<sup>3</sup> [https://httpd.apache.org/security/vulnerabilities\\_24.html](https://httpd.apache.org/security/vulnerabilities_24.html)

<sup>4</sup> <https://www.cybersecurity-help.cz/vdb/SB2020122214>