

Auditoría de infraestructura en nube del Programa de Resultados Preliminares Electorales

Elección 2018, gobernador, diputaciones locales y ayuntamientos



Facultad de Estudios Superiores
Acatlán

Junio de 2018

Contenido

Control de Versiones	2
Definiciones.....	3
Antecedentes	5
Objetivo.....	5
Alcance	5
Conclusiones	6
Reporte técnico de hallazgos	7
Vectores de Ataque	8
Red Interna.....	8
Aplicativos Web.....	8
Recomendaciones	9
Desarrollo del servicio.....	10
Anexo A. Puertos y servicios	19
Anexo B. Marco metodológico y mejores prácticas.....	20
Herramientas utilizadas	20

Control de Versiones

Nombre del proyecto

Versión	Descripción
1.0	Resultado de las pruebas de penetración a la estructura tecnológica del PREP del Instituto Electoral y de Participación Ciudadana de Tabasco

Elaborado por

Responsable	Fecha de elaboración
Lic. Fernando I González Trejo Lic. Daniel Cordero Vazquez	20 de junio de 2018

Definiciones

Para facilitar la lectura y comprensión de este documento, se consideran las siguientes definiciones:

<i>Término</i>	<i>Definición</i>
Activo	Cualquier recurso de cómputo, ya sea físico o digital que pueda considerarse como crítico para la continuidad del negocio.
Amenaza	Es una causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.
Análisis de vulnerabilidades (AV)	Un análisis de vulnerabilidades tiene como objetivo identificar y medir el riesgo de las vulnerabilidades existentes en los activos evaluados, así como aquellas prácticas inseguras de configuración que pudiera afectar la integridad, disponibilidad o confidencialidad de la información.
Ataque	Acción de tratar de traspasar los controles de seguridad en un sistema de información.
Control de seguridad en la información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
CVSS	Por sus siglas en inglés de Common Vulnerability Scoring System es la norma que proporciona una manera de captar las principales características de una vulnerabilidad y producir una puntuación numérica cualitativa (baja, media, alta y crítica) que refleje su gravedad para ayudar a las organizaciones a evaluar y priorizar las vulnerabilidades de los activos de la institución.
DoS	(Denial of Service). Es una práctica de ataque de red o a sistemas que busca que el recurso o el servicio provisto sea inaccesible, consiste en la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
Falso positivo	Cuando se detecta una vulnerabilidad inexistente.
Falso negativo	Cuando no se detecta una vulnerabilidad existente.
FES Acatlán	Facultad de Estudios Superiores Acatlán.
Hackeo ético	Son técnicas que permiten identificar vulnerabilidades en los sistemas, analizar el nivel de seguridad de los activos de información.
IEPCT	Instituto Electoral y de Participación Ciudadana de Tabasco.

OSSTMM	(Open Source Security Testing Methodology Manual). Es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad en Sistemas de Cómputo.
OWASP	(Open Web Application Security Project). Es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para Aplicativos Web.
Statement of Work (Acuerdo de Trabajo).	Es el documento formal donde se definen las actividades de trabajo y la línea de tiempo que la FES Acatlán ejecutará sobre el servicio que preste al IEPCT.
Riesgo	Es la probabilidad de que una amenaza se materialice sobre un activo de información.
Vulnerabilidad	La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Antecedentes

Debido a la creciente necesidad de proteger los datos generados, almacenados y difundidos por las organizaciones y en específico, los considerados como potenciales blancos para recibir ataques que traten de afectar la disponibilidad, confidencialidad e integridad de la información. Motivo por el cual, el Instituto Electoral y de Participación Ciudadana de Tabasco (IEPCT) ha decidido contratar los servicios de penetración a la estructura tecnológica del PREP de la FES Acatlán, dicho servicio realizado por el Centro de Desarrollo Tecnológico de la FES Acatlán.

Objetivo

Evaluar los sistemas operativos de los dispositivos que conforman la infraestructura tecnológica del PREPET.

Alcance

Las pruebas de penetración se llevaron a cabo en infraestructura del IEPCT el 18 de junio de 2018, por el equipo de penetration testers de la FES Acatlán, enfocándose en la búsqueda de brechas de seguridad y verificando la factibilidad de acceso a aquellos activos que así lo permitieran.

Se llevaron a cabo pruebas basadas en la metodología empleada por la FES Acatlán, entre las que se comprenden OSSTMM y OWASP, para poder identificar posibles vulnerabilidades, que permitieran el acceso no autorizado a los sistemas o aplicativos y que tuvieran afectaciones en la disponibilidad, integridad y confidencialidad de los mismos.

A continuación, se enlistan los activos dentro del alcance:

ID	IP/URL	Homologada
1	www.prepet.mx	18.221.45.126

Nota. Para el caso de los equipos que hospedan un servidor web y a sí mismo tengan aplicaciones montadas, se considerará un activo de información por cada aplicativo para su revisión.

Por ejemplo: Si el equipo 10.0.0.100 hospeda a un portal web <http://www.ejemplo.com/> y a sí mismo aloja aplicativos en diversos host virtuales: <http://www.ejemplo.com/intranet> <http://www.ejemplo.com/vpn> se considerará un activo de información (de los 10 disponibles en cada servicio) por cada aplicativo que se evalúe en el equipo 10.0.0.100.

Conclusiones

Se realizó el servicio de pruebas de penetración a la infraestructura de los activos designados por el IEPCT durante el 18 de junio de 2018, para la explotación de posibles brechas de seguridad que permitieran el acceso no autorizado en los sistemas o aplicativos.

Acorde con el esfuerzo requerido para llevar a cabo la explotación de las vulnerabilidades identificadas y de acuerdo con las mejores prácticas, se considera un nivel de riesgo **Medio** sobre el activo evaluado, entre las vulnerabilidades identificadas se encuentra:

El certificado digital cuenta con una versión vieja de TLS en su versión 1.0, se recomienda el uso de TLS versión 1.2 o superior, así mismo cuenta con suites de cifrado con fortaleza media y baja.

Se identifica la navegación entre directorios del activo web, así como el uso del método OPTIONS, se recomienda evitar la divulgación de métodos permitidos por el servidor.








Se identificó el uso de una autenticación del tipo BASIC que emplea BASE64 para el envío de credenciales de usuario, se recomienda cambiar ese tipo de autenticación con la finalidad de evitar que las credenciales puedan ser capturadas por un usuario mal intencionado.

El uso de HSTS no está implementado, sin embargo existe un redireccionamiento sobre el sitio que permite forzar el uso de HTTPS sobre HTTP.







El servidor web Apache es inmune a ataques por directorio transversal, se concluyen las pruebas sin éxito.

Reporte técnico de hallazgos

Para una mejor interpretación de los hallazgos identificados y su ponderación por probabilidad de ocurrencia (riesgo) y complejidad de explotación de la vulnerabilidad, se emplea la siguiente tabla como referencia:

	Crítica	Alta	Media	Baja
Probabilidad de Ocurrencia				
Complejidad de Explotación				

En la siguiente sección se enumeran y detallan las vulnerabilidades encontradas durante las diferentes fases de la evaluación.

Id	Hallazgo	Probabilidad de Ocurrencia	Complejidad de Explotación
1	Múltiples problemas con el certificado digital.		
2	Ausencia de HSTS.		
3	Navegación entre directorios del aplicativo.		

Impacto	Vulnerabilidad	Activo Afectado
Medio	Múltiples problemas con el certificado digital.	www.prepet.mx
Medio	Ausencia de HSTS.	www.prepet.mx
Medio	Navegación entre directorios del aplicativo.	www.prepet.mx

Vectores de Ataque

Red Interna

- Reconocimiento de los activos para la obtención de mayor información, entre lo cual se identificó el uso de servicios web en los puertos 80 y 443, así como el uso de ssh por el puerto 22.
- Se identificó el uso de un servidor Apache versión 2.4.18
- Se realizaron pruebas basadas en OSSTMM sobre el activo y su ip homologada. No se identifica problemas asociados a esta capa de análisis.

Aplicativos Web

- Se desarrollaron pruebas de penetración web siguiendo la metodología de OWASP en su top 10 de vulnerabilidades para el aplicativo `www.prepet.mx`
- Se realizaron análisis pasivos y activos para la obtención de tecnologías empleadas en los sitios con la intención de analizar la superficie de ataque.
- Se realizaron pruebas de inyección de código SQL y JavaScript, sin éxito, de haberse materializado pudieran haber generado un defacement en el aplicativo web.
- Se realizaron pruebas de enumeración de directorios del sitio con lo que fue posible crear una copia total del sitio, ya que carece de protección ante esta clase de ataques.
- Se identifica el uso de certificado digital con el uso de TLS versión 1.0, se recomienda el uso de TLS versión 1.2 en adelante, así como suites de cifrado de fortaleza débil.
- Se realizaron pruebas sobre el HSTS.
- Intento de ataque por diccionario transversal.

Nota: Para un detalle más puntual favor de ir a la sección de Desarrollo del servicio.




Recomendaciones

A continuación, se presentan las recomendaciones puntuales para la mejora continua de los procesos de seguridad:

Tecnología:

- Implementar cuentas con los mínimos privilegios necesarios para la administración y para usuarios finales.
- Mantener una política robusta de creación y manejo de contraseñas para cuentas con privilegios de administración.
- Evitar en todo momento contraseñas predecibles o diccionario simple.
- Crear una campaña de difusión de la política institucional de cuentas de usuario y contraseñas, donde se incluya lo siguiente:
 - Establecer contraseñas robustas para los usuarios de la institución (15 caracteres alfanuméricos como mínimo, que incluyan mayúsculas, minúsculas y símbolos).
 - Establecer contraseñas robustas para los servicios de administración remota en los servidores de IEPCT (18 caracteres alfanuméricos como mínimo, que incluyan mayúsculas, minúsculas y símbolos).
 - Implementar políticas de vigencia de contraseñas.
- Restringir el acceso a cada uno de recursos compartidos sólo para los usuarios administradores de cada equipo o estrictamente a usuarios para los que sea necesario el acceso a estos recursos.
- Implementación o reemisión del certificado digital con TLS versión 1.2
- Implementar un control de HSTS para garantizar la navegación del sitio por HTTPS y no solo por el redireccionamiento del mismo.

Desarrollo del servicio

18.221.45.126 www.prepet.mx		Riesgo	Vulnerabilidad																																																																							
		Medio	Múltiples problemas con el certificado digital. Ausencia de HSTS. Navegación entre directorios del aplicativo.																																																																							
Descripción:	<ul style="list-style-type: none">Se realizó un escaneo de la red para encontrar los puertos, protocolos y servicios que estén disponibles en el equipo.Se realizó un análisis de vulnerabilidades sobre el activo con una herramienta automatizada para identificar vulnerabilidades que fueran explotables.Se obtuvo la mayor información posible de forma pasiva sobre el activo, identificando tecnologías empleadas en el servidor web.Se identifica el uso del método OPTIONS en el servidor web.Se identificó el control de acceso por BASIC Authentication en el activo con base64 como codificación.Se identificaron tecnologías empleadas en el aplicativo.Se realizaron pruebas sobre el certificado digital SSL del servidor web, se identifican múltiples fallos sobre el mismo.Se realizaron pruebas de enumeración de directorios, en todos los casos es posible navegar entre los directorios del aplicativo.Se realizaron pruebas de directorios transversales, sin éxito.Se realizaron pruebas sobre el HSTS, no se identifica la presencia del mismo, sin embargo, existe un redireccionamiento de HTTP a HTTPS																																																																									
Resultado o repuesta del análisis:	<div><table><tr><td>Site title</td><td colspan="3">PREPET TABASCO</td></tr><tr><td>Site rank</td><td colspan="3"></td></tr><tr><td>Description</td><td colspan="3">Not Present</td></tr><tr><td>Keywords</td><td colspan="3">Not Present</td></tr><tr><td>Netcraft Risk Rating [FAQ]</td><td>10/10</td><td colspan="2"><div></div></td></tr></table><div>Identificación pasiva de tecnologías y proveedores empleados en el activo web</div><div><div>Network</div><table><tr><td>Site</td><td>http://www.prepet.mx</td><td>Netblock Owner</td><td colspan="2">Amazon Technologies Inc.</td></tr><tr><td>Domain</td><td>prepet.mx</td><td>Nameserver</td><td colspan="2">ns33.domaincontrol.com</td></tr><tr><td>IP address</td><td>18.221.45.126</td><td>DNS admin</td><td colspan="2">dns@jomax.net</td></tr><tr><td>IPv6 address</td><td>Not Present</td><td>Reverse DNS</td><td colspan="2">ec2-18-221-45-126.us-east-2.compute.amazonaws.com</td></tr><tr><td>Domain registrar</td><td>unknown</td><td>Nameserver organisation</td><td colspan="2">whois.wildwestdomains.com</td></tr><tr><td>Organisation</td><td>unknown</td><td>Hosting company</td><td colspan="2">Amazon - US East (Ohio) datacenter</td></tr><tr><td>Top Level Domain</td><td>Mexico (.mx)</td><td>DNS Security Extensions</td><td colspan="2">unknown</td></tr><tr><td>Hosting country</td><td> us</td><td colspan="3"></td></tr></table><div><div>Hosting History</div><table><tr><td>Netblock owner</td><td>IP address</td><td>OS</td><td>Web server</td><td>Last seen</td></tr><tr><td>Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109</td><td>18.221.45.126</td><td>Linux</td><td>Apache/2.4.18 Ubuntu</td><td>19-Jun-2018</td></tr></table></div></div></div>				Site title	PREPET TABASCO			Site rank				Description	Not Present			Keywords	Not Present			Netcraft Risk Rating [FAQ]	10/10	<div></div>		Site	http://www.prepet.mx	Netblock Owner	Amazon Technologies Inc.		Domain	prepet.mx	Nameserver	ns33.domaincontrol.com		IP address	18.221.45.126	DNS admin	dns@jomax.net		IPv6 address	Not Present	Reverse DNS	ec2-18-221-45-126.us-east-2.compute.amazonaws.com		Domain registrar	unknown	Nameserver organisation	whois.wildwestdomains.com		Organisation	unknown	Hosting company	Amazon - US East (Ohio) datacenter		Top Level Domain	Mexico (.mx)	DNS Security Extensions	unknown		Hosting country	 us				Netblock owner	IP address	OS	Web server	Last seen	Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	18.221.45.126	Linux	Apache/2.4.18 Ubuntu	19-Jun-2018
Site title	PREPET TABASCO																																																																									
Site rank																																																																										
Description	Not Present																																																																									
Keywords	Not Present																																																																									
Netcraft Risk Rating [FAQ]	10/10	<div></div>																																																																								
Site	http://www.prepet.mx	Netblock Owner	Amazon Technologies Inc.																																																																							
Domain	prepet.mx	Nameserver	ns33.domaincontrol.com																																																																							
IP address	18.221.45.126	DNS admin	dns@jomax.net																																																																							
IPv6 address	Not Present	Reverse DNS	ec2-18-221-45-126.us-east-2.compute.amazonaws.com																																																																							
Domain registrar	unknown	Nameserver organisation	whois.wildwestdomains.com																																																																							
Organisation	unknown	Hosting company	Amazon - US East (Ohio) datacenter																																																																							
Top Level Domain	Mexico (.mx)	DNS Security Extensions	unknown																																																																							
Hosting country	 us																																																																									
Netblock owner	IP address	OS	Web server	Last seen																																																																						
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	18.221.45.126	Linux	Apache/2.4.18 Ubuntu	19-Jun-2018																																																																						

```
Initiating NSE at 21:44
Completed NSE at 21:44, 1.05s elapsed
Nmap scan report for www.prepet.mx (18.221.45.126)
Host is up, received reset ttl 128 (0.021s latency).
rDNS record for 18.221.45.126: ec2-18-221-45-126.us-east-2.compute.amazonaws.com
Scanned at 2018-06-19 21:32:34 CDT for 721s

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 128   OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 c8:2a:16:1f:48:6b:c3:93:8b:40:3e:d3:08:97:2a:85 (RSA)
|_   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCS0a3GdEM8KgKFGazNvhN1bAaWBw6/RH/mRN464Y1VtewZb7WmsLASTra19/
xHNLum4/h6qS/s6k14jTF1K/Ud+2v6BgrPzN5o6aRk5nMwsaNgEj0m/adz8b8X9JX4ThrcuLyju6L/n/fBrWXGlagjM8ez3X6XAc
|_   256 b1:ce:16:50:dc:e8:64:98:38:3e:1b:25:c1:f3:18:8a (ECDSA)
|_   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBypFIKUrXkmW3dRuUK5qNSQ05
|_   256 74:ab:a6:28:52:30:7e:ff:3a:e8:06:06:a4:d2:ac:ae (ED25519)
|_   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK1nPZg0u4uERQdzYzAH3MQxESfM3Yidb4INQ8sV6Lob
80/tcp    open  http      syn-ack ttl 128   Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: PREPET TABASCO
443/tcp   open  ssl/ssl   syn-ack ttl 128   Apache httpd (SSL-only mode)
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Acceso Denegado :: Prep Tabasco 2016
|_ ssl-cert: Subject: commonName=www.prepet.mx/organizationalUnitName=Domain Control Validated
|_ Subject Alternative Name: DNS:www.prepet.mx, DNS:prepet.mx
|_ Issuer: commonName=Go Daddy Secure Certificate Authority - G2/organizationName=GoDaddy.com, Inc./s
ame=Scottsdale
|_ Public Key type: rsa
|_ Public Key bits: 2048
```

Identificación del
método OPTIONS
en el servidor web

Request to https://www.prepet.mx:443 [18.221.45.126]

Forward Drop Intercept is on Action

Raw Headers Hex

GET / HTTP/1.1
Host: www.prepet.mx
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic c2ltYWxhY3JvOnMxY2M/MjAxOA==

c2ltYWxhY3JvOnMxY2M/MjAxOA==

simulacro:s1cc?2018

Autenticación BASIC para
ingresar al sitio, uso de BASE
64 para el envío de credenciales
de usuario

Pruebas de penetración a la infraestructura del PREP 2018
Elección 2018, gobernador, diputaciones locales y ayuntamientos

Página principal del aplicativo

PREPET | Gubernatura - E: x

Es seguro | https://www.prepet.mx/#/gubernatura-por-entidad

Elecciones Estatales de Tabasco

Programa de Resultados Electorales Preliminares

Alcance del Simulacro 2

IEPC TABASCO

PREP 2018 TAB

Gubernatura | Diputaciones | Presidencias Municipales y Regidurías | Ayuda

Votos por Candidatura | Candidatura Independiente

Inicio | Gubernatura - Entidad

Entidad
Distrito
Sección-Casilla

ACTAS CAPTURADAS:

2,912 de 2,912
100.0000 %

PARTICIPACIÓN CIUDADANA

18.9734 %

ÚLTIMO CORTE

04:56 horas (UTC-5)
Hora local, 18 de junio de 2018

Actualizar Base de datos

Gubernatura - Entidad

El total de votos calculado y porcentaje que se muestran, se refieren a los votos asentados en las Actas PREP hasta el momento. Por presentación, los decimales de los porcentajes muestran sólo cuatro dígitos. No obstante, al considerar todos los decimales, suman 100%. El total de votos mostrado a nivel Entidad representa la suma del voto emitido en territorio estatal.

Diputaciones - Entidad

El total de votos calculado y porcentaje que se muestran, se refieren a los votos asentados en las Actas PREP hasta el momento. Por presentación, los decimales de los porcentajes muestran sólo cuatro dígitos. No obstante, al considerar todos los decimales, suman 100%.

Mapa Distritos Electorales

El mapa resalta los distritos electorales donde aventaja el partido político, coalición o candidatura independiente hasta el momento.

DIPUTACIONES

OBTENIDAS POR:

Wappalyzer

Analítica

- Google Analytics

Framework JavaScript

- AngularJS 1.5.8
- jQuery 3.3.1

Tipografía

- Font Awesome
- Google Font API

Framework Web

- Bootstrap

Servidor Web

- Apache 2.4.18

Gráficos JavaScript

- Highcharts 4.1.9
- Raphael 2.2.0

Sistema Operativo

- Ubuntu

Tag Manager

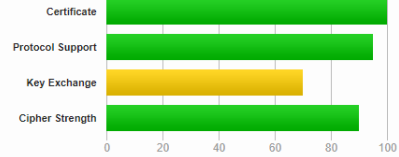
- Google Tag Manager

Identificación de tecnologías en empleadas en el aplicativo web

SSL Report: www.prepet.mx (18.221.45.126)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO >](#)

This server's certificate chain is incomplete. Grade capped to B.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.prepet.mx Fingerprint SHA256: 702ad03ab0e9e03496fd1361edc3c0f83404da38d0185f28da028db39496f20 Pin SHA256: 5fnIWZTxc39qRPlaySydvB7G1o7WLLCX7ZNNHBXjdTGY=
Common names	www.prepet.mx
Alternative names	www.prepet.mx prepet.mx
Serial Number	23e8ec313864cb5a
Valid from	Mon, 11 Jun 2018 03:22:44 UTC
Valid until	Tue, 11 Jun 2019 03:22:44 UTC (expires in 11 months and 22 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Go Daddy Secure Certificate Authority - G2 AIA: http://certificates.godaddy.com/repository/gdigi2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.godaddy.com/gdigi2s1-838.crl OCSP: http://ocsp.godaddy.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	1 (1590 bytes)
Chain issues	Incomplete



Certification Paths

[Click here to expand](#)

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 23.

Cipher Suites

TLS 1.2 (server has no preference)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS

128

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK

128

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH sect571r1 (eq. 15360 bits RSA) FS

128

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS

128

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK

128

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH sect571r1 (eq. 15360 bits RSA) FS

128

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH sect571r1 (eq. 15360 bits RSA) FS

128

TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS

256

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK

256

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH sect571r1 (eq. 15360 bits RSA) FS

256

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS

256

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK

256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH sect571r1 (eq. 15360 bits RSA) FS

256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH sect571r1 (eq. 15360 bits RSA) FS

256

TLS 1.1 (server has no preference)

TLS 1.0 (server has no preference)

Se identifica el uso de TLS 1.0. Se recomienda usar TLS 1.2 o superior

14

Pruebas de penetración a la infraestructura del PREP 2018 Elección 2018, gobernador, diputaciones locales y ayuntamientos



Handshake Simulation

Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp283k1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp571r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp571r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp571r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp571r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 65 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 59 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 8 / XP No FS ¹ No SNI ²	Server sent fatal alert: handshake_failure		
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 2048 FS
OpenSSL 1.0.1j R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp571r1 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp571r1 FS

Pruebas de penetración a la infraestructura del PREP 2018
Elección 2018, gobernador, diputaciones locales y ayuntamientos



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x2f
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	With some browsers (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp256k1, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (Server has no preference)
SSL 2 handshake compatibility	Yes



HTTP Requests

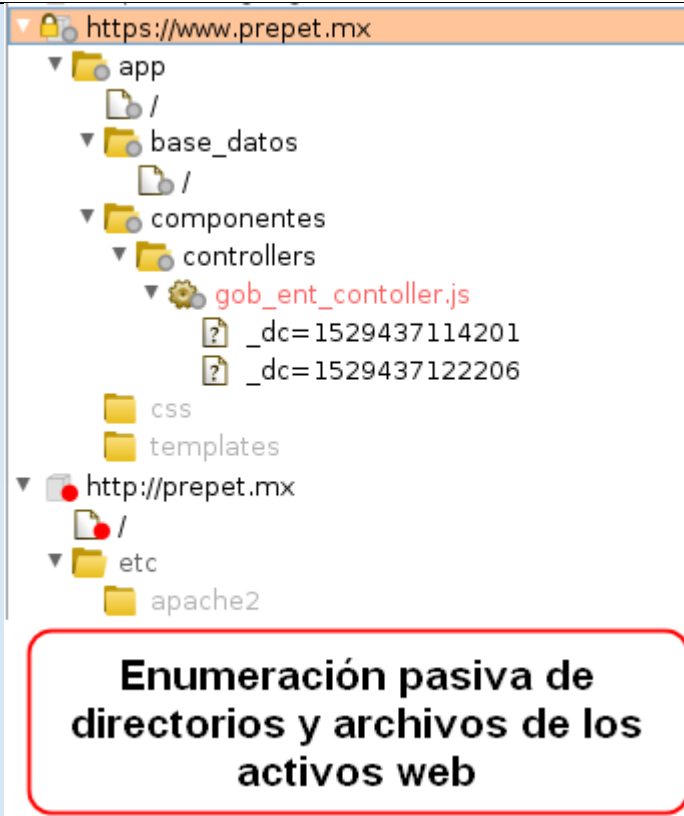


1 https://www.prep.mx/ (HTTP/1.1 401 Unauthorized)



Miscellaneous

Test date	Tue, 19 Jun 2018 22:13:44 UTC
Test duration	117.328 seconds
HTTP status code	401
HTTP server signature	Apache/2.4.18 (Ubuntu)
Server hostname	ec2-18-221-45-126.us-east-2.compute.amazonaws.com



Index of /assets				Index of /app			
Name	Last modified	Size	Description	Name	Last modified	Size	Description
Parent Directory		-		Parent Directory		-	
AlcanceSimulacro2.pdf	2018-06-17 23:39	378K		HeaderService.js	2018-06-04 19:08	4.9K	
as1.pdf	2018-06-17 23:18	378K		Services.js	2018-06-14 16:06	41K	
global/	2018-06-15 16:39	-		base_datos/	2018-06-18 09:56	-	
img/	2018-06-17 22:30	-		componentes/	2018-06-15 17:43	-	
layouts/	2018-06-17 23:23	-		css/	2018-06-17 22:29	-	
Apache/2.4.18 (Ubuntu) Server at www.prepet.mx Port 443				directives.js	2018-06-01 16:24	2.5K	
Navegación entre directorios del aplicativo está habilitada				json/	2018-06-15 17:43	-	
				main.js	2018-06-13 11:27	21K	
				templates/	2018-06-17 23:42	-	
				Apache/2.4.18 (Ubuntu) Server at www.prepet.mx Port 443			

	<pre>[+] Report name: Reports/www.prepet.mx_06-19-2018_19-15.txt [===== TARGET INFORMATION =====] [+] Hostname: www.prepet.mx [+] Protocol: http [+] Port: 80 [===== TRAVERSAL ENGINE =====] [+] Creating Traversal patterns (mix of dots and slashes) [+] Multiplying 6 times the traversal patterns (-d switch) [+] Creating the Special Traversal patterns [+] Translating (back)slashes in the filenames [+] Adapting the filenames according to the OS type detected (unix) [+] Including Special suffixes [+] Traversal Engine DONE ! - Total traversal tests created: 11028 [===== TESTING RESULTS =====] [+] Ready to launch 3.33 traversals per second [+] Press Enter to start the testing (You can stop it pressing Ctrl + C) [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./././etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./././././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/./././././etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././././etc/issue [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././././etc/passwd [*] HTTP Status: 400 Testing Path: http://www.prepet.mx:80/././././././etc/issue [*] HTTP Status: 404 Testing Path: http://www.prepet.mx:80/./%5Cetc%5Cpasswd [*] HTTP Status: 404 Testing Path: http://www.prepet.mx:80/./%5Cetc%5Cissue</pre> <div data-bbox="1162 344 1450 432" style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p>Intento de ataque por directorio transversal</p> </div> <div data-bbox="396 890 477 966" style="float: left; margin-right: 10px;"> </div> <div data-bbox="493 907 1156 949" style="float: left;"> <h3>Strict transport security not enforced</h3> </div> <div data-bbox="396 999 993 1142" style="clear: both;"> <p>Issue: Strict transport security not enforced Severity: Low Confidence: Certain Host: https://www.prepet.mx Path: /</p> </div> <div data-bbox="1006 1016 1442 1134" style="border: 1px solid red; padding: 5px; margin: 10px 0; float: right;"> <p>Ausencia de HSTS en el servidor web</p> </div> <div data-bbox="396 1159 1442 1234" style="background-color: black; color: white; padding: 5px; margin: 10px 0;"> <pre>root@kali:~# curl -s -D- https://www.prepet.mx grep -i "Strict" root@kali:~#</pre> </div> <div data-bbox="396 1276 1354 1352" style="border: 1px solid red; padding: 5px; margin: 10px 0; text-align: center;"> <p>Ejemplo de sitio web con HSTS habilitado</p> </div> <div data-bbox="396 1360 1347 1423" style="background-color: black; color: white; padding: 5px; margin: 10px 0;"> <pre>root@kali:~# curl -s -D- https://owasp.org grep -i "Strict" Strict-Transport-Security: max-age=15768000</pre> </div>
<p>Recomendación</p>	<p>Emitir un nuevo certificado que cubra los problemas actuales. Implementar HSTS. Bloquear la navegación entre directorios del aplicativo.</p>

Anexo A. Puertos y servicios

Dirección IP	Nombre	Servicio	Sistema Operativo
18.221.45.126 www.prepet.mx		IEPCT	Linux
Puerto	Protocolo	Servicio	
22	tcp	ssh	
80	tcp	http	
443	tcp	https	
5060	tcp	sip	

Anexo B. Marco metodológico y mejores prácticas

El servicio de pruebas de penetración a la infraestructura del IEPCT tiene como finalidad identificar las debilidades, huecos y áreas de oportunidad en materia de seguridad de la información a las que está expuesta la infraestructura tecnológica, identificando el origen de la vulnerabilidad (producto de la deficiencia en la implementación del control de seguridad), de ser posible explotarla e intentar movimientos hacia otros objetivos, una vez terminado el servicio se emitirán las recomendaciones pertinentes para su mitigación.

A continuación, se enumeran las actividades que se llevaron a cabo:

1. El IEPCT proporcionó la lista de direcciones IP autorizadas para ser evaluadas.
2. Mediante técnicas manuales y automatizadas, se identificaron aquellos dispositivos que se encontraban activos.
3. Se identificaron de los servicios que se encuentran publicados en los servidores de la red interna e internet.
4. Se identificaron y analizaron las vulnerabilidades, debilidades y configuraciones inseguras en los activos designados.
5. Se realizaron pruebas de penetración a los activos designados, empleando las metodologías de OSSTMM y OWASP.

Como parte de la metodología empleada para la clasificación de vulnerabilidades, se utiliza la métrica provista por el CVSS (Common Vulnerability Scoring System) en su versión 2, en conjunto con la experiencia del equipo de consultores asignados a la ejecución del servicio.

De acuerdo con lo descrito por el CVSS, es posible clasificar el impacto de las vulnerabilidades tecnológicas basándose en el análisis matemático con respecto a una puntuación situada en una escala entre 0 y 10, y un vector que representa los valores empleados para la obtención de dicha puntuación.

Las ecuaciones y valores de las variables para cada una de los grupos pueden ser consultados en <https://www.first.org/cvss/v2/guide>

Herramientas utilizadas

Las herramientas utilizadas para el servicio brindado se enlistan a continuación:

- Escáner de puertos
- Escáner de servicios
- Scripts automatizados para análisis de vulnerabilidades
- Herramientas de explotación