

Un dibujo con letras

Descripción generada automáticamente con confianza media

**ENERGIA ARGENTINA SA**

Pentest (Pruebas de Intrusión)

Informe Técnico

05/08/2025

Tabla de Contenidos

**No se encontraron entradas de tabla de contenido.**

# Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Pentest (Pruebas de Intrusión)** sobre la infraestructura de **ENERGIA ARGENTINA SA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **14/07/2025** y el **30/07/2025**.

# Alcance

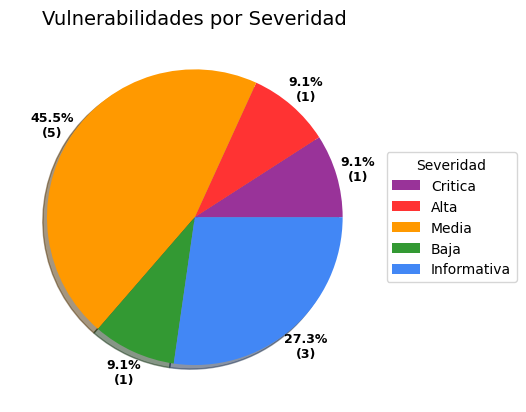
Las siguientes redes o rangos IP fueron suministrados para realizar un descubrimiento de hosts activos:  
**190.220.133.0/27**  
**200.61.169.64/27**

Luego del descubrimiento se acordaron los siguientes hosts para realizar una evaluación del tipo Pentest (Pruebas de Intrusión).

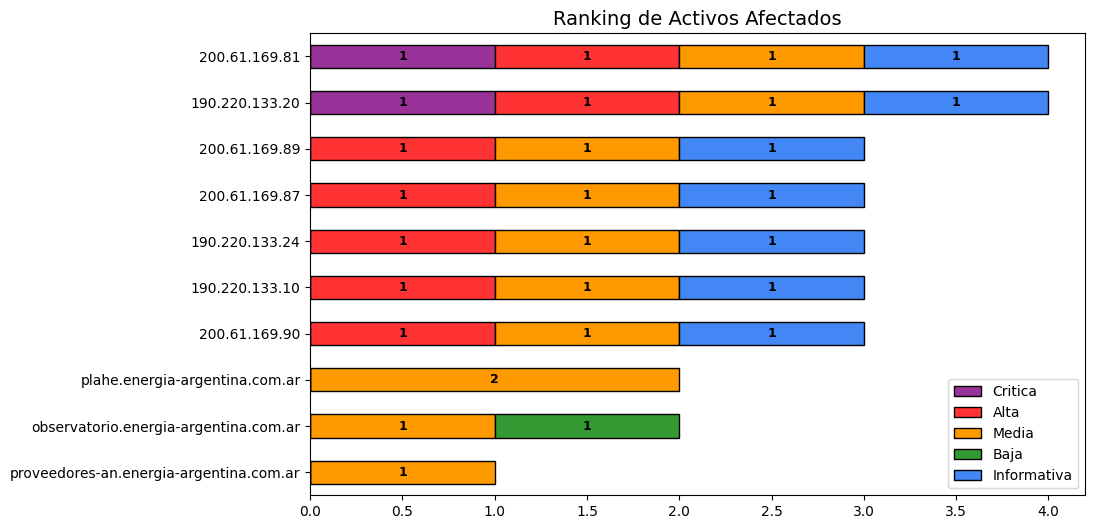
**190.220.133.1**  
**190.220.133.10**  
**190.220.133.20**  
**190.220.133.22**  
**190.220.133.24**  
**190.220.133.25**  
**190.220.133.3**  
**190.220.133.4**  
**190.220.133.8**  
**200.61.169.65**  
**200.61.169.67**  
**200.61.169.70**  
**200.61.169.71**  
**200.61.169.75**  
**200.61.169.79**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

# Resumen

Como resultado del análisis se han identificado **11** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **1** de severidad crítica, **1** de severidad alta, **5** de severidad media, **1** de severidad baja y **3** 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 detectadas.



# Hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

| #ID | Nombre | Severidad | Hosts Afectados |
| --- | --- | --- | --- |
| #1 | Hypertext Preprocessor (PHP) Multiple Vulnerabilities | **Critica** | 2 |
| #2 | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) | **Alta** | 7 |
| #3 | Insecure Direct Object Reference (IDOR) | **Media** | 1 |
| #4 | TLS/SSL Weak Cipher Suites | **Media** | 7 |
| #5 | Insufficient File Type Validation in File Uploads | **Media** | 1 |
| #6 | GIT Detected | **Media** | 1 |
| #7 | User enumeration | **Media** | 1 |
| #8 | Development configuration files | **Baja** | 1 |
| #9 | Open TCP Services List | **Informativa** | 6 |
| #10 | Firewall Detected | **Informativa** | 12 |
| #11 | Open UDP Services List | **Informativa** | 2 |

# 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 |
| Ocurrencias: 2 | **Privileges Required** | None | **Integrity Impact** | High |
| **User Interaction** | None | **Availability Impact** | High |

### Recursos Afectados

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

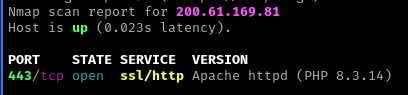
### Solución

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

### Evidencias

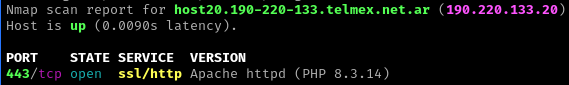
Recurso: 200.61.169.81 Puerto: TCP/443

Vulnerable version of PHP detected on port 443 over TCP.   
Date: Tue, 22 Jul 2025 15:21:36 GMT  
Server: Apache  
X-Powered-By: PHP/8.3.14  
X-Redirect-By: WordPress  
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  
Location: :///  
Cache-Control: max-age=0  
Expires: Tue, 22 Jul 2025 15:21:36 GMT  
Vary: Accept-Encoding  
Content-Length: 0  
Connection: close  
Content-Type: text/html; charset=UTF-8  
X-XSS-Protection: 1  
Content-Security-Policy: object-src 'self';frame-ancestors 'self'  
Set-Cookie: ADC\_CONN\_539B3595F4E=A4D5B85C1677127C8E1680B1ACA5F9C5EFD50803A1A03D15994D0CA45A1AAD1B26B7201A6E5F794F; expires=Tue, 22 Jul 2025 16:22:02 GMT; HttpOnly; Secure; SameSite=Strict  
Set-Cookie: ADC\_REQ\_2E94AF76E7=96EA1E0E4B48B897E507C7E16FE7112E90BED18551D650160D428B1D5F058AD7235B6023CC2CB0D8; expires=Tue, 22 Jul 2025 16:22:02 GMT; Path=/; HttpOnly; Secure; SameSite=Strict



Recurso: 190.220.133.20 Puerto: TCP/443

Vulnerable version of PHP detected on port 443 over TCP.   
Date: Mon, 14 Jul 2025 14:11:11 GMT  
Server: Apache  
X-Powered-By: PHP/8.3.14  
X-Redirect-By: WordPress  
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  
Location: :///  
Cache-Control: max-age=0  
Expires: Mon, 14 Jul 2025 14:11:11 GMT  
Vary: Accept-Encoding  
Content-Length: 0  
Connection: close  
Content-Type: text/html; charset=UTF-8  
X-XSS-Protection: 1  
Content-Security-Policy: object-src 'self';frame-ancestors 'self'  
Set-Cookie: ADC\_CONN\_539B3595F4E=CE1036282D222B723071C6FB5302625FDCA84B41253EE261E0CA2C711F71E799CB87DA101A20EF12; expires=Mon, 14 Jul 2025 15:11:25 GMT; HttpOnly; Secure; SameSite=Strict  
Set-Cookie: ADC\_REQ\_2E94AF76E7=767A5B09899E87583E69AD1B850831002C22D042900073FBC0E5C4CF924B37B3C56624BD9B5BB021; expires=Mon, 14 Jul 2025 15:11:25 GMT; Path=/; HttpOnly; Secure; SameSite=Strict



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #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 |
| Ocurrencias: 7 | **Privileges Required** | None | **Integrity Impact** | None |
| **User Interaction** | None | **Availability Impact** | None |

### Recursos Afectados

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

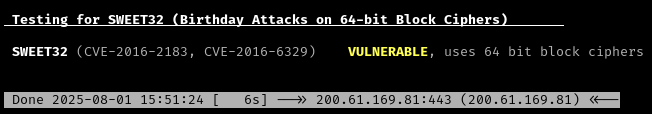
### Solución

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

### Evidencias

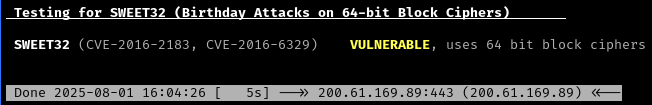
Recurso: 200.61.169.81 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



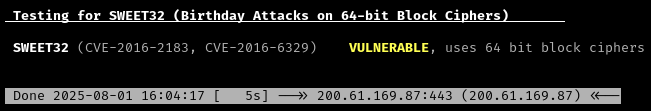
Recurso: 200.61.169.89 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



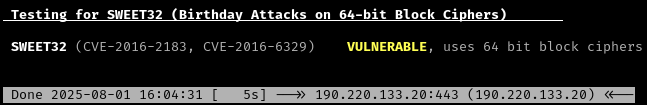
Recurso: 200.61.169.87 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



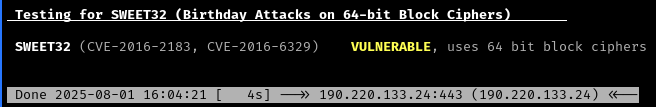
Recurso: 190.220.133.20 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



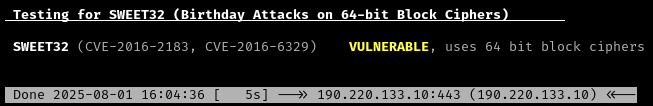
Recurso: 190.220.133.24 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



Recurso: 190.220.133.10 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



Recurso: 200.61.169.90 Puerto: TCP/443

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE  
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED   
DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM  
EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #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 |

### Recursos Afectados

https://plahe.energia-argentina.com.ar/php/ws-get-reportes-by-aprovs.php

### 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

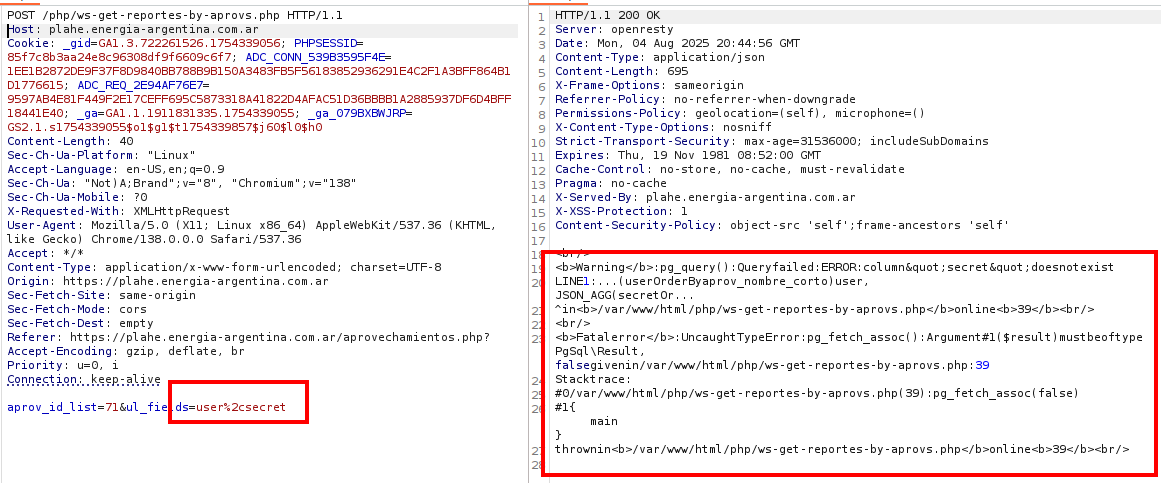
La forma más infalible de prevenir las vulnerabilidades y los ataques de IDOR es realizar una validación de acceso. Si un atacante intenta manipular una aplicación o base de datos modificando la referencia dada, el sistema debería poder cerrar la solicitud, verificando que el usuario no tenga las autorizaciones 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: https://plahe.energia-argentina.com.ar/php/ws-get-reportes-by-aprovs.php

En el request original se pueden agregar o quitar campos de la consulta a ser ejecutada en la base de datos. En el ejemplo se obtuvo el campo "User" recibiendo el valor "appadmin". A su vez se puede observar una inyección SQL incompleta, al utilizar campos que no existen en la tabla consultada, divulgando información del motor de Base de Datos utilizado.





|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #4 TLS/SSL Weak Cipher Suites | | | | |
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 6.5 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 7 | **Privileges Required** | None | **Integrity Impact** | Low |
| **User Interaction** | None | **Availability Impact** | None |

### Recursos Afectados

https://190.220.133.10  
https://190.220.133.20  
https://190.220.133.24  
https://200.61.169.81  
https://200.61.169.87  
https://200.61.169.89  
https://200.61.169.90

### Descripción

El host remoto admite suites TLS/SSL con propiedades débiles o inseguras.

### 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

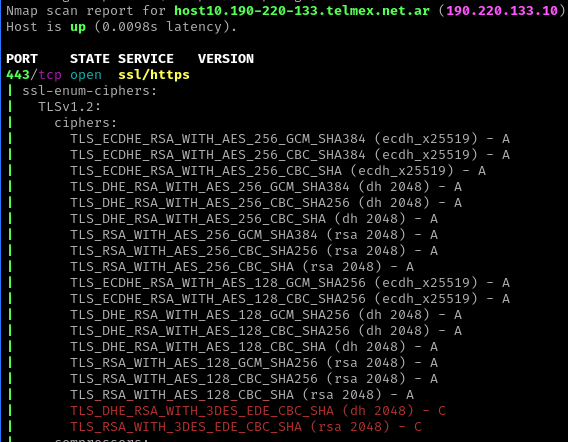
### Solución

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

### Evidencias

Recurso: https://190.220.133.10

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)



Recurso: https://200.61.169.90

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
  
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)

Recurso: https://200.61.169.89

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)

Recurso: https://190.220.133.24

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)

Recurso: https://190.220.133.20

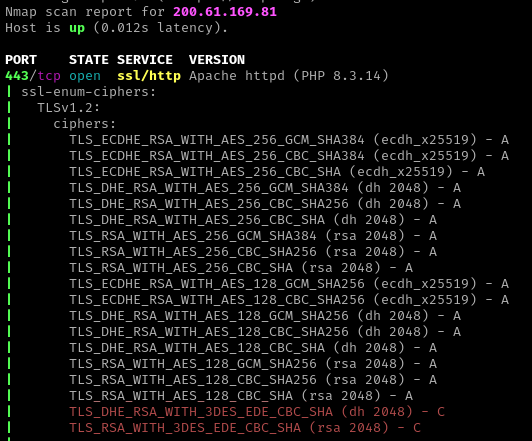
Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)

Recurso: https://200.61.169.87

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)

Recurso: https://200.61.169.81

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):   
   
\* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)  
\* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (Medium strength encryption algorithm (3DES).)



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #5 Insufficient File Type Validation in File Uploads | | | | |
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 6.3 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | Low |
| **User Interaction** | Required | **Availability Impact** | Low |

### Recursos Afectados

https://proveedores-an.energia-argentina.com.ar/\_layouts/15/enarsa/AltaProvisoria.aspx?AN=SI

### 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, como scripts PHP, 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 PHP 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.

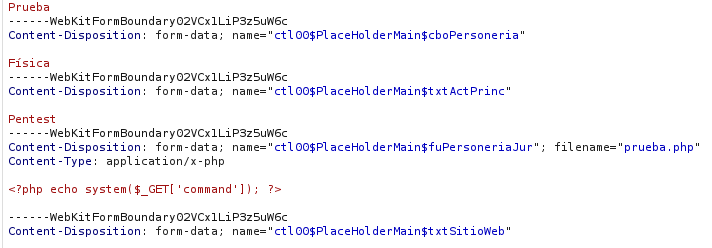
### Solución

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: https://proveedores-an.energia-argentina.com.ar/\_layouts/15/enarsa/AltaProvisoria.aspx?AN=SI

Se permitió la subida de un archivo con extensión PHP sin validación.





|  |
| --- |
| #6 GIT Detected |
| Severidad: Media |
| CVSS: 5.8 |
| Ocurrencias: 1 |

### Recursos Afectados

https://observatorio.energia-argentina.com.ar

### 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/

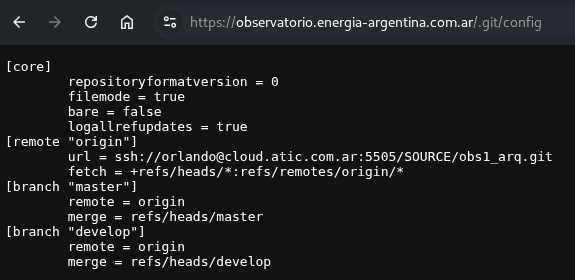
### Solución

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://observatorio.energia-argentina.com.ar

Git files found at : /.git/config   
   
Repository files/directories:   
 \* CMD-login.php  
 \* CMD-logout.php  
 \* Get\_Link.php  
 \* MICROSERVICIOS/CRED/conf.php  
 \* MICROSERVICIOS/CRED/index.php  
 \* MICROSERVICIOS/MIC-CATALOGO/CAPA-APLICACION/QUERY/REPOSITORIO-QUERY.php  
 \* MICROSERVICIOS/MIC-CATALOGO/CAPA-APLICACION/SERVICIO/REPOSITORIO-SERVICIO.php  
 \* MICROSERVICIOS/MIC-CATALOGO/CAPA-DATOS/capa-acceso.php  
 \* MICROSERVICIOS/MIC-CATALOGO/CAPA-DOMINIO/CLASES/Clases.php  
 \* MICROSERVICIOS/MIC-CATALOGO/CAPA-DOMINIO/DTOS/DTOS.php  
 \* ...



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #7 User enumeration | | | | |
| 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 |

### Recursos Afectados

https://plahe.energia-argentina.com.ar/login.php

### 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.

### Evidencias

Recurso: https://plahe.energia-argentina.com.ar/login.php

Se verifica que al utilizar el usuario "admin" responde "errorAccess", y con el usuario "appadmin" el mensaje es "errorUser"





|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #8 Development configuration files | | | | |
| Severidad: Baja | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 3.1 | **Attack Complexity** | High | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| **User Interaction** | Required | **Availability Impact** | None |

### Recursos Afectados

https://observatorio.energia-argentina.com.ar/composer.lock

### 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.

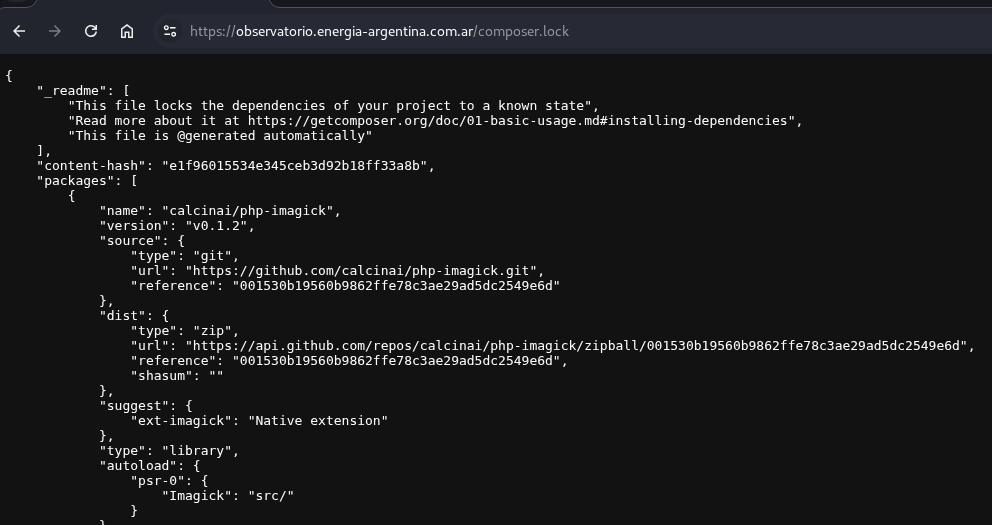
### Solución

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

### Evidencias

Recurso: https://observatorio.energia-argentina.com.ar/composer.lock

Development configuration files:  
 \* https://observatorio.energia-argentina.com.ar/ \*\*composer.lock\*\*   
   
 composer.lock => Composer lock file. Composer is a dependency manager for PHP.



|  |
| --- |
| #9 Open TCP Services List |
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 6 |

### Recursos Afectados

190.220.133.10  
190.220.133.20  
190.220.133.24  
200.61.169.81  
200.61.169.87  
200.61.169.89

### Descripción

Se identificaron servicios accesibles mediante conexiones TCP en el perímetro de red, visibles durante el reconocimiento activo. 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

La exposición de servicios TCP permite a un atacante mapear 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

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: 200.61.169.89

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

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

Port IANA Assigned Ports/Services Description Service Detected OS On Redirected Port  
72 netrjs-2 Remote Job Service unknown Unknown  
80 www-http World Wide Web HTTP http   
443 https http protocol over TLS/SSL http over ssl   
5346 unknown unknown unknown Unknown  
6682 unknown unknown unknown Unknown

Recurso: 190.220.133.24

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: 190.220.133.10

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   
5194 unknown unknown unknown Unknown  
10901 unknown unknown unknown Unknown  
13984 unknown unknown unknown Unknown

|  |
| --- |
| #10 Firewall Detected |
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 12 |

### Recursos Afectados

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 mecanismo de filtrado perimetral (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.

### Evidencias

Recurso: 190.220.133.8

Firewall responded to TCP probes sent to port 20 with RST packets (hopcount to firewall 8 vs hopcount to target 9).

Recurso: 190.220.133.22

Some of the ports filtered by the firewall are: 25.  
  
Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
16,32,36,226,229-230,232,237,247,249,251-252,269-271,275,283,286,294,  
298-299,303-304,306-307,312-314,326-328,334,341,355-356,358,368,584,589,  
597,632,650,654-655,657,659,687,692,694-695,706,718,720,723-724,726,735,  
745,768,802-803,810-812,825-826,835,847-848,857,859,861,863,872,876,893,  
898-899,905,913,915-917,919,927,936,944,947,949,960-961,967,971,974,980,  
982,984,1013,1018,1102-1103,1107,1124,1126,1139-1140,1157-1158,1161,1168-1169,  
1172,1174,1187-1188,1201,1204,1218,1237,1239,1246,1255,1258,1262,1270-1271,  
1273-1275,1278,1280,1286,1309,1312,1315,1317,1321,1323-1324,1329,1333,  
1626,1629,1632,1775,1817,1826,1834,1841,1845,1849,1851-1852,1857, and more.  
We have omitted from this list 14436 higher ports to keep the report size manageable.

Recurso: 200.61.169.79

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-21,23-316,318-349,351-381,383-560,562-613,615-834,836-963,965-1024,  
1026-1071,1073-1338,1340-1384,1386-1468,1470-1475,1477-1528,1530-1544,  
1546-1649,1651-1868,1870-2019,2021-2165,2167-2290,2292-2535,2537-3099,  
3101-3118,3120-3495,3497-3529,3531-3853,3855-4093,4095-4352,4354-4381,  
4383-4552,4554-4960,4962-5014,5016-5175,5177-5180,5182-5313,5315-5322,  
5324-5586,5588-5730,5732-6128,6130-6224,6226-6526,6528-7054,7056-7301,  
7303-7305,7307-7371,7373-7447,7449-7523,7525-7526,7528-7707,7709-7714,  
7716-8113,8115-8119,8121-8145,8147-8217,8219-8287,8289-9134,9136-9251,  
9253-9459,9461-9738,9740-9760,9762-10027,10029-10092,10094-10228,10230-10456,  
10458, and more.  
We have omitted from this list 54884 higher ports to keep the report size manageable.

Recurso: 200.61.169.94

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.  
  
Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,  
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,  
5551-5559,5561-5569,5571-5579,5581-5630,5632-5699,5701,5703-6013,6015-6128,  
6130-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535

Recurso: 190.220.133.1

Some of the ports filtered by the firewall are: 22, 23.  
  
Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
22-23

Recurso: 190.220.133.3

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.  
  
Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,  
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,  
5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,  
7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535

Recurso: 200.61.169.90

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-141,143-216,218-266,268-381,383-697,699-894,896-945,947-1067,1069-1250,  
1252-1381,1383-1415,1417-1456,1458-1609,1611-1936,1938-2025,2027-2305,  
2307-2752,2754-2824,2826-2987,2989-3090,3092-3107,3109-3147,3149-3310,  
3312-3704,3706-3896,3898-4627,4629,4631-4657,4659-4740,4742-4768,4770-4973,  
4975-5070,5072-5339,5341-5806,5808-5925,5927-6006,6008-6090,6092-6128,  
6130-6182,6184-6263,6265-6448,6450-6509,6511-6599,6601-6633,6635-6734,  
6736-6911,6913-7007,7009-7103,7105-7124,7126-7256,7258-7341,7343-7356,  
7358-7458,7460-7498,7500-7750,7752-7765,7767-8410,8412-8627,8629-8870,  
8872-9320,9322-9406,9408-9504,9506-9724,9726-9987,9989-10013,10015-10667,  
10669, and more.  
We have omitted from this list 54674 higher ports to keep the report size manageable.

Recurso: 190.220.133.25

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-355,357-381,383-995,997-1640,1642-2030,2032-2120,2122-2197,2199-2524,  
2526-3205,3207-3782,3784-3882,3884-3899,3901-3977,3979-4079,4081-4104,  
4106-4264,4266-4327,4329-4399,4401-4827,4829-5115,5117-5195,5197-5223,  
5225-5289,5291-5406,5408-5717,5719-5856,5858-5924,5926-6071,6073-6128,  
6130-6422,6424-6434,6436-6545,6547-6633,6635-6783,6785-7321,7323-7455,  
7457-7510,7512-7600,7602-7777,7779-8097,8099-8246,8248-8341,8343-8398,  
8400-8465,8467-8679,8681-8885,8887-9032,9034-9137,9139-9658,9660-10031,  
10033-10606,10608-10765,10767-10940,10942-11179,11181-11190,11192-11202,  
11204-11589,11591-11628,11630-11668,11670-11680,11682-11848,11850-12047,  
12049, and more.  
We have omitted from this list 53290 higher ports to keep the report size manageable.

Recurso: 200.61.169.71

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-124,126-381,383-420,422-430,432-523,525-801,803-1188,1190-1296,1298-1353,  
1355-1960,1962-1968,1970-1978,1980-2349,2351-2529,2531-2620,2622-2841,  
2843-3134,3136-3202,3204-3326,3328-3781,3783-4119,4121-4177,4179-4750,  
4752-5386,5388-5585,5587-5608,5610-5782,5784-5829,5831-6128,6130-6198,  
6200-6225,6227-6322,6324-6502,6504-6513,6515-6517,6519-6617,6619-6825,  
6827-6933,6935-7060,7062-7132,7134-7536,7538-7585,7587-7604,7606-7694,  
7696-8019,8021-8437,8439-8958,8960-8966,8968-9147,9149-9162,9164,9166-9430,  
9432-9460,9462-9521,9523-9727,9729-9761,9763-9793,9795-9946,9948-10001,  
10003-10098,10100-10119,10121-10206,10208-10639,10641-10688,10690-10771,  
10773, and more.  
We have omitted from this list 54569 higher ports to keep the report size manageable.

Recurso: 200.61.169.70

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-148,150-201,203-381,383-598,600-750,752-777,779-890,892-1023,1025-1099,  
1101-1298,1300-2154,2156-2166,2168-2220,2222-2554,2556-2688,2690-2776,  
2778-2794,2796-3258,3260-3488,3490-3510,3512-3592,3594-4063,4065-4185,  
4187-4244,4246-5046,5048-5367,5369-5423,5425-5599,5601-5741,5743-5831,  
5833-6019,6021-6043,6045-6098,6100-6128,6130-6244,6246-6399,6401-6595,  
6597-6633,6635-6637,6639-6642,6644-6781,6783-6798,6800-7175,7177-7383,  
7385-7422,7424-7677,7679-8161,8163-8711,8713-9070,9072-9278,9280-9420,  
9422-9539,9541-9719,9721-10262,10264-10337,10339-10429,10431-10464,10466-10785,  
10787-10922,10924-10932,10934-11175,11177-11243,11245-11544,11546-11568,  
11570, and more.  
We have omitted from this list 53771 higher ports to keep the report size manageable.

Recurso: 200.61.169.65

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.  
  
Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,  
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,  
5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,  
7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535

Recurso: 200.61.169.75

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports are probed.  
1-99,101-136,138-381,383-584,586-676,678-757,759-784,786-1117,1119-1235,  
1237-1327,1329-1836,1838-1969,1971-2111,2113-2208,2210-2213,2215-2277,  
2279-2375,2377-2624,2626-2812,2814-2878,2880-2915,2917-2971,2973-2987,  
2989-3346,3348-3371,3373-3568,3570-3626,3628-3770,3772-3963,3965-4101,  
4103-4318,4320-4531,4533-4574,4576-4610,4612-5140,5142-5468,5470-5684,  
5686-5926,5928-6128,6130-6241,6243-6468,6470-6507,6509-7476,7478-7570,  
7572-7582,7584-7616,7618-7707,7709-7864,7866-8056,8058-8224,8226-8352,  
8354-8501,8503-8929,8931-9159,9161-9256,9258-9326,9328-9974,9976-10149,  
10151-10557,10559-10799,10802-10916,10918-11314,11316-11539,11541-11626,  
11628, and more.  
We have omitted from this list 53714 higher ports to keep the report size manageable.

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

### Recursos Afectados

190.220.133.1  
190.220.133.4

### 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

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

Recurso: 190.220.133.4

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

# Pruebas de Intrusión

Durante las pruebas de intrusión del presente análisis, se detectó ...

# Conclusiones

En base a las vulnerabilidades detectadas y el análisis de las mismas, se puede determinar el siguiente nivel de severidad general, dada la existencia de **1** vulnerabilidad con dicha severidad.

|  |  |
| --- | --- |
| Nivel de Severidad | Critica |

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 |
| --- | --- |
| Aplicar parches o actualizar el software obsoleto o con vulnerabilidades conocidas a las versiones recomendadas por los fabricantes. | **#1 Hypertext Preprocessor (PHP) Multiple Vulnerabilities** |
| Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, RC2, MD5, RC4, SHA1), en favor de protocolos criptográficamente más fuertes. | **#2 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)** |
| **#4 TLS/SSL Weak Cipher Suites** |
| 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. | **#3 Insecure Direct Object Reference (IDOR)** |
| 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** |
| Eliminar o restringir el acceso al directorio .git en entornos productivos. | **#6 GIT Detected** |
| Asegurar que los mensajes de errores de acceso, o al intentar recuperar la contraseña, no permitan diferenciar si el usuario existe o no en la aplicación | **#7 User enumeration** |
| Deshabilitar, eliminar, o restringir el acceso a las páginas por defecto y archivos de configuración que pueden otorgar más información a un atacante. | **#8 Development configuration files** |
| 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. | **#9 Open TCP Services List** |
| **#11 Open UDP Services List** |
| Revisar la configuración del firewall aplicando el principio de mínimo privilegio, unificando respuestas a puertos no autorizados y complementando con monitoreo y registros de intentos de escaneo. | **#10 Firewall Detected** |

# 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

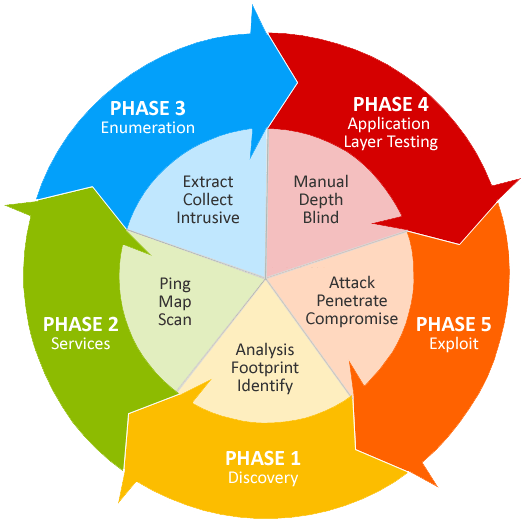
En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de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