



El futuro digital  
es de todos

Gobierno  
de Colombia  
MinTIC

# **Análisis de Vulnerabilidades *Unidad Nacional de Protección***

## **CSIRT Gobierno *Diciembre 2021***



## Aviso Legal

Todos los derechos reservados 2021

Este documento contiene información confidencial y propietaria la cual es de uso exclusivo de la Unidad Nacional de Protección. La reproducción o uso no autorizado de este documento está totalmente prohibido.

Las pruebas de análisis de vulnerabilidades revelan las vulnerabilidades relevantes conocidas a la fecha de este reporte. Debido a que nuevas vulnerabilidades son encontradas y estas generan nuevas amenazas de seguridad, se recomienda que se realicen evaluaciones de seguridad después de cualquier cambio importante en la configuración del sistema y periódicamente en intervalos entre 6 o 12 meses como máximo.

## LIMITACIONES A LA DIVULGACIÓN Y USO DE ESTE INFORME

Este informe contiene la información relativa a las posibles vulnerabilidades del sitio(s) web de la Entidad. CSIRT Gobierno recomienda que sean tomadas precauciones especiales para proteger la confidencialidad de este documento y la información contenida en este. CSIRT Gobierno ha mantenido y asegurado una copia de este informe para consulta por parte de la entidad. La Evaluación de la seguridad es un proceso incierto, basado en las experiencias, la información actualmente disponible y las amenazas conocidas. Se debe entender que todos los sistemas de información, por su naturaleza dependen de los seres humanos y son vulnerables en cierto grado.

Por lo tanto, mientras que CSIRT Gobierno considera que las vulnerabilidades de seguridad más importantes de los sistemas analizados se han identificado, no existe ninguna garantía de que en la ejecución de cualquier ejercicio de esta naturaleza se logren identificar todas las posibles vulnerabilidades o se propongan todas las recomendaciones exhaustivas y viables operativamente para mitigar los riesgos asociados. De igual forma, el análisis establecido aquí se basa en las tecnologías y las amenazas conocidas a la fecha de este informe. Dado que las tecnologías y los riesgos cambian con el tiempo, las vulnerabilidades asociadas con la operación de los sistemas de Artesanías de Colombia descritas en este informe, así como las acciones necesarias para reducir la exposición a estas vulnerabilidades, también van a cambiar. CSIRT Gobierno no tiene ningún compromiso de complementar o actualizar este informe sobre la base del cambio de circunstancias o hechos de los cuales CSIRT Gobierno tenga conocimiento después de la fecha del presente informe sin un acuerdo por escrito que lo especifique así, para realizar un análisis complementario o actualizado.

Este informe se podrá recomendar a la Unidad Nacional de Protección, acciones a seguir para una posible remediación o mitigación de las vulnerabilidades encontradas, CSIRT Gobierno basa estas recomendaciones a partir de su experiencia previa, sin embargo, no se puede y no debe garantizar que una determinada acción funcionará. Este informe fue preparado por CSIRT Gobierno para el uso y beneficio exclusivo de la unidad Nacional de Protección y se considera **información confidencial**.

## Contenido

INTRODUCCIÓN.....	5
ALCANCE .....	5
OBJETIVO.....	5
METODOLOGÍA DE CLASIFICACIÓN.....	6
INFORME EJECUTIVO .....	7
INFORME TÉCNICO.....	9
Listado de puertos abiertos .....	9
Análisis Cabeceras HTTP Aplicaciones Web.....	10
1. VULNERABILIDADES IDENTIFICADAS .....	12
1.1 VULNERABILIDADES DE CRITICIDAD MEDIO .....	12
1.1.1 Uso de los Protocolos TLS 1.0 TLS 1.1 obsoletos .....	12
1.1.2 Librerías JavaScript Vulnerables .....	14
1.1.3 Algoritmos de cifrado débil (CBC Ciphers, Triple Des/IDEA).....	16
2.1 VULNERABILIDADES DE CRITICIDAD BAJO .....	19
2.1.1 Sitio vulnerable a ClickJacking.....	19
2.1.2 Ausencia de cabecera HSTS .....	21
2.1.3 Falta de mecanismos de protección frente a ataques de fuerza bruta sobre el login .....	23
METODOLOGÍA .....	27
DEFINICIONES.....	27

## INTRODUCCIÓN

De acuerdo con el catálogo de servicios ofrecido por CSIRT Gobierno y la solicitud realizada por la Unidad Nacional de Protección, se realizaron pruebas de análisis de vulnerabilidades sobre el/los sitio(s) web, con el propósito de identificar los problemas de seguridad y sus servicios asociados identificados.

Durante las pruebas se descubren las vulnerabilidades, su nivel de riesgo, y se generan recomendaciones que permitan a la Unidad Nacional de Protección realizar la remediación de estas. En cada sección de este informe se detallan los aspectos importantes de la forma en que un atacante podría utilizar la vulnerabilidad para comprometer y obtener acceso no autorizado a información sensible. Se incluyen además directrices que al ser aplicadas mejoraran los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

## ALCANCE

Las pruebas se realizaron sobre la siguientes URLs.

- Portal – <https://unp.gov.co>
- Correo – <https://correo.unp.gov.co/owa>

## OBJETIVO

Detectar las vulnerabilidades tecnológicas existentes en el/los sitio(s) web reportados, generar un informe de estas y emitir recomendaciones con el fin de que la Unidad Nacional de Protección las tenga presentes y pueda llegar a mitigar el riesgo existente sobre su infraestructura tecnológica.

El análisis de vulnerabilidades realizado tiene los objetivos específicos siguientes:

- Comprobación del estado de la seguridad en los servicios, mediante el descubrimiento de vulnerabilidades existentes que puedan comprometer la seguridad en términos de Confidencialidad de la información, la Integridad de los datos y de la Disponibilidad de los servicios ofrecidos.
- Posibles puntos de mejora para corregir o contrarrestar el impacto que podrían tener la explotación de las vulnerabilidades.

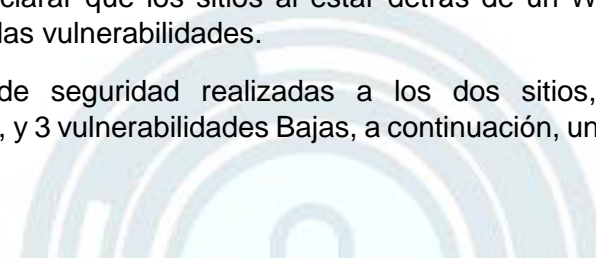
## METODOLOGÍA DE CLASIFICACIÓN

La escala de calificación de las vulnerabilidades que se utilizó es la indicada por la CVE (Common Vulnerabilities and Exposures), estándar de clasificación y calificación de vulnerabilidades de aceptación mundial. Las vulnerabilidades pueden ser clasificadas en Críticas, Altas, Medias, Bajas o Informativas de acuerdo con su nivel de explotabilidad en cuanto a código malicioso disponible y dificultad de ejecutarlo.

## INFORME EJECUTIVO

Como resumen y a la vista de los resultados del análisis de seguridad de los sitios web evaluados, se han mantenido buenas prácticas de seguridad en varios aspectos, se puede afirmar que la aplicación posee una seguridad buena, dado que no se hallaron vulnerabilidades críticas y altas, no obstante, se debe aclarar que los sitios al estar detrás de un WAF o CDN no es posible identificar por completo las vulnerabilidades.

Durante las pruebas de seguridad realizadas a los dos sitios, se han identificado, 6 vulnerabilidades Medias, y 3 vulnerabilidades Bajas, a continuación, un resumen de los hallazgos identificados.



### Vulnerabilidades por criticidad

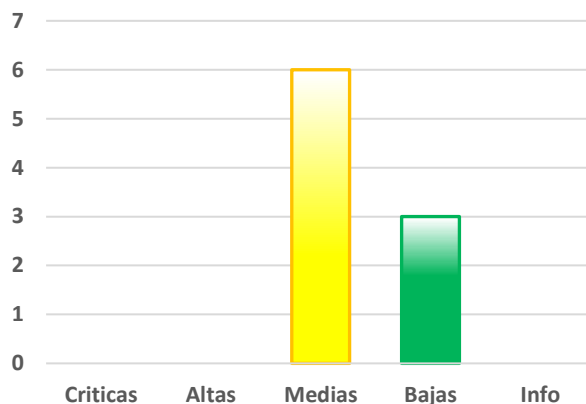


Ilustración 1 - Vulnerabilidades encontradas por criticidad.

Se identifican un total de un sitio con una librería jquery en una version obsoleta, usando cifrado débil y utilización de los protocolos TLS 1.0 Y TLS 1.1 que tienen vulnerabilidades conocidas, falta de configuración en parámetros de seguridad en las cookies.

Se consiguen identificar las aplicaciones utilizadas y algunas versiones de las mismas, esto permite que un atacante recolecte información relevante, que puede utilizar para realizar un ataque dirigido.

Tras las pruebas realizadas se muestra una tabla informativa clasificando las vulnerabilidades encontradas, en cada sitio.

Sitio	Vulnerabilidades	Criticidad
https://www.unp.gov.co	Algoritmos de cifrado débil (CBC Ciphers)	Media
	Librería JavaScript Vulnerable	Media
	Sitio vulnerable a ClickJacking	Baja
	Algoritmos de cifrado débil (CBC Ciphers, Triple Des/IDEA)	Media
https://correo.unp.gov.co/owa	Uso de los Protocolos TLS 1.0 TLS 1.1 obsoletos	Media
	Algoritmos de cifrado débil (CBC Ciphers)	Media
	Algoritmos de cifrado débil (CBC Ciphers, Triple Des/IDEA)	Media
	Ausencia de cabecera HSTS	Baja
	Falta de mecanismos de protección frente a ataques de fuerza bruta sobre el login	Baja

Tabla 1 – Resumen de vulnerabilidades.

## RECOMENDACIONES

A continuación, se indican una serie de recomendaciones generales para resolver y prevenir vulnerabilidades como las encontradas durante las pruebas realizadas.

- Dentro de lo posible mantener actualizadas las aplicaciones utilizadas en el servidor con los últimos parches de seguridad liberados por el fabricante.
- Ofuscar el código de la página para que no pueda ser visto y/o modificado.
- Habilitar el redireccionamiento por HTTPS.
- Se recomienda implementar ajustar los flags del encabezado HTTP con el fin de mitigar posibles ataques.
- Cambiar los tipos de cifrado utilizados en el sitio ya que los usados actualmente cuentan con vulnerabilidades que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información.
- Realizar un plan de remediación de las vulnerabilidades encontradas.
- Realizar pruebas de seguridad periódicas, no sólo para asegurar que las vulnerabilidades detectadas en auditorías anteriores han sido subsanadas, sino también para detectar nuevas vulnerabilidades que hayan podido aparecer debido a los cambios en las aplicaciones y/o



infraestructura, así como la multitud de vulnerabilidades que se descubren a diario en sistemas operativos y software en general.

## INFORME TÉCNICO

Como parte de las pruebas de seguridad de aplicaciones web es necesario localizar aquellos puntos de la red del cliente que contienen servicios web disponibles al público.

Para localizar estos puntos de entrada se ha realizado un escaneo de puertos, en busca de dichos servicios, se han podido detectar los siguientes:

### Listado de puertos abiertos

Sitio	Puerto TCP	Servicio
https://www.unp.gov.co/ IP 200.91.240.163	80/TCP	http
	443/TCP	ssl/http
https://correo.unp.gov.co/owa IP 200.91.233.115	25/TCP	smtp Microsoft Exchange
	80/TCP	http Microsoft IIS httpd 10.0
	143/TCP	imap Microsoft Exchange 2007
	443/TCP	ssl/http Microsoft IIS httpd 10.0
	587/TCP	smtp Microsoft Exchange
	993/TCP	ssl/imap Microsoft Exchange 2007-2010

Tabla 2 – Identificación de puertos abiertos.


## Análisis Cabeceras HTTP Aplicaciones Web

Las cabeceras HTTP son la parte central de esas solicitudes y respuestas HTTP, y transportan información sobre el navegador cliente, la página solicitada, el servidor y más.

A continuación, se expone el resultado de los encabezados para cada uno de los sitios analizados, se debe tener en cuenta que se mide en una escala desde A+ siendo el más seguro, y F el menos seguro.

- <https://www.unp.gov.co/>

En análisis realizado se evidencio que las cabeceras están con una calificación F.

Security Report Summary	
	Redirect: <a href="https://www.unp.gov.co/">Click here</a> to follow the redirect to <a href="https://www.unp.gov.co/">https://www.unp.gov.co/</a> .
	Site: <a href="http://www.unp.gov.co/">http://www.unp.gov.co/</a> - (Scan again over https)
	IP Address: 190.145.207.80
	Report Time: 31 Dec 2021 06:30:16 UTC
	Headers: <span>✖ Content-Security-Policy</span> <span>✖ X-Frame-Options</span> <span>✖ X-Content-Type-Options</span> <span>✖ Referrer-Policy</span> <span>✖ Permissions-Policy</span>
	Warning: Grade capped at A, please see warnings below.

A continuación, se muestran las cabeceras que se recomiendan ajustar con el fin de que el sitio sea menos vulnerable:

Missing Headers	
<b>Strict-Transport-Security</b>	<a href="#">HTTP Strict Transport Security</a> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
<b>Content-Security-Policy</b>	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<b>X-Frame-Options</b>	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
<b>X-Content-Type-Options</b>	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
<b>Referrer-Policy</b>	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<b>Permissions-Policy</b>	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.

- <https://correo.unp.gov.co/owa>

En análisis realizado se evidencio que las cabeceras están con una calificación F.

### Security Report Summary



<b>Redirect:</b>	<a href="https://correo.unp.gov.co/owa/auth/logon.aspx?url=https%3a%2f%2fcorreo.unp.gov.co%2fowa&amp;reason=0">Click here</a> to follow the redirect to <a href="https://correo.unp.gov.co/owa/auth/logon.aspx?url=https%3a%2f%2fcorreo.unp.gov.co%2fowa&amp;reason=0">https://correo.unp.gov.co/owa/auth/logon.aspx?url=https%3a%2f%2fcorreo.unp.gov.co%2fowa&amp;reason=0</a> .
<b>Site:</b>	<a href="https://correo.unp.gov.co/owa">https://correo.unp.gov.co/owa</a>
<b>IP Address:</b>	190.145.207.72
<b>Report Time:</b>	31 Dec 2021 06:35:31 UTC
<b>Headers:</b>	<span>✘ Strict-Transport-Security</span> <span>✘ Content-Security-Policy</span> <span>✘ X-Frame-Options</span> <span>✘ X-Content-Type-Options</span> <span>✘ Referrer-Policy</span> <span>✘ Permissions-Policy</span>

A continuación, se muestran las cabeceras que se recomiendan ajustar con el fin de que el sitio sea menos vulnerable:

### Missing Headers

<b>Strict-Transport-Security</b>	<a href="#">HTTP Strict Transport Security</a> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
<b>Content-Security-Policy</b>	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<b>X-Frame-Options</b>	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
<b>X-Content-Type-Options</b>	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
<b>Referrer-Policy</b>	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<b>Permissions-Policy</b>	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.

**CSIRT**

## 1. VULNERABILIDADES IDENTIFICADAS

### 1.1 VULNERABILIDADES DE CRITICIDAD MEDIO

#### 1.1.1 Uso de los Protocolos TLS 1.0 TLS 1.1 obsoletos

Estado	Activa
Fecha de identificación	13/12/2021
Fecha de certificación	
Activos afectados	<a href="https://correo.unp.gov.co/owa">https://correo.unp.gov.co/owa</a>
Criticidad	Media
Impacto	4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Prueba	Manual
Código	CVE-2014-3566   CVE-2014-8730
Plataforma	Web

#### Descripción

El servidor admite conexiones SSL utilizando TLSv1.0 y TLSv1.1 de los protocolos, los cuales presentan una serie de debilidades como por ejemplo Poodle que podría provocar que la comunicación entre el cliente y el servidor no sea segura.

Un atacante puede intentar forzar (mediante Man-in-the-middle) a que la comunicación entre cliente y servidor se realice utilizando esta versión protocolo, lo cual dejaría dicha comunicación expuesta

#### Impacto

El uso de algoritmos de cifrado con vulnerabilidades publicadas puede provocar que la comunicación entre el cliente y el servidor no sea segura. Llegando a ser posible interceptar dicha comunicación para obtener información sensible o incluso modificarla.

#### Evidencia

Ministerio de Tecnologías de la Información y las Comunicaciones  
Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13  
Código Postal: 111711. Bogotá, Colombia  
CSIRT Tel: +57 018000910742 Opción 3



En la siguiente captura de pantalla se puede observar como el protocolo TLS v1.0 y TLS v1.1 está habilitado y utilizado por los sitios web.

```

-->> 190.145.207.72:443 [correo.unp.gov.co] <<--
rDNS (190.145.207.72): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 h2, http/1.1 (offered)

Testing cipher categories

NULL ciphers (no encryption)           not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)          not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA              offered
Obsoleted CBC ciphers (AES, ARIA etc.)  offered
Strong encryption (AEAD ciphers) with no FS offered (OK)
Forward Secrecy strong encryption (AEAD ciphers) offered (OK)

```

Ilustración 2 Protocolos aceptados por el servidor de correo UNP

### Mitigación / Solución / Recomendación

Es necesario configurar las opciones SSL del servidor Web para deshabilitar los TLSv1.0 y TLSv1.1 del protocolo SSL:

Es necesario modificar claves del registro para establecer los algoritmos soportados. Sirva como ejemplo de configuración la siguiente:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

Por otro lado, es recomendable habilitar "forward secrecy" y "TLS\_FALLBACK\_SCSV"

Ministerio de Tecnologías de la Información y las Comunicaciones  
Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13  
Código Postal: 111711, Bogotá, Colombia  
CSIRT Tel: +57 018000910742 Opción 3



Por último, utilizar siempre la última versión disponible de TLS.

## Referencias

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html>

### 1.1.2 Librerías JavaScript Vulnerables

Estado	Activa
Fecha de identificación	9/12/2021
Fecha de certificación	
Activos afectados	<a href="https://www.unp.gov.co/">https://www.unp.gov.co/</a>
Criticidad	<b>Media</b>
Impacto	4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Prueba	Manual
Código	CVE-2015-9251, CVE-2019-11358, CVE-2015-9251
Plataforma	Web



### Mitigación / Solución / Recomendación

Se recomienda actualizar el software haciendo uso de los parches de seguridad disponibles para el producto, con el fin de poder corregir las vulnerabilidades detectadas.

### Referencias

[https://www.cvedetails.com/cve-details.php?cve\\_id=CVE-2015-9251](https://www.cvedetails.com/cve-details.php?cve_id=CVE-2015-9251)

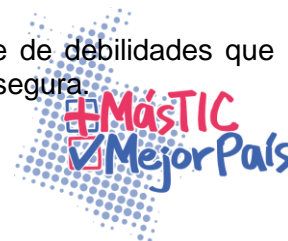
### 1.1.3 Algoritmos de cifrado débil (CBC Ciphers, Triple Des/IDEA)

Estado	Activa
Fecha de identificación	9/12/2021
Fecha de certificación	
Activos afectados	<a href="https://www.unp.gov.co">https://www.unp.gov.co</a> , <a href="https://correo.unp.gov.co/owa">https://correo.unp.gov.co/owa</a>
Criticidad	Media
Impacto	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Prueba	Manual
Código	CWE-16; OWASP 2013-A5; OWASP 2017-A6
Plataforma	Web

### Descripción

La configuración del servicio SSL en el servidor Web presenta una serie de debilidades que podrían provocar que la comunicación entre el cliente y el servidor no sea segura.

Ministerio de Tecnologías de la Información y las Comunicaciones  
Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13  
Código Postal: 111711. Bogotá, Colombia  
CSIRT Tel: +57 018000910742 Opción 3





El servicio SSL presente en el servidor tiene habilitados algoritmos de cifrado considerados como débiles o con vulnerabilidades publicadas. Un atacante puede intentar forzar (mediante Man-in-the-middle) a que la comunicación entre cliente y servidor se realice con un algoritmo débil, lo cual dejaría dicha comunicación expuesta.

## Impacto

El uso de algoritmos de cifrado considerados débiles o con vulnerabilidades publicadas pueden provocar que la comunicación entre el cliente y el servidor no sea segura. Llegando a ser posible interceptar dicha comunicación para obtener información sensible o incluso modificarla.

Por ejemplo, un atacante podría intentar forzar (mediante Man-in-the-middle) a que la comunicación entre cliente y servidor se realice con un algoritmo débil, lo cual dejaría dicha comunicación expuesta.

## Evidencia

En este caso simplemente se ha comprobado cuáles eran los protocolos criptográficos soportados por el servidor web y verificado si estaban afectados por las distintas vulnerabilidades públicas que afectan a dichos protocolos.

Algoritmos débiles habilitados (uso de CBC, algoritmo con vulnerabilidades publicadas:

```
-->> 190.145.207.80:443 (www.unp.gov.co) <<--
rDNS (190.145.207.80): --
Service detected: Couldn't determine what's running on port 443, assuming no HTTP service => skipping all HTTP checks

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 not offered

Testing cipher categories
NULL ciphers (no encryption)          not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)         not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES ciphers / IDEA             not offered
Obsoleted CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) with no FS offered (OK)
Forward Secrecy strong encryption (AEAD ciphers) offered (OK)
```

Ilustración 4 tipo de cifrado débil sitio unp

```
-->> 190.145.207.72:443 (correo.unp.gov.co) <<--
rDNS (190.145.207.72): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 h2, http/1.1 (offered)

Testing cipher categories

NULL ciphers (no encryption)                not offered (OK)
Anonymous NULL Ciphers (no authentication)  not offered (OK)
Export ciphers (w/o ADH+NULL)                not offered (OK)
Low 64 Bit w/ DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA                    offered
Obsoleted CBC ciphers (AES, ARIA etc.)       offered
Strong encryption (AEAD ciphers) with no FS  offered (OK)
Forward Secrecy strong encryption (AEAD ciphers) offered (OK)
```

Ilustración 5 tipo de cifrado débil sitio correo

### Mitigación / Solución / Recomendación

Es necesario configurar las opciones SSL del servidor Web para deshabilitar los algoritmos de cifrado débiles:

Es necesario modificar claves del registro para establecer los algoritmos soportados, como, por ejemplo:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
```

Sustituir los conjuntos de cifrado identificados como “de bajo cifrado” por algoritmos más robustos, por ejemplo, SHA256 o uno de mayor fortaleza. Son considerados como cifrados de nivel alto aquellos que superan longitudes mayores a 128 bits o no tienen vulnerabilidades publicadas.

### Referencias

[https://www.owasp.org/index.php/Testing\\_for\\_Weak\\_SSL/TSL\\_Ciphers,\\_Insufficient\\_Transport\\_Layer\\_Protection\\_\(OWASP-EN-002\)](https://www.owasp.org/index.php/Testing_for_Weak_SSL/TSL_Ciphers,_Insufficient_Transport_Layer_Protection_(OWASP-EN-002))

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808>

Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13  
Código Postal: 111711, Bogotá, Colombia  
CSIRT Tel: +57 018000910742 Opción 3



Buenas prácticas de despliegue o endurecimiento del cifrado en servidores Web:

<https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/>

## 2.1 VULNERABILIDADES DE CRITICIDAD BAJO

### 2.1.1 Sitio vulnerable a ClickJacking

Estado	Activa
Fecha de identificación	9/12/2021
Fecha de certificación	
Activos afectados	<a href="https://www.unp.gov.co/">https://www.unp.gov.co/</a>
Criticidad	Baja
Impacto	3.5 (AV:N/AC:M/Au:S/C:P/I:N/A:N)
Prueba	Manual y Automática
Código	CAPEC-103   CWE-693
Plataforma	Web

#### Descripción

La aplicación permite cargar sus páginas web dentro de un marco HTML de aplicaciones externas al dominio legítimo. El ataque consiste en engañar a un usuario confiado haciéndole pulsar sobre un contenido distinto al que realmente está percibiendo:

Caso 1): Un atacante puede definir una página HTML que contenga un marco de tipo iframe dónde se carga una página legítima de la compañía, y establece en un segundo marco transparente y superpuesto al primero. El usuario interactuará sin saberlo (mediante clicks del ratón o pulsaciones de teclado) con el marco transparente (no con la página legítima), y ejecutará sin ser consciente de ello cualquier código ideado por el atacante (por ejemplo, si la página legítima es un formulario de acceso, el atacante podría programar el envío de dichas credenciales a una dirección propia).

Caso 2): Un atacante puede definir una página HTML con un marco de tipo iframe transparente en el que carga una página legítima de la compañía (no será visible al estar en el marco transparente), mientras que en un segundo marco en segundo plano (pero visible al ser el

primer marco transparente) carga una página gancho que incite al usuario legítimo a interactuar con ella. Sin saberlo las interacciones las estará ejecutando sobre el marco transparente que contiene la aplicación, pudiendo resultar en la ejecución de operaciones en beneficio del atacante.

## Impacto

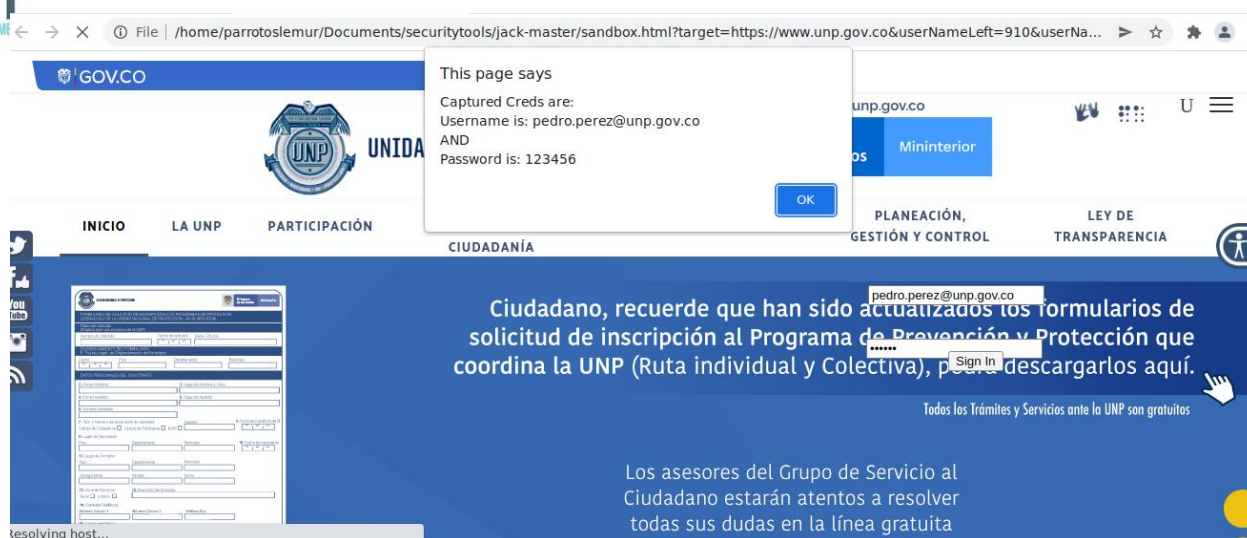
Mediante este tipo o técnica de ataque, es posible para un atacante burlar defensas contra ataques del tipo Cross-Site Request Forgery, resultando en la ejecución de acciones no autorizadas. En este caso en concreto, sería posible engañar a un usuario legítimo para que introduzca sus credenciales de acceso en un falso formulario controlado por el atacante.

## Evidencia

Se intento montar el sitio en un iframe pero aparece error de conexión, con este se confirma que el sitio no es vulnerable.



Ilustración 6 Se carga sitio de UNP en un iframe exitosamente.



**Ilustración 7** Sitio web UNP identificado como vulnerable a **ClickJacking**

### Mitigación / Solución / Recomendación

Para evitar ataques con marcos de tipo iframe de manera eficaz, la aplicación debe devolver una cabecera de respuesta con el parámetro X-Frame-Options y de valor DENY, para evitar que todo vaya en el mismo marco, o el valor SAMEORIGIN para permitir que se enmarque solamente las páginas del mismo origen que la respuesta en sí misma. Tenga en cuenta que la cabecera SAMEORIGIN se puede omitir parcialmente si la propia aplicación puede llamar a marcos de sitios web que no son de confianza.

### Referencias

- <https://www.owasp.org/index.php/Clickjacking>
- [https://www.owasp.org/index.php/Clickjacking\\_Defense\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet)
- <https://capec.mitre.org/data/definitions/103.html>

### 2.1.2 Ausencia de cabecera HSTS

Estado	Activa
Fecha de identificación	9/12/2021
Fecha de certificación	
Activos afectados	<a href="https://correo.unp.gov.co/owa">https://correo.unp.gov.co/owa</a>
Criticidad	Baja
Impacto	3.3 (AV:A/AC:L/Au:N/C:P/I:N/A:N)
Prueba	Manual
Código	OTG-CONFIG-007
Plataforma	Web

### Descripción

HTTP Strict Transport Security (HSTS) es una característica de seguridad que permite a una aplicación web informar al navegador que solo deben comunicarse utilizando HTTPS, en lugar de HTTP. Esto permite protegerse de ataques de tipo Man-In-The-Middle ya que en caso de que un atacante obligue a usar HTTP sin cifrar para poder inspeccionar el tráfico, el navegador web no lo permitirá. HSTS también imposibilita navegar si se ha establecido HSTS y se intentan hacer peticiones a través de un certificado SSL inválido. Esta característica ya está siendo ampliamente soportada por la mayoría de navegadores actuales.

### Impacto

Un atacante podría realizar ataques de tipo Man-In-The-Middle (MitM) contra un usuario víctima y obtener datos sensibles, como credenciales, o cuentas bancarias.

### Evidencia

Durante la ejecución de las pruebas se identificó que las respuestas del servidor web no cuenta con la cabecera de seguridad HSTS.

```
Testing HTTP header response @ "/owa"  
  
HTTP Status Code      302 Found, redirecting to "https://correo.unp.gov.co/owa/auth/logon.aspx?url=https%3a%2f%2fcorreo.unp.  
gov.co%2fowa&reason=0"  
HTTP clock skew      -1 sec from localtime  
Strict Transport Security not offered  
Public Key Pinning   --  
Server banner        Microsoft-IIS/10.0  
Application banner   X-Powered-By: ASP.NET  
Cookie(s)            (none issued at "/owa") -- maybe better try target URL of 30x  
Security headers     --  
Reverse Proxy banner --
```

Ilustración 8 sin cabecera HSTS

### Mitigación / Solución / Recomendación

Para implementar HSTS en la aplicación, debe establecerse en la configuración del servidor web donde esté alojado el servicio.

Por ejemplo, para configurar HSTS en Apache, debe cargarse el módulo mod\_headers y añadir la siguiente directiva en el fichero .htaccess:

```
<IfModule mod_headers.c>  
    Header set Strict-Transport-Security: max-age=10886400  
</IfModule>
```

### Referencias

[https://www.owasp.org/index.php?title=Test\\_HTTP\\_Strict\\_Transport\\_Security\\_%28OTG-CONFIG-007%29](https://www.owasp.org/index.php?title=Test_HTTP_Strict_Transport_Security_%28OTG-CONFIG-007%29)

### 2.1.3 Falta de mecanismos de protección frente a ataques de fuerza bruta sobre el login

Estado	Activa
Fecha de identificación	9/12/2021
Fecha de certificación	
Activos afectados	<a href="https://correo.unp.gov.co/owa">https://correo.unp.gov.co/owa</a>
Criticidad	Baja
Impacto	3.5 (AV:N/AC:M/Au:S/C:P/I:N/A:N)
Prueba	Manual
Código	CWE-287   WASC-011   OWASP-AT-004
Plataforma	Web

### Descripción

El servicio identificado permite realizar un ataque de fuerza bruta en el inicio de sesión, pues no existe ningún tipo de restricción en la forma de autenticarse, pudiendo realizar múltiples intentos de conexión consecutivos. Estos ataques pueden ser básicamente:

- Verticales: se fija el nombre del usuario y se varía la contraseña.
- Horizontales: se fija una contraseña, y se varía el nombre de usuario
- Diagonales: se varían tanto el usuario como la contraseña.

### Impacto

En caso de que un atacante averiguara la contraseña de un usuario, el atacante tendría acceso a la interfaz de administración del sitio web pudiendo modificar su contenido a voluntad, comprometiendo de esa manera la integridad e incluso la disponibilidad del sitio.

### Evidencia

Es posible realizar ataques de fuerza bruta a los paneles de Login detectados, ya que no existe mecanismo que impida este tipo de ataque. El panel de login es:

<https://correo.unp.gov.co/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fcorreo.unp.gov.co%2fowa>



Para demostrar la posibilidad de ejecutar ataques de fuerza bruta, se han intentado ataques de averiguación de contraseñas basadas en diccionario y por fuerza bruta sobre el panel de logueo detectado. La siguiente imagen muestra como se ha podido ejecutar el ataque sin que la aplicación haya interrumpido el ataque de ninguna forma:

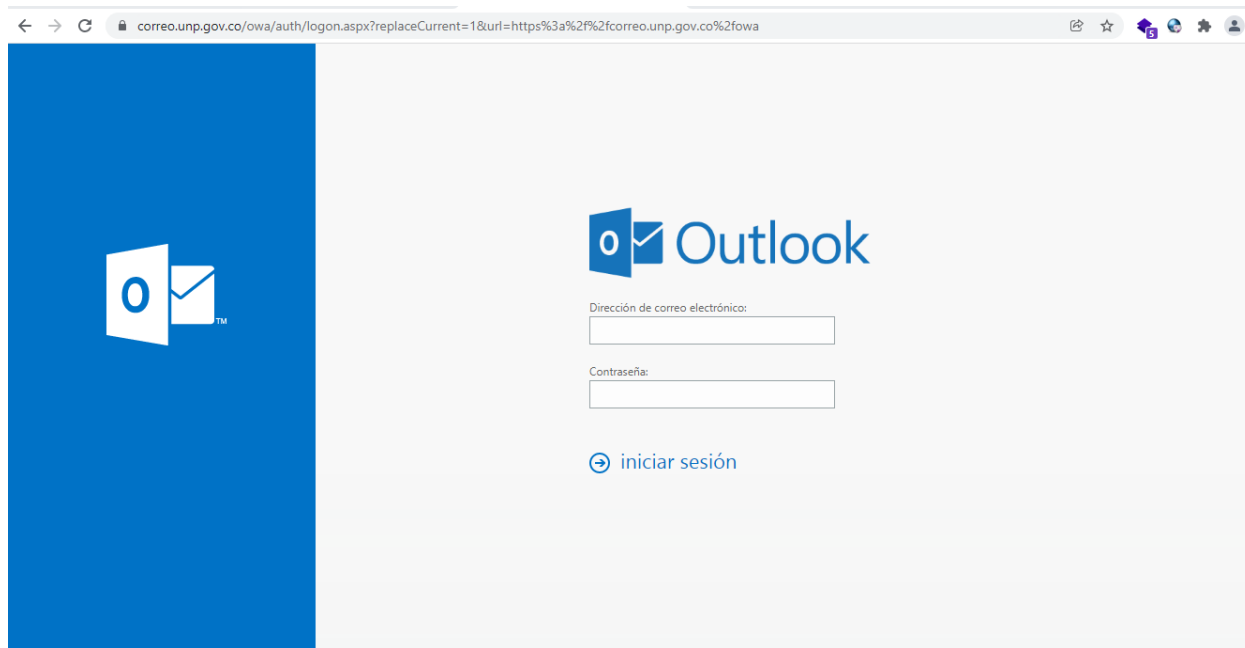
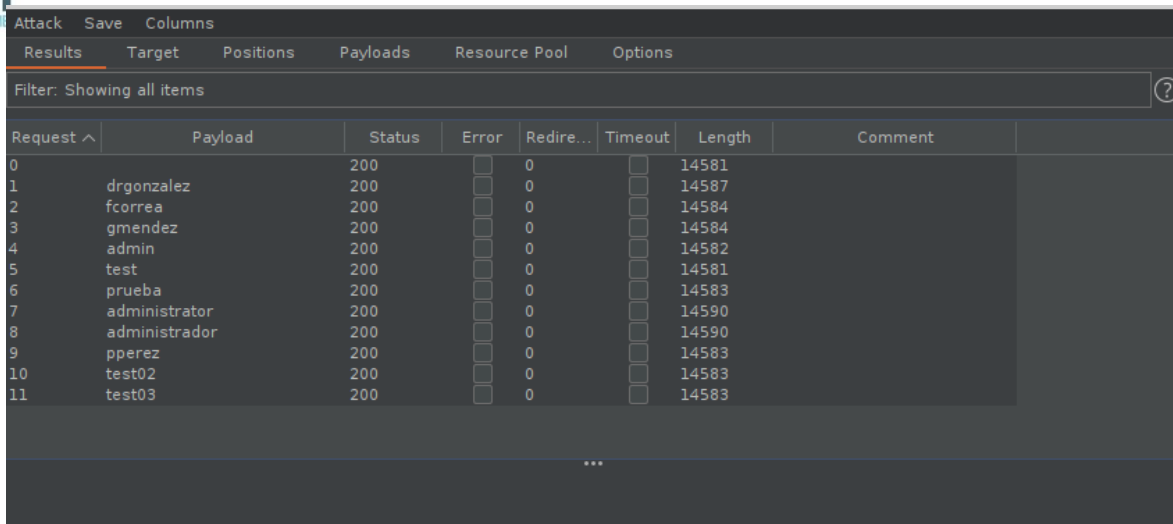


Ilustración 9 entrada login sitio correo



Request ^	Payload	Status	Error	Redire...	Timeout	Length	Comment
0		200	<input type="checkbox"/>	0	<input type="checkbox"/>	14581	
1	drgonzalez	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14587	
2	fcorrea	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14584	
3	gmendez	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14584	
4	admin	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14582	
5	test	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14581	
6	prueba	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14583	
7	administrator	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14590	
8	administrador	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14590	
9	pperez	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14583	
10	test02	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14583	
11	test03	200	<input type="checkbox"/>	0	<input type="checkbox"/>	14583	

Ilustración 10 Ataque de fuerza bruta no impedido

### Mitigación / Solución / Recomendación

Es necesario fijar un mecanismo de proyección para minimizar el riesgo de este tipo de ataques:

1. Fijar un número máximo de intentos de conexión consecutivos, bloqueando el acceso durante un tiempo prudencial (1 hora) en caso de detectar un ataque.
2. Implementando un mecanismo captcha.
3. Utilizar autenticación fuerte

Si no es posible implementar alguno de estos mecanismos, se pueden implementar alternativas que dificulten la posibilidad de éxito del ataque:

4. Bloquear una contraseña tras varios intentos fallidos seguidos de inicio de sesión (prevención de ataques verticales)
5. Utilizar cadenas aleatorias (o semi-aleatorias) de 12 o más caracteres como nombres de usuario (prevención de ataques horizontales)
6. Formular una pregunta adicional como parte de las credenciales de acceso, como por ejemplo nombre de usuario, apellido (o NIF, o algún otro dato) y contraseña.

Utilizar un motor de riesgo, el cual utiliza muchas variables relacionadas con el inicio de sesión (hora, geolocalización, fingerprint del equipo cliente) para determinar el nivel de riesgo de un intento de acceso, y si dicho riesgo supera un umbral predeterminado se le formula al usuario un reto/pregunta cómo puede ser que introduzca un código enviado por SMS a su teléfono móvil.

## Referencias

[https://www.owasp.org/index.php/Brute\\_force\\_attack](https://www.owasp.org/index.php/Brute_force_attack)

## METODOLOGÍA

Para la realización de las pruebas de seguridad, se utilizó como base las principales metodologías de pruebas de seguridad como:

**OSSTMM** (*Open Source Security Testing Methodology Manual*) – Metodología General de Análisis de Seguridad.

**OWASP** (*Open Web Application Security Project*) – Guía de realización de pruebas de seguridad en aplicaciones Web.

## DEFINICIONES

**Vulnerabilidad:** Un error, falla, debilidad, o la exposición de una aplicación, sistema, dispositivo o servicio que podría dar lugar a un incumplimiento de la confidencialidad, integridad o disponibilidad.

**Amenaza:** La frecuencia o probabilidad de que un hecho dañino se produzca.

**Riesgo:** Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.

**Activo:** Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La empresa asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

**Confidencialidad:** Garantía de que únicamente accederán a la información los elementos autorizados para ello, y que dichos elementos no van a convertir esa información en disponible para otras entidades.

**Integridad:** Garantía de que la información únicamente puede ser modificada por elementos autorizados asegurando métodos de proceso exactos y completos.

**Disponibilidad:** Garantía de que la información y los activos relacionados deben estar accesibles a elementos autorizados en tiempo, modo y lugar adecuado.



El futuro digital  
es de todos

Gobierno  
de Colombia  
MinTIC

En caso de ser necesario puede comunicarse con CSIRT Gobierno por medio de los siguientes canales:



[Csirtgob@mintic.gov.co](mailto:Csirtgob@mintic.gov.co)



018000910742 Opción 2.



CSIRT

Ministerio de Tecnologías de la Información y las Comunicaciones  
Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13  
Código Postal: 111711. Bogotá, Colombia  
CSIRT Tel: +57 018000910742 Opción 3

