telecom

BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Análisis de Vulnerabilidades

Informe Técnico

08/09/2025

Tabla de Contenidos

Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Análisis de Vulnerabilidades** sobre la infraestructura de **BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **07/07/2025** y el **11/07/2025**.

Alcance

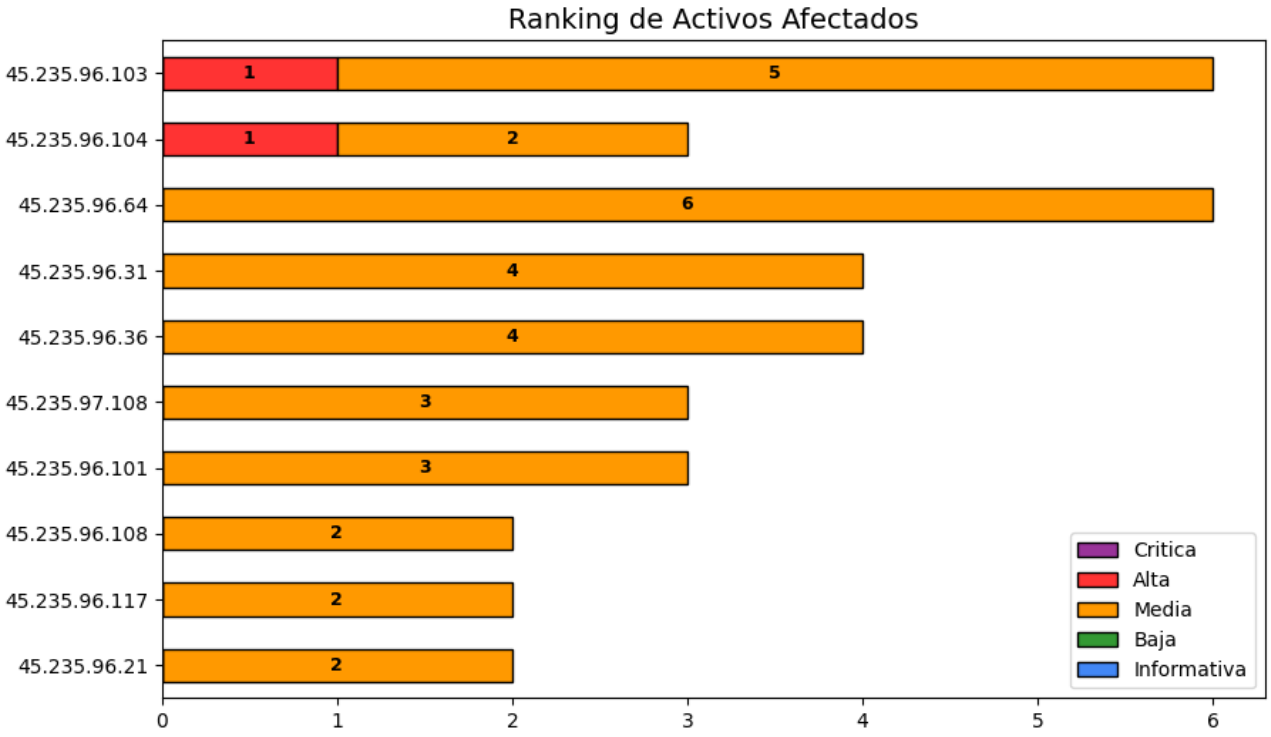
Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Análisis de Vulnerabilidades.

45.235.96.101
45.235.96.103
45.235.96.104
45.235.96.108
45.235.96.109
45.235.96.110
45.235.96.111
45.235.96.117
45.235.96.118
45.235.96.151
45.235.96.158
45.235.96.160
45.235.96.169
45.235.96.18
45.235.96.201
45.235.96.21
45.235.96.25
45.235.96.253
45.235.96.27
45.235.96.28
45.235.96.29
45.235.96.31
45.235.96.35
45.235.96.36
45.235.96.4
45.235.96.40
45.235.96.44
45.235.96.50
45.235.96.53
45.235.96.58
45.235.96.64
45.235.96.8
45.235.96.9
45.235.97.1
45.235.97.100
45.235.97.101
45.235.97.108
45.235.97.109
45.235.97.150
45.235.97.152
45.235.97.169
45.235.97.201
45.235.97.25
45.235.97.253
45.235.97.26
45.235.97.28
45.235.97.40
45.235.97.53
45.235.97.7
45.235.97.8

Resumen

Como resultado del análisis se han identificado **14** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **1** de severidad alta y **13** de severidad media. 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.



Resumen de Hallazgos

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

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#1	EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected	Alta	2
#2	Incomplete SSL Certificate Chain Vulnerability	Media	35
#3	SSL Certificate - Invalid Maximum Validity Date Detected	Media	1
#4	SSL Certificate - Self-Signed Certificate	Media	1
#5	SSL Certificate - Signature Verification Failed Vulnerability	Media	2
#6	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	Media	2
#7	GIT Detected	Media	2
#8	Information disclosure	Media	6
#9	HTTP Security Header Not Detected	Media	6
#10	Account Brute Force Possible Through IIS NTLM Authentication Scheme	Media	2
#11	Deprecated Public Key Length	Media	1
#12	Microsoft ASP.NET Custom Errors Found Turned Off	Media	2
#13	Frameable response (potential Clickjacking)	Media	1
#14	Weak SSL/TLS Key Exchange	Media	1

Detalle de Hallazgos

#1 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected				
Severidad: Alta	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 8.8	**Attack Complexity**	Low	**Confidentiality Impact**	High
Ocurrencias: 2	**Privileges Required**	Low	**Integrity Impact**	High
	User Interaction	None	**Availability Impact**	High

Recursos Afectados

45.235.96.103 (www2.bcra.gob.ar)

45.235.96.104 (www3.bcra.gob.ar.96.235.45.in-addr.arpa)

Descripción

Se ha detectado la presencia de Microsoft Internet Information Services (IIS) 8.5, una versión que ha alcanzado oficialmente su fin de vida útil (EOL, End of Life). Esto implica que Microsoft ya no proporciona actualizaciones de seguridad ni soporte técnico para esta versión, lo que expone al sistema a vulnerabilidades conocidas y futuras sin posibilidad de mitigación por parte del fabricante.
IIS es el servidor web de Microsoft, integrado en la familia Windows NT, y es responsable de manejar protocolos como HTTP, HTTPS, FTP, SMTP, entre otros. Aunque sigue siendo ampliamente utilizado, es fundamental que se mantenga actualizado para garantizar la seguridad del entorno.
Versiones afectadas:
IIS 8.5 en Windows 8.1 llegó a su fin de vida el 10 de enero de 2023.
IIS 8.5 en Windows Server 2012 R2 alcanzó su fin de vida el 10 de octubre 2023.

Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

Referencias

IIS 8.5 End of Life
https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis

Solución

Se recomienda a los clientes actualizar a la última versión de IIS compatible.

Evidencias

Recurso: 45.235.96.103 (www2.bcra.gob.ar)

```
EOL/Obsolete version of IIS 8.5 is Detected on port 443 -
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html
Expires: Fri, 11 Jul 2025 00:36:37 GMT
Server: Microsoft-IIS/8.5
Set-Cookie: ASPSESSIONIDCWDDAAAQ=JAPCGCODLEDNAGOGLOJDECMM; secure; path=/
X-Powered-By: ASP.NET
Set-Cookie: HttpOnly; Secure
Access-Control-Allow-Origin: *
Date: Fri, 11 Jul 2025 00:37:36 GMT
Connection: close
Content-Length: 85209


<!DOCTYPE HTML>
<html lang="es">

<head>

<meta http-equiv="Expires" content="0">
```

```
<meta http-equiv="Last-Modified" content="0">
<meta http-equiv="Cache-Control" content="no-cache, mustrevalidate">
<meta http-equiv="Pragma" content="no-cache">
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','//www.google-analytics.com/analytics.js','ga');

ga('create', 'UA-72541502-1',
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html
Expires: Wed, 06 Aug 2025 13:16:09 GMT
Server: Microsoft-IIS/8.5
Set-Cookie: ASPSESSIONIDSGAQCQCD=MFPDKLJBCMKNOIMBHDNEFEOH; secure; path=/
X-Powered-By: ASP.NET
Set-Cookie: HttpOnly; Secure
Access-Control-Allow-Origin: *
Date: Wed, 06 Aug 2025 13:17:08 GMT
Content-Length: 83265
```

Recurso: 45.235.96.104 (www3.bcra.gob.ar.96.235.45.in-addr.arpa)

```
EOL/Obsolete version of IIS 8.5 is Detected on port 443 -
Content-Type: text/html
Server: Microsoft-IIS/8.5
WWW-Authenticate: Basic realm="bcra.gov.ar"
X-Powered-By: ASP.NET
Date: Thu, 10 Jul 2025 23:04:59 GMT
Connection: close
Content-Length: 1311

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>401 - No autorizado: acceso denegado debido a credenciales no v lidas.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{marg
```

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html
Server: Microsoft-IIS/8.5
WWW-Authenticate: Basic realm="bcra.gov.ar"
X-Powered-By: ASP.NET
Date: Wed, 06 Aug 2025 13:18:26 GMT
Content-Length: 1311
```

#2 Incomplete SSL Certificate Chain Vulnerability				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 38	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados

45.235.96.103 (www2.bcra.gob.ar) Puerto: 443
45.235.96.104 (www3.bcra.gob.ar.96.235.45.in-addr.arpa) Puerto: 443
45.235.96.108 (notificacioneselectronicas.bcra.gob.ar) Puerto: 443
45.235.96.109 Puerto: 443
45.235.96.110 Puerto: 443
45.235.96.111 Puerto: 443
45.235.96.117 (www5.bacen.bcra.gob.ar) Puerto: 443
45.235.96.118 Puerto: 443
45.235.96.151 Puerto: 443
45.235.96.158 (reasignacionimportaciones.homologacion.bcra.gob.ar) Puerto: 443
45.235.96.160 Puerto: 443
45.235.96.169 Puerto: 443
45.235.96.18 (sicap.bcra.gov.ar) Puerto: 443
45.235.96.201 Puerto: 443
45.235.96.21 (ps.bcra.gob.ar) Puerto: 443
45.235.96.25 (qa.bcra.gob.ar) Puerto: 443
45.235.96.253 Puerto: 443
45.235.96.27 Puerto: 443
45.235.96.28 (view.bcra.gob.ar) Puerto: 443
45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: 443
45.235.96.36 Puerto: 21443
45.235.96.36 Puerto: 4172
45.235.96.36 Puerto: 443
45.235.96.36 Puerto: 8443
45.235.96.40 (wp.bacen.bcra.gob.ar) Puerto: 443
45.235.96.44 Puerto: 443
45.235.96.50 Puerto: 443
45.235.96.58 (reasignacionimportaciones.bcra.gob.ar) Puerto: 443
45.235.96.8 Puerto: 443
45.235.97.100 Puerto: 443
45.235.97.108 (bcraweb.bcra.gob.ar) Puerto: 443
45.235.97.150 Puerto: 443
45.235.97.169 Puerto: 443
45.235.97.201 Puerto: 443
45.235.97.25 (qa.bcra.gob.ar) Puerto: 443
45.235.97.253 Puerto: 443
45.235.97.28 (view.bcra.gob.ar) Puerto: 443
45.235.97.40 (wp.bacen.bcra.gob.ar) Puerto: 443

Descripción

El servidor presenta un certificado válido, pero no envía la cadena completa de certificados intermedios. Esto impide que ciertos clientes puedan validar la autenticidad del certificado, provocando errores de confianza.

Impacto

Usuarios o aplicaciones que no dispongan del certificado intermedio en su caché pueden rechazar la conexión o aceptar manualmente el certificado sin validación, debilitando la seguridad TLS.

Referencias
https://cwe.mitre.org/data/definitions/296.html

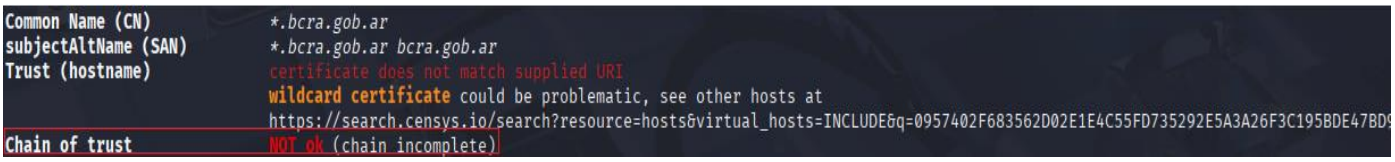
Solución
Verificar que el archivo configurado en el servidor web (Apache, Nginx, IIS, Tomcat, etc.) contenga tanto el certificado del servidor como los certificados intermedios en el orden correcto.

Evidencias
Recurso: 45.235.96.103 (www2.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

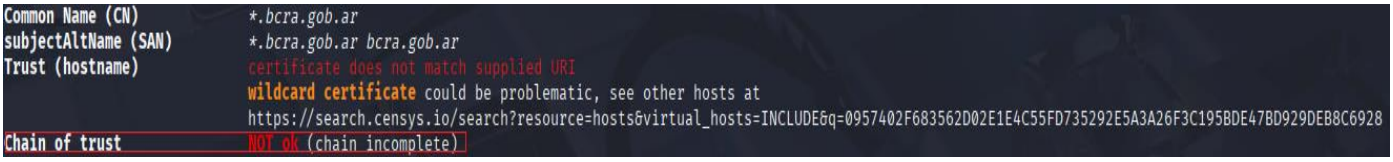
Recurso: 45.235.96.104 (www3.bcra.gob.ar.96.235.45.in-addr.arpa) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.96.108 (notificacioneselectronicas.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

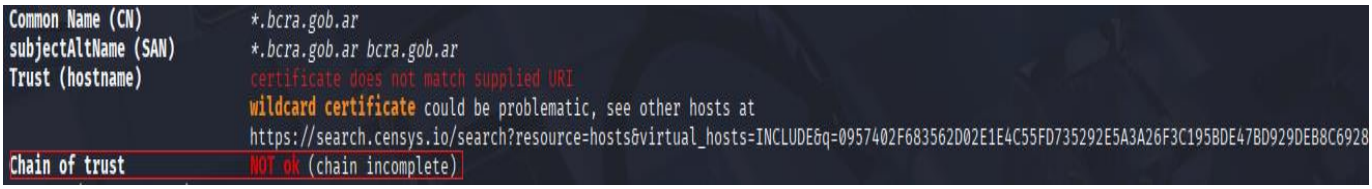


Recurso: 45.235.96.109 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

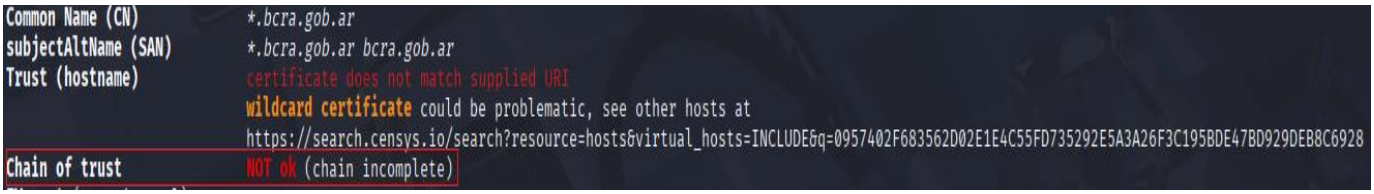
Recurso: 45.235.96.110 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



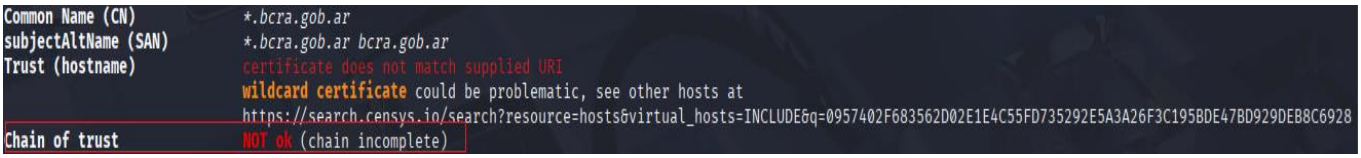
Recurso: 45.235.96.111 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



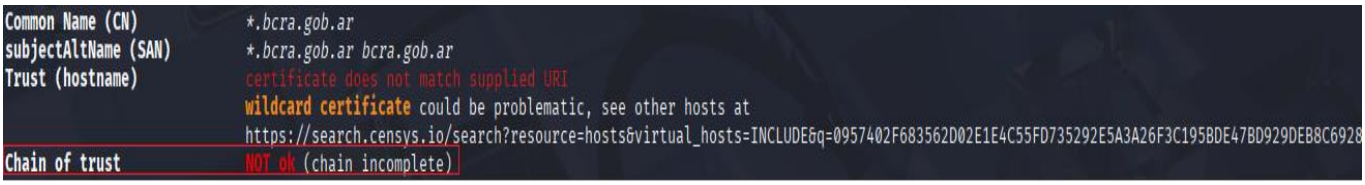
Recurso: 45.235.96.117 (www5.bacen.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.96.118 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.96.151 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.158 (reasignacionimportaciones.homologacion.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.160 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.169 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.18 (sicap.bcra.gov.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.201 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.21 (ps.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.25 (qa.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.253 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.27 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.28 (view.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

Recurso: 45.235.96.36 Puerto: 21443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

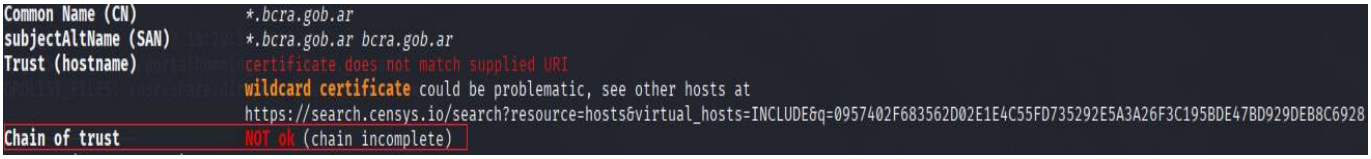
Recurso: 45.235.96.36 Puerto: 4172

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

```
Common Name (CN)            *.bcra.gob.ar
subjectAltName (SAN)        *.bcra.gob.ar bcra.gob.ar
Trust (hostname)            certificate does not match supplied URI
                            wildcard certificate could be problematic, see other hosts at
                            https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=0957402F683562D02E1E4C55FD735292E5A3A26F3C195BDE47BD929DEB8C6928
Chain of trust              NOT ok (chain incomplete)
```

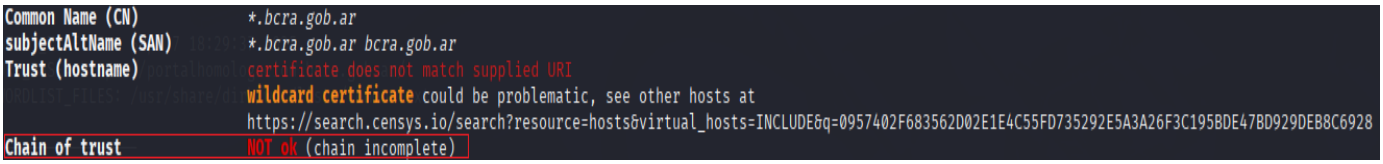
Recurso: 45.235.96.36 Puerto: 8443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



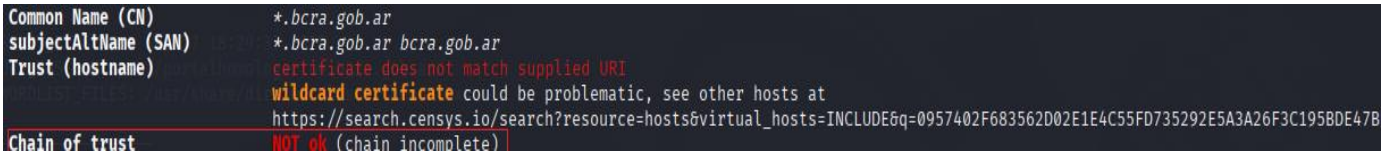
Recurso: 45.235.96.36 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



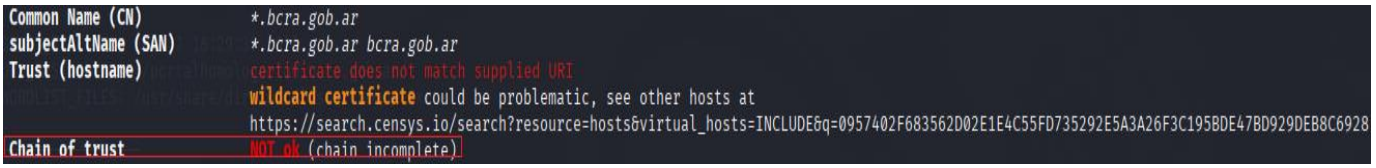
Recurso: 45.235.96.40 (wp.bacen.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



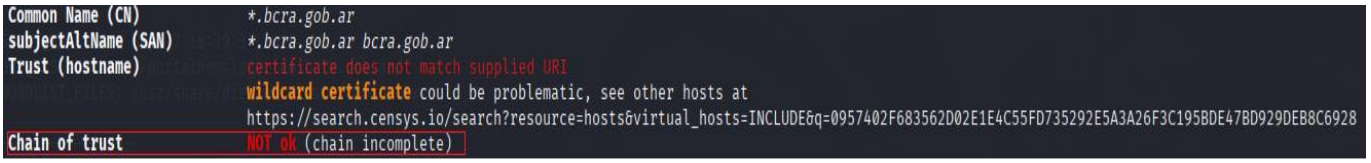
Recurso: 45.235.96.44 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



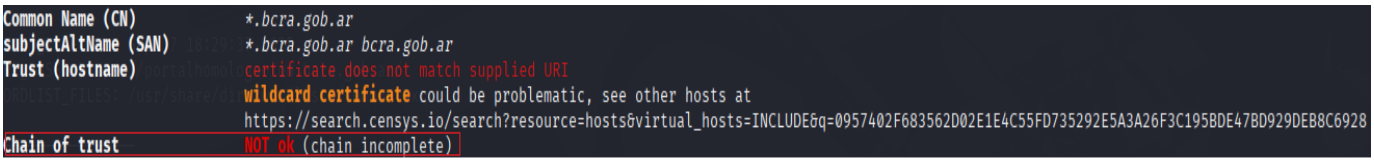
Recurso: 45.235.96.50 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



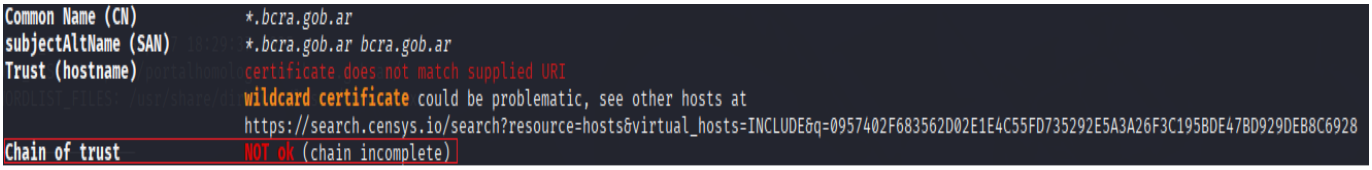
Recurso: 45.235.96.58 (reasignacionimportaciones.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



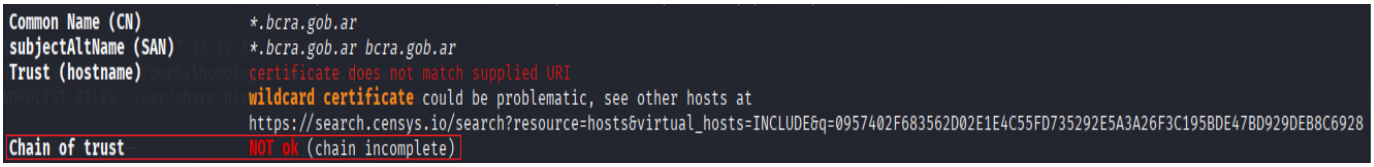
Recurso: 45.235.96.8 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



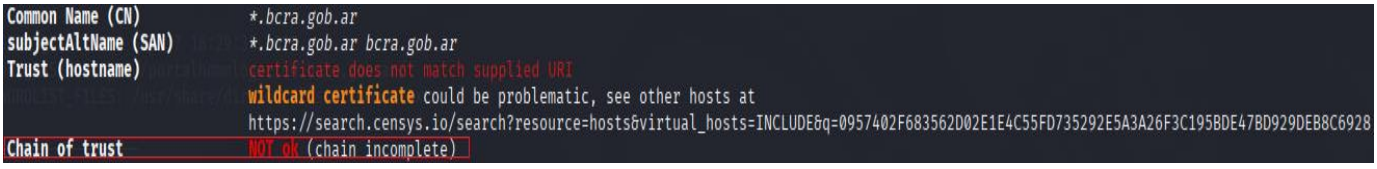
Recurso: 45.235.97.100 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



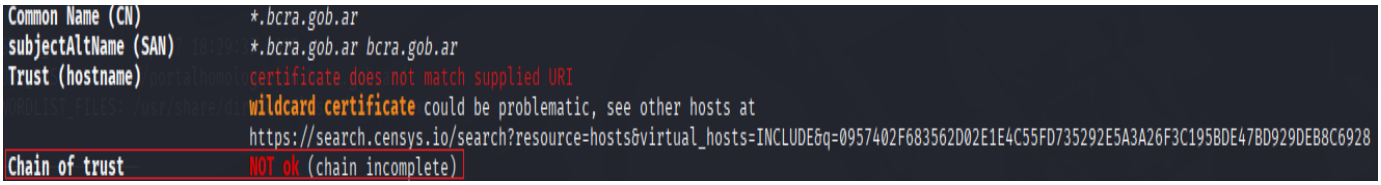
Recurso: 45.235.97.108 (bcraweb.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.97.150 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

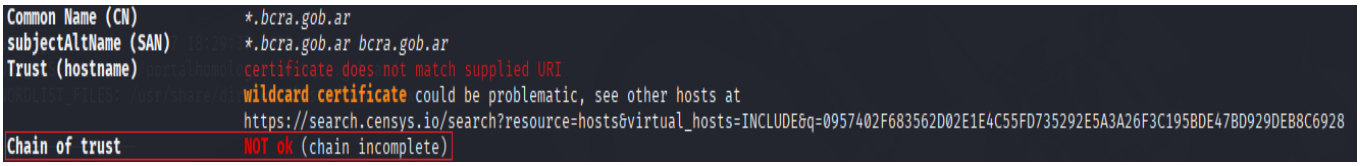


Recurso: 45.235.97.169 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

Recurso: 45.235.97.201 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

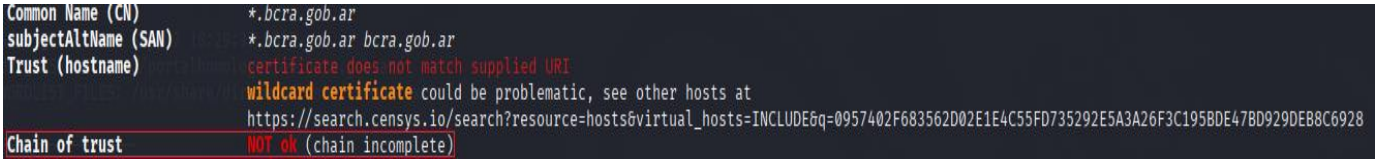


Recurso: 45.235.97.25 (qa.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

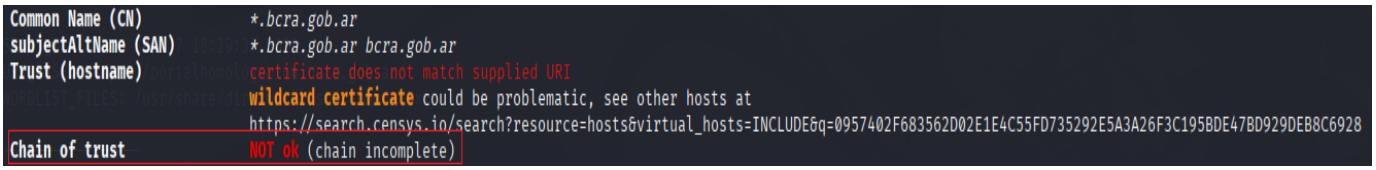
Recurso: 45.235.97.253 Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.97.28 (view.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```



Recurso: 45.235.97.40 (wp.bacen.bcra.gob.ar) Puerto: 443

```
Certificate #0 CN=*.bcra.gob.ar
ISSUER:_CN=Sectigo_RSA_Domain_Validation_Secure_Server_CA,O=Sectigo_Limited,L=Salford,ST=Gre
ater_Manchester,C=GB unable to get local issuer certificate
```

#3 SSL Certificate - Invalid Maximum Validity Date Detected				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados

45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

Descripción

Los certificados emitidos a partir del 1 de septiembre de 2020 NO DEBEN tener un período de validez superior a 398 días. (13 meses). Certificados emitidos después del 1 de marzo de 2018, pero antes del 1 de septiembre de 2020, NO DEBEN tener un Período de Validez superior a 825 días. (27 meses).
Certificados emitidos después del 1 de julio de 2016 pero antes del 1 de marzo de 2018 NO DEBEN tener un período de validez superior a 39 meses.
Los certificados SSL tienen períodos de validez limitados para que la información de identidad del titular del certificado se vuelva a actualizar con más frecuencia.
Se detecta que la validez máxima del certificado en el sistema es superior a la recomendada.

Impacto

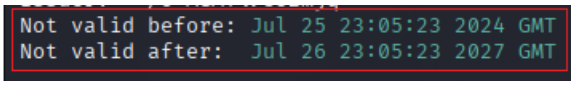
Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-medio (man-in-the-middle).

Referencias
https://www.ssl.com/blogs/398-day-browser-limit-for-ssl-tls-certificates-begins-september-1-2020/

Solución
Instalar un certificado de servidor con la máxima validez recomendada.

Evidencias
Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

```
Certificate #0 CN=VSINTREC_VPN_Certificate,O=MGMT..852mjq ISSUER:_O=MGMT..852mjq  is valid
for more than 398 days
```



#4 SSL Certificate - Self-Signed Certificate				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

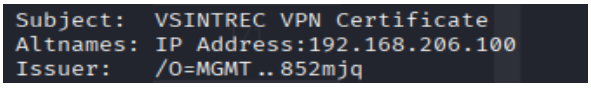
Descripción
Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura.
El cliente puede confiar en que el Certificado de Servidor pertenece al servidor sólo si es firmado por una autoridad de certificado de terceros de confianza mutua (CA). Los certificados autofirmados se crean generalmente para fines de prueba o para evitar pagar CAs de terceros. Estos no deben utilizarse en producción o servidores críticos.
Al explotar esta vulnerabilidad, un atacante puede imitar al servidor presentando un falso certificado auto-firmado. Si el cliente sabe que el servidor no tiene un certificado de confianza, aceptará este certificado de prueba y se comunicará con el servidor malicioso.

Impacto
Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-medio (man-in-the-middle).

Solución
Por favor, instale un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.

Evidencias
Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

```
Certificate #1 O=MGMT..852mjq  is a self signed certificate.
```



#5 SSL Certificate - Signature Verification Failed Vulnerability				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 3	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados

45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443
45.235.96.9 Puerto: TCP/443
45.235.96.9 Puerto: TCP/5061

Descripción

Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente auténtica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura. La autenticación se realiza verificando que la clave pública del certificado es firmada por una autoridad de certificado de terceros de confianza.
Si un cliente no puede verificar el certificado, puede abortar la comunicación o incitar al usuario a continuar la comunicación sin autenticación.

Impacto

Aprovechando esta vulnerabilidad, pueden producirse ataques de hombre-en-el-medio (man-in-the-middle) junto con el envenenamiento de la caché DNS.

Referencias

https://apidog.com/articles/ssl-certificate-signature-verification-failure-vulnerability/

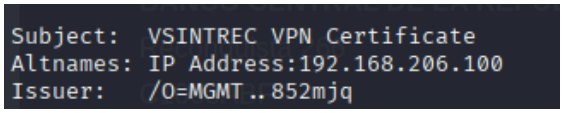
Solución

Instale un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.

Evidencias

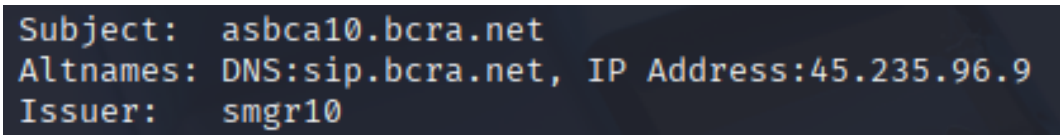
Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

```
Certificate #0 CN=VSINTREC_VPN_Certificate,O=MGMT..852mjq ISSUER:_O=MGMT..852mjq self signed
certificate in certificate chain
```



Recurso: 45.235.96.9 Puerto: TCP/5061

```
Certificate #0 C=AR,ST=CABA,L=CABA,O=BCRA,OU=IT,CN=asbca10.bcra.net
ISSUER:_O=AVAYA,OU=MGMT,CN=smgr10 unable to get local issuer certificate
```



Recurso: 45.235.96.9 Puerto: TCP/443

```
Certificate #0 C=AR,ST=CABA,L=CABA,O=BCRA,OU=IT,CN=asbca10.bcra.net
ISSUER:_O=AVAYA,OU=MGMT,CN=smgr10 unable to get local issuer certificate
```

```
Subject:  asbca10.bcra.net
Altnames: DNS:sip.bcra.net, IP Address:45.235.96.9
Issuer:   smgr10
```

#6 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 6.5	**Attack Complexity**	High	**Confidentiality Impact**	High
Ocurrencias: 2	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados

45.235.96.117 (www5.bacen.bcra.gob.ar) Puerto: TCP/80
45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

Descripción

TLS es capaz de utilizar una gran cantidad de algoritmos de cifrado para crear los pares de llaves públicos y privados.
Por ejemplo, TLSv1.0 usa el cifrado de flujo RC4 o un cifrado de bloques en modo CBC. RC4 es conocido por tener sesgos y el cifrado de bloque en modo CBC es vulnerable al ataque POODLE.
TLSv1.0, si está configurado para utilizar las mismas suites de cifrado que SSLv3, incluye un medio por el cual una implementación TLS puede degradar la conexión a SSL v3.0, debilitando así la seguridad.
Esta vulnerabilidad es un PCI FAIL automático de acuerdo con los estándares PCI.
NOTA: El 31 de marzo de 2021 las versiones de TLS 1.0 (RFC 2246) y 1.1 (RFC 4346) fueron oficialmente declaradas obsoletas. Puede consultar más información en las Referencias.

Impacto

Un atacante puede explotar fallas criptográficas para realizar ataques de tipo hombre-en-el-medio (man-in-the-middle) o para descifrar comunicaciones.
Por ejemplo: Un atacante podría forzar un descenso del protocolo TLS al protocolo SSLv3.0 y explotar la vulnerabilidad POODLE, leer comunicaciones seguras o modificar mensajes. El ataque POODLE también podría lanzarse directamente en TLS sin negociar un descenso a SSL.

Referencias

Deprecating TLS 1.0 and TLS 1.1 https://tools.ietf.org/html/rfc8996
PCI: ASV Program Guide v3.1 (page 27) https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf
PCI: Uso de los escáneres SSL Early TLS y ASV https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf

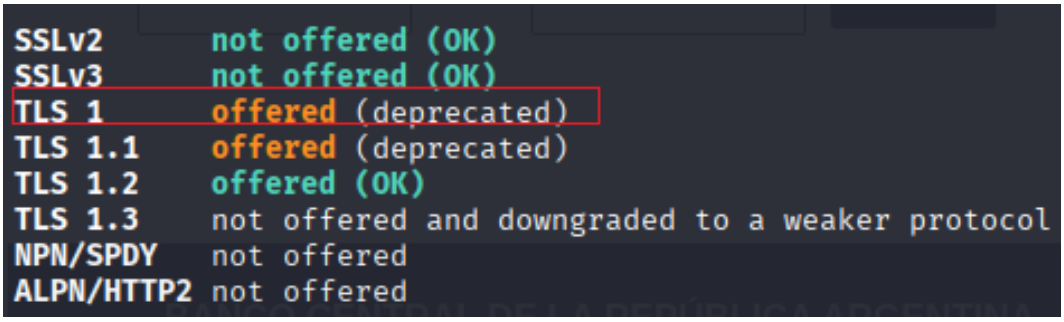
Solución

Desactivar el uso del protocolo TLSv1.0 en favor de un protocolo criptográficomente más fuerte como TLSv1.2.

Evidencias

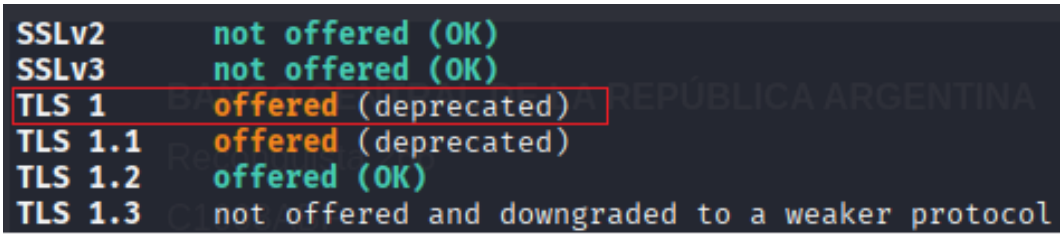
Recurso: 45.235.96.117 (www5.bacen.bcra.gob.ar) Puerto: TCP/80

```
TLSv1.0 is supported
```



Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

```
TLSv1.0 is supported
```



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

Recursos Afectados

/.git/

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: /.git/

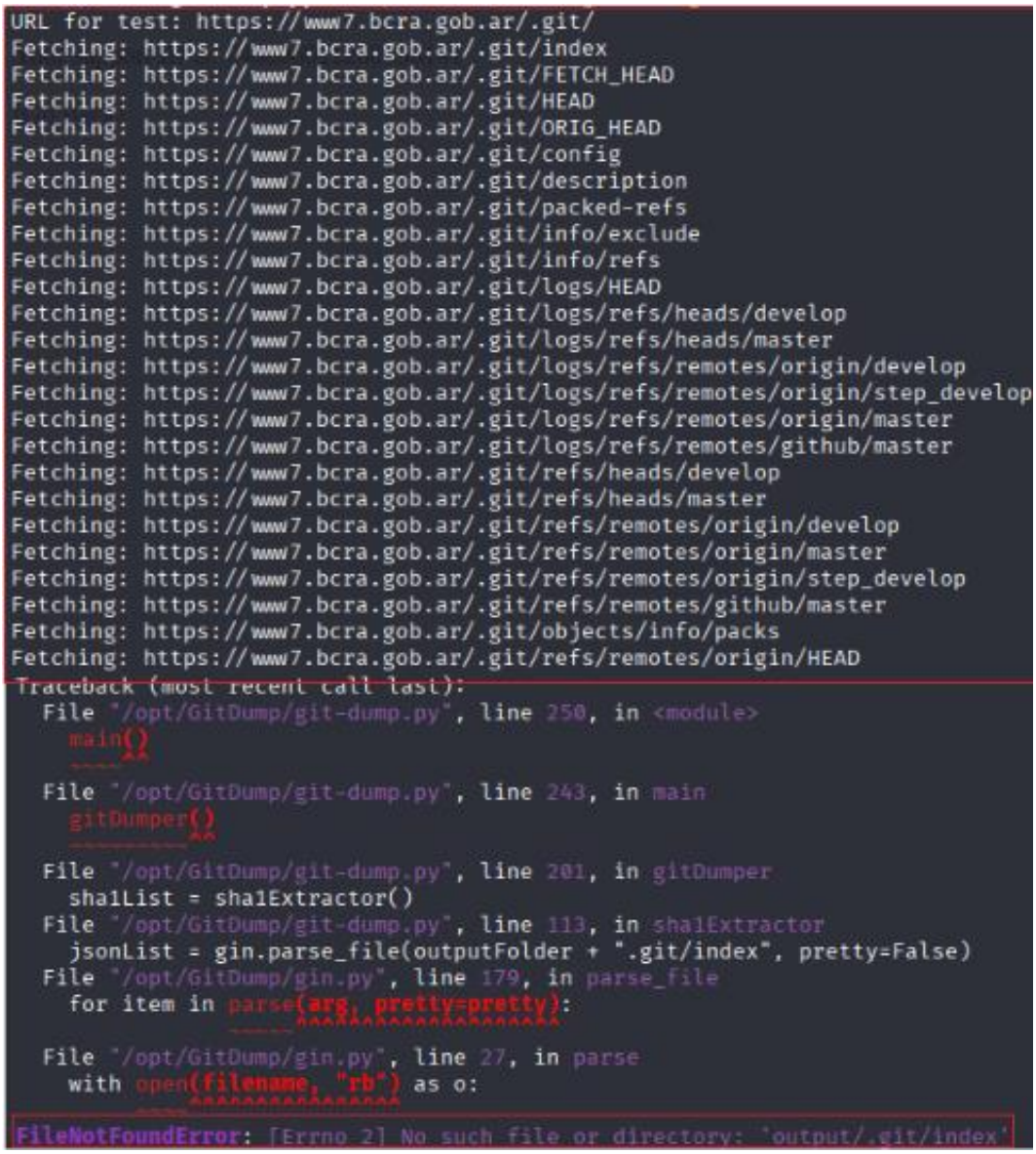
Se detectó acceso público al directorio .git/, lo cual posibilita la reconstrucción del repositorio y la exposición de código fuente, ramas y metadatos de desarrollo.

```
https://www2.bcra.gob.ar/.git/
```

Recurso: /.git/

Durante el análisis se observó que el servidor expone el directorio .git/.
La exposición del archivo .git/index en particular representa un riesgo crítico, ya que contiene la información necesaria para reconstruir el árbol completo del proyecto, permitiendo a un atacante acceder a todo el código fuente y archivos sensibles del sistema.

```
+ https://www7.bcra.gob.ar/.git/HEAD (CODE:200|SIZE:16)
```


URL for test: https://www7.bcra.gob.ar/.git/
Fetching: https://www7.bcra.gob.ar/.git/index
Fetching: https://www7.bcra.gob.ar/.git/FETCH_HEAD
Fetching: https://www7.bcra.gob.ar/.git/HEAD
Fetching: https://www7.bcra.gob.ar/.git/ORIG_HEAD
Fetching: https://www7.bcra.gob.ar/.git/config
Fetching: https://www7.bcra.gob.ar/.git/description
Fetching: https://www7.bcra.gob.ar/.git/packed-refs
Fetching: https://www7.bcra.gob.ar/.git/info/exclude
Fetching: https://www7.bcra.gob.ar/.git/info/refs
Fetching: https://www7.bcra.gob.ar/.git/logs/HEAD
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/heads/develop
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/heads/master
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/remotes/origin/develop
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/remotes/origin/step_develop
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/remotes/origin/master
Fetching: https://www7.bcra.gob.ar/.git/logs/refs/remotes/github/master
Fetching: https://www7.bcra.gob.ar/.git/refs/heads/develop
Fetching: https://www7.bcra.gob.ar/.git/refs/heads/master
Fetching: https://www7.bcra.gob.ar/.git/refs/remotes/origin/develop
Fetching: https://www7.bcra.gob.ar/.git/refs/remotes/origin/master
Fetching: https://www7.bcra.gob.ar/.git/refs/remotes/origin/step_develop
Fetching: https://www7.bcra.gob.ar/.git/refs/remotes/github/master
Fetching: https://www7.bcra.gob.ar/.git/objects/info/packs
Fetching: https://www7.bcra.gob.ar/.git/refs/remotes/origin/HEAD
Traceback (most recent call last):
File "/opt/GitDump/git-dump.py", line 250, in <module>
main()
File "/opt/GitDump/git-dump.py", line 243, in main
gitDumper()
File "/opt/GitDump/git-dump.py", line 201, in gitDumper
shaList = shaExtractor()
File "/opt/GitDump/git-dump.py", line 113, in shaExtractor
jsonList = gin.parse_file(outputFolder + ".git/index", pretty=False)
File "/opt/GitDump/gin.py", line 179, in parse_file
for item in parse(arg, pretty=pretty):
File "/opt/GitDump/gin.py", line 27, in parse
with open(filename, "rb") as o:
FileNotFoundError: [Errno 2] No such file or directory: 'output/.git/index'

#8 Information disclosure				
Severidad: Media	**Attack Vector**	Network	**Scope**	Changed
CVSS: 5.8	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 7	**Privileges Required**	None	**Integrity Impact**	None
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
/aol/ADMIN/login.asp?Action=Login&Return=%2Faol%2FADMIN%2FDefault%2Easp%3F
/sicapweb/servlet/hlogin
45.235.96.31 (controlcambio.bcra.gob.ar)
https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/_vti_bin/
https://bcraweb.bcra.gob.ar/apprecursos/Documentos%20compartidos/admin.pl
https://www3.bcra.gob.ar/
https://www6.bcra.gob.ar/satag/

Descripción
Una exposición de información es la divulgación intencionada o no intencionada de información a un actor que no está explícitamente autorizado a tener acceso a este tipo de datos.

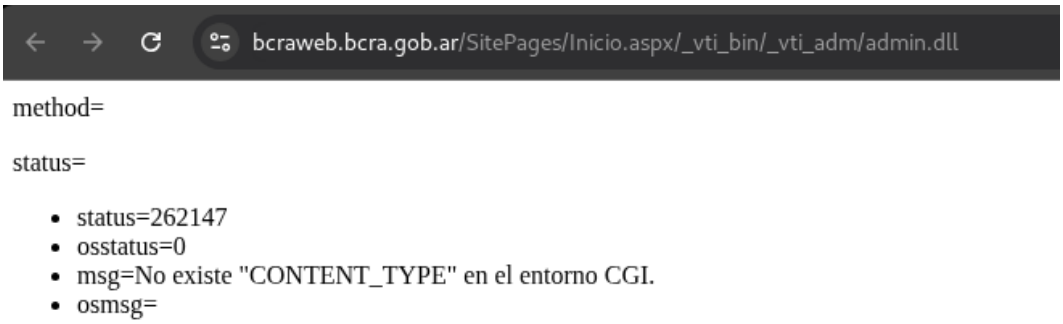
Impacto
Esta vulnerabilidad afecta la confidencialidad de la información.

Referencias
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/README
https://cwe.mitre.org/data/definitions/200.html

Solución
Validar la necesidad de contar con dicho activo expuesto a Internet sin autenticación previa, y limitar el acceso en caso de corresponder.

Evidencias
Recurso: https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/_vti_bin/

```
PRUEBAS DE FUZZING MANUAL
---- Scanning URL: https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/ ----
+ https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/_vti_bin/_vti_adm/admin.dll
(CODE:200|SIZE:20)
+ https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/_vti_bin/_vti_aut/author.dll
(CODE:200|SIZE:20)
+ https://bcraweb.bcra.gob.ar/SitePages/Inicio.aspx/_vti_bin/shtml.dll (CODE:200|SIZE:38)
```



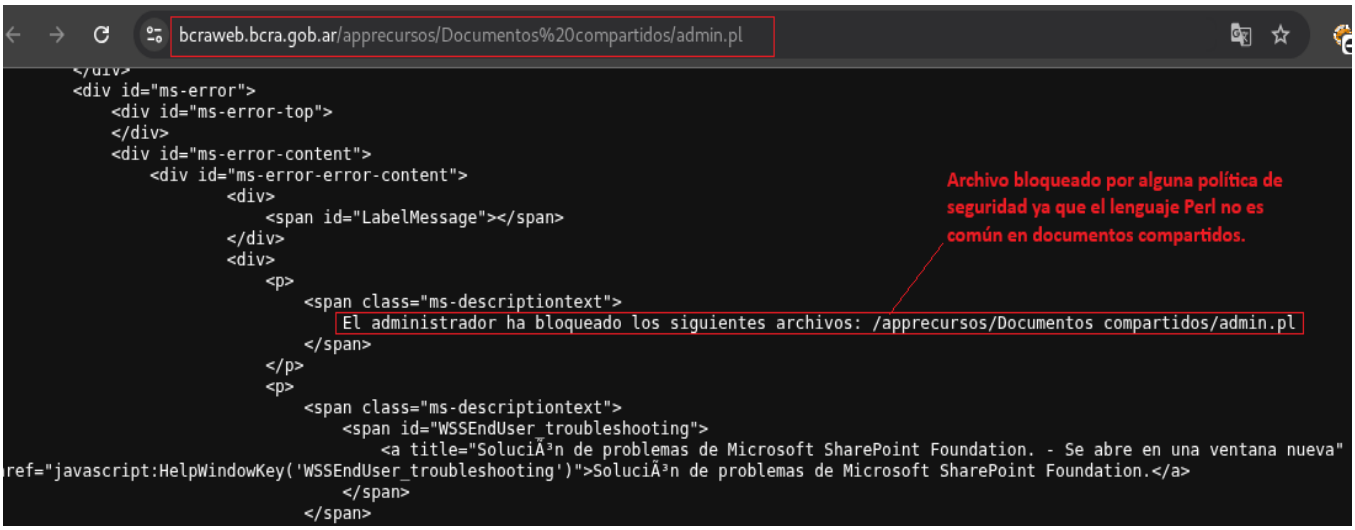
Recurso: https://www6.bcra.gob.ar/satag/

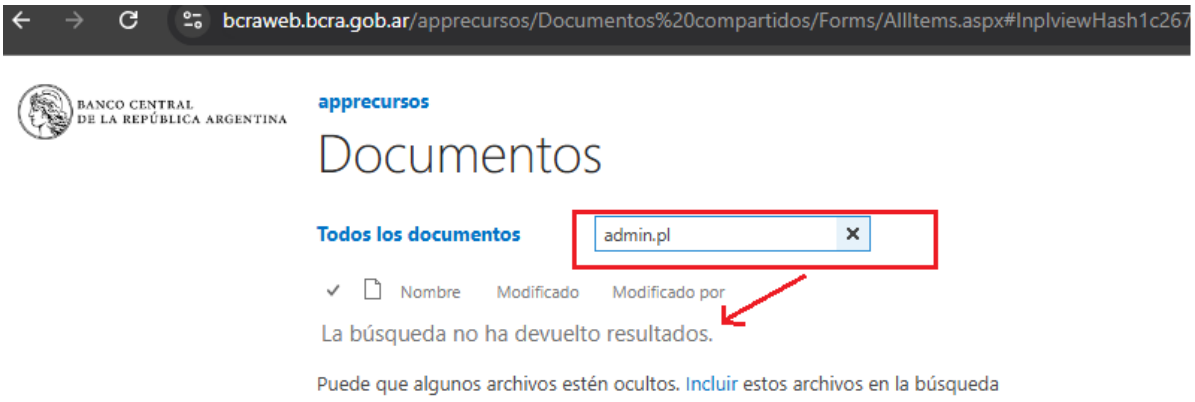
```
POST /satag/satprovinicioenrolamiento.asp HTTP/1.1
Host: www6.bcra.gob.ar
Cookie: ASPSESSIONIDQWCADQRQ=BDILDHKDKCDFPLIHGABONCJA;
TS015e958a=01532640e84b85b4172a7a5d71e2c7d721871a7936739fd79051d70cf60bc295b4e66230fda122219
88b2b98a4d00b0d2fd5f2ee4efc358a80e8cb028b0d0dd07ee9d377b0;
TSf44d3953027=08403d584cab2000f0e6ba3a71e288412e1eceb1fe16e314ad21cb217489cf50f9fa3fe15f465f
2d088f04bc5611300062c794eb1f1e10a33b00ac349260d796bc3b6cf40e9c816ad01862b09cd63432243484f37b
d5a87be15624b1d9e93745
Content-Length: 65
Cache-Control: max-age=0
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Origin: https://www6.bcra.gob.ar
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: iframe
Referer: https://www6.bcra.gob.ar/satag/satprovinicioenrolamiento.asp
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

Accion=EnrollWithCode&hdPermitirIngresoCodigo=1&EnrollCode=123456
```

Recurso: https://bcraweb.bcra.gob.ar/apprecursos/Documentos%20compartidos/admin.pl

```
<!-- _lcid="3082" _version="15.0.5259" _dal="1" -->
<!-- _LocalBinding -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html dir="<%$Resources:wss,multipages_direction_dir_value%>;" xmlns:o="urn:schemas-
microsoft-com:office:office" runat="server">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=9"/>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <meta http-equiv="Expires" content="0" />
        <meta name="SharePointError" content=""/>
        <meta name="Robots" content="NOINDEX" />
        <base href="https://bcraweb.bcra.gob.ar/apprecursos/_layouts/15/3082/errorv4.htm">
        <title id="onetidTitle">Error</title>
        <link rel="stylesheet" type="text/css"
href="/_layouts/15/3082/styles/Themable/corev15.css">
        <link rel="stylesheet" type="text/css" href="/_layouts/15/3082/styles/error.css">
        <script type="text/javascript" src="init.js"></script>
        <script type="text/javascript" src="core.js"></script>
    </head>
    <body id="ms-error-body">
        <script type="text/javascript">

        </script>
        <div id="ms-error-header" class="ms-pr">
                <h1 class="ms-core-pageTitle">
                    Error
                </h1>
        </div>
        <div id="ms-error">
            <div id="ms-error-top">
            </div>
            <div id="ms-error-content">
                <div id="ms-error-error-content">
                        <div>
                            <span id="LabelMessage"></span>
                        </div>
                        <div>
                            <p>
                                <span class="ms-descriptiontext">
                                    El administrador ha bloqueado los siguientes archivos:
/apprecursos/Documentos compartidos/admin.pl
```

```
                                </span>
                            </p>
                            <p>
                                <span class="ms-descriptiontext">
                                    <span id="WSSEndUser_troubleshooting">
                                        <a title="SoluciÃ³n de problemas de Microsoft
SharePoint Foundation. - Se abre en una ventana nueva"
href="javascript:HelpWindowKey('WSSEndUser_troubleshooting')">SoluciÃ³n de problemas de
Microsoft SharePoint Foundation.</a>
                                    </span>
                                </span>
                            </p>
                        </div>
                        <div class="ms-error-techMsg">
                            <hr />
                        </div>
                </div>
                <div id="ms-error-gobackcont">
                        <a class="ms-calloutLink" href="/apprecursos"
id="SimpleGoBackToHome">Volver al sitio</a>
                </div>
            </div>
        </div>
    </body>
</html>
```





Recurso: /aol/ADMIN/login.asp?Action=Login&Return=%2Faol%2FADMIN%2FDefault%2Easp%3F

Al tratarse de un formulario de login, se realizaron pruebas controladas de inyección SQL (SQLi) y de fuerza bruta con diccionarios de usuarios/contraseñas, con el objetivo de verificar si era posible evadir los controles de acceso, manipular la lógica de autenticación o acceder indebidamente al sistema.

```
https://www2.bcra.gob.ar/aol/ADMIN/login.asp?Action=Login&Return=%2Faol%2FADMIN%2FDefault%2E
asp%3F
Esta expuesto publicamente un panel de acceso a cuentas de administracion de chat
```

```
[17:45:39] [WARNING] POST parameter 'Username' does not seem to be injectable
[17:45:39] [INFO] testing if POST parameter 'Password' is dynamic
[17:45:39] [WARNING] POST parameter 'Password' does not appear to be dynamic
[17:45:39] [WARNING] heuristic (basic) test shows that POST parameter 'Password' might not be injectable
[17:45:39] [INFO] testing for SQL injection on POST parameter 'Password'
[17:45:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:45:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:45:40] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:45:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:45:42] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[17:45:43] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:45:43] [INFO] testing 'Generic inline queries'
[17:45:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:45:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:45:45] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:45:45] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[17:45:46] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[17:45:47] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[17:45:48] [INFO] testing 'Oracle AND time-based blind'
[17:45:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:45:58] [WARNING] POST parameter 'Password' does not seem to be injectable
```

Ambos parámetros no son vulnerables a sqli

4. Intruder attack of https://www2.bcra.gob.ar

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

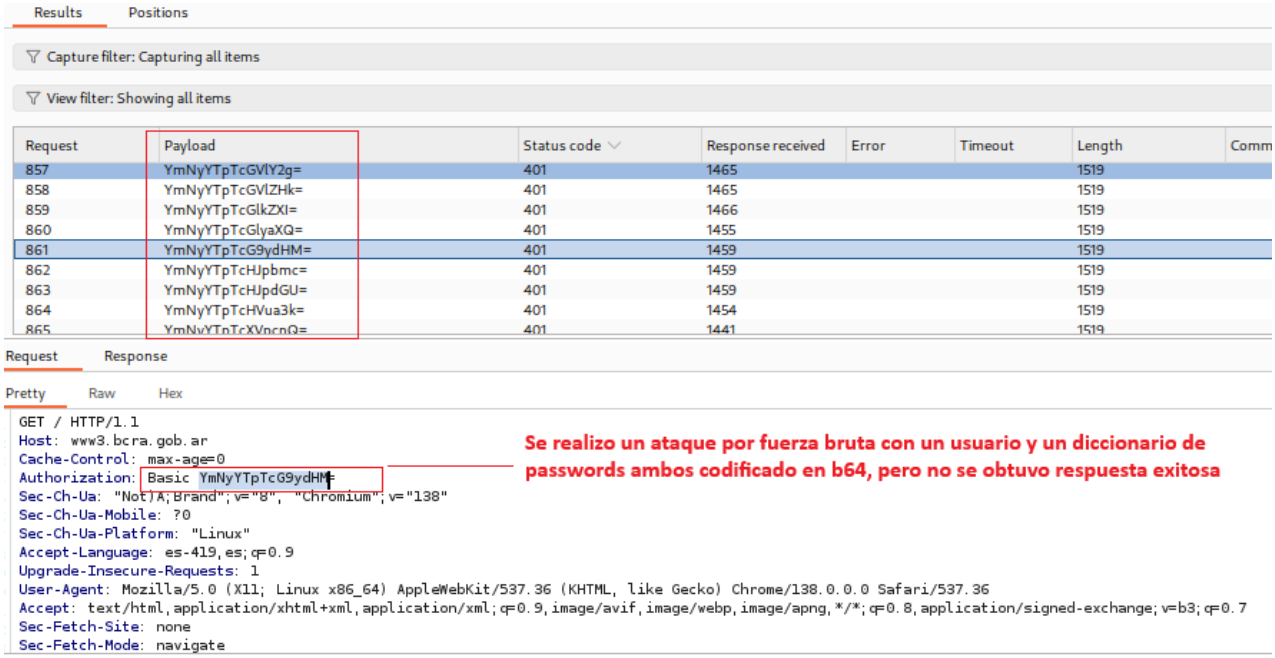
Se aplico un ataque por fuerza bruta con un diccionario creado a partir del dominio oficial y nombres comunes, pero no se obtuvo la autenticacion

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Leng
0			200	75			2173
1	admin@bcra.gob.ar	admin	200	75			2173
2	soporte@bcra.gob.ar	admin	200	75			2175
3	encuestas@bcra.gob.ar	admin	200	77			2177
4	guest@bcra.gob.ar	admin	200	73			2173
5	admin@bcra.gob.ar	123456	200	82			2173
6	soporte@bcra.gob.ar	123456	200	83			2175
7	encuestas@bcra.gob.ar	123456	200	84			2177
8	guest@bcra.gob.ar	123456	200	83			2173
9	admin@bcra.gob.ar	12345	200	83			2173
10	soporte@bcra.gob.ar	12345	200	39			2175
11	encuestas@bcra.gob.ar	12345	200	43			2177
12	guest@bcra.gob.ar	12345	200	39			2173
13	admin@bcra.gob.ar	123456789	200	41			2173
14	soporte@bcra.gob.ar	123456789	200	41			2175
15	encuestas@bcra.gob.ar	123456789	200	46			2177
16	guest@bcra.gob.ar	123456789	200	46			2173
17	admin@bcra.gob.ar	password	200	48			2173
18	soporte@bcra.gob.ar	password	200	49			2175
19	encuestas@bcra.gob.ar	password	200	48			2177
20	guest@bcra.gob.ar	password	200	38			2173
21	admin@bcra.gob.ar	iloveyou	200	38			2173
22	soporte@bcra.gob.ar	iloveyou	200	31			2175

Recurso: https://www3.bcra.gob.ar/

Se identificó que el servicio implementa Basic Authentication como único mecanismo de acceso. Este método transmite las credenciales en cada solicitud y carece de protecciones modernas como tokens antifalsificación (CSRF), gestión de sesión segura o autenticación multifactor.
Esto no constituye un ataque de tipo Man-in-the-Middle (MiTM), sino que representa la forma más sencilla de aplicar ataques de fuerza bruta, ya que un atacante puede automatizar pruebas masivas de usuario/contraseña hasta obtener acceso válido.
La única mitigación posible en este escenario es implementar rate limiting y restringir el acceso mediante VPN corporativa para reducir la exposición en Internet.

```
GET / HTTP/1.1
Host: www3.bcra.gob.ar
Cache-Control: max-age=0
Authorization: Basic cXVhbHlzOnF1YWx5cw
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: es-419,es;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```



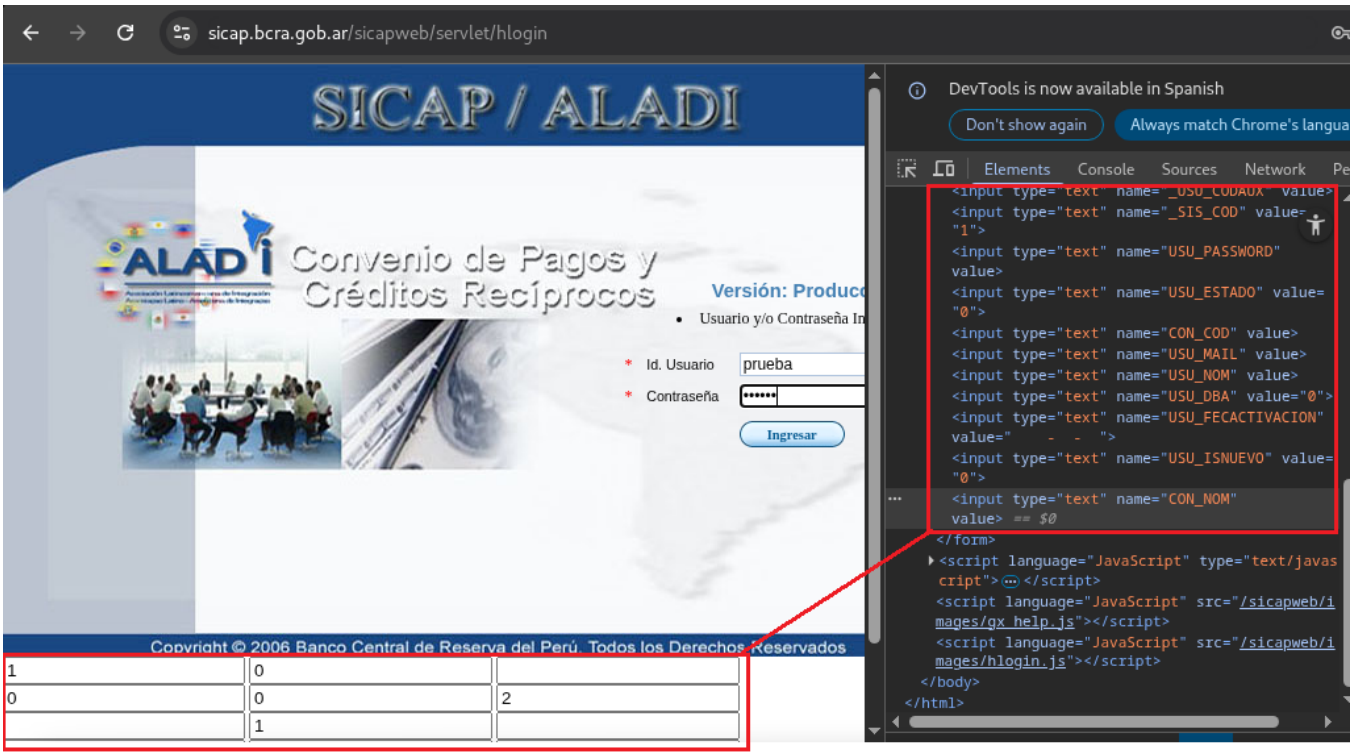
Recurso: /sicapweb/servlet/hlogin

Se identificó que el formulario de login expone múltiples campos ocultos (hidden) con valores internos por defecto. Esta práctica puede permitir la manipulación de parámetros y derivar en divulgación de información sensible o incluso en escalamiento de privilegios en caso de que un atacante disponga de credenciales válidas. Cabe destacar que, para concretar este tipo de pruebas, es necesario contar previamente con acceso legítimo al sistema (usuario/contraseña válidos). Durante el presente análisis no fue posible obtener credenciales válidas, por lo que el impacto no pudo ser verificado en un escenario real. Sin embargo, la exposición de esta información en el cliente representa una mala práctica de seguridad.

```
URL https://sicap.bcra.gob.ar/sicapweb/servlet/hlogin

<form id="MAINFORM" onsubmit="try{return GXValidForm()}catch(e){return true;}"
name="MAINFORM" method="POST" action="hlogin">

<input type="hidden" name="_EventName" value="">
```

```
<input type="hidden" name="_EventGridId" value="">
<input type="hidden" name="_EventRowId" value=""><table id="TBLLOGIN" class="Table"
cellpadding="1" cellspacing="2" "="" style="BACKGROUND-IMAGE:
url(/sicapweb/images/loginsicap.jpg); height: 450px; width: 780px;"><tbody>
<tr>
<td valign="bottom" align="middle">
<p><br><br> </p></td>
<td style="WIDTH: 40%" valign="center" width="40%">
<p> </p>
<p><table id="TABLE1" class="Table" border="  0" cellpadding="2" cellspacing="2" "=""
style="border-width:  0; width: 100%;"><tbody>
<tr>
<td colspan="3">
<p align="center"><span id="VERSION" class="Title" "="" style="">Versión: Producción
2.0</span></p></td></tr>
<tr>
<td colspan="3">
<p><span class="ErrorViewer" style=""></span></p><menu><li>Usuario y/o Contraseña
Incorrecta</li></menu><p></p></td></tr>
<tr>
<td><font color="#ff0000">*</font></td>
<td><span id="TEXTBLOCK2" class="TextBlock" "="" style="color:#000000">Id. Usuario</span>
</td>
<td style="BORDER-BOTTOM-COLOR: #000000; BORDER-TOP-COLOR: #000000; BORDER-RIGHT-COLOR:
#000000; BORDER-LEFT-COLOR: #000000" bordercolor="#000000"><input type="text" id="_USU_COD"
name="_USU_COD" value="asd" size="25" maxlength="20" class="Attribute" style="font-
family:'Arial'; font-size:9pt; font-weight:normal; font-style:normal" gxctx="_"
onfocus="gxonfocus(this, 7,'','',0)" onchange="gxonchange(this)" onblur=";GXOnBlur(7);"
gxvalid="0" gxoldvalue="prueba" gxctrlchanged="1"></td></tr>
<tr>
<td><font color="#ff0000">*</font></td>
<td><span id="TEXTBLOCK1" class="TextBlock" "="" style="color:#000000">Contraseña</span>
</td>
<td><input type="password" id="_USU_PASSWORD" name="_USU_PASSWORD" value="asd" size="25"
maxlength="50" class="Attribute" style="font-family:'Arial'; font-size:9pt; font-
weight:normal; font-style:normal" gxctx="_" onfocus="gxonfocus(this, 9,'','',0)"
onchange="gxonchange(this)" onblur=";GXOnBlur(9);" gxvalid="0" gxoldvalue="prueba"
gxctrlchanged="1"></td></tr>
<tr>
<td></td>
<td></td>
<td><font color="#000000" size="1"><input type="SUBMIT" name="BUTTON2" value="Ingresar"
class="ActionButtons" style="" gxevent="EENTER." onclick="GX_setevent('EENTER.');" gxctx="_"
onfocus="gxonfocus(this, 10,'','',0)"> </font></td></tr>
<tr>
<td><font color="#ff0000"></font></td>
<td><strong></strong></td>
<td><font color="#000000" size="1">
</font><p align="right"><font color="#000000" size="1"><font color="#ff0000">* <span
id="TEXTBLOCK3" class="TextBlock" "="" style="color:#000000">Campos obligatorios</span>
</font></font></p></td></tr></tbody></table></p></td></tr></tbody></table>
<input type="hidden" name="sCallerURL" value="https://sicap.bcra.gob.ar/sicapweb/">
<input type="text" name="_SIS_CODSICAP" value="1">
<input type="text" name="SIS_COD" value="0">
<input type="text" name="USU_COD" value="">
<input type="text" name="ROL_COD" value="0">
<input type="text" name="USU_PERFILPRED" value="0">
<input type="text" name="_SIS_CODSEGUR" value="2">
<input type="text" name="_USU_CODAUX" value="">
<input type="text" name="_SIS_COD" value="1">
<input type="text" name="USU_PASSWORD" value="">
<input type="text" name="USU_ESTADO" value="0">
<input type="text" name="CON_COD" value="">
<input type="text" name="USU_MAIL" value="">
<input type="text" name="USU_NOM" value="">
<input type="text" name="USU_DBA" value="0">
```

```
<input type="text" name="USU_FECACTIVACION" value="    -  -  ">
<input type="text" name="USU_ISNUEVO" value="0">
<input type="text" name="CON_NOM" value=""></form>
```



Recurso: 45.235.96.31 (controlcambio.bcra.gob.ar)

El portal comparte credenciales con www3.bcra.gob.ar, lo que implica una autenticación federada insegura. Esto expone a que el compromiso de un sistema permita acceso no autorizado a otros servicios críticos.

```
URL https://controlcambio.bcra.gob.ar/

<div id="ctl00_ContentPlaceHolderBody_UpdatePanel1">

            <div style="text-align: center; font-weight: 500; line-height: 1.1; font-family:
Calibri, Candara, Segoe, 'Segoe UI', Optima, Arial, sans-serif; color: #344968; margin-
bottom: 2%; font-size: 1.6452vw;">
                Bienvenido al Portal Operadores de Cambio BCRA
            </div>

            <div id="ctl00_ContentPlaceHolderBody_panel1">

                <table style="width: 40%; text-align: center; margin-left: 21.172539vw;
padding-top: 1vw;">
                    <tbody><tr>
                        <td width="15%" style="line-height: 1.5;">
                            <span id="ctl00_ContentPlaceHolderBody_lUsuario"
class="textBoxLogin">CUIT</span>
                        </td>

                        <td width="50%" style="line-height: 1.5;">
                            <div>
                                <input name="ctl00$ContentPlaceHolderBody$tbUsuario"
type="number" value="20367230836" maxlength="11" id="ctl00_ContentPlaceHolderBody_tbUsuario"
class="inputLogin" style="border: 1px solid rgb(51, 51, 51); background-color: rgb(255, 255,
255);">
                            </div>
                        </td>
```

```
                        <td style="text-align: left; line-height: 1.5;">
                            <span id="ctl00_ContentPlaceHolderBody_rfv1" class="lblError"
style="color:Red;visibility:hidden;">Ingrese cuit</span>
                        </td>
                    </tr>
                    <tr>
                        <td width="15%" style="line-height: 1.5;">

                            <span id="ctl00_ContentPlaceHolderBody_lbNombreUsuario"
class="textBoxLogin">Usuario</span>
                        </td>

                        <td width="50%" style="line-height: 1.5;">
                            <input name="ctl00$ContentPlaceHolderBody$tbNombreUsuario"
type="password" maxlength="12" id="ctl00_ContentPlaceHolderBody_tbNombreUsuario"
class="inputLogin" style="border: 1px solid rgb(51, 51, 51); background-color: rgb(255, 255,
255);">

                        </td>
                        <td style="text-align: left; line-height: 1.5;">
                            <span id="ctl00_ContentPlaceHolderBody_RequiredFieldValidator2"
class="lblError" style="color:Red;visibility:hidden;">Ingrese usuario</span>
                        </td>
                    </tr>
                    <tr style="border-top: 10px;">
                        <td width="15%" style="line-height: 1.5;">

                            <span id="ctl00_ContentPlaceHolderBody_lPassword"
class="textBoxLogin" style="width: 120px">Contraseña</span>
                        </td>

                        <td width="50%" style="line-height: 1.5;">
                            <input name="ctl00$ContentPlaceHolderBody$tbPassword"
type="password" id="ctl00_ContentPlaceHolderBody_tbPassword" class="inputLogin"
style="border: 1px solid rgb(235, 60, 60); background-color: rgb(250, 202, 202);">

                        </td>
                        <td style="text-align: left; line-height: 1.5;">
                            <span id="ctl00_ContentPlaceHolderBody_RequiredFieldValidator1"
class="lblError" style="color: red; visibility: visible;">Ingrese password</span>
                        </td>
                    </tr>
                    <tr>
                        <td colspan="2" style="text-align: center;">

                            <br>
                            <span id="ctl00_ContentPlaceHolderBody_lblErrorCredenciales"
class="lblError" style="width: 120px">Usuario inexistente.</span>



                        </td>
                    </tr>
                    <tr>
                        <td colspan="2" style="text-align: center; line-height: 7.5;">

                            <input type="submit"
name="ctl00$ContentPlaceHolderBody$bIngresar" value="Acceder" onclick="return Validate();"
id="ctl00_ContentPlaceHolderBody_bIngresar" class="boton">

                        </td>
                    </tr>

                    <tr>
                        <td colspan="2" style="text-align: center; font-family: Calibri,
Candara, Segoe, 'Segoe UI', Optima, Arial, sans-serif; font-size: 0.8vw; color: #344968
```

```
!important">
                            <span style="font-weight: bold;">¿Primera vez que
ingresa?</span>
                            <br>
                            <a id="ctl00_ContentPlaceHolderBody_lbCrearUsuario"
href="javascript:WebForm_DoPostBackWithOptions(new
WebForm_PostBackOptions("ctl00$ContentPlaceHolderBody$lbCrearUsuario", "", true,
"validacion", "", false, true))" style="text-decoration: underline">Obtener usuario</a>
                        </td>
                    </tr>
                </tbody></table>


    </div>



            <div id="ctl00_ContentPlaceHolderBody_divInfo" style="background-color: #F29334;
color: #fff; margin: 2vw; width: 75%; margin-left: 12%; height: 3vw; font-size:
0.8333333333333334vw; text-align: center; padding: 0.3125vw;">
                Para acceder debe ingresar el cuit y contraseña utilizados en www3 para BCRA
- Registro Operadores de Cambio. De no poseer usuario para operar en este sitio por favor
ingrese a Obtener Usuario.
            </div>

            <div id="ctl00_ContentPlaceHolderBody_UpdateProgress1" style="display:none;"
role="status" aria-hidden="true">

                    <div id="progressBackgroundFilter"></div>
                    <div id="processMessage" style="margin-left: 290px;">
                        Ingresando al sistema
                <br>
                        <br>
                        <img alt="Loading" src="Images/Progress.gif">
                    </div>


    </div>


            <script type="text/javascript">

                function Validate() {
                    var isValid = false;
                    isValid = Page_ClientValidate('validacion');
                    if (isValid) {
                        isValid = Page_ClientValidate('validacion2');
                    }

                    return isValid;
                }
            </script>

</div>
```

#9 HTTP Security Header Not Detected				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 5.3	**Attack Complexity**	Low	**Confidentiality Impact**	None
Ocurrencias: 6	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados

45.235.96.158 (reasignacionimportaciones.homologacion.bcra.gob.ar) Puerto: TCP/443
45.235.96.21 (ps.bcra.gob.ar) Puerto: TCP/443
45.235.96.25 (qa.bcra.gob.ar) Puerto: TCP/443
45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: TCP/443
45.235.96.58 (reasignacionimportaciones.bcra.gob.ar) Puerto: TCP/443
45.235.97.25 (qa.bcra.gob.ar) Puerto: TCP/443

Descripción

Se detecta la ausencia de las siguientes algunas de las siguientes Cabeceras HTTP (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) según [CWE-693: Mecanismo de protección](https://cwe.mitre.org/data/definitions/693.html):
X-Frame-Options: este encabezado de respuesta HTTP mejora la protección de las aplicaciones web contra los ataques de clickjacking. Clickjacking, también conocido como "UI redress attack", permite a un atacante usar múltiples capas transparentes u opacas para engañar a un usuario específico para que haga clic en un botón o enlace en otra página cuando intenta hacer clic en la página de nivel superior.
X-XSS-Protection: este encabezado HTTP habilita el filtro de Cross-Site Scripting (XSS) incorporado en el navegador para evitar ataques de secuencias de comandos entre sitios. X-XSSProtection: 0; deshabilita esta funcionalidad.
X-Content-Type-Options: este encabezado HTTP evita los ataques basados en el desajuste tipo MIME. El único valor posible es nosniff. Si su servidor devuelve X-Content-Type-Options: nosniff en la respuesta, el navegador

rechazará cargar los estilos y scripts en caso de que tengan un MIMEtype incorrecto. Content-Security-Policy: este encabezado HTTP ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS), ataques de detección de paquetes y ataques de inyección de datos. Strict-Transport-Security: el encabezado de respuesta HTTP Strict-Transport-Security (HSTS) es una característica de seguridad que permite a un sitio web decirle a los navegadores que solo se debe comunicar mediante HTTPS, en lugar de utilizar HTTP.

Impacto

Dependiendo de la vulnerabilidad que se explote, un atacante remoto no autenticado podría llevar a cabo ataques de Cross-site scripting (XSS), clickjacking o MIME-type sniffing attacks.

Solución

Dependiendo de su software de servidor, los clientes pueden establecer directivas en su configuración de sitio o archivos Web.config. Algunos ejemplos son:
X-Frame-Options:
Apache: El encabezado siempre agrega X-Frame-Options SAMEORIGIN
nginx: add_header X-Frame-Options SAMEORIGIN;
HAProxy: rspadd X-Frame-Options: \ SAMEORIGIN
IIS: <HTTPPROTOCOL> <CUSTOMHEADERS> <ADD NAME = "X-Frame-Options" VALUE = "SAMEORIGIN"> </ ADD> </ CUSTOMHEADERS> </ HTTPPROTOCOL>
X-XSS-Protection:
Apache: El encabezado siempre establece X-XSS-Protection "1; mode = block"
PHP: encabezado ("X-XSS-Protection: 1; mode = block");
El encabezado de respuesta HTTP X-XSS-Protection es una función de Internet Explorer, Chrome y Safari que evita que las páginas se carguen cuando detectan ataques de scripts de sitios cruzados (XSS) reflejados. Aunque estas protecciones son en gran medida innecesarias en los navegadores modernos cuando los sitios implementan una política de seguridad de contenido sólida que deshabilita el uso de JavaScript en línea ('inseguro-en línea'), aún pueden brindar protecciones para los usuarios de navegadores web más antiguos que aún no lo hacen.
Opciones de X-Content-Type:
Apache: El encabezado siempre establece X-Content-Type-Options: nosniff
Content-Security-Policy: (Tenga en cuenta que estos valores pueden diferir de un sitio web a otro. Los siguientes valores son solo informativos. El escáner simplemente busca la presencia del encabezado de seguridad).
Apache: Encabezado establecido Content-Security-Policy "script-src 'self'; object-src 'self'"
IIS: <SYSTEM.WEBSERVER> <HTTPPROTOCOL> <CUSTOMHEADERS> <ADD NAME = "Content-Security-Policy" VALUE = "default-src 'self';"> </ ADD> </ CUSTOMHEADERS> </ HTTPPROTOCOL> </ SYSTEM.WEBSERVER>
nginx: add_header Content-Security-Policy "default-src 'self'; script-src 'self';

Evidencias

Recurso: 45.235.96.21 (ps.bcra.gob.ar) Puerto: TCP/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: ps.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



<head>
<meta http-equiv='refresh' content='0; URL=../psp/sup/SUPPLIER/ERP/h/?tab=DEFAULT' />
</head>

Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Date: Thu, 10 Jul 2025 23:19:15 GMT
```

```
Accept-Ranges: bytes
Content-Length: 105
Content-Type: text/html;charset=utf-8
Last-Modified: Thu, 07 Dec 2023 20:34:07 GMT
X-ORACLE-DMS-ECID: e953b3e5-5462-4b2a-8022-6963ad9746b4-0001dd27
X-ORACLE-DMS-RID: 0
Set-Cookie:
TS96493f31027=08403d584cab2000cff33b5f3200c6589f08492f21a6ffcde6fd0cbc78a0632b5448cf0830f75b
0108a1bd273d11300066aa0e98e917e6eb735c0b6aac8602e727662f9550ad46986a3afc43179b79237dc60c0039
09ed0e01e1b0f5fba3fe35; Path=/
```

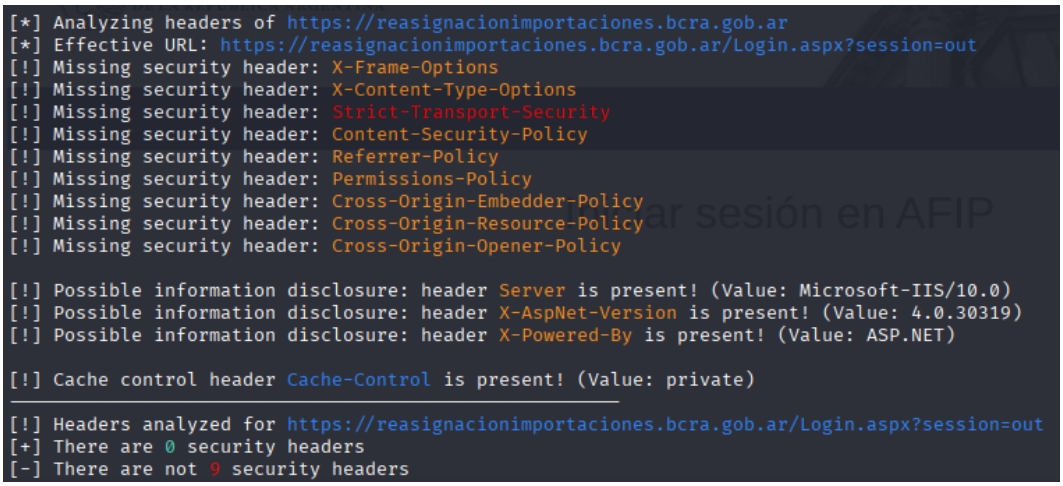
```
[*] Analyzing headers of https://ps.bcra.gob.ar
[*] Effective URL: https://ps.bcra.gob.ar
[!] Missing security header: X-Frame-Options
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy
[!] Missing security header: Referrer-Policy
[!] Missing security header: Permissions-Policy
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[!] Missing security header: Cross-Origin-Opener-Policy

[*] No information disclosure headers detected

[*] No caching headers detected
-------------------------------------------------------------

[!] Headers analyzed for https://ps.bcra.gob.ar
[+] There are 0 security headers
[-] There are not 9 security headers
```

Recurso: 45.235.96.58 (reasignacionimportaciones.bcra.gob.ar) Puerto: TCP/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: reasignacionimportaciones.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge" /><meta
name="viewport" content="width=device-width, initial-scale=1.0" /><title>
Banco Central de la Repblica Argentina
</title><link rel="icon" href="../../Content/images/favicon.ico" sizes="16x16"
type="image/ico" /><link rel="stylesheet" type="text/css"
href="../../Content/lib/fontawesome/css/all.min.css" /><link rel="stylesheet"
type="text/css" href="../../Content/lib/bootstrap/css/bootstrap.min.css" /><link
rel="stylesheet" type="text/css" href="../../Content/css/estilos.css" />
<script src="../../Content/lib/jquery/jquery-3.5.1.min.js"></script>
<script src="../../Scripts/umd/popper.min.js"></script>
<script src="../../Content/lib/bootstrap/js/bootstrap.bundle.min.js"></script>
<script src="../../Scripts/jquery.inputmask.bundle.js"></script>

</head>
<body class="d-flex flex-column min-vh-100">
<div class="container">
<header>
<div class="containner">
<div class="topnav-barra" style="position: relative; z-index: 2;">
```

```
<div class="row mt-1 ml-1">
<div class="col float-left">
<h3>Certificados de importaciones de bienes</h3>
</div>

</div>
</div>
<img src="../../Content/images/encabezado.jpg" id="imgEncabezado" style="width: 100%;
height: auto" draggable="false" class="img-fluid" />
<div class="topnav-barra topnav-barra-title-custom " style="text-align: center; position:
relative; z-index: 1;">
<h2 id="lblNombreSistema" class="mt-1 mt-sm-0"></h2>
</div>
</div>
</header>
<main class="flex-grow-1" style="margin-bottom: 30%">
<form method="post" action="./Login.aspx?session=out" id="form1" style="/*height: 100vh;
*/">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="a/owY5bhN7Jy2tQanrK5bIKl+ZbNxoikGBD1UiInRv151/hfeNMg5a1uvoAnIHruh6rsyuS6NGDhiBDPaUQCW
etTYkSEM7Dp6zQ/D0Vp2vp1W8jxgn9g4hxfZHyIFfn84PzFd2P59y8vcscmiPWtHPUF01XGjEpl8s3Q9PHnybOAV5Hxa
ZkVrAHuLzJ8VnLX" />

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="C2EE9ABB"
/>
<div class="row">
<div class="container body-content h-100 main">
<div class="row">
<div class="col-md-12">
<div class="row">
<label id="msjLoginManual" class="col col-sm-12 text-center color-custom mt-3" style="font-
size:2rem">Iniciar sesión en AFIP</label>

</div>
</div>
</div>
</div>
</div>

</form>
</main>
<footer class="footer-bcra">
<div class="row">
<div class="col-xs-12 col-sm-6 col-md-8 footer-bcra-contacto">
<ul>
<li style="font-weight: bolder">BANCO CENTRAL DE LA REPBLICA ARGENTINA</li>
<li>Reconquista 266 C1003ABF CABA Argentina</li>
<li>(011) 4348-3500</li>
<li>www.bcra.gob.ar</li>
</ul>
</div>
<div class="col-xs-6 col-sm-3 col-md-4 footer-bcra-contacto">
<ul>
<li style="font-weight: bolder">Atencin en Lnea</li>
<li>mesadeayudastaf@bcra.gob.ar</li>
</ul>
</div>
</div>
</footer>
<section style="text-align: center; margin: 10px auto; color: #B4B4B4; font-size: 100%;
font-family: Calibri, Candara, Segoe, Optima, Arial, sans-serif;">
<p>
Copyright 2006-<span id="lblAnioActual">2025</span>
| Banco Central de la Repblica Argentina | Todos los derechos reservados
</p>
</section>
```

```
</div>
</body>
</html>
Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Set-Cookie: .ASPXAUTH=; expires=Tue, 12-Oct-1999 03:00:00 GMT; path=/; HttpOnly;
SameSite=Lax
X-Powered-By: ASP.NET
Date: Thu, 10 Jul 2025 23:23:24 GMT
Content-Length: 4326
```



Recurso: 45.235.96.158 (reasignacionimportaciones.homologacion.bcra.gob.ar) Puerto: TCP/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: reasignacionimportacioneshomologacion.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0




<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge" /><meta
name="viewport" content="width=device-width, initial-scale=1.0" /><title>
Banco Central de la Repblica Argentina
</title><link rel="icon" href="../../Content/images/favicon.ico" sizes="16x16"
type="image/ico" /><link rel="stylesheet" type="text/css"
href="../../Content/lib/fontawesome/css/all.min.css" /><link rel="stylesheet"
type="text/css" href="../../Content/lib/bootstrap/css/bootstrap.min.css" /><link
rel="stylesheet" type="text/css" href="../../Content/css/estilos.css" />
<script src="../../Content/lib/jquery/jquery-3.5.1.min.js"></script>
<script src="../../Scripts/umd/popper.min.js"></script>
<script src="../../Content/lib/bootstrap/js/bootstrap.bundle.min.js"></script>
<script src="../../Scripts/jquery.inputmask.bundle.js"></script>

</head>
<body class="d-flex flex-column min-vh-100">
```

```
<div class="container">
<header>
<div class="containner">
<div class="topnav-barra" style="position: relative; z-index: 2;">
<div class="row mt-1 ml-1">
<div class="col float-left">
<h3>Certificados de importaciones de bienes</h3>
</div>

</div>
</div>
<img src="../../Content/images/encabezado.jpg" id="imgEncabezado" style="width: 100%;
height: auto" draggable="false" class="img-fluid" />
<div class="topnav-barra topnav-barra-title-custom " style="text-align: center; position:
relative; z-index: 1;">
<h2 id="lblNombreSistema" class="mt-1 mt-sm-0"></h2>
</div>
</div>
</header>
<main class="flex-grow-1" style="margin-bottom: 30%">
<form method="post" action="./Login.aspx?session=out" id="form1" style="/*height: 100vh;
*/">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="6IvVywfvwRE54XNjRcnxRujf2OdY6RGGGM7wWJyW8dGxqY+5rfkVRkOXYUgd0qAkDTvESzV5CDtBzz484ZQKe
AGJCzIzEhWicJ8v8zSHPvsMDzctcoPN4lLZqimf+5S9PTNBQndXczjLJLyGvdl/YE0IOCHC0olQ4PuHgM4b2m27hB0dU
94eQ+txfiGrSVc6" />

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="C2EE9ABB"
/>
<div class="row">
<div class="container body-content h-100 main">
<div class="row">
<div class="col-md-12">
<div class="row">
<label id="msjLoginManual" class="col col-sm-12 text-center color-custom mt-3" style="font-
size:2rem">Iniciar sesión en AFIP</label>

</div>
</div>
</div>
</div>
</div>

</form>
</main>
<footer class="footer-bcra">
<div class="row">
<div class="col-xs-12 col-sm-6 col-md-8 footer-bcra-contacto">
<ul>
<li style="font-weight: bolder">BANCO CENTRAL DE LA REPBLICA ARGENTINA</li>
<li>Reconquista 266 C1003ABF CABA Argentina</li>
<li>(011) 4348-3500</li>
<li>www.bcra.gob.ar</li>
</ul>
</div>
<div class="col-xs-6 col-sm-3 col-md-4 footer-bcra-contacto">
<ul>
<li style="font-weight: bolder">Atencin en Lnea</li>
<li>mesadeayudastaf@bcra.gob.ar</li>
</ul>
</div>
</div>
</footer>
<section style="text-align: center; margin: 10px auto; color: #B4B4B4; font-size: 100%;
font-family: Calibri, Candara, Segoe, Optima, Arial, sans-serif;">
<p>
```

```
Copyright 2006-<span id="lblAnioActual">2025</span>
| Banco Central de la Repblica Argentina | Todos los derechos reservados
</p>
</section>
</div>
</body>
</html>
Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Set-Cookie: .ASPXAUTH=; expires=Tue, 12-Oct-1999 03:00:00 GMT; path=/; HttpOnly
X-Powered-By: BCRA
Date: Thu, 10 Jul 2025 23:22:17 GMT
Content-Length: 4326
```

```
[*] Analyzing headers of https://reasignacionimportacioneshomologacion.bcra.gob.ar
[*] Effective URL: https://reasignacionimportacioneshomologacion.bcra.gob.ar/Login.aspx?session=out
[!] Missing security header: X-Frame-Options
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy
[!] Missing security header: Referrer-Policy
[!] Missing security header: Permissions-Policy
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[!] Missing security header: Cross-Origin-Opener-Policy

[!] Possible information disclosure: header Server is present! (Value: Microsoft-IIS/10.0)
[!] Possible information disclosure: header X-Powered-By is present! (Value: BCRA)
[!] Possible information disclosure: header X-AspNet-Version is present! (Value: 4.0.30319)

[!] Cache control header Cache-Control is present! (Value: private)
---------------------------------------------------------------
[!] Headers analyzed for https://reasignacionimportacioneshomologacion.bcra.gob.ar/Login.aspx?session=out
[+] There are 0 security headers
[-] There are not 9 security headers
```

Recurso: 45.235.96.25 (qa.bcra.gob.ar) Puerto: TCP/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: qa.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



<head>
<meta http-equiv='refresh' content='0; URL=../psp/sup/SUPPLIER/ERP/h/?tab=DEFAULT' />
</head>

Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Date: Fri, 11 Jul 2025 00:20:09 GMT
Accept-Ranges: bytes
Content-Length: 105
Content-Type: text/html;charset=utf-8
Last-Modified: Fri, 01 Dec 2023 20:30:52 GMT
X-ORACLE-DMS-ECID: 4f8d6b29-63ce-48e0-8db0-9ff4bf7c61a2-000351ad
X-ORACLE-DMS-RID: 0
Set-Cookie:
TS66dffa1d027=08403d584cab2000a01a4d84edac48d7fb4df86ffacde2e08612f9e15a2052a7511ced980639b9
4408aef14b4f1130002e887cf7be715f4e5331ab547f8cbce6ff5b3a95c649d559d4aabc9398059a8a2901aa7b8a
d35ae75e2ce5218ea4178c; Path=/
```

```
[*] Analyzing headers of https://qa.bcra.gob.ar
[*] Effective URL: https://qa.bcra.gob.ar
[!] Missing security header: X-Frame-Options
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy
[!] Missing security header: Referrer-Policy
[!] Missing security header: Permissions-Policy
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[!] Missing security header: Cross-Origin-Opener-Policy

[*] No information disclosure headers detected

[*] No caching headers detected
---------------------------------------------------------------
[!] Headers analyzed for https://qa.bcra.gob.ar
[+] There are 0 security headers
[-] There are not 9 security headers
```

Recurso: 45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: TCP/443

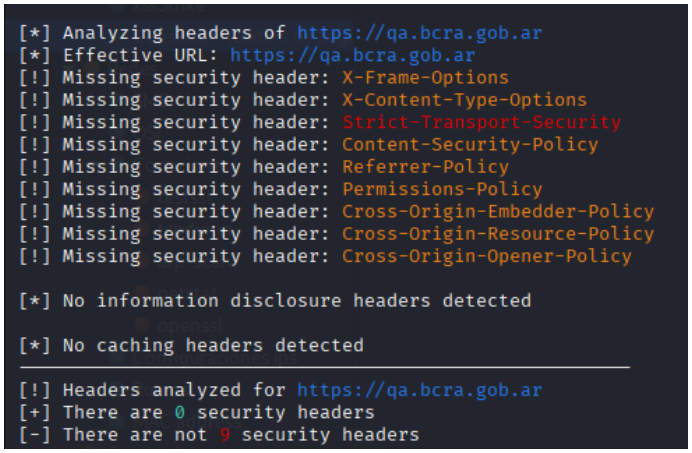
```
Strict-Transport-Security HTTP Header missing on port 443.

GET / HTTP/1.1
Host: controlcambio.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Set-Cookie: ASP.NET_SessionId=bl2vberawh1fr1sglc1gymw4; path=/; secure; HttpOnly;
SameSite=Strict
X-XSS-Protection: 1; mode=block
X-Frame-Options: deny
X-Content-Type-Options: nosniff
Date: Fri, 11 Jul 2025 00:21:54 GMT
Content-Length: 28002
```

```
[*] Analyzing headers of https://controlcambio.bcra.gob.ar
[*] Effective URL: https://controlcambio.bcra.gob.ar
[*] Header X-XSS-Protection is present! (Value: 1; mode=block)
[*] Header X-Frame-Options is present! (Value: deny)
[*] Header X-Content-Type-Options is present! (Value: nosniff)
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy
[!] Missing security header: Referrer-Policy
[!] Missing security header: Permissions-Policy
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[!] Missing security header: Cross-Origin-Opener-Policy

[*] No information disclosure headers detected

[!] Cache control header Cache-Control is present! (Value: no-cache)
[!] Cache control header Pragma is present! (Value: no-cache)
---------------------------------------------------------------
[!] Headers analyzed for https://controlcambio.bcra.gob.ar
[+] There are 3 security headers
[-] There are not 7 security headers
```

Recurso: 45.235.97.25 (qa.bcra.gob.ar) Puerto: TCP/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
```

```
Host: qa.bcra.gob.ar
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



<head>
<meta http-equiv='refresh' content='0; URL=../psp/sup/SUPPLIER/ERP/h/?tab=DEFAULT' />
</head>

Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Date: Fri, 11 Jul 2025 03:20:57 GMT
Accept-Ranges: bytes
Content-Length: 105
Content-Type: text/html;charset=utf-8
Last-Modified: Fri, 01 Dec 2023 20:30:52 GMT
X-ORACLE-DMS-ECID: 4f8d6b29-63ce-48e0-8db0-9ff4bf7c61a2-00038539
X-ORACLE-DMS-RID: 0
```



#10 Account Brute Force Possible Through IIS NTLM Authentication Scheme				
Severidad: Media	**Access Vector**	Network	**Confidentiality Impact**	Partial
CVSS: 5.0	**Access Complexity**	Low	**Integrity Impact**	None
Ocurrencias: 2	**Authentication**	None	**Availability Impact**	None

Recursos Afectados

45.235.96.108 (notificacioneselectronicas.bcra.gob.ar) Puerto: TCP/443
45.235.97.108 (bcraweb.bcra.gob.ar) Puerto: TCP/443

Descripción

La autenticación NTLM está activada en el servidor web de Microsoft IIS. Esto permite a un usuario remoto realizar ataques de fuerza bruta, solicitando un recurso HTTP no existente o un recurso HTTP existente que en realidad no requiere autenticación. Las solicitudes incluirían el campo "Authorization: NTLM".

Impacto

Un atacante puede intentar ataques de fuerza bruta contra identificadores de Windows conocidos, incluyendo la cuenta de Administrador. Windows también tiene algunos nombres predeterminados fáciles de adivinar para cuentas incorporadas.
Si el host tiene una política de bloqueo de cuenta en su lugar, un usuario remoto puede explotar esta vulnerabilidad para bloquear a un usuario local, siempre que se conozca el mismo.
Si el host no tiene una política de bloqueo de cuenta en su lugar, un usuario remoto puede explotar esta vulnerabilidad para realizar un ataque de fuerza bruta con un diccionario de contraseñas.
Además, si la solicitud tiene el atributo NTLMSSP_REQUEST_TARGET hablitado, el servidor Web puede responder a la solicitud con un desafío NTLM que contiene información sensible, como la versión de Windows y el dominio en el que se comprobará la autenticación.

Solución

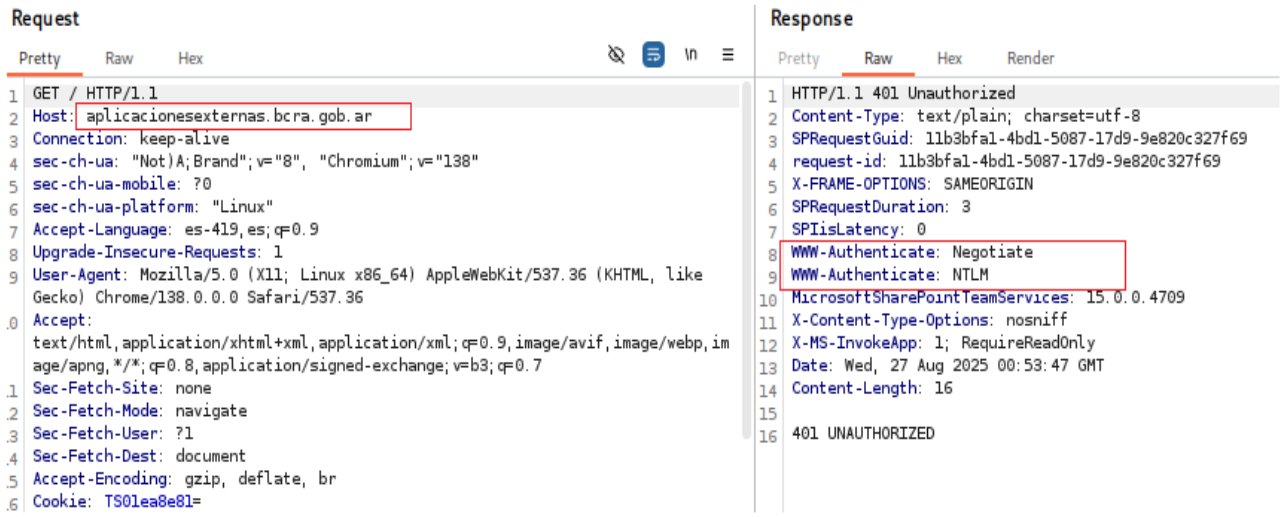
Actualmente no hay ningún vendedor suministrado parches disponibles para este problema.
Workaround:
1) Desactivar la autenticación NTLM para su servidor Web. Esto se puede hacer desmarcando "Authentication Method" en "Authentication Method" bajo "Directory Security" en "Default Web Site Properties".
Nota: Si la NTLM no puede ser deshabilitada, una opción de remediación alternativa para este tema es realizar las siguientes 2 acciones:
1) Asegurar que exista una política de bloqueo de cuentas.
2) Asegurar que la Cuenta Administradora haya sido renombrada a algo diferente.
Una política de bloqueo asegurará que un atacante no tenga una cantidad ilimitada de tiempo y los intentos de adivinar la contraseña. La Cuenta Admin debe ser renombrada porque por defecto la política de bloqueo no se aplica a la Cuenta Administradora.
Para IIS 7.x , consulte Autenticación de Windows (http://www.iis.net/configreference/system.webserver/security/authentication/windowsauthentication) para más detalles.

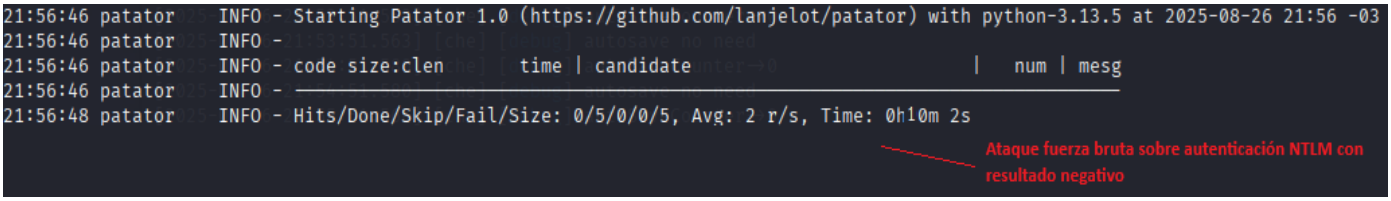
Evidencias

Recurso: 45.235.96.108 (notificacioneselectronicas.bcra.gob.ar) Puerto: TCP/443

```
GET / HTTP/1.1
Host: aplicacionesexternas.bcra.gob.ar
Connection: Keep-Alive
Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAgAAAADwAPACAAAABRVUFMWVMtR08wSVFZWU4AAA==



HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM
TlRMTVNTUAACAAAACAAIADgAAAAFgoECjulce9guKwkAAAAAAAAAAJwAnABAAAAABgOAJQAAAA9CAEMAUgBBAAIACABC
AEMAUgBBAAEAFgBQAFIATwBEAEQATQBaAFMASABGAEUABAAWAGIAYwByAGEALgBnAG8AdgAuAGEAcgADAC4AUABy AG8A
```

```
ZABEAE0AWgBTAGgARgBlAC4AYgBjAHIAYQAuAGcAbwB2AC4AYQByAAUAFgBiAGMAcgBhAC4AZwBvAHYALgBhAHIABwAI
APlNiTP88dsBAAAAAA==
SPRequestGuid: 8b91b0a1-9bac-5087-17d9-9930abffeaaf
request-id: 8b91b0a1-9bac-5087-17d9-9930abffeaaf
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 1
SPIisLatency: 0
WWW-Authenticate: Negotiate
MicrosoftSharePointTeamServices: 15.0.0.4709
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Fri, 11 Jul 2025 00:39:02 GMT
Content-Length: 0
Set-Cookie:
TS01ea8e81=01532640e80ada0424ffcda521ed6d84614665edb04f0a21e64dc16f1a265f41ba4b78e6b27409ddc
4d54838e2866425e4efb53a93; Path=/; HttpOnly;
```





Recurso: 45.235.97.108 (bcraweb.bcra.gob.ar) Puerto: TCP/443

```
GET / HTTP/1.1
Host: aplicacionesexternas.bcra.gob.ar
Connection: Keep-Alive
Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAgAAAADwAPACAAAABRVUFMWVMtR08wSVFZWU4AAA==



HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM
TlRMTVNTUAACAAAACAAIADgAAAAFgoEClGydcUOgosoAAAAAAAAAAJwAnABAAAAABgOAJQAAAA9CAEMAUgBBAAIACABC
AEMAUgBBAAEAFgBQAFIATwBEAEQATQBaAFMASABGAEUABAAWAGIAYwByAGEALgBnAG8AdgAuAGEAcgADAC4AUABy AG8A
ZABEAE0AWgBTAGgARgBlAC4AYgBjAHIAYQAuAGcAbwB2AC4AYQByAAUAFgBiAGMAcgBhAC4AZwBvAHYALgBhAHIABwAI
ADGGa98B8tsBAAAAAA==
SPRequestGuid: de93b0a1-9b5d-5087-17d9-994b3bdca804
request-id: de93b0a1-9b5d-5087-17d9-994b3bdca804
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 1
```

```
SPIisLatency: 0
WWW-Authenticate: Negotiate
MicrosoftSharePointTeamServices: 15.0.0.4709
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Fri, 11 Jul 2025 01:19:39 GMT
Content-Length: 0
Set-Cookie:
TS01ea8e81=01532640e810be08d347f3ae92a8c0350941123d7190e1001a6cf1019d1e61d701cff8b4f9fb0589a
cf64080c51c440833621ff3b1; Path=/; HttpOnly;
```

Request

Pretty Raw Hex

```
1  GET / HTTP/1.1
2  Host: aplicacionesexternas.bcra.gob.ar
3  Connection: keep-alive
4  Cache-Control: max-age=0
5  sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Linux"
8  Accept-Language: es-419,es;q=0.9
9  Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/138.0.0.0 Safari/537.36
11 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
   age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate, br
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 401 Unauthorized
2  Content-Type: text/plain; charset=utf-8
3  SPRequestGuid: e7aebfa1-0b51-5087-17d9-99242a2f5f2e
4  request-id: e7aebfa1-0b51-5087-17d9-99242a2f5f2e
5  X-FRAME-OPTIONS: SAMEORIGIN
6  SPRequestDuration: 2
7  SPIisLatency: 0
8  WWW-Authenticate: Negotiate
9  WWW-Authenticate: NTLM
10 MicrosoftSharePointTeamServices: 15.0.0.4709
11 X-Content-Type-Options: nosniff
12 X-MS-InvokeApp: 1; RequireReadOnly
13 Date: Tue, 26 Aug 2025 23:40:58 GMT
14 Content-Length: 16
15
16 401 UNAUTHORIZED
```

```
21:15:34 patator    INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.13.5 at 2025-08-26 21:15 -03
21:15:34 patator    INFO -
21:15:34 patator    INFO - code size:clen       time | candidate                          |   num | mesg
21:15:34 patator    INFO - -----------------------------------------------------------------------------
21:15:36 patator    INFO - Hits/Done/Skip/Fail/Size: 0/5/0/0/5, Avg: 2 r/s, Time: 0h 20 2s
```

Fuerza bruta NTLM (resultado negativo)

#11 Deprecated Public Key Length				
Severidad: Media	**Access Vector**	Network	**Confidentiality Impact**	None
CVSS: 5.0	**Access Complexity**	Low	**Integrity Impact**	Partial
Ocurrencias: 1	**Authentication**	None	**Availability Impact**	None

Recursos Afectados
45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

Descripción
NIST tiene una publicación especial [SP800-131A]
(http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf)
en la que hace varias recomendaciones sobre el uso de algoritmos criptográficos y la longitud de las claves. La recomendación para la longitud de la clave es:
- las longitudes de clave inferiores a 1024 bits no están permitidas, lo que significa que se consideran débiles y no deben utilizarse.
- las longitudes de clave entre 1024 bits y 2047 bits están obsoletas.
- las longitudes de clave a partir de 2048 bits están aprobadas y su uso es seguro.

Impacto
Una clave debe ser lo suficientemente grande como para que un ataque de fuerza bruta sea inviable, es decir, que tarde demasiado en ejecutarse.

Solución
Obtenga un certificado de clave pública de 2048 bits o más de su autoridad de certificación.

Evidencias
Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

```
Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:bc:56:72:bb:09:45:02:18:6e:a0:1f:cb:c8:24:
7c:74:0d:dd:b2:33:bd:7b:8e:23:e8:59:d8:04:02:
73:a1:5c:77:8b:f9:ae:b2:b3:f8:a9:1b:3f:a0:7c:
69:6f:47:8e:9a:80:c1:5e:a5:de:39:97:8c:cb:83:
5e:a1:5f:19:de:4f:96:a4:bc:45:4f:33:28:4d:de:
05:14:ea:54:64:c5:6c:cb:40:80:81:1e:2a:46:a7:
17:23:57:1c:c6:c0:cc:a6:48:e3:f4:60:5a:8a:f6:
37:29:30:17:9f:93:ea:8a:9b:78:22:d6:fa:28:55:
39:df:7d:15:5e:05:b3:ee:93
Exponent: 65537 (0x10001)
```

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    1024
```

#12 Microsoft ASP.NET Custom Errors Found Turned Off				
Severidad: Media	**Access Vector**	Network	**Confidentiality Impact**	Partial
CVSS: 5.0	**Access Complexity**	Low	**Integrity Impact**	None
Ocurrencias: 2	**Authentication**	None	**Availability Impact**	None

Recursos Afectados
45.235.96.103 (www2.bcra.gob.ar) Puerto: TCP/443
45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: TCP/443

Descripción
La etiqueta "customErrors" en ASP. Los archivos de configuración NET afectan cómo se gestionan las páginas de error en un ASP. Aplicación NET y si los desarrolladores pueden redirigir a los usuarios a sus páginas de error personalizadas cuando se lanza una excepción.
ASP. NET produce una página de error cuando una aplicación lanza una excepción sin manipular o cuando usted implementa un archivo .aspx cuya fuente contiene un error de sintaxis. Sin errores personalizados, la página de error generada podría contener extractos del código fuente de la página o los rastros de pila, con información confidencial no destinada a clientes remotos.

Impacto
La información sensible revelada a clientes remotos puede utilizarse para lanzar futuros ataques. Al redirigir el navegador del cliente a una página de error personalizado sanitizada, se evita cualquier fuga de información.

Solución
Utilice las opciones de configuración "On" o "RemoteOnly" para los atributos "customErrors" en la máquina global. config o el archivo web.config específico de instalación. Véase [ASP.NET Seguridad](http://msdn.microsoft.com/en-us/library/91f66yxt\(v=vs.100\).aspx) en Microsoft MSDN para obtener información sobre los servicios Web.
Tenga en cuenta que, hemos encontrado que ASP. NET 1.0 no implementa los modos personalizadosErrors correctamente, e incluso con un modo establecido en 'On' o 'RemoteOnly', el sistema puede todavía generar mensajes de excepción de solicitudes de remoción. Si la sección Resultados abajo sólo muestra la prueba de remoción ".soap", y no la prueba de servicio web ".asmx", entonces este es el caso. Si es posible, por favor actualice a ASP. Marco NET 1.1. Else, si la remoción no se utiliza, deshabilita el manejador ".soap" usando la configuración IIS o la siguiente configuración en la máquina. archivo config:

▪ httpHandlers
.rem
Tipo="System.Web.HtpForbiddenHandler"/

##
##
##
Tipo="System.Web.HtpForbiddenHandler"/
■/httpHandlers

Si se requiere remoción, entonces ASP. NET versión 1.1 proporciona una configuración personalizadaErrors para la remoción específicamente:

▪configuración

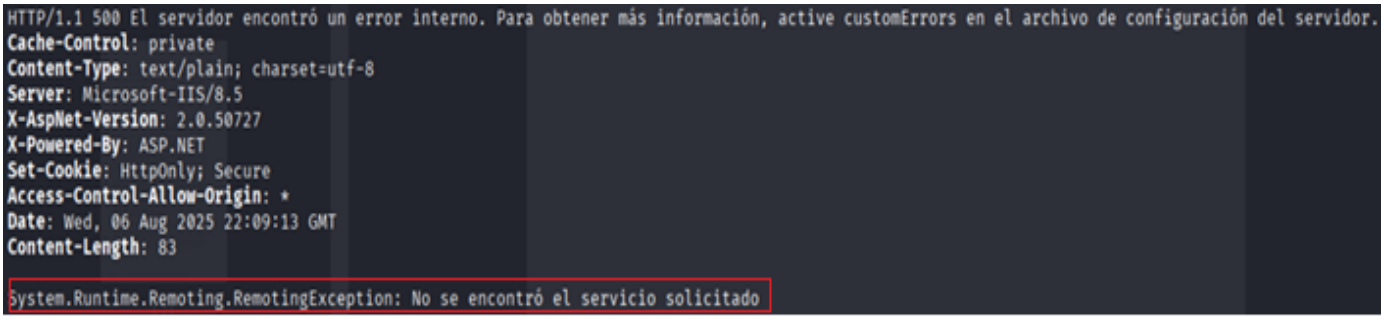
##
##
##

"Modo de terrores" ="off"
■/system.runtime.remoting
Identificado/configuración

Evidencias

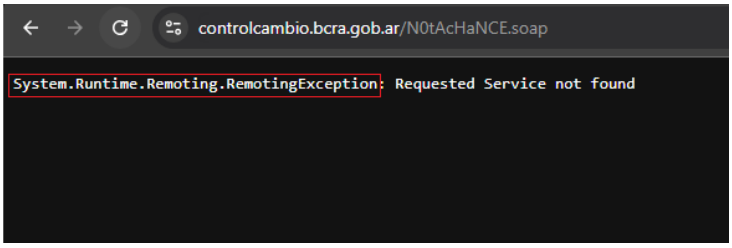
Recurso: 45.235.96.103 (www2.bcra.gob.ar) Puerto: TCP/443

```
GET /N0tAcHaNCE.soap HTTP/1.1
Host: www2.bcra.gob.ar
Connection: Keep-Alive



System.Runtime.Remoting.RemotingException: No se encontr el servicio solicitado
```



Recurso: 45.235.96.31 (controlcambio.bcra.gob.ar) Puerto: TCP/443

```
GET /N0tAcHaNCE.soap HTTP/1.1
Host: controlcambio.bcra.gob.ar
Connection: Keep-Alive



System.Runtime.Remoting.RemotingException: Requested Service not found
```



#13 Frameable response (potential Clickjacking)				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 5.0	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
https://45.235.96.103/

Descripción
Si una página no establece un encabezado HTTP adecuado X-Frame-Options o Content-Security-Policy, puede ser posible que una página controlada por un atacante la cargue dentro de un iframe. Esto puede permitir un ataque de secuestro de clicks, en el que la página del atacante superpone la interfaz de la aplicación de destino con una interfaz diferente proporcionada por el atacante. Al inducir a los usuarios a realizar acciones tales como clicks de ratón y pulsaciones de teclas, el atacante puede hacer que realicen involuntariamente acciones dentro de la aplicación que está siendo apuntada. Esta técnica permite al atacante eludir las defensas contra la falsificación de solicitud inter-sitio, y puede resultar en acciones no autorizadas.
Tenga en cuenta que algunas aplicaciones intentan evitar estos ataques dentro de la propia página HTML, utilizando el código "framebusting". Sin embargo, este tipo de defensa es normalmente ineficaz y generalmente puede ser eludido por un atacante.
Usted debe determinar si cualquier función accesible dentro de páginas enmarcables puede ser utilizado por los usuarios de aplicaciones para realizar cualquier acción sensible dentro de la aplicación.
Referencias:
  * [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options)

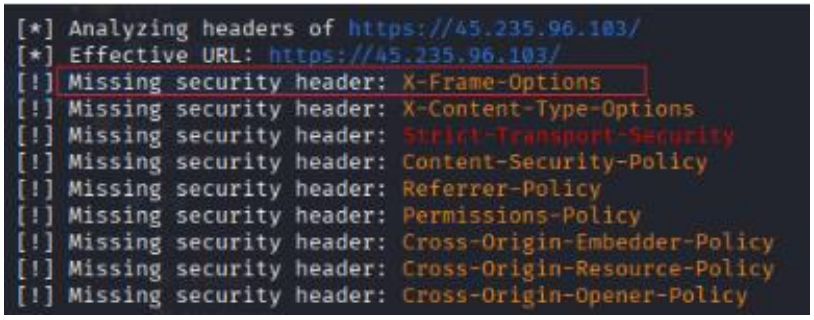
Impacto
* [CWE-693: Mecanismo de protección](https://cwe.mitre.org/data/definitions/693.html)

Referencias
* [Web Security Academy: Clickjacking](https://portswigger.net/web-security/clickjacking)
  * [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options)

Solución
Para prevenir eficazmente los ataques de framing, la aplicación debe devolver un encabezado de respuesta con el nombre **X-Frame-Options** y el valor **DENY** para evitar el encuadre total, o el valor **SAMEORIGIN** permitir el encuadre sólo por páginas en el mismo origen que la respuesta misma. Tenga en cuenta que el encabezado SAMEORIGIN puede ser eliminado parcialmente si la aplicación en sí puede ser hecha para enmarcar sitios web no confiables.

Evidencias
Recurso: https://45.235.96.103/

```
GET / HTTP/1.1
Host: 45.235.96.103
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Connection: close
Cache-Control: max-age=0
```



#14 Weak SSL/TLS Key Exchange				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 4.8	**Attack Complexity**	High	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

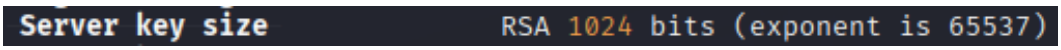
Descripción
El servidor SSL/TLS admite intercambios de llaves que son criptográficamente más débiles de lo recomendado. Los intercambios de clave deben proporcionar al menos 112 bits de seguridad, lo que se traduce en un tamaño mínimo de 2048 bits para intercambios de clave Diffie Hellman y RSA.

Impacto
Un atacante con acceso a suficiente poder computacional podría recuperar la clave de sesión y descifrar el contenido de sesión.

Solución
Cambie la configuración del servidor SSL/TLS para permitir solo intercambios de llaves fuertes.

Evidencias
Recurso: 45.235.96.64 (vpn.bcra.gob.ar) Puerto: TCP/443

PROTOCOL	CIPHER NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1	AES256-SHA	RSA	1024	no	80	low
TLSv1	AES128-SHA	RSA	1024	no	80	low
TLSv1.1	AES256-SHA	RSA	1024	no	80	low
TLSv1.1	AES128-SHA	RSA	1024	no	80	low
TLSv1.2	AES256-SHA256	RSA	1024	no	80	low
TLSv1.2	AES128-SHA256	RSA	1024	no	80	low
TLSv1.2	AES256-GCM-SHA384	RSA	1024	no	80	low
TLSv1.2	AES128-GCM-SHA256	RSA	1024	no	80	low
TLSv1.2	AES256-SHA	RSA	1024	no	80	low
TLSv1.2	AES128-SHA	RSA	1024	no	80	low



Conclusiones y recomendaciones finales

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

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
Aplicar parches o actualizar el software obsoleto o con vulnerabilidades conocidas a las versiones recomendadas por los fabricantes.	Alto	#1 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected
Configurar el servidor para enviar la cadena de certificados completa (incluyendo todos los intermedios necesarios hasta la CA raíz de confianza).	Medio	#2 Incomplete SSL Certificate Chain Vulnerability
Instalar un certificado que no exceda la validez máxima recomendada acorde a las buenas prácticas de seguridad.	Medio	#3 SSL Certificate - Invalid Maximum Validity Date Detected
Instalar un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.	Medio	#4 SSL Certificate - Self-Signed Certificate
	Medio	#5 SSL Certificate - Signature Verification Failed Vulnerability
Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, CBC, RC2, RC4, MD5, SHA1), en favor de protocolos criptográficamente más fuertes.	Medio	#6 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
	Medio	#14 Weak SSL/TLS Key Exchange
Eliminar o restringir el acceso al directorio .git en entornos productivos.	Medio	#7 GIT Detected
Dejar de publicar a Internet servicios que no se encuentren en uso o sean innecesarios.	Medio	#8 Information disclosure
Configurar el servidor web para utilizar todos los encabezados de seguridad HTTP acordes a las buenas prácticas de seguridad.	Medio	#9 HTTP Security Header Not Detected
Configurar los servicios utilizados de acuerdo a las buenas prácticas y recomendaciones de seguridad indicadas por los fabricantes.	Medio	#10 Account Brute Force Possible Through IIS NTLM Authentication Scheme
Utilizar claves públicas de longitudes consideradas seguras (mínimo 2048 bits)	Medio	#11 Deprecated Public Key Length

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 determinar la superficie de ataque.

Etapa 2: Detección de Vulnerabilidades

Se utilizaron herramientas automatizadas para identificar y evaluar vulnerabilidades en los sistemas auditados. 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 algunos de los elementos buscados, 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.

Etapa 3: Análisis de Resultados

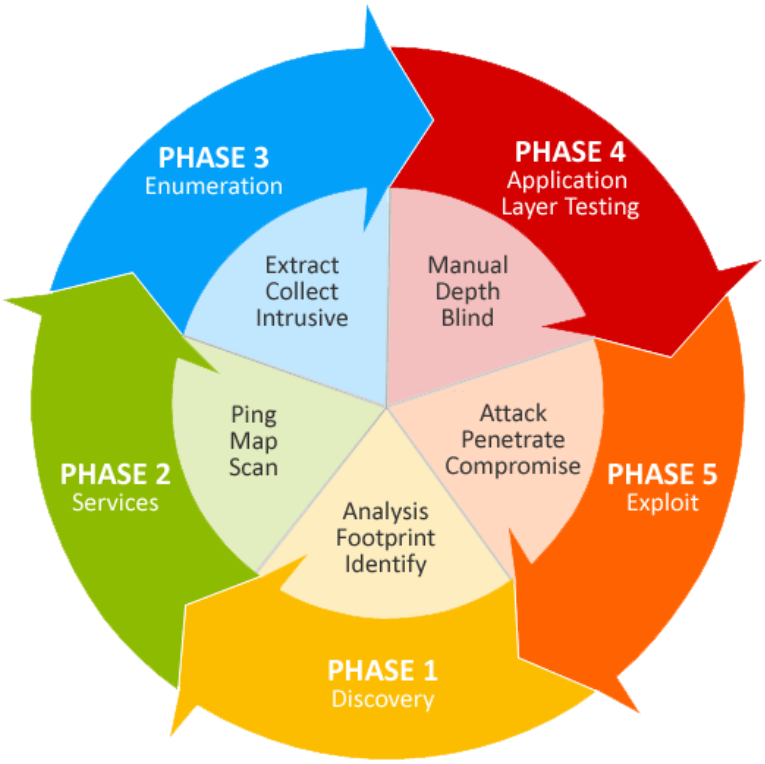
Se realizó un análisis detallado de las vulnerabilidades detectadas con verificaciones manuales, a fin de eliminar los “falsos positivos”, corroborar las detecciones y obtener la evidencia necesaria.

Etapa 4: 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, destacando el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información asociada necesaria 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.
- Nikkto: Escanner que se utiliza para realizar pruebas de seguridad en servidores web. Permite identificar configuraciones inseguras, versiones desactualizadas de software, archivos y scripts potencialmente peligrosos, así como prácticas inseguras en HTTP/HTTPS.
- 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.