Your Global Cyber-Security Partner

REPORTE DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA COPA AIRLINES

Septiembre 28, 2018

COSTA DEL ESTE, AVE. LA ROTONDA, EDIF. PRIME TIME, PISO 24 , OFICINA 24A
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

PROPIEDADES DEL DOCUMENTO

Título	Black Box Penetration Testing Report
Versión	V 1.0
Autor	Daniel Ortiz
Pen-testers	Daniel Ortiz
Revisado por	Sergio Heker
Clasificación	Confidencial

CONTROL DE VERSIÓN

Versión	V 1.0
Fecha	28/09/2018
Autor	Confidencial
Descripción	Reporte final

CONFIDENCIAL

ÍNDICE DE CONTENIDO

REPORTE DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA COPA

CONFIDENCIAL

ÍNDICE DE TABLAS, IMÁGENES Y GRÁFICOS

CONFIDENCIAL

1 REPORTE EJECUTIVO

El presente informe detalla las auditorías realizadas a la infraestructura indicada por COPA durante el período 17 al 21 de septiembre. La finalidad de la presente auditoría es verificar la postura de seguridad y poder identificar posibles fallas de seguridad.

CONFIDENCIAL

1.1 ALCANCE DE LA AUDITORÍA

Este análisis de seguridad cubre los recursos identificados en el archivo "GLESEC Assessment Questionnaire". El presente estudio fue abordado desde una perspectiva Black Box, donde únicamente fue suministrada la IP de los equipos para realizar estas pruebas.

1.2 OBJETIVOS DE LA AUDITORÍA

El presente estudio tiene como finalidad poder identificar aquellos equipos y servicios que se encuentran vulnerables y que pueden ser accesibles desde internet. Las vulnerabilidades fueron clasificadas según el impacto y el nivel de amenaza.

1.3 SUPOSICIONES

Durante la elaboración de este informe se tuvo presente que algunos equipos fueron accesibles desde Internet, esto permitió realizar pruebas más exhaustivas en estos equipos, dejando a un lado aquellos equipos que no fueron posibles de ser accesados.

1.4 CRONOGRAMA DE LA AUDITORÍA

A continuación, se detallan el plan de actividades y su tiempo de duración ara la presente auditoría:

Actividad	Fecha de Inicio	Fecha de Finalización
Penetration testing	17/09/2018	25/09/2018
Elaboración del informe	26/09/2018	28/09/2018

Tabla 1. Cronograma del estudio.

1.5 RESUMEN DE HALLAZGOS

Riesgo	Número de vulnerabilidades
Info	**78**
Bajo	**2**
Mediano	**7**
Alto	**0**

Tabla 2. Resumen de Hallazgos.

Fue posible identificar vulnerabilidades de rango mediano en 2 equipos de los 5 incluidos en la auditoría, debido a la naturaleza de las vulnerabilidades, es posible que un atacante pueda robar información sensible del negocio al realizar un ataque de MITM, la carencia de certificados digitales de confianza permite que sea posible no

CONFIDENCIAL

validar la autenticidad del origen y que los usuarios de la plataforma puedan ser objetivos potenciales de phishing.

Adicionalmente fue posible obtener información importante de los servicios que están corriendo en estos dos equipos, permitiendo formular un ataque más sofisticado en la plataforma, como también aprovechar alguna vulnerabilidad desarrollando algún exploit o aprovechando alguno disponible.

Para finalizar, se encontraron endpoints que no utilizan métodos de autenticación, esto permite la posibilidad de ataques de DoS a componentes específicos de la aplicación.

CONFIDENCIAL

2. METODOLOGÍA

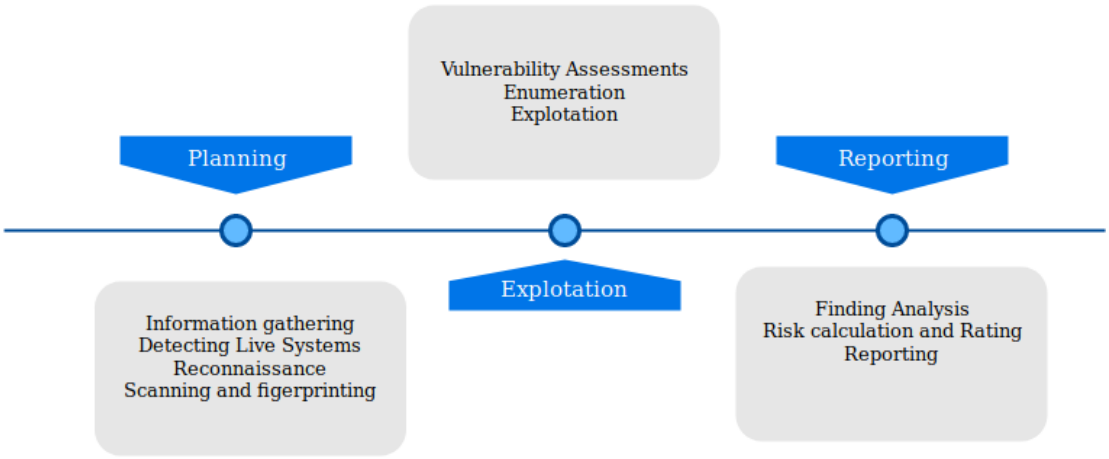


Imagen 1. Penetration testing methodology.

2.1 PLANIFICACIÓN

Durante las pruebas se recolectó información de los equipos disponibles utilizando diferentes fuentes. Adicionalmente aprovechando la conectividad de los equipos de GLESEC desde AWS, se efectuaron técnicas de fingerprinting y scanning con el objetivo de recolectar mayor información.

2.2 EXPLOTACIÓN

Luego de la información recolectada durante la etapa de fingerprinting y scanning, se procedió a buscar la forma de explotar alguna vulnerabilidad en los sistemas auditados.

2.3 REPORTE

Posterior a la obtención de los resultados, se procedió a la medición de riesgo y a la elaboración del presente informe.

3. NARRATIVA DEL ATAQUE

3.1 SCANNING AND FINGERPRINTING FROM THE WEB

A continuación se presentan los equipos que se encuentran visibles desde internet y la información que un atacante podría obtener haciendo un escaneo de puertos.

IP	SYSTEM TYPE	OS INFORMATION	OPEN PORTS			
			PORT	PROTOCOL	SERVICE NAME	STATUS
52.205.206.235	SERVER	LINUX	22	TCP	SSH	**OPEN**
			80	TCP	HTTP	CLOSED

CONFIDENCIAL

			443	TCP	HTTPS	**OPEN**
18.209.36.128	SERVER	LINUX	22	TCP	SSH	**OPEN**
			80	TCP	HTTP	CLOSED
			443	TCP	HTTPS	**OPEN**
52.201.64.250	SERVER	LINUX	4443	TCP	PHAROS	**OPEN**

Tabla 3. Scanning and fingerprinting from the web.

CONFIDENCIAL

3.2 JUICY INFORMATION FROM SHODAN

La información recolectada en el escaneo anterior por sí sola no es muy útil, ya que no es posible identificar los servicios ni las versiones que se encuentran en ejecución. Un atacante podría utilizar otros mecanismos para obtener información de sus objetivos, uno de ellos puede ser **SHODAN** (https://www.shodan.io/) que es un **search engine** empleado para obtener información de cualquier dispositivo conectado a internet.

A continuación utilizando la API de SHODAN se desarrolló un script que consulta la base de datos de este servicio con el objetivo de identificar si hay disponible algún tipo de información de los servidores presentes en la auditoría.

```
from providers.search_engine import ShodanEngine
from providers import config


def main():
    """ Main method """
    ips = ['52.201.64.250', "18.213.166.25", "18.233.210.129", "52.205.206.233", "18.209.36.128"]
    for i in ips:
        search_ip(i.__str__())



def search_ip(ip):
    """ Search for specific IP Address"""
    client = ShodanEngine(config.API_KEY_SHODAN)
    api = client.init_shodan()
    try:
        host = api.host(ip)
        for item in host['data']:
            print("""
                Port: {}
                Banner: {}

                """.format(item['port'], item['data']))
    except Exception:
        print("No information available about " + ip)


if __name__ == '__main__':
    main()
```

Imagen 2. Script para consultar API de SHODAN.

Luego de la ejecución del script se obtuvo información interesante de los servidores, es importante mencionar que este servicio "**SHODAN**" es público y puede ser utilizado por cualquier persona. El script se encuentra disponible en la sección de anexos.

A continuación, el detalle de los equipos utilizando la información obtenida con SHODAN:

CONFIDENCIAL

3.3 DETALLES DE SISTEMAS ENCONTRADOS EN SHODAN

IP	**52.201.64.250**
SERVER	APACHE-COYOTE/1.1
SET-COOKIE	AWSALB=WYVLJRKCSDJW7GT4ZLORMFJU4HJ5USLEIC1NXGHTJQZDJHHM7ZRYOJC95UYKWNSX3291ETNFCCJJHTMOTCSX0EREXPBYN4KI3STYFLGXH5R6/6GWOHQKPXFMBPW9
OPEN PORTS	4443
XSS-PROTECTION	1
SET-COOKIE	CURRENTCOUNTRY=; PATH=/; SECURE
STRICT-TRANSPORT	HTTPS://52.201.64.250/ES/WEB/GUEST
STRICT-TRANSPORT-SECURITY	MAX-AGE:86400; INCLUDESUBDOMAINS
X-FRAME-OPTIONS	SAMEORIGIN
SET-COOKIE	JSESSIONID=B46507CBCCBC25EE0766E2697168905F.NODE3214; PATH=/; SECURE; HTTPONLY
SET-COOKIE	COOKIE_SUPPORT=TRUE; EXPIRES=WED, 15-APR-2065 19:25:12 GMT; PATH=/; HTTPONLY
SET-COOKIE	GUEST_LANGUAGE_ID=EN_US; EXPIRES=WED, 15-APR-2065 19:25:12 GMT; PATH=/; HTTPONLY
ACCESS-CONTROL-ALLOW-ORIGIN:	HTTP://52.201.64.250

Tabla 4.1. Sistemas encontrados en SHODAN.

CONFIDENCIAL

IP	**52.205.206.233**
SERVER	APACHE/2.4.6 (CENTOS) OPENSSL/1.0.2K-FIPS MOD_FCGID/2.3.9 MOD_NSS/1.0.14 NSS/3.28.4 PHP/5.4.16 MOD_WSGI/3.4 PYTHON/2.7.5
OPEN PORTS	443, 80

Tabla 4.2. Sistemas encontrados en SHODAN.

3.4 AVAILABLE ENDPOINTS

Fue posible identificar un conjunto de endpoints que utiliza la aplicación para sus propias operaciones (búsqueda de vuelos, búsqueda de reservas, entre otros), este código se encuentra ofuscado pero con herramientas de de-ofuscación fue posible obtener una versión legible del código. A continuación se muestran parte de los endpoints encontrados:

```
{
    searchFlight: function(e) {
        return a.a.get("/osl-reservation/reservation?pnr=" + e).then(function(e) {
            return e.data
        })
    }
},
reservation: {
    findReservation: function(e) {
        var t = e.code,
            n = e.lastName;
        return a.a.get("/osl-reservation/reservation/" + t + "/" + n).then(function(e) {
            return e.data
        })
    }
},
```

Imagen 3. Available Endpoints.

Se pudo notar que estos endpoints no solicitaban autenticación y fue posible obtener información mediante request POST y GET. Un atacante podría utilizar estos endpoints para elaborar un ataque de DoS (Denial of Service) y colocar en un estado de indisponibilidad algunos componentes de la aplicación.

CONFIDENCIAL

Se realizaron request a varios endpoints, y como resultado se obtuvo respuesta por parte del endpoint **/osl-reservation/parameters/countries** a solicitudes de tipo GET, tal como se muestra a continuación:


```
[
    {
        "frecuentFlyerCode": "CM",
        "frecuentFlyerDesc": "ConnectMiles",
        "usedByCopa": "Y"
    },
    {
        "frecuentFlyerCode": "UA",
        "frecuentFlyerDesc": "Mileage Plus",
        "usedByCopa": "Y"
    },
    {
        "frecuentFlyerCode": "AC",
        "frecuentFlyerDesc": "Aeroplan",
        "usedByCopa": "Y"
    },
    {
        "frecuentFlyerCode": "NZ",
        "frecuentFlyerDesc": "Airpoints",
        "usedByCopa": "Y"
```


Imagen 4. Resultado de request.

Se recomienda realizar pruebas de tipo WhiteBox para poder determinar si estos endpoints son susceptibles a ataques DoS.

CONFIDENCIAL

4. HALLAZGOS EN SERVIDORES

A continuación, se mencionan las vulnerabilidades encontradas en los servidores. Es importante destacar que algunos equipos no fueron accesibles por internet ni tampoco desde los equipos en AWS.

4.1 SERVIDOR 1: 52.205.206.235.

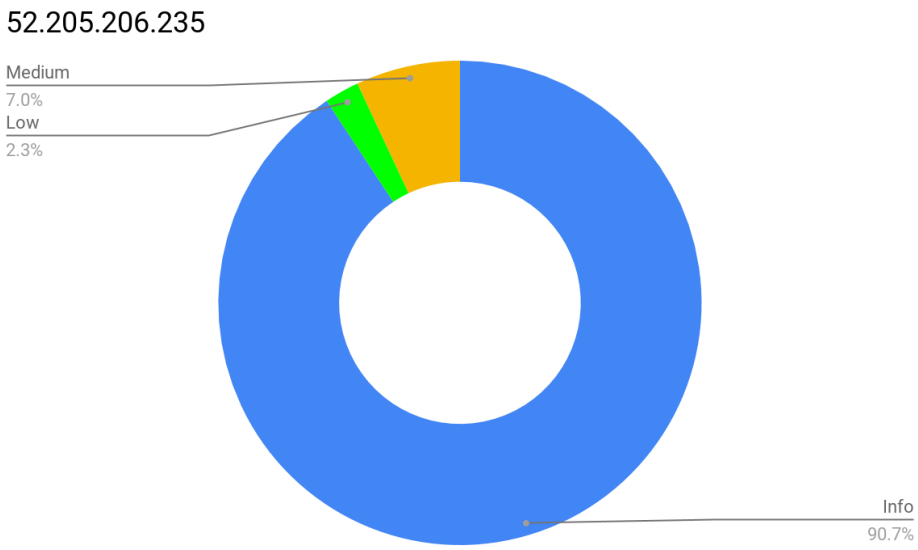


Gráfico 1.1. Hallazgos en Servidores.

CONFIDENCIAL

4.1.1 SSL CERTIFICATE CANNOT BE TRUSTED

Nivel	MEDIO
Descripción	El certificado utilizado por el sitio web no puede ser validado. Esta situación ocurre cuando la entidad emisora del certificado no puede ser validada.
Impacto	En el caso de servidores que se encuentran públicos, la validación del certificado puede dificultar la autenticidad del sitio. Un atacante podría copiar el sitio web y hacerse pasar como la organización.
Remediación	Instalar un certificado digital proveniente de una entidad emisora de certificados.

Tabla 5.1. SSL Certificate cannot be trusted.

4.1.2 SSL CERTIFICATE SIGNED USING WEAK HASHING ALGORITHM

Nivel	MEDIO
Descripción	El certificado utilizado por este sitio fue firmado con un algoritmo de cifrado que se considera susceptible, haciendo posible un ataque de colisión de hash. Algoritmos como SHA1, MD5, no deben ser utilizados
Impacto	Un atacante podría realizar un ataque de colisión de hash con la finalidad de obtener información sensible del usuario luego de encontrarse en el mismo medio para interceptar los datos.
Remediación	Instalar un certificado con un nivel de cifrado más seguro.

Tabla 5.2. SSL Certificate signed using weak hashing algorithm.

CONFIDENCIAL

4.1.3 SSL SELF-SIGNED CERTIFICATE

Nivel	MEDIO
Descripción	El certificado utilizado por el sitio web no se reconoce como un certificado emitido por una entidad certificadora.
Impacto	En caso de que el servidor se encuentre en producción, al carecer de un certificado válido un atacante podría realizar un MITM attack contra el host remoto y obtener información sensible del sitio.
Remediación	Evitar el uso de self-signed certificates cuando el equipo se encuentra disponible en internet.

Tabla 5.3. SSL self-signed certificate.

CONFIDENCIAL

4.2 SERVIDOR 2: 18.209.36.128.

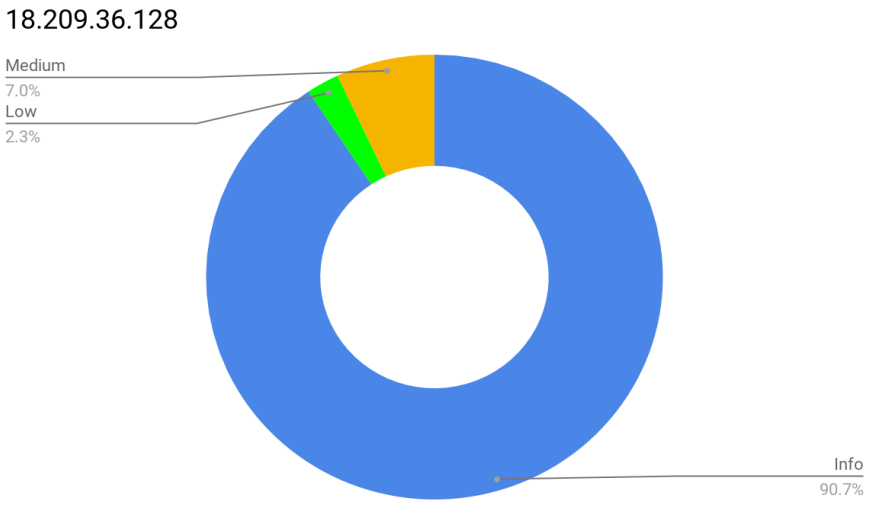


Gráfico 1.2. Hallazgos en Servidores.

4.2.1 SSL CERTIFICATE CANNOT BE TRUSTED

Nivel	MEDIO
Descripción	El certificado utilizado por el sitio web no puede ser validado. Esta situación ocurre cuando la entidad emisora del certificado no puede ser validada.
Impacto	En el caso de servidores que se encuentran públicos, la validación del certificado puede dificultar la autenticidad del sitio. Un atacante podría copiar el sitio web y hacerse pasar como la organización.
Remediación	Instalar un certificado digital proveniente de una entidad emisora de certificados.

Tabla 6.1. SSL Certificate cannot be trusted.

4.2.2 SSL CERTIFICATE SIGNED USING WEAK HASHING ALGORITHM

Nivel	MEDIO
Descripción	El certificado utilizado por este sitio fue firmado con un algoritmo de cifrado que se considera susceptible, haciendo posible un ataque de colisión de hash. Algoritmos como SHA1, MD5, no deben ser utilizados
Impacto	Un atacante podría realizar un ataque de colisión de hash con la finalidad de obtener información sensible del usuario luego de encontrarse en el mismo medio para interceptar los datos.
Remediación	Instalar un certificado con un nivel de cifrado más seguro.

CONFIDENCIAL

Tabla 6.2. SSL Certificate signed using weak hashing algorithm.

4.2.3 SSL SELF-SIGNED CERTIFICATE

Nivel	MEDIO
Descripción	El certificado utilizado por el sitio web no se reconoce como un certificado emitido por una entidad certificadora.
Impacto	En caso de que el servidor se encuentre en producción, al carecer de un certificado válido un atacante podría realizar un MITM attack contra el host remoto y obtener información sensible del sitio.
Remediación	Evitar el uso de self-signed certificates cuando el equipo se encuentra disponible en internet.

Tabla 6.3. SSL self-signed certificate.

CONFIDENCIAL

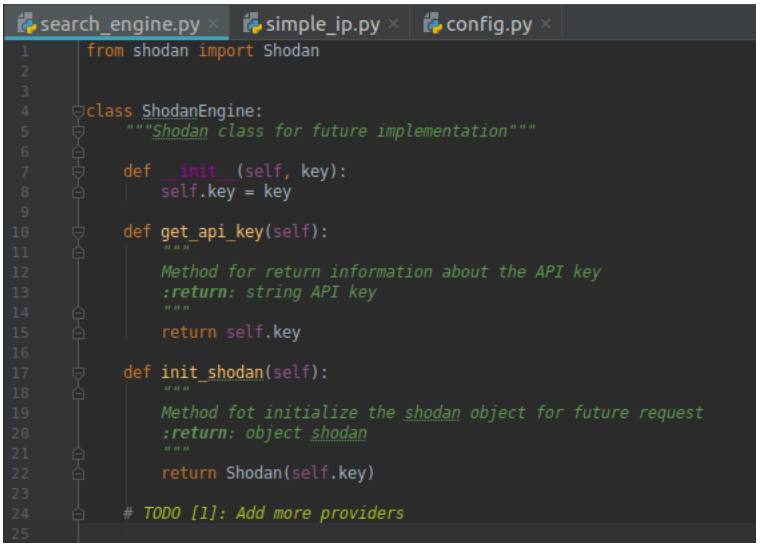
5. RECOMENDACIONES FINALES

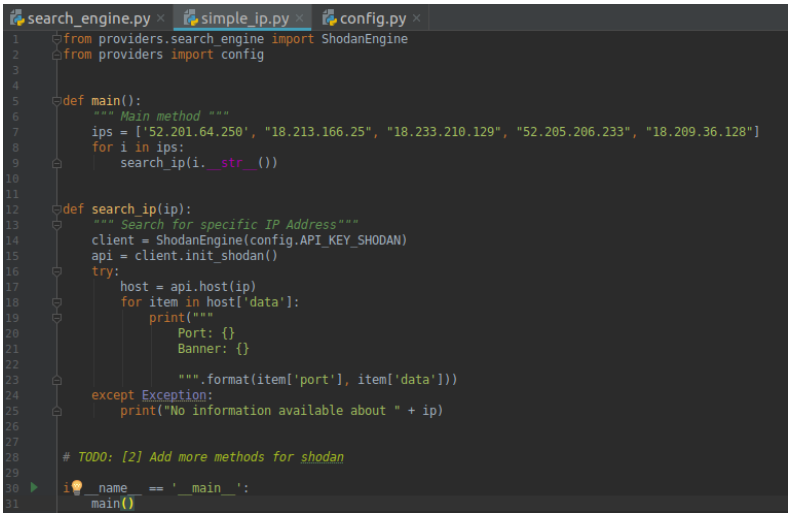
Luego de los resultados obtenidos en la auditoría se recomienda tomar las siguientes acciones:

1. Instalar certificados digitales válidos y firmados por una entidad de confianza.
2. Habilitar autenticación en los endpoints usando:
    a. Login Callback.
    b. OAuth.
    c. Client side authentication function.
    d. Validar el request de lado del servidor.

ANEXOS

Los siguientes scripts se utilizaron para obtener información de los equipos incluidos en la presente auditoría. Utilizando el servicio de SHODA se instancio un objeto de tipo SHODAN y se invocó el método host para obtener información de los servidores.





CONFIDENCIAL

A continuación, se detalla la información que devuelve el script luego de su ejecución:

54.201.64.250
PORT: 4443
BANNER: HTTP/1.1 302 FOUND
DATE: SAT, 01 SEP 2018 16:43:04 GMT
CONTENT-LENGTH: 0
CONNECTION: KEEP-ALIVE
SET-COOKIE:
AWSALB=WYVLJRKCSDJW7GT4ZLORMFJU4HJ5USLEIC1NXGHTJQZDJHHM7ZRYOJC95UYKW
NSX3291ETNFCCJJHTMOTCSX0EREXPBYN4KI3STYFLGXH5R6/6GWOHQKPXFMBPW9;
EXPIRES=SAT, 08 SEP 2018 16:43:04 GMT; PATH=/
SERVER: APACHE-COYOTE/1.1
X-CONTENT-TYPE-OPTIONS: NOSNIFF
X-XSS-PROTECTION: 1
SET-COOKIE: JSESSIONID=B46507CBCCBC25EE0766E2697168905F.NODE3214; PATH=/;
SECURE; HTTPONLY
SET-COOKIE: COOKIE_SUPPORT=TRUE; EXPIRES=WED, 15-APR-2065 19:25:12 GMT; PATH=/;
HTTPONLY
SET-COOKIE: GUEST_LANGUAGE_ID=EN_US; EXPIRES=WED, 15-APR-2065 19:25:12 GMT;
PATH=/; HTTPONLY
ACCESS-CONTROL-ALLOW-ORIGIN: HTTP://52.201.64.250
CONTENT-SECURITY-POLICY: DEFAULT-SRC 'SELF' HTTP://LOCALHOST HTTP://LOCALHOST:8080
HTTP://LOCALHOST:8081 HTTP://COPA.SJV.IO HTTPS://*.COPAAIR.COM HTTPS://*.COPAAIR.COM
HTTPS://*.COPA.COM HTTPS://*.COPA.COM HTTPS://*.GOOGLE.COM HTTPS://*.GOOGLE.COM.CO
HTTPS://*.GOOGLE.SK HTTPS://*.GOOGLETAGMANAGER.COM HTTPS://*.GSTATIC.COM
HTTPS://*.GOOGLE-ANALYTICS.COM HTTPS://*.GOOGLE-ANALYTICS.CO HTTPS://*.GOOGLEAPIS.COM
HTTPS://*.TRACKEDLINK.NET HTTPS://*.FACEBOOK.NET HTTPS://*.FACEBOOK.COM
HTTPS://*.FACEBOOK.COM HTTPS://*.BING.COM HTTPS://TRACKEDWEB.NET HTTPS://*.W55C.NET
HTTPS://*.W55C.NET HTTPS://*.MSN.COM HTTPS://*.ADNXS.COM HTTPS://*.QUALTRICS.COM
HTTPS://*.DOUBLECLICK.NET HTTPS://*.FLIGHTVIEW.COM HTTPS://*.INNOSKED.COM
HTTPS://*.INNOSKED.COM HTTPS://*.INTELLIRESPONSE.COM HTTPS://*.INTELLIRESPONSE.COM
HTTPS://*.FREQUENTFLYER.AERO HTTPS://*.FREQUENTFLYER.AERO HTTPS://*.FLTMAPS.COM
HTTPS://*.FLTMAPS.COM HTTPS://*.NBXAPPS.COM HTTPS://PANAMAESPOSIBLE.COM
HTTPS://MIPARAISOATLANTIS.COM HTTPS://*.GOOGLEADSERVICES.COM
HTTPS://*.HAVASDIGITALCOLOMBIA.COM HTTPS://*.NORTON.COM HTTPS://*.MCAFEESECURE.COM
HTTPS://WWW.YOUTUBE.COM HTTPS://COPA.SJV.IO 'UNSAFE-INLINE' 'UNSAFE-EVAL' DATA: BLOB:
X-CONTENT-SECURITY-POLICY: DEFAULT-SRC 'SELF' HTTP://LOCALHOST HTTP://LOCALHOST:8080
HTTP://LOCALHOST:8081 HTTP://COPA.SJV.IO HTTPS://*.COPAAIR.COM HTTPS://*.COPAAIR.COM
HTTPS://*.COPA.COM HTTPS://*.COPA.COM HTTPS://*.GOOGLE.COM HTTPS://*.GOOGLE.COM.CO
HTTPS://*.GOOGLE.SK HTTPS://*.GOOGLETAGMANAGER.COM HTTPS://*.GSTATIC.COM
HTTPS://*.GOOGLE-ANALYTICS.COM HTTPS://*.GOOGLE-ANALYTICS.CO HTTPS://*.GOOGLEAPIS.COM
HTTPS://*.TRACKEDLINK.NET HTTPS://*.FACEBOOK.NET HTTPS://*.FACEBOOK.COM
HTTPS://*.FACEBOOK.COM HTTPS://*.BING.COM HTTPS://TRACKEDWEB.NET HTTPS://*.W55C.NET

CONFIDENCIAL

HTTPS://*.W55C.NET HTTPS://*.MSN.COM HTTPS://*.ADNXS.COM HTTPS://*.QUALTRICS.COM
HTTPS://*.DOUBLECLICK.NET HTTPS://*.FLIGHTVIEW.COM HTTPS://*.INNOSKED.COM
HTTPS://*.INNOSKED.COM HTTPS://*.INTELLIRESPONSE.COM HTTPS://*.INTELLIRESPONSE.COM
HTTPS://*.FREQUENTFLYER.AERO HTTPS://*.FREQUENTFLYER.AERO HTTPS://*.FLTMAPS.COM
HTTPS://*.FLTMAPS.COM HTTPS://*.NBXAPPS.COM HTTPS://PANAMAESPOSIBLE.COM
HTTPS://MIPARAISOATLANTIS.COM HTTPS://*.GOOGLEADSERVICES.COM
HTTPS://*.HAVASDIGITALCOLOMBIA.COM HTTPS://*.NORTON.COM HTTPS://*.MCAFEESECURE.COM
HTTPS://WWW.YOUTUBE.COM HTTPS://COPA.SJV.IO 'UNSAFE-INLINE' 'UNSAFE-EVAL' DATA: BLOB:
X-PERMITTED-CROSS-DOMAIN-POLICIES: MASTER-ONLY
X-FRAME-OPTIONS: SAMEORIGIN
STRICT-TRANSPORT-SECURITY: MAX-AGE:86400; INCLUDESUBDOMAINS
SET-COOKIE: CURRENTCOUNTRY=; PATH=/; SECURE
LOCATION: HTTPS://52.201.64.250/ES/WEB/GUEST

NO INFORMATION AVAILABLE ABOUT 18.213.166.25
NO INFORMATION AVAILABLE ABOUT 18.233.210.129

52.205.206.233
PORT: 443
BANNER: HTTP/1.1 200 OK
DATE: TUE, 18 SEP 2018 14:55:52 GMT
SERVER: APACHE/2.4.6 (CENTOS) OPENSSL/1.0.2K-FIPS MOD_FCGID/2.3.9 MOD_NSS/1.0.14
NSS/3.28.4 PHP/5.4.16 MOD_WSGI/3.4 PYTHON/2.7.5
LAST-MODIFIED: WED, 28 FEB 2018 13:44:21 GMT
CONTENT-LENGTH: 3274
ETAG: "CCA-56645F0C78DCC"
ACCEPT-RANGES: BYTES
AGE: 80150
CONTENT-TYPE: TEXT/HTML; CHARSET=UTF-8

PORT: 80
BANNER: HTTP/1.1 200 OK
DATE: MON, 03 SEP 2018 00:09:38 GMT
SERVER: APACHE/2.4.6 (CENTOS) OPENSSL/1.0.2K-FIPS MOD_FCGID/2.3.9 MOD_NSS/1.0.14
NSS/3.28.4 PHP/5.4.16 MOD_WSGI/3.4 PYTHON/2.7.5
LAST-MODIFIED: WED, 28 FEB 2018 13:44:21 GMT
CONTENT-LENGTH: 3274
ETAG: "CCA-56645F0C78DCC"
ACCEPT-RANGES: BYTES
AGE: 52144
CONTENT-TYPE: TEXT/HTML; CHARSET=UTF-8

NO INFORMATION AVAILABLE ABOUT 18.209.36.128

CONFIDENCIAL