

# Pruebas ofensivas portalverificacionbp y Formiik

25/06/2021

# Objetivos

- Ejecutar un retest sobre el sitio **portalverificacionbp.azurewebsites.net** y confirmar la implementación de controles asociados a los atributos de las cookies y manejo de sesiones.
- Ejecutar también un retest sobre **<https://app.formiik.com/>**

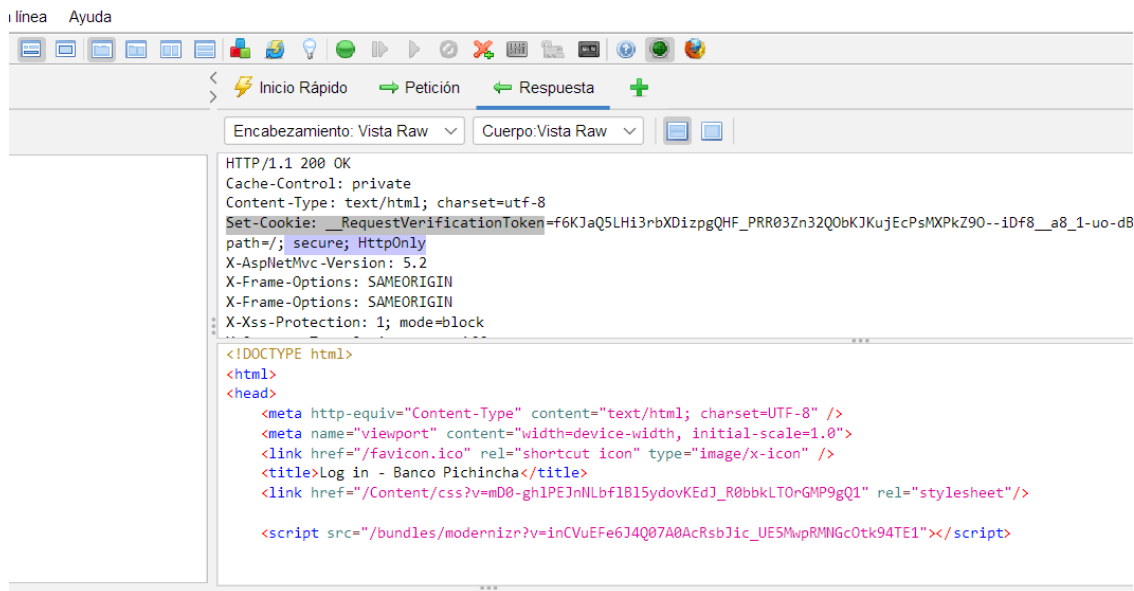


---

# Análisis Dinámico - portalverificacionbp

# Atributos de las cookies

Se realiza un análisis de vulnerabilidades y se logra confirmar que la cookie de sesión contiene los atributos HttpOnly y Secure. Esto evita que la cookie viaje por un canal inseguro y que pueda ser alterada por un script ejecutado del lado del cliente.



```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: RequestVerificationToken=f6KJaQ5LHi3rbXDizpgQHF_PRR03Zn32Q0bKJKuJcPsMXPkZ90--1Df8__a8_1-uo-dB
path=/; secure; HttpOnly
X-AspNetMvc-Version: 5.2
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block

<!DOCTYPE html>
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
  <title>Log in - Banco Pichincha</title>
  <link href="/Content/css?v=mD0-gh1PEJnNLbf1B15ydovKEdJ_R0bbkLT0rGMP9gQ1" rel="stylesheet"/>

  <script src="/bundles/modernizr?v=inCVuEF6J4Q07A0AcRsbJic_UE5MwpRMINGc0tk94TE1"></script>
```



# Manejo de sesión

Se realizan pruebas internas sobre el portal, cerrando sesión e intentando acceder y consumir los servicios. Se logra evidenciar que al momento de cerrar sesión del lado del cliente no es posible consumir los APIS que retornan la información.

**Request**

Raw Params Headers Hex

```
POST /ConsultasBP/GetConsulte HTTP/1.1
Host: bportalverificaciontest.azurewebsites.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 127
Origin: https://bportalverificaciontest.azurewebsites.net
DNT: 1
Connection: close
Referer: https://bportalverificaciontest.azurewebsites.net/ConsultasBP/Index?type=0
Cookie: ClientTimeZone=-300;
__RequestVerificationToken=Lk5lpMCCPRACKShor314wY_M6TTPvX42g0dc6xuv6dF_o-Xq6eBNhathCvApbAG_71FD21VV4R
Maawthg0MA70phBKS_1xFhD480BqnJHL; ClientTimeZone=-300;
.ASPXAUTH=B0C345E5A6B01143497C079EB875060A31CF572C0AD005F653AF9401012674F0C04120543503FE003F5DD6755CD
623C0003B54AA736ADB70BFD870626374A1417AFC30FC6CBC7FF3254E2ED54F40F32F07B149774A0037C16E9CD76FDE;
.AspNet.ApplicationCookie=431a7107d4e01pmhW8RV3j17kLjxdJCaADaGxvW4B-Bylq-tmj9SDr77XgKlcYQXWVqHpE_maj
CSU1XTP6P5F53VVTgtz2PFC7b7XNoCB-Uxsv-uldp7Cv648v9S4u40xADgm3DN9eFFS10PIT_qdKpVWYChj2x0Yx8aMLvFyLGC3p
Dj1ukmHMO7a5vDQ1ZkLvBdwl0v9AGUcWLj_OgQ2w5T5KaTKTg1w0cS3LegasCv6GPHqu5SavHvHCTB3atyq1Yk00_q55RZTHr6
ZcUcDGL3AJyBcInhJe-ue9C4dWSD36FQCC-6r7xPDW0LcmNuV8Ru02gH936SoTrevIKTocAwe-TqPp7u3gIH1NoS0-D1YtirCcGjH
HBM-BApJkTeevahi7xHecaklyGs-CpyWH1CST710

{"TypeId": "0001", "NumberId": "1750078545", "FirstName": "", "SecondName": "", "FirstSurname": "", "SecondSurname": "", "TypeConsult": "0"}
```

**Response**

Raw Headers Hex HTML Render

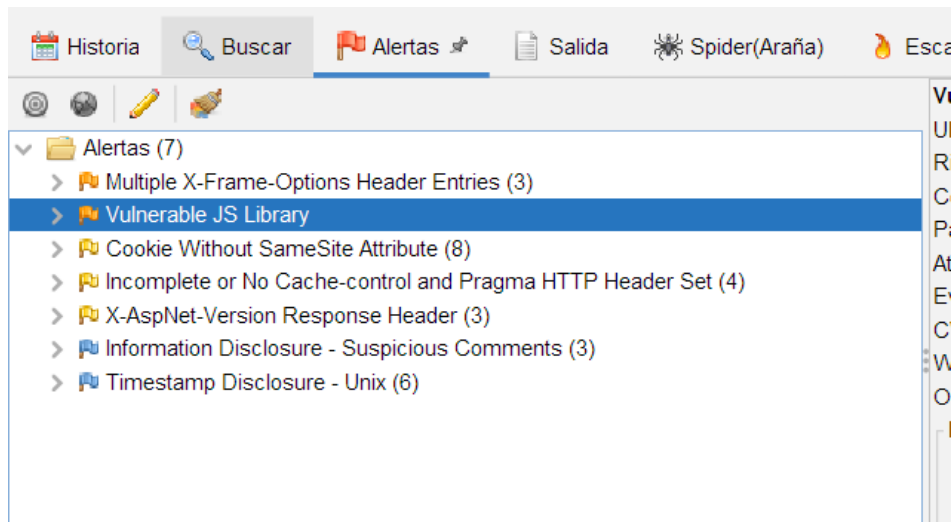
```
HTTP/1.1 302 Found
Cache-Control: private, s-maxage=0
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Location: /Account/Login
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=x5gdce55yo5ivg3tw3rvhnb; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie: .AspNet.ApplicationCookie=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Fri, 10 Jun 2021 15:41:21 GMT
Connection: close
Content-Length: 131

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Account/Login">here</a>.</h2>
</body></html>
```



# Debilidades adicionales

El escaneo de vulnerabilidades arroja algunas alertas relacionadas con librerías vulnerables como jquery y la falta de un atributo adicional SameSite en la cookie de sesión. No se considera explotables estas alertas y no se encuentra algún vector de ataque que pueda ser aprovechado.

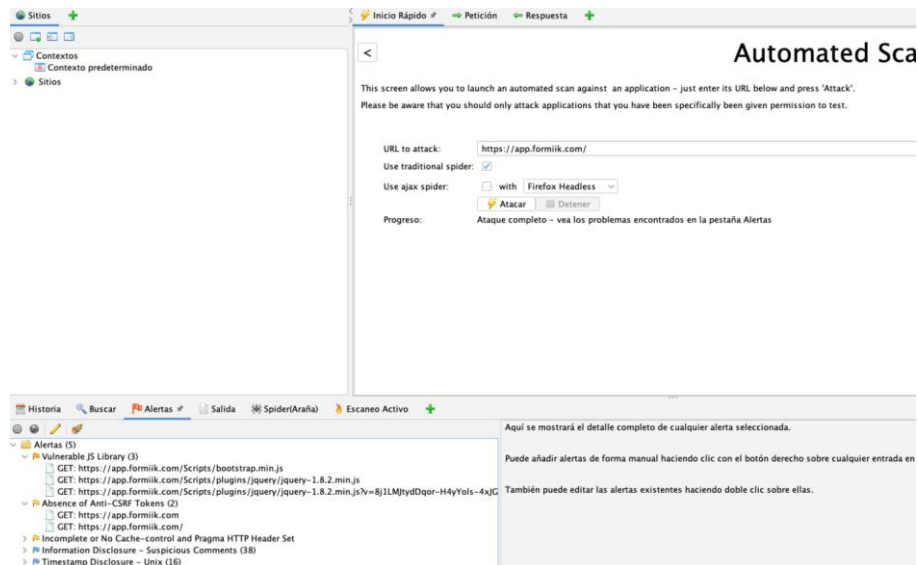


---

# Pruebas app.formiik

# Escaneo de vulnerabilidades

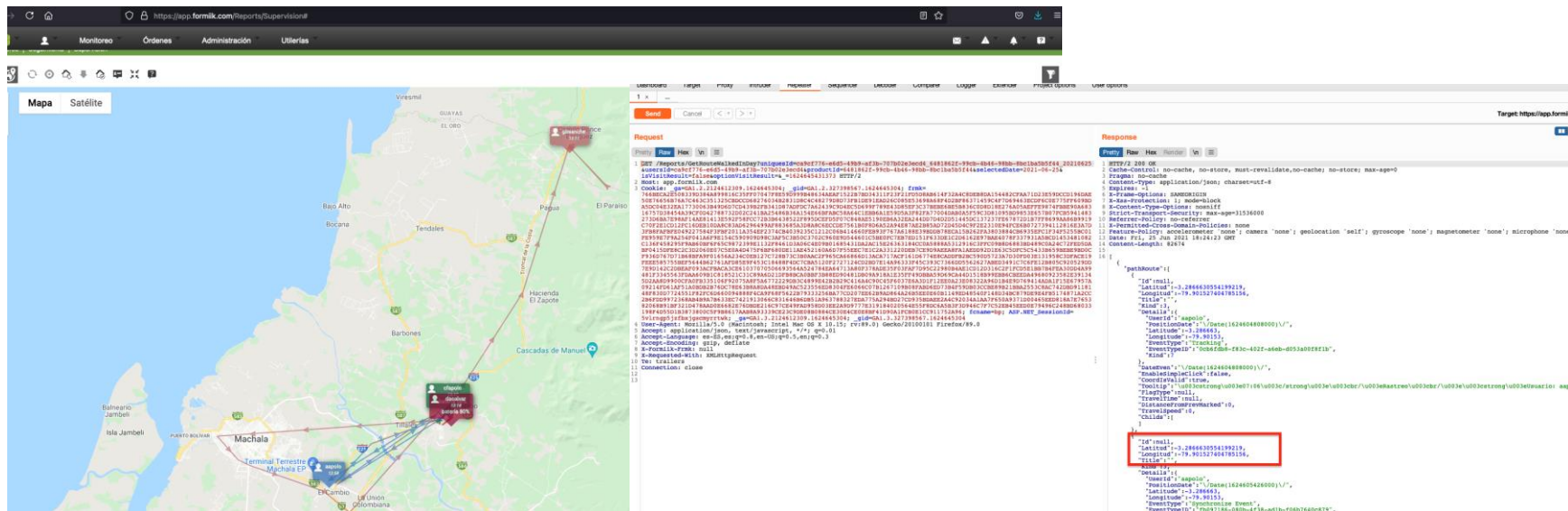
El escaneo de vulnerabilidades arroja algunas alertas relacionadas con librerías vulnerables como jquery. No se considera explotables estas alertas y no se encuentra algún vector de ataque que pueda ser aprovechado.





# Pruebas dinámicas

En la aplicación Formiik no se han detectados problemas relacionados con el manejo de sesión, se realizan nuevas pruebas y la sesión y el consumo de apis responde correctamente durante el tiempo de vida de sesión, al momento de cerrar sesión desde el front end no es posible consumir mas servicios desde el backend.



# Pruebas dinámicas – Valides de la sesión

Decoder: Dashboard | Comparer: Target | Logger: Proxy | Extender: Intruder | Project options: Repeater | User options: Sequencer

1 x ...

Send Cancel < >

Target: https://app.formiik.com

**Request**

1 GET /reports/GetRouteWalkedInDay?uniqueid=ca9cf776-e6d5-49b9-af3b-707b02e3ec d4 6481862f-99cb-4b46-98bb-8bcb1ba5 b5f44 20210625&usersId=ca9cf776-e6d5-49b9-af3b-707b02e3ec d4&productId=6481862f-99cb-4b46-98bb-8bcb1ba5b5f44&selectedDate=2021-06-25&isVisitResult=false&optionVisitResult=&\_id=1624645431373 HTTP/2

2 Host: app.formiik.com

3 Cookies: ga=GA1.2.2124612309.1624645304; gid=GA1.2.327398567.1624645304; frmk=7668ECA2E508339D384A899816C35FF070 478E59D99984634AEAF152287BD34311 F23F21FD5D8A8614F32A4C8DEB8D15448 2CFAA71D23E59DCCD196DAE50E76656B76 A7C463C351325CBDCDD68276034B2831D8 C4C48279D8D73FB1DE91EAD046C08E5E369 8A68F4D2BF6371459C4F7D69463ECD6FC 0E775FF609BDA5DC04E32EA17730063849 D6D7CDA39B2F341D87ADDFC7A62439C9D 4EC5D699F789E43D85EF3C37BE8E6E5B88 36C0D8D18E276A05AEFF9874FB8E90A68 316757D38454A39CF0B42788732D0C241 BA25A86B36A154E668FABC58A64C1E8B6A 1E59D5A3F82FA77004DAB0A5F59C3D8109 5BD9853E657B07FCB5941483273D6BA7E9 8AF14AE81413E592F58FC72B3B6438522 F895C8EFD0F07C84BAE5190B8A32BA244 DD7D4D2D51445DC137237FE67872D1B7FF 8699AAB699919C70F2E1CD12FC16DEB1D0 A8C8AD6296499AF883685A3DBA8C6ECCD E7561B0F8D6A52A94E87AE2B85AD72D45D 4C9CF2E2310E94FC6B0727394112816E3A 7D3F88F8F8E049227584F3FB2011A354 EF2374CB4039235C1212C068414660FEB9 3F767A6188E39BDB78ECA15B262FA3803 884CB6935EFC1F34F5255BC01FE959E7F9 A254F041A6F9E154C590909D98C3AF5C3B 50C3702C960890544601C38E0FC7EB7E01 51F633DE1C2D6162E97BAE4078F37931A 5BCD1453481082C136F458295F9AB60BF6 F65C872399E1132F8461D3A06C40B9801 685431DADAC15E26363184CC0A588A511

**Response**

1 HTTP/2 499

2 Cache-Control: private, no-cache, no-store, max-age=0

3 Pragma: no-cache

4 Content-Type: application/json; charset=utf-8

5 Expires: 0

6 X-Frame-Options: SAMEORIGIN

7 X-XSS-Protection: 1; mode=block

8 X-Content-Type-Options: nosniff

9 Strict-Transport-Security: max-age=31536000

10 Referrer-Policy: no-referrer

11 X-Permitted-Cross-Domain-Policies: none

12 Feature-Policy: accelerometer 'none'; camera

13 Date: Fri, 25 Jun 2021 18:25:33 GMT

14 Content-Length: 60

15 "La sesión ha expirado por favor escriba sus

formiik MOBILE

INSPECTOR

Nombre de usuario

Contraseña

Enviar

Versión: 6.0.0

BANCO PICHINCHA

---

# Conclusiones y oportunidades de mejora

# Conclusiones

- Se encuentran mejoras en el manejo de sesión con respecto a la expiración de la cookie una vez se cierre sesión del lado del cliente.
- La cookie de sesión ya cuenta con los atributos “Secure” y “HttpOnly” que evitan vectores de ataque asociados al secuestro de cookies.
- Se encuentran algunas alertas adicionales con respecto a una librería (Jquery) con alguna vulnerabilidad.



# Oportunidades de mejora

- Mantener todas las librerías actualizadas para evitar futuros ataques sobre la aplicación.
- Configurar el atributo “SameSite” sobre la variable de sesión.



# Muchas gracias.



Confidencialidad: Este documento contiene información de uso exclusivo de Banco Pichincha. Su distribución y reproducción total o parcial a personal ajeno al Banco Pichincha está prohibida a menos que tenga autorización por escrito. Todos los derechos reservados Banco Pichincha 2018.