DETALLE DE LAS VULNERABILIDADES IDENTIFICADAS

A continuación, se presentan los resultados obtenidos durante las pruebas de RETEST realizadas sobre el alcance definido en la parte superior de este documento.

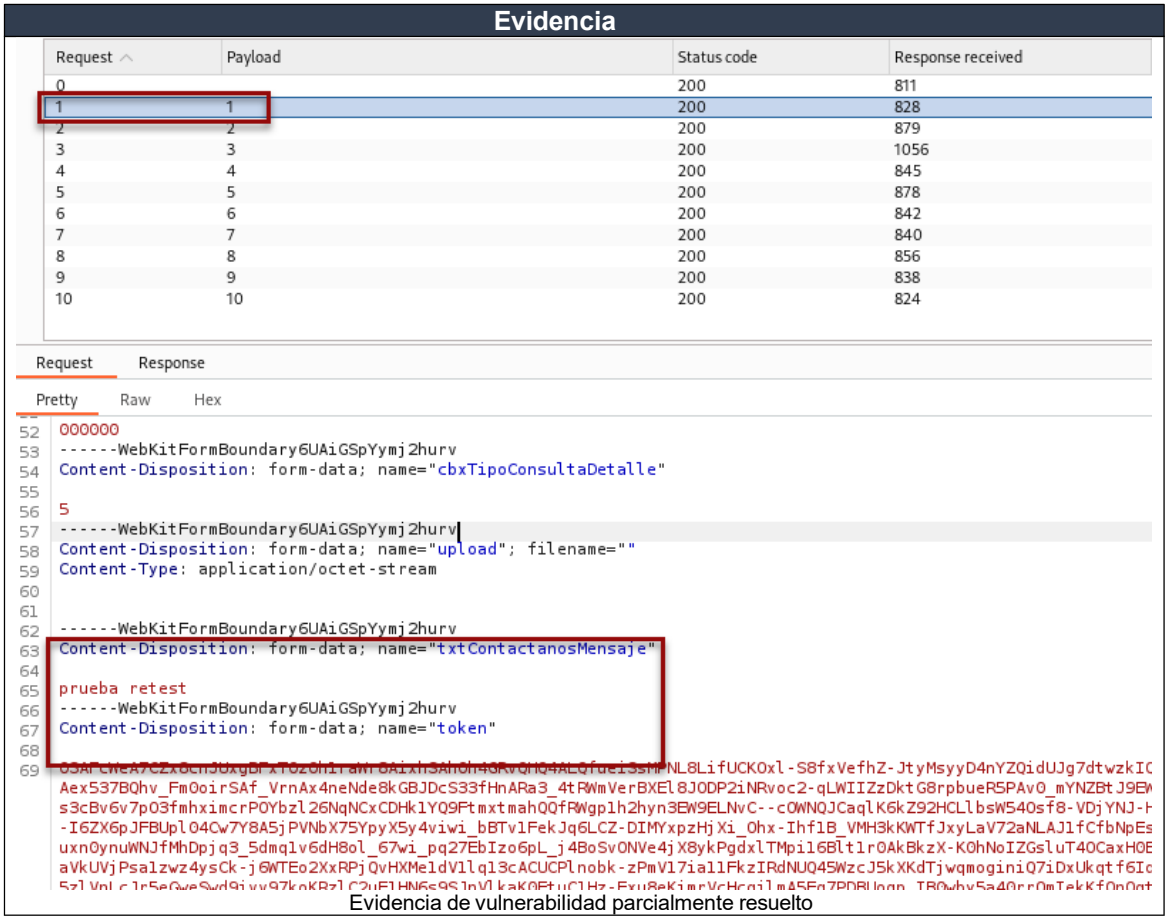
Nro.	Descripción de la vulnerabilidad identificada y el riesgo asociado	Categoría	Estado	Descripción
Pruebas de Ethical Hacking – Aplicaciones				
SISTEMA DE INFORMACIÓN – Portal Institucional				
28	Formulario susceptible ante ataques recurrentes	MEDIO	PARCIALMENTE RESUELTO	Se identificó que se ha tomado acción sobre la vulnerabilidad, sin embargo, aún es posible realizar un ataque recurrente de envío de información. Por lo que la vulnerabilidad se da como: Parcialmente resuelto.
30	Inadecuado filtrado de puertos expuestos a la red	MEDIO	PARCIALMENTE RESUELTO	Se identificó que se ha tomado acción sobre la vulnerabilidad, sin embargo, aún se encuentran expuestos diversos puertos a Internet.” Por lo que la vulnerabilidad se da como: Parcialmente resuelto.
31	Debilidades en cabeceras del protocolo HTTP	BAJO	PARCIALMENTE RESUELTO	Se identificó que se ha realizado configuraciones sobre el protocolo HTTP, sin embargo, aún se expone información innecesaria: “server: nginx” Por lo que la vulnerabilidad se da como: Parcialmente resuelto.

EVIDENCIAS RETEST

PRUEBAS DE RETEST - APLICACIONES WEB

Formulario susceptible ante ataques recurrentes

Evidencia



Request	Payload	Status code	Response received
0		200	811
1	1	200	828
2	2	200	879
3	3	200	1056
4	4	200	845
5	5	200	878
6	6	200	842
7	7	200	840
8	8	200	856
9	9	200	838
10	10	200	824

Request Response

Pretty Raw Hex

```
000000
------WebKitFormBoundary6UAiGSpYymj2hurv
Content-Disposition: form-data; name="cbxTipoConsultaDetalle"

5
------WebKitFormBoundary6UAiGSpYymj2hurv
Content-Disposition: form-data; name="upload"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary6UAiGSpYymj2hurv
Content-Disposition: form-data; name="txtContactanosMensaje"

prueba retest
------WebKitFormBoundary6UAiGSpYymj2hurv
Content-Disposition: form-data; name="token"
```

Evidencia de vulnerabilidad parcialmente resuelto

Evidencia

Request	Payload	Status code	Response received
0		200	811
1	1	200	828
2	2	200	879
3	3	200	1056
4	4	200	845
5	5	200	878
6	6	200	842
7	7	200	840
8	8	200	856
9	9	200	838
10	10	200	824

Request Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx
3  Date: Sun, 01 Jun 2025 21:18:03 GMT
4  Content-Type: application/json
5  Connection: keep-alive
6  Cache-Control: must-revalidate, no-cache, private
7  X-UA-Compatible: IE=edge
8  Content-language: es
9  X-Content-Type-Options: nosniff
10 Expires: Sun, 19 Nov 1978 05:00:00 GMT
11 Vary:
12 Content-Security-Policy: upgrade-insecure-requests;
13 X-Frame-Options: SAMEORIGIN
14 Strict-Transport-Security: max-age=31536000; includeSubdomains
15 Referrer-Policy: no-referrer
16 X-XSS-Protection: 1; mode=block
17 X-Permitted-Cross-Domain-Policies: none
18 Content-Length: 22
19
20 {
     "response":"success"
   }
```

Evidencia de vulnerabilidad parcialmente resuelto

Evidencia

Request	Payload	Status code	Response received
0		200	811
1	1	200	828
2	2	200	879
3	3	200	1056
4	4	200	845
5	5	200	878
6	6	200	842
7	7	200	840
8	8	200	856
9	9	200	838
10	10	200	824

Request Response

Pretty Raw Hex

```
49 ------WebKitFormBoundary6UAiGSpYymj2hurv
50 Content-Disposition: form-data; name="cbxDistrito"
51
52 000000
53 ------WebKitFormBoundary6UAiGSpYymj2hurv
54 Content-Disposition: form-data; name="cbxTipoConsultaDetalle"
55
56 5
57 ------WebKitFormBoundary6UAiGSpYymj2hurv
58 Content-Disposition: form-data; name="upload"; filename=""
59 Content-Type: application/octet-stream
60
61
62 ------WebKitFormBoundary6UAiGSpYymj2hurv
63 Content-Disposition: form-data; name="txtContactanosMensaje"
64
65 prueba retest
66 ------WebKitFormBoundary6UAiGSpYymj2hurv
67 Content-Disposition: form-data; name="token"
68
69 03AFcWeA7CZx8cnJUxgBFxT0zOh1raWr8AixhSAh0h4GRvQHQ4ALQfueiSsMPNL8LifUCKOxl-S8fxVefhZ-JtyMsyyD4nYZQidUJg7dtwzkIQ
   Aex537BQhv_FmOoirSAf_VrnAx4neNde8kGBJDcS33fHnARa3_4tRWmVerBXEl8JODP2iNRvoc2-qLWIIZzDktG8rpbueR5PAvO_mYNZBtJ9EW
   s3cBv6v7pO3fmhximcrPOYbzl26NqNCxCDHk1YQ9FtmxtmahQQfRWgp1h2hyn3EW9ELNvC--cOWNQJCaqlK6kZ92HCLlbsW54Osf8-VDjYNJ-H
```

Evidencia de vulnerabilidad parcialmente resuelto

Evidencia

Request	Payload	Status code	Response received
0		200	811
1	1	200	828
2	2	200	879
3	3	200	1056
4	4	200	845
5	5	200	878
6	6	200	842
7	7	200	840
8	8	200	856
9	9	200	838
10	10	200	824

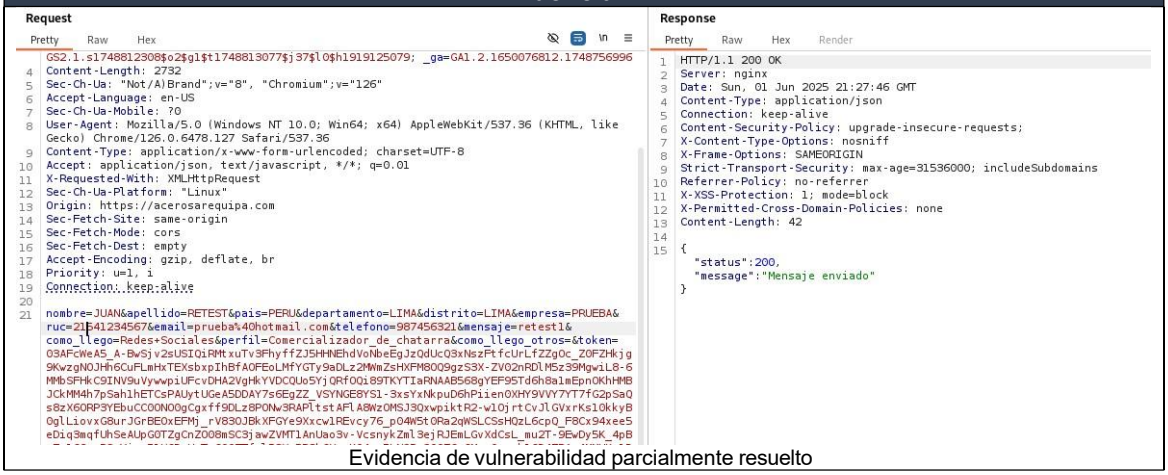
Request Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx
3  Date: Sun, 01 Jun 2025 21:18:10 GMT
4  Content-Type: application/json
5  Connection: keep-alive
6  Cache-Control: must-revalidate, no-cache, private
7  X-UA-Compatible: IE=edge
8  Content-language: es
9  X-Content-Type-Options: nosniff
10 Expires: Sun, 19 Nov 1978 05:00:00 GMT
11 Vary:
12 Content-Security-Policy: upgrade-insecure-requests;
13 X-Frame-Options: SAMEORIGIN
14 Strict-Transport-Security: max-age=31536000; includeSubdomains
15 Referrer-Policy: no-referrer
16 X-XSS-Protection: 1; mode=block
17 X-Permitted-Cross-Domain-Policies: none
18 Content-Length: 22
19
20 {
     "response":"success"
   }
```

Evidencia de vulnerabilidad parcialmente resuelto

Evidencia



Evidencia de vulnerabilidad parcialmente resuelto

Inadecuado filtrado de puertos expuestos a la red

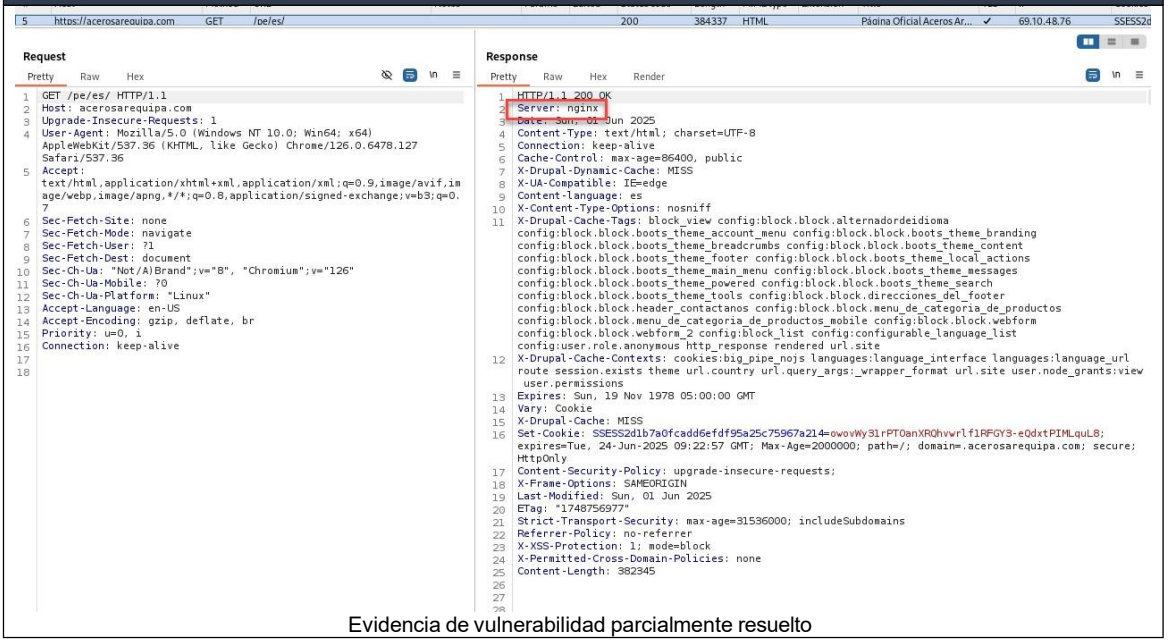
Evidencia

```
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for acerosarequipa.com (69.10.48.76)
Host is up (0.12s latency).
Not shown: 89 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Evidencia de vulnerabilidad parcialmente resuelto

Debilidades en cabeceras del protocolo HTTP

Evidencia



Evidencia de vulnerabilidad parcialmente resuelto