	Servicio de Ethical Hacking 2024 Aceros Arequipa	Código: EH-AQ-IR
	Informe Retest	Versión: 1.0 Fecha: 02/06/2025 Página: 1 de 5

## 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
<b>Pruebas de Ethical Hacking – Aplicaciones</b>				
<b>SISTEMA DE INFORMACIÓN – Portal Institucional</b>				
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

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	<pre> 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 -----WebKitFormBoundary6UAIgSpYymj2hurv 62 Content-Disposition: form-data; name="txtContactanosMensaje" 63 64 prueba retest 65 -----WebKitFormBoundary6UAIgSpYymj2hurv 66 Content-Disposition: form-data; name="token" 67 68 69 05af47e27c2x6cn3UxgBpx70z0h1r am 0AIxh3AH0h40RvQh04ALofuei3sm#NL8Li fUCK0xl - S8fxVefhZ - JtyMsyyD4nYZQidUJg7dtwzkIC Aex537B0hv_Fm0oirSAf_VrnAx4neNde8kGBJdcS33fHnAra3_4tRwMVerBXEL8JODP2iNRvoc2-qLWIIzZDktG8rpbueR5PAv0_mYNZBtJ9E s3cBv6v7p03fmhximcrPOYbz126NqNCxCDHk1YQ9Ftmxtmah0QfRWgp1h2hyn3EW9ELNvc--c0WNQJCaqLK6kZ92HCLlbsW540sf8-VDjYnj-t -I6ZX6pJFBUp104Cw7Y8A5jPVNbX75YpyX5y4vivi_bBTv1FekJq6LCZ-DIMYxpzHjXi_Ohx-Ihf1B_VMH3kKWTfJxyLaV72anLAJ1fCfbNpEs uxn0ynuWNJfMhDpj q3_5dmq1v6dH8ol_67wi_pq27EbIzo6pL_j4BoSvONVe4jX8ykPgdxlTMpi16Bltr0AkBkzX-K0hNoIZGsluT40CaxHOE aVkuVjPsalzww4ysck-j6WTEo2XxRPjQvHXMe1dV1lq13cACUCPLnobk-zPmV17ia11FkzIRdNUQ45WzcJ5kXKdTjwqmogini07iDxUkqt f6Ic 5z1Vnl r1r5eQweSwdqiuv97knRz1C2uF1HNR9S7nVl kak0Ftu01H7-Fyu8eKiamVcHrcil m45Fn7PDRlloq TR0qhv5a40r0mTekKf0n0nt           </pre>

**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 -----WebKitFormBoundary6UAiGSpYymj2hurv
62 Content-Disposition: form-data; name="txtContactanosMensaje"
63
64 prueba retest
65 -----WebKitFormBoundary6UAiGSpYymj2hurv
66 Content-Disposition: form-data; name="token"
67
68
69 03AFCWeA7Cz8cnJUxgBFxT0z0h1raWr8AixhSAh0h4GRv0HQ4ALQfueiSsMPNL8Li fUCKOx1 - S8fxVefhZ- JtyMsyyD4nYZ0idUJg7dtwzkIO
Aex537BQhv_Fm0oirSaf_VrnAx4neNde8kGBJDcS33fHnAra3_4tRwMVerBXEL8J0DP2iNRvoc2-qLWIIzZDktG8rpbueR5PAv0_mYNZBtJ9EW
s3cBv6v7p03fmximcrP0YbzL26NqNCxCDHk1YQ9Ft mxtmahQ0fRWgp1h2hyn3EW9ELNvC--cOWNQJCaqLk6kZ92HCL1bsW540s78-VDJYnJ-H
T57v61EBU13407Y0AE-DmkKv7EYvVE4444 k0F1E-L16L72 DMVx4BvYi_0kx Thf1B VMU8kWTf1u1v72-N141166fMkE-

```

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

Request	Response
<pre> 1 GS2.1..s17488123068205g1st17488130775j37s10sh1919125079; _ga=GA1.2.1650076812.1748756996 4 Content-Length: 2732 5 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126" 6 Accept-Language: en-US 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like   Gecko) Chrome/126.0.6478.127 Safari/537.36 9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 10 Accept: application/json, text/javascript, */*; q=0.01 11 X-Requested-With: XMLHttpRequest 12 Sec-Ch-Ua-Platform: "Linux" 13 Origin: https://acerosarequipa.com 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 Connection: keep-alive 20 21 nombre=JUAN&amp;apellido=RETEST&amp;pais=PERU&amp;departamento=LIMA&amp;distrito=LIMA&amp;empresa=PRUEBA&amp;   ruc=21541234567&amp;email=prueba40@hotmail.com&amp;telefono=987456321&amp;mensaje=retest1&amp;   como_llego=Redes+ Sociales&amp;perfil=Comercializador_de_chatarra&amp;como_llego_otros=&amp;token=   09AFcweAS_A-BwSjv2sUSIQ1RhtxuTv3PhyffZJ5HhHNdvoNbeEgJzQdUC03xNszPtfCULfZZg0c_Z0F2hkjg   9KwzqN0Jh6GcuFLmXTEVsbxpjhbFAOFcoLmHYGTy9aDLz2MwZsHMFK90099zS3X-ZV0ZnRDlNSz39HgwLL6-6   MhBSPFKCS9IN9UvYvwp1UFCvDHA2VgHkYVDC0Uo5yJQRFO0L89TKYIARNAAB568yEFP95TD6h8a1eEpnOKHMB   JcM4H7pSah1HETCsPAUytUGeASDDAY7s6EGZZ_VSYNGE8YSL-3xSyxNkpuD6PiienOXHY9VY7Y7f7G2pSa0   s8zX60RP3YEbuCC0N00gCgxff9DLzBPONw3RAPLstAPLAWzOHSJ30xwpiktR2-v10jrtCvJGVxrkS10kyB   0gLLovxG8urJGrBE0xEPFm_rV830JbkXF0Ye9Xxcv1REvcy76_p04W5t0Ra2qWLSLCSsH0zL6cp0_F8cx94xee5   eBiq3eafuhSeAUpGOTZgChZ00m5C3jawZVMT1AnUao3v-VcsnykZml3ejRJEhLGVxdCsL_mu2Tf-9EwDy5K_4p8 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sun, 01 Jun 2025 21:27:46 GMT 4 Content-Type: application/json 5 Connection: keep-alive 6 Content-Security-Policy: upgrade-insecure-requests; 7 X-Content-Type-Options: nosniff 8 X-Frame-Options: SAMEORIGIN 9 Strict-Transport-Security: max-age=31536000; includeSubdomains 10 Referrer-Policy: no-referrer 11 X-XSS-Protection: 1; mode=block 12 X-Permitted-Cross-Domain-Policies: none 13 Content-Length: 42 14 15 {   "status": 200,   "message": "Mensaje enviado" } </pre>

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

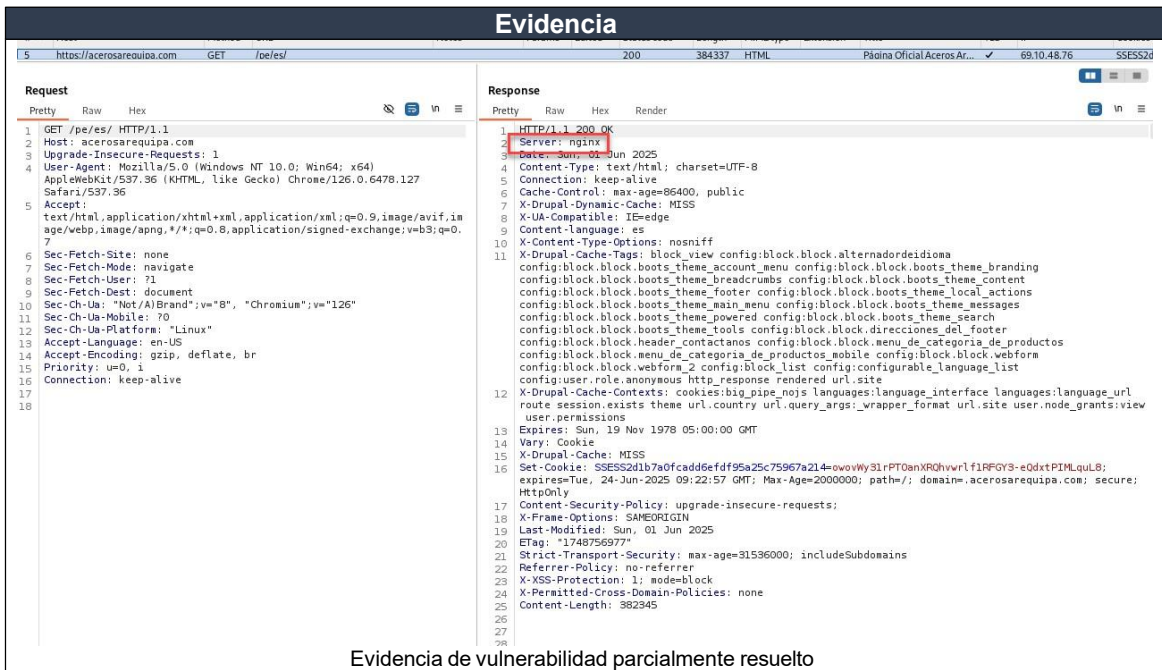
Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds

root@kali:~#
```

Evidencia de vulnerabilidad parcialmente resuelto

### Debilidades en cabeceras del protocolo HTTP

**Evidencia**



Evidencia de vulnerabilidad parcialmente resuelto