

Hacking de Aplicaciones WEB

SESION 1

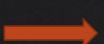
 @WilliamMarchand

Para entendernos mejor...



Prácticas
maliciosas

Formar un equipo de 2 personas e identificarlo con un SEUDONIMO



Curso



Temario General

- ◊ 1. Introducción al Hacking Web
- ◊ 2. Protocolos y arquitectura web
- ◊ 3. Escaneo y enumeración de servicios Web
- ◊ 4. Inyección SQL (SQLi)
- ◊ 5. Cross Site Scripting (XSS)
- ◊ 6. Uso de herramientas (ZAP, BurpSuite)
- ◊ 7. File Upload
- ◊ 8. Explotación
- ◊ 9. Pruebas de autenticación.

3

Introducción al web hacking

- ◊ Actualmente, la mayoría de las aplicaciones web soportan y dan acceso a servicios e información que pueden ir desde una simple noticia a datos confidenciales y personales.
- ◊ Una de las principales preocupaciones de los administradores de aplicaciones debería ser el factor de seguridad con la que están desarrolladas y gestionadas.
- ◊ El tipo mas común de ataque es el *deface*, que afecta a la mayoría de las páginas Web.
- ◊ El curso está orientado a conocer los ataques mas comunes y básicos.

4

Conceptos Previos

- ◊ **SERVIDOR WEB:** Sistema informático que alberga páginas o aplicaciones web, consiste en hardware (servidor, storage) y software (plataforma Apache, GlasFish, etc.)
- ◊ **DNS:** Sistema de Nombres de Dominio que registra las direcciones IP asociadas a los dominios de las aplicaciones web, correo electrónico, FTP, etc. Los nombres de dominio facilitan la identificación y navegación en Internet, porque es más fácil memorizar palabras (www.unas.edu.pe) que números (200.37.135.91).
 - ◊ Existen diferentes niveles de consultas DNS: **Local** (caché DNS del equipo), DNS Primario y DNS secundario.
 - ◊ Existen dos tipos básicos de consulta DNS: **Consulta Recursiva** y **Consulta Iterativa**.

5

Conceptos Previos

- ◊ Ejemplo de registro del caché DNS de un equipo con S.O. Windows.

◊ Visualizar caché DNS

Ipconfig /displaydns

◊ Borrar caché DNS

Ipconfig /flushdns

NOTA: revisar los servicios activos si en caso hay errores en la visualización del caché DNS

```
www.facebook.com
-----
Nombre de registro . . . : www.facebook.com
Tipo de registro . . . : 5
Período de vida . . . : 13
Longitud de datos . . . : 8
Sección . . . . . : respuesta
Registro CNAME. . . . . : star-mini.c10r.facebook.com

Nombre de registro . . . : star-mini.c10r.facebook.com
Tipo de registro . . . : 1
Período de vida . . . : 13
Longitud de datos . . . : 4
Sección . . . . . : respuesta
Un registro (host). . . : 31.13.73.36

epg.unas.edu.pe
-----
Nombre de registro . . . : epg.unas.edu.pe
Tipo de registro . . . : 1
Período de vida . . . : 3001
Longitud de datos . . . : 4
Sección . . . . . : respuesta
Un registro (host). . . : 200.37.135.91
```

6

Conceptos Previos

- ◊ **HTTP:** Protocolo de Transferencia de Hipertexto. La versión comúnmente utilizada en los servidores es el HTTP/1.1
- ◊ Para la conexión entre cliente y servidor se utilizan **cabeceras** o **headers**, siendo principalmente cabeceras de petición (por ejemplo el tipo de lenguaje y codificación acepta el navegador web, identifica el sistema operativo, navegador web, etc.) y cabeceras de respuesta (datos de servidor). Las peticiones son identificadas con el prefijo **User-Agent**.
- ◊ **Métodos HTTP:** Permiten indicar al servidor que es lo que se desea realizar. Los métodos más importantes son: POST, GET, PUT, DELETE y HEAD.

7

Conceptos Previos

- ◊ **URL:** Localizador Uniforme de Recursos.
- ◊ **URN:** Nombre Uniforme de Recurso
- ◊ **URI:** Identificador Uniforme de Recursos.

URI => URL + URN

Ejemplo:

esquema://máquina:puerto/ruta_directorio/archivo#fragmento

- ◊ Actualmente, es común utilizar URI en lugar de URL.

8

Códigos de Mensajes de respuesta HTTP

- ◊ 404 Not Found
- ◊ 403 Forbidden
- ◊ 400 Bad request

Error cliente

```
root@kali:~# nc -vv 192.168.2.20 80
192.168.2.20: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.2.20] 80 (http) open
TRACE /hola HTTP/1.1
192.168.2.20

HTTP/1.1 400 Bad Request
Date: Fri, 13 Jan 2017 16:20:28 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 378
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
root@kali:~# nc -vv www.unas.edu.pe 80
Warning: inverse host lookup failed for 200.37.135.91
www.unas.edu.pe [200.37.135.91] 80 (http) open
GET /admin HTTP/1.1
host:www.unas.edu.pe

HTTP/1.1 404 Not Found
Date: Fri, 13 Jan 2017 20:31:26 GMT
Server: Apache/2.2.15 (CentOS)
Content-Length: 284
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
root@kali:~# nc -vv www.unas.edu.pe 80
Warning: inverse host lookup failed for 200.37.135.91: Unknown
www.unas.edu.pe [200.37.135.91] 80 (http) open
POST /web/admin HTTP/1.1
host:www.unas.edu.pe

HTTP/1.1 403 Forbidden
Date: Fri, 13 Jan 2017 20:50:50 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.29
Expires: Sun, 18 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: es
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 7 (http://drupal.org)
Connection: close
```

9

Otros Códigos de Mensajes de respuesta HTTP

- ◊ **2xx: Peticiones correctas**
 - ◊ 200 - OK
 - ◊ 201 - Created
 - ◊ 202 - Accepted
 - ◊ 204 - No Content
- ◊ **3xx: Redirecciones**
 - ◊ 301 - Moved Permanently
 - ◊ 302 - Found
 - ◊ 305 - Use Proxy (desde HTTP/1.1)
 - ◊ 308 - Permanent Redirect

- ◊ **5xx Errores de servidor**
 - ◊ 500 - Internal Server Error
 - ◊ 501 - Not Implemented
 - ◊ 502 - Bad Gateway
 - ◊ 503 - Service Unavailable
 - ◊ 504 - Gateway Timeout
 - ◊ 505 - HTTP Version Not Supported

Fuente: RFC 2616

10

Escaneo y enumeración

Herramientas de consultas y escaneos

11

Herramientas de consulta DNS

◊ DIG

Herramienta para consultar información de los servidores DNS.

```
root@kali2016:~# dig ns congreso.gob.pe
; <>> DiG 9.9.5-12.1-Debian <>> ns congreso.gob.pe
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51031
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;congreso.gob.pe.           IN      NS
;; ANSWER SECTION:
congreso.gob.pe.        3600    IN      NS      dns1.unired.net.pe.
congreso.gob.pe.        3600    IN      NS      dns2.unired.net.pe.
;; ADDITIONAL SECTION:
dns2.unired.net.pe.     2409    IN      A       200.37.10.35
dns1.unired.net.pe.     2622    IN      A       200.37.10.34
;; Query time: 33 msec
;; SERVER: 200.48.225.130#53(200.48.225.130)
;; WHEN: Wed Jan 11 21:45:04 PET 2017
;; MSG SIZE  rcvd: 125
```

Herramientas de consulta DNS

◊ NSLOOKUP

Otra herramienta útil para consultar las direcciones IP de los dominios deseados y de los servidores DNS.

```
C:\Users\... nslookup
Servidor predeterminado: cachewas.tdp.net.pe
Address: 200.48.225.130

> set q=ns
> congreso.gob.pe
Servidor: cachewas.tdp.net.pe
Address: 200.48.225.130

Respuesta no autoritativa:
congreso.gob.pe nameserver = dns1.unired.net.pe
congreso.gob.pe nameserver = dns2.unired.net.pe

dns1.unired.net.pe      internet address = 200.37.10.34
dns2.unired.net.pe      internet address = 200.37.10.35
>
```

```
root@kali2016:~# nslookup www.google.com
Server: 200.48.225.130
Address: 200.48.225.130#53

Non-authoritative answer:
Name: www.google.com
Address: 74.125.21.103
Name: www.google.com
Address: 74.125.21.106
Name: www.google.com
Address: 74.125.21.147
Name: www.google.com
Address: 74.125.21.105
Name: www.google.com
Address: 74.125.21.99
Name: www.google.com
Address: 74.125.21.104
```

13

Herramientas de consulta DNS

◊ NSLOOKUP, para el registro SOA (*Start Of Authority*)

```
> set q=soa
> www.unas.edu.pe
Servidor: cachewas.tdp.net.pe
Address: 200.48.225.130

unas.edu.pe
primary name server = dns1.unired.net.pe
responsible mail addr = hostmaster.unired.net.pe
serial = 2016053113
refresh = 28800 <8 hours>
retry = 7200 <2 hours>
expire = 604800 <7 days>
default TTL = 86400 <1 day>
```

14

Herramientas de consulta DNS

- ❖ **DIG**, para el registro SOA

```
root@kali2016:~# dig SOA www.unas.edu.pe

; <>> Dig 9.9.5-12.1-Debian <>> SOA www.unas.edu.pe
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49824
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.unas.edu.pe.           IN      SOA

;; AUTHORITY SECTION:
unas.edu.pe.          3600    IN      SOA      dns1.unired.net.pe. hostmaster.u
nired.net.pe. 2016053113 28800 7200 604800 86400
```

15

DNS: Transferencia de zona

- ❖ Realizar una transferencia de zona es volcar la información de un servidor de DNS a otro servidor DNS (generalmente del servidor DNS primario al secundario); y para los atacantes puede ser muy útil tener toda esa información. Para realizar una transferencia de zona “no autorizada” el servidor DNS debe estar MAL configurado.
- ❖ Actualmente muchos servidores han corregido esta vulnerabilidad de **Transferencia de Zona**.
- ❖ Existen múltiples herramientas, tanto a nivel de escritorio como online, entre ellas: **Dig** con el parámetro AXFR, **nslookup** con el comando **ls -d dominio.com**, **whois** (<http://whois.domaintools.com/>), **DNSStuuf** (<http://www.dnsstuff.com/tools>), **Fierce**, entre otros.

16

DNS: Transferencia de zona

- ◊ Transferencia de Zona con NSLOOKUP

```

> nslookup -oquery < tu query>
> unas.edu.pe
Servidor: cachewas.tdp.net.pe
Address: 200.48.225.130

Respuesta no autoritativa:
unas.edu.pe      nameserver = dns1.unired.net.pe
unas.edu.pe      nameserver = dns2.unired.net.pe

dns2.unired.net.pe      internet address = 200.37.10.35
dns1.unired.net.pe      internet address = 200.37.10.34
server dns1.unired.net.pe
servidor predeterminado: dns1.unired.net.pe
Address: 200.37.10.34

> ls -d unas.edu.pe
[dnsl.unired.net.pe]
*** No se puede hacer una lista del dominio unas.edu.pe: Query refused
El servidor DNS rechazó la transferencia de la zona unas.edu.pe a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para unas.edu.pe en el servidor DNS en la dirección IP 200.37.10.34.
>
```

17

DNS: Transferencia de zona

- ◊ Transferencia de zona exitoso

```

root@kali:~# dig @192.168.2.21 midarknet.com AXFR
; <>> DiG 9.9.5-9+deb8u3-Debian <>> @192.168.2.21 midarknet.com AXFR
; (1 server found)
;; global options: +cmd
midarknet.com.      604800  IN      SOA     ServerDNS. root.ServerDNS. 2 604
800 86400 2419200 604800
midarknet.com.      604800  IN      NS      ServerDNS.
midarknet.com.      604800  IN      A       192.168.2.21
midarknet.com.      604800  IN      AAAA    ::1
midarknet.com.      604800  IN      SOA     ServerDNS. root.ServerDNS. 2 604
800 86400 2419200 604800
;; Query time: 1 msec
;; SERVER: 192.168.2.21#53(192.168.2.21)
;; WHEN: Thu Jan 12 16:08:14 PET 2017
;; XFR size: 5 records (messages 1, bytes 175)
```

18

Herramienta Fierce

- ❖ Recopila información del servidor DNS, intentando realizar una transferencia de zona y buscando subdominios.

```
root@kali2016:~# fierce -dns unas.edu.pe
DNS Servers for unas.edu.pe:
dns1.unired.net.pe
dns2.unired.net.pe

Trying zone transfer first...
Testing dns1.unired.net.pe
Request timed out or transfer not allowed.
Testing dns2.unired.net.pe
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
200.37.135.91 academico.unas.edu.pe
200.37.135.92 apps.unas.edu.pe
200.37.135.102 datos.unas.edu.pe
200.37.135.91 ftp.unas.edu.pe
200.37.135.91 www.unas.edu.pe

Subnets found (may want to probe here using nmap or unicornscan):
200.37.135.0-255 : 5 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 5 entries.
```

19

NetCat

- ❖ Netcat con el método **HEAD**

```
root@kali2016:~# nc -vv www.munitingomaria.gob.pe 80
DNS fwd/rev mismatch: munitingomaria.gob.pe != dl.sipanserver.com
munitingomaria.gob.pe [64.20.40.34] 80 (http) open
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Last-Modified: Tue, 30 Aug 2016 20:45:01 GMT
Content-Type: text/html
Content-Length: 111
Date: Fri, 13 Jan 2017 01:16:03 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

sent 17, rcvd 208
```

20

NetCat

- ◊ NetCat con el método **GET**

```
root@kali2016:~# nc -vv www.munitingomaria.gob.pe 80
DNS fwd/rev mismatch: munitingomaria.gob.pe != dl.sipanserver.com
munitingomaria.gob.pe [64.20.40.34] 80 (http) open
GET /index.html HTTP/1.1

HTTP/1.1 200 OK
Last-Modified: Tue, 30 Aug 2016 20:45:01 GMT
Content-Type: text/html
Content-Length: 111
Date: Fri, 13 Jan 2017 01:32:24 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"></head><body></body></html>
sent 26, rcvd 319
```

21

NetCat

- ◊ NetCat con el método **GET**

```
root@kali2016:~# nc -vv www.unheval.edu.pe 80
Warning: inverse host lookup failed for 190.235.204.85: Unknown host
unheval.edu.pe [190.235.204.85] 80 (http) open
GET / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Fri, 13 Jan 2017 01:24:26 GMT
Server: Apache/2.4.17 (Unix) OpenSSL/1.0.1p PHP/5.6.14 mod_perl/2.0.8-dev Perl/v5.16.3
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
```

22

NetCat

◊ NetCat con el método **TRACE**

```
root@kali:~# nc -vv www.unas.edu.pe 80
Warning: inverse host lookup failed for 200.37.135.91: Unknown host
www.unas.edu.pe [200.37.135.91] 80 (http) open
TRACE /hola HTTP/1.1
host:www.unas.edu.pe

HTTP/1.1 200 OK
Date: Fri, 13 Jan 2017 20:59:14 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http

2f
TRACE /hola HTTP/1.1
host: www.unas.edu.pe

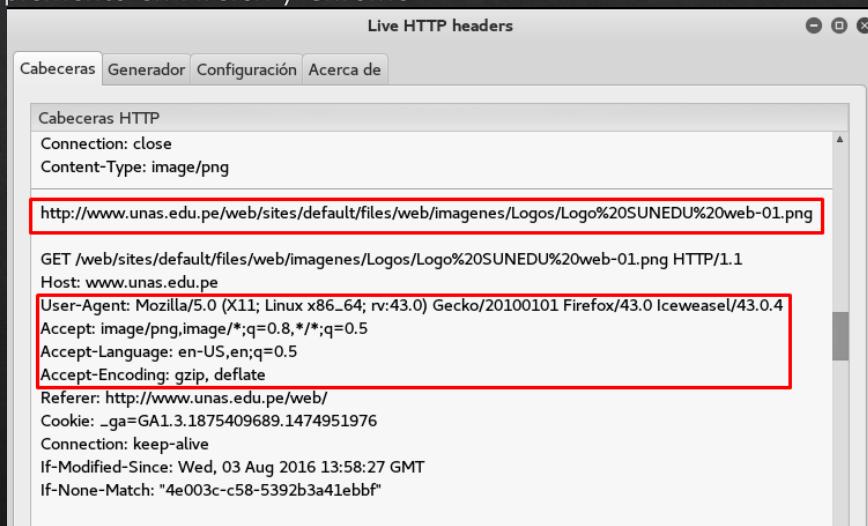
0

sent 43, rcvd 221
```

23

Live HTTP Headers

◊ Complemento en Firefox y Chrome



24

Live HTTP Headers

Información sobre nuestro equipo y navegador

```

GET /web/sites/default/files/web/imagenes/Logos/Logo%20SUNEDU%20web-01.png HTTP/1.1
Host: www.unas.edu.pe
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.unas.edu.pe/web/
Cookie: _ga=GA1.3.1875409689.1474951976
Connection: keep-alive
If-Modified-Since: Wed, 03 Aug 2016 13:58:27 GMT
If-None-Match: "4e003c-c58-5392b3a41ebbf"

```

Lo que el cliente acepta.

25

Live HTTP Headers

◊ Método POST

http://www.unas.edu.pe/web/user	Cuenta de usuario
POST /web/user HTTP/1.1	Iniciar sesión Solicitar una nueva contraseña
Host: www.unas.edu.pe	Nombre de usuario/a *
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/3	admin
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Escriba su nombre de usuario UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA.
Accept-Language: en-US,en;q=0.5	Contraseña *
Accept-Encoding: gzip, deflate	Escriba la contraseña asignada a su nombre de usuario.
Referer: http://www.unas.edu.pe/web/user	<input type="button" value="Iniciar sesión"/>
Cookie: _ga=GA1.3.891285735.1484262845; has_js=1	
Connection: keep-alive	
Content-Type: application/x-www-form-urlencoded	
Content-Length: 126	
name=admin&pass=admin&form_build_id=form-apoB3ogbRmdrQRJNQYAYTr2afJMtrQFdbmer9hlty..	

26

Live HTTP Headers

- ❖ Método **POST** para subir archivos

Choose an image to upload:

No file selected.

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.2.250
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.250/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=59l5h32jgmkqvsmvt1dubcg14
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----981524394370226121148342181
Content-Length: 832188
-----
-----981524394370226121148342181
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----
-----981524394370226121148342181
Content-Disposition: form-data; name="uploaded"; filename="bombita.png"
Content-Type: image/png


```

27

HTTP Fingerprinting

- ❖ **Banner Grabbing.** Técnica utilizada para obtener información de las características del servidor Web. Utiliza el método HEAD.

```
root@kali:~# nc -vv www.unas.edu.pe 80
Warning: inverse host lookup failed for 200.37.135.91: Unknown host
www.unas.edu.pe [200.37.135.91] 80 (http) open
HEAD / HTTP/1.1
host:www.unas.edu.pe

HTTP/1.1 302 Found
Date: Fri, 13 Jan 2017 21:22:37 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.29
Location: /web
Connection: close
Content-Type: text/html; charset=UTF-8
```



28

TIP

❖ Para minimizar la información que un atacante pueda obtener del servidor o por lo menos hacerlo un poco mas “difícil” se puede configurar el archivo **httpd.conf** o **apache2.conf** de un servidor ya instalado.

❖ Modificar o agregar lo siguiente:

ServerSignature Off

ServerTokens Prod

29

HTTP Fingerprinting

Host	Port	Banner Reported	Banner Deduced	Conf.%
www.unas.edu.pe	80	<input type="checkbox"/> Apache/2.2.15 (CentOS)	Lotus-Domino/6.x	52.41
192.168.2.20	80	<input type="checkbox"/> Apache/2.4.7 (Ubuntu)	Apache/2.0.x	72.29
www.pronis.gob.pe	80	<input type="checkbox"/> Microsoft-IIS/7.5	Microsoft-IIS/6.0	75.90

Apache/2.4.7 (Ubuntu)
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC50D7645B5811C9DC5811C9DC5CD37187C11DC7D7811C9DC5811C9DC52655F350FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC56ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C295E2CE6923E2CE69236ED3C295811C9DC5E2CE6927ECE6923

Apache/2.0.x: 120 72.29
Apache/1.3 [1-3]: 112 56.49
Apache/1.3 [4-24]: 112 56.49
Apache/1.3.27: 111 54.69

Report File: K:\Tools\HTTPrint\htprint_301\win32\htprintoutput.html html xml csv Clear All Options

htprint has been completed..

30

DESAFIO 1

- ◊ Obtener información de los servidores DNS y WEB de los siguientes dominios:
 - ◊ munitingomaria.gob.pe
 - ◊ elcomercio.pe
 - ◊ pcm.gob.pe
 - ◊ sunedu.gob.pe
 - ◊ concytec.gob.pe

NOTA: Para la obtención de puntos se deberá presentar la información ORDENADA.

PUNTOS G: 5

31