

## **Seguridad en Apache (CertBot)**

Práctica 3Bis Unidad de Trabajo 3

SERVICIOS DE RED E INTERNET

Cristóbal Suárez Abad

2º ASIR

1. Prueba a implementar uno de dichos certificados públicos en tu servidor web (tu casa o AWS), creando un sitio seguro para dicho dominio y visita tu web segura (<https://2asirXY.institutodh.net>), debes facilitar a tu profesor la URL/IP de tu web pública o AWS para la actualización del DNS.

Instalamos “certbot” en la máquina Ubuntu donde tenemos nuestro servidor web, en este caso Apache:

***sudo apt-get update***

***sudo apt-get install certbot python3-certbot-apache***

```
? packages can be upgraded. Run 'apt list --upgradable' to see them.  
Ubuntu@onepunchman:~$ sudo apt-get install certbot python3-certbot-apache |
```

Si fuese un servidor nginx, usaríamos:

***sudo apt-get install certbot python3-certbot-nginx***

Después usamos:

**“sudo certbot --apache -d tudominio.com”**

O

**“sudo certbot --nginx -d tudominio.com”**

```
onepunchman.institutodh.net
ubuntu@onepunchman:~$ sudo certbot --apache -d onepunchman.institutodh.net
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): cristobal2590@gmail.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.5-February-24-2025.pdf. You must
agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: Y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
Account registered.

Requesting a certificate for onepunchman.institutodh.net

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/onepunchman.institutodh.net/fullchain.pem
Key is saved at:      /etc/letsencrypt/live/onepunchman.institutodh.net/privkey.pem
This certificate expires on 2026-02-02.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for onepunchman.institutodh.net to /etc/apache2/sites-available/000-default-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://onepunchman.institutodh.net

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
 * Donating to EFF:                  https://eff.org/donate-le
-----
ubuntu@onepunchman:~$ |
```

Te indica donde ha enviado la dirección del certificado.

```
Deploying certificate
Successfully deployed certificate for onepunchman.institutodh.net to /etc/apache2/sites-available/000-default-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://onepunchman.institutodh.net
```

Comprobamos que funciona.



Page Info — https://onepunchman.institutodh.net/

General Media Permissions Security

**Website Identity**

Website: onepunchman.institutodh.net  
Owner: This website does not supply ownership information.

Verified by: **Let's Encrypt** [View Certificate](#)

**Privacy & History**

Have I visited this website prior to today? No

Is this website storing information on my computer? No [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

**Technical Details**

Conexión cifrada (TLS\_AES\_128\_GCM\_SHA256, claves de 128 bits, TLS 1.3)  
La página que está viendo fue cifrada antes de transmitirse por Internet.  
El cifrado dificulta que personas no autorizadas vean la información que viaja entre sistemas. Es, por tanto, improbable que nadie lea esta página mientras viajó por la red.  
Este sitio web cumple con la directiva de transparencia de certificados.

[Help](#)

## Certificate

onepunchman.institutodh.net	E7	ISRG Root X1
<b>Subject Name</b>		
Common Name	onepunchman.institutodh.net	
<b>Issuer Name</b>		
Country	US	
Organization	Let's Encrypt	
Common Name	E7	
<b>Validity</b>		
Not Before	Tue, 04 Nov 2025 07:09:41 GMT	
Not After	Mon, 02 Feb 2026 07:09:40 GMT	
<b>Subject Alt Names</b>		
DNS Name	onepunchman.institutodh.net	
<b>Public Key Info</b>		
Algorithm	Elliptic Curve	
Key Size	256	
Public Value	04:37:C5:29:74:40:42:81:1F:2F:2E:0C:F2:FD:E9:A9:08:A6:FD:60:C4:44:1C:AC:BB:A...	
<b>Miscellaneous</b>		
Serial Number	05:E0:E0:65:E5:64:7A:0D:E5:B0:96:D3:AB:3B:32:B6:53:2F	

### IMPORTANTE:

**“Certbot incluye un servicio de renovación automática para asegurarse de que tus certificados nunca caduquen. Los certificados de Let's Encrypt tienen una valididad de 90 días, por lo que es esencial configurar la renovación automática.**

**Certbot actualmente NO añade automáticamente una tarea cron al instalar un certificado, debe añadir al cron:”**

**sudo certbot renew**