

Mastering 403 Bypass

Jesus Lujan (Aka. s4yhii)

```
> ERROR CODE: "HTTP 403 Forbidden"
> ERROR CODE: "HTTP 403 Forbidden"
> ERROR DESCRIPTION: "Access Denied. You Do Not Have The Permission To Access This Page On This Server"
> ERROR POSSIBLY CAUSED BY: [execute access forbidden, read access forbidden, write access forbidden, ssl required, ssl 128 required, ip address rejected, client certificate required, site access denied, too many users, invalid configuration, password change, license required, client certificate revoked, directory listing denied, client access denied, licenses exceeded, client certificate is untrusted or invalid, client certificate has expired or is not yet valid, passport logon failed, source access denied, infinite depth is denied, too many requests from the same client ip.]] ACCESS: [Home Page, About Us, Contact Us, Blog...]
> SOME PAGES ON THIS SERVER THAT YOU DO HAVE PERMISSION TO ACCESS: [Home Page, About Us, Contact Us, Blog...]
> HAVE A NICE DAY SIR AXLEROD :-)
```

Hack The Box Meetup:
Lima, PE.



\$whoami



- Appsec Engineer at Inside Sec (Banco de Chile)
- Mentor CibersecUNI Appsec Squad

Jesus Lujan Montufar (Aka. s4yhii)
OSCP+ | CBBH | eWPTX | eCPPT | eMAPT

Ingeniero de sistemas - UNI (👽)

Blog : s4yhii.github.io

Linked: <https://www.linkedin.com/in/jesusluj4n/>



Contenido



Nociones necesarias

1. Cuando debemos tratar de bypasear 403?
2. Ambiente de R.Proxy/Waf
3. En que contexto estamos y cómo lo identificamos?
4. Ejemplos de reportes de Hackerone (X-Rewrite-URL, X-Forwarded-For, Uppercase bypass) (ez \$\$)
5. Uso de plugin 403 Bypasser en Caido (<https://github.com/bebiksior/Caido403Bypasser>)

Formas de bypass

- Encoding (encode URL, double URL Encode, unicode normalization)
- # is a delimiter?, uso de # para crear inconsistencia.
- Traversals(./, ../, ../, /-> \, //, ../)
- Diferentes escenarios (SSRF, Desde adentro de la red?)
- Headers para reescribir el path
 - <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/403-and-401-bypasses#http-headers-fuzzing>
 - X-Rewrite-Url para cambiar host header, path.
 - Use de param miner para encontrar headers, cookie params, body params, etc.
- Caracteres no imprimibles (ver blog de rafa, espacios, tabs, saltos de linea, null bytes, etc)
- Uso IIS cookieless feature para crear inconsistencia. (/admin/S(x)/main.aspx)

Kelvin Symbol Normalization?



bi.tk/utf8.html



```
const kelvin = 'K';  
console.log(kelvin.toLowerCase());
```



```
const kelvin = 'K';  
const normalizedNFKD = kelvin.normalize('NFKD');  
console.log(normalizedNFKD);
```

Excalidraw



- <https://excalidraw.com/#json=T12GEw285Z028Vfvx9jr9,d-azHhZx0zaHBS2G6GA6wQ>

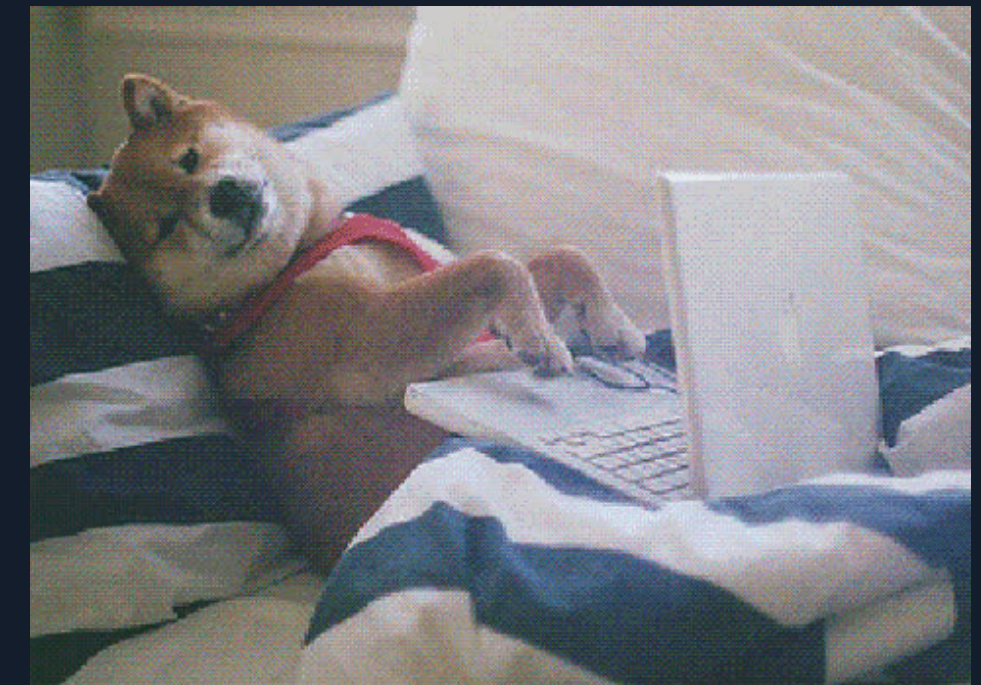
Lab (Practica!)

- <https://github.com/s4yhii/Talk-Resources/raw/refs/heads/main/403Bypasslab.zip>

Recursos 403



- <https://rafa.hashnode.dev/exploiting-http-parsers-inconsistencies>
- <https://portswigger.net/research/gotta-cache-em-all>
- <https://soroush.me/blog/2023/08/cookieless-duodrop-iis-auth-bypass-app-pool-privesc-in-asp-net-framework-cve-2023-36899/>
- <https://bi.tk/utf8.html>
- <https://www.youtube.com/watch?v=28xWcRegncw>
- <https://www.youtube.com/watch?v=euO9WbYHm0s>
- <https://www.youtube.com/watch?v=PvpXRBor-Jw>





CTF TIME

**Accede a `http://localhost:1337/admin`
y encuentra la flag.**

Premio: htb voucher vip+ al 1ro
OBS: no vale fuzzing, no es por ahi



HACKTHEBOX



Graciass