Web Service & API Attacks - Skills Assessment

Our client tasks us with assessing a SOAP web service whose WSDL file resides at `http://<TARGET IP>:3002/wsdl?wsdl`.

Assess the target, identify an SQL Injection vulnerability through SOAP messages and answer the question below.

VPN Servers

Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 163ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 13 Submit the password of the user that has a username of "admin". Answer format: FLAG{string}. Please note that the service will respond successfully only after submitting the proper SQLi payload, otherwise it will hang or throw an error.

FLAG{1337_SQL_INJECTION_IS_FUN_:)}

Submit

Previous Finish

? Go to Questions

Table of Contents

Web Service & API Fundamentals

- Introduction to Web Services and APIs
- Web Services Description Language (WSDL)

Web Service Attacks

- SOAPAction Spoofing
- Command Injection
- Attacking WordPress' 'xmlrpc.php'

API Attacks

- Information Disclosure (with a twist of SQLi)
- Arbitrary File Upload
- Local File Inclusion (LFI)
- Cross-Site Scripting
- Server-Side Request Forgery (SSRF)
- Regular Expression Denial of Service (ReDoS)
- XML External Entity (XXE) Injection
- Web Service & API Attacks - Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left