Nikolay Kasapov § Georgi Pazhev

Live Hacking – DVWA And HackTheBox

SEEBURGER
Business Integration

Agenda

1. DVWA – Damn Vulnerable Web Application

- Command Injection – Reverse Shell
- SQL Injection – Dumping Database
- Relfected XSS – Cookie Stealing
- Stored XSS – KeyLogger
- Insecure File Upload – Reverse Shell

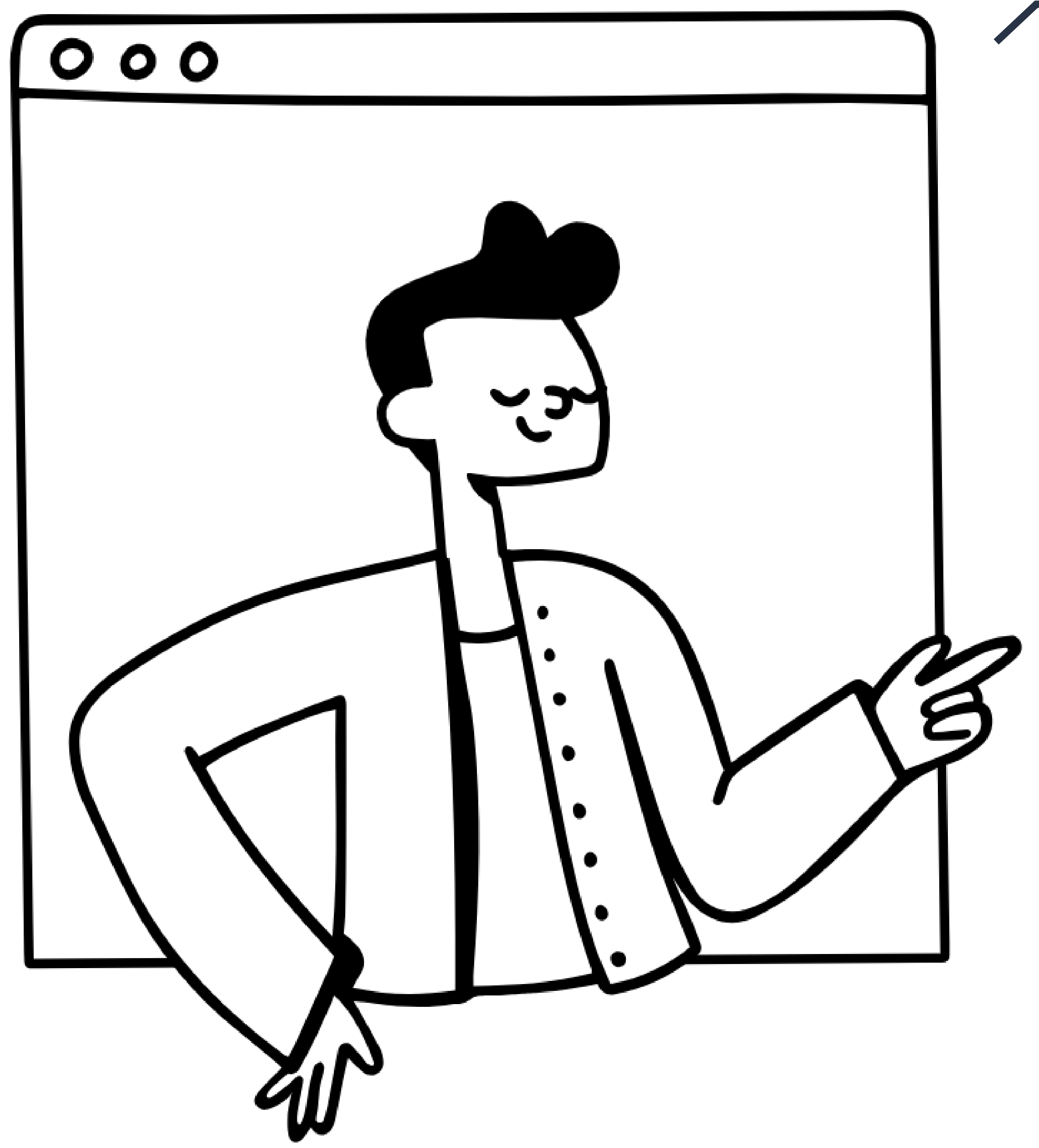
2. Hack The Box

- Scanning with nmap
- Path Traversal
- Reverse Shell
- LinPEAS
- Local Privilege Escalation

DVWA – Damn Vulnerable Web Application

Deliberately vulnerable web application created for educational and training purposes

Provides a web application environment with intentionally implemented vulnerabilities that users can exploit. It is written in PHP and uses MySQL as the database backend. The application includes a wide range of security vulnerabilities



Designed to help individuals learn and practice various web application security techniques, including identifying and exploiting common vulnerabilities.

Free and Open Source.

Installation: https://github.com/digininja/DVWA or https://hub.docker.com/r/vulnerables/web-dvwa

Hack The Box

Hack The Box (HTB) is an online platform that offers a range of virtual machines (VMs) and challenges designed to test and improve penetration testing skills

Provides a realistic environment for learning and practicing various security techniques in a legal and controlled manner.

HTB offers a catalog of vulnerable VMs, referred to as "boxes," that simulate real-world scenarios and contain multiple security vulnerabilities

Offers free and paid subscriptions.

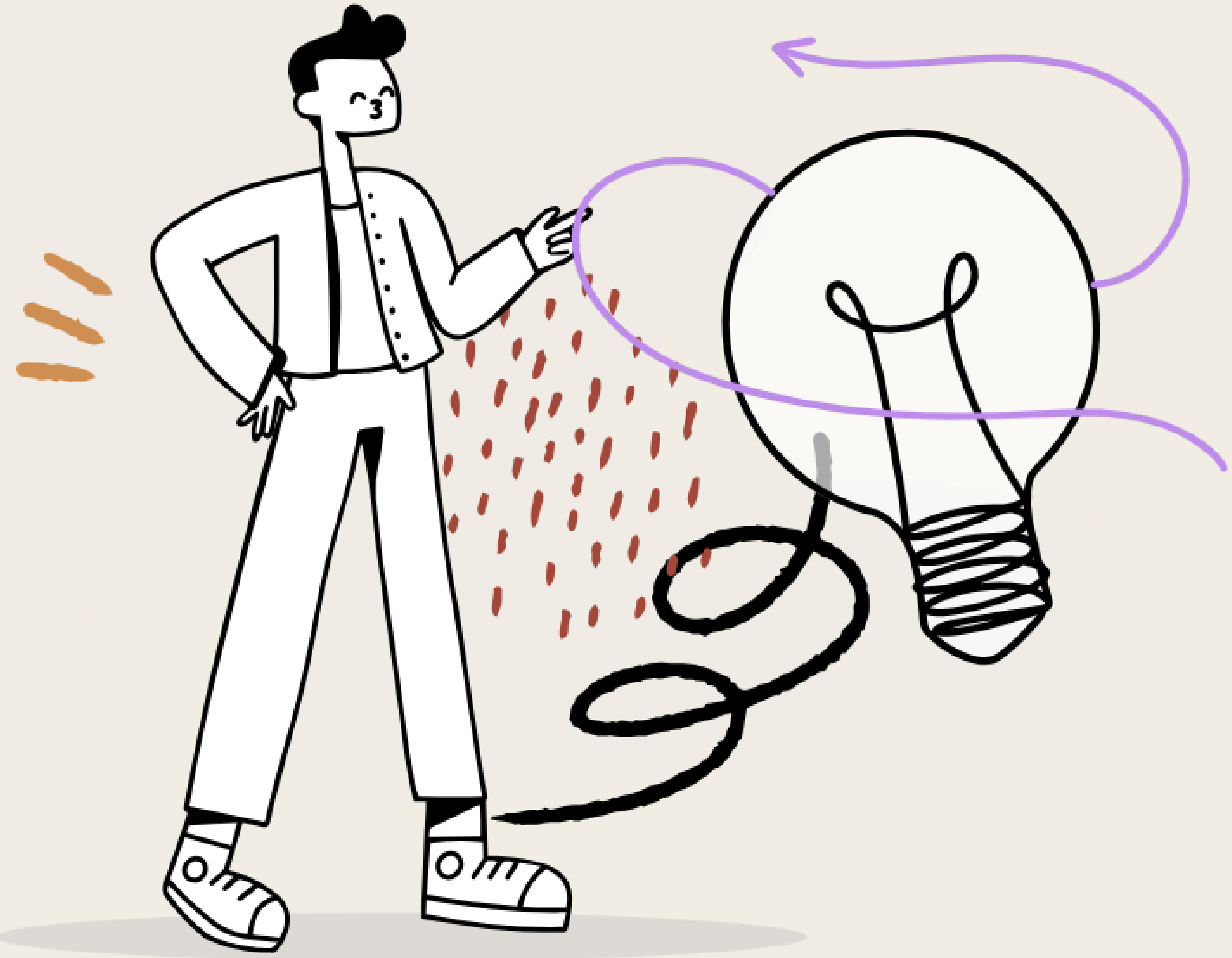
Site: https://www.hackthebox.com/

Disclamer

In no event shall we (**SEEBURGER**) be liable for any direct, indirect, incidental, consequential, or punitive damages arising out of or in connection with the use, missuse or inability to use the tools, techniques and information presented in these slides.

Keep in mind hacking is highly illegal and you and only you is responsible for you actions.

All exploits, techniques, tools and information in these slides is presented only for educational purpose.

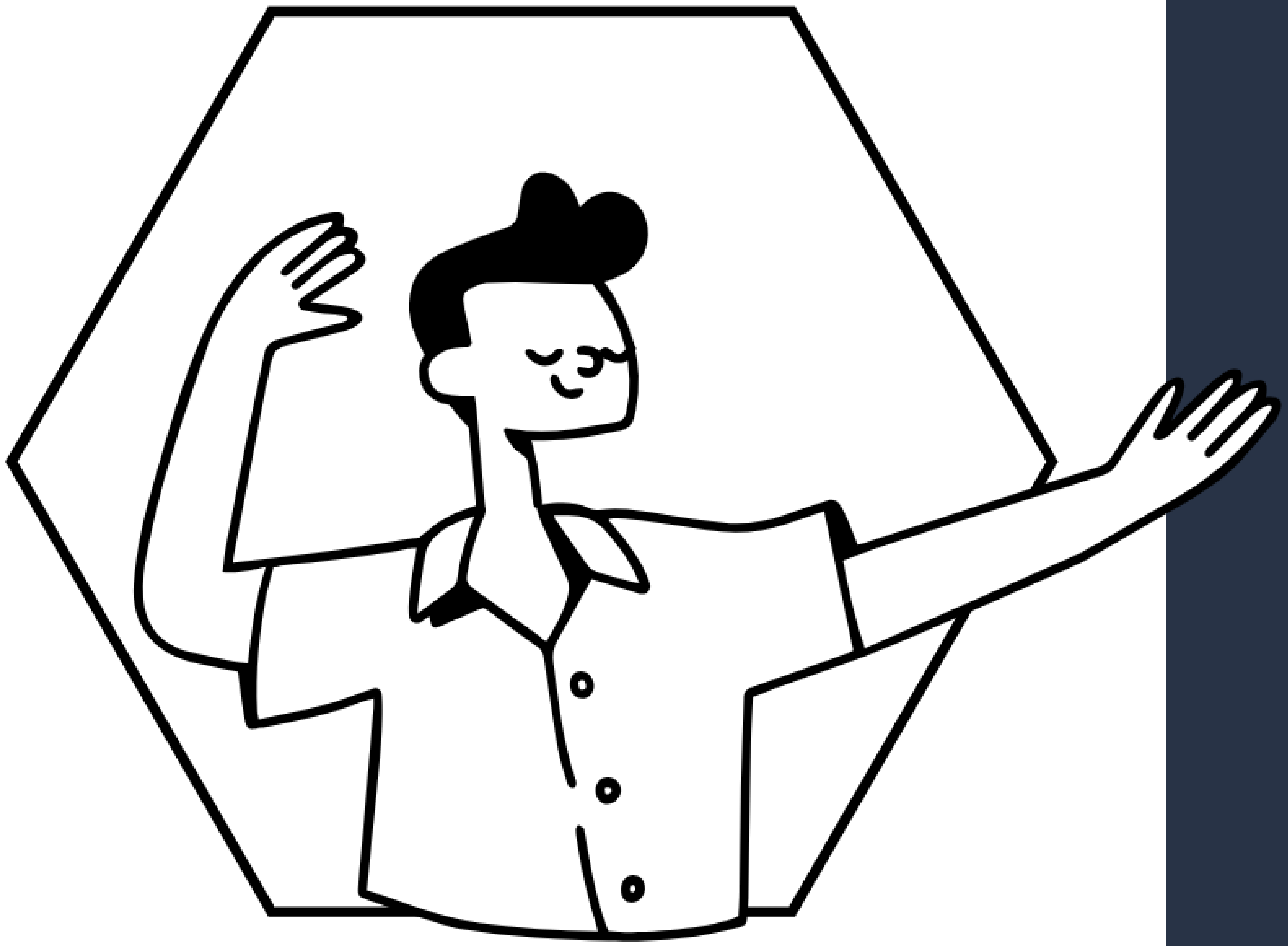


Questions?

SEEBURGER
BUSINESS INTEGRATION

Join Our Team

www.seeburger.bg



Thank You!

Nikolay Kasapov

n.kasapov@seeburger.com

SEEBURGER
Business Integration