Web Application Security

Web application security (also known as Web AppSec) is the idea of building websites to function as expected, even when they are under attack. The concept involves a collection of security controls engineered into a Web application to protect its assets from potentially malicious agents.

Why web applications security is important?

- In order to be safe from hackers and cyber-thieves from accessing sensitive information.
- For the reduction of business risk, the spread and escalation of malware.
- Without it, attacks may happen on the other websites too.
- If a hacker is successful, attacks can spread from computer to computer, making it difficult to find the origin.

How do keep it secured?

❖ Use Strong Passwords

- make passwords at least 8 characters with a mixture of lower-case letters, capitals, numbers, and a special character like an exclamation mark is highly recommended.
- Don't make your password a familiar phrase.

❖ Two-Factor Authorization.

- It provides security as in if a person knows id and password and he/she try to login, in that case he/she needs to authenticate with origin devices it is logged in either by text, phone call, or even through yes or no.

❖ Always Use Secure Networks

- If the address starts with HTTPS, then you know it is secured (by the added "s"). If it doesn't, then you either have the wrong login page or it is possibly a spoof (fake) website.

❖ Use More Than One Email Address

- The email you use for your personal banking might be more secure if you use a different email for things like Facebook, Twitter, and even EBay. If someone were to hack into one then they would not automatically have access to the others.

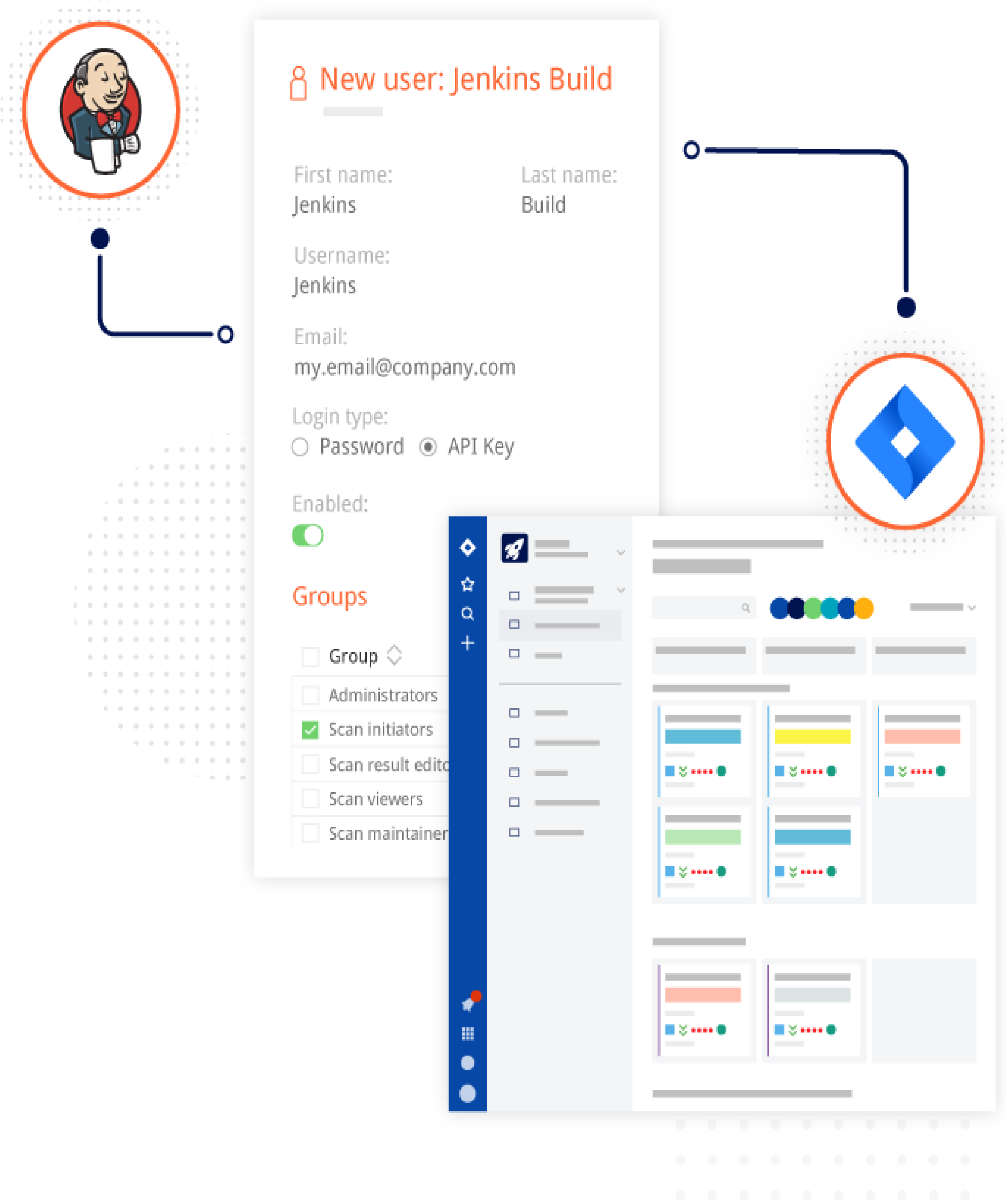
❖ Be Cautious About Posting Your Email Address Online

- This is simply an invitation for spam if nothing else, but it also opens up a message of "Hey, hack me. Here's my email." Avoid posting your email address on forums, review sites, and message boards where spammers can easily pick up your address.

Burp Suite Enterprise Edition

Integrate security with development

Integrated security is a security strategy that leverages a common set of configurations, rules, policies and practices to secure all of an organization's workloads. In other words, integrated security provides a unified solution for every type of service that you run. Its a methodology (often associated with DevSecOps) for creating software that incorporates security into every phase of the software development life cycle (SDLC).



New user: Jenkins Build

First name: Jenkins

Last name: Build

Username: Jenkins

Email: my.email@company.com

Login type: ○ Password ● API Key

Enabled:

Groups

☐	Group
☐	Administrators
☑	Scan initiators
☐	Scan result edito
☐	Scan viewers
☐	Scan maintainer

- Bake security into software development processes
  - A wide array of integrations (e.g., CI/CD, bug-tracking systems, and a rich API) means you can bake security into your software development.

- Security technology, accessible for all
  - Get fast, easily-digested feedback on vulnerabilities, tailored to you.

- Collaborate with AppSec teams to fix security bugs
  - Native Jira integration, featuring ticket options for severity and confidence level triggers, means developers can collaborate with teams to remediate critical issues.

Integration Features

- All major CI/CD platforms
- Integrate with platforms including Jenkins and TeamCity. See vulnerabilities in your development environment.

- Bug tracking systems
- Track issues with Jira and other systems. Auto ticket generation, severity / confidence level triggers, and unlimited boards.

- API-driven workflow
- Integrate with your existing systems to initiate scans and obtain results, via the REST API.

- GraphQL API
- Initiate, schedule, cancel, update, and work through your scans, to get the exact data you need, with a GraphQL API.

- Vulnerability management platforms
- Integrate scanning and security reporting into your own management and orchestration systems.

- Role based access control
- Multi-user, role-based functionality for site hierarchy, scan detail and reporting. Give everyone control.

- Burp extensions
- Tailor Burp Scanner to your exact requirements, by writing your own extensions, or by downloading them from the BApp Store.

- Compatible configurations
- Manually integrate configurations from Burp Suite Pro, directly into your fully automated Enterprise environment.

- ❖ Multiple deployment options
- Choose from a standard deployment with an interactive installer, or a Kubernetes deployment using a Helm chart.

Note: Jenkins, REST API, GraphQL API, Tailor burp, BApp, Kubernetes, Helm Chart -will be explained tomorrow.