Creating SECURE SOFTWARE

Smartphone apps have become an integral part of our lives; used for an ever-expanding variety of purposes. There are apps for raising awareness and tackling the worldwide conversation about climate change, and other apps are educating citizens about wildlife preservation. Mobile apps have turned smartphones into virtual classrooms with students and instructors interacting while fully remote. There are even apps designed to help fight poverty and support charity organizations in unique ways.

Whether for communication, shopping, or to pay taxes, consumers reap the benefits offered by mobile apps, solving problems anytime and anywhere, as users often prefer to interact with organizations at their own convenience. Businesses have realized the potential of well-designed, user-friendly apps and have invested in agile, secure software development methodologies.

CSSLP. Certified Secure Software Lifecycle Professional
An (ISC)² Certification

WHY APPLICATIONS FAIL

Developing an application does not always go as planned. Coding mistakes and oversights result in flawed applications which can then lead to business disruptions. The examples of well-known software failures are numerous, from air traffic services to police and healthcare systems, these projects were derailed for various reasons.

Here are the 7 main reasons why mistakes happen during app development:

- Insufficient project deadlines which lead to low quality and usability for the sake of completion.
- Insufficient budget and allocation of required resources.
- Poor communication between development team members.
- Poor overall project management.
- Inadequate testing to discover bugs and security gaps or testing in production environment.
- Lack of quality assurance and documentation.
- Lack of compliance with industry standards (ISO or W3C).

In our recent member study, we asked software engineers what the most common causes of software project failures were.

91% said “a lack of testing to discover bugs and security gaps”

31% said “poor overall project management”

4 SEVERE IMPACTS OF SOFTWARE FAILURES

Knowing the traps that result in software failures is important. Equally important is to know the impact of a malfunctioning app. The CSSLP certified developers concluded that the four most severe consequences are the following:

1 **Weak access management controls**. Allowing access to applications with options and tasks that do not correspond to the employee profile, resulting in a chaotic situation, with workflow disruptions and imminent data security and privacy violations.

2 **Attacks associated with public facing services**. Failure to integrate security controls during development phases, due to assuming that network and server security controls would be enough to reduce the risk. Traditional network and server defensive controls are not sophisticated enough to withstand security incidents or data breaches, such as the ones caused by cross-site scripting (XSS) attacks.

3 **Sensitive data left unprotected**. Protection of sensitive data is based on encryption. However, merely applying a cryptographic algorithm does not solve all challenges. Weak algorithms or improper data encryption to protect databases and data sets might lead to unauthorized disclosure of sensitive information to unauthenticated users.

4 **Time and cost**. Many developers do not integrate security in their development and operations (DevOps) processes, relying on the security at the infrastructure level. The lack of a security mindset from the early stage of development results in an inefficient cost investment, while the amount of time and workload required to build in security controls will be expended at a later stage.

To demonstrate the impact of what happens when software projects go wrong, read the **stories of software developers here.**

CSSLP
Certified Secure
Software Lifecycle Professional
An (ISC)² Certification

HOW YOU CAN ERADICATE 99% OF TYPICAL SOFTWARE FAILURES

Developers can avoid these devastating software failures by becoming subject matter experts. They should possess the foundational knowledge and skills about secure software lifecycle. Security should be embedded throughout the software lifecycle as an ever thought, rather than an afterthought.

> *“CSSLP doesn’t simply tell me what to do for building secure software. It lets me understand how to build software securely”*

Successful security execution at each phase of the software development lifecycle requires a good understanding of these eight knowledge domains:

1. Foundational concepts.
2. Requirements definition.
3. Architecture and design.
4. Implementation.
5. **Testing and validation.**
6. **Lifecycle management.**
7. **Deployment, operations, and maintenance.**
8. **Software supply chain.**

> *“The CSSLP CBK addresses ways to prevent trivial design faults that can lead to breach events”*

The eight domains of knowledge relating to the secure software lifecycle are covered by the (ISC)^2 Certified Secure Software Lifecycle Professional (CSSLP) Common Body of Knowledge (CBK). The CSSLP CBK provides an end-to-end view of the secure software development lifecycle, while emphasizing security best practices.

By applying the knowledge gained with the study for the CSSLP exam, software developers can avoid predictable and costly errors and build a security-by-design mindset to view application security as a necessity. Software architects become strong advocates of proper security architecture development and foster a cultural change in their organization. They become the leaders who help not only to meet regulatory compliance requirements but also to deliver high quality, secure end products that are user-friendly, scalable, and meet all requirements set by their customers.

> *“The CSSLP CBK addresses ways to prevent trivial design faults that can lead to breach events”*

In addition, certified developers have a foundational understanding of how to implement an end-to-end secure software framework. The CSSLP certification provides the required knowledge to perform secure software implementation, testing, and robust lifecycle management.

Organizations can also reap the benefits of investing in training their development teams. Investing wisely in strengthening your team’s foundational and versatile skillset for secure software development will help build their self-confidence to integrate security into the fast-paced agile process. Building teams of well-trained, knowledgeable developers can increase your organization’s ability to deliver high quality, secure applications. These specialized skills can lower the chances of inherent flaws that could be exploited by criminals. Secure applications will also eliminate the danger of potential legal penalties, liabilities, as well as loss of revenue due to reputational damage.

CSSLP. Certified Secure Software Lifecycle Professional

An (ISC)^2 Certification

HOW THE CSSLP CERTIFICATION CAN HELP YOUR CAREER

The knowledge obtained from the CSSLP certification is beneficial for both the organization and the individual in multiple ways, from professional growth to self-confidence and reputation, to a deeper understanding of the secure software lifecycle

> *“The CSSLP has enabled me to communicate risk and security issues in all phases of the lifecycle to multiple teams, departments, and stakeholders.”*

CSSLP is the industry’s premier secure software development certification. Earning this globally recognized certification is a proven way to build your career and better incorporate security practices into each phase of the software development lifecycle (SDLC).
The CSSLP credential distinguishes leading application security skills. It shows employers and peers that you have the advanced technical skills and knowledge necessary for authentication, authorization, and auditing throughout the SDLC using best practices, policies, and procedures established by the cybersecurity experts at (ISC)².

Are you ready to take the NEXT STEP?

To learn more about CSSLP, check out **our training options**, or download our white paper, **How to Reap the Benefits of DevSecOps**.

CSSLP

How to Reap the Benefits of DevSecOps

[illegible]

Fast pace application development
The fast pace of a DevOps process can lead to an increase in coding mistakes, which could result in undetected bugs and errors. Attackers look for flaws in the code they can exploit to gain access to corporate assets.

Cloud security
The application development process, together with businesses, has migrated to the cloud. Developers are taking advantage of stateless containers and

[illegible]

Implementing security in CI/CD
[illegible]

CSSLP Certified Secure Software Lifecycle Professional
An (ISC)² Certification