SAP Penetration Testing Course

Course level: Advanced

Duration: 2 business days

RedRays, Inc

1111B S Governors Ave STE 7629 Dover, DE 19904 US

+1-564-544-85-07

support@redrays.io

Contents

Short summary

This advanced two-days course offers a deep dive into SAP security testing, featuring extensive hands-on exercises and a practical course.

On the first day, participants explore the fundamentals of SAP security, including the importance of protecting these systems, security assessment tools, common SAP software and its typical vulnerabilities, as well as analysis of SAP ports and services. **Each topic is accompanied by practical exercises to reinforce the knowledge gained.**

The second day is dedicated to more advanced techniques, such as exploiting various SAP attack vectors, privilege escalation methods, and strategies for compromising the entire SAP landscape. Additional topics include attacks on SAP Cloud Connector, exploitation of Remote Function Calls (RFC), and Remote Method Invocation (RMI). Participants will engage in hands-on exercises for each of these aspects.

Special attention is given to the development and use of specialized tools. Participants will be provided with, and collaboratively develop, scripts for analyzing recently patched vulnerabilities. This will enable the detection and potential development of exploits for 0-day and 1-day vulnerabilities. Such skills are particularly valuable for identifying new attack vectors and conducting in-depth security analysis of SAP systems. A significant portion of time will be devoted to practical work with these tools and scripts.

The course is led by Vahagn Vardanyan, a recognized expert in enterprise application security, ensuring high-quality course and the relevance of the information provided. **The course is structured to provide participants with maximum practical experience, allowing them to immediately apply the knowledge gained in real-world scenarios.**

Day 1: Foundations and Key Concepts

1. Introduction to SAP Security and Its Importance

This section provides an overview of the significance of SAP Security, discussing the business risks and operational impacts of security breaches in SAP systems. Participants will gain an understanding of the critical importance of protecting SAP systems.

2. Overview of Common SAP Software and Architectures

Here, participants will become familiar with different types of SAP software and study SAP system architectures. This foundational understanding is necessary for subsequent comprehension of security concepts and vulnerabilities.

3. SAP Ports and Services

This section will conduct a detailed review of open services and ports in various types of SAP systems. Participants will gain practical understanding of potential entry points for attacks, which is crucial for effective security provision.

4. Tools for SAP Security Assessment

This hands-on section is dedicated to testing and using various tools and software for SAP Security assessment. Participants will gain practical experience with security tools in real-world scenarios.

5. OWASP in SAP

This section will examine critical and interesting vulnerabilities discovered in SAP in the past. Applying OWASP concepts in the SAP context will provide a broader understanding of how common web application vulnerabilities manifest in the SAP environment.

6. Segregation of Duties (SoD) Concept in SAP from Attacker's Point of View

This section is devoted to understanding SoD from a security perspective. Examining this concept from an attacker's point of view will aid in identifying weaknesses and reinforcing security measures.

7. Critical SAP T-codes: Security Implications and Controls

This section will explore T-Codes and their impact on security. Participants will learn about methods to mitigate risks associated with T-Code misuse, which is critical for ensuring the security of SAP functionality.

8. Remote Function Call (RFC) Security

This section addresses security concerns related to RFCs in SAP. Securing RFCs is crucial as they are often targeted in attacks due to their ability to execute functions remotely.

9. RMI Security

Here, security aspects of Remote Method Invocation (RMI) in SAP will be covered. Participants will learn how to secure RMI, preventing unauthorized remote method calls.

10. SAP Profile Parameters

This section is dedicated to discussing security-related SAP profile parameters. Correct configuration of profile parameters is essential for securing SAP systems. Best practices and common configuration mistakes will be covered here.

Day 2: Vulnerabilities and Exploitation

1. Vulnerability Detection

This section will review methods for detecting vulnerabilities in SAP. Participants will learn about the importance of staying updated with the latest vulnerabilities and detection methods for proactive security management.

2. Analyzing Structure of SAP Patches and PoC Development

This technical section is devoted to understanding how SAP patches are structured and how to develop Proof of Concept (PoC) exploits. Participants will gain deep insight into how to apply patches effectively and the potential risks if not applied correctly.

3. Critical Vulnerabilities for SAP Systems and SAP Landscape Compromission Vectors

This section will provide a detailed analysis of critical vulnerabilities and compromission vectors in SAP systems. Participants will study vulnerabilities such as directory traversal and privilege escalation, gaining insights into how attackers exploit these weaknesses and how to defend against them. Special attention will be given to topics such as the reasons for the high danger of directory traversal, risks associated with developer privileges, methods of escalating privileges to SYSTEM level, and techniques for decrypting various secure storages in SAP systems.

Trainer's Expertise

- Development of custom SAP security assessment frameworks and automation tools
- Expertise in reverse engineering SAP kernel and application-layer protocols
- Advanced knowledge of SAP ABAP and Java stack internals for vulnerability research
- Experience in developing and deploying SAP security monitoring and incident response solutions

Trainer Profile

Vahagn Vardanyan, Co-founder and CTO of RedRays, is a distinguished expert in enterprise application security, with a focus on SAP and Oracle systems. His extensive experience includes:

- Founder and Author of SAP Security Benchmark for CIS
- Discovering and publishing numerous vulnerabilities in critical business applications, over 150 critical 0-day issues
- Authoring whitepapers and surveys on ERP, CRM, SRM, banking, and processing software security
- Presenting at globally recognized conferences such as BlackHat, Nsec, Hack in Paris, Troopers, and OWASP
- Contributing to the cybersecurity field through research and thought leadership

During the course, Vahagn will share exclusive scripts and code used by RedRays for SAP system Penetration Testing and Vulnerability Assessment, providing attendees with practical, real-world tools and techniques.