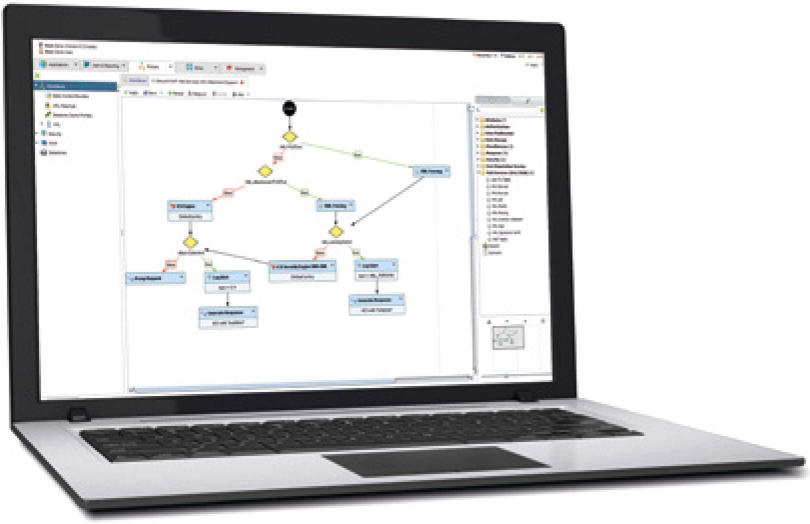
Application Security
Certification Training
2019

ROHDE&SCHWARZ
Cybersecurity

Table of contents



1 Overview

Rohde & Schwarz Cybersecurity offers customers and partners a range of certified training programs covering the implementation cycle of Application Security products. Our courses are mainly designed for security architects, implementation engineers and system administrators and may be taken by anyone tasked with implementing or managing the Rohde & Schwarz Cybersecurity products. The product certificates are issued at the end of each course upon successful completing of the assessment.

More advanced web attack training providing deeper understanding into how to design effective security to protect web applications is available on demand.

All training classes are instructor-led and are delivered in one of our Rohde & Schwarz Cybersecurity locations (see table below). Our courses can also be tailored to meet specific requirements and delivered on customer premises. Our instructors are able to deliver the training in English, German and French.

Please contact us if you do not find the dates or location corresponding to your requirements.

2 Schedule

	R&S®Web Application Firewall		Web Access Manager	API Security		
Duration	**3 days**		**2 days**	**2 days**		
January	28-30 🟢		-	30-1st 🟢		
February	25-27 🔵		-	28-1st 🔵		
March	4-6 🟢		11-12 🟢	7-8 🟢		
April	8-10 ⚫	24-26 🔵	-	11-12 ⚫		
May	-		-	-		
June	3-5 🟢		17-18 🟢	6-7 🟢		
July	-		-	-		
August	12-14 ⚫		-	15-16 ⚫		
September	9-11 🟢	23-25 🔵	16-17 🟢	12-13 🟢		
October	-		-	-		
November	-		-	-		
December	2-4 🔵 🟢	9-11 ⚫	9-10 🟢	5-6 🔵	5-6 🟢	12-13 ⚫

🔵 German ⚫ English 🟢 French

3 Prerequisites

3.1 Course setup requirements

Adequate network access will be provided.
All participants must bring the following equipment:

- A 64-bit laptop with minimum 4 GB of RAM
- A recent browser is required with software or an extension to the HTTP trace connector (HttpFox, HttpWatch, TamperData, Wireshark, etc)
- A Virtualization solution (VMware, VirtualBox, etc)

3.2 Understanding prerequisites

- Knowledge of HTTP / HTTPS and TCP / IP network protocols
- Basic knowledge of the reverse proxy technology
- Basic knowledge of regular expressions
- Basic knowledge of the Linux System Administration

3.3 Web Access Manager requirements

- Basic knowledge of web application authentication and / or SAML
- Basic knowledge of LDAP / Active directory / PKI
- Basic knowledge of HTML

3.4 API Security requirements

- Knowledge of XML standards XSD, WSDL
- Basic knowledge of Web Services

4 Product training

4.1 Learning objectives

To obtain knowledge and experience necessary to install, configure, maintain, monitor and control R&S®Web Application Firewall.

	R&S®Web Application Firewall	Web Access Manager	API Security
Duration	3 days	2 days	2 days
Price	3.000 €	2.000 €	2.000 €
Audience	Security Engineers & Administrators		
Content Delivery	50 % theory / 50 % practice		
Certification	X	-	-
Agenda	ı Getting Started ı Security attacks and defenses (ICX, workflow, forensic) ı Reliability and continuity of traffic (high-availability, load balancing) ı Performance & optimization (caching, compression, SSL acceleration) ı Administration (maintenance, log management, monitoring) ı Troubleshooting and diagnostics	ı Perimeter authentication ı Web SSO ı Authorization Policies ı Management of logs ı Customization ı Troubleshooting and Diagnostics	ı Compliance scheme ı Encryption ı Signature ı Workflow Workshops

4.2 Technical prerequisites

- HTTP/HTTPS protocols
- TCP/IP Networks
- Reverse Proxy Technology
- Basic knowledge of Web Services
- LDAP / Active directory
- PKI
- Regular Expression
- Linux Administration
- Knowledge of XML, XSD, WSDL standards
- Web application authentication and / or SAML

4.3 Description

The training is carried out on the latest stable version of the product, the content covering the latest features and capabilities. The list below only outlines some of the items that may be covered during the training. Each module consists of two parts: an instructor-led presentation and a hands-on practical workshop.

5 Web attack training

5.1 Overview

Web attack is a live classroom training designed to broaden your knowledge of web application attacks and bypass mechanisms used by hackers to counter modern application security. With experienced security professional is mind, it provides valuable student-instructor interaction working on real case studies. This training is only available on demand is always run at customer location.

Duration	3 days
Price	4.500 € (minimum 8 participants)
Audience	Security Teams

5.2 Learning objectives

By the end of this training, every participant should be able to achieve the following:

- Identify families of specific web application vulnerabilities (XSS, SQL Injection, CSRF, XXE, SSRF)
- Exploit previously identified vulnerabilities
- Bypass basic protection mechanisms
- Operate the most common tools
- Adapt the tools to their specific needs

5.3 Technical prerequisites

- HTTP/HTTPS protocols
- TCP/IP Networks

5.4 Description

- Reminders on http:
  - Requests and responses, status and cache management, redirection, authentication, encryption, implicit browser actions...
- Common attacks:
  - Introduction to “OWASP Top 10”: injections (HTML and SQL), unsecured direct references, CSRF, version management.
- Tools:
  - Browser extensions (Chrome, Firefox), interception and replay tools (ZAP, Burp Suite)
- Practical exercises:
  - SQL injection, query manipulation (cookies and settings), password cracking, data extraction...
- Advanced exploitation:
  - Advanced techniques related to the exploitation of SQL and XSS Injection: access to the file system, bypassing filters, mass exploitation, chaining of techniques...
- Vulnerabilities outside “OWASP Top 10”:
  - Theory and practice of modern attacks (JSONP injection, SSRF, XXE...)

6 Enrollment & payment

Rohde & Schwarz Cybersecurity training is available as classroom training at one of our training centers or at your company location. To register, please:

- Go to our website

  www.rohde-schwarz.com/cybersecurity/training

  and sign up using the form

- Or contact your account team for more information

Payment should be made by bank transfer.
After your registration, our team will get in touch with you.

Service that adds value

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity is an IT security company that protects companies and public institutions around the world against espionage and cyberattacks. With more than 500 employees, the company develops and produces technologically leading solutions for information and network security. Development of the trusted IT solutions is based on the security-by-design approach for proactively preventing cyberattacks.

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

Rohde & Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier | 92366 Meudon, France
Info: +33 (0)1 46 20 96 00
Email: sales-fr.cybersecurity@rohde-schwarz.com

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 5216.4479.32 | Version 01.01 | February 2019 (sch)
Application Security Certification Training 2019

Data without tolerance limits is not binding | Subject to change

5215991932

5216.4479.32 01.01 PDP 1 en