



Mit offenen Karten

White Box Application Pentests

it-sa 2022 , 26. Oktober 2022, Jan-Tilo Kirchhoff

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Geschäftsführer Compass Security Deutschland GmbH
- verheiratet, zwei erwachsene Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
 - Netzwerk Sicherheitsprüfungen
 - ICT- Security (VoIP, PSTN, GSM ...)
 - IT-Forensik

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security



Certified Information
Systems Security Professional



Red Team Operator

Awarded to Jan-Tilo Kirchhoff
Issued on 28.03.2022 at 9:36 PM

Compass Crew



Was macht Compass?

seit 1999

Penetration Tests



Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation.

Digital Forensics



Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung.

Security Reviews



Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung.

Security Trainings



Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor.

Wir sind “nette” Hacker



Bild von [Free Photos](#) auf [Pixabay](#)

Tiger Teams



Definitionen (1)

Penetrationstest / Penetrationtest / Pentest

- Eindringversuch

Vulnerability Assessment

- (Umfassende) Suche nach Angriffspunkten

Security Assessment

- (Ganzheitliche) Bewertung der Sicherheit

Red Team

- Angriffssimulation
- (ursprünglich Querdenker/2.Meinung)

Weitere Arten von Sicherheitsprüfungen

- Vulnerability Scans (automatisierte Prüfungen)
- Security Audit (ISO 27000, PCI)



Definitionen (2)

Risiko = Schwachstelle x Bedrohung x Kosten

Schwachstelle (Vulnerability)

- Meist Konfigurations- oder Softwarefehler, die einen möglichen Angriffspunkt darstellen.

Bedrohung (Threat)

- Hier geht es um die tatsächliche bzw. anzunehmende Gefährdung. Wie wahrscheinlich ist es das eine Schwachstelle genutzt wird?

Risiko (Risk)

- Die wirtschaftliche Bewertung der Sicherheit



Defintions (3)

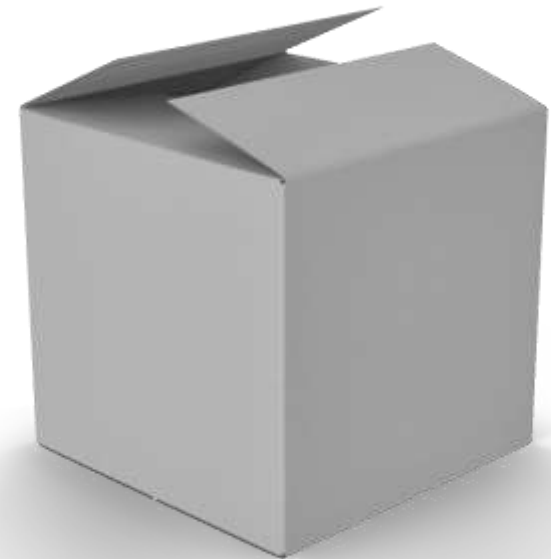
Black, White and Gray Box Testing



Ohne Vorwissen



Volle Transparenz



Teilwissen

Whitebox Pentest

Aus Sicht der Tester

- Bessere Testabdeckung
- Höhere Testtiefe
- Geringerer Zeitaufwand
- Realistischer Ergebnisse

Aus Sicht der Entwickler

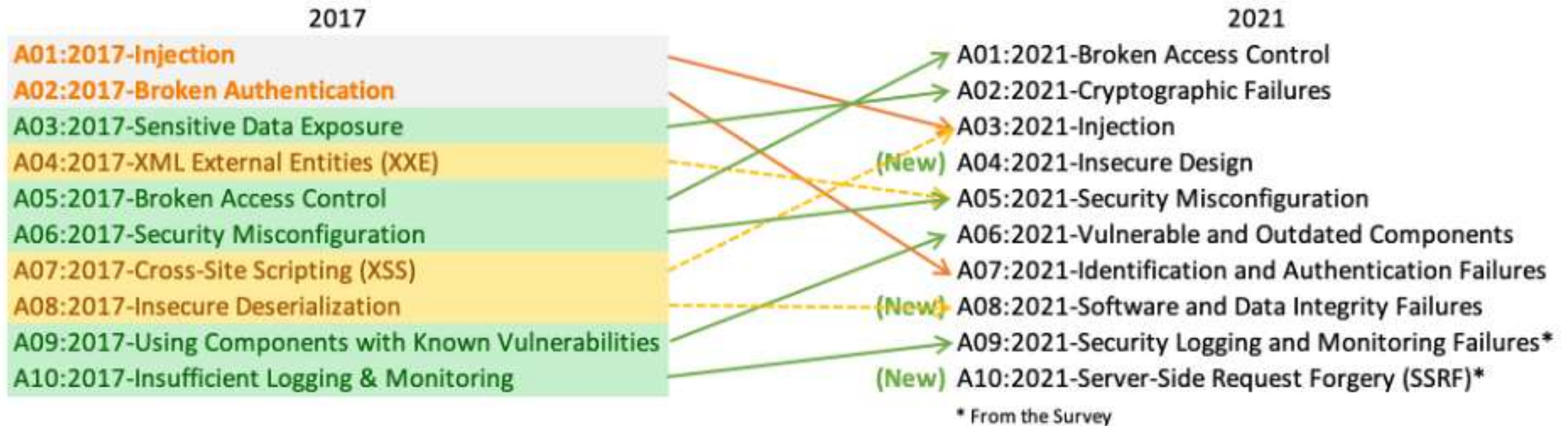
- Weniger False Positives
- Präzisere Informationen
- Kürzere Bearbeitungszeiten



Mitre ATT&CK Matrix

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (13)	BITS Jobs	BITS Jobs	Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (3)	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extensions	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (3)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (2)	Scheduled Task/Job (6)	Create Account (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (13)	Event Triggered Execution (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (2)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	OS Credential Dumping (3)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Implant Internal Image	Hide Artifacts (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Modify Authentication Process (4)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Process Injection (11)	Impair Defenses (2)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Scheduled Task/Job (6)	Scheduled Task/Job (6)	Indicator Removal on Host (3)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
				Office Application Startup (3)	Valid Accounts (4)	Indirect Command Execution	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
				Pre-OS Boot (3)		Masquerading (7)		Peripheral Device Discovery		Screen Capture	Web Service (3)		
				Scheduled Task/Job (6)		Modify Authentication Process (4)		Permission Groups Discovery (3)		Video Capture			
				Server Software Component (4)		Modify Cloud Compute Infrastructure (4)		Process Discovery					
				Traffic Signaling (1)		Modify Registry		Query Registry					
				Valid Accounts (4)		Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (3)		System Information Discovery					
						Pre-OS Boot (3)		System Location Discovery (1)					
						Process Injection (11)		System Network Configuration Discovery (1)					
						Reflective Code Loading		System Network Connections Discovery					
						Rogue Domain Controller		System Owner/User Discovery					
						Rootkit		System Service Discovery					
						Signed Binary Proxy Execution (12)		System Time Discovery					
						Signed Script Proxy Execution (1)		Virtualization/Sandbox Evasion (2)					
						Subvert Trust Controls (3)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (2)							
						Weaken Encryption (2)							
						XSL Script Processing							

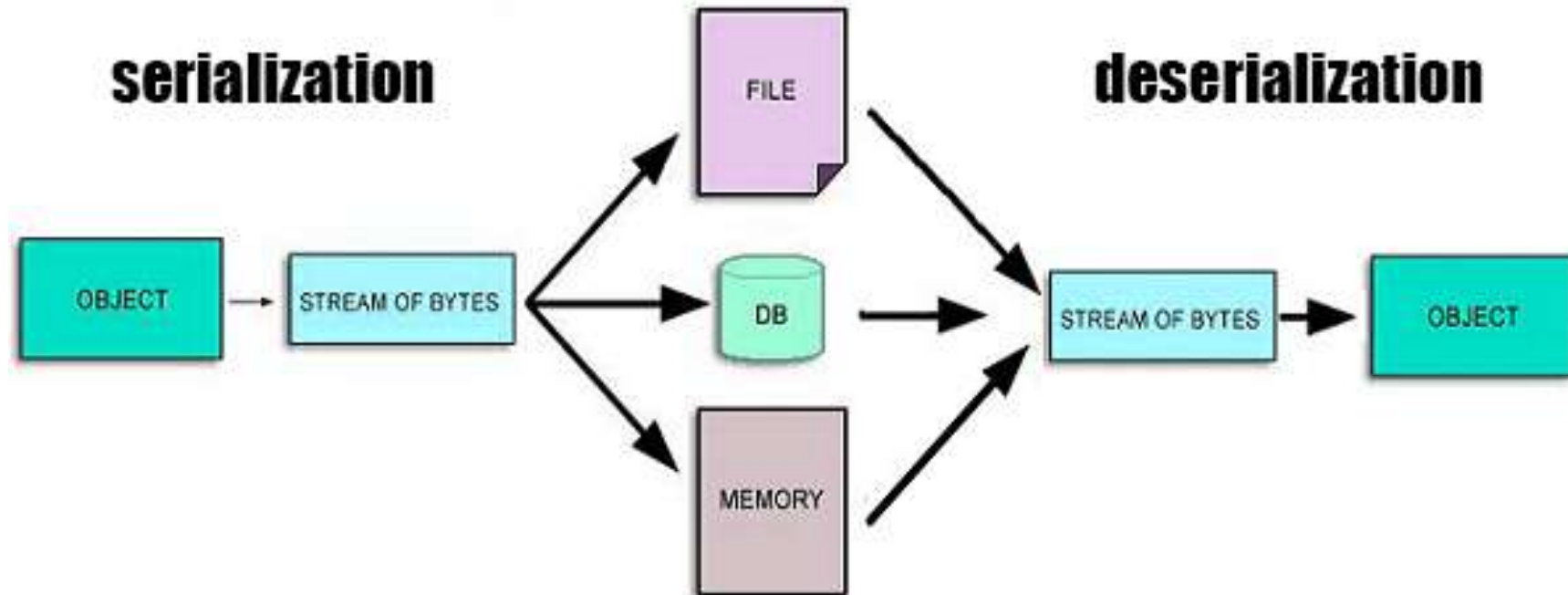
OWASP Top 10 – 2021



A8 Insecure Deserialization (OWASP Top 10 – 2017)

New: “A8 Software and Data Integrity Failures” (OWASP Top 10 -2021)

- Easy to miss and hard to exploit without prior knowledge



Vielen Dank!



**Vielen Dank für Ihre
Aufmerksamkeit!**



Besuchen Sie uns an unserem Messestand

Halle 7 Stand Nr. 7-449





Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

team.csde@compass-security.com

Bildnachweis

Aufstellung der Bildquellen, soweit diese nicht von Compass zur Verwendung lizenziert oder selbst angefertigt wurden:

https://upload.wikimedia.org/wikipedia/commons/a/a4/Deutsche_Spielkarten_mit_fr%C3%A4nkischem_Bild.jpg

https://c1.staticflickr.com/5/4081/4809326028_ff2ced002e_b.jpg

<https://pixabay.com/de/photos/tiger-raubtier-fell-sch%C3%B6n-4697690/>

https://commons.wikimedia.org/wiki/File:Deal_Castle_Aerial_View.jpg

<https://www.publicdomainpictures.net/de/view-image.php?image=101786&picture=elefant>

<https://www.pexels.com/de-de/foto/tier-auge-insekt-schwarzer-hintergrund-9927833/>

<https://owasp.org/Top10/assets/mapping.png>

<https://upload.wikimedia.org/wikipedia/commons/f/f4/Serialization.jpg>

https://commons.wikimedia.org/wiki/File:S%C3%A1rospatak_-_Castle.jpg

https://upload.wikimedia.org/wikipedia/commons/9/9c/The_Turkish_Siege_of_Vienna.JPG

https://de.wikipedia.org/wiki/30,5-cm-Belagerungsm%C3%B6rser#/media/File:Austro-hungarian_305_mm_Howitzer.jpg