more security. usd

ASV SCAN REPORT SUMMARY

Zeitfracht Medien GmbH

Author Roman Fojtik

Version 1.0
Date 09/24/2025
Scan # 21175

ATTESTATION OF SCAN COMPLIANCE

Scan Customer Information

Company:	Zeitfracht Medien GmbH		
Contact Name:	Jochen Walter		
Job Title:	Leiter e-commerce		
Telephone:	0491727119761	E-mail:	e-commerce@zeitfracht.de
Business Address:	Ferdinand-Jühlke-Straße 7		
ZIP:	99095	City:	Erfurt
State/Province:		Country:	Germany
Website/URL:			

Approved Scanning Vendor Information

Company:	usd AG		
Contact Name:	PCI Competence Center		
Job Title:			
Telephone:	+49 6102 8631-90	E-mail:	pci@usd.de
Business Address:	Frankfurter Str. 233, Haus C1		
ZIP:	63263	City:	Neu-Isenburg
State/Province:		Country:	Germany
Website/URL:	pci.usd.de		

Scan Status

Date scan completed:	24 September, 2025	Scan expiration date (90 days from date scan completed):	23 December, 2025
Compliance status:	PASS	Scan report type:	Full scan
Number of unique in-scope components scanned:			1
Number of identified failing vulnerabilities:			0
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:			0

Scan Customer Attestation

Zeitfracht Medien GmbH attests on 01 October, 2025 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions - including compensating controls if applicable - is accurate and complete.
Zeitfracht Medien GmbH also acknowledges
1) accurate and complete scoping of this external scan is my responsibility, and
2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

This scan and report was prepared and conducted by usd AG under certificate number 3999-01-19, according to internal processes that meet PCI DSS Requirement 11.3.2 and the ASV Program Guide.

usd AG attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of
1) disputed or incomplete results,
2) false positives,
3) compensating controls (if applicable), and
4) active scan interference.
This report and any exceptions were reviewed by Roman Fojtik.

ASV SCAN REPORT SUMMARY

Part 1. Scan Information

Scan customer company:	Zeitfracht Medien GmbH	ASV Company:	usd AG
Date scan was completed:	24 September, 2025	Scan expiration date:	23 December, 2025

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):	20.79.89.13/www.buchkatalog.de	PASS

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by ASV for this Vulnerability)
20.79.89.13 www.buchkatalog.de port 443/tcp	12689 - Wordpress Newsletter Plugin Cross-Site Scripting Vulnerability Wordpress Newsletter Plugin	MED	6.5	PASS	We do not have any PHP application installen on our system, like Wordpress or Joomla. The response for the request you're requesting, is an error page (404, This page could not be found).
20.79.89.13 www.buchkatalog.de port 80/tcp	150004 - Predictable Resource Location Via Forced Browsing	MED	5.3	PASS	
20.79.89.13 www.buchkatalog.de port 443/tcp	11827 - HTTP Security Header Not Detected	MED	5.3	PASS	We do use X-Frame-Options with the value "deny", so our content can not fetched from an iframe. Also http is not possible. A request will be forwared always to https. This is done on the server. The other headers like X-Content-Type-Options and Content Security Policy , we currently do not use. Were looking into this to hopefully get those included with the next release
20.79.89.13 www.buchkatalog.de port 443/tcp	730735 - Joomla Webservice Endpoints Improper Access Control Vulnerability (Active Check) CVE-2023-23752, Joomla Security Advisory	MED	5.3	PASS	We do not have any PHP application installen on our system, like Wordpress or Joomla. The response for the request you're requesting, is an error page (404, This page could not be found).
20.79.89.13 www.buchkatalog.de port 443/tcp	150004 - Predictable Resource Location Via Forced Browsing	MED	5.3	PASS	
20.79.89.13 www.buchkatalog.de port 443/tcp-SSL	38655 - X.509 Certificate SHA1 Signature Collision Vulnerability	MED	5.3	PASS	this is a false positive, since the SHA1 algorithm is only used for the root certificate.

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely or removed
20.79.89.13 www.buchkatalog.de	Embedded links detected	External Links Discovered 150010 - External Links Discovered (Web Application) :port 80/tcp Number of links: 38 https://bestproducts.buchkatalog.de/ https://bestproducts.buchkatalog.de/alleNonbookKategorien https://zeitfracht.de/ https://www.tiktok.com/search?q=booktok%20deutsch%22t%3D1690780005617 https://multimedia.knv.de/cover/03/15/91/0315919700001Z.jpg https://multimedia.knv.de/cover/29/99/79/2999792800001Z.jpg https://multimedia.knv.de/cover/43/90/85/4390859000001Z.jpg https://multimedia.knv.de/cover/81/03/56/8103562800001Z.jpg https://multimedia.knv.de/cover/87/86/53/8786535000001Z.jpg https://multimedia.knv.de/cover/90/62/29/9062290000001Z.jpg https://multimedia.knv.de/cover/95/09/53/9509538800001Z.jpg https://multimedia.knv.de/cover/95/66/07/9566074200001Z.jpg https://multimedia.knv.de/cover/96/22/02/9622029400001Z.jpg https://multimedia.knv.de/cover/96/22/38/9622385600001Z.jpg https://multimedia.knv.de/cover/96/39/53/9639532700001Z.jpg https://multimedia.knv.de/cover/96/98/95/9698950000001Z.jpg https://multimedia.knv.de/cover/97/04/17/9704173400001Z.jpg https://multimedia.knv.de/cover/97/04/17/9704176500001Z.jpg https://multimedia.knv.de/cover/97/05/26/9705262700001Z.jpg https://multimedia.knv.de/cover/97/06/81/9706810000001Z.jpg https://multimedia.knv.de/cover/97/13/97/9713977000001Z.jpg https://multimedia.knv.de/cover/97/22/15/9722159600001Z.jpg https://multimedia.knv.de/cover/97/29/16/9729169900001Z.jpg https://multimedia.knv.de/cover/97/47/02/9747026700001Z.jpg https://multimedia.knv.de/cover/97/47/59/9747597300001Z.jpg https://multimedia.knv.de/cover/97/54/36/9754369800001Z.jpg https://multimedia.knv.de/cover/97/59/37/9759375500001Z.jpg https://multimedia.knv.de/cover/97/74/22/9774220300001Z.jpg https://multimedia.knv.de/cover/97/74/81/9774811900001Z.jpg https://multimedia.knv.de/cover/97/75/10/9775103000001Z.jpg https://multimedia.knv.de/cover/97/75/13/9775138400001Z.jpg https://multimedia.knv.de/cover/97/75/15/9775157900001Z.jpg https://multimedia.knv.de/cover/97/76/32/9776320100001Z.jpg https://multimedia.knv.de/cover/98/23/75/9823754500001Z.jpg https://multimedia.knv.de/cover/98/25/29/9825296400001Z.jpg https://pixabay.com/de/users/photomix-company-1546875/ https://v91-prod.zeitfracht.digital/wcsstore/77740/favicon.ico https://v91-prod.zeitfracht.digital/wcsstore/77740/logos/shopLogo/BuchkatalogLogo20251.png	We confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely.
20.79.89.13 www.buchkatalog.de	Embedded links detected	External Links Discovered 150010 - External Links Discovered (Web Application) :port 443/tcp Number of links: 32 https://bestproducts.buchkatalog.de/	We confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely.

		https://bestproducts.buchkatalog.de/alleNonbookKategorien https://zeitfracht.de/ https://www.tiktok.com/search?q=booktok%20deutsch%22t%3D1690780005617 https://multimedia.knv.de/cover/03/15/91/0315919700001Z.jpg https://multimedia.knv.de/cover/29/99/79/2999792800001Z.jpg https://multimedia.knv.de/cover/43/90/85/4390859000001Z.jpg https://multimedia.knv.de/cover/81/03/56/8103562800001Z.jpg https://multimedia.knv.de/cover/87/86/53/8786535000001Z.jpg https://multimedia.knv.de/cover/90/62/29/9062290000001Z.jpg https://multimedia.knv.de/cover/95/09/53/9509538800001Z.jpg https://multimedia.knv.de/cover/95/66/07/9566074200001Z.jpg https://multimedia.knv.de/cover/96/22/38/9622385600001Z.jpg https://multimedia.knv.de/cover/96/39/53/9639532700001Z.jpg https://multimedia.knv.de/cover/96/98/95/9698950000001Z.jpg https://multimedia.knv.de/cover/97/04/17/9704173400001Z.jpg https://multimedia.knv.de/cover/97/04/17/9704176500001Z.jpg https://multimedia.knv.de/cover/97/05/26/9705262700001Z.jpg https://multimedia.knv.de/cover/97/13/97/9713977000001Z.jpg https://multimedia.knv.de/cover/97/22/15/9722159600001Z.jpg https://multimedia.knv.de/cover/97/29/16/9729169900001Z.jpg https://multimedia.knv.de/cover/97/47/59/9747597300001Z.jpg https://multimedia.knv.de/cover/97/54/36/9754369800001Z.jpg https://multimedia.knv.de/cover/97/75/10/9775103000001Z.jpg https://multimedia.knv.de/cover/97/75/13/9775138400001Z.jpg https://multimedia.knv.de/cover/97/75/15/9775157900001Z.jpg https://multimedia.knv.de/cover/97/76/32/9776320100001Z.jpg https://multimedia.knv.de/cover/98/23/75/9823754500001Z.jpg https://multimedia.knv.de/cover/98/25/29/9825296400001Z.jpg https://pixabay.com/de/users/photomix-company-1546875/ https://v91-prod.zeitfracht.digital/wcsstore/77740/favicon.ico https://v91-prod.zeitfracht.digital/wcsstore/77740/logos/shopLogo/BuchkatalogLogo20251.png	
20.79.89.13 www.buchkatalog.de	Web Servers detected	Predictable Resource Location Via Forced Browsing 150004 - Predictable Resource Location Via Forced Browsing (Web Application) :port 80/tcp https://www.buchkatalog.de/_next/data	The access to this file or directory is permitted. We're using the next.js Webframework for our frontend. The URL you're pointing out, is a response of this Interface and not a webserver directory browsing. /_next/data, is the cache from the frontend. This is all public data, accessible anyway or is loaded when you visit the store. No sensitive data can be found here. The cache must be public and is used, among other things, to improve performance/loading speed. This is common practice for sites that use Next.JS.
20.79.89.13 www.buchkatalog.de	Web Servers detected	Predictable Resource Location Via Forced Browsing 150004 - Predictable Resource Location Via Forced Browsing (Web Application) :port 443/tcp https://www.buchkatalog.de/_next/data	The access to this file or directory is permitted. We're using the next.js Webframework for our frontend. The URL you're pointing out, is a response of this Interface and not a webserver directory browsing. /_next/data, is the cache from the frontend. This is all public data, accessible anyway or is loaded when you visit the store. No sensitive data can be found here. The cache must be public and is used, among other things, to improve performance/loading speed. This is common practice for sites that use Next.JS.

Part 3c. Special Notes - Full Text

Note

Embedded links detected

Special Note to Scan Customer: Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.

Web Servers detected

Special Note to Scan Customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scan Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

20.79.89.13 / www.buchkatalog.de

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

20.79.89.13 / www.buchkatalog.de

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

Requires description for each IP Address/range/subnet, domain, URL

-

Please provide feedback on our services to the PCI Security Standards Council.
Download the ASV feedback form here: http://my-pci.usd.de/pub/english/asv_feedback_form_-_client.pdf

SUMMARY OF VULNERABILITIES

Vulnerabilities Total	61	Average Security Risk	4

Ordered by Severity

Severity	Confirmed	Potential	Information Gathered	Vulnerabilities Total
1	0	0	49	49
2	3	1	3	7
3	1	0	3	4
4	1	0	0	1
5	0	0	0	0
Total	5	1	55	61

Ordered by PCI Severity

PCI Severity	Confirmed	Potential	Vulnerabilities Total
Low	0	0	0
Medium	5	1	6
High	0	0	0
Total	5	1	6

APPENDIX

Overall Scan Duration

3 hours, 15 minutes, 30 seconds

Scan Start Time

09/24/2025 04:00:07

Option Profile

Payment Card Industry (PCI) Options

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities with a PCI status of FAIL caused the host to receive the PCI compliance status FAIL. These vulnerabilities and potential vulnerabilities must be remediated to pass the PCI compliance requirements. Vulnerabilities with a PCI status of PASS are vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

A PCI compliance status of PASS for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASS indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAIL for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAIL indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels

A vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.