CRASHTEST SECURITY

WEB VULNERABILITY SCANNING REPORT

Cofys

19 JAN 22 16:00 CET
https://demo.cofys.de

1 Overview

1.1 Vulnerability Overview

Based on our testing, we identified **6** vulnerabilities.

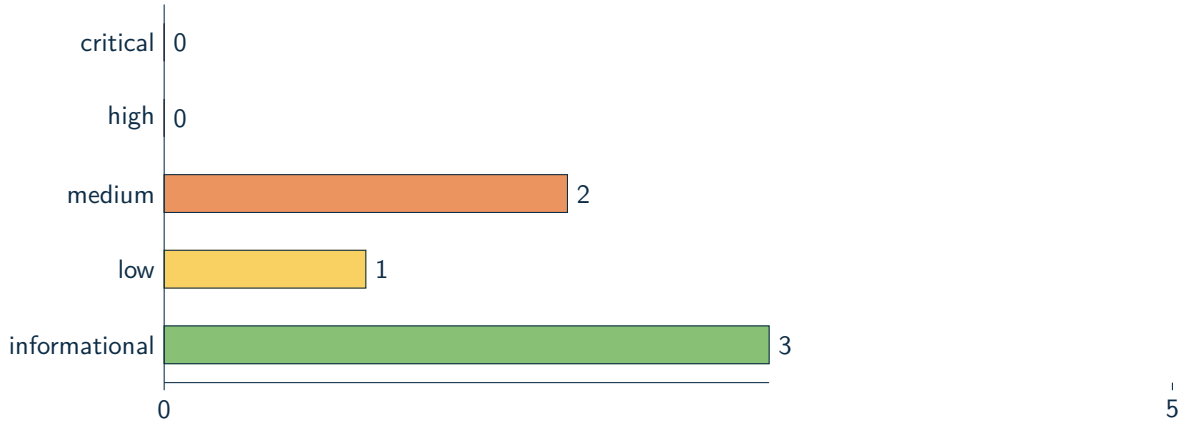


Figure 1.1: Total number of vulnerabilities for "Cofys"

STATE	DESCRIPTION	BASE SCORE
CRITICAL	These findings are very critical whilst posing an immediate threat. Fixing these issues should be the highest priority, regardless of any other issues.	**9 - 10**
HIGH	Findings in this category pose an immediate threat and should be fixed immediately.	**7 - 8.9**
MEDIUM	Medium findings may cause serious harm in combination with other security vulnerabilites. These findings should be considered during project planning and be fixed within short time.	**4 - 6.9**
LOW	Low severity findings do not impose an immediate threat. Such findings should be reviewed for their specific impact on the application and be fixed accordingly.	**0.1 - 3.9**
INFO	Informational findings do not pose any threat but have solely informational purpose.	**0**

1.2 Scanner Overview

During the scan, the Crashtest Security Suite was looking for the following kinds of vulnerabilities and security issues:

- ✓ Server Version Fingerprinting
- ✓ Web Application Version Fingerprinting
- ✓ CVE Comparison
- ✓ Heartbleed
- ✓ ROBOT
- ✓ BREACH
- ✓ BEAST
- ✓ Old SSL/TLS Version
- ✓ SSL/TLS Cipher Order
- ✓ SSL/TLS Perfect Forward Secrecy
- ✓ SSL/TLS Session Resumption
- ✓ SSL/TLS secure algorithm
- ✓ SSL/TLS key size
- ✓ SSL/TLS trust chain
- ✓ SSL/TLS expiration date
- ✓ SSL/TLS revocation (CRL, OCSP)
- ✓ SSL/TLS OCSP stapling
- ✓ Security Headers
- ✓ Content-Security-Policy headers
- ✓ Portscan
- ✓ Boolean-based blind SQL Injection
- ✓ Time-based blind SQL Injection
- ✓ Error-based SQL Injection
- ✓ UNION query-based SQL Injection
- ✓ Stacked queries SQL Injection
- ✓ Out-of-band SQL Injection
- ✓ Reflected Cross-site scripting (XSS)
- ✓ Stored Cross-site scripting (XSS)
- ✓ Cross-Site Request Forgery (CSRF)
- ✓ File Inclusion
- ✓ Directory Fuzzer
- ✓ File Fuzzer
- ✓ Command Injection
- ✓ XML External Entity Processing (XXE)

1.2.1 Status for executed Scanners

SCANNER	PERCENTAGE	STATUS
Portscan	100%	1 completed
SQL Injection	100%	5 completed
Transport Layer Security (TLS/SSL)	100%	1 completed
Command Injection	100%	5 completed
Multipage Crawler	100%	1 completed
Cross-Site Request Forgery (CSRF)	100%	5 completed
File Inclusion	100%	5 completed
Fingerprinting	0%	0 completed, 1 failed
Fuzzer	100%	1 completed
Cross-Site Scripting (XSS)	100%	5 completed
XML External Entity (XXE)	100%	5 completed
Deserialization	100%	5 completed
HTTP Header	100%	1 completed
	98%	**40 completed, 1 failed**

1.3 Findings Checklist

1.3.1 PORTSCAN

STATE	FINDING RESULT	NOTICED	FIXED
0.0	Found open port "443/tcp" with service name "nginx"	☐	☐
0.0	Found open port "80/tcp" with service name "nginx"	☐	☐

1.3.2 SSL/TLS

STATE	FINDING RESULT	NOTICED	FIXED
2.2	OCSP_stapling is not offered by the server.	☐	☐
0.0	DNS Certification Authority Authorization (CAA) Resource Record / RFC6844: Not offered	☐	☐

1.3.3 HTTPHEADER

STATE	FINDING RESULT	NOTICED	FIXED
6.5	The Content-Security-Policy header contains the 'unsafe' keyword. This weakens the security of the policy. This was found on URL https://demo.cofys.de	☐	☐
6.5	The Content-Security-Policy header allows loading resources from external URLs. This weakens the security of the policy. This was found on URL https://demo.cofys.de	☐	☐

Contents

2 Findings

2.1 SSL/TLS

2.1.1 What is this?

Transport Layer Security (TLS), more widely known by its predecessor Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission over the Internet. It encrypts the communication between server and client. The most obvious part of it is HTTPS, with which providers can secure all communications between their servers and web browsers. This ensures that valuable information like usernames, passwords and credit card information cannot be stolen by someone analyzing the network traffic. The "S" in HTTPS stands for SSL. For secure connection with HTTPS a certificate is needed. Those certificates offer different levels of security and have a fixed start- and expiration-date. To ensure a secure connection, webservers must use well configured certificates. With some misconfigured certificates it is possible to bypass the encryption, others may be blocked by web browsers because they are outdated or unknown.

2.1.2 OCSP Stapling

Severity

Base Score:	low (2.2/10)
Impact:	low (1.4/10)
Exploitability:	low (0.7/10)

All values are based on the Common Vulnerability Scoring System v3.

Description

OCSP Stapling is disabled on your server. Therefore, your certificate authority might track which users visit your site.

Finding

+ OCSP_stapling is not offered by the server.

How to fix

OSCP stapling can be enabled in the servers configuration (apache/nginx). For Let's Encrypt Certificates OCSP stapling can be activated during the creation of the certificate by adding the "–staple-oscp" parameter. More details on how to fix this problem can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/certificate-revocation

2.1.3 Missing SSL CAA record

Severity

Base Score:	informational (0/10)
Impact:	informational (0/10)
Exploitability:	low (3.9/10)

All values are based on the Common Vulnerability Scoring System v3.

Description

The domains DNS zone does not specify any Certification Authority Authorization (CAA) record. This means that all certificate authorities (CAs) are allowed to issue certificates for this domain. To decrease the risk of rogue certificates, append the CAA settings to the DNS records.

Finding

+ DNS Certification Authority Authorization (CAA) Resource Record / RFC6844: Not offered

How to fix

The domains DNS zone does not specify any Certification Authority Authorization (CAA) record. This means that all certificate authorities (CAs) are allowed to issue certificates for this domain. To decrease the risk of rogue certificates, the CAA setting needs to be added to the DNS records. More details on how to set the CAA setting can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/enable-missing-ssl-caa-record

2.2 HTTPHEADER

2.2.1 What is this?

When visiting a website the response from the server will include HTTP response headers. These headers tell the browser how to behave while the user is interacting with the website. Modern browsers support a variety of security headers, which are part of the HTTP response headers. This scanner will check if the recommended security headers are set and will also verify if the headers are configured in a secure way.

2.2.2 Content-Security-Policy Header

Severity

Base Score:	medium (6.5/10)
Impact:	low (2.5/10)
Exploitability:	low (3.9/10)

All values are based on the Common Vulnerability Scoring System v3.

Description

The Content-Security-Policy header tells the browser which domains are whitelisted to download further resources such as scripts, images or stylesheets from. This can prevent various XSS and other Cross-Site-Scripting attacks.

Finding

+ The Content-Security-Policy header contains the 'unsafe' keyword. This weakens the security of the policy. This was found on URL https://demo.cofys.de
+ The Content-Security-Policy header allows loading resources from external URLs. This weakens the security of the policy. This was found on URL https://demo.cofys.de

How to fix

Configure the Content-Security-Policy header in a way that it only allows loading resources from trusted resources such as 'self'. Do not include 'unsafe-eval' or 'unsafe-inline' in order to prevent direct injections into the website.

Recommendations

https://wiki.crashtest-security.com/enable-security-headers

2.3 PORTSCAN

2.3.1 What is this?

A port is a kind of door on the server that can be used to connect to a specific service. For a webserver the port 80 and port 443, which are for HTTP/HTTPS, are most likely open to serve the website to the users. Other ports should be closed if they are not needed for any service. The portscanner tests the webserver with a SYN scan for a wide range of possibly open ports and reports them back. If there are any other open ports except of port 80 and port 443, they should be blocked by the firewall if they are not needed.

2.3.2 Portscanner

Severity

Base Score:	informational (0/10)
Impact:	informational (0/10)
Exploitability:	informational (0/10)

All values are based on the Common Vulnerability Scoring System v3.

Description

Unneeded open ports on the webserver opens a large attack surface to a malicious user. This can be used to find unmaintained and possibly vulnerable network services that can be targeted.

Finding

+ Found open port "443/tcp" with service name "nginx"
+ Found open port "80/tcp" with service name "nginx"

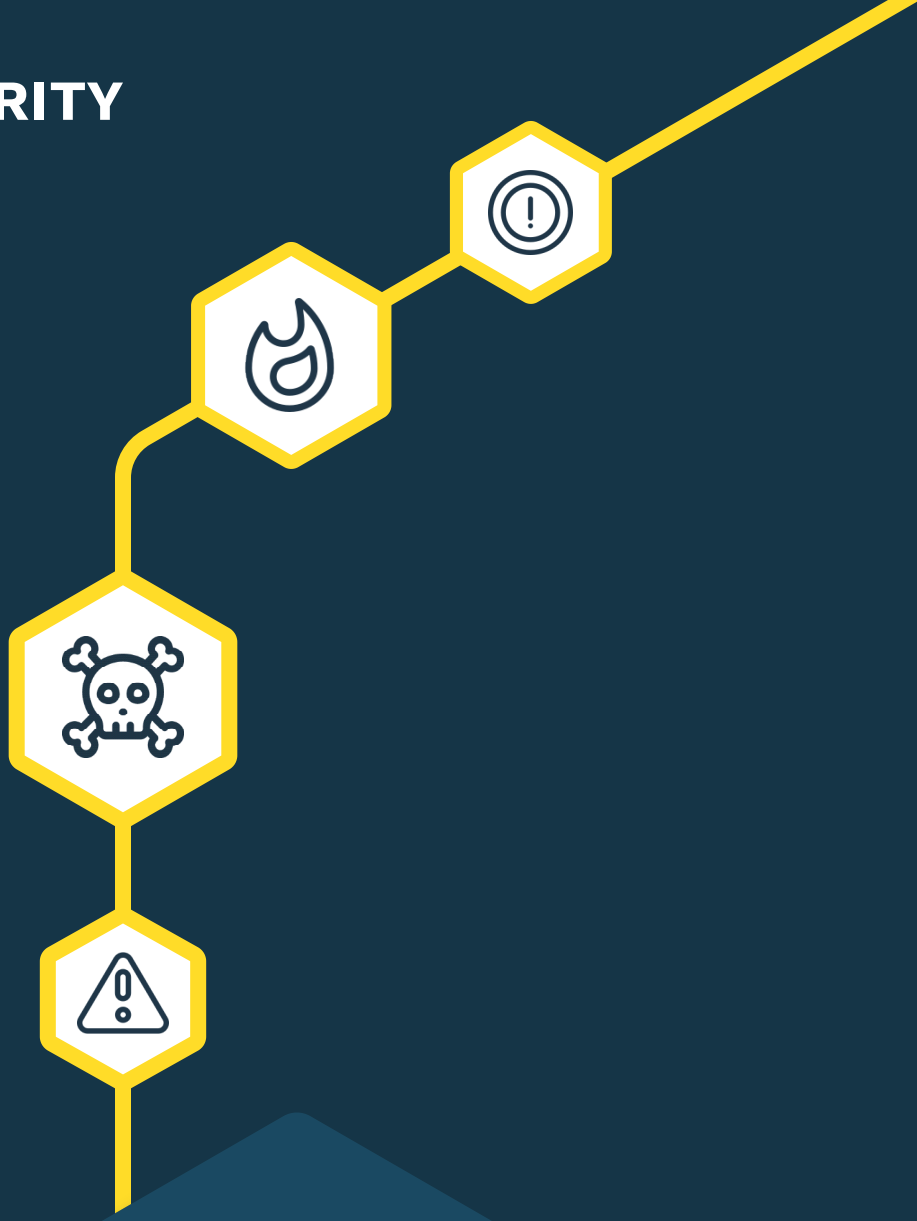
How to fix

Unnecessarily open ports can be closed by setting up a firewall and block connections to all ports except of those that are needed by the server. Furthermore services that are not needed should be uninstalled.

Recommendations

https://wiki.crashtest-security.com/insecure-network-services-open-port-scanner

CRASHTEST **SECURITY**



Crashtest Security is a German IT security company specialized in automated web application security testing. The fully automated penetration test lets developers discover vulnerabilities in real-time and supports the remediation through an integrated knowledge base.

CONTACT US:

Crashtest Security GmbH
Leopoldstr. 21
80802 München
+49 (0) 89 215 41 665