CRASHTEST SECURITY

WEB VULNERABILITY SCANNING REPORT

react applicatie pollstar front end

14 JAN 22 23:40 CET
https://wet-fish-39.loca.lt

1 Overview

1.1 Vulnerability Overview

Based on our testing, we identified **18** vulnerabilities.

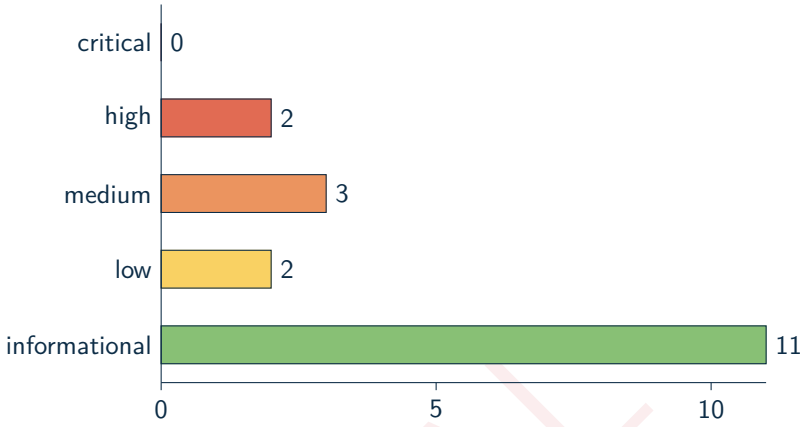


Figure 1.1: Total number of vulnerabilities for "react applicatie pollstar front end"

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

1.2.1 Used Scanners

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

1.2.2 Additional Scanners

The following scanners are also available in the Crashtest Security Suite but are only available for full scans. Please change the environment of your project to ”FULL SCAN” in order to scan against all vulnerabilites.

- ⌀ 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)

TRIAL

1.2.3 Status for executed Scanners

SCANNER	PERCENTAGE	STATUS
CVE	100%	1 completed
HTTP Header	0%	0 completed, 1 failed
Fingerprinting	100%	1 completed
Portscan	100%	1 completed
Transport Layer Security (TLS/SSL)	100%	1 completed
	80%	**4 completed, 1 failed**

TRIAL

1.3 Findings Checklist

1.3.1 SSL/TLS

STATE	FINDING RESULT	NOTICED	FIXED
0.0	DNS Certification Authority Authorization (CAA) Resource Record / RFC6844: Not offered	☐	☐
3.7	The server is configured to use average ciphers like SEED + 128+256 Bit CBC ciphers (AES, CAMELLIA and ARIA) which are deprecated	☐	☐
4.3	VULNERABLE – but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)	☐	☐
2.2	OCSP_stapling is not offered by the server.	☐	☐
8.2	TLS 1.1 is offered by the server. This version of TLS is deprecated. You should use TLS 1.2 or TLS 1.3	☐	☐
8.2	TLS 1.0 is offered by the server. This version of TLS is deprecated. You should use TLS 1.2 or TLS 1.3	☐	☐
4.3	BEAST TLS1: The BEAST attack leverages weakness in the cipher block chaining (CBC) which allows man in the middle attacks.	☐	☐

1.3.2 FINGERPRINTING

STATE	FINDING RESULT	NOTICED	FIXED
5.3	The webserver is running nginx 1.17.9 (There are no known CVE issues for this finding)	☐	☐

1.3.3 PORTSCAN

STATE	FINDING RESULT	NOTICED	FIXED
0.0	Found open port "32775/tcp"	☐	☐
0.0	Found open port "32785/tcp"	☐	☐
0.0	Found open port "34573/tcp"	☐	☐
0.0	Found open port "32779/tcp"	☐	☐
0.0	Found open port "443/tcp" with service name "nginx"	☐	☐
0.0	Found open port "80/tcp" with service name "nginx"	☐	☐
0.0	Found open port "32773/tcp"	☐	☐
0.0	Found open port "3000/tcp"	☐	☐
0.0	Found open port "22/tcp" with service name "OpenSSH"	☐	☐

STATE	FINDING RESULT	NOTICED	FIXED
0.0	Found open port "44501/tcp"	☐	☐

TRIAL

Contents

TRIAL

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 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.

TRIAL

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

2.1.3 SSL Cipherlist AVERAGE

Severity

Base Score:	low (3.7/10)
Impact:	low (1.4/10)
Exploitability:	low (2.2/10)

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

Description

The server is configured to support average Ciphers like SEED + 128+256 Bit CBC ciphers (AES, CAMELLIA and ARIA). This means, that an attacker can make use of an insecure SSL/TLS connection.

Finding

+ The server is configured to use average ciphers like SEED + 128+256 Bit CBC ciphers (AES, CAMELLIA and ARIA) which are deprecated

How to fix

The list of supported HTTPS ciphers includes insecure ciphers. This means, that an attacker can make use of in insecure SSL/TLS connection. In the SSL/TLS configuration, the allowed ciphers and their order should be set to match secure values. More details on how to set these values can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/secure-tls-configuration

TRIAL

2.1.4 SSL BEAST

Severity

Base Score:	medium (4.3/10)
Impact:	low (2.9/10)
Exploitability:	high (8.6/10)

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

Description

The server is vulnerable for BEAST (Browser Exploit Against SSL/TLS) attacks. By using weaknesses in cipher block chaining, an attacker can use a Man-In-The-Middle attacks to decrypt and obtain authentication tokens.

Finding

+ VULNERABLE – but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)

How to fix

BEAST attacks can be prevented by ensuring, that neither SSLv3 nor TLSv1 are used. More details on how to fix this problem can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/prevent-ssl-beast

TRIAL

2.1.5 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

TRIAL

2.1.6 SSL Protocol Version

Severity

Base Score:	high (8.2/10)
Impact:	medium (4.2/10)
Exploitability:	low (3.9/10)

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

Description

A SSL/TLS version offered by the server is outdated. The deprecated versions contain weak implementations that cannot be considered as secure anymore. Please use TLS 1.2 or TLS 1.3 instead.

Finding

+ TLS 1.1 is offered by the server. This version of TLS is deprecated. You should use TLS 1.2 or TLS 1.3
+ TLS 1.0 is offered by the server. This version of TLS is deprecated. You should use TLS 1.2 or TLS 1.3

How to fix

The webserver is using a deprecated SSL/TLS version and needs to be updated. The webserver needs to be configured to use strong and trusted certificates. In addition they need to be configured to use the newest version of SSL and TLS as well as strong cipher suites. More details on how to configure these certificates can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/disable-deprecated-ssl-protocol-versions

TRIAL

2.1.7 SSL Cipher Block Chaining TLS1

Severity

Base Score:	medium (4.3/10)
Impact:	low (2.9/10)
Exploitability:	high (8.6/10)

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

Description

The webserver is configured to allow connections encrypted with TLS V1 in Cipher Block Chaining Mode (CBC). Connections using this settings contain predictable information that allow an attacker to break the encryption using the BEAST attack.

Finding

+ BEAST TLS1: The BEAST attack leverages weakness in the cipher block chaining (CBC) which allows man in the middle attacks.

How to fix

The webserver needs to be configured to use strong and trusted certificates. In addition they need to be configured to use the newest version of SSL and TLS as well as strong cipher suites. More details on how to configure these certificates can be found in the knowledge database (see Recommendations)

Recommendations

https://wiki.crashtest-security.com/secure-tls-configuration

TRIAL

2.2 FINGERPRINTING

2.2.1 What is this?

The responses a server sends to its client often contain more information then necessary. This surplus of information makes it possible to draw conclusions about the servers software or used programming languages. It could reveal the version of the web application and the libraries in use. The analysis of these information is called fingerprinting. Based on fingerprinting, an attacker can get valuable input to plan and carry out his attack. Without it, an attacker is attacking blindly. Whenever a special version of a server or a web application is vulnerable for an attack, crawlers search the web for traces of this version and start an attack if they found one. So it is likely that someone gets attacked just because they leak these information, and therefore show that your application or server is vulnerable.

2.2.2 Fingerprint Web Server

Severity

Base Score:	medium (5.3/10)
Impact:	low (1.4/10)
Exploitability:	low (3.9/10)

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

Description

The webserver publicly provides information about itself such as the name or version. This opens attackers the possibility to look for exploits specifically targetting the webserver in its exact version.

TRIAL

Finding

+ The webserver is running nginx 1.17.9 (There are no known CVE issues for this finding)

How to fix

The amount of information a server is sharing can be set in its configuration files. Depending on the used webserver, the configuration file can be found on different locations (see Recommendations to find the exact location). In most cases it is sufficient to change one or two settings to avoid publishing unnecessary information. After saving the changes, it is recommended to restart or reload the webserver to activate the changes.

Recommendations

https://wiki.crashtest-security.com/server-version-fingerprinting

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.

TRIAL

Finding

+ Found open port "32775/tcp"
+ Found open port "32785/tcp"
+ Found open port "34573/tcp"
+ Found open port "32779/tcp"
+ Found open port "443/tcp" with service name "nginx"
+ Found open port "80/tcp" with service name "nginx"
+ Found open port "32773/tcp"
+ Found open port "3000/tcp"
+ Found open port "22/tcp" with service name "OpenSSH"
+ Found open port "44501/tcp"

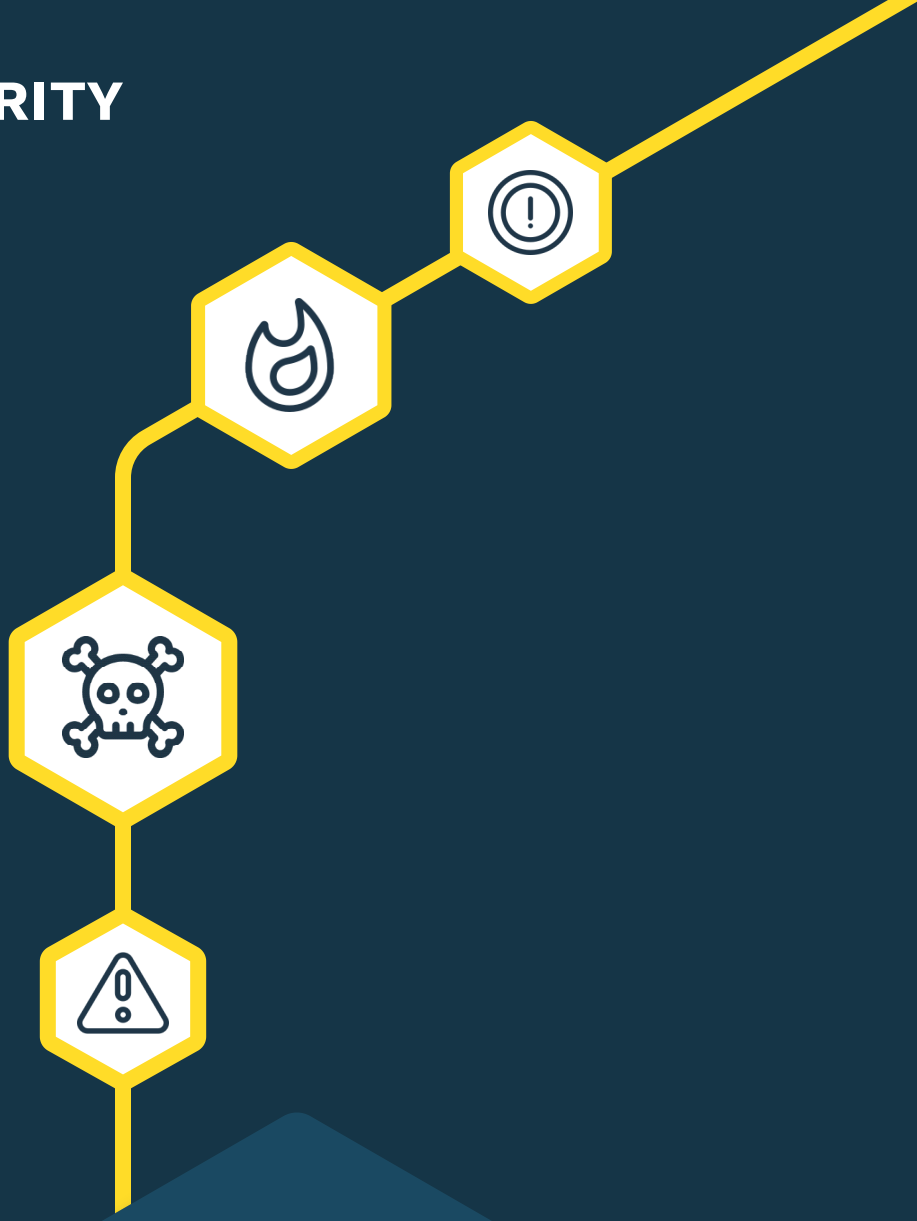
How to fix

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