CRASHTEST SECURITY

WEB VULNERABILITY SCANNING REPORT

LowExpectations

11 DEC 21 15:07 CET
https://peahi.be

1 Overview

1.1 Vulnerability Overview

Based on our testing, we identified **9** vulnerabilities.

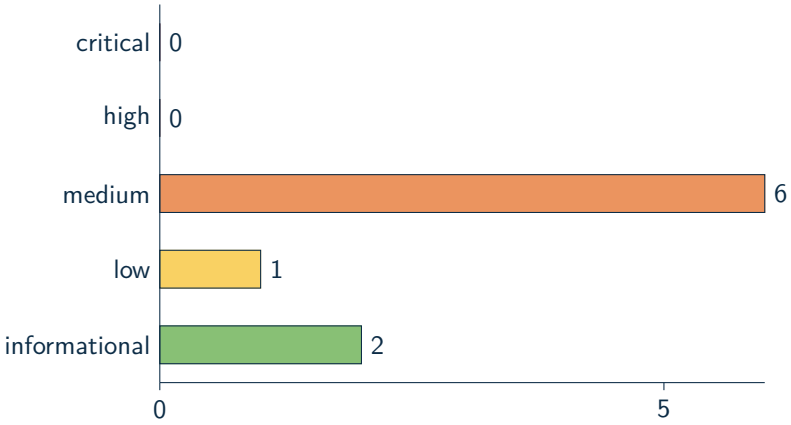


Figure 1.1: Total number of vulnerabilities for "LowExpectations"

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
CVE	100%	1 completed
Transport Layer Security (TLS/SSL)	100%	1 completed
Fuzzer	100%	1 completed
Portscan	100%	1 completed
Fingerprinting	100%	1 completed
Multipage Crawler	100%	1 completed
HTTP Header	100%	1 completed
	100%	**7 completed**

1.3 Findings Checklist

1.3.1 HTTPHEADER

STATE	FINDING RESULT	NOTICED	FIXED
4.3	The Referrer-Policy header is not set for URL https://peahi.be.	☐	☐
6.5	The X-Frame-Options header is not set for URL https://peahi.be.	☐	☐
6.5	The Content-Security-Policy header is not set for URL https://peahi.be.	☐	☐
4.3	The X-Content-Type-Options header is not set for URL https://peahi.be.	☐	☐

1.3.2 FINGERPRINTING

STATE	FINDING RESULT	NOTICED	FIXED
5.3	The webserver is running Microsoft-IIS 10.0 (There are no known CVE issues for this finding)	☐	☐

1.3.3 PORTSCAN

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

1.3.4 SSL/TLS

STATE	FINDING RESULT	NOTICED	FIXED
2.2	OCSP_stapling is not offered by the server.	☐	☐
5.8	OpenSSL handshake didn't succeed	☐	☐

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 SSL Secure Renegotiation

Severity

Base Score:	medium (5.8/10)
Impact:	medium (4.9/10)
Exploitability:	high (8.6/10)

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

Description

The renegotiation process of the SSL encryption is vulnerable. It allows two negotiations (one before the renegotiation, and one after) to be handled by different parties. This leaves the data vulnerable to Man-In-The-Middle attacks.

Finding

+ OpenSSL handshake didn't succeed

How to fix

Secure Renegotiation has been fixed in the newer versions of OpenSSL. OpenSSL can be updated using the preferred package manager of your system and update/upgrade OpenSSL.

Recommendations

https://wiki.crashtest-security.com/secure-ssl-renegotiation

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 Referrer-Policy Header

Severity

Base Score:	medium (4.3/10)
Impact:	low (1.4/10)
Exploitability:	low (2.8/10)

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

Description

The Referrer-Policy header defines how much information about the referrer is sent, when the user clicks on a link. A misconfiguration or missing header may leak sensitive information to third party websites that are visited by the click on a link.

Finding

+ The Referrer-Policy header is not set for URL https://peahi.be.

How to fix

Set the Referrer-Policy header to a secure value such as 'strict-origin-when-cross-origin' to overwrite the Referer header with your domain instead of the full path when clicking on external links and keep the Referer for internal links, but only when the connection is not downgraded from HTTPS to HTTP.

Recommendations

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

2.2.3 X-Frame-Options Header

Severity

Base Score:	medium (6.5/10)
Impact:	low (3.6/10)
Exploitability:	low (2.8/10)

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

Description

The X-Frame-Options header declares whether this site may be embedded as a frame into other websites. If this header is not configured correctly, your application can be embedded into third party websites which makes it vulnerable for clickjacking attacks.

Finding

+ The X-Frame-Options header is not set for URL https://peahi.be.

How to fix

Configure the X-Frame-Options header as 'deny' to prevent it to be embedded at all. The values 'sameorigin' or 'allow-from DOMAIN' can be used to allow it to be embedded on certain websites while forbidding embedding on other websites

Recommendations

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

2.2.4 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 is not set for URL https://peahi.be.

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

2.2.5 X-Content-Type-Options Header

Severity

Base Score:	medium (4.3/10)
Impact:	low (1.4/10)
Exploitability:	low (2.8/10)

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

Description

The X-Content-Type-Options prevents the browser from trying to detect MIME-types on downloaded files. This protects against attacks in cases where a malicious file is offered with an unsuspicious MIME-type.

Finding

+ The X-Content-Type-Options header is not set for URL https://peahi.be.

How to fix

Set the X-Content-Type-Options header to 'nosniff' in order to prevent the browser from detecting MIME-types based on file content.

Recommendations

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

2.3 FINGERPRINTING

2.3.1 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.

2.3.2 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.

Finding

+ The webserver is running Microsoft-IIS 10.0 (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

2.4 PORTSCAN

2.4.1 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.

2.4.2 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 "80/tcp" with service name "Amazon CloudFront httpd"
+ Found open port "443/tcp" with service name "Amazon CloudFront httpd"

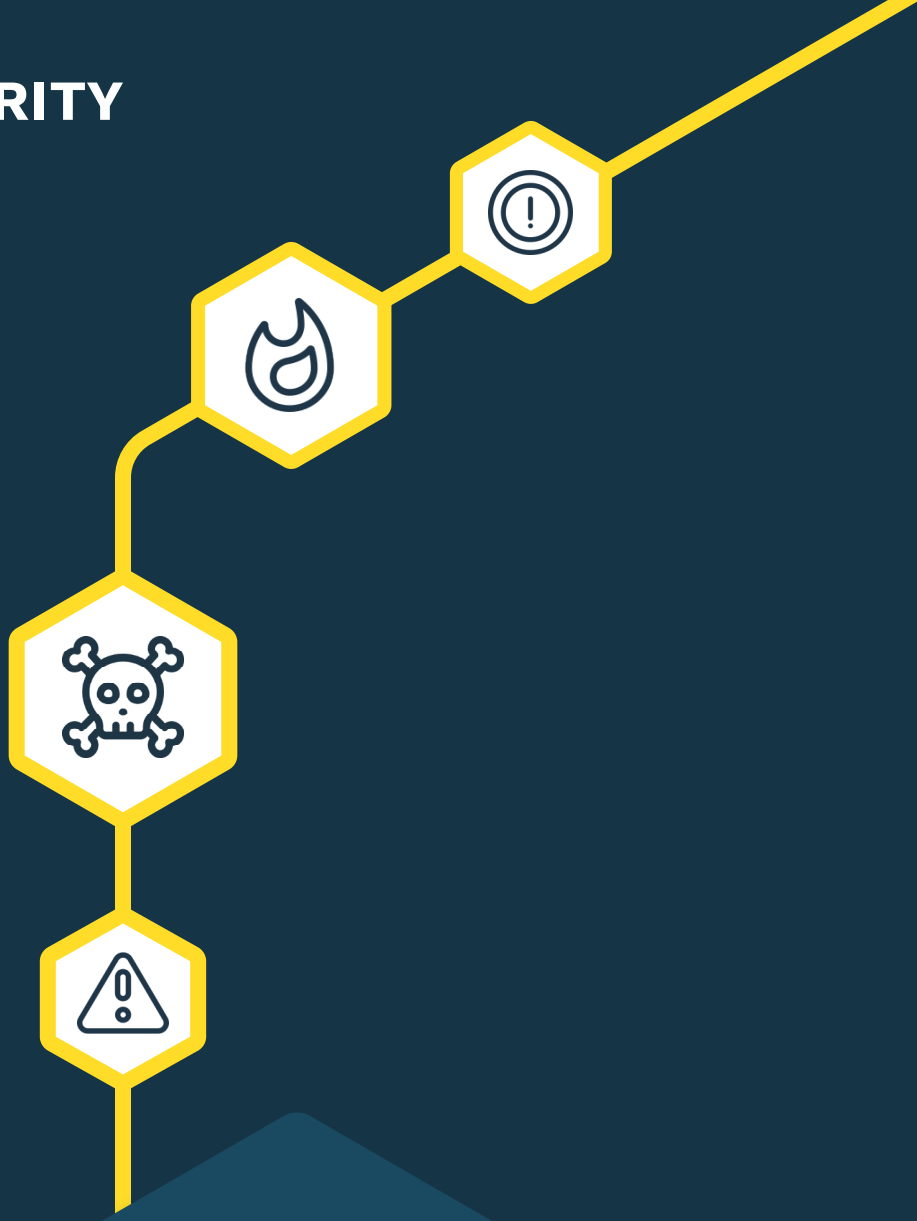
How to fix

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