SampleCompany Ltd

**Sample Pentest Engagement**

DRAFT - 1.0

23rd August 2021

**CONFIDENTIAL**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Issued** | **Reviewed** | **Date** |
| 0.1 | Pentest Tools |  | 23rd August 2021 |

Table of Contents

[1. Document control 3](#_Toc529192338)

[2. Introduction 4](#_Toc529192339)

[2.1 Background 4](#_Toc529192340)

[2.2 Objectives 4](#_Toc529192341)

[2.3 Scope 4](#_Toc529192342)

[2.4 Approach 4](#_Toc529192343)

[2.5 Methodology 4](#_Toc529192344)

[2.6 Disclaimer 4](#_Toc529192345)

[3 Executive summary 5](#_Toc529192346)

[4 Findings 6](#_Toc529192347)

[5 Addendum 8](#_Toc529192349)

[5.1 Tools and techniques 8](#_Toc529192350)

# Document control

**Distribution list**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Representing** |
| Pentest Tools | Security Consultant | PentestTools SRL |
|  |  |  |
|  |  |  |

**Revision history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Status** | **Peer Review** |
| 1.0 | 23rd August 2021 | Pentest Tools | Draft |  |
|  |  |  |  |  |

# Introduction

## Background

PentestTools SRL was contracted by SampleCompany Ltd to perform a penetration test on its Internet facing systems in order to determine the effectiveness of the implemented security measures.The test was agreed in the Contract No. SC340023 of 01 March 2020 between SampleCompany Ltd and PentestTools SRL.The fieldwork was completed between 15 April 2020 and 30 April 2020.

## Objectives

The objective of the penetration test was to evaluate the current state of the websites in scope from a security perspective and determine the risk of a successful attack by a malicious hacker or nefarious user from the Internet.

## Scope

The following systems belonging to SampleCompany Ltd were in scope:TargetDescriptionhttp://demo.pentest-tools.com

## Approach

The penetration test was performed in a "black box" manner, meaning that we did not have any prior information about the target systems.Our tests simulated an external threat (hacker, malicious user) located somewhere on the Internet who tried to find vulnerabilities in the target systems and exploit them in order to gain unauthorized access to sensitive information or affect the correct functionality of the systems.

## Methodology

All of our tests were performed by combining our professional experience with well known methodologies such as OWASP Top 10 and NIST 800-115.

## Disclaimer

Please note that it is impossible to test networks, information systems and people for every potential security vulnerability. This report does not form a guarantee that your assets are secure from all threats. The tests performed and their results are only from the point of view of PentestTools SRL.PentestTools SRL is unable to ensure or guarantee that your assets are completely safe from any form of attack, including those that are not known at the time of the penetration test.Furthermore, any changes to the tested systems may have an impact on their security level either in a negative or positive way.Our tests were performed in a time limited approach and our service was best-effort.

# Executive summary

The penetration test revealed several high risk vulnerabilities together with multiple medium and low risk issues. We recommend implementing the measures suggested for each finding in order to improve the security posture of the affected systems.This is a visual representation of the findings and their criticality levels:
The table below summarizes the findings identified in this penetration test:IDTargetFinding / Risk level / Verified4.1http://demo.pentest-tools.comVulnerabilities found for server-side softwareHigh✘Communication is not secureMedium✘Server software and technology foundLow✘Missing security header: Content-Security-PolicyLow✘Missing security header: Referrer-PolicyLow✘Missing security header: X-Content-Type-OptionsLow✘Missing security header: X-XSS-ProtectionLow✘Missing security header: X-Frame-OptionsLow✘✔ - manually verified finding

# Findings (by target)

## Target: http://demo.pentest-tools.com

### Vulnerabilities found for server-side software

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| High | http://demo.pentest-tools.com | Open |

#### Finding

Vulnerabilities found for server-side software

#### Evidence

Risk LevelCVSSCVESummaryExploitAffected softwareHigh7.5CVE-2017-3167In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap\_get\_basic\_auth\_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.N/Ahttp\_server 2.4.10High7.5CVE-2017-3169In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_ssl may dereference a NULL pointer when third-party modules call ap\_hook\_process\_connection() during an HTTP request to an HTTPS port.N/Ahttp\_server 2.4.10High7.5CVE-2017-7668The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap\_find\_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap\_find\_token() to return an incorrect value.N/Ahttp\_server 2.4.10High7.5CVE-2017-7679In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.N/Ahttp\_server 2.4.10High7.5CVE-2021-26691In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflowN/Ahttp\_server 2.4.10

#### Risk

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

#### Recommendation

We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-1026OWASP Top 10 - 2013A9 - Using Components with Known VulnerabilitiesOWASP Top 10 - 2017A9 - Using Components with Known VulnerabilitiesCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Communication is not secure

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Medium | http://demo.pentest-tools.com | Open |

#### Finding

Communication is not secure

#### Evidence

URLEvidencehttp://demo.pentest-tools.comCommunication is made over unsecure, unencrypted HTTP.

#### Risk

The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

#### Recommendation

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-311OWASP Top 10 - 2013A6 - Sensitive Data ExposureOWASP Top 10 - 2017A3 - Sensitive Data ExposureCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Server software and technology found

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Server software and technology found

#### Evidence

Software / VersionCategoryDebianOperating SystemsApache 2.4.10Web Servers

#### Risk

An attacker could use this information to mount specific attacks against the identified software type and version.

#### Recommendation

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc. More information about this issue:https://owasp.org/www-project-web-security-testing-guide/stable/4-Web\_Application\_Security\_Testing/01-Information\_Gathering/02-Fingerprint\_Web\_Server.html.

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)N/AOWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Missing security header: Content-Security-Policy

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Missing security header: Content-Security-Policy

#### Evidence

URLEvidencehttp://demo.pentest-tools.comResponse headers do not include the HTTP Content-Security-Policy security header

#### Risk

The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

#### Recommendation

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.Read more about CSP:https://cheatsheetseries.owasp.org/cheatsheets/Content\_Security\_Policy\_Cheat\_Sheet.htmlhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-693OWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Missing security header: Referrer-Policy

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Missing security header: Referrer-Policy

#### Evidence

URLEvidencehttp://demo.pentest-tools.comResponse headers do not include the Referrer-Policy HTTP security header

#### Risk

The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the Referer header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

#### Recommendation

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value no-referrer of this header instructs the browser to omit the Referer header entirely.Read more:https://developer.mozilla.org/en-US/docs/Web/Security/Referer\_header:\_privacy\_and\_security\_concerns

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-693OWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Missing security header: X-Content-Type-Options

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Missing security header: X-Content-Type-Options

#### Evidence

URLEvidencehttp://demo.pentest-tools.comResponse headers do not include the X-Content-Type-Options HTTP security header

#### Risk

The HTTP header X-Content-Type-Options is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

#### Recommendation

We recommend setting the X-Content-Type-Options header such as X-Content-Type-Options: nosniff.More information about this issue:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options.

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-693OWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Missing security header: X-XSS-Protection

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Missing security header: X-XSS-Protection

#### Evidence

URLEvidencehttp://demo.pentest-tools.comResponse headers do not include the HTTP X-XSS-Protection security header

#### Risk

The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

#### Recommendation

We recommend setting the X-XSS-Protection header to X-XSS-Protection: 1; mode=block.More information about this issue:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-693OWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Missing security header: X-Frame-Options

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Low | http://demo.pentest-tools.com | Open |

#### Finding

Missing security header: X-Frame-Options

#### Evidence

URLEvidencehttp://demo.pentest-tools.comResponse headers do not include the HTTP X-Frame-Options security header

#### Risk

Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:https://owasp.org/www-community/attacks/Clickjacking

#### Recommendation

We recommend you to add the X-Frame-Options HTTP header with the values DENY or SAMEORIGIN to every page that you want to be protected against Clickjacking attacks.More information about this issue:https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\_Defense\_Cheat\_Sheet.html

#### Classification

CategoryID / ValueCWE (Common Weakness Enumeration)CWE-693OWASP Top 10 - 2013A5 - Security MisconfigurationOWASP Top 10 - 2017A6 - Security MisconfigurationCVSS ScoreN/ACVE (Common Vulnerability and Exposures)N/A

### Nothing was found for HttpOnly flag of cookie.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for HttpOnly flag of cookie.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Website is accessible.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Website is accessible.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for enabled HTTP debug methods

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for enabled HTTP debug methods

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for client access policies.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for client access policies.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for Secure flag of cookie.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for Secure flag of cookie.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for robots.txt file.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for robots.txt file.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for missing HTTP header - Strict-Transport-Security.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for missing HTTP header - Strict-Transport-Security.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for domain too loose set for cookies.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for domain too loose set for cookies.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for directory listing.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for directory listing.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

### Nothing was found for use of untrusted certificates.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Affected target** | **Status** |
| Info | http://demo.pentest-tools.com | Open |

#### Finding

Nothing was found for use of untrusted certificates.

#### Evidence

#### Risk

#### Recommendation

#### Classification

No classification for this finding

# Addendum

## Tools and techniques

This is a list of tools used during the penetration test:

ToolTargetStart TimeWebsite Scannerhttp://demo.pentest-tools.com2021-08-23 15:02:28 UTC+03