Web Application and Server Penetration Testing
By Petar Antonic

April 7th 2020

Prepared For:

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

Contents

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

1 Executive Summary

A penetration testing of a "https://www.draw.io/" web application and server was conducted. The testing was conducted externally over the Internet from the perspective of both unauthenticated and authenticated user.

The application testing consisted of the following activities:

- Research and information gathering
- Automated and manual testing
- Verification and validation of findings
- Reporting

To conduct the tests, scans of the Web application(s) and Web server(s) was performed. The initial testing began on February 6th 2020, and progressed through April 7th 2020.

The findings revealed during testing and presented in this report should be further validated if necessary.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

2 Project scope & Methodology

The scope of the application assessment focused entirely on:

- Black box penetration testing of web application and its supported infrastructure
- Gray box penetration testing of web application and its supported infrastructure

Constraints and Limitations

The tests were conducted externally from Internet and the result(s) / finding(s) made are highly subjective to "https://www.draw.io/ and any discovered assets visibility (in terms of perimeter access rules) and availability at that given point of time.

Manual and Automated Testing

The testing of the server and application consisted of using commercial & open source/freeware tools. The testing methods included looking for known vulnerabilities in the application as well as using simulated attacks (excluding Denial of Service attacks) to find weaknesses. Some of the discovered vulnerabilities were analysed further using manual procedures.

Vulnerability Research & Analysis

Using the information gathered by the automated and manual testing, vulnerabilities were researched using commercial databases and Internet sites containing relevant vulnerability data.

Application and Server Information Independent research was performed to obtain public information about the application and Web server. In the process, certificate information, all supported ciphers, open and closed ports, and information on the Web server was acquired.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

Open / Closed Ports

```
Nmap scan report for www.draw.io (104.22.57.156)
Host is up (0.010s latency).
Other addresses for www.draw.io (not scanned): 104.22.56.156
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          cloudflare
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http-proxy    cloudflare
8443/tcp open  ssl/https-alt cloudflare
```

```
Nmap scan report for 138.68.108.119
Host is up.
All 1000 scanned ports on 138.68.108.119 are filtered
```

```
Nmap scan report for exp.draw.io (199.38.85.80)
Host is up (0.14s latency).
Other addresses for exp.draw.io (not scanned): 162.255.23.33 162.253.133.20
rDNS record for 199.38.85.80: static.199.38.85.80.macminivault.com
Not shown: 994 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.9 (protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http    Apache httpd
179/tcp  filtered bgp
443/tcp  open     ssl/ssl Apache httpd (SSL-only mode)
8000/tcp open     http    Node.js Express framework
```

```
Nmap scan report for 178.62.223.29
Host is up (0.040s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE       VERSION
22/tcp   open     ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http          Apache httpd 2.4.29
443/tcp  open     ssl/http      Apache httpd 2.4.29 ((Ubuntu))
8090/tcp open     opsmessaging?
```

Only main domain is added to the list, that is behind Cloudflare, rest of the subdomains are excluded.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

3 OWASP TOP 10 2017 Mapping

This section maps the application's security posture to OWASP TOP 10 2017 vulnerabilities. Below table illustrates the same:

c	Web Application Security Risks	Status	Responsible Finding
A.1	Injection	COMPLIANT	
A.2	Broken Authentication	COMPLIANT	
A.3	Sensitive Data Exposure	NON-COMPLIANT	5.1, 5.7
A.4	XML External Entities (XXE)	COMPLIANT	
A.5	Broken Access Control	COMPLIANT	
A.6	Security Misconfiguration	NON-COMPLIANT	5.2, 5.4 5.5, 5.6
A.7	Cross-Site Scripting (XSS)	COMPLIANT	
A.8	Insecure Deserialization	COMPLIANT	
A.9	Using Components with Known Vulnerabilities	NON-COMPLIANT	5.3
A.10	Insufficient Logging & Monitoring	COMPLIANT	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

4 Security Roadmap

This section contains findings, risks, and recommendations resulting from automated and manual testing. The scans were performed with minimal background information. There was no detailed interaction with the programmers who developed the application.

The findings are presented in order of criticality to assist in the remediation assessment.

Graphical Representation of Vulnerabilities

The following table is the abstract of findings, which summaries the overall risks identified during the pen test. For details, refer to section "Technical Findings – Details".

Total of **07** unique risks were identified during the test.

Target Application	Total Vulnerabilities		
	HIGH	MEDIUM	LOW
https://www.draw.io/	00	02	00
https://support.draw.io/	01	02	01
https://about.draw.io/	00	02	00
https://exp.draw.io/	00	02	00
https://app.draw.io/	00	02	00
https://app.diagrams.net/	00	03	00
https://178.62.223.29/	01	03	01

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5 Technical Findings – Details

The security assessment found 01 high, 04 medium risk and 01 low risk vulnerabilities.

No.	Finding	Criticality Rating
5.1	Disclosure of Origin IP	**HIGH**
5.2	Cleartext Submission of Password	**HIGH**
5.3	Weak Cipher Suites	**MEDIUM**
5.4	Content Sniffing not disabled	**MEDIUM**
5.5	Browser Cross Site Scripting filter missing	**MEDIUM**
5.6	Strict Transport Security not enforced	**MEDIUM**
5.7	Information Disclosure	**LOW**

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.1 Disclosure of Origin IP — Criticality:HIGH

Details: CloudFlare is CDN(content delivery network) that is used for faster content delivery and security (against DDOS as well as web application firewall). Cloudflare acts as a proxy between the server and the client, filtering any malicious incoming traffic. It is possible to obtain origin IP of domain 'support.draw.io'.

Affected host:

https://support.draw.io/

Proof of Concept:

```
A direct-connect IP address was found: draw.io 178.62.223.29
NETHERLANDS

An attempt to fetch a page from this IP was unsuccessful.

Previous lookups for this domain:
2017-12-07: draw.io 178.62.223.29 NETHERLANDS
2017-12-07: draw.io 138.68.108.119 UNITED STATES
```

Figure 1 showing origin IP related to 'draw.io' DNS records

Risk: Malicious actor can bypass Cloudflare's security mechanisms and send requests directly to the server in question.
Recommendation: Edit the DNS records to resolve this.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.2 Cleartext Submission of Password — Criticality:HIGH

Details: IP Address 178.62.223.29 is IP address of support.draw.io

As shown on page 5, this IP address has a hosted application on port 8090 that works over plain HTTP protocol. Any data transmit via this channel is insecure and can be extracted in clear-text.

Affected host:

https://support.draw.io/

Proof of Concept:

```
POST /dologin.action HTTP/1.1
Host: 178.62.223.29:8090
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3
Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://178.62.223.29:8090/login.action?language=et_EE
Content-Type: application/x-www-form-urlencoded
Content-Length: 150

os_username=testa&os_password=testa&os_cookie=
a'a%5c'b%22c%3e%3f%3e%25%7d%7d%25%25%3ec%3c[[%3f$%7b%7b%25%7d%7dcake%5c&login=Logi+sisse&os_destination=
```

Figure 2 showing cleartext submition of credentials

Risk: This issue allows malicious user to exploit users of the application via man-in-the-middle attacks (presence on the same network).

Recommendation: Use HTTPS TLS v1.3 for this channel.

Reference: https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.3 Old versions of TLS supported — Criticality:MEDIUM

Details: Older versions of TLS are known to have security issues and are deprecated.

Affected host:

https://178.62.223.29:443/

Proof of Concept:

```
Testing SSL server 178.62.223.29 on port 443 using SNI name
178.62.223.29

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled
```

Figure 3 Cipher suites used for HTTPS connections

Risk: Malicious actor that is well positioned on victims network can extract clear-text data from seemingly secured channel.

Recommendation: Use only TLS v1.3, also check cipher suites for current standards.

Reference: https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.4 Content Sniffing not disabled — Criticality:MEDIUM

Details: There was no "X-Content-Type-Options" HTTP header with the value *nosniff* set in the response.

Affected hosts:

https://support.draw.io/
https://www.draw.io/
https://178.62.223.29:8090/

Risk: The lack of this header causes that certain browsers, try to determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks.

Recommendation: Set the following HTTP header at least in all responses which contain user input:

```
X-Content-Type-Options: nosniff
```

Reference: https://owasp.org/www-project-secure-headers/

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.5 Browser Cross Site Scripting filter missing — Criticality:MEDIUM

Details: No X-XSS-Protection header was set in the response.

Affected hosts:

https://support.draw.io/
https://www.draw.io/
https://178.62.223.29:8090/

Risk: This means that the browser uses default behavior that detection of a cross-site scripting attack never prevents rendering.

Recommendation: The following header should be set:

```
X-XSS-Protection: 1; mode=block
```

Reference: https://owasp.org/www-project-secure-headers/

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.6 Strict Transport Security not enforced — Criticality:MEDIUM

Details: The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection.

https://app.diagrams.net/

Risk: To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

Recommendation: The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

Reference: HTTP Strict Transport Security

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.

5.7 Information Disclosure — Criticality:LOW

Details: Sensitive information in terms of exact version of the technology used is leaked via servers HTTP banners as show on page #5 of this report. In addition to this, sensitive information is leaked via error response.

Error code: 400

https://178.62.223.29:8090/

Proof of Concept:

Figure 4 Disclosure of Apache Tomcat version

Risk: Malicious user can use this information to search the web for publicly available exploits or purchase 0day exploits if any available on black market.

Recommendation: Customize errors not to disclose sensitive information.

Reference: https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT
This document contains information that is confidential and proprietary to the subject of the Penetration Testing Report. The document and the information contained within it and its attachment(s) as applicable may be used by the subject of the Assessment Report for its intended purpose. All information remains the property of its respective owner and any other use or disclosure of this information requires prior written approval.