Precise Testing Solution Pvt. Ltd

Security Testing Report

www.precisetestingsolution.com

PRECISE
Testing Solution

To,

Maharashtra Knowledge Corporation Ltd.

MKCL Seawood BO, Plot No. 30, Sector 42-A, Nerul,Navi Mumbai 400706 , Maharashtra, INDIA.

B-5, Second Floor Sector 64 Noida(UP)201301 | Precise Testing Solution Pvt. Ltd
M- +91-8447088848 USA- +1 -7183128801

Contents

Precise Testing Solution Pvt. Ltd (PTS)

Precise Testing **Solution** Pvt. Ltd is a private limited company based in Noida, Uttar Pradesh, India.

Precise Testing **Solution** is working towards becoming a leading quality services provider for Testing and QC/QA for all types of domains and applications.

Introduction

PTS is committed to deliver best-in-class quality control assurance and software testing **Solution**s to our clients. Using proven testing methodologies and industry's best practices. We help companies to optimize the quality, performance and availability of their applications. The wide range of testing **Solution**s that we offer, give organizations a fast start in developing and deploying software of the highest quality while reducing the risks, costs and time associated with it.

PTS is **ISO 9001:2008** and **27001:2013** Certified and has already served **400+** customers and having completed**40,000** hours of testing. We have discovered more than **2,40,000** bugs in various applications.

We are empaneled vendor of **STQC government of India** and we are under process of emplacement of Indian Computer Emergency Response Team (ICERT).We have certified, specialized and experienced testers for all types of testing. We have close to 100% project success ratio and 60% returned customer.

Our focused customers are Government and Defence.

Control Page

Reporter ID	PTS-STQC-2021/PT/AS-006
Report Type	Final Report
Date	15/01/2021
Document Type	Audit Report
Client Name	Maharashtra Knowledge Corporation Ltd.
Client Address	MKCL Seawood BO, Plot No. 30, Sector 42-A, Nerul,Navi Mumbai 400706 , Maharashtra, INDIA.
Type of Audit	Security Audit
Project Name/ID	Assam Skill Development Mission
Test Environment	https://sdmms-stqc.mkcl.org/
Production Environment	https://www.skillmissionassam.org/
Test Method	Manual
Reference Document/Base Document	OWASP 10 Vulnerabilities
Audit Start Date	15/01/2021
Audit End Date	16/03/2021
Compliance Date	17/03/2021
Prepared By	Bhim Bhadur
Review By	Mr. Vikash Kumar
Approve By	Mr.Vikash Kumar

Disclaimer

This report has been issued based upon our work at during 15-01-2021 to 16-03-2021 and compliance on 17-03-2021. The scope of work was to conduct functional audit.

The report prepared for the period prescribed in the report as an account of work allocated by Government of Assam Skill Development Mission to Precise Testing Solution Pvt. *Ltd. (herein after referred as ''PTS'')*. Though all efforts have been made to ensure the accuracy of the content in this Report, the same should not be construed as a statement of law, Policy or used for any legal purposes. Assam Skill Development Mission advised to verify/check any information with the relevant Authorities(s), and to obtain any appropriate professional advice before acting on the information provided in the report.

Links in the form of recommendation as mentioned in the report if any, are provided for reference and further reading only. PTS is not responsible for the contents or reliability of linked websites and does not necessarily endorse the view expressed within them.

Details mentioned in the report to be considered as *"Confidential"* and caution to maintain the material to be accurately and to be used in a derogatory manner or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledge. The terms and conditions shall be governed by and construed in accordance with the Indian laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India Noida.

Document Information

Project Name	Assam Skill Development Mission
Product Version No	Application Version : 1.0 MD5 Hash : f30eea2626c12429e1058f428c463256
Audit Period	15/01/2021 to 16/03/2021
Audit completed Date	17/March/2021
Report Prepared By	Bhim Bhadur
Reviewed By	Mr. Vikash Kumar
Final Report	17/03/2021
Review Date	16/03/2021
Document Owner	Maharashtra Knowledge Corporation Ltd. MKCL Seawood BO, Plot No. 30, Sector 42-A, Nerul, Navi Mumbai 400706 , Maharashtra, INDIA.

Intended Recipient

S.N	Intended Recipient
1	Maharashtra Knowledge Corporation Ltd. MKCL Seawood BO, Plot No. 30, Sector 42-A, Nerul Navi Mumbai 400706 , Maharashtra, INDIA.

Restriction of Circulation

For Internal Circulation Only

Audit Team

S.N	Name	Project Role	Email Address
1	Vikash Kumar	Delivery In Charge	info@precisetestingsolution.com
2	Gaurav Kumar	Audit Executive	Gaurav.kumar@precisetestingsolution.com
3	BhimBhadur	Audit Executive	Bhim@precisetestingsolution.com

Coordinating Team Detail

S.N	Name	Email id
1	Anand Kulkarni Program Coordinator	anandku@mkcl.org

Objective of Audit

Security Testing For Skill Development Mission Management Website.

Scope of Audit

www.mkcl.org

3. **Scope of work**: You are expected to carry out an assessment on basis of below scope:

No	Question	Application Details 1
1	What is the application used for? Anything special about the architecture? (eg. Tiered application, Citrix based, Wireless GPRS, Mainframe, Embedded System)	Tiered Application
2	What are the different types of user roles for the application?	Department User 1,Department User 2,Department User 3,Assessing Body, Assessing Body User, TP ,SPMU ,Department Executive, Sub Department, Sub Department User, Department Executive 2,File Lead Supervisor, PM,APM,MD,AMD,RM Reports, System Admin, Organization ,Knowledge Partner, Regional Manager, Learner, applicant, Joint Venture Administrator, Authorised Learning Centre, Authorised Learning Centre, Accountant, RLC,LLC
	Are there different privileges/roles for users in the application?	Yes
3	What sensitive data is handled by the application?	User password, mobile number, adhaar card, Pan card, Voter Id
	Which users handle this data?	System User
4	URL of the application for Development and/or	Will be informed once setup is ready
	Test and/or Staging and/or Production Server	
5	No. of business/application modules	26
6	Technologies the application makes use of (e.g. J2EE / DOT NET / PHP / WebSphere etc.), python	Backend : Node JS, Java for Reporting Front end: Angular JS Database : MYSQL
7	Approximate number of pages in the application.	400-500 Pages
8	No. of dynamic pages in the application.	400-500 Pages

Approach &Methodology

1. **Document Referred**
   OWASP top 10 Venerability and OWASP top 10 checklist
2. **Standard & Guideline**
   International Professional Practices framework (PPF)

3. **Methodology**
   - Understanding the requirement
   - Preparation of checklist/Test Case for sample audit bases on requirement, understanding of documents under reference, and auditor's judgment

- Verification of parameters
- Execution of test cases for assumed output and making note of the exception
- Process verification by interview and other supporting document
- Observation and noting
- Discussion/Interaction with Maharashtra Knowledge Corporation Ltd.
- Conclusion

Introduction

Assam Skill Development Mission is registered under Society Act in 2015 and is working under newly created Skill, Employment & Entrepreneurship Department, Govt. of Assam with the visions of capacity building of unemployed youth and to deliver quality skill training leading to meaningful employment to stimulate economy of the state. The Mission started its functioning from January, 2017 as:

- An apex body of all skill initiatives in the state to achieve skilling target of 1.50 lakhs youths in a year.
- To provide quality skill training for gainful employment of educated unemployed youth.
- To encourage development of entrepreneurs in different sectors.
- To implement central sponsored skilling schemes in the state.

Risk Classification

This document is an exception-bases report highlighting the control weakness and potential improvement area with risk levels assigned. The risk level assigned are as follows depending on the impact and occurrence. The risk are assigned as per below table.

Control Importance	Impact	
Metrics	**Severity**	**Priority**
Critical	HIGH	HIGH
Medium	LOW	HIGH
Medium	HIGH	LOW
Low/Minor	LOW	LOW

Audit Environment

The Assam Skill Development Mission to undertake security Audit of Assam Skill Development Mission V1.0 application with a view to check the resilience of the application.

We have tested application as per defined OWASP top 10 Venerability and OWASP top 10 checklist.

Observation Summery

S.N	Risk Category (Functional & Security Testing)	No. Of Observation	Open Observation
1	High	1	0
2	Medium	8	0
3	Low /Minor	8	0
	Total	17	

Conclusion

We have closely worked with the team Maharashtra Knowledge Corporation Ltd. and checked each and every application Functionality related with Assam Skill Development Mission. We have performed the evaluation of functionality, system process and domain application of Assam Skill Development Mission software, which includes integrity and confidentiality of information and further ensure compliance to regulatory and corporate security. We have covered all the scope of work, which also includes in SRS of We have checked the functionality as per the provided process as per prevailing standard available as on date.

During testing of Assam Skill Development Mission V 1.0, we have found some bugs which is mention in above “Observation Summery” and all bugs are fixed by development team, now application functional flow working fine and don’t have any major bugs.

Following functionality were audited

Application audit for Security Standard
Implementation carried out as per User manual and defined standard
Verification of the reports provided in the application including Number of generated, updated, downloaded etc.

Assam Skill Development Mission Security Testing Environment

S.N	Main Functionality	Environment
1	https://sdmms-stqc.mkcl.org/	DEMO

Security Testing Observation:

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about the true software security risks.

We will test based on OWASP recommendations.

BUG SEVERITY: HIGH

BUG ID 1: SQL Injection

Severity: High

Description: Due to the requirement for dynamic content of today's web applications, many rely on a database backend to store data that will be called upon and processed by the web application (or other programs). Web applications retrieve data from the database by using Structured Query Language (SQL) queries.

Reference Id(s):

- OWASP Top 10 – A1:2017-Injection
- CWE-89

Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/#/candidateSearchFacility/14/166

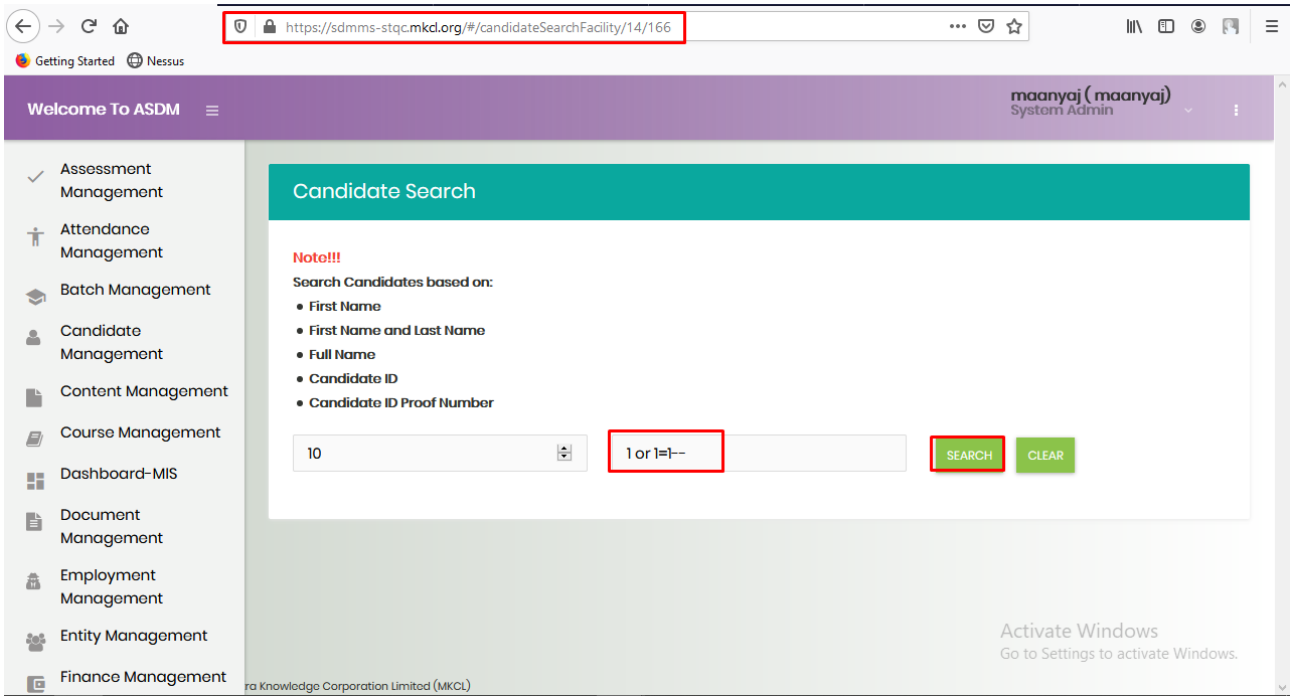
Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

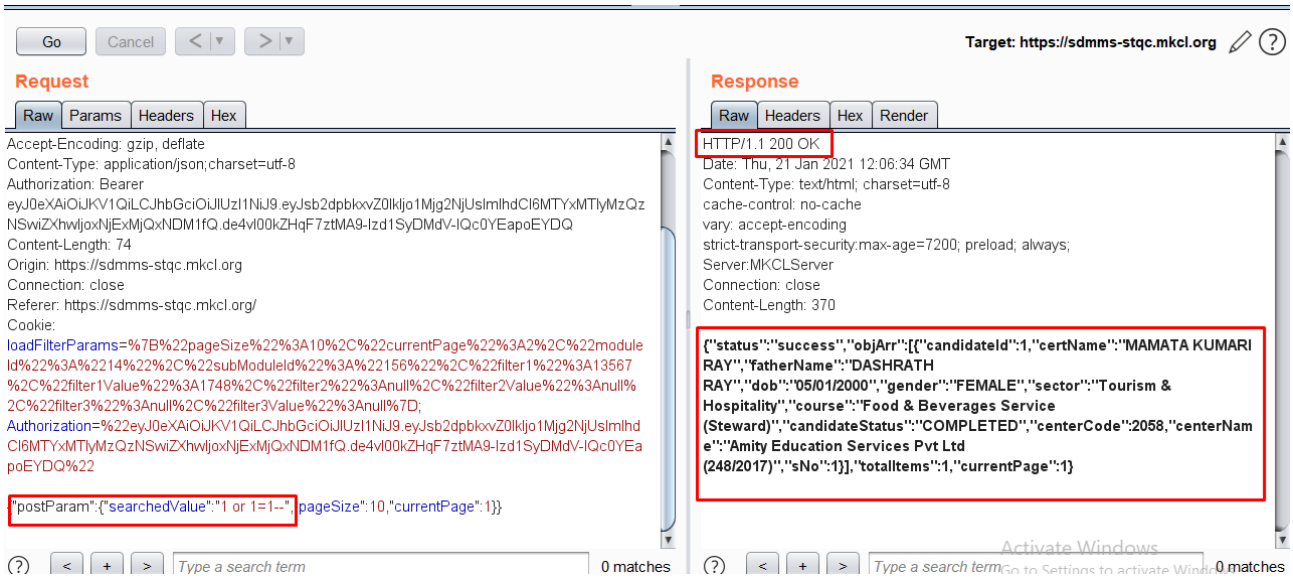
1. Open browser
2. Open burpsuite
3. Open Assam skil development webiste
4. login as – username: maanyaj, password: test#123
5. Open the following url in browser

   https://sdmms-stqc.mkcl.org/#/candidateSearchFacility/14/166

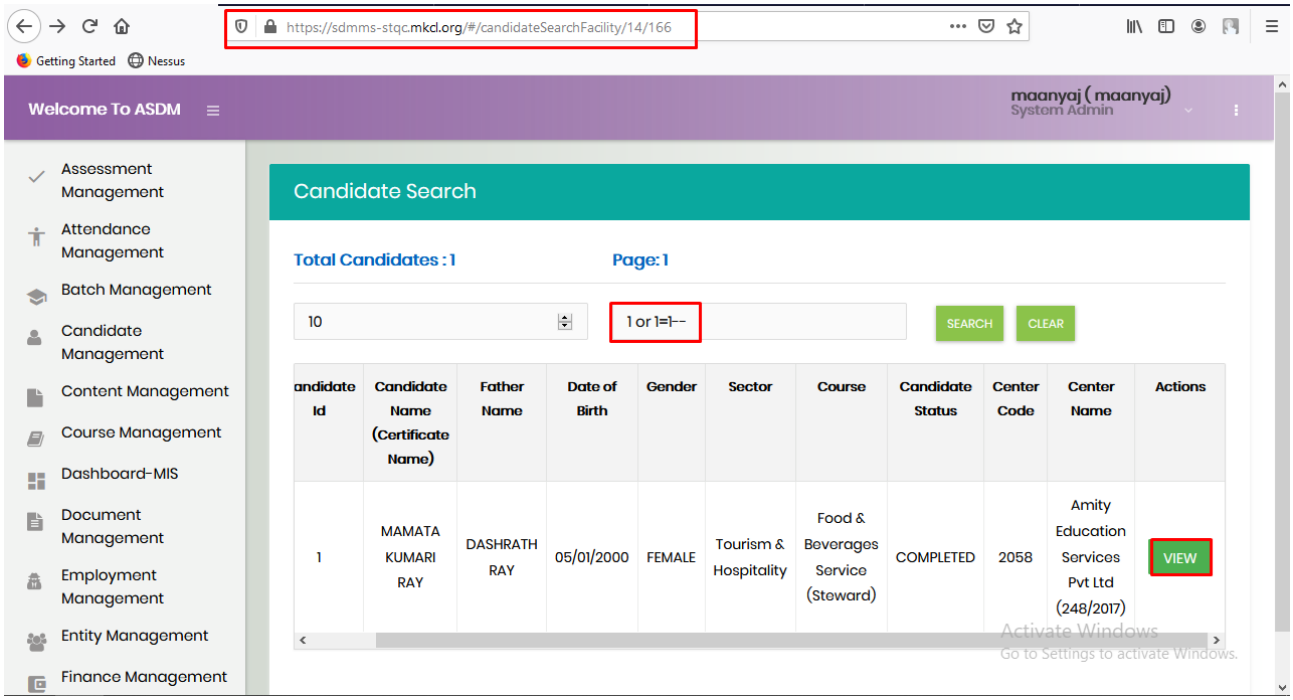
6. Put the sql injection as 1or1=1-- into search bar



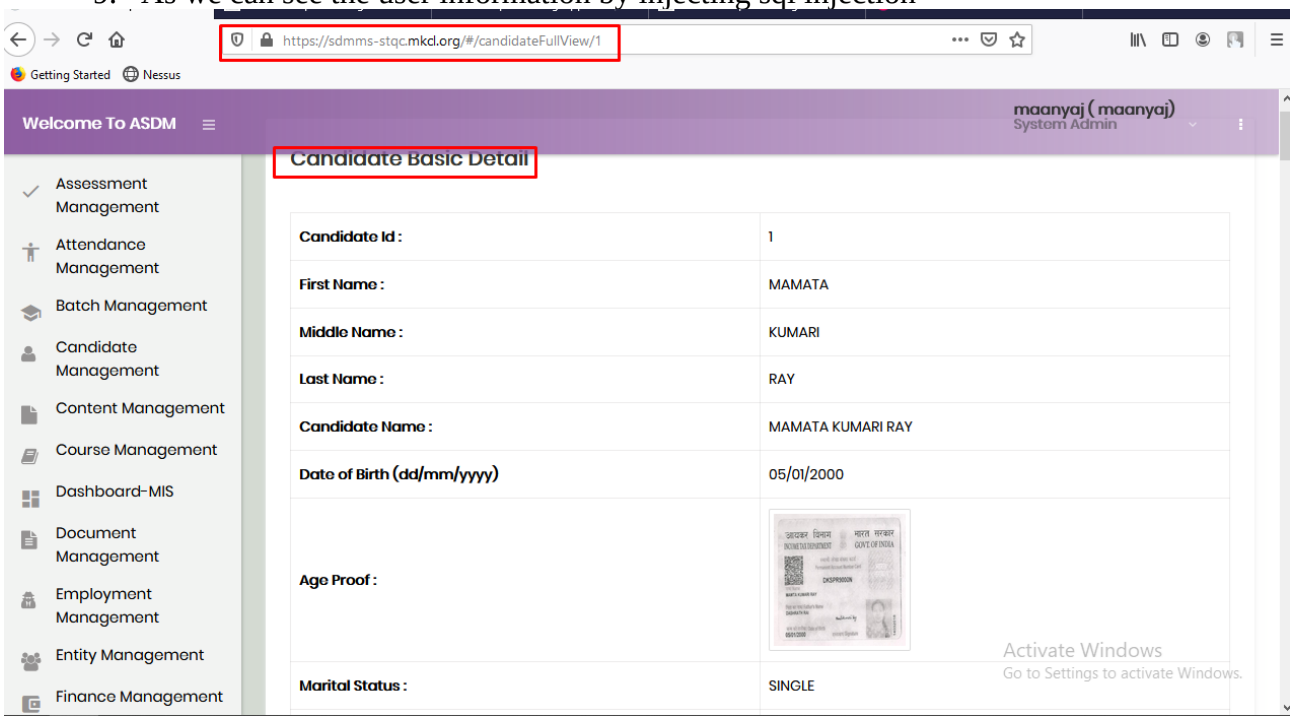
7. And click search



8. As we can see the response in brupsuite after putting sql injection in search bar, an SQL injection occurs when a value originating from the client's request is used within a SQL query without prior sanitisation. This could allow cyber-criminals to execute arbitrary SQL code and steal data or use the additional functionality of the database server to take control of more server components.



9. As we can see the user information by injecting sql injection



Solution: The only proven method to prevent against SQL injection attacks while still maintaining full application functionality is to use parameterized queries (also known as prepared statements). When utilising this method of querying the database, any value supplied by the client will be handled as a string value rather than part of the SQL query.

Additionally, when utilising parameterized queries, the database engine will automatically check to make sure the string being used matches that of the column. For example, the database engine will check that the user supplied input is an integer if the database column is configured to contain integers.

Status: Closed
BUG SEVERITY: MEDIUM

BUG ID 2: Parameter Tampering Attack

Severiyt: Medium

Description: The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

Reference Id(s):

- OWASP Top 10 (2017): A5-Broken Access Control
- CWE-472

Vulnerable Point(s):

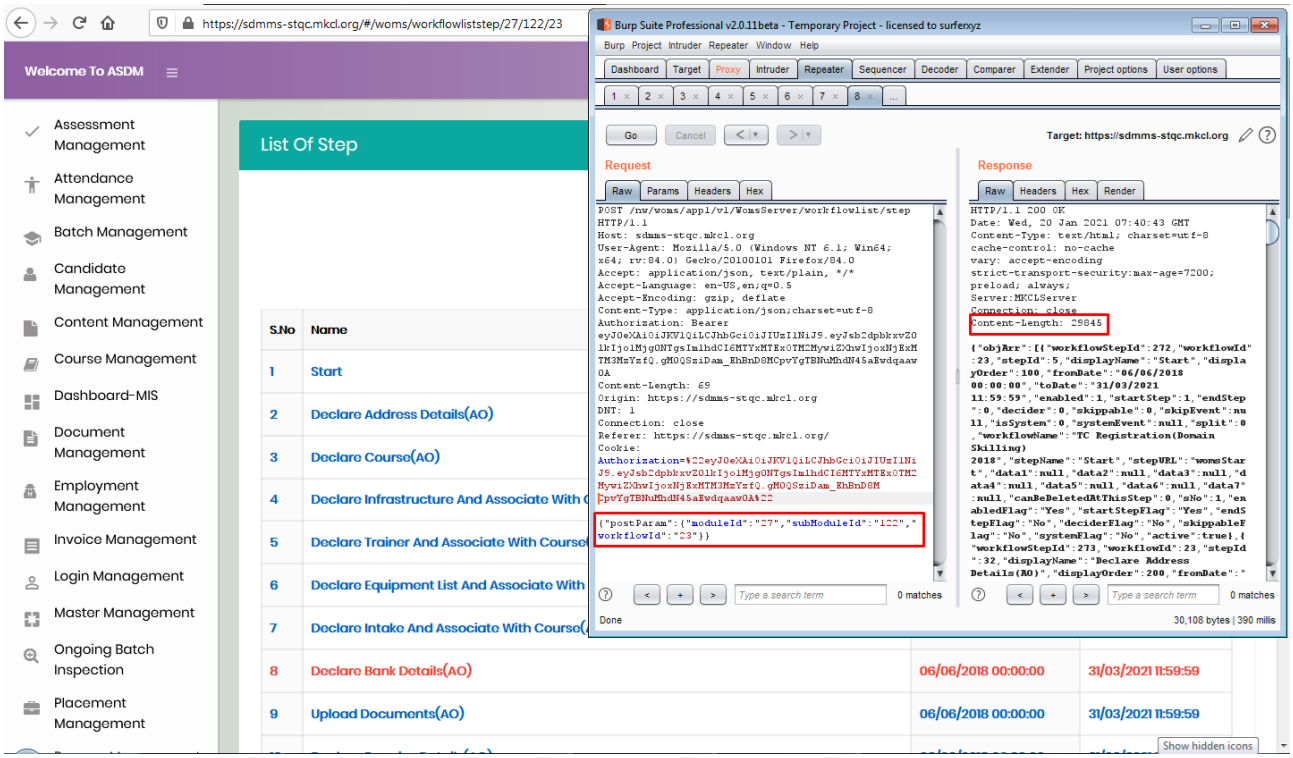
1. https://sdmms-stqc.mkcl.org/#/woms/workflowliststep/27/122/23

Proof of Concept(PoC):

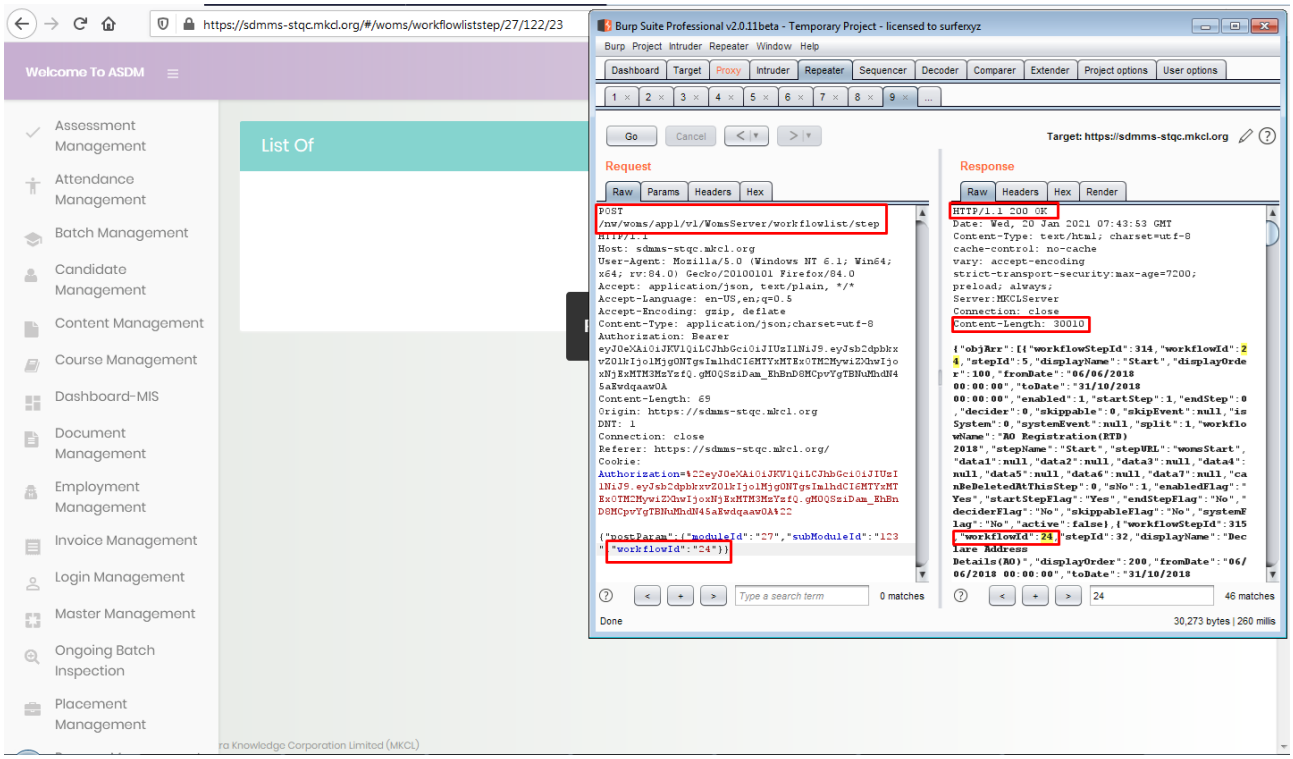
- Proof of Concept of Vulnerable Point Number 1

1. Open mozilla firefox
2. Open burpsuite
3. Open Asam skill development website
4. Enter credentals as usernam: maanyaj, password: test#123
5. open the following url and start intercepting

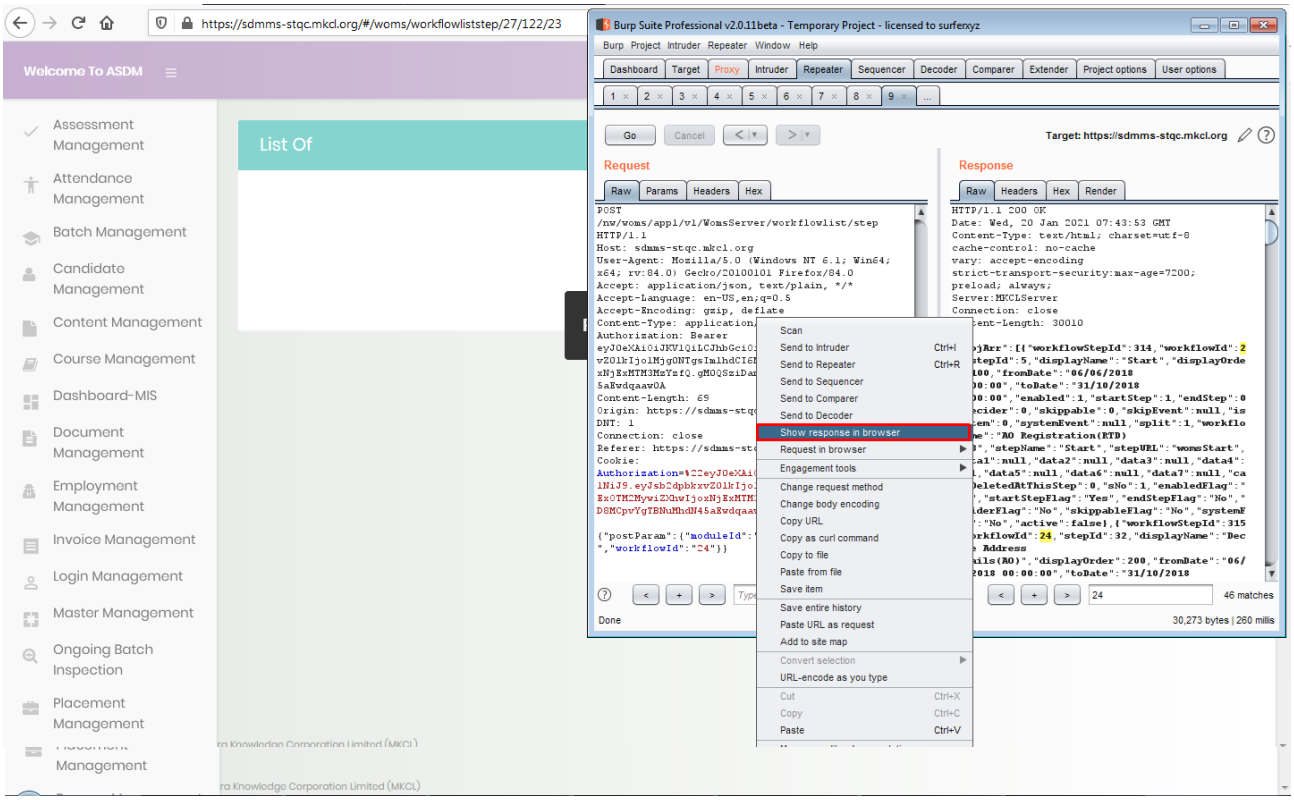
https://sdmms-stqc.mkcl.org/#/woms/workflowliststep/27/122/23

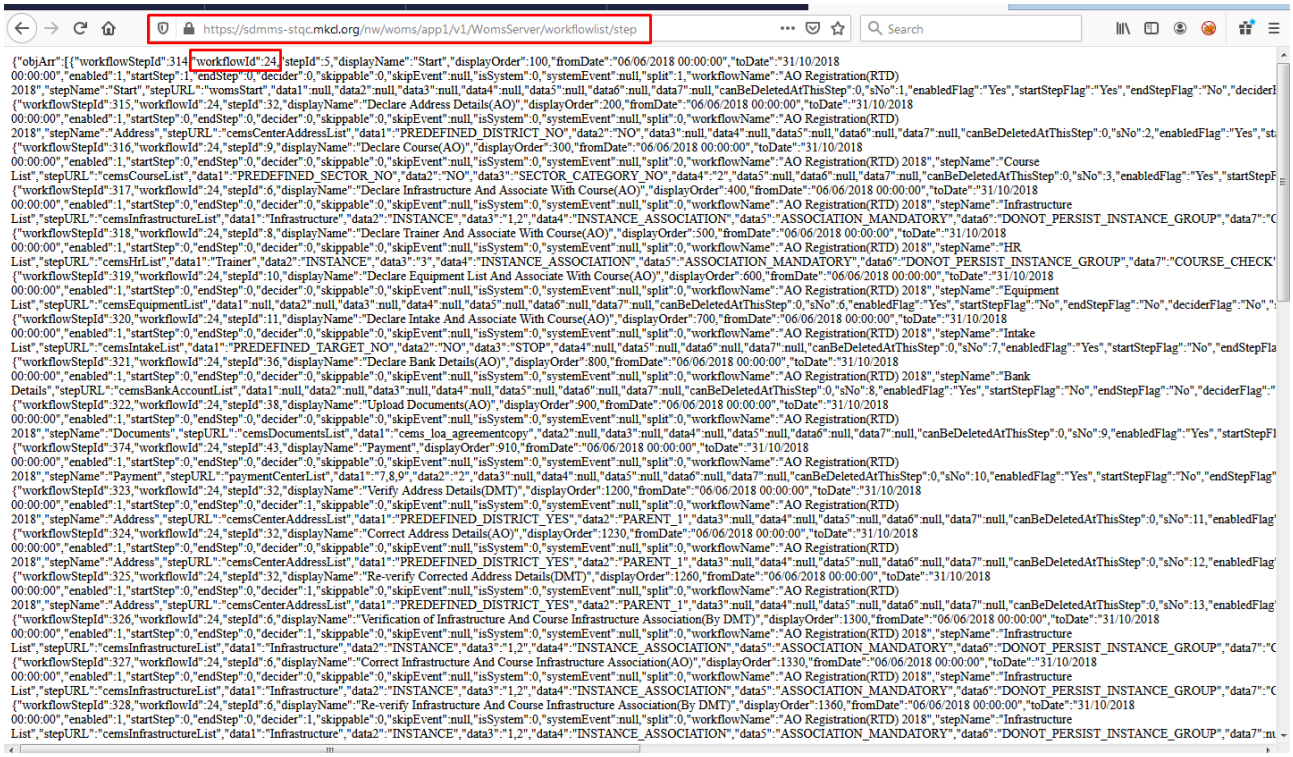


6. We have temperd the workflow id 23 to 24 and send the request to server and recive server response 200 ok with the information of 24 workflow id



7. Right click and click on show response in browser.





Solution:

The forms on the site should have some built-in protection

2. Using regex to limit or validate data
3. Server-side validation compared with all inputs
4. Avoid unwanted or hidden data
5. Don't allow interception

Status: Closed

BUG ID 3: Sensitive Information Disclosure (MITM)

Severity: Medium

Description: Cyberattack where a malicious actor inserts him/herself into a conversation between
two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it istoo late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM,

Reference Id(s):

- OWASP Top 10 (2017): A3 - Sensitive Data Exposure
- CWE-311
- WASC-13

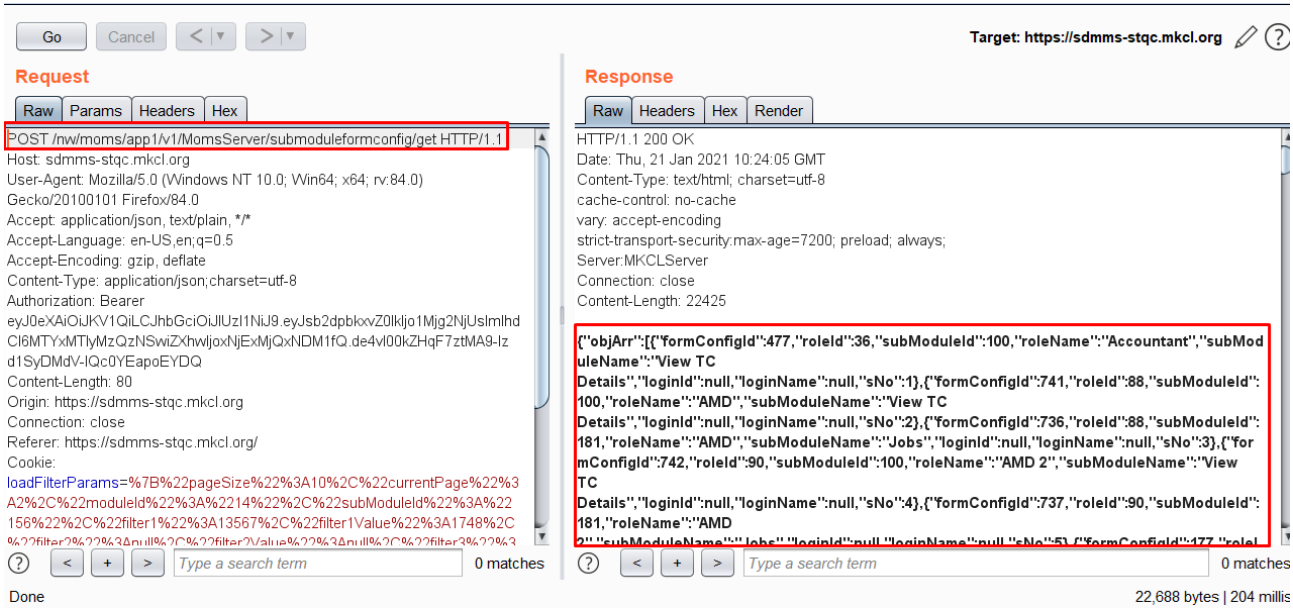
Vulnerable Point(s):

1. htpps://stqc.mkcl.org/nw/moms/app1/v1/MomsServer/sudbmoduleformconfig

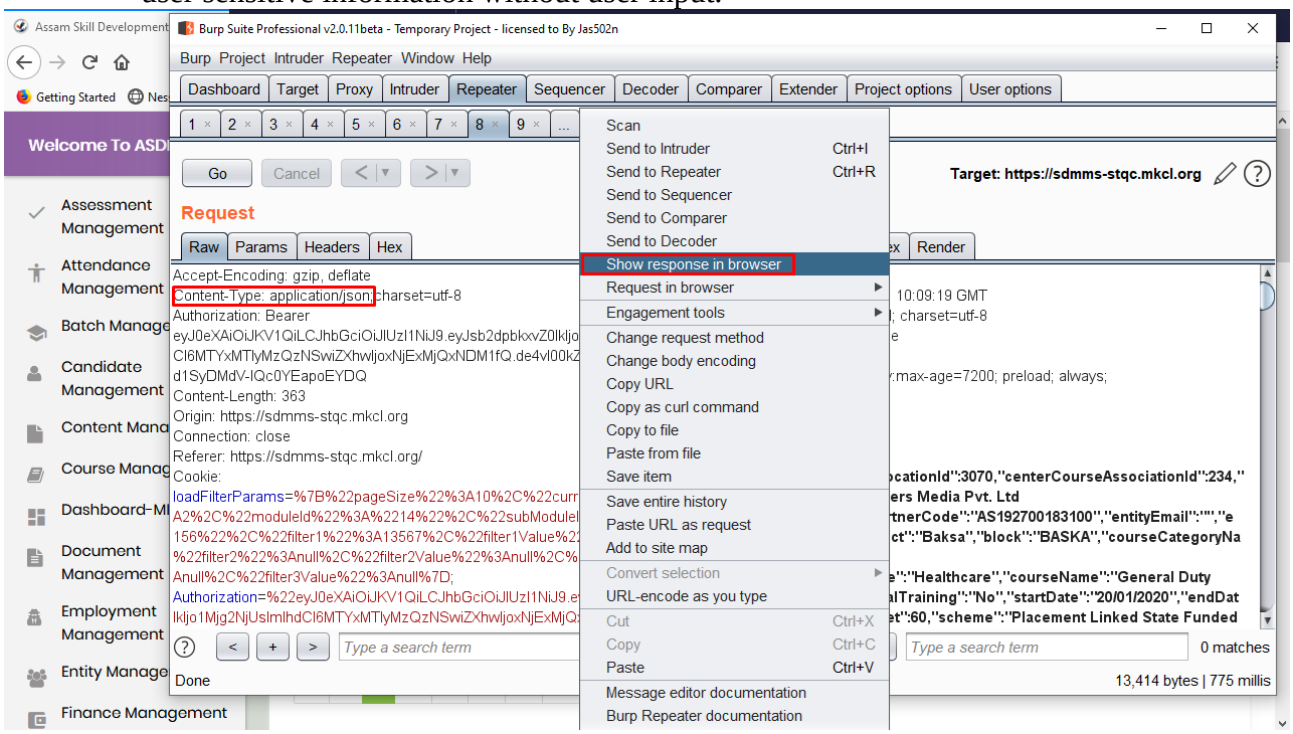
Proof of Concept(PoC):

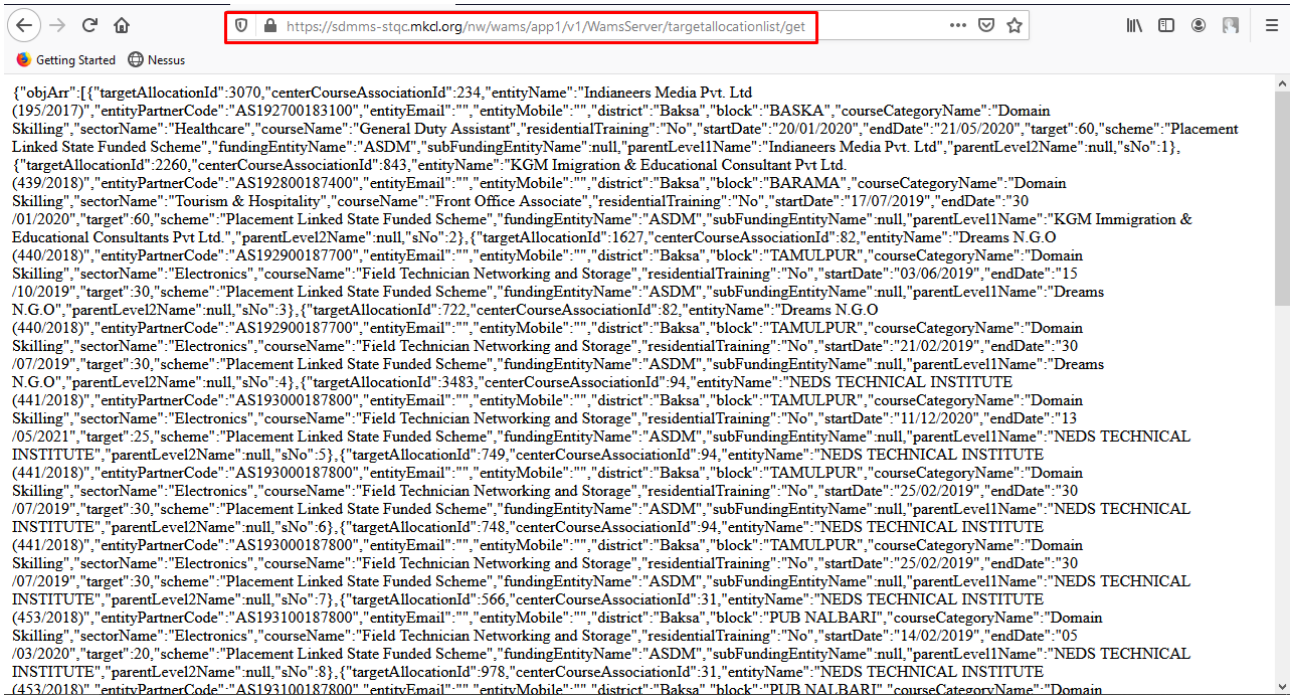
- Proof of Concept of Vulnerable Point Number 1

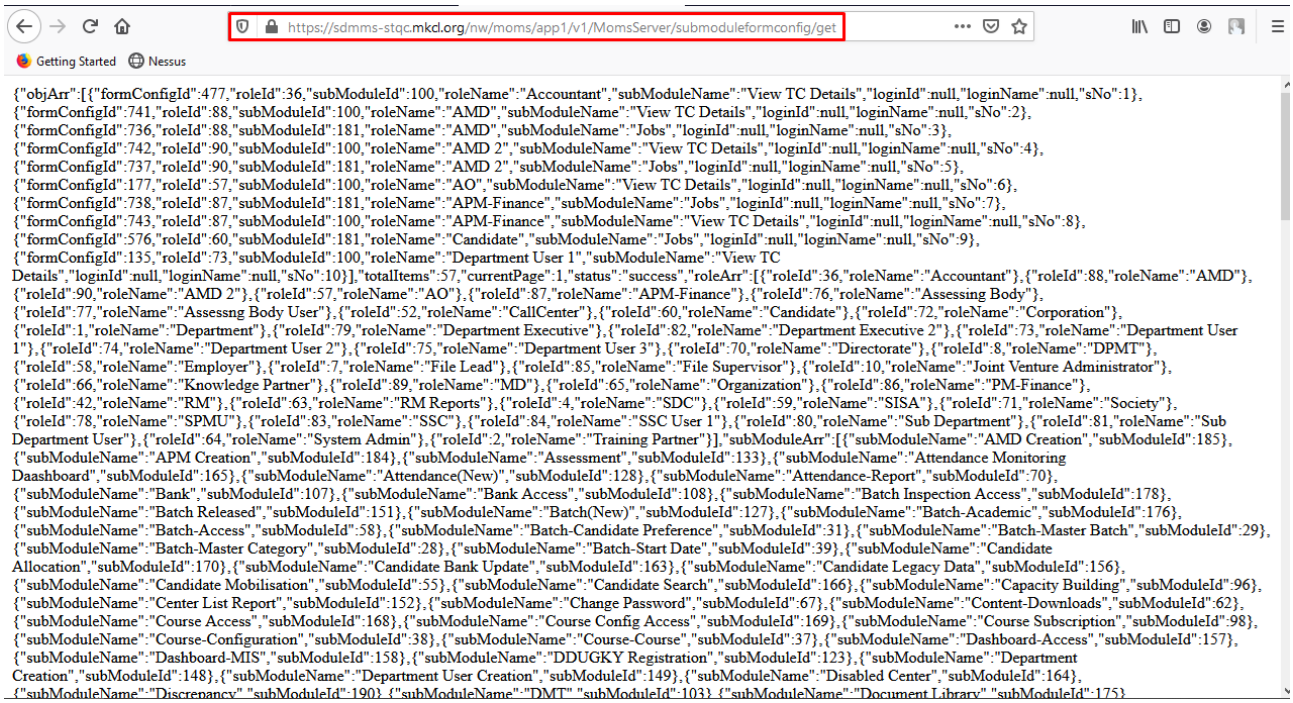
1. Open mozilla firefox
2. Open burpsuite
3. Open Asam skill development website
4. Enter credentals as usernam: maanyaj, password: test#123
5. open the following url and start intercepting
6. **htpps://stqc.mkcl.org/nw/moms/app1/v1/MomsServer/sudbmoduleformconfig**



7. As we can see by just clicking on Submit button the burp intercept and showing all user sensitive information without user input.







Solution: Both types of data should be protected. When thinking about data in transit, one way to
protect it on a website is by having an SSL certificate. SSL is the acronym for Secure Sockets Layer. It is the standard security technology for establishing an encrypted link between a web server and a browser. SSL certificates help protect the integrity of the data in transit between the host (web server or firewall) and the client (web browser).

Status: Closed

BUG ID 4: Vulnerable JS Library

Seveiryt: Medium

Description: The identified library jquery, version 1.11.2 is vulnerable.

Reference Id(s):

- CVE-2020-11023
- CVE-2020-11022
- CVE-2015-9251
- WASC-829

Vulnerable Point(s):

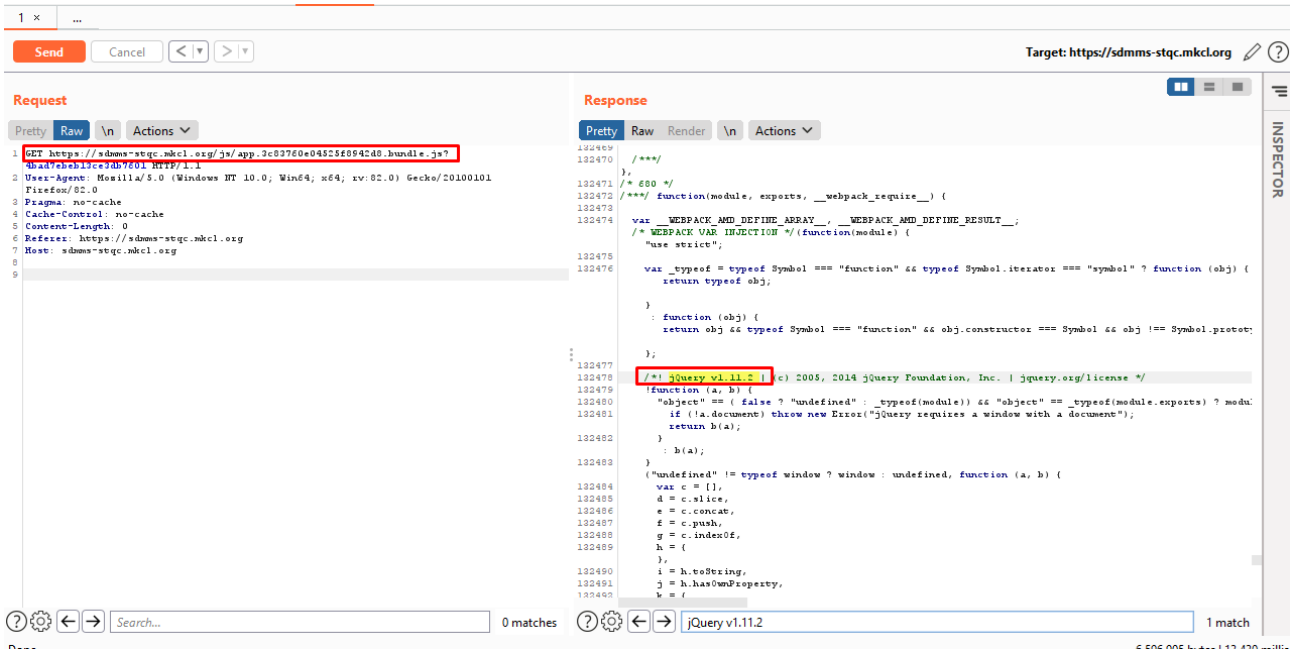
1. vulnerable js library

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open browser
2. Open burpsuite
3. Start intercepting the following url

https://sdmms-stqc.mkcl.org/js/app.3c83760e04525f8942d8.bundle.js

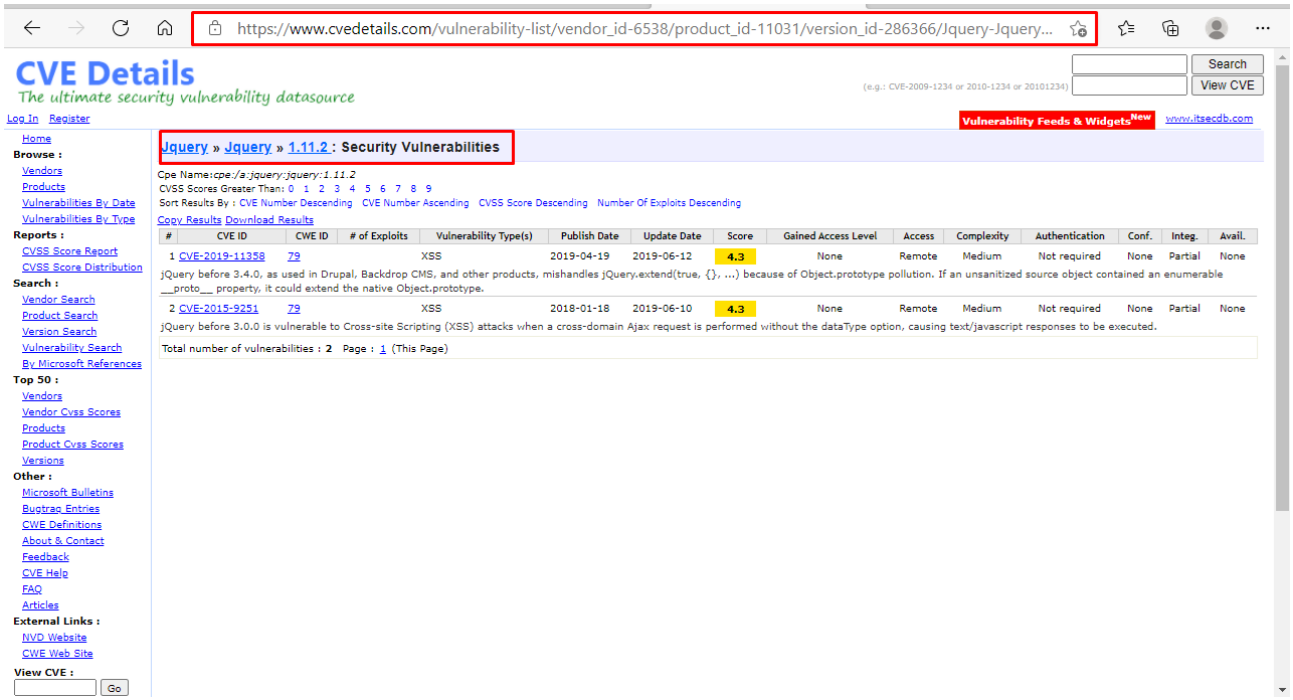


4. Send request to repeater and click go

5. In response shows that jquery version 1.11.2 is vulnerable.

6. Reference link: Jquery Jquery version 1.11.2 : Security vulnerabilities

(cvedetails.com)



Solution: Please upgrade to the latest version of jquery.

Status: Closed

BUG ID 5: Weak Lockout Mechanism

Severity: Medium

Description: Account lockout mechanisms require a balance between protecting accounts from
unauthorized access and protecting users from being denied authorized access. Accounts are typicallylocked after 3 to 5 unsuccessful attempts and can only be unlocked after a predetermined period of time,via a self-service unlock mechanism, or intervention by an administrator.

Reference Id(s):

- OWASP Top 10 (2017): A62- Broken Authentication
- CWE-1216
- WASC-15

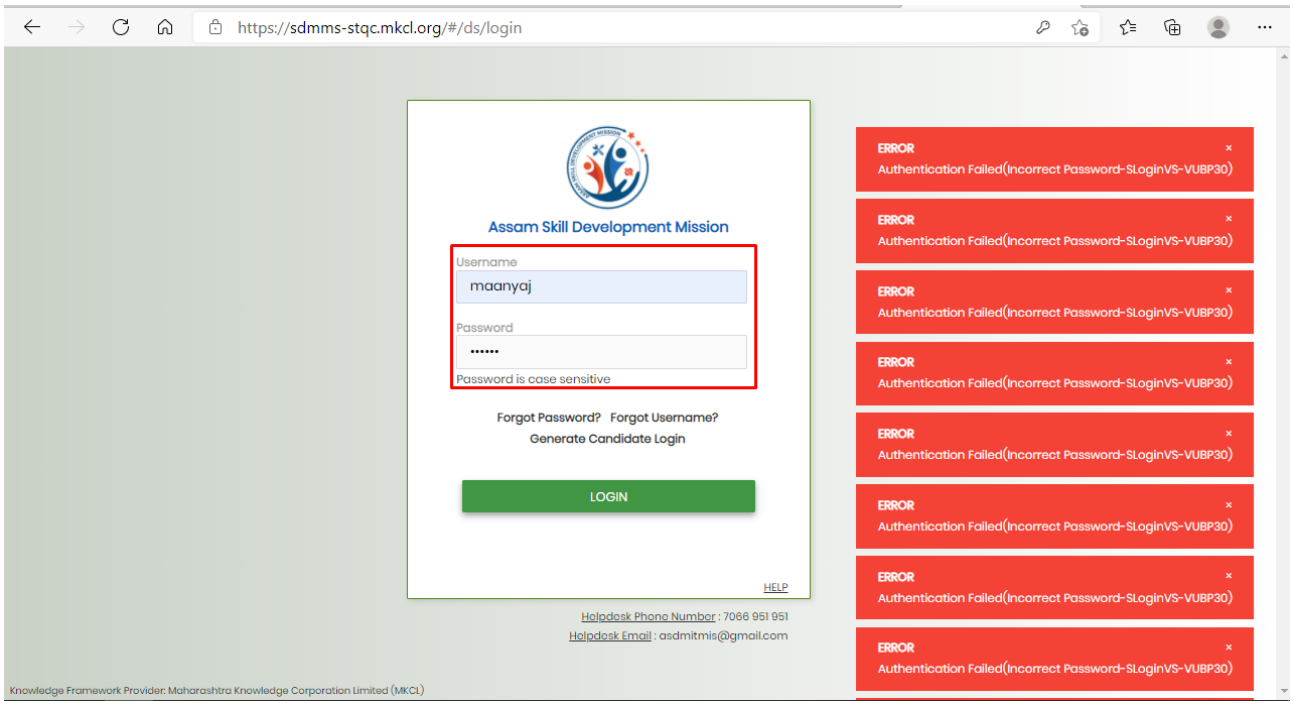
Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/#/ds/login

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open the Web Application using main URL https://sdmms-stqc.mkcl.org
2. Login with user id as maanyaj and put the invalid password and repeat it 7-8 times



Solution: Apply account unlock mechanisms depending on the risk level. In order from lowest to highest assurance,need to apply Time-based lockout and unlock. Self-service unlock (sends unlock email to registered emailaddress). Manual administrator unlock. Manual administrator unlock with positive user identification.

Status: Closed

BUG ID 6: Clear Text Transmission Of Credentials

Severity: Medium

Description: Applications transmit passwords and username over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Reference Id(s):

- OWASP Top 10 (2017): A6 - Security Misconfiguration
- CWE-319, 310

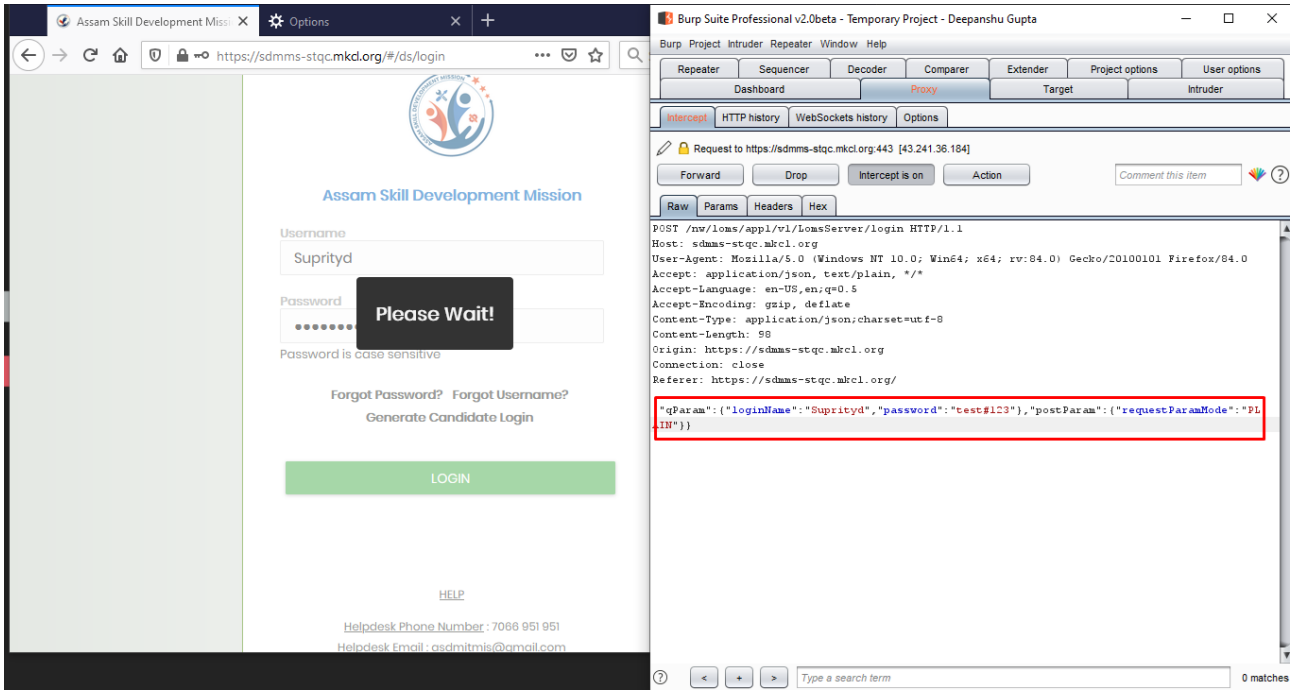
Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/#/ds/login

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open mozilla firefox browser
2. Open burpsuite
3. Open the following url - **https://sdmms-stqc.mkcl.org/#/ds/login**
4. Enter credentials as username: suprityd, password; test#123
5. Then start intercepting in the burpsuite



Solution: Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent ransmission over clear-text HTTP.

Status: Closed

BUG ID 7: Insufficient Session Expiration

Severity: Medium

Description: The application does not timeout inactive sessions within an appropriate amount of time. Once an individual session is established, it remains active for an extended period of time. This allows user sessions to remain valid longer than necessary leaving them open to attacks.

Reference Id(s):

- CWE-613

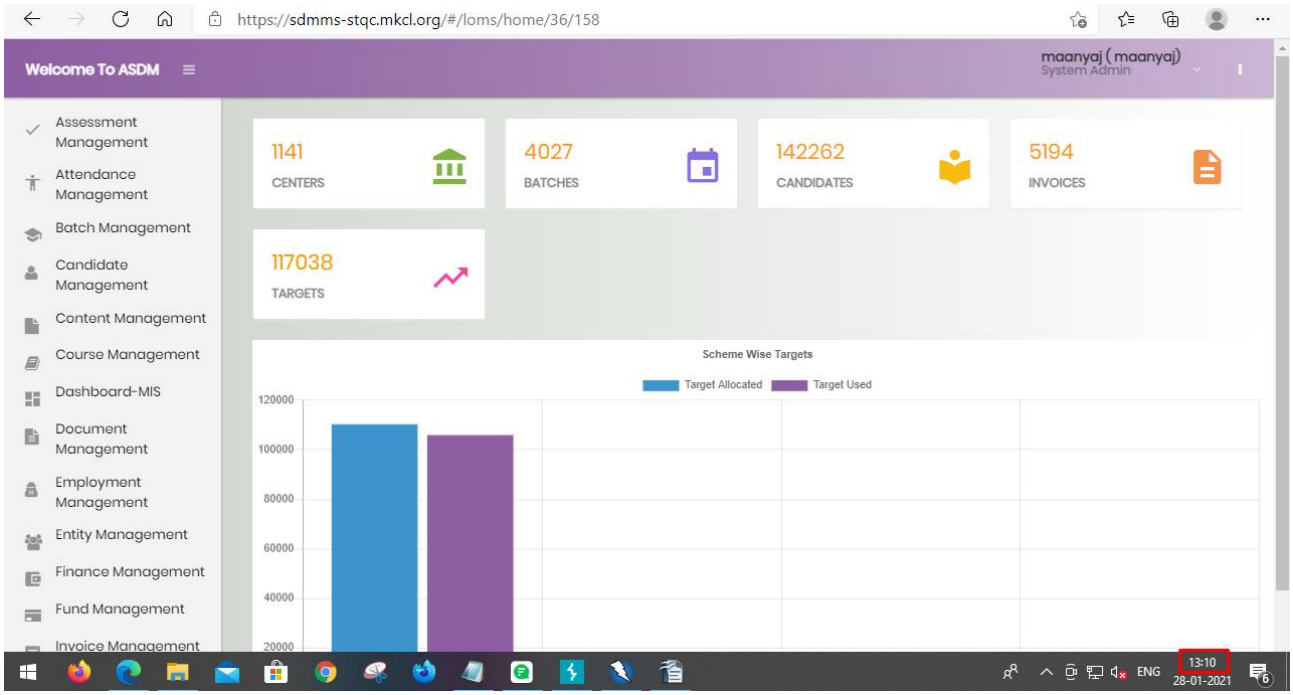
Vulnerable Point(s):

1. session timeout
2.

Proof of Concept(PoC):

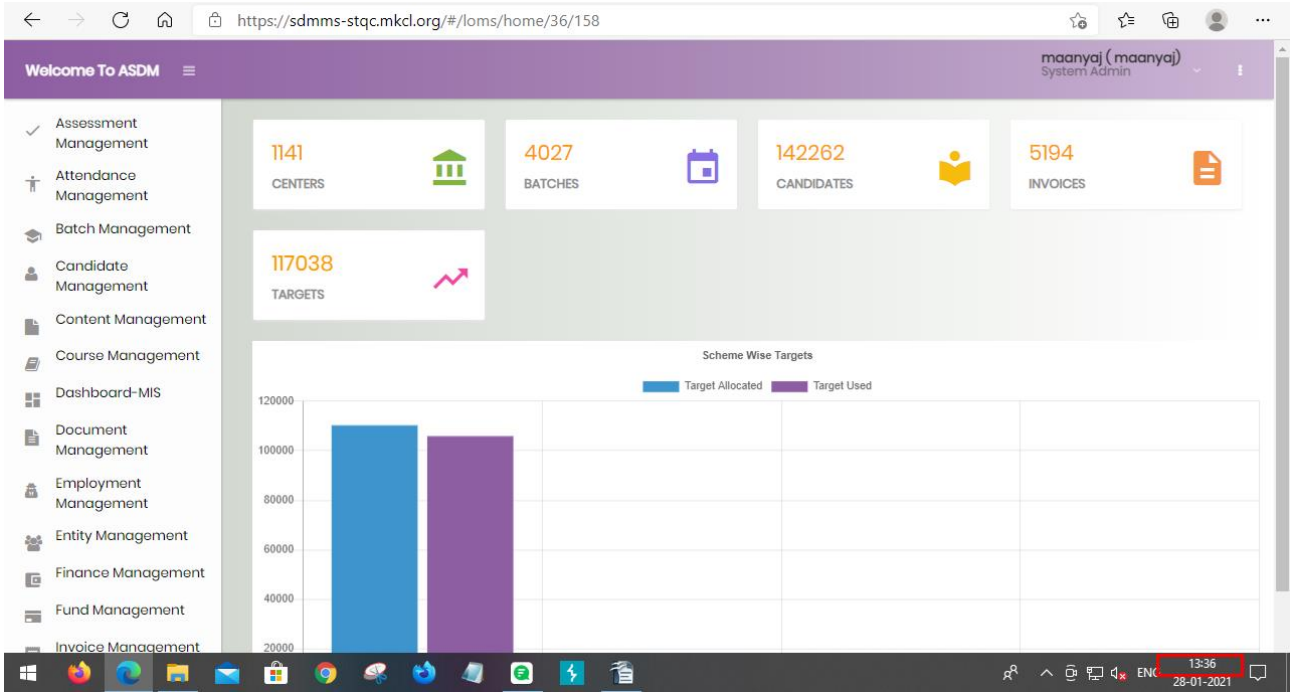
- Proof of Concept of Vulnerable Point Number 1

1. Open browser



2. Open Asam skill development website

3. Enter credentals as usernam: maanyaj, password: test#123we have login at 13:10 and minimize the window for 20 min and then refresh the website it show that applicaton doest not have session time out mechanism



Solution: Terminate a user's session on the server after an organization-defined period of inactivity appropriate for the application's level of sensitivity.

Status: Closed

BUG ID 8: Arbitrary File Downloading

Severity: Medium

Description: If the web application doesn't check the file name required by the user, any malicious user can exploit this vulnerability to download sensitive files from the server. Limit user from viewing or downloading files, a malicious user may attempt to view or download any file from your server. Attackers may construct malicious requests to download sensitive files from the server, and further embed website webshell files to control the website server host.

Reference Id(s):

- OWASP Top 10 (2017): A6 – Security Misconfiguration
- CWE-494
- WASC-14

Vulnerable Point(s):

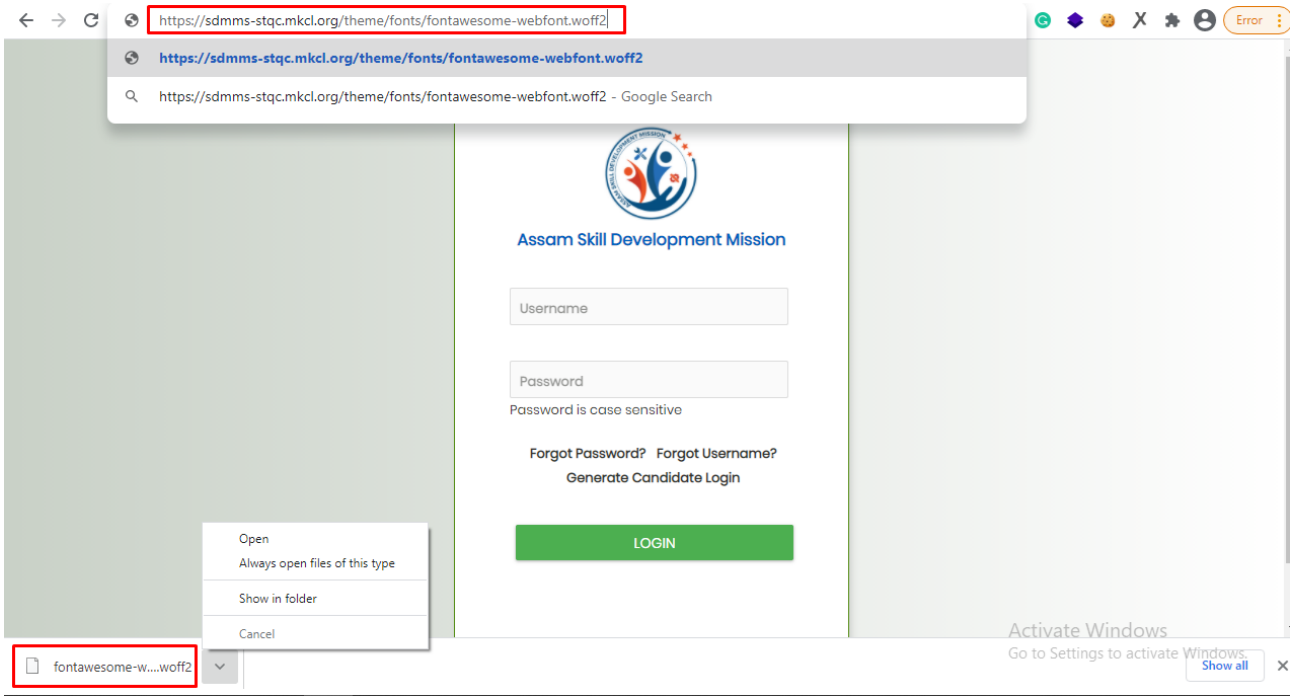
1. https://sdmms-stqc.mkcl.org/theme/fonts/fontawesome-webfont.woff2

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open browser
2. Open the following url on browser

https://sdmms-stqc.mkcl.org/theme/fonts/fontawesome-webfont.woff2



Solution: Update the plug-in you are using to the latest version. Delete the file with the vulnerability if it is no longer being used. Ensure that the application server is never running with root privileges. Restrict the privileges to a limited user account.

Status: Closed

BUG ID 9: Clear Text Transmission Of PAN/Aadhar/Voter ID Number

Severity: Medium

Description: The web application sends the request over to the server in cleartext. If an attacker
manages to steal the clear plain text, they could perform various types of cyber attacks against the user to whom the plain text. For example, an attacker could impersonate the victim user, and perform activities in their name. This could adversely affect the victim

Reference Id(s):

- OWASP Top 10 2017: A3 (Sensitive Data Exposure)
- CWE-311

- WASC-50

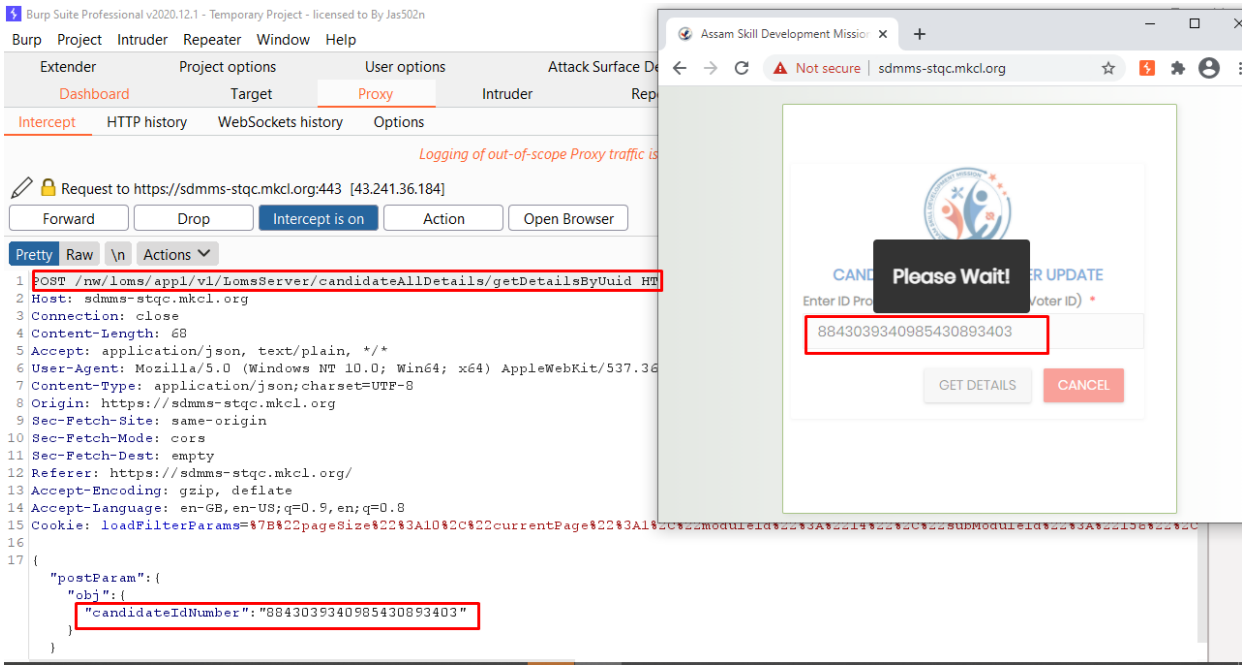
Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/#/candidateContactUpdate

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open mozilla firefox browser
2. Open burpsuite
3. Start intercepting the following url after entering the adhar or pan number



https://sdmms-stqc.mkcl.org/#/candidateContactUpdate

Soultion: Encrypt the request before transmitting it to the server

Status: Closed

BUG SEVERITY: LOW

BUG ID 10: X-Frame-Options Header Not Set

Seveiryt: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Reference Id(s):

- CWE-16
- WASC-15

Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org

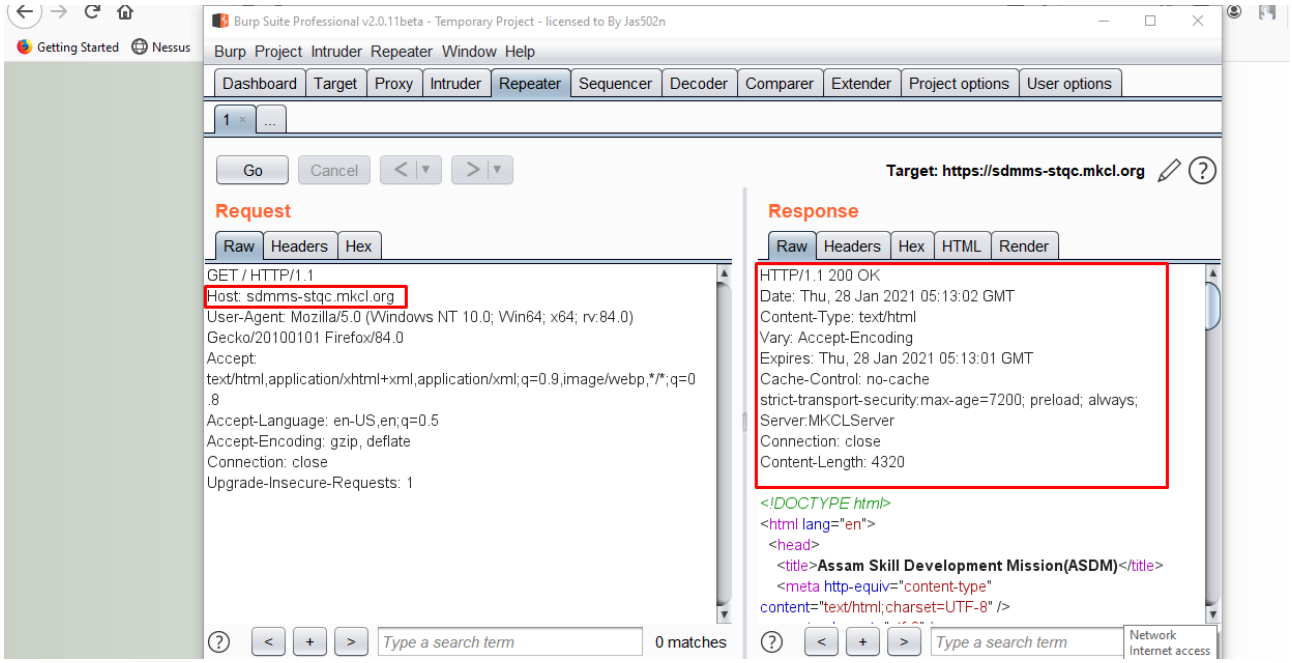
Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open Burpsuite
2. Open Browser
3. Start Intercept The Following url

https://sdmms-stqc.mkcl.org

4. The Following Response shows that content-type-options header is missing



Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Status: Closed

BUG ID 11: X-XSS-Protection header is not defined

Severity: Low

Description: The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.The server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack

Reference Id(s):

- OWASP Top 10 (2017): A6 - Security Misconfiguration
- CWE-16

Vulnerable Point(s):

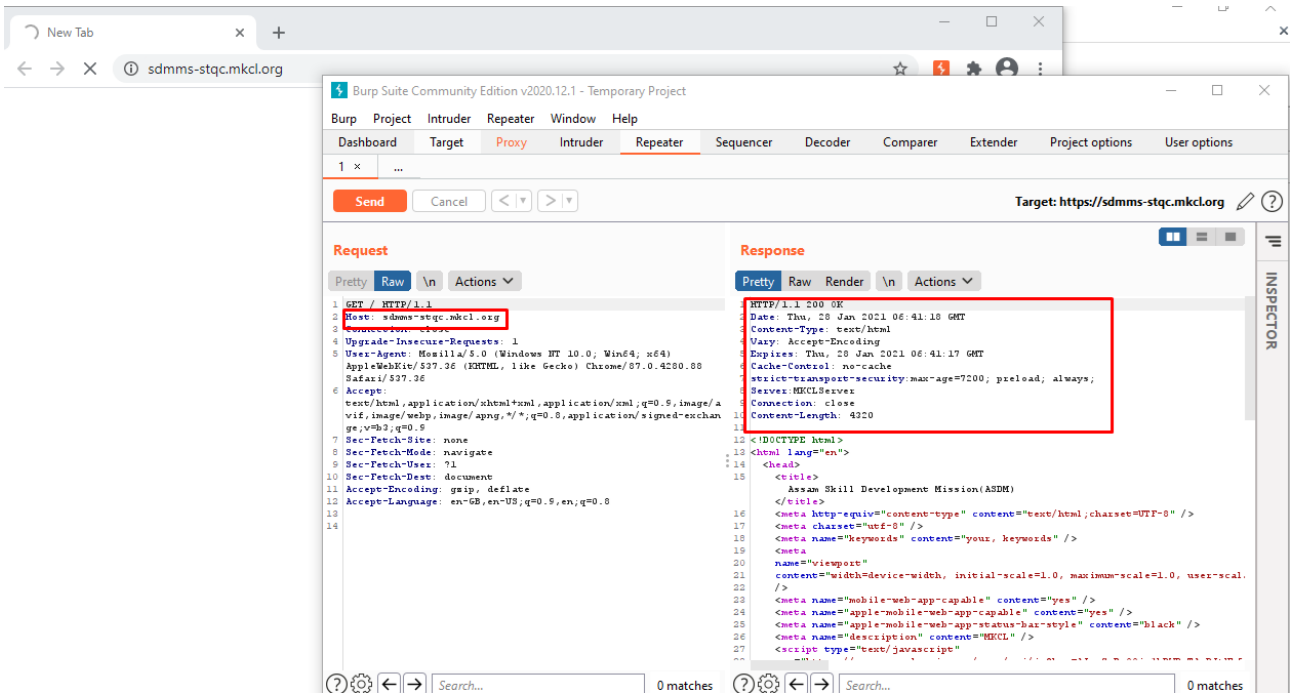
1. XSS protection header not defined

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open browser
2. Open brupsuite
3. Start Intercepting the following url

https://sdmms-stqc.mkcl.org



4. In Burp-suit Response there is no x-xss protection header not enabled

Solution: Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages.

Status: Closed

BUG ID 12: X-Frame-Options Header Not Set

Severity: Low

Description: X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Reference Id(s):

- CWE-16
- WASC-15

Vulnerable Point(s):

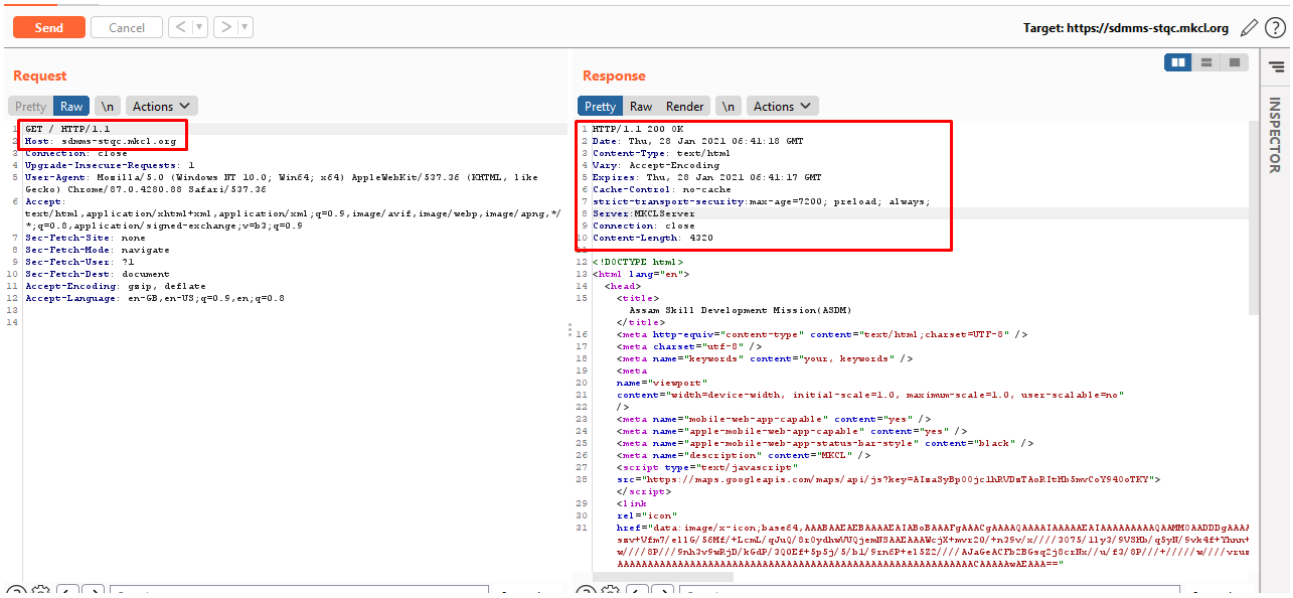
1. https://sdmms-stqc.mkcl.org

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open burpsuite
2. Open browser
3. Start intercepting the following url

https://sdmms-stqc.mkcl.org



Solution: Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browser)

Status: Closed

BUG ID 13: Cross-Domain JavaScript Source File Inclusion

Severity: Low

Description: The page includes one or more script files from a third-party domain.

Reference Id(s):

- CWE-829
- WASC-15

Vulnerable Point(s):

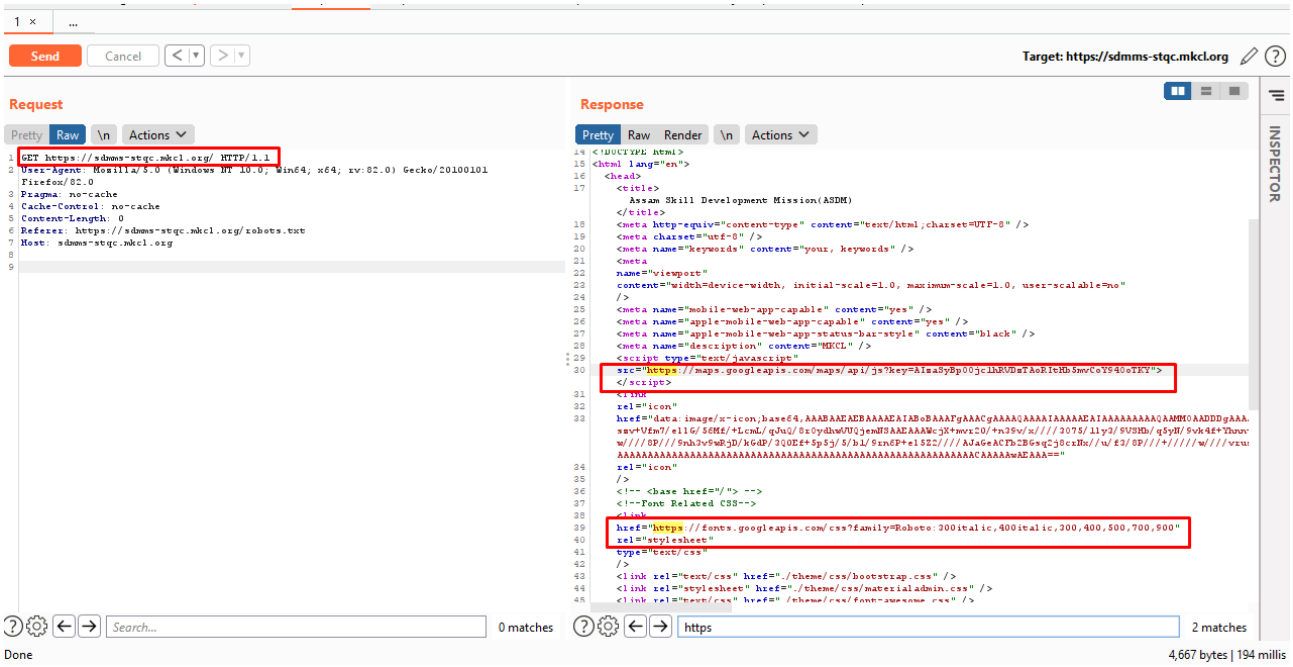
1. https://sdmms-stqc.mkcl.org

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open browser
2. Open burpsuite

3. Start intercepting the following url
4. Send to repeater and click go



Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Status: Closed

BUG ID 14: Browser Back Button Vulnerability

Severity: Low

Description: The web application is leaking sensitive information through the web browser's history. An attacker could steal this sensitive information using just the back button of the web browser, The back, forward and refresh buttons of the browser can be used to steal the password of a previous user, the back and forward buttons on the browser make use of this history to display the pages that the user visited recently

Reference Id(s):

- OWASP Top 10 2017: A2 (Broken Authentication)
- CWE-525, 287
- WASC-47

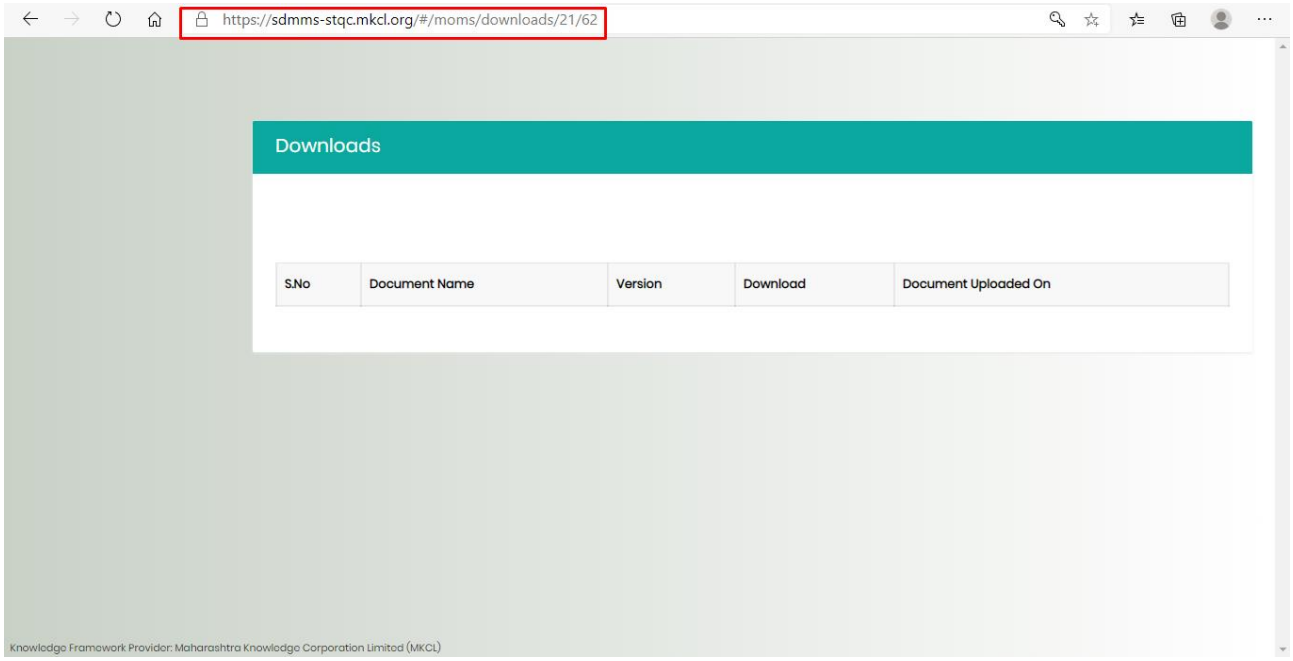
Vulnerable Point(s):

1. Browser Cache Weakness

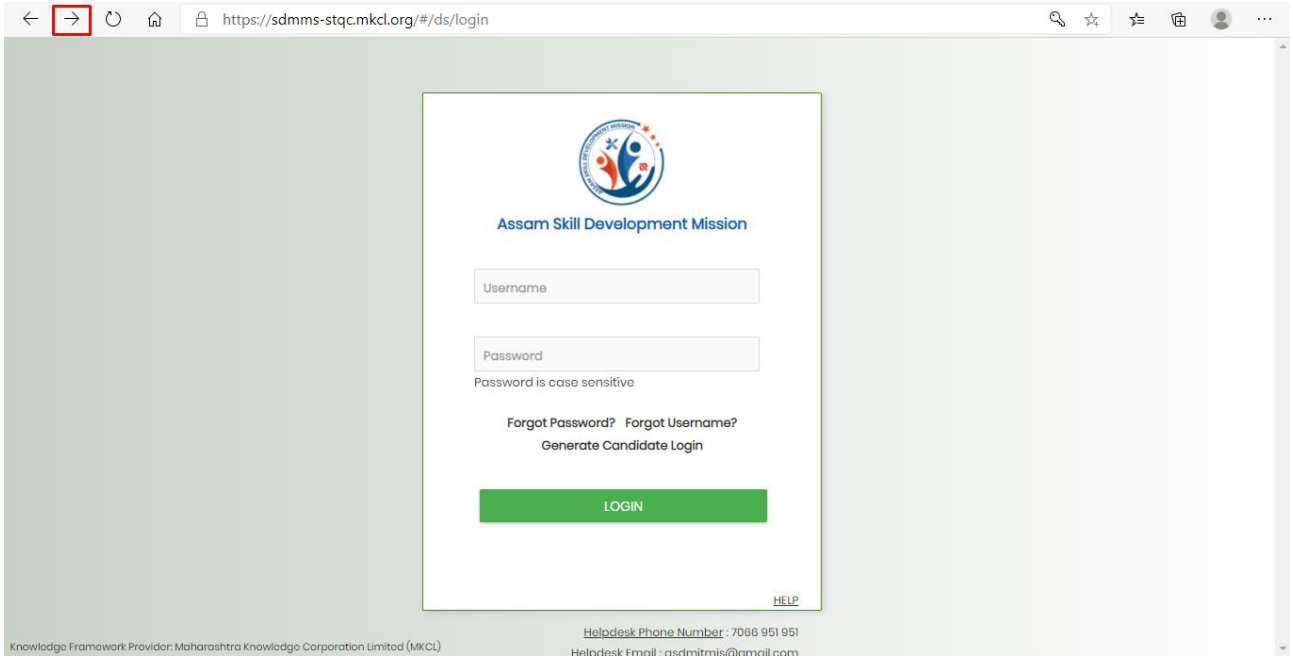
Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open mozilla firefox
2. Open burpsuite
3. Open Asam skill development website
4. Enter credentals as usernam: maanyaj, password: test#123.
5. As User Dashboard is loaded or shown with appropriate user detail
6. If user wants to exit or quiet from application he will have to follow the Logout process as Logout option is also available.
7. As we can see the Back button is enabled or showing, we just press on Back button to check that session / Browser cache weakness vulnerability.



8. After press Back button on browser the application back the all request without any browser cache expire or no authentication required.



Solution: Make sure that the web page is always delivered over HTTPS.

- Use proper session management including session cookies/token/authentication.
- Set the Cache-control header with the "must-revalidate" attribute. This indicates that the browser should not use the information that is cached for that particular request–response pair.

Status: Closed

BUG ID 15: Cross Site Scripting Weakness (Reflected in JSON Response)

Severity: Low

Description: Application is refelecting xss the payload injection in json response

Reference Id(s):

- CWE-79

Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/nw/nsdc/app1/v1/NSDCServer/nsdc/report

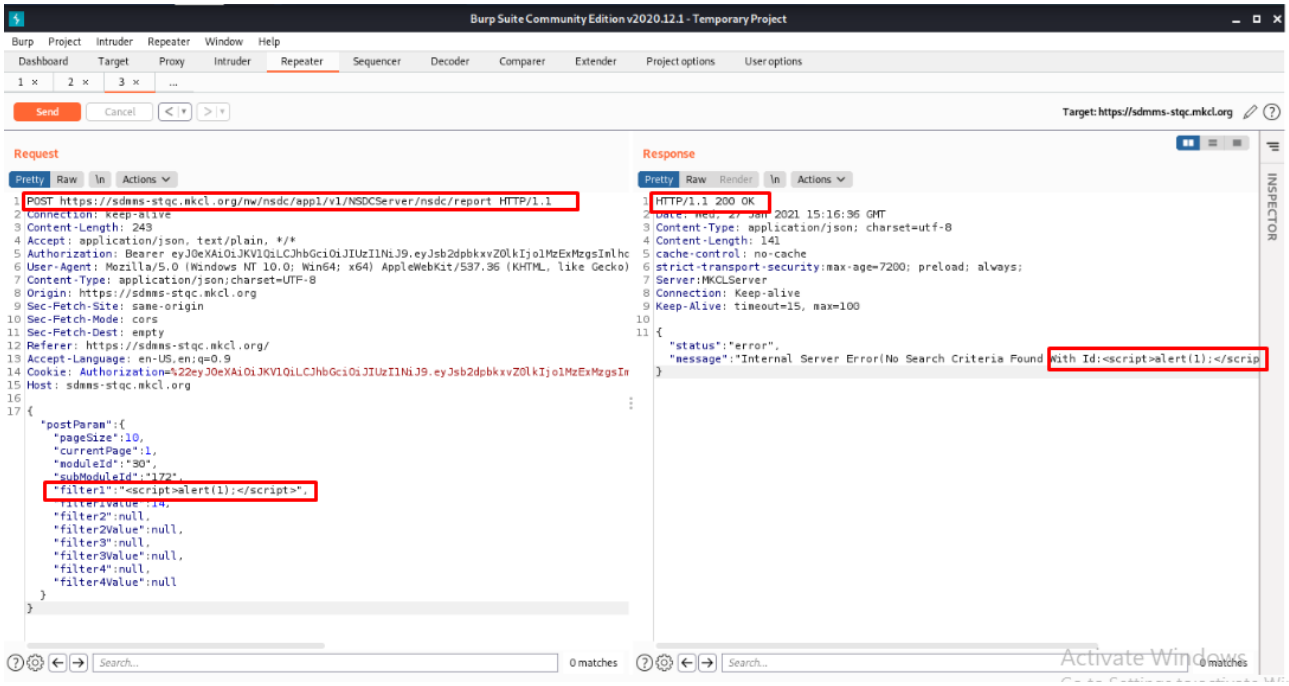
Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open burpsuite
2. Open mozilla firefox
3. start intercepting the following url

https://sdmms-stqc.mkcl.org/nw/nsdc/app1/v1/NSDCServer/nsdc/report

4. We put the xss payload in filter and its we can see the response the payload injection we put that is reflecting



Solution: Use xss protection header option to sanatize input value

Status: Closed

BUG ID 16: Embedded Open Type File Download

Severity: Low

Description: Application is allowing to download the Eot file form server, If the web application doesn't check the file name required by the user, any malicious user can exploit this vulnerability to download sensitive files from the server. Limit user from viewing or downloading files, a malicious user may attempt to view or download any file from your server. Attackers may construct malicious requests to download sensitive files from the server, and further embed website webshell files to control the website server host.

Reference Id(s):

- OWASP Top 10 (2017): A6 – Security Misconfiguration
- CWE-494
- WASC-14

Vulnerable Point(s):

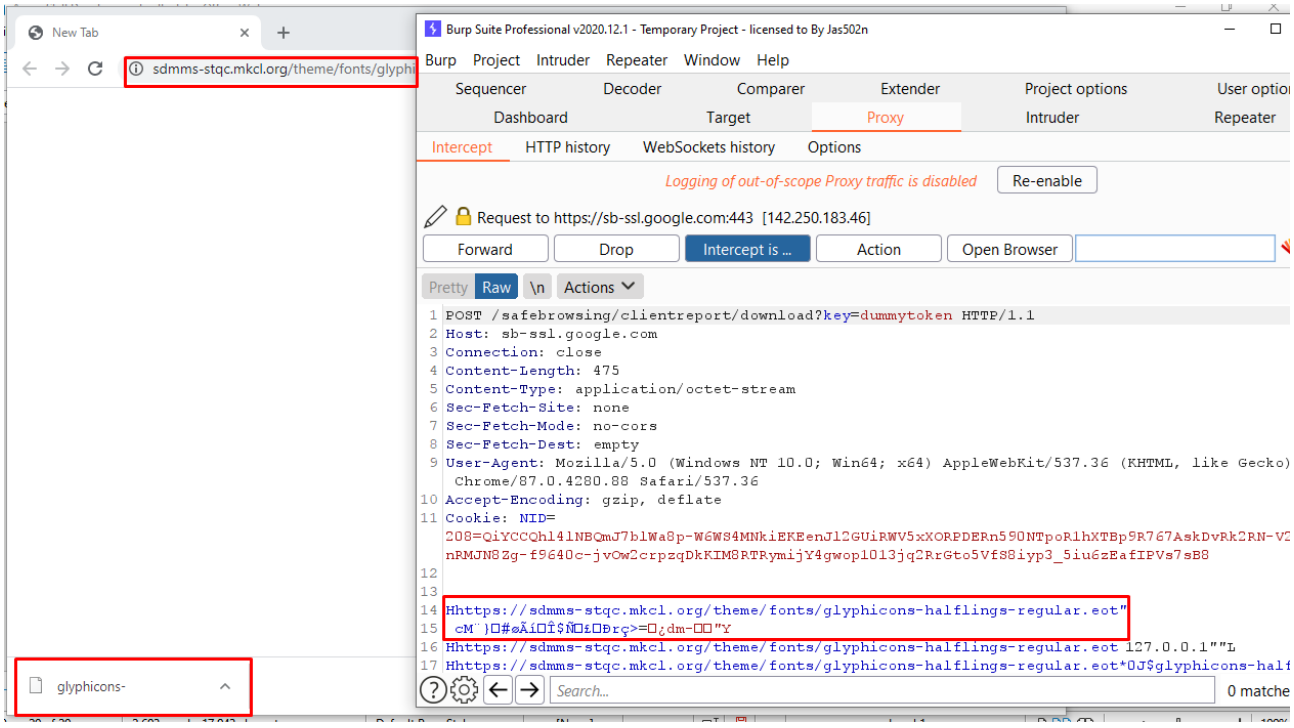
1. https://sdmms-stqc.mkcl.org/theme/fonts/glyphicons-halflings-regular.eot

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open mozilla firefox browser
2. Open the followng url in browser

https://sdmms-stqc.mkcl.org/theme/fonts/glyphicons-halflings-regular.eot



Solution:
Configure the web application to not to downlaod any arbitary file and eot file(s) from client side.

Status: Closed

BUG ID 17: Mixed content

Severity: Low

Description: The response is loaded over HTTPS, but loads other resources over an unencrypted connection. The following "passive" resource is loaded over HTTP. An attacker able to modify traffic could influence the application's appearance and behavior

The application loads pages over HTTPS that load other resources over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with these resources, which may indirectly disclose information about the user's activity on the application itself. Furthermore, an attacker able to modify traffic could alter these resources and potentially influence the application's

appearance and behavior. Due to these concerns, users' web browsers may automatically display warnings and disable affected components of the page. As a result, this vulnerability currently has more of an impact on usability than security.

Reference Id(s):

- CWE-16

Vulnerable Point(s):

1. https://sdmms-stqc.mkcl.org/js/app.3c83760e04525f8942d8.bundle.js

Proof of Concept(PoC):

- Proof of Concept of Vulnerable Point Number 1

1. Open browser
2. Open burpsuite
3. Open the following url

https://sdmms-stqc.mkcl.org/js/app.3c83760e04525f8942d8.bundle.js

4. Start intercepting wih burpsuite

5. Right click send repeater click send

Solution:

Ensure that all external resources the page references are loaded using HTTPS.

Status: Closed

Note: If any changes required in report or in testing, please let us know within 7 days of final report submitting, after 7 days, we will consider, it will auto accept no changes required.