Bug Report Summary

February 20, 2024

Contents

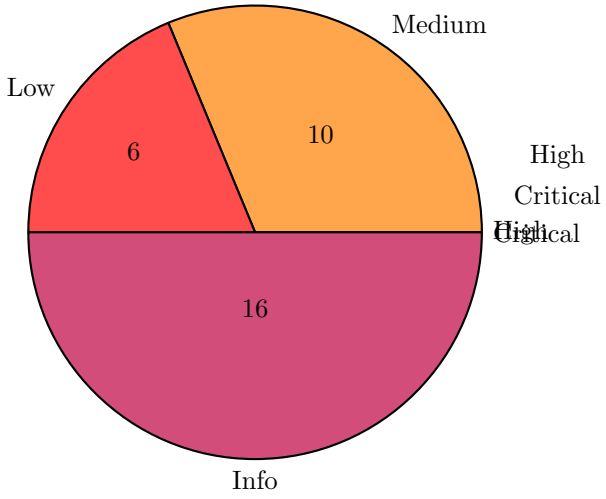

Figure 1: Pie Chart

1 Executive Summary

1.1 Strategic Recommendation

It is recommended to fix all critical, high and medium vulnerabilities before releasing the application to customer.

1.2 Scope of Work

The scope of this penetration test was limited to the URL mentioned below:

Scope Details			
Sr. No.	**Application Name**	**Application URL**	**Scope**
1.	Callyzer	http://65.21.6.24/	Callyzer web Application Manually & using Burpsuite

1.3 Summary of Findings

- Graphical Summary

Severity	Count
Critical	0
High	0
Medium	12
Low	6
Informational	16
Total	34

2 CVSS: Score Vulnerabilities

there are three types of scores that can be calculated: a base score, a temporal score and an environmental score. For purposes of reporting in this document, the CVSS base score will be provided. The base score assesses the following characteristics:

Characteristics	Description
Attack Vector	Assesses whether or an adversary can mount attack from a remote network, a local network or if an adversary must be logged on to the target of evaluation or physically connected.
Attack Complexity	Assesses the complexity of an attack dependent on how many of the attack variables are within the control of the adversary.
Privileges Required	Assesses the level of access that an attacker needs to mount a successful attack.
User Interaction	Assesses the extent to which actions of the victim are required for an attack to be successful.
Scope	Assess whether the impact of an attack is limited to the target of evaluation or if the attack has impact on other systems as well.
Confidentiality	Assesses the negative impact that an attack can have on the target of evaluation's confidentiality.
Integrity	Assesses the negative impact that an attack can have on the target of evaluation's integrity.
Availability	Assesses the negative impact that an attack can have on the target of evaluation's availability.

As indicated above, the assessment of these characteristics results in a severity score which ranges from 1-10. This score can be further broken down into the following rating levels:

Range	Rating	Description

9.0 - 10.0	Critical	These types of vulnerabilities should be reviewed immediately for impact to the business. This rating usually indicates that an exploit exists that could easily be use severely impact confidentiality, integrity and/or availability.
7.0 - 8.9	High	These types of vulnerabilities need to be assessed in the short term for impact to the business. A score in this range indicates that a vulnerability could be exploited with low to medium complexity and could have moderate or high impact on confidentiality, integrity and/or availability.
4.0 - 6.9	Medium	These vulnerabilities should also be evaluated for impact to the business, but the base score shows that these types of vulnerabilities may be only exploitable with increased effort or have little impact to confidentiality, integrity and/or availability.
0.1 - 3.9	Low	These vulnerabilities should also be evaluated, but from evaluating the base characteristics, the exploitation of these vulnerabilities is likely to result in little negative impact to confidentiality, integrity and/or availability.

The CVSS score provided in this report is meant to serve as a tool to assist with the prioritizing vulnerability resolution. This score, however, does not take into consideration the context of the business. For some business IT contexts some lower-scored vulnerabilities could have serious business impact. Hence, all of the reported vulnerabilities should be taken into consideration.

2.1 How to use this report

The vulnerabilities reported in this document provide a view of the target of evaluation's security posture at the time of testing. This timeframe, "at the time of testing", is important to highlight because the report cannot address future changes to the target of evaluation,

changes in the systems that support the target of evaluation and emerging, publicly disclosed exploits that could have an impact on the target of evaluation.

The goal of this document is to provide input to help identify and prioritize the vulnerabilities that were detected at the time of testing and to provide some guidance as to how the vulnerabilities might be mitigated.

Characteristics	Description
Status	This field will contain either "Verified" or "Detected". If this value is "Verified", then the tester exploited this vulnerability during the penetration test. If it is "Detected", then evidence of the vulnerability was found, but it was not exploited during testing. There are many reasons why a tester may not be able to exploit a vulnerability during testing. Examples include threat of system instability after exploit, lack of time during testing and/or inability to find a vector by which a vulnerability could be exploited.
CVSSv3.1 Scoring	This provides the overall severity score for a vulnerability including the individual assessments for attack vector, attack complexity, privileges required, user interaction, scope, confidentiality, integrity and availability.
Vulnerability Description	This provides an overview of the identified vulnerability including how it could be useful to an adversary.
Proof of Concept	This provides a description of how the vulnerability was detected and/or a description of how it can be reproduced for testing purposes.
Affected Uri	This provides a list of the url that are relevant to the vulnerability.
Recommendation	This provides suggestions on how to mitigate the vulnerability.
References	This provides links to CVEs, CWEs and other known resources to learn more about the vulnerability and how to mitigate the vulnerability.

The report is broken up into three major sections: an executive summary, a technical detail report and an appendix. The executive summary will provide a high-level overview of the vulnerabilities detected during the penetration test.

The technical detail report will provide the details of the vulnerabilities identified during the penetration test. Each vulnerability will include the following descriptors.

The appendix will contain information about the testing environment and further details gathered during testing that do not fit within the first three chapters. This information is necessary to have a complete picture of the penetration test, but it is in the appendix to make accessing the testing results more userfriendly.

3 Findings Overview

The following table summarizes the list of findings discovered during the security assessment

Summary Table				
Sr. No.	**Vulnerability Name**	**OWASP Category**	**Severity**	**CVSS Score++**
1	Application Does Not Implement HSTS Best Practices	Security Misconfiguration	Informational	2.5
2	Inadequate, Inconsistent or Missing Cookie Attributes	Security Misconfiguration	Informational	2.1
3	Missing Content Security Policy Header	Security Misconfiguration	Informational	2.8
4	Application Displays Web Server Banner	Security Misconfiguration	Informational	2.0
5	Misconfigured Content Security Policy	Security Misconfiguration	Informational	0.2
6	Application does not have a strong password policy	Security Misconfiguration	Informational	3.1
7	Application is Vulnerable to Clickjacking	Security Misconfiguration	Informational	2.4
8	Application is vulnerable to Improper Session Management	Security Misconfiguration	Informational	2.9
9	Application is vulnerable to Session Fixation Attack.	Security Misconfiguration	Informational	3.7
10	Application is vulnerable to Session Hijacking	Security Misconfiguration	Informational	2.4

11	HTTP Methods enabled on server(HEAD, PUT, DELETE, TRACE, TRACK, OPTIONS, DEBUG, PROPFIND)	Security Misconfiguration	Informational	3.2
12	Reset Password Link not expire	Security Misconfiguration	Informational	2.2
13	Response modification	Security Misconfiguration	Informational	2.4
14	Jquery version disclose	Security Misconfiguration	Informational	4.1
15	Session logout add member	Security Misconfiguration	Informational	4.0
16	Simultaneous login	Security Misconfiguration	Informational	4.3
17	Time based sql injection in remove user	Security Misconfiguration	Informational	2.3
18	User id and password in clear text	Security Misconfiguration	Informational	2
19	Email Spoofing Mail Server Misconfiguration	Security Misconfiguration	Informational	2.6

4 Technical Reports

The following findings were made during the assessment.

Finding Name	Remediation Effort
Critical Severity Findings	
High Severity Findings	
Medium Severity Findings	
Reflected Cross Site Scripting (XSS)	Quick
Low Severity Findings	
Informational Findings	
Application Does Not Implement HSTS Best Practices	Planned
Inadequate, Inconsistent or Missing Cookie Attributes	Planned
Missing Content Security Policy Header	Quick
Application Displays Web Server Banner	Planned
Misconfigured Content Security Policy	Planned
Application does not have a strong password policy	Planned
Application is Vulnerable to Clickjacking	Planned
Application is vulnerable to Improper Session Management	Planned
Application is vulnerable to Session Fixation Attack.	Planned
Application is vulnerable to Session Hijacking	Planned
HTTP Methods enabled on server(HEAD, PUT, DELETE, TRACE, TRACK, OPTIONS, DEBUG, PROPFIND)	Quick
Reset Password Link not expire	Planned
Response modification	Planned
Jquery version disclose	Planned
Session logout add member	Quick
Simultaneous login	Planned
Time based sql injection in remove user	Quick
User id and password in clear text	Planned

Email Spoofing Mail Server Misconfiguration	Planned

4.1 Application Does Not Implement HSTS Best Practices

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.5

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.2 Inadequate, Inconsistent or Missing Cookie Attributes

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.1

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.3 Missing Content Security Policy Header

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.8

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Quick

4.4 Application Displays Web Server Banner

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.0

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.5 Misconfigured Content Security Policy

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 0.2

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.6 Application does not have a strong password policy

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 3.1

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.7 Application is Vulnerable to Clickjacking

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.4

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.8 Application is vulnerable to Improper Session Management

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.9

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.9 Application is vulnerable to Session Fixation Attack.

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 3.7

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.10 Application is vulnerable to Session Hijacking

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.4

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.11 HTTP Methods enabled on server(HEAD, PUT, DELETE, TRACE, TRACK, OPTIONS, DEBUG, PROPFIND)

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 3.2

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Quick

4.12 Reset Password Link not expire

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.2

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.13 Response modification

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.4

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.14 Jquery version disclose

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 4.1

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.15 Session logout add member

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 4.0

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Quick

4.16 Simultaneous login

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 4.3

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.17 Time based sql injection in remove user

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.3

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Quick

4.18 User id and password in clear text

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned

4.19 Email Spoofing Mail Server Misconfiguration

Status: New

Severity: Informational

OWASP Category: Security Misconfiguration

CVSS Score: 2.6

Affected Hosts/URLs:

http://65.21.6.24/dashBoard

Summary:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict-Transport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP StrictTransport Security (HSTS) implementation is not as strict as is typically advisable. The browser will expire the HSTS header after the number of seconds configured in the max-age attribute. HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

proof of concept:

Remediation:

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year). The strongest protection is to ensure that all requested resources use only TLS with a well-formed HSTS header. It is advisable to assign the max-age directive's value to be greater than 10368000 seconds (120days) and ideally to 31536000 (one year).

Remediation effect:

Planned