Government of India
Ministry of Communications & Information Technology
Department of Information Technology

NATIONAL
INFORMATICS
CENTRE

Web-Application Penetration Testing Report

For

Website URL: http://amplifi.mohua.gov.in/

Date: 24th May 2022

Contact Us :

Application Security Audits and Assessment Division
(Application Security Group)
National Informatics Centre
A – Block,CGO Complex, Lodhi Road
New Delhi – 110003

011-2430-5877
011-2430-5142
011-2430-5934
011-2430-5215

Contributions:

	Name	Role
1.	Mr. Pradeep Kumar Mrs. Alka Upadhyay	Reviewer
2.	Mr. Rajesh Mishra	HOD
3.	Mrs. Ratnaboli Ghorai Dinda	HOG

Key Findings

1. **Weak Hashing Algorithm – High**
2. **Directory Listing – High**
3. **Critical Resource Disclosure – High**
4. **DOS Attack – High**
5. **TLS/SSL Vulnerability - Medium**
6. **Insecure Cookie Attributes – Low**
7. **Insecure HTTP Method - Low**
8. **Information Disclosure – Low**
9. **Using Components with known Vulnerabilities – Low**
10. **Default Server Page Accessible - Low**

1. Weak Hashing Algorithm

Incident URL: https://amplifi.mohua.gov.in/login

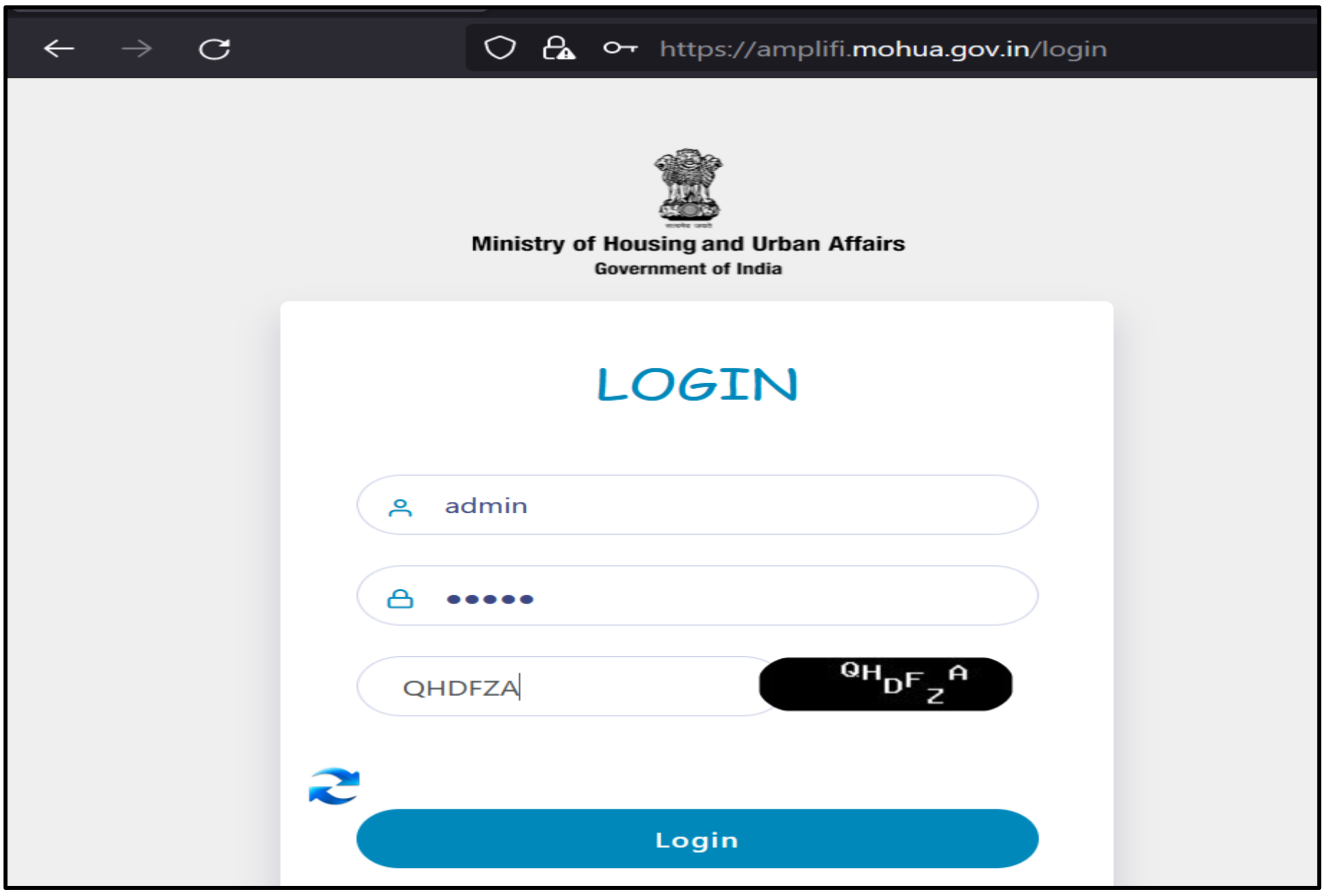
Description: The application has not implemented Salted Hashing Technique for the transmitting of password from client to server.

Impact: This vulnerability allows an attacker to steal the hashed password and can replay to login to the application.

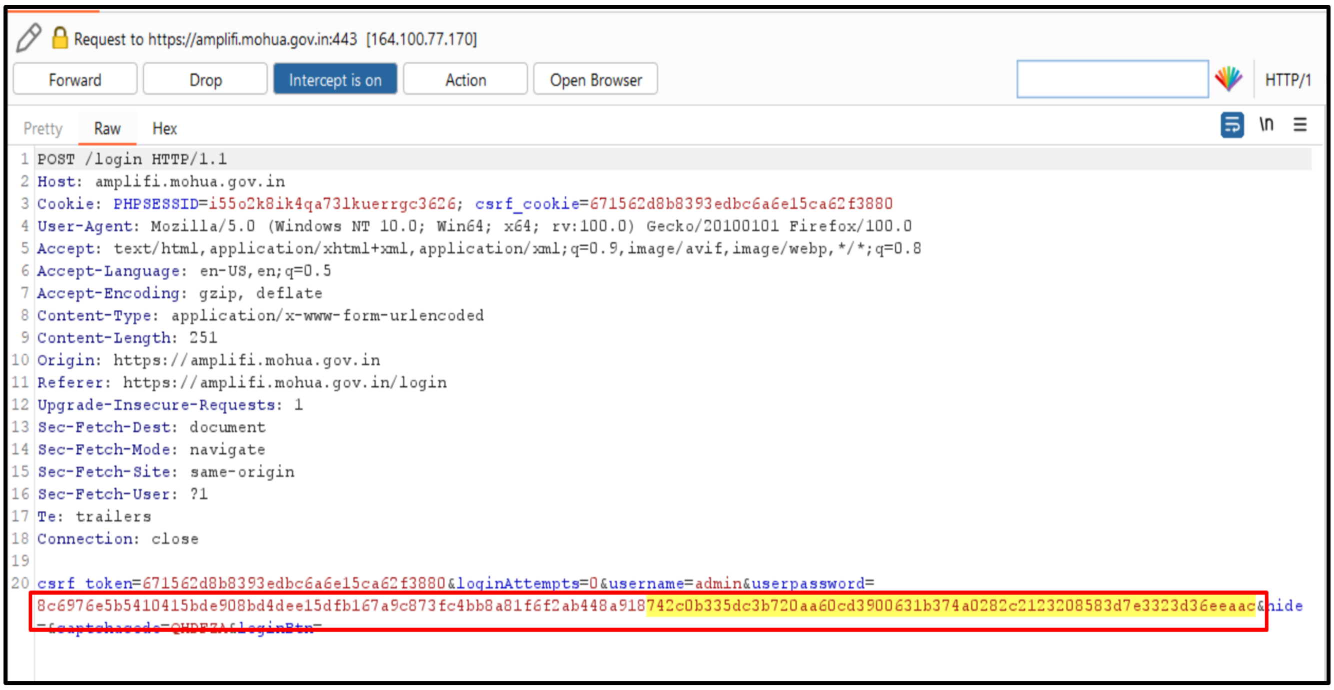
Severity: High

How to Test:

Step#1: A victim user navigates to the application at URL: https://amplifi.mohua.gov.in/login and login with credential as shown below:

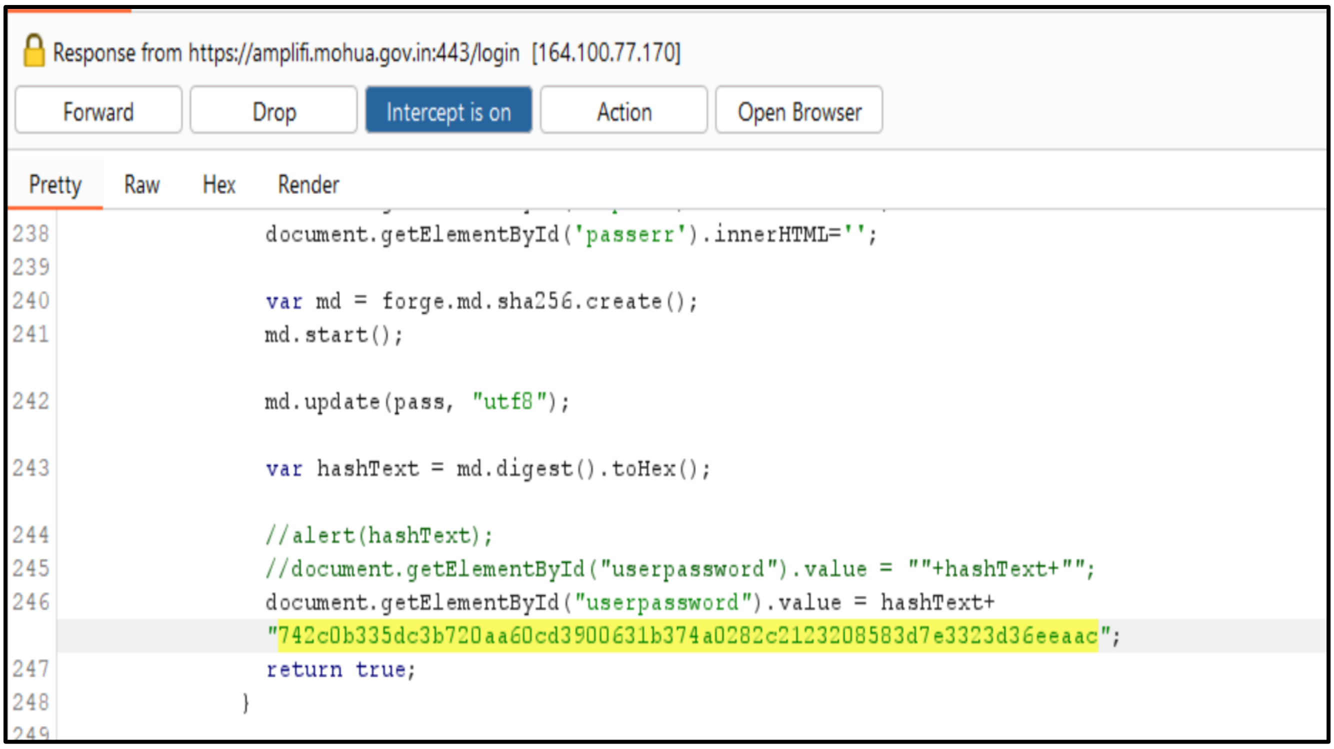

https://amplifi.mohua.gov.in/login
Ministry of Housing and Urban Affairs
Government of India
LOGIN
admin
●●●●●
QHDFZA
QHDFZA
Login

Step#2: The login button is clicked, and the request is being captured in an HTTP interceptor. It was observed that the application using simple SHA256 hashing algorithm appended with the salt value as shown below:



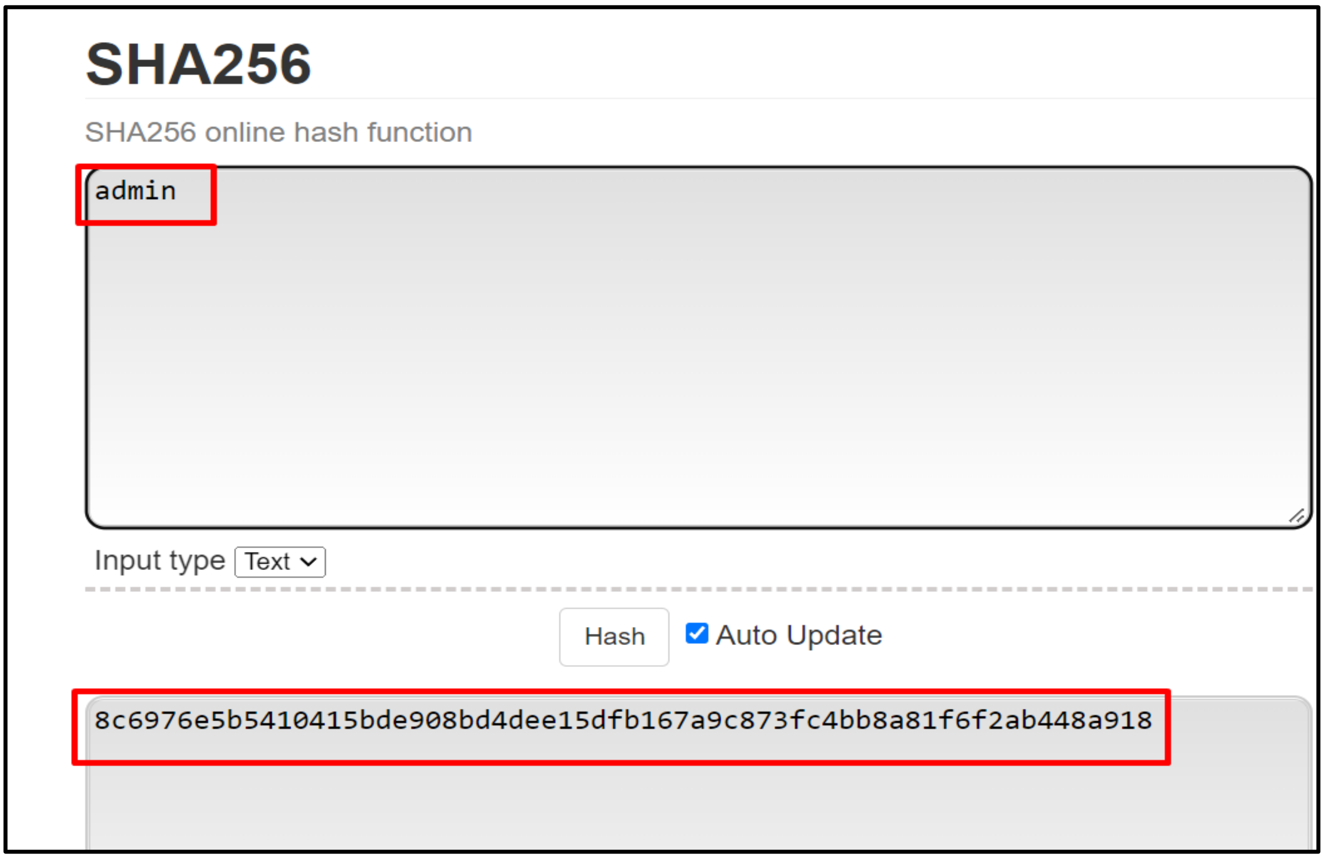
```
POST /login HTTP/1.1
Host: amplifi.mohua.gov.in
Cookie: PHPSESSID=i55o2k8ik4qa73lkuerrgc3626; csrf_cookie=671562d8b8393edbc6a6e15ca62f3880
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 251
Origin: https://amplifi.mohua.gov.in
Referer: https://amplifi.mohua.gov.in/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

csrf_token=671562d8b8393edbc6a6e15ca62f3880&loginAttempts=0&username=admin&userpassword=
8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918742c0b335dc3b720aa60cd3900631b374a0282c2123208583d7e3323d36eeaac&hide
=&captchacode=QHDFZA&loginBtn=
```

Step#3: When checked in response it was observed that the application using simple SHA256 hashing algorithm appended with the salt value as shown below:


Response from https://amplifi.mohua.gov.in:443/login [164.100.77.170]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
Render

```
                    document.getElementById('passerr').innerHTML='';

                    var md = forge.md.sha256.create();
                    md.start();

                    md.update(pass, "utf8");

                    var hashText = md.digest().toHex();

                    //alert(hashText);
                    //document.getElementById("userpassword").value = ""+hashText+"";
                    document.getElementById("userpassword").value = hashText+
                    "742c0b335dc3b720aa60cd3900631b374a0282c2123208583d7e3323d36eeaac";
                    return true;
                }
```

Step#4: The SHA256 hashed value of the password is shown below.


SHA256

SHA256 online hash function

admin

Input type: Text

```
8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
```

Same Vulnerability exists in following URL:

https://amplifi.mohua.gov.in/data

https://amplifi.mohua.gov.in/state/login

Recommendation(s):

1. Password and Sensitive data should travel in SHA256/512 or encrypted form respectively.
2. Password should be always hashed with random salt and salt should be unique for every request.
3. Salt should be generated at server side and properly validated.

2. Directory Listing

Incident URL: https://amplifi.mohua.gov.in/icons/.

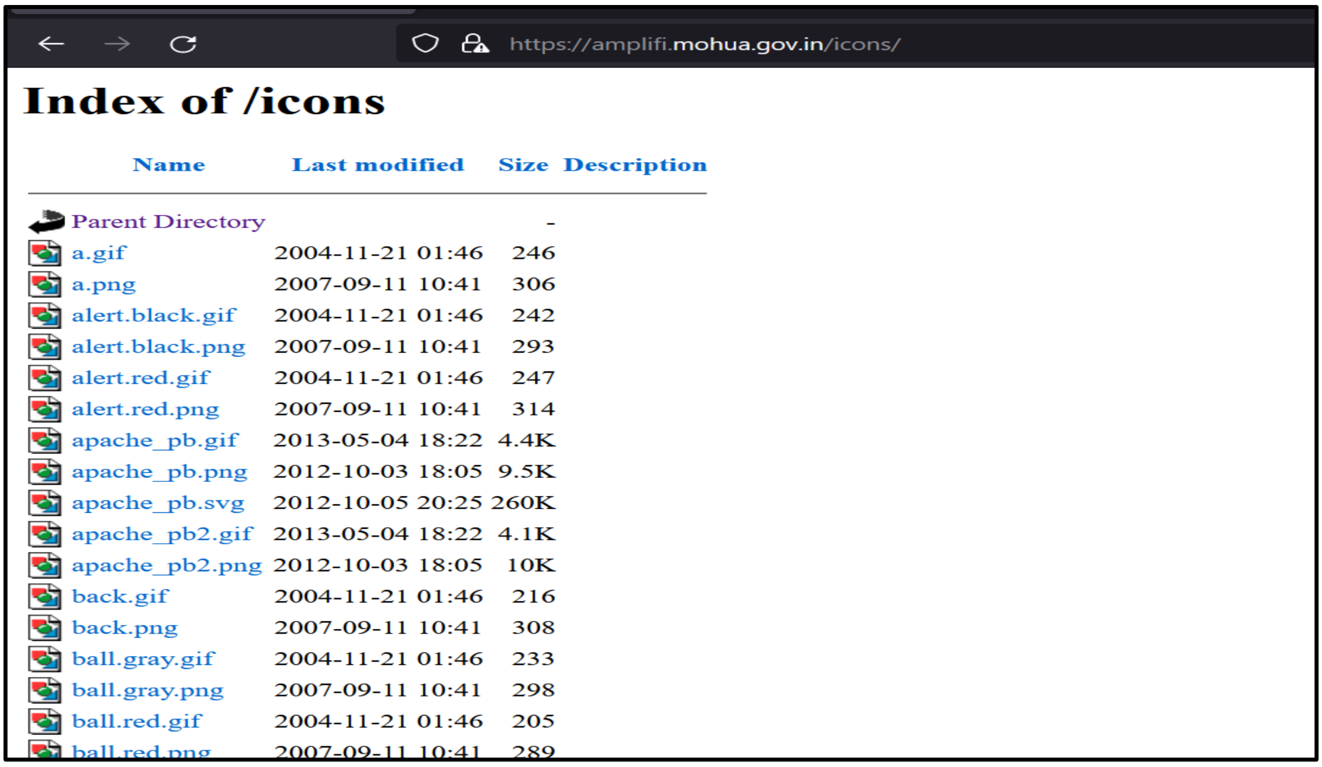
Description: An attacker can browse directories of the site and gain access to potentially sensitive data.

Impact: An attacker can gain access to sensitive data through directory listing.

Severity: High

How to Test:

Step#1: Upon navigating to the URL: https://amplifi.mohua.gov.in/icons/ the following page is shown:



https://amplifi.mohua.gov.in/icons/

Index of /icons

Name	Last modified	Size	Description
Parent Directory		-	
a.gif	2004-11-21 01:46	246	
a.png	2007-09-11 10:41	306	
alert.black.gif	2004-11-21 01:46	242	
alert.black.png	2007-09-11 10:41	293	
alert.red.gif	2004-11-21 01:46	247	
alert.red.png	2007-09-11 10:41	314	
apache_pb.gif	2013-05-04 18:22	4.4K	
apache_pb.png	2012-10-03 18:05	9.5K	
apache_pb.svg	2012-10-05 20:25	260K	
apache_pb2.gif	2013-05-04 18:22	4.1K	
apache_pb2.png	2012-10-03 18:05	10K	
back.gif	2004-11-21 01:46	216	
back.png	2007-09-11 10:41	308	
ball.gray.gif	2004-11-21 01:46	233	
ball.gray.png	2007-09-11 10:41	298	
ball.red.gif	2004-11-21 01:46	205	
ball.red.png	2007-09-11 10:41	289	

Recommendation(s):

1. Directory Listing should be disabled for all directories on the website.

3. Critical Resource Disclosure

Incident URL: https://amplifi.mohua.gov.in/mail.php

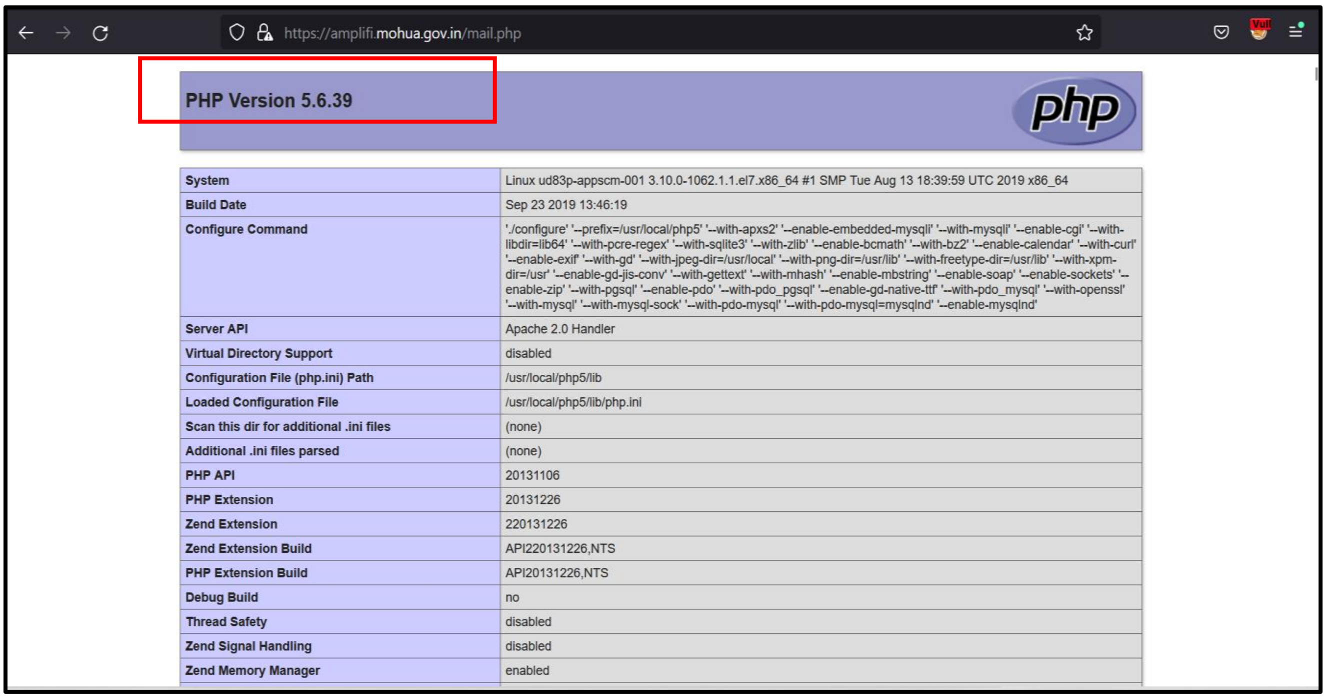
Description: An attacker can gain critical information from the critical resource disclosure of the application.

Impact: It allows an attacker to use the critical information to carry out known attacks for server.

Severity: High

How to Test:

Step#1: Upon entering the URL: https://amplifi.mohua.gov.in/mail.php the critical resource is disclosed as shown below:



PHP Version 5.6.39

System	Linux ud83p-appscm-001 3.10.0-1062.1.1.el7.x86_64 #1 SMP Tue Aug 13 18:39:59 UTC 2019 x86_64
Build Date	Sep 23 2019 13:46:19
Configure Command	'./configure' '--prefix=/usr/local/php5' '--with-apxs2' '--enable-embedded-mysqli' '--with-mysqli' '--enable-cgi' '--with-libdir=lib64' '--with-pcre-regex' '--with-sqlite3' '--with-zlib' '--enable-bcmath' '--with-bz2' '--enable-calendar' '--with-curl' '--enable-exif' '--with-gd' '--with-jpeg-dir=/usr/local' '--with-png-dir=/usr/lib' '--with-freetype-dir=/usr/lib' '--with-xpm-dir=/usr' '--enable-gd-jis-conv' '--with-gettext' '--with-mhash' '--enable-mbstring' '--enable-soap' '--enable-sockets' '--enable-zip' '--with-pgsql' '--enable-pdo' '--with-pdo_pgsql' '--enable-gd-native-ttf' '--with-pdo_mysql' '--with-openssl' '--with-mysql' '--with-mysql-sock' '--with-pdo-mysql' '--with-pdo-mysql=mysqlnd' '--enable-mysqlnd'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php5/lib
Loaded Configuration File	/usr/local/php5/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

Recommendation(s):

1. Application should not disclose the critical resources to the end users.

4. No CAPTCHA – Denial of Service Attack

Incident URL: https://amplifi.mohua.gov.in/ .

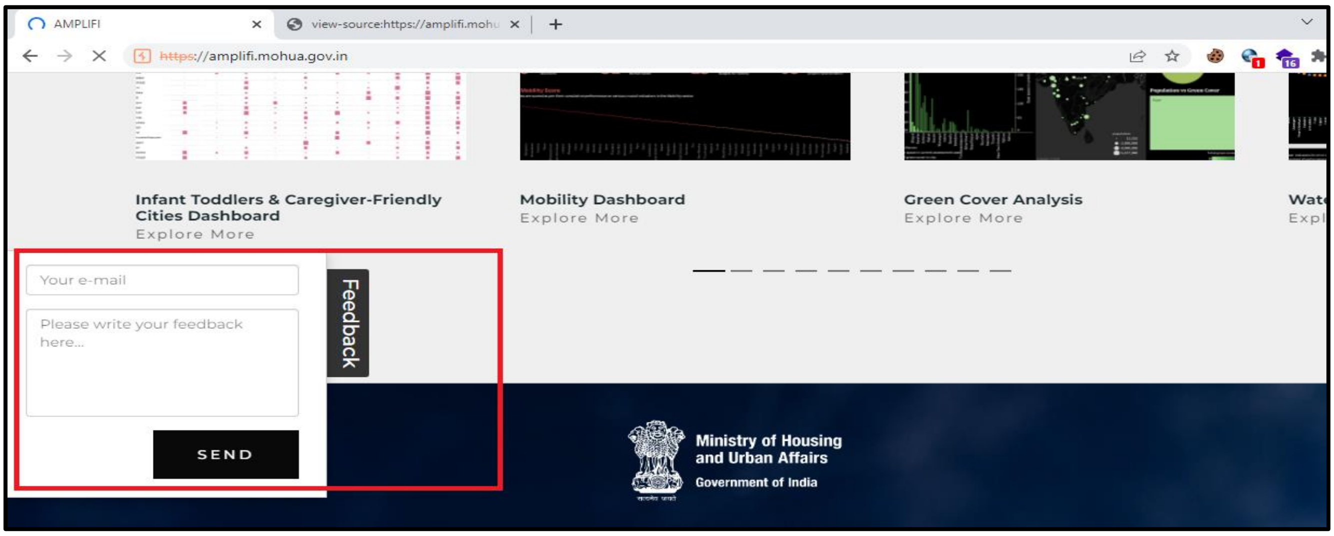
Description: An attacker over the internet can launch an automated denial of service attack against the Feedback page of the application as there is no CAPTCHA present.

Impact: An attacker over the internet can launch an automated denial of service attack against the application which can cause unavailability of the resources for genuine user.

Severity: High

How to Test:

Step#1: An attacker navigates to the 'Feedback' Page of the application at URL: https://amplifi.mohua.gov.in/ and observes that no CAPTCHA has been implemented:


AMPLIFI
view-source:https://amplifi.mohu
https://amplifi.mohua.gov.in
Infant Toddlers & Caregiver-Friendly Cities Dashboard
Explore More
Mobility Dashboard
Explore More
Green Cover Analysis
Explore More
Your e-mail
Please write your feedback here...
SEND
Feedback
Ministry of Housing and Urban Affairs
Government of India

Recommendation(s):

The application may restrict such attacks by implementing a CAPTCHA to ensure that no automated attack can be run.

CAPTCHA Guidelines:

a) CAPTCHA should always be an image.
b) CAPTCHA value should not travel from server to client side in clear text or any text format.
c) CAPTCHA should be randomly generated from the server and not from client side.
d) Strength of CAPTCHA: Minimum of 6 characters, Alpha-numeric and case sensitive.
e) After each incorrect user credential, the server should return the login page with a new CAPTCHA.

5. TLS/SSL Vulnerability

Incident URL: https://amplifi.mohua.gov.in/

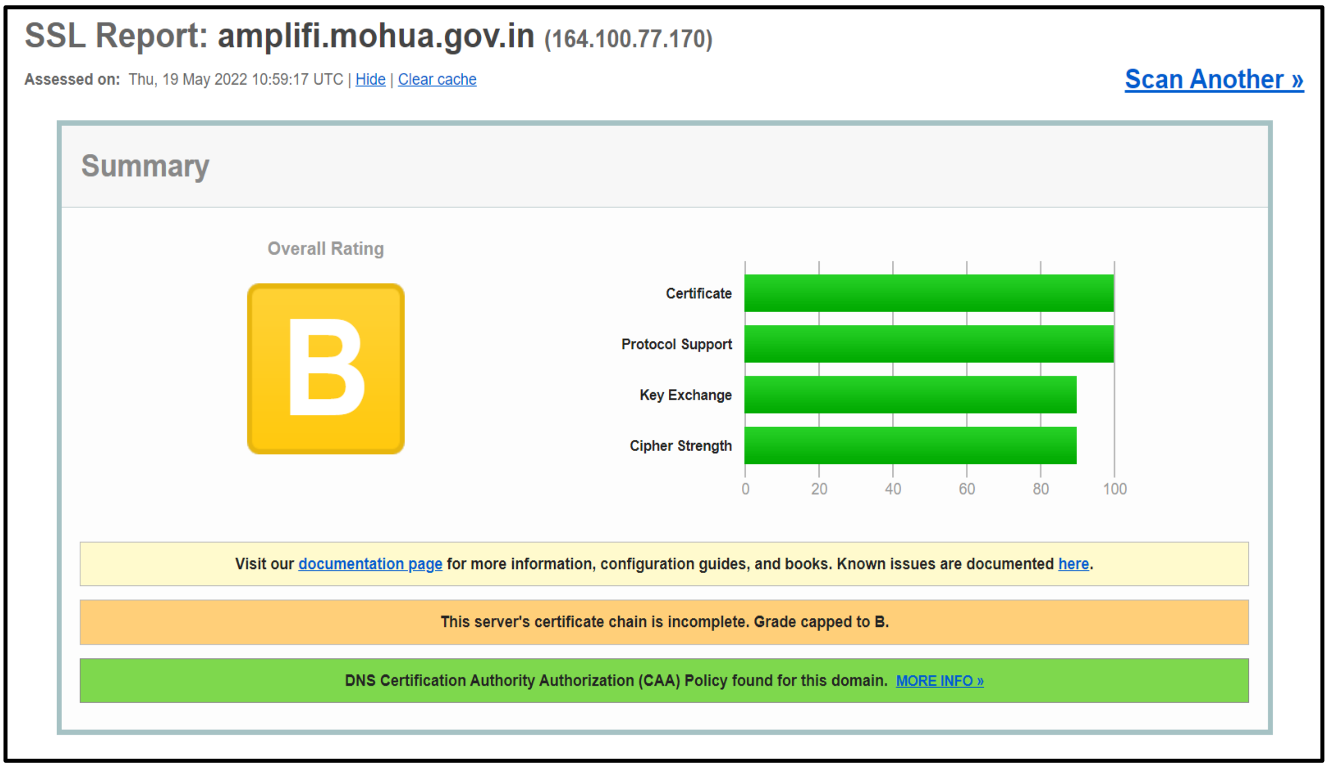
Description: The transport layer connection of the application is using weak cipher.

Impact: The application is using weak cipher which leads an attacker to perform man-in-the middle attacks.

Severity: Low

How to Test:

Step#1: The following screenshots of the SSL test for the domain: https://amplifi.mohua.gov.in/ confirm that the application supports weak cipher as shown below:


SSL Report: amplifi.mohua.gov.in (164.100.77.170)

Assessed on: Thu, 19 May 2022 10:59:17 UTC | Hide | Clear cache

Scan Another »

Summary

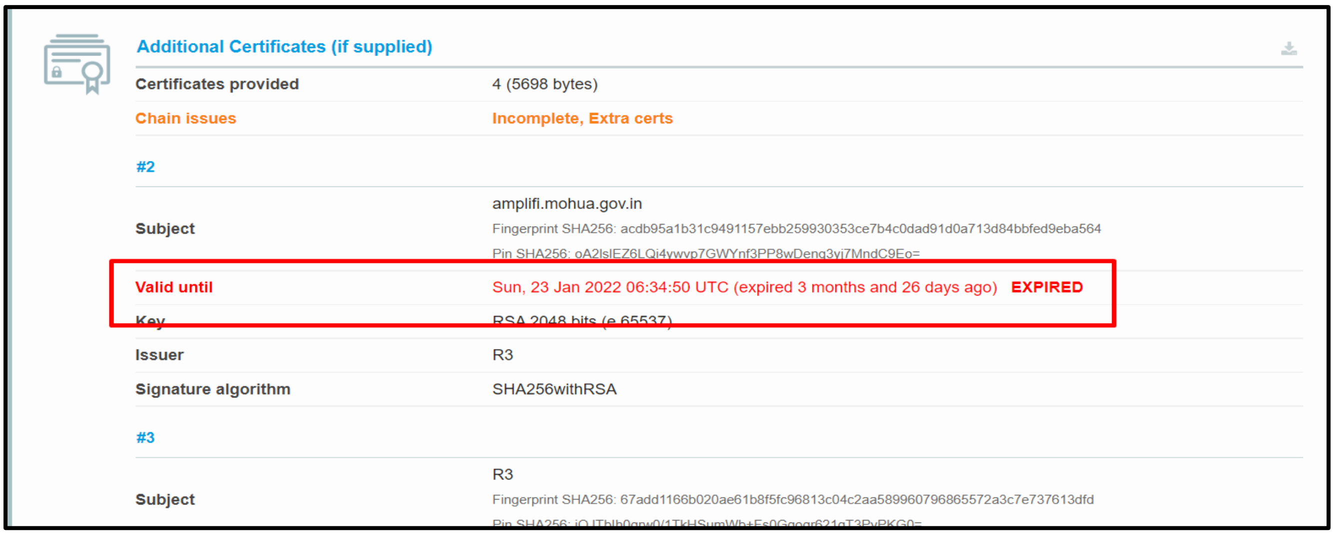
Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate chain is incomplete. Grade capped to B.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »


Additional Certificates (if supplied)

Certificates provided	4 (5698 bytes)
Chain issues	Incomplete, Extra certs
#2	
Subject	amplifi.mohua.gov.in Fingerprint SHA256: acdb95a1b31c9491157ebb259930353ce7b4c0dad91d0a713d84bbfed9eba564 Pin SHA256: oA2lslEZ6LQi4ywvp7GWYnf3PP8wDenq3yj7MndC9Eo=
Valid until	Sun, 23 Jan 2022 06:34:50 UTC (expired 3 months and 26 days ago) EXPIRED
Key	RSA 2048 bits (e 65537)
Issuer	R3
Signature algorithm	SHA256withRSA
#3	
Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=

Recommendation(s):

1. Disable support for all weak/ insecure protocols and completely support TLS 1.2 or greater.
2. Remove all weak and insecure ciphers.

6. Insecure Cookie Attributes

Incident URL: https://amplifi.mohua.gov.in/

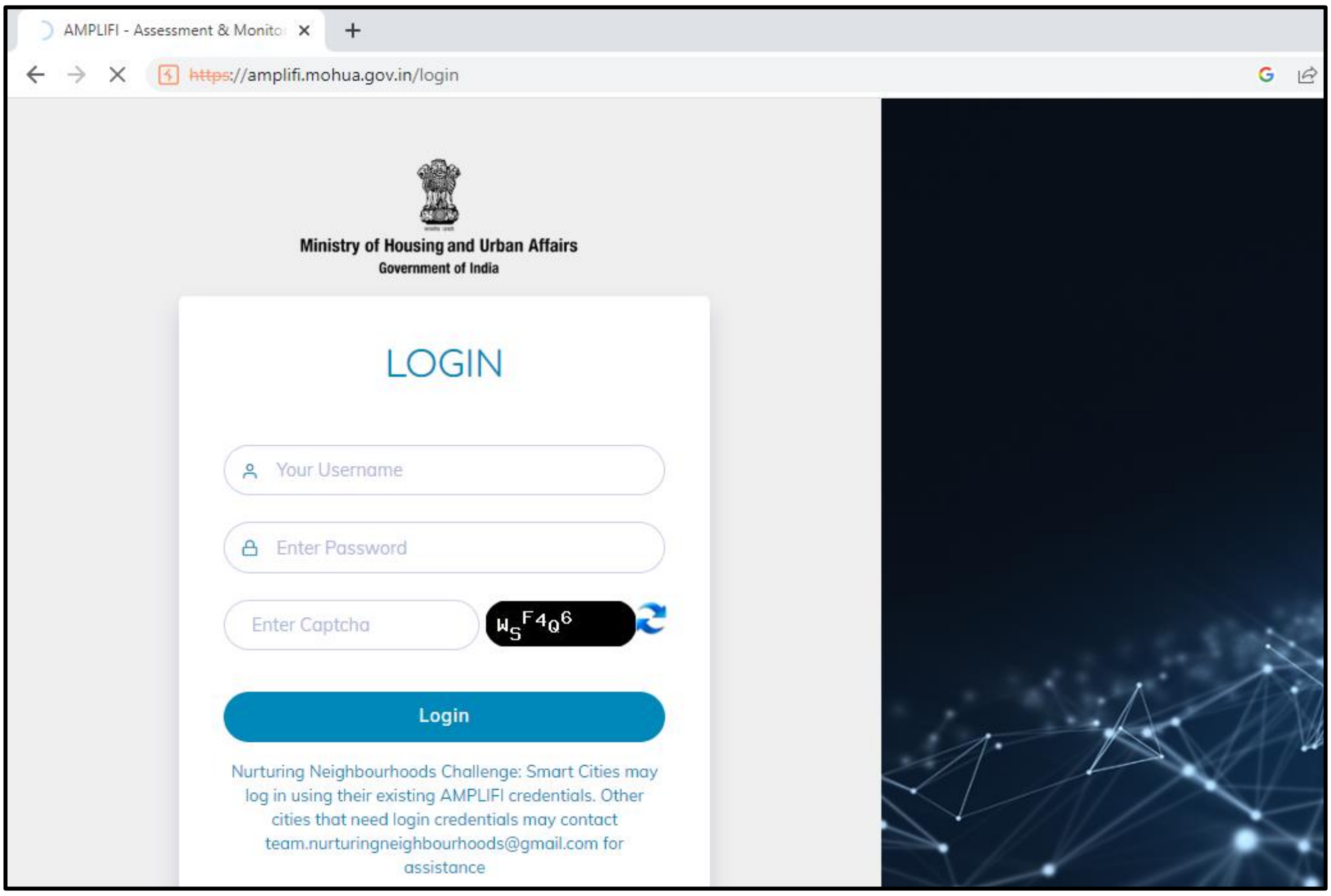
Description: The application has not implemented 'Domain' and 'Secure' cookie attributes and 'Path' has been improperly set to root.

Impact: This vulnerability allows an attacker to steal sensitive information like session token and allows launching further attacks.

Severity: Low

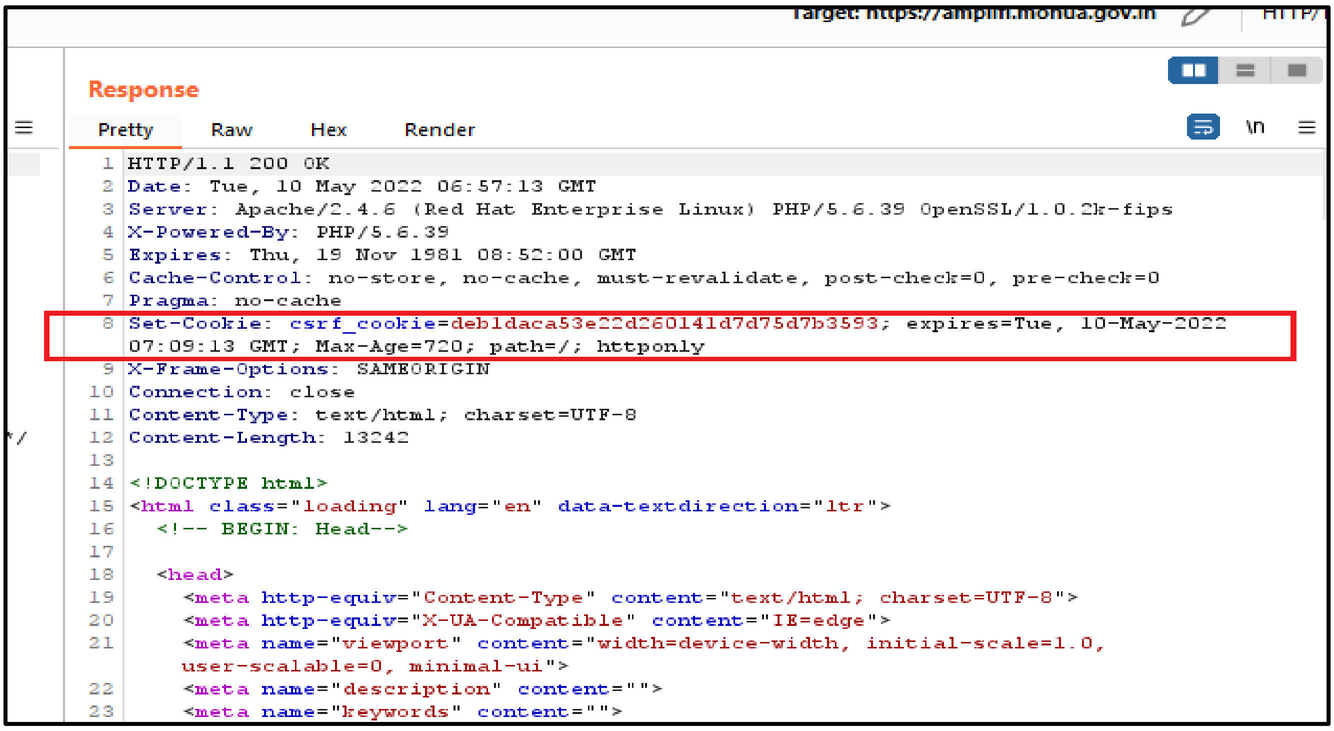
How to Test:

Step#1: An attacker navigates to the home page of the application at URL: https://amplifi.mohua.gov.in/ .


AMPLIFI - Assessment & Monito
https://amplifi.mohua.gov.in/login
Ministry of Housing and Urban Affairs
Government of India
LOGIN
Your Username
Enter Password
Enter Captcha
Login

Nurturing Neighbourhoods Challenge: Smart Cities may log in using their existing AMPLIFI credentials. Other cities that need login credentials may contact team.nurturingneighbourhoods@gmail.com for assistance

Step#2: Upon intercepting the response, it was observed that domain and secure cookie attribute is not used, and path is set to root.



```
HTTP/1.1 200 OK
Date: Tue, 10 May 2022 06:57:13 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.6.39 OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.39
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: csrf_cookie=deb1daca53e22d260141d7d75d7b3593; expires=Tue, 10-May-2022
07:09:13 GMT; Max-Age=720; path=/; httponly
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 13242

<!DOCTYPE html>
<html class="loading" lang="en" data-textdirection="ltr">
  <!-- BEGIN: Head-->

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0,
    user-scalable=0, minimal-ui">
    <meta name="description" content="">
    <meta name="keywords" content="">
```

Recommendation(s):

1. 'Path' should not set to root Instead a sub folder path should be used.
2. Also, the "Domain" cookie attribute should be set as restrictive as possible and the complete application domain should be provided for this attribute.
3. The application should set 'Domain', 'HTTP Only' & 'Secure' cookie attributes for both pre authentication Session ID and post authentication Session ID in the application.

7. Insecure HTTP Method

Incident URL: https://amplifi.mohua.gov.in/

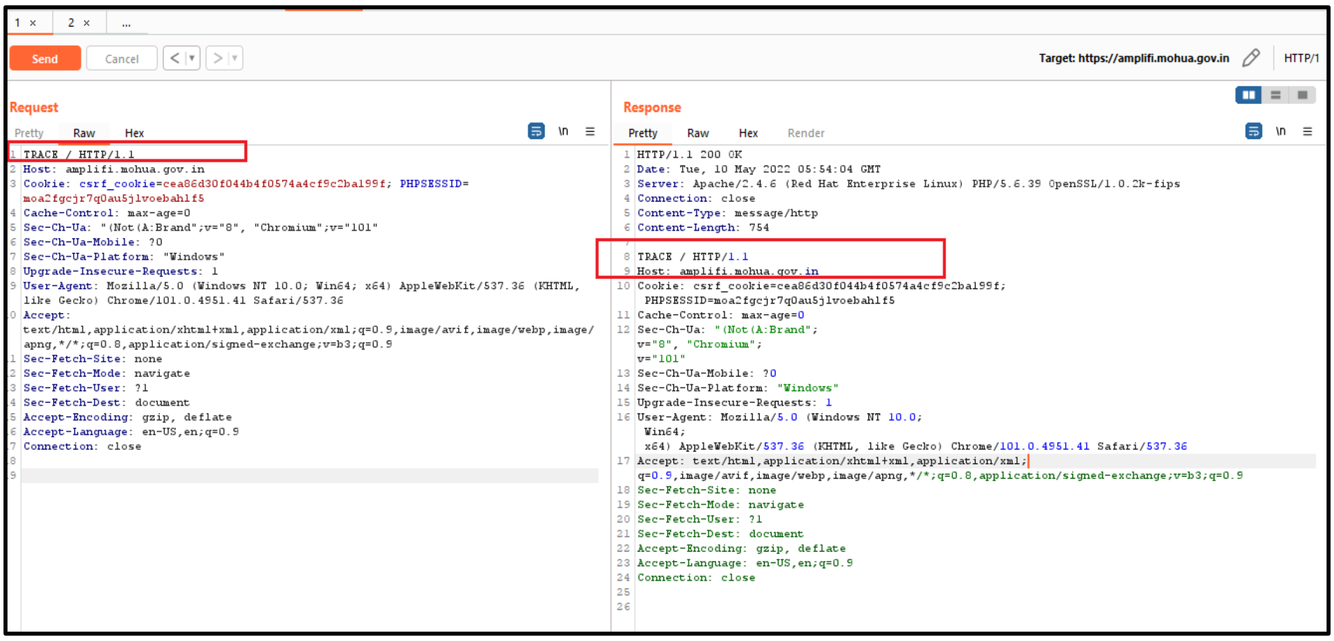
Description: The insecure 'TRACE' HTTP method is enabled in the application.

Impact: It allows an attacker to perform further attacks based on the HTTP methods which are enabled.

Severity: Low

How to Test:

Step#1: An attacker browses the page of the web services at URL: https://amplifi.mohua.gov.in/, intercepts in the HTTP interceptor and send a **"TRACE"** request to the server as shown below.



```
TRACE / HTTP/1.1
Host: amplifi.mohua.gov.in
Cookie: csrf_cookie=cea86d30f044b4f0574a4cf9c2ba199f; PHPSESSID=
moa2fgcjr7q0au5jlvoebahlf5
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="101"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.41 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 10 May 2022 05:54:04 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.6.39 OpenSSL/1.0.2k-fips
Connection: close
Content-Type: message/http
Content-Length: 754

TRACE / HTTP/1.1
Host: amplifi.mohua.gov.in
Cookie: csrf_cookie=cea86d30f044b4f0574a4cf9c2ba199f;
 PHPSESSID=moa2fgcjr7q0au5jlvoebahlf5
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand";
v="8", "Chromium";
v="101"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
 Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Recommendation(s):

1. It is recommended to allow only GET, POST and HEAD HTTP methods.

8. Information Disclosure

Incident URL: https://amplifi.mohua.gov.in/ .

Description: An attacker can gain server-side information like server and framework name and version from the HTTP response of the application.

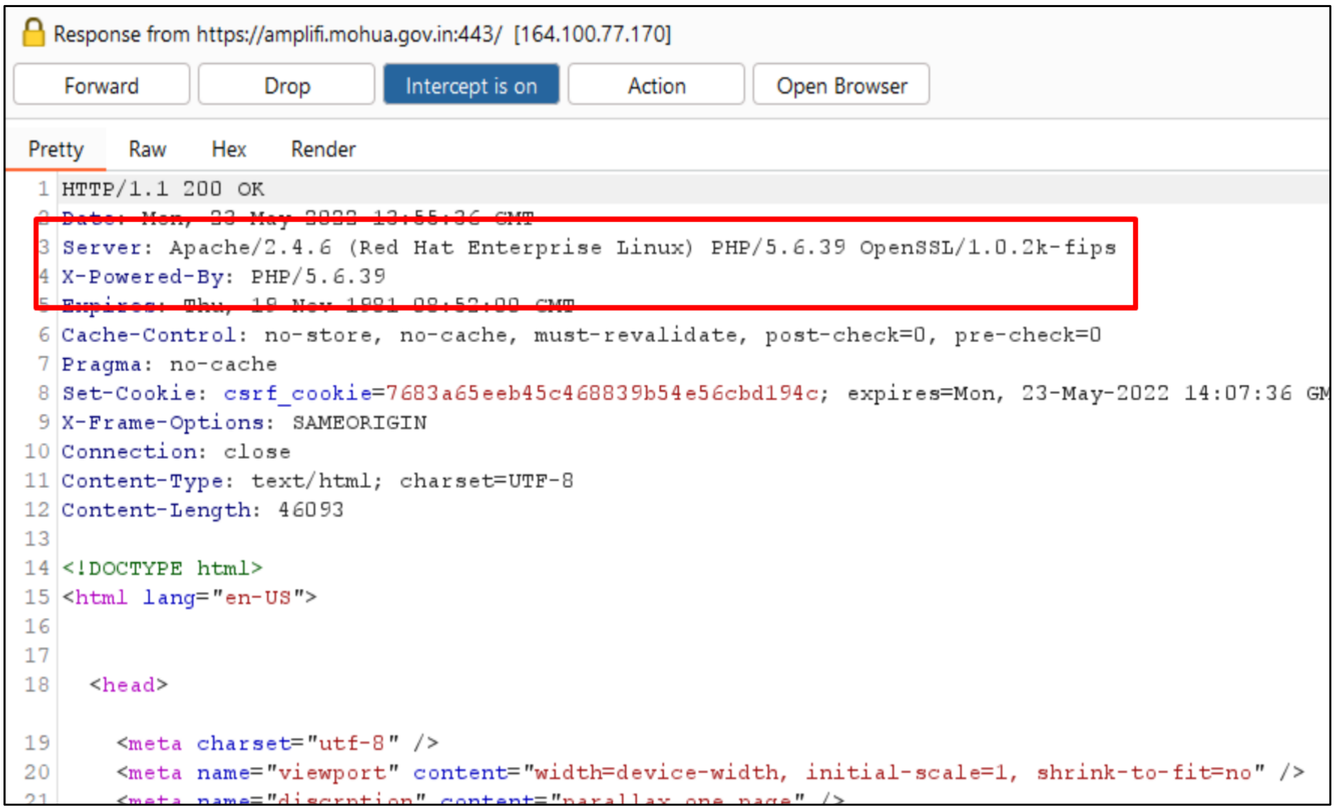
Impact: An attacker can gain server-side information like server name from the HTTP response of the application that may allow an attacker to carry out specific known targeted attacks for remote server.

Severity: Low

How to Test:

Enter the URL: https://amplifi.mohua.gov.in/.

Instance#1: The below response which was captured in an HTTP interceptor shows that the application discloses server and framework name and versions.


Response from https://amplifi.mohua.gov.in:443/ [164.100.77.170]

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2022 13:55:36 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.6.39 OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.39
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: csrf_cookie=7683a65eeb45c468839b54e56cbd194c; expires=Mon, 23-May-2022 14:07:36 GM
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46093

<!DOCTYPE html>
<html lang="en-US">


  <head>

    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
    <meta name="discrption" content="parallax one page" />
```

Recommendation(s):

1. The application should not display server and framework related information to the application users.
2. The server banner must be removed from the server.

9. Using Components with known Vulnerabilities

Incident URL: https://amplifi.mohua.gov.in/assets/js/jquery
https://amplifi.mohua.gov.in/

Description: The application is using vulnerable version of jQuery and Apache (3.3.1/3.3.6)

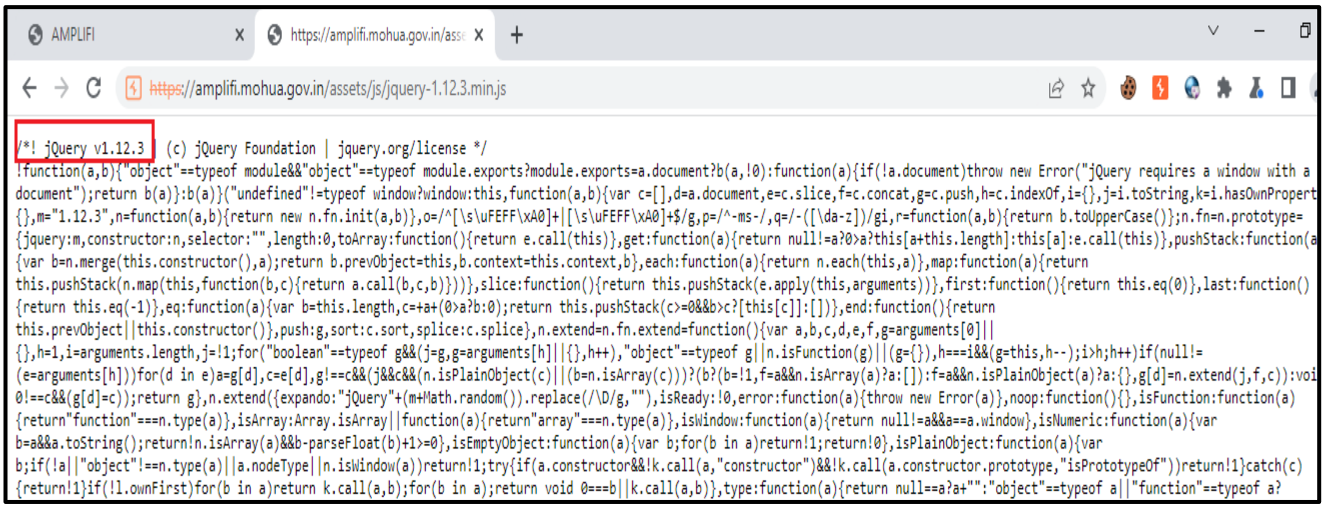
Impact: The application is using vulnerable versions of jQuery and Apache because of which an attacker can possibly exploit already known vulnerabilities.

Severity: Low

How to Test:

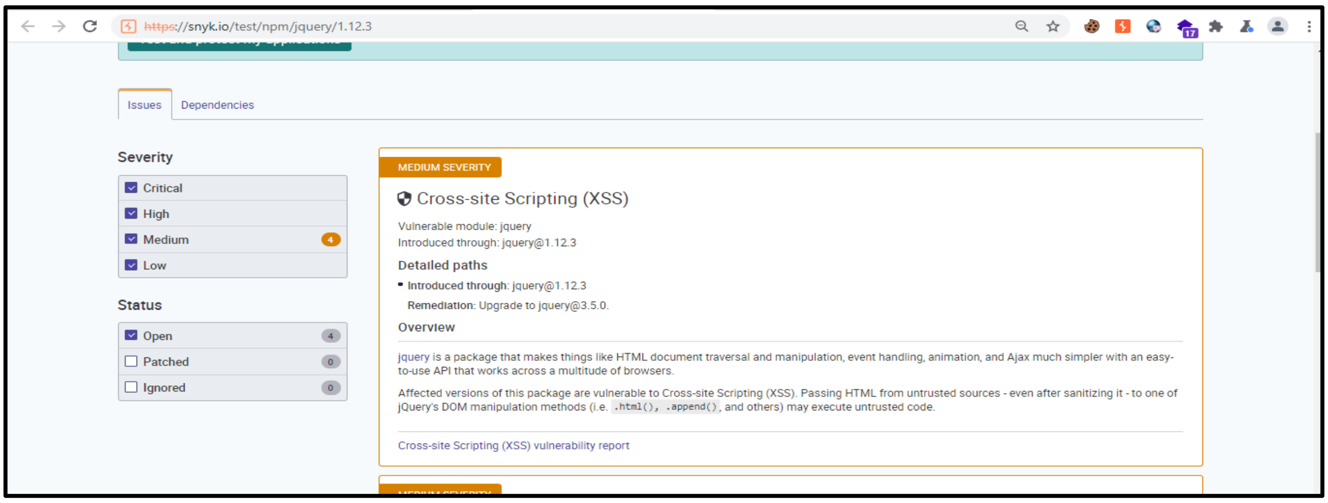
Instance#1: jQuery v1.12.3

Step#1: A malicious user navigates to the view source page of the application at URL:view-source: https://amplifi.mohua.gov.in/assets/js/jquery and observes that the application is using vulnerable version of jQuery as shown below:


AMPLIFI
https://amplifi.mohua.gov.in/asse
https://amplifi.mohua.gov.in/assets/js/jquery-1.12.3.min.js

```
/*! jQuery v1.12.3 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a
document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnPropert
{},m="1.12.3",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype=
{jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a
{var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return
this.pushStack(n.map(this,function(b,c){return a.call(b,c,b)}))},slice:function(){return this.pushStack(e.apply(this,arguments))},first:function(){return this.eq(0)},last:function()
{return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor()},push:g,sort:c.sort,splice:c.splice},n.extend=n.fn.extend=function(){var a,b,c,d,e,f,g=arguments[0]||
{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&(j=g,g=arguments[h]||{},h++),"object"==typeof g||n.isFunction(g)||(g={}),h===i&&(g=this,h--);i>h;h++)if(null!=
(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(n.isPlainObject(c)||(b=n.isArray(c)))?(b?(b=!1,f=a&&n.isArray(a)?a:[]):f=a&&n.isPlainObject(a)?a:{},g[d]=n.extend(j,f,c)):voi
0!==c&&(g[d]=c));return g},n.extend({expando:"jQuery"+(m+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function(){},isFunction:function(a)
{return"function"===n.type(a)},isArray:Array.isArray||function(a){return"array"===n.type(a)},isWindow:function(a){return null!=a&&a==a.window},isNumeric:function(a){var
b=a&&a.toString();return!n.isArray(a)&&b-parseFloat(b)+1>=0},isEmptyObject:function(a){var b;for(b in a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==n.type(a)||a.nodeType||n.isWindow(a))return!1;try{if(a.constructor&&!k.call(a,"constructor")&&!k.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c)
{return!1}if(!l.ownFirst)for(b in a)return k.call(a,b);for(b in a);return void 0===b||k.call(a,b)},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof a?
```

Step 2: The attacker checks for the 'synk' details for the same i.e., **'jQuery v1.12.3'** and finds that the framework version is vulnerable.



https://snyk.io/test/npm/jquery/1.12.3

Issues | Dependencies

Severity
- ☑ Critical
- ☑ High
- ☑ Medium 4
- ☑ Low

Status
- ☑ Open 4
- ☐ Patched 0
- ☐ Ignored 0

MEDIUM SEVERITY

Cross-site Scripting (XSS)

Vulnerable module: jquery
Introduced through: jquery@1.12.3

Detailed paths
- Introduced through: jquery@1.12.3
  Remediation: Upgrade to jquery@3.5.0.

Overview

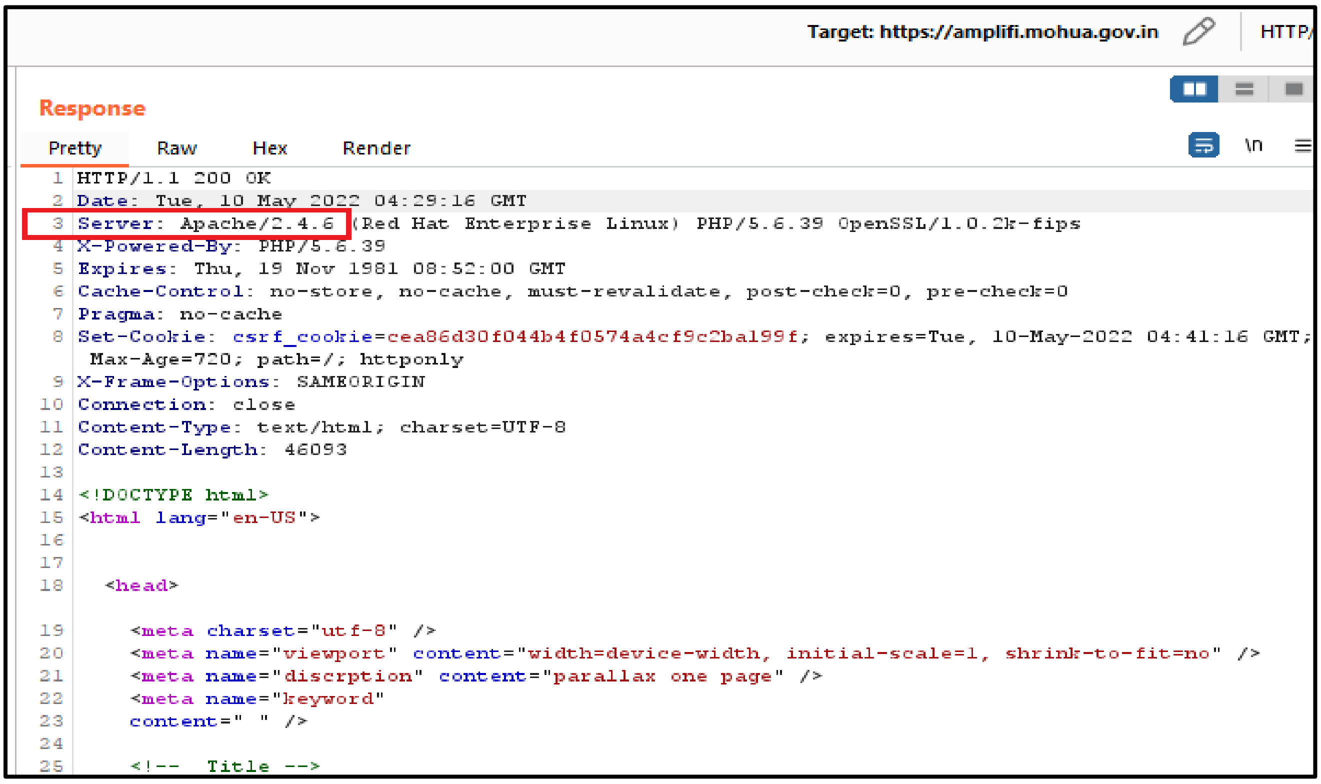
jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS). Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html(), .append()`, and others) may execute untrusted code.

Cross-site Scripting (XSS) vulnerability report

Instance#2: Apache 2.4.6

Step#1: A malicious user navigates to the view source page of the application at URL: https://amplifi.mohua.gov.in/ and observes that the application is using vulnerable version of Apache 2.4.6 as shown below:



Target: https://amplifi.mohua.gov.in

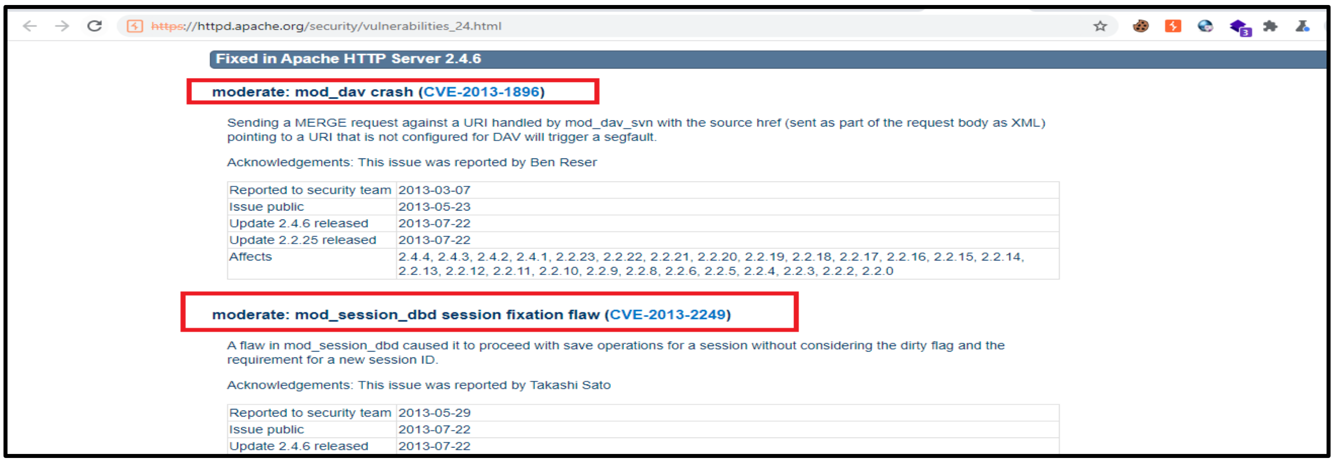
Response

Pretty | Raw | Hex | Render

```
HTTP/1.1 200 OK
Date: Tue, 10 May 2022 04:29:16 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.6.39 OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.39
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: csrf_cookie=cea86d30f044b4f0574a4cf9c2ba199f; expires=Tue, 10-May-2022 04:41:16 GMT;
 Max-Age=720; path=/; httponly
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46093

<!DOCTYPE html>
<html lang="en-US">


  <head>

    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
    <meta name="discrption" content="parallax one page" />
    <meta name="keyword"
    content=" " />

    <!-- Title -->
```

Step 2:

The attacker checks for the 'cve' details for the same i.e., 'Apache 2.4.6' and finds that the server version is vulnerable.



https://httpd.apache.org/security/vulnerabilities_24.html

Fixed in Apache HTTP Server 2.4.6

moderate: mod_dav crash (CVE-2013-1896)

Sending a MERGE request against a URI handled by mod_dav_svn with the source href (sent as part of the request body as XML) pointing to a URI that is not configured for DAV will trigger a segfault.

Acknowledgements: This issue was reported by Ben Reser

Reported to security team	2013-03-07
Issue public	2013-05-23
Update 2.4.6 released	2013-07-22
Update 2.2.25 released	2013-07-22
Affects	2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

moderate: mod_session_dbd session fixation flaw (CVE-2013-2249)

A flaw in mod_session_dbd caused it to proceed with save operations for a session without considering the dirty flag and the requirement for a new session ID.

Acknowledgements: This issue was reported by Takashi Sato

Reported to security team	2013-05-29
Issue public	2013-07-22
Update 2.4.6 released	2013-07-22

Recommendation(s):

1. The application must use the latest stable version of framework for jQuery and Apache or patch and update the components on regular basis.

10. Default Server Page Accessible

Incident URL: https://amplifi.mohua.gov.in/manual/

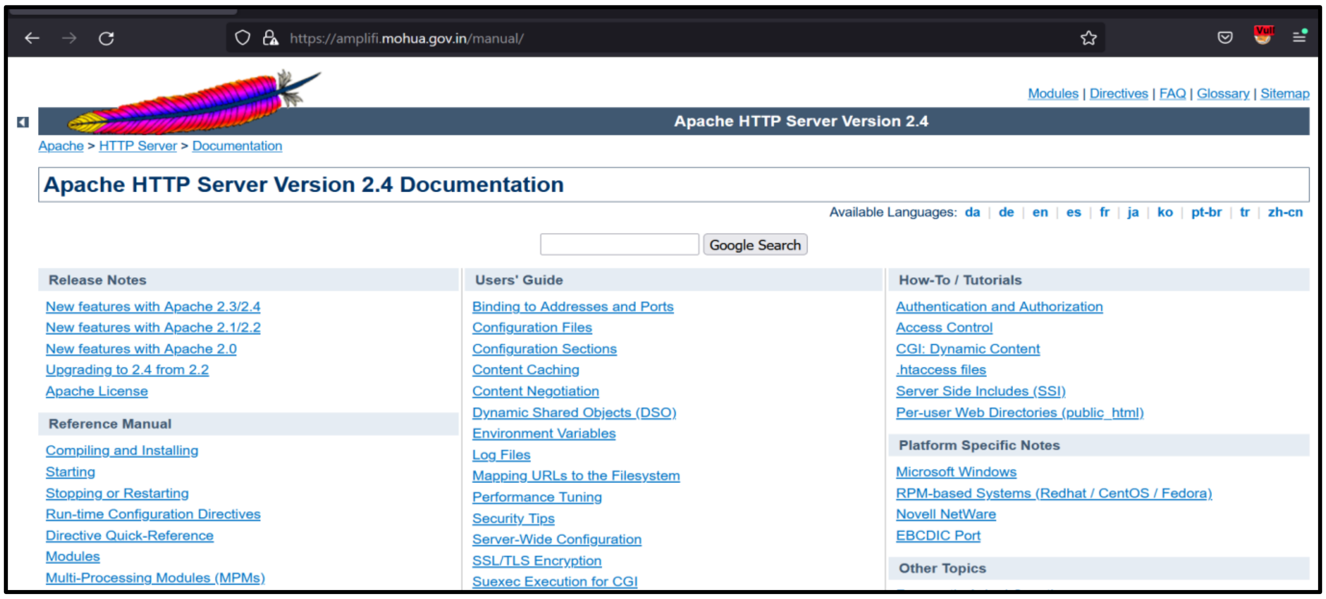
Description: The Default Server Administrative page is accessible over the internet.

Impact: An attacker can access the server management console and can gain unauthorized access to application and configurations controls.

Severity: Low

How to Test:

Step#1: On navigating the following URL: https://amplifi.mohua.gov.in/manual/, the default server administrative page is accessible.



https://amplifi.mohua.gov.in/manual/

Modules | Directives | FAQ | Glossary | Sitemap

Apache HTTP Server Version 2.4

Apache > HTTP Server > Documentation

Apache HTTP Server Version 2.4 Documentation

Available Languages: da | de | en | es | fr | ja | ko | pt-br | tr | zh-cn

Google Search

Release Notes
- New features with Apache 2.3/2.4
- New features with Apache 2.1/2.2
- New features with Apache 2.0
- Upgrading to 2.4 from 2.2
- Apache License

Reference Manual
- Compiling and Installing
- Starting
- Stopping or Restarting
- Run-time Configuration Directives
- Directive Quick-Reference
- Modules
- Multi-Processing Modules (MPMs)

Users' Guide
- Binding to Addresses and Ports
- Configuration Files
- Configuration Sections
- Content Caching
- Content Negotiation
- Dynamic Shared Objects (DSO)
- Environment Variables
- Log Files
- Mapping URLs to the Filesystem
- Performance Tuning
- Security Tips
- Server-Wide Configuration
- SSL/TLS Encryption
- Suexec Execution for CGI

How-To / Tutorials
- Authentication and Authorization
- Access Control
- CGI: Dynamic Content
- .htaccess files
- Server Side Includes (SSI)
- Per-user Web Directories (public_html)

Platform Specific Notes
- Microsoft Windows
- RPM-based Systems (Redhat / CentOS / Fedora)
- Novell NetWare
- EBCDIC Port

Other Topics

Recommendation(s):

1. It is recommended that the Default Server page should be restricted and should not be accessible over the internet.
2. It should be IP restricted for the authorized individuals only.

Note: Vulnerabilities should be patched throughout the website.