11/20/2020

Web Application Security Audit Report
https://www.bimastreet.com/

Credentials-

1) Admin Role -

User id - bms@gmail.com
Password - BMS@4321

2) SOP Role -

User id -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

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

Item	Company Description
Author	Recon Business Advisory Pvt ltd.
Auditor Name	Ashutosh Sharma
Reviewed By	Rohit Kumar

Table of Contents

1. Executive Summary

Recon Business Advisory Pvt. Ltd. carried out Web Application security assessment of the following website **17th November 2020 to 20th 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
Password - BMS@4321

2) SOP Role -

User id -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	**Safe**	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 *Standard* or *Destructive* scan/s.
2	**Standard**	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	**Destructive**	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

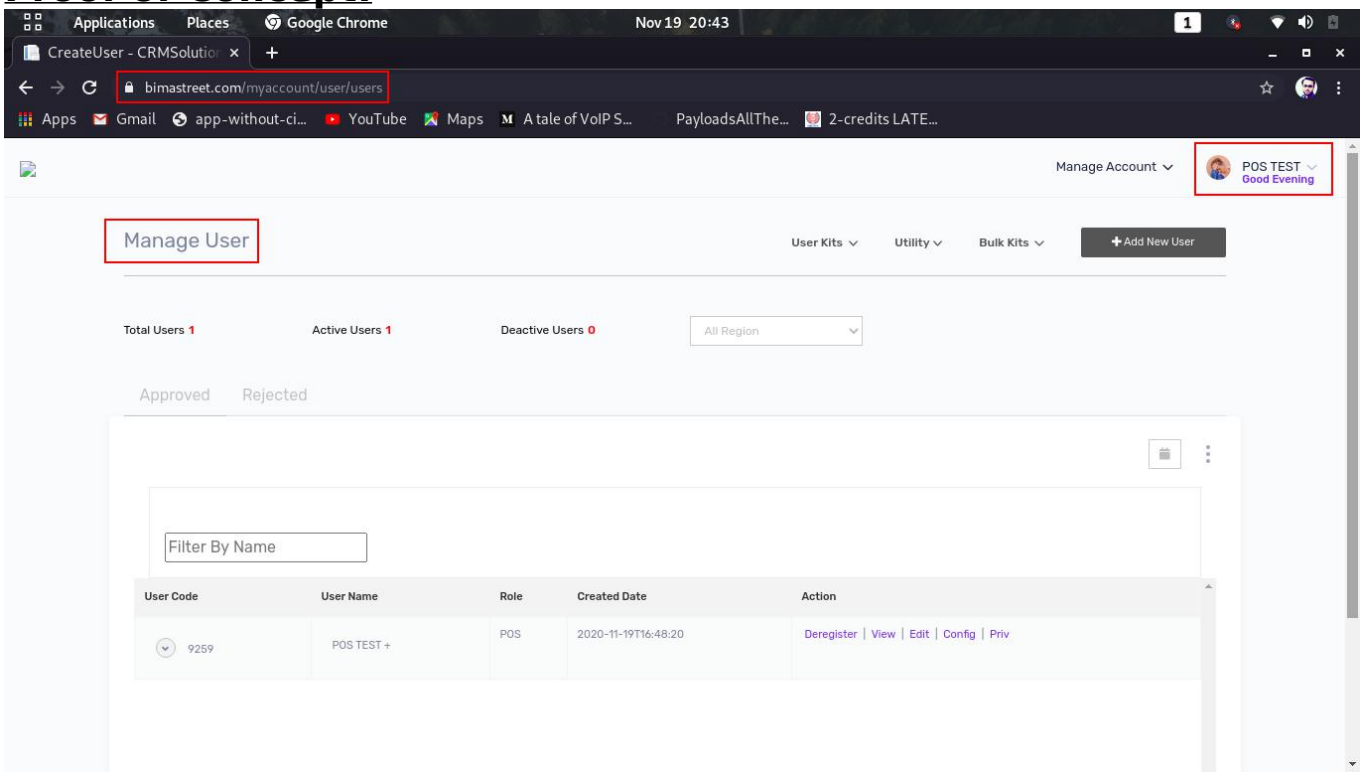
10.1 Privilege Escalation:

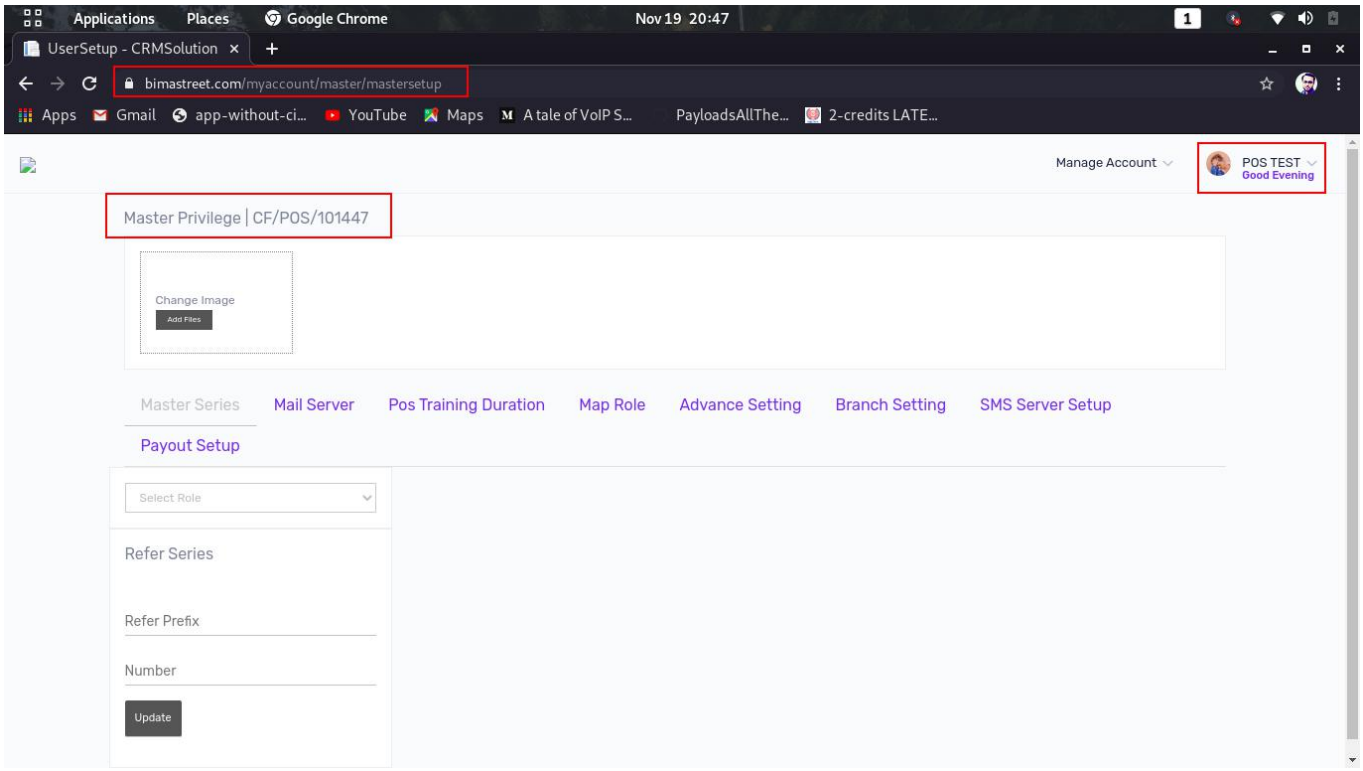
Name of Vulnerability	Privilege Escalation
URL	https://www.bimastreet.com/myaccount/user/users https://www.bimastreet.com/myaccount/master/mastersetup https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup https://www.bimastreet.com/myaccount/Business/MissingPolicy https://www.bimastreet.com/myaccount/products/renewals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

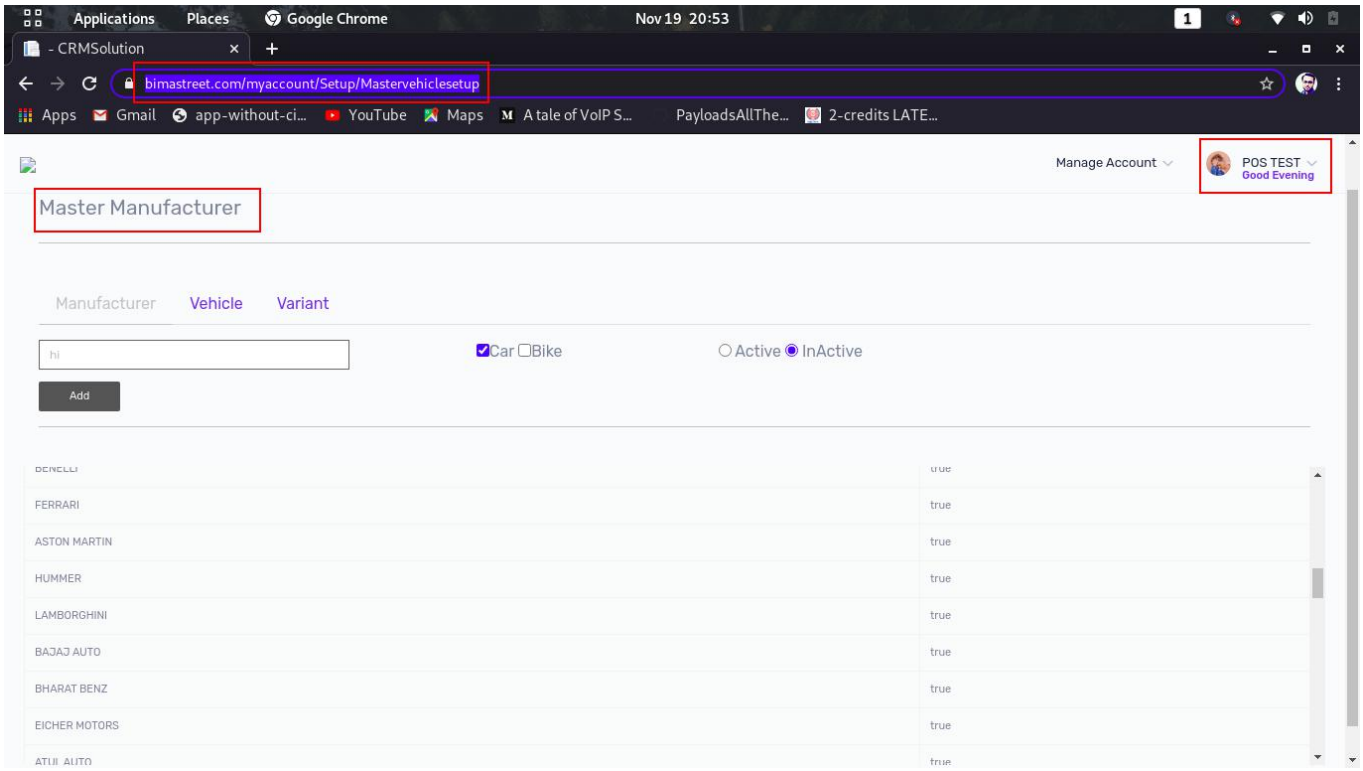
Description:

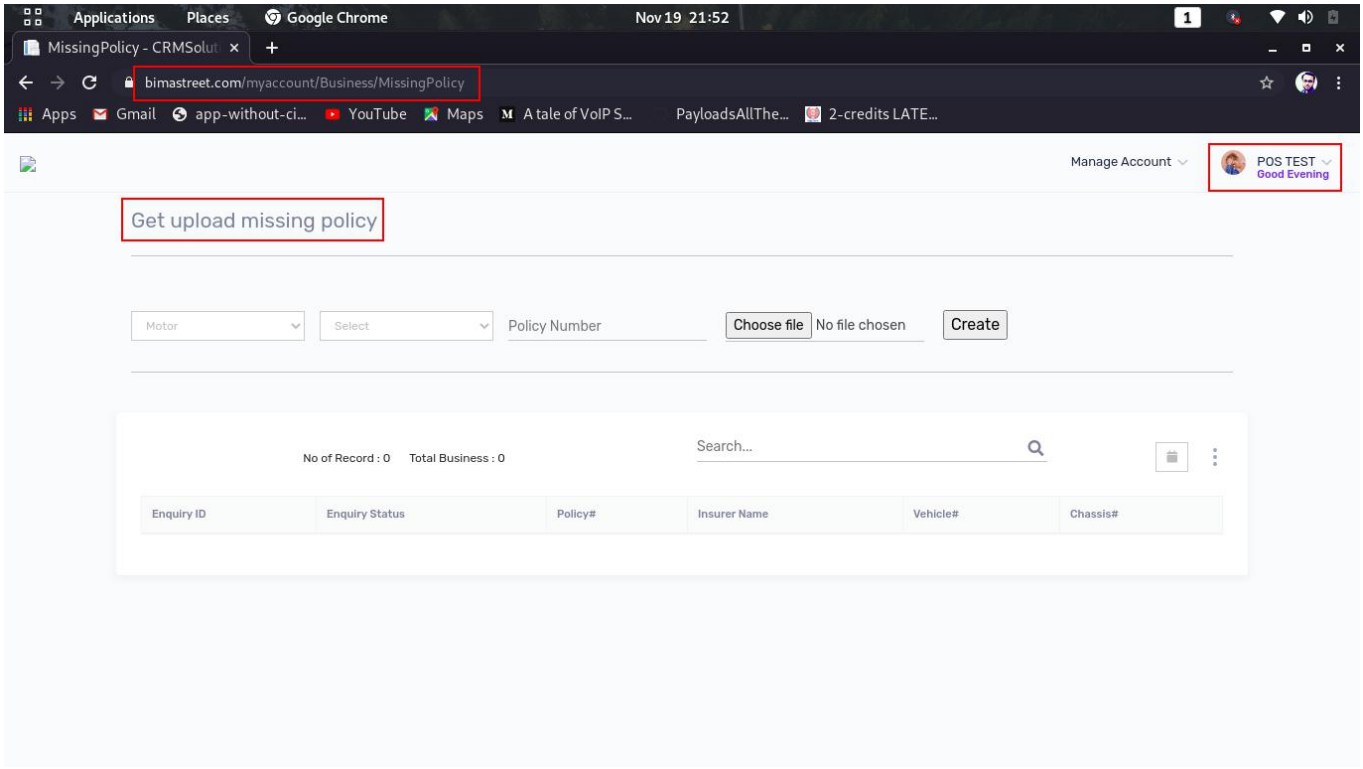
Privilege escalation, in simple words, means getting privileges to access something that should not be accessible. Attackers use various privilege escalation techniques to access unauthorized resources. For web application security, privilege escalation is an important concern because web intrusions 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.

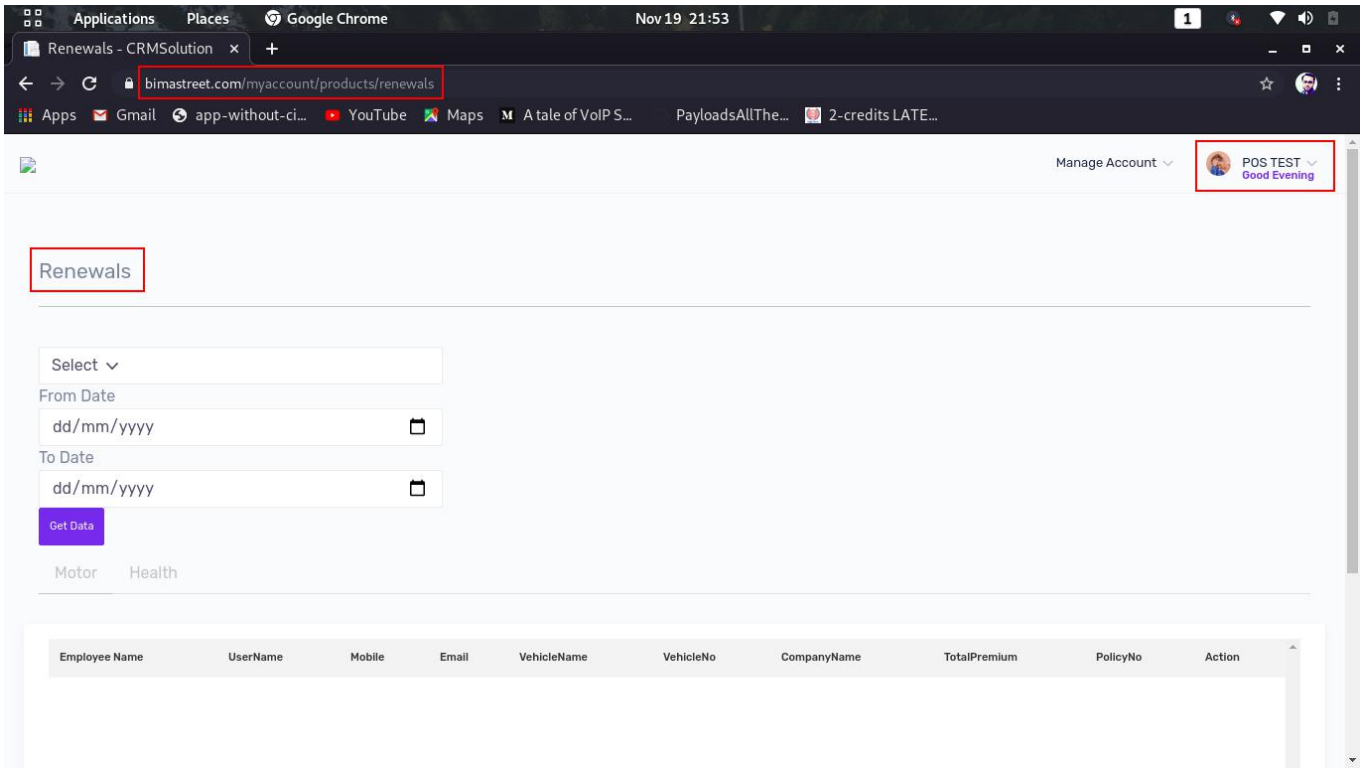
Proof of Concept:

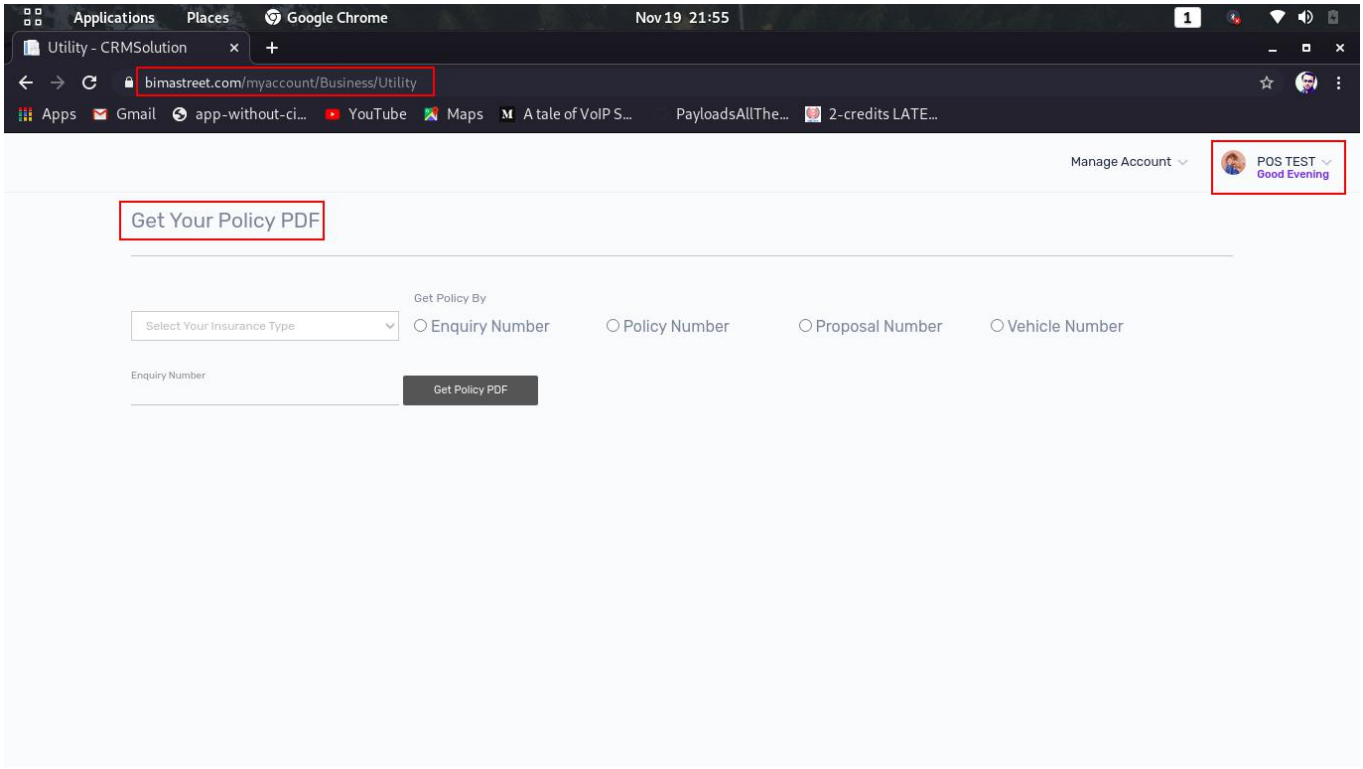


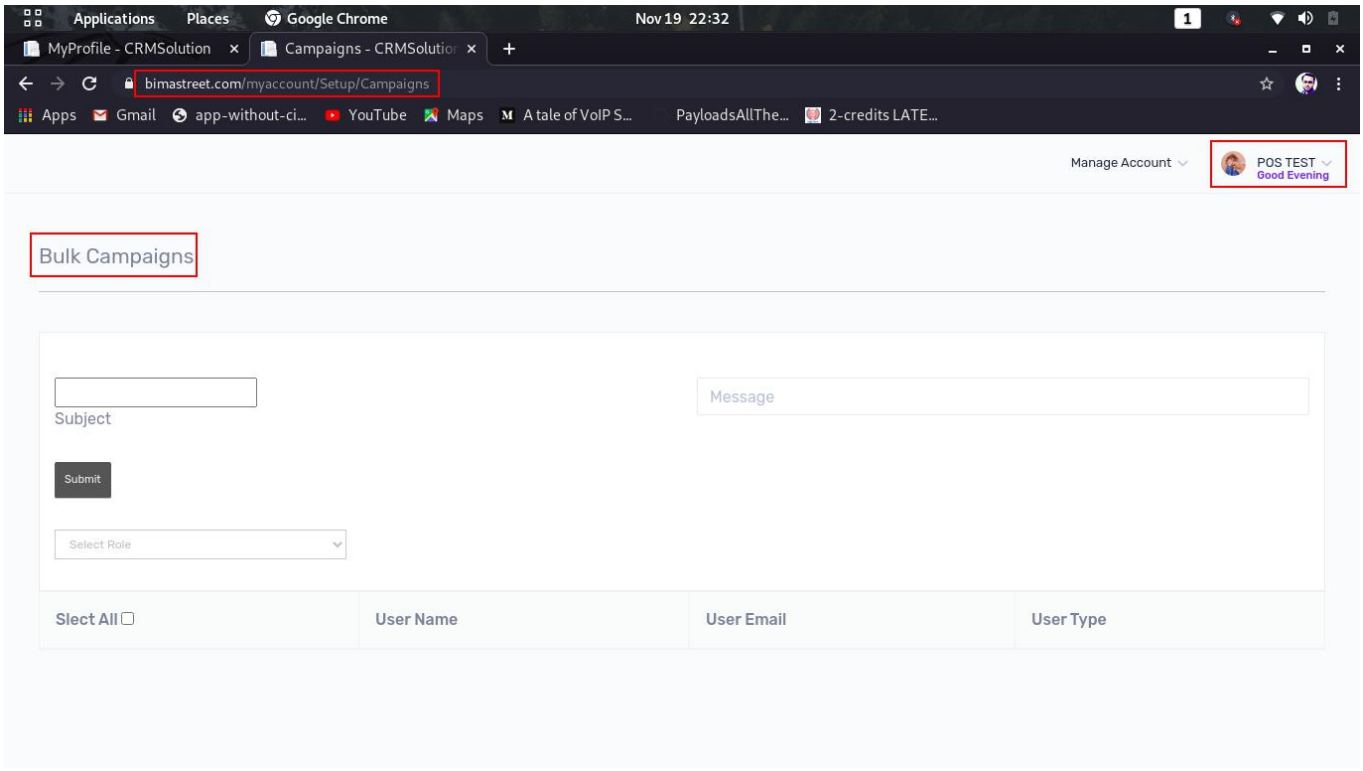


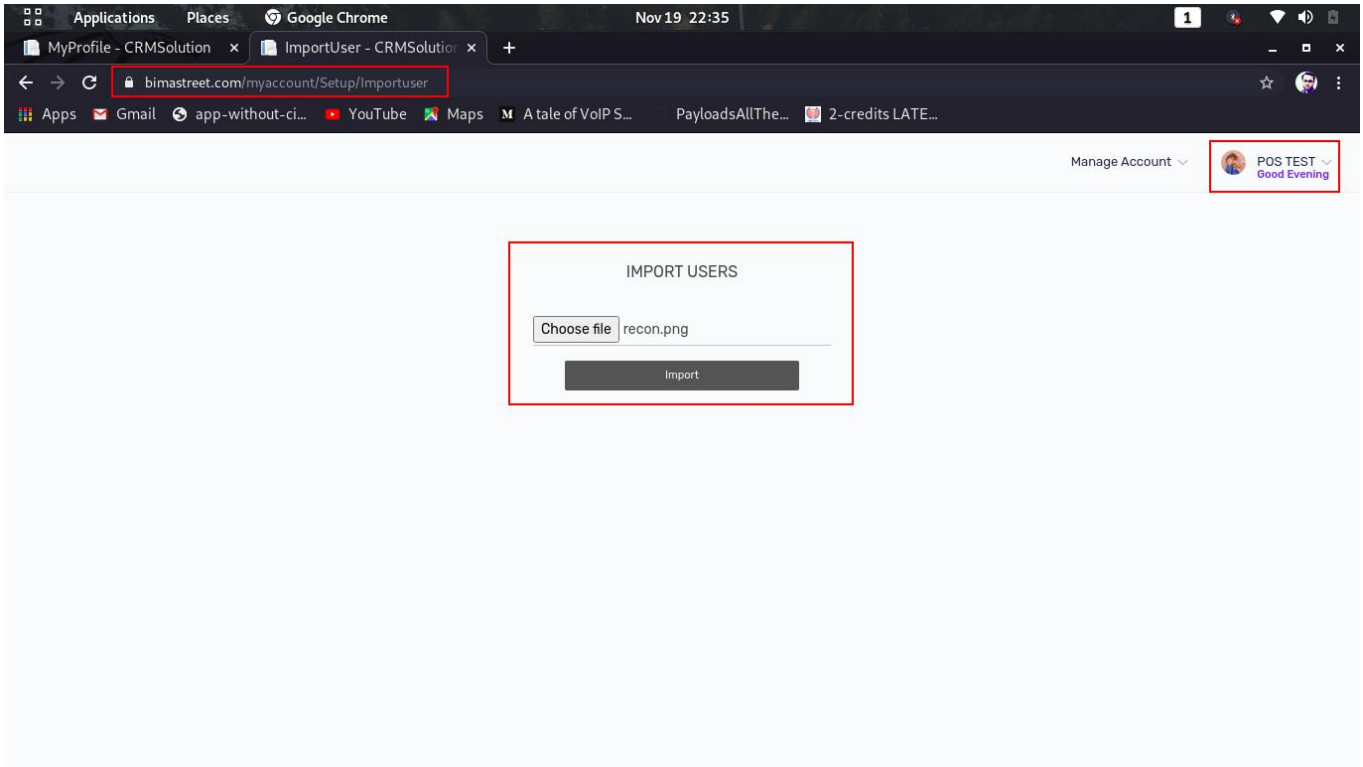


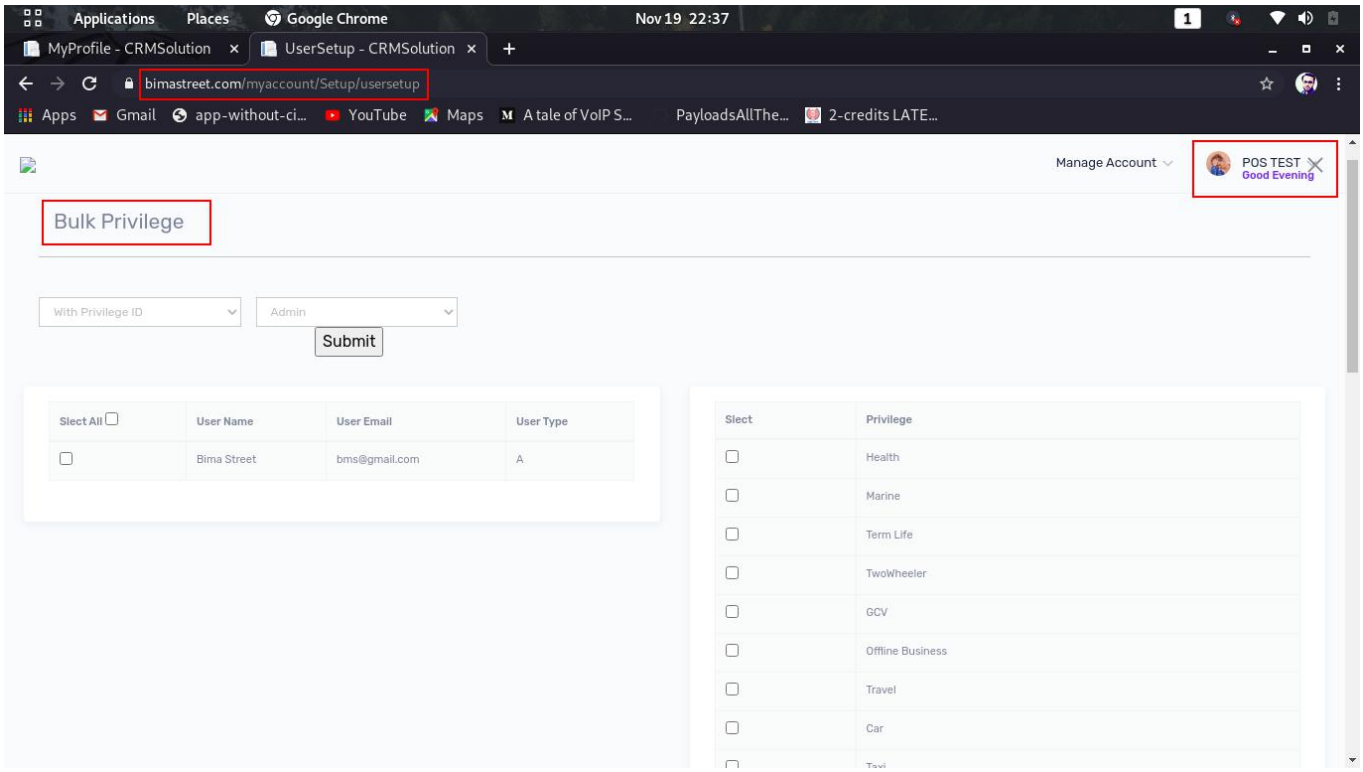


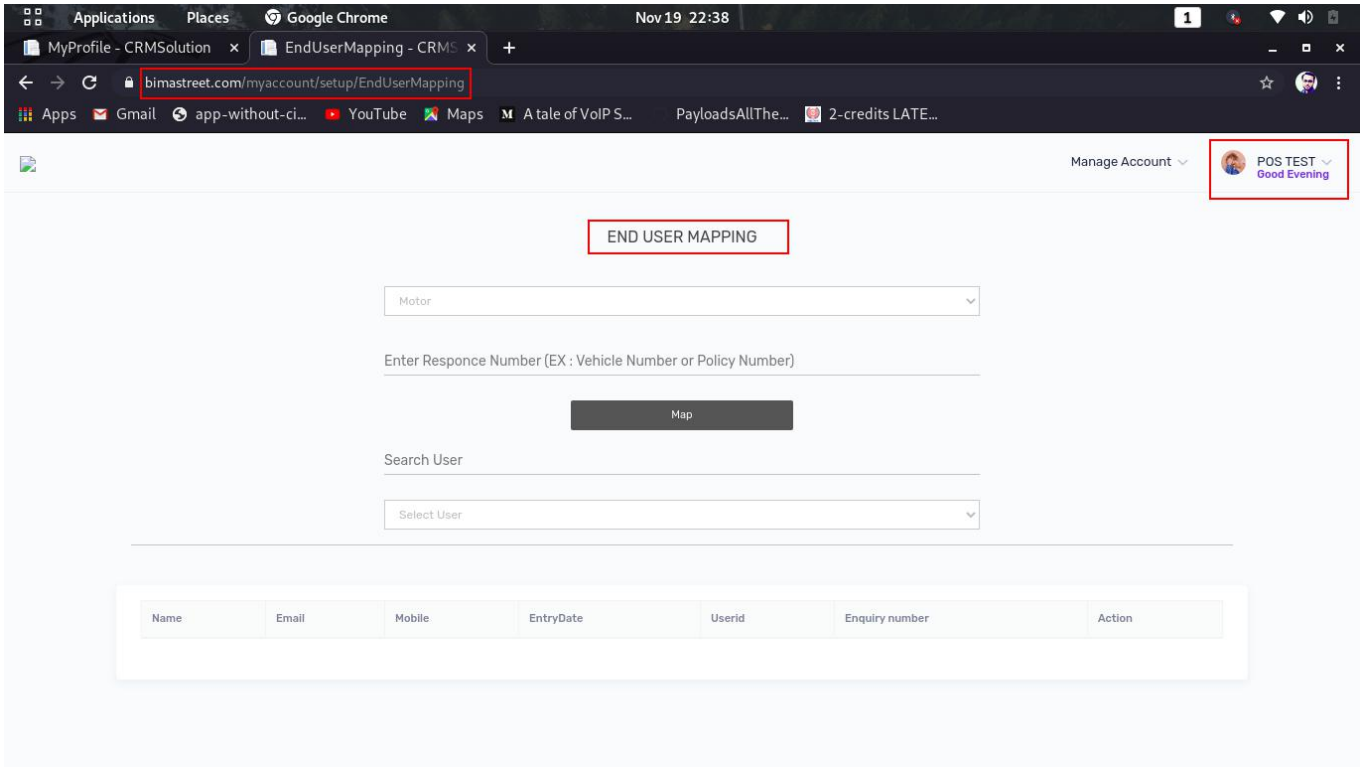


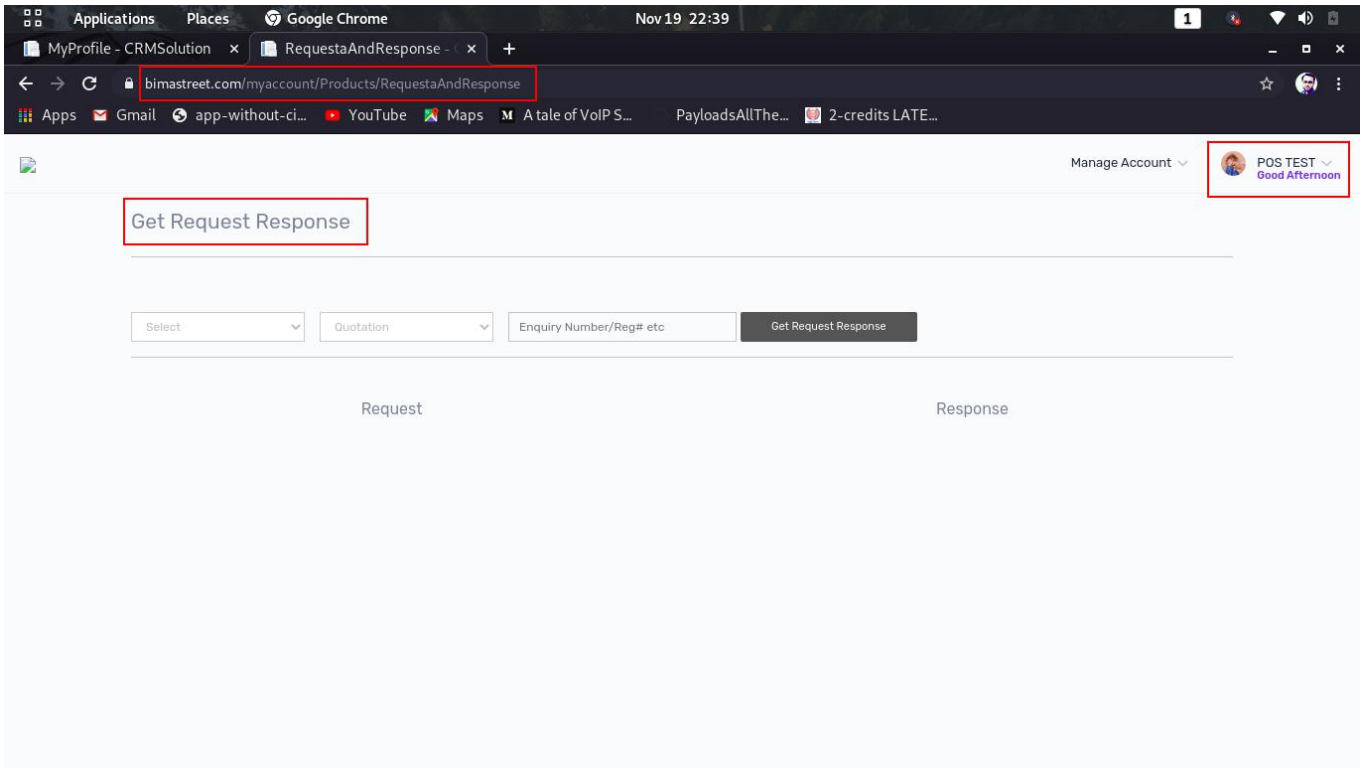


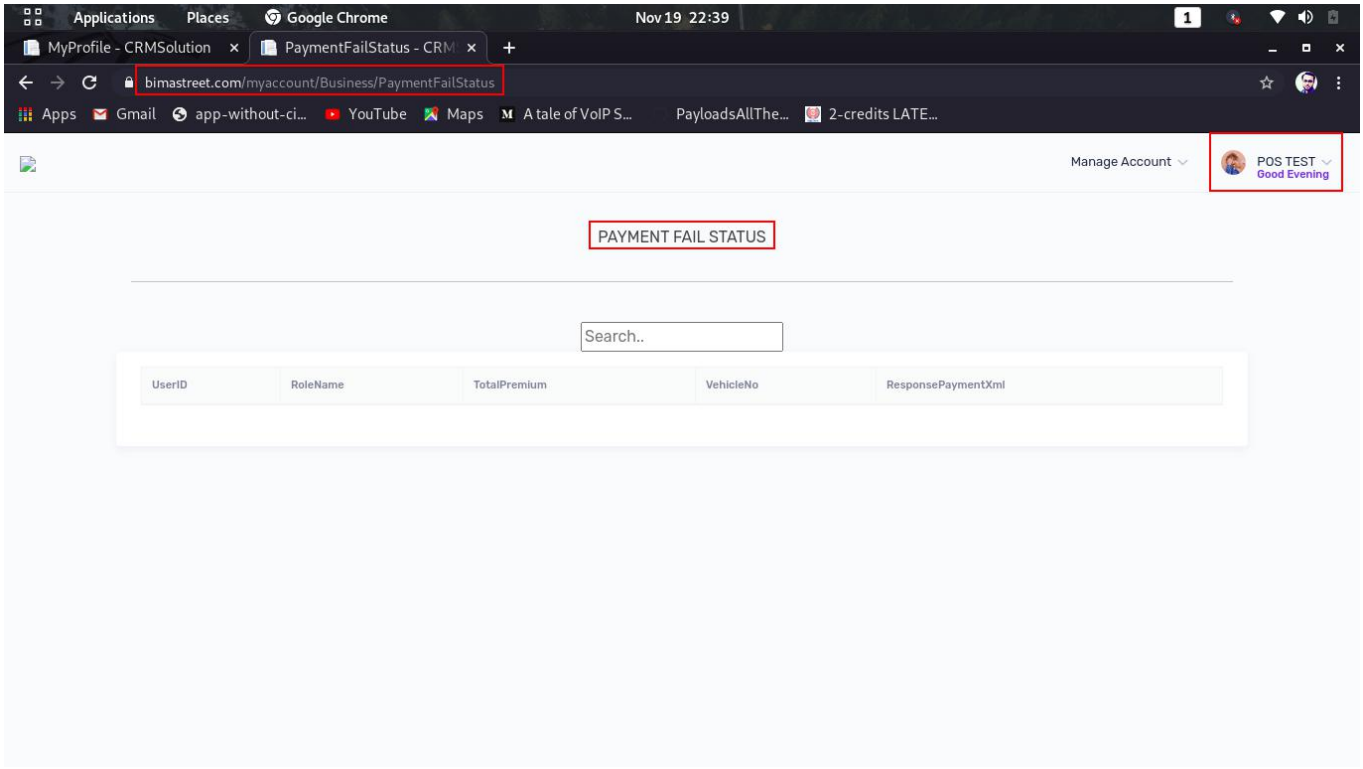


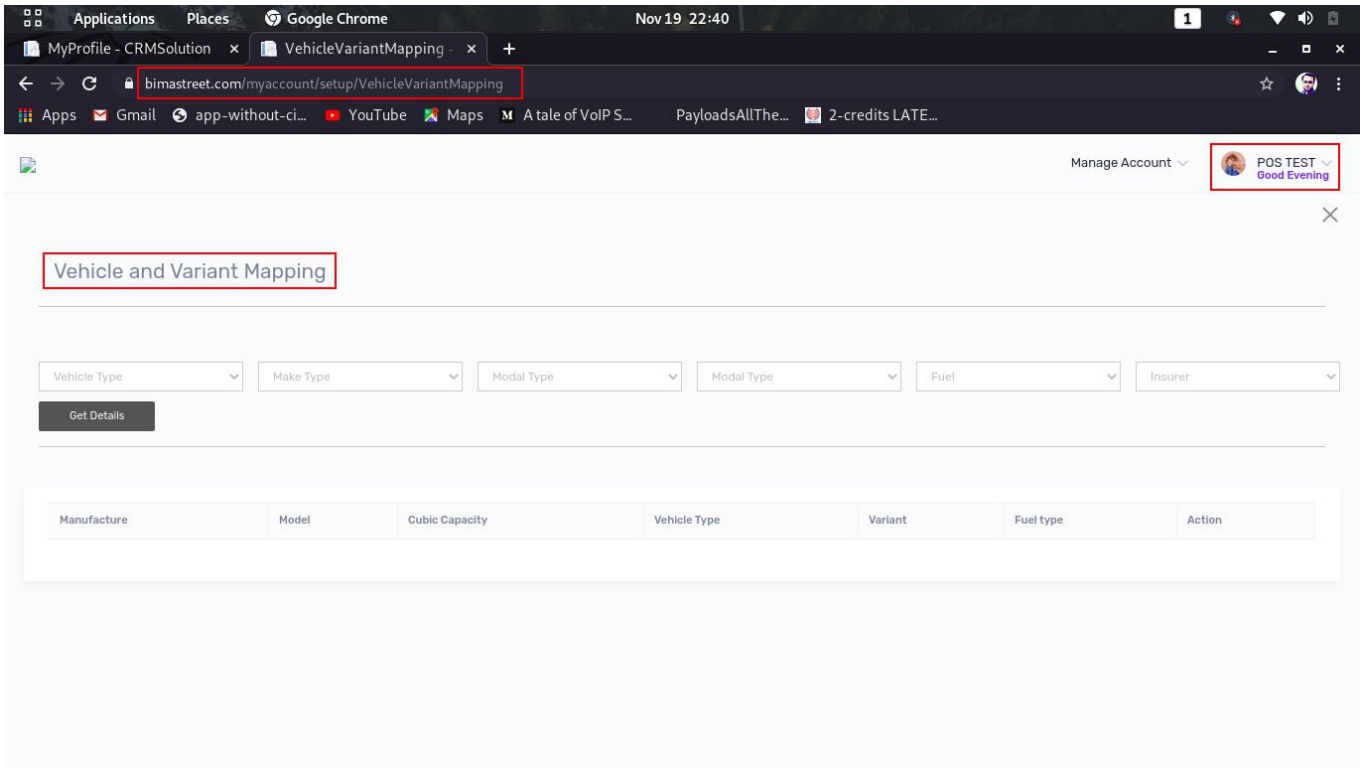


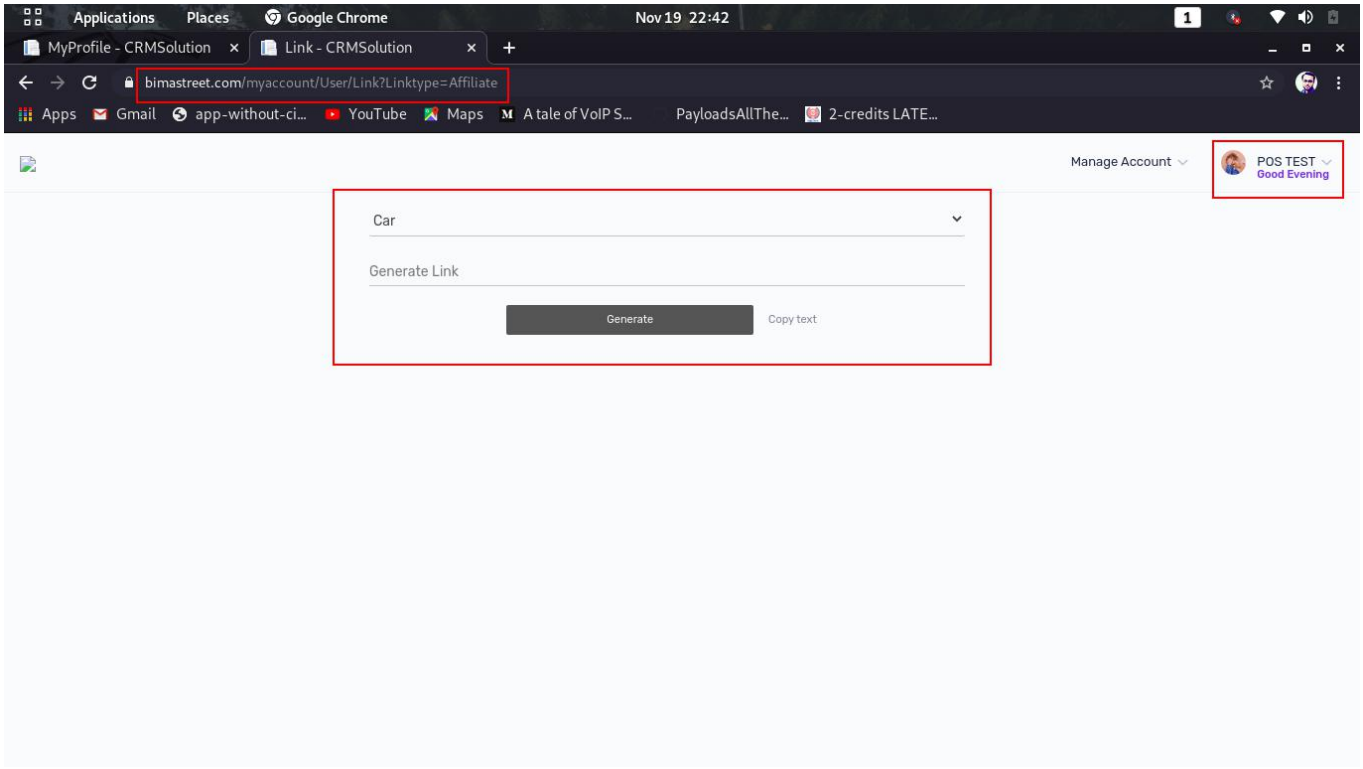


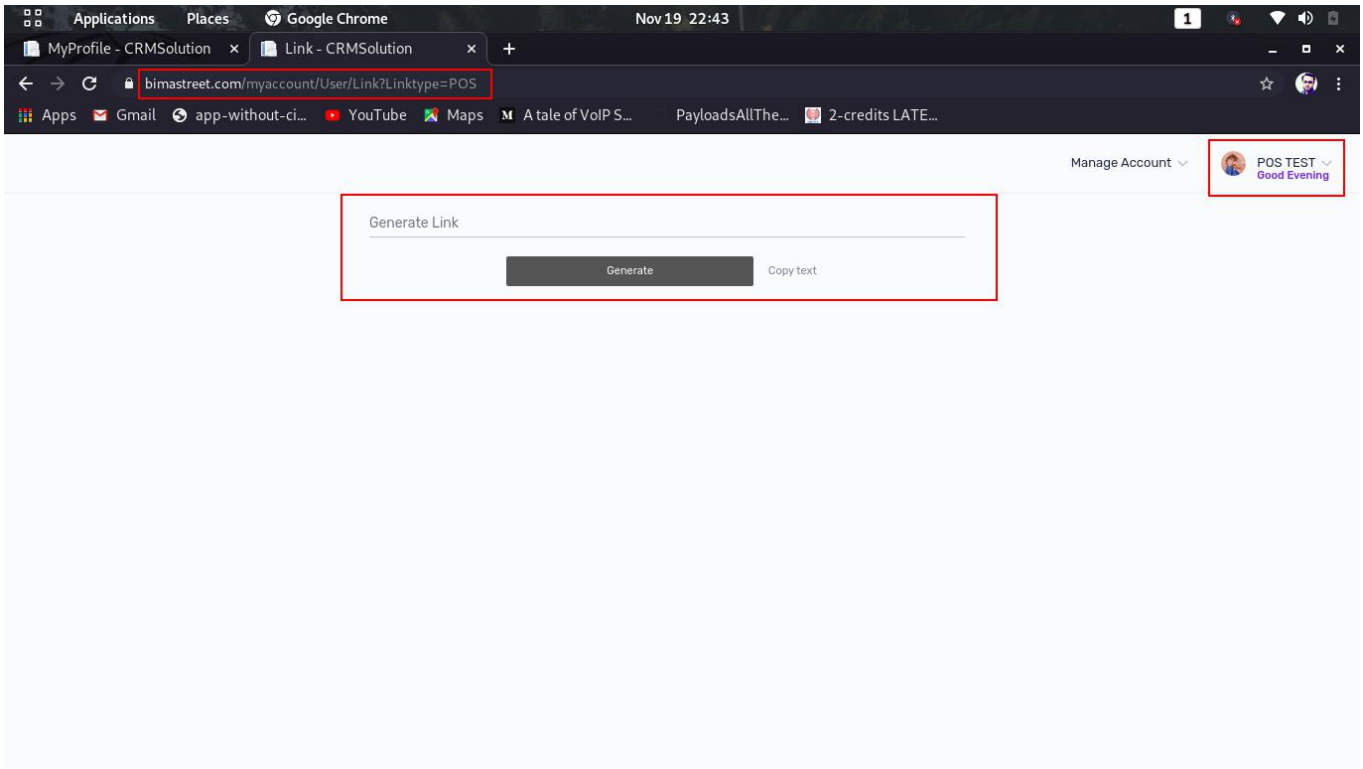












Recommendation:

Properly implement the access control.

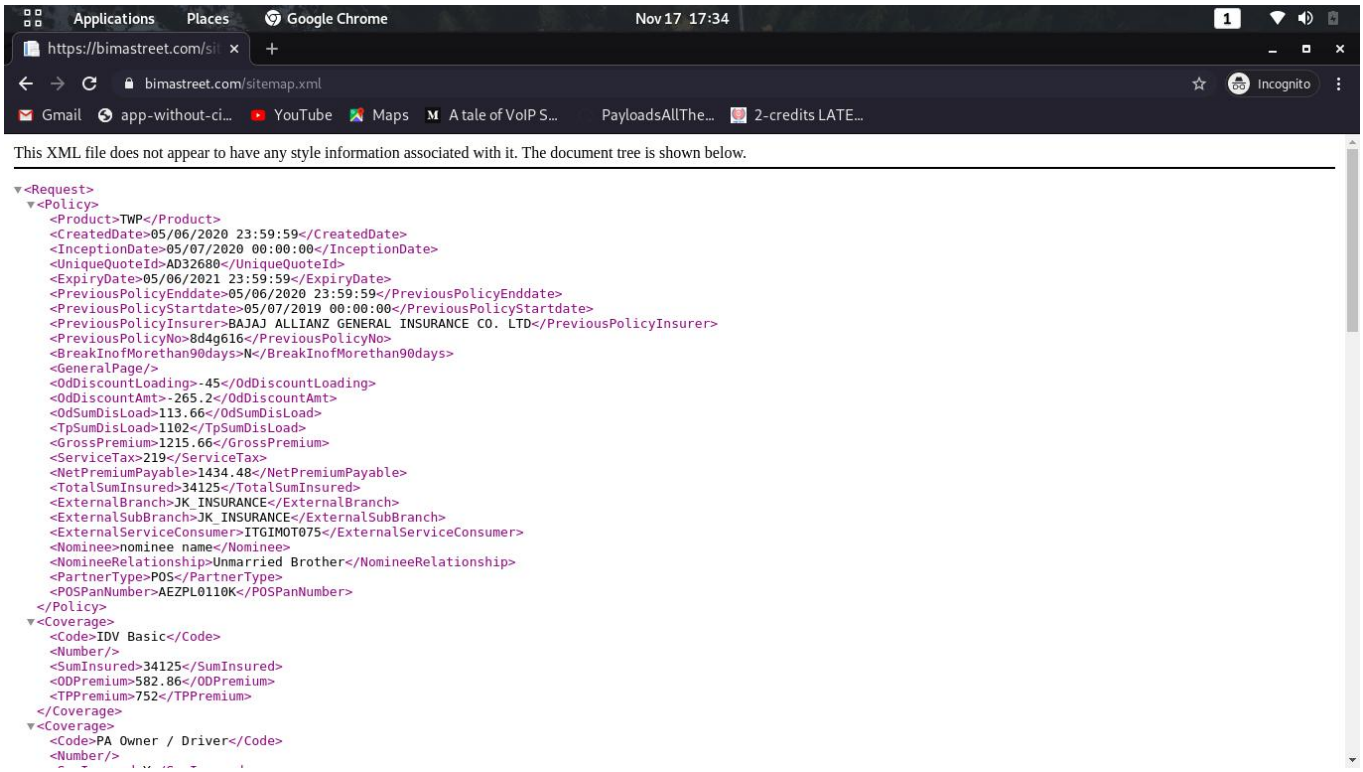
10.2 Uncommon URLs Found:

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

Description:

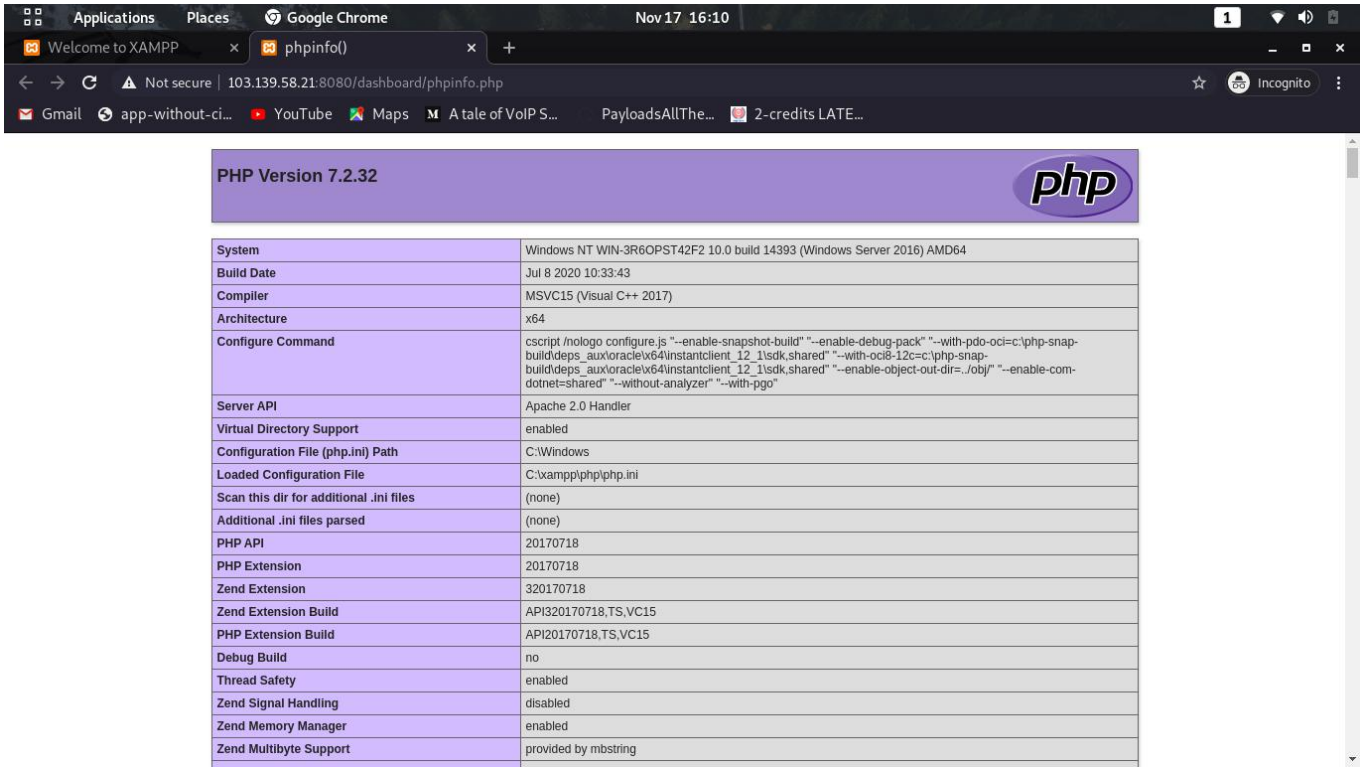
These URLs containing sensitive information about user of the application and server information and all URLs are publicly accessible.

Proof of Concept:



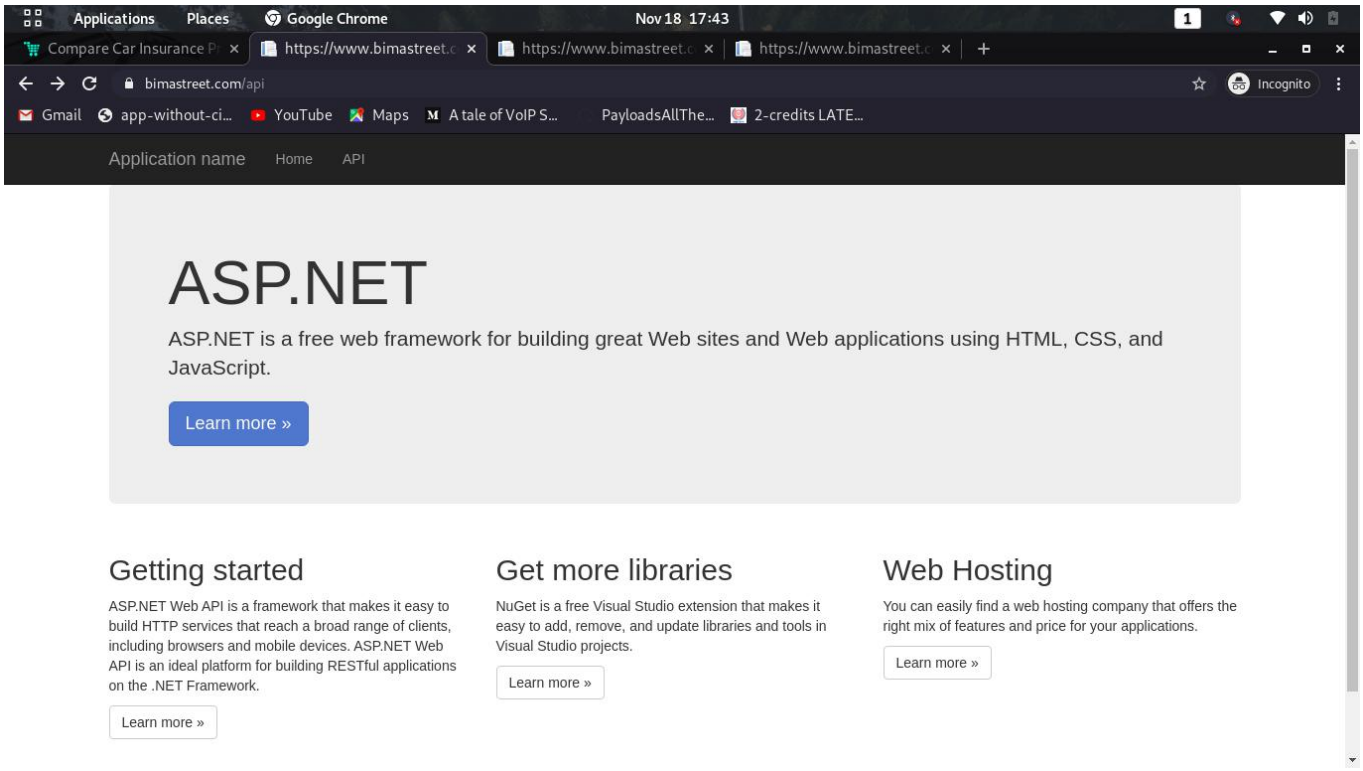
This XML file does not appear to have any style information associated with it. The document tree is shown below.

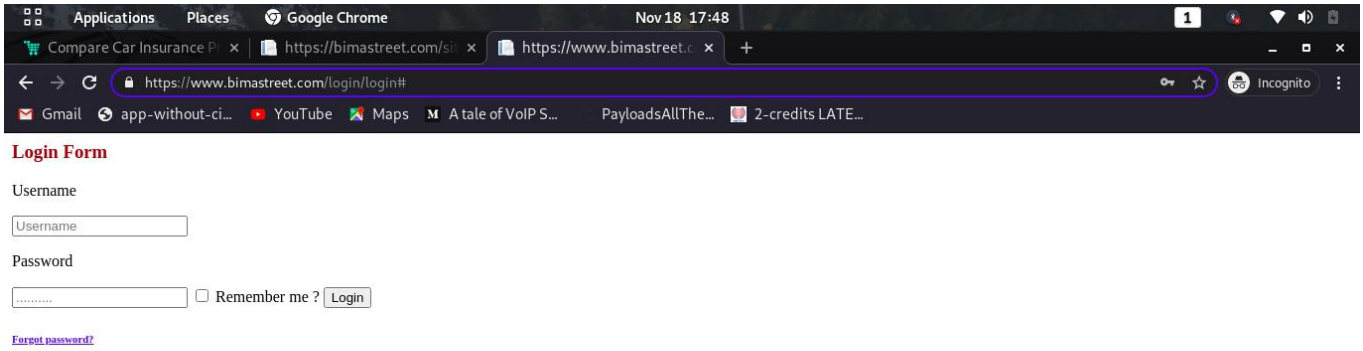

```
▼<Request>
 ▼<Policy>
    <Product>TWP</Product>
    <CreatedDate>05/06/2020 23:59:59</CreatedDate>
    <InceptionDate>05/07/2020 00:00:00</InceptionDate>
    <UniqueQuoteId>AD32680</UniqueQuoteId>
    <ExpiryDate>05/06/2021 23:59:59</ExpiryDate>
    <PreviousPolicyEnddate>05/06/2020 23:59:59</PreviousPolicyEnddate>
    <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/>
```

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	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
Zend Multibyte Support	provided by mbstring





Recommendation:

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

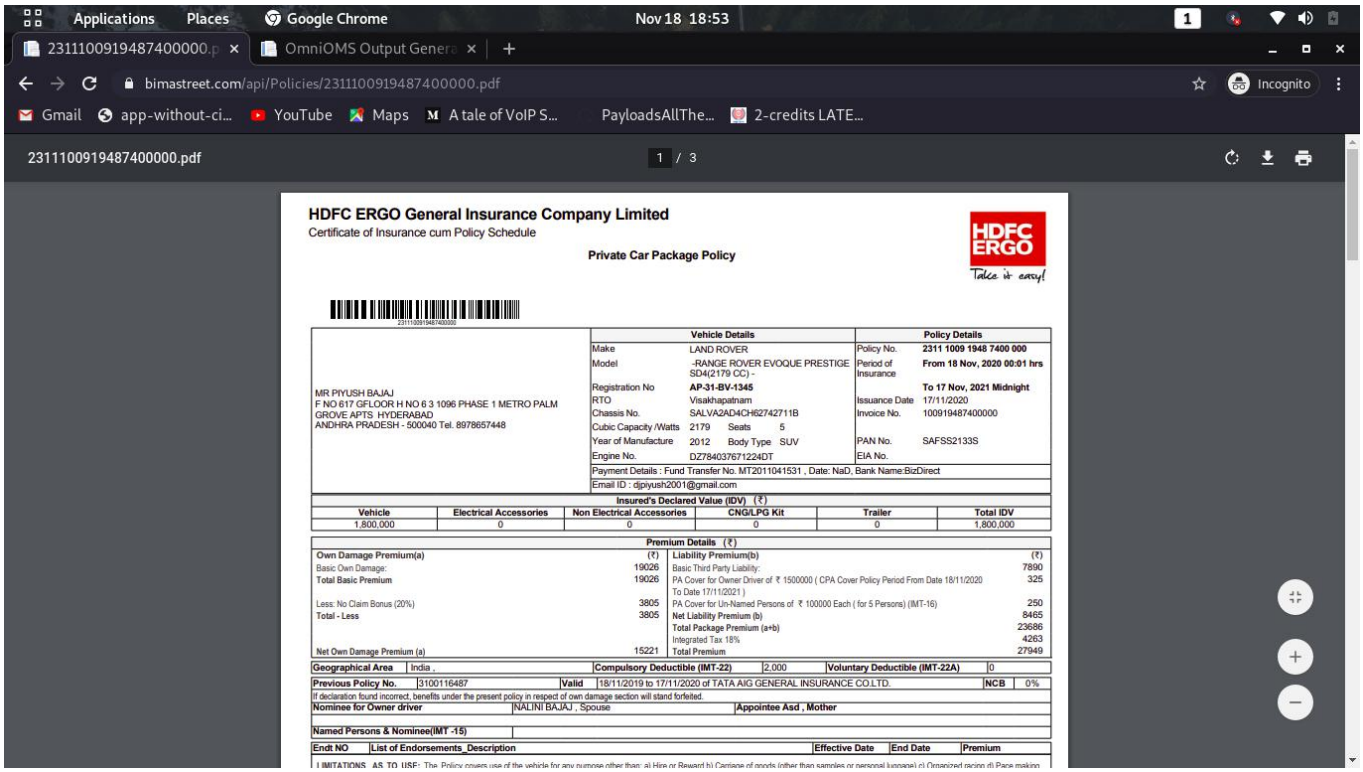
10.3 Broken Access Control:

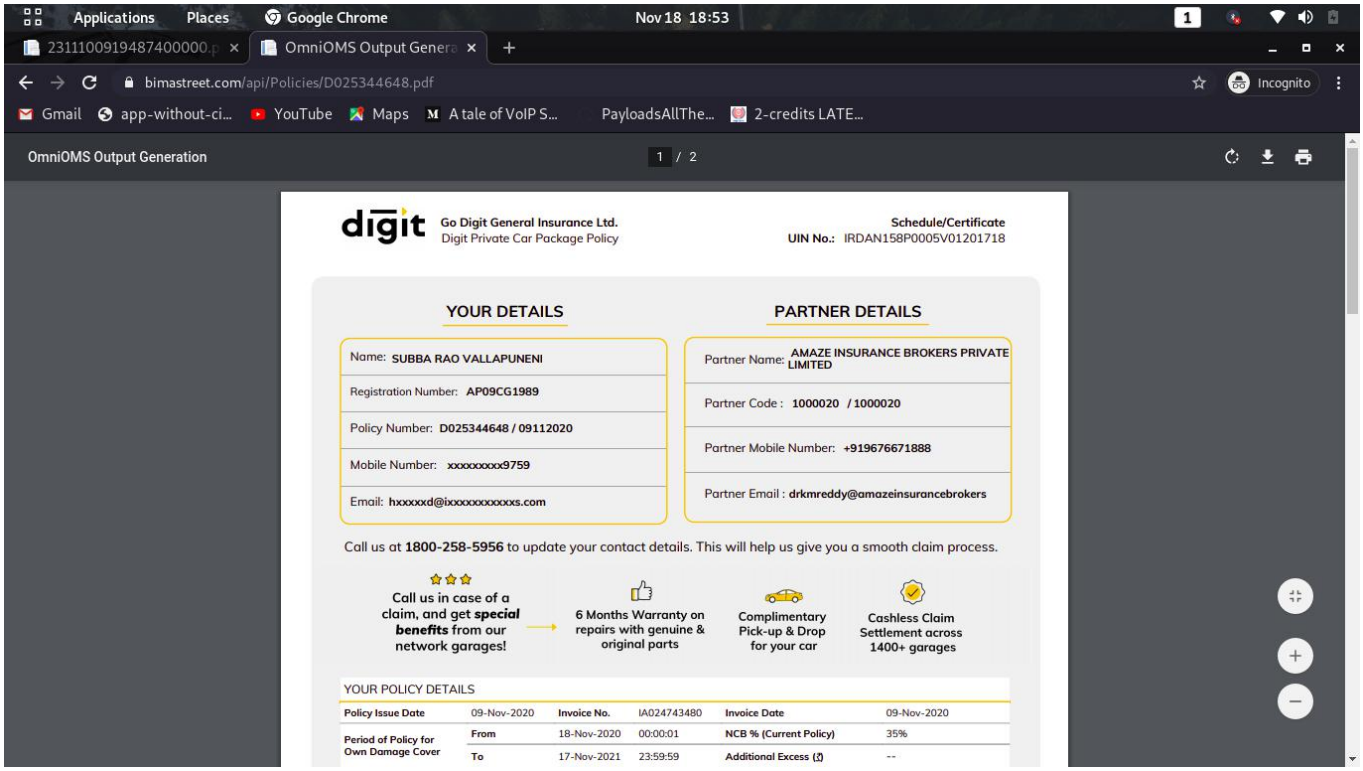
Name of Vulnerability	Broken Access Control
URL	https://www.bimastreet.com/api/Policies/2311100919487400000.pdf https://www.bimastreet.com/api/Policies/D025344648.pdf https://www.bimastreet.com/myaccount/user/myprofile https://www.bimastreet.com/myaccount/Home/Index https://www.bimastreet.com/myaccount/master/mastersetup https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup https://www.bimastreet.com/myaccount/Business/MissingPolicy https://www.bimastreet.com/myaccount/products/renewals https://www.bimastreet.com/myaccount/Business/Utility https://www.bimastreet.com/myaccount/user/users https://www.bimastreet.com/myaccount/Business/BusinessReport https://www.bimastreet.com/Car/Quotes?policytype=R&Data=/uCKcos82ln/b/wtIt2W4A==
Risk	High

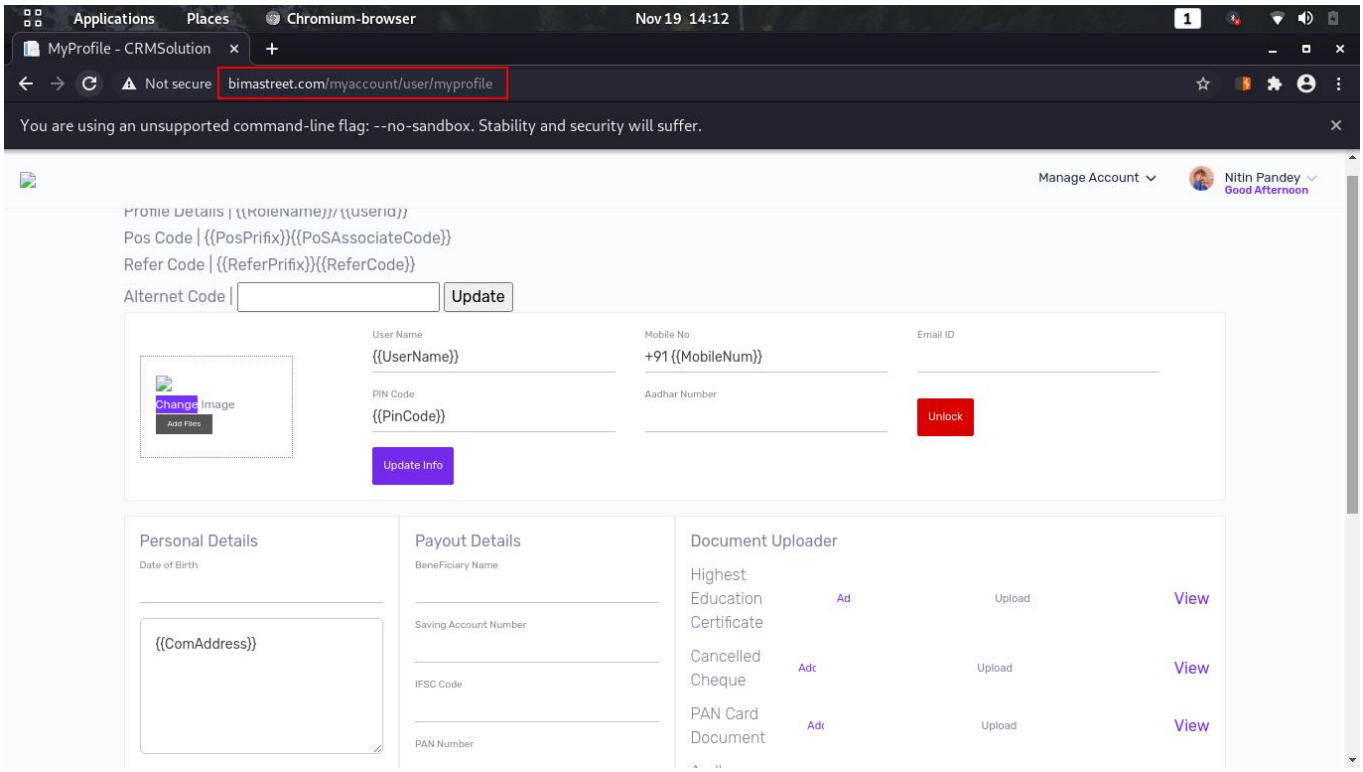
Description:

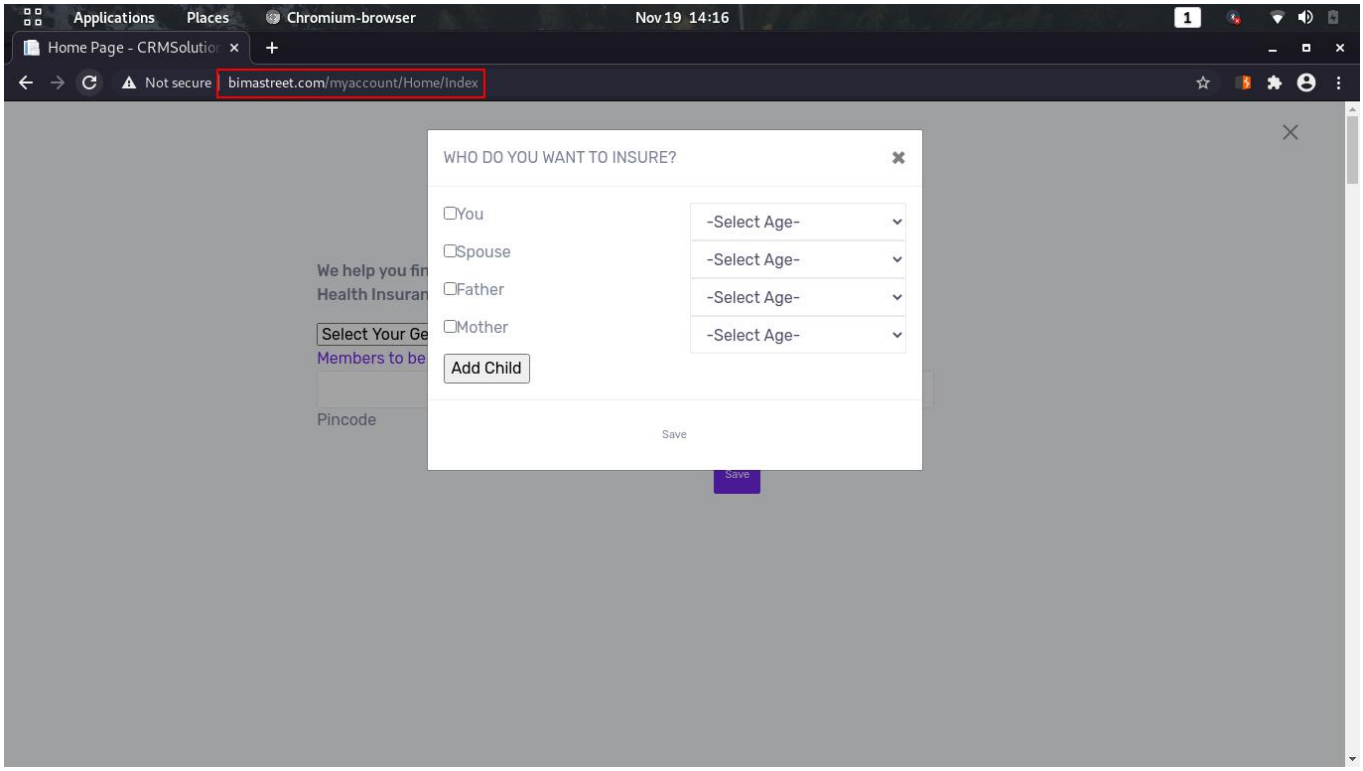
Normally these URLs are only used after user logged in in the application but these URLs are publicly accessible without any authentication and authorization. So, any user can access these URLs without any authentication and access the crucial data and perform any action.

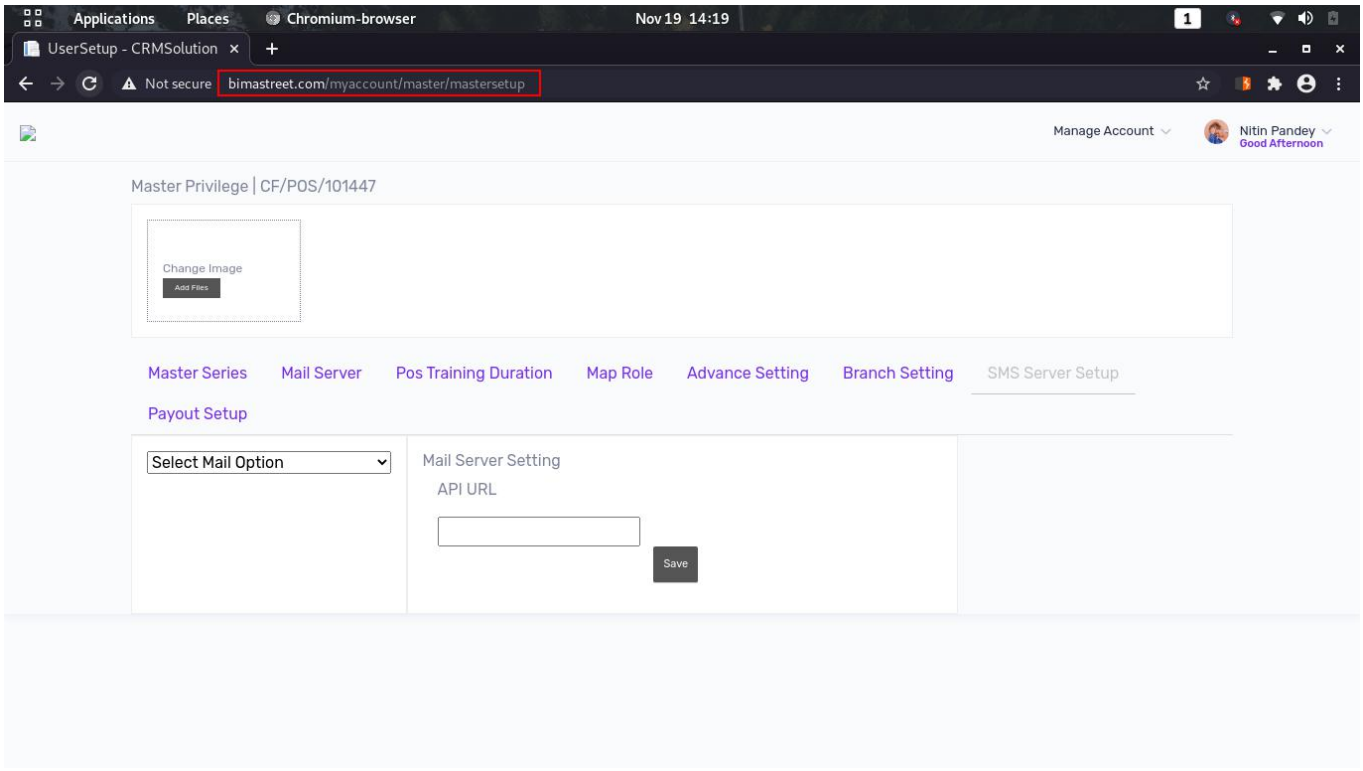
Proof of Concept:

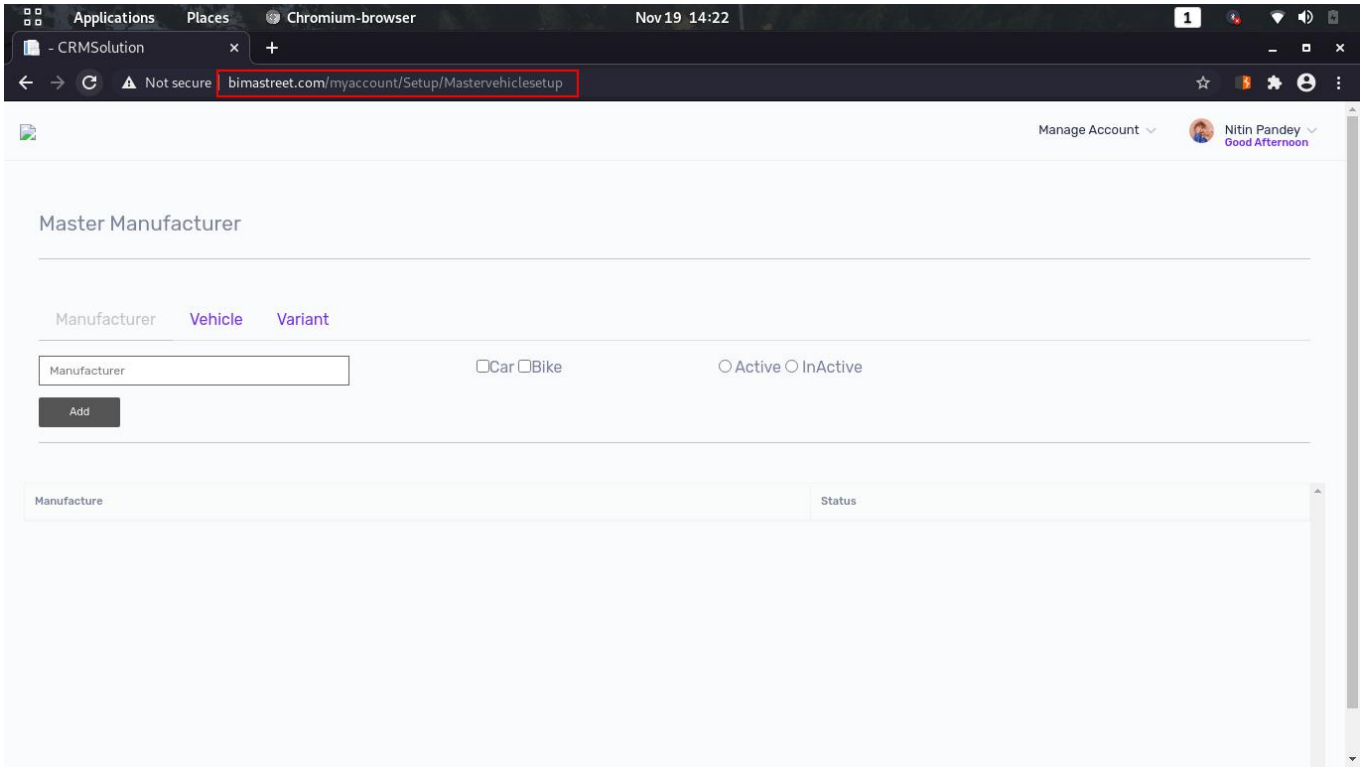


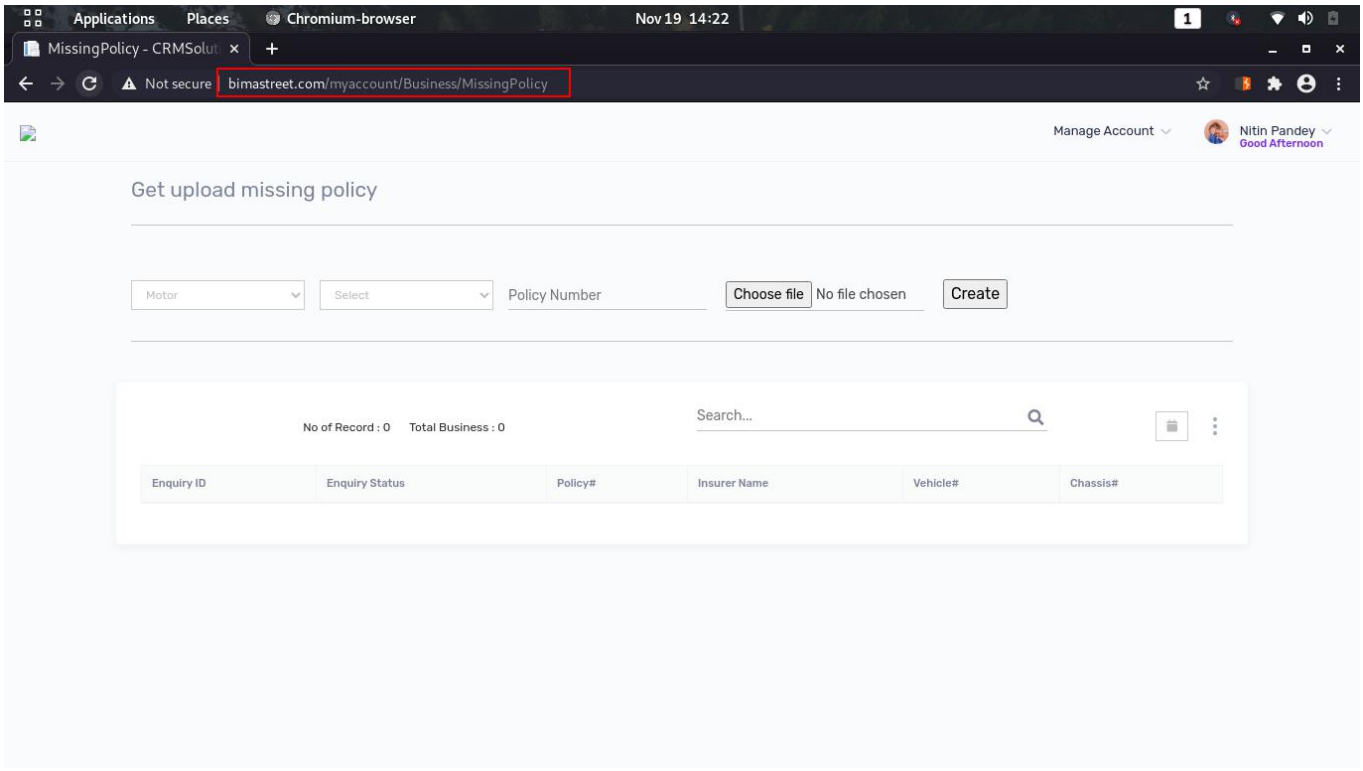


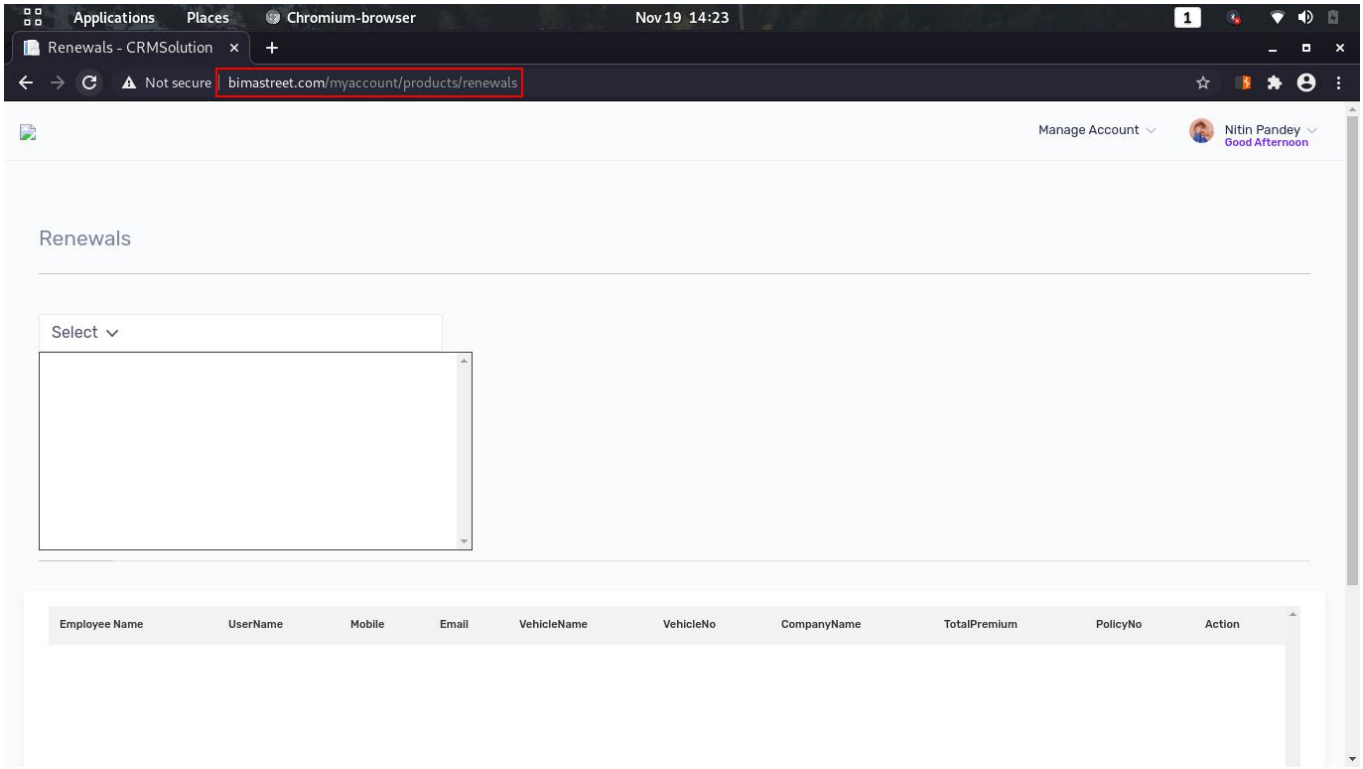


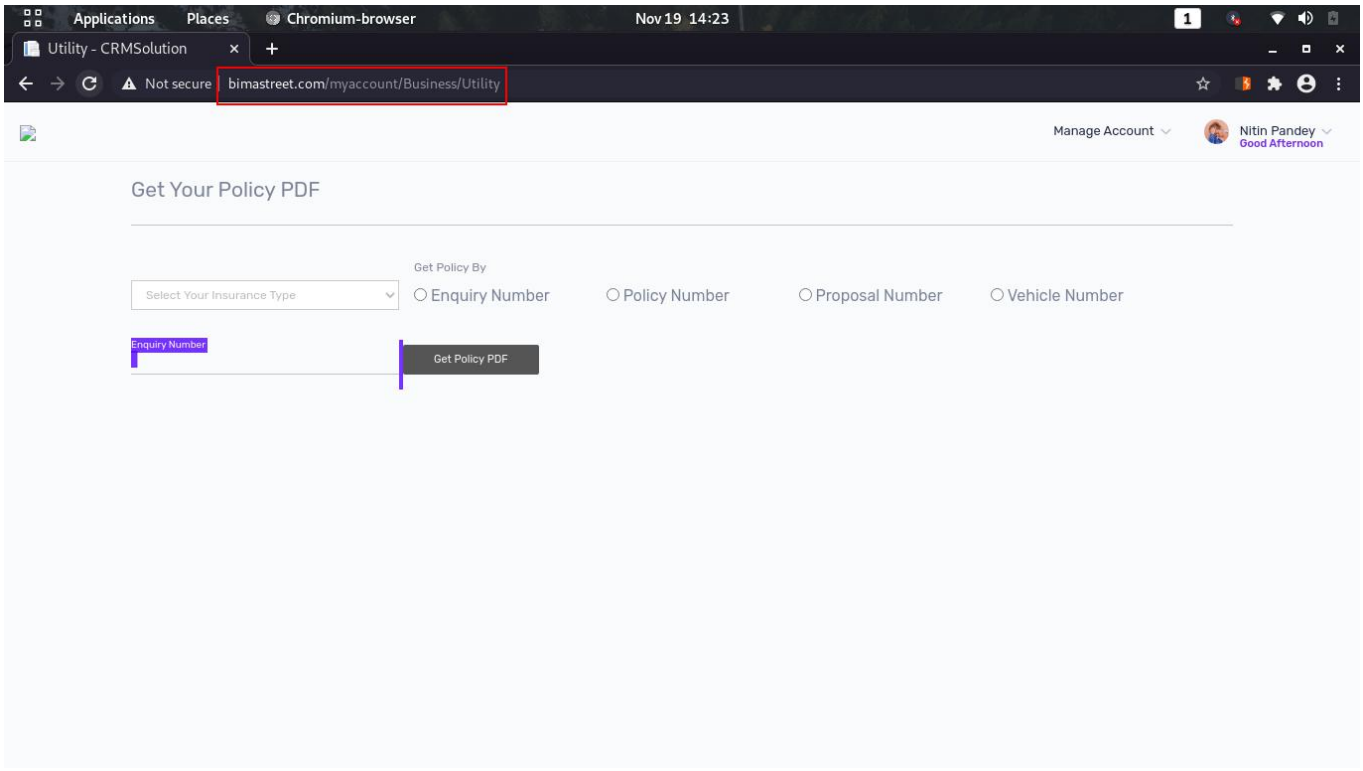


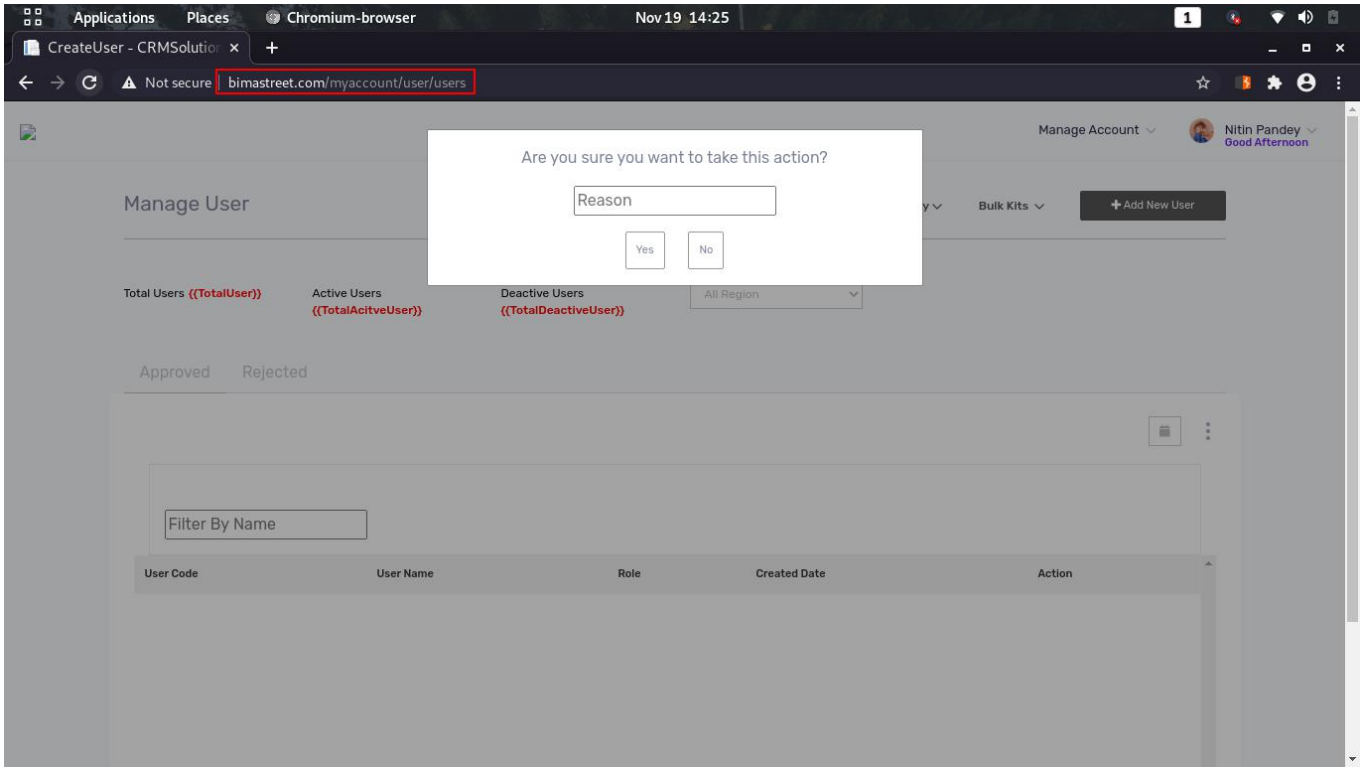


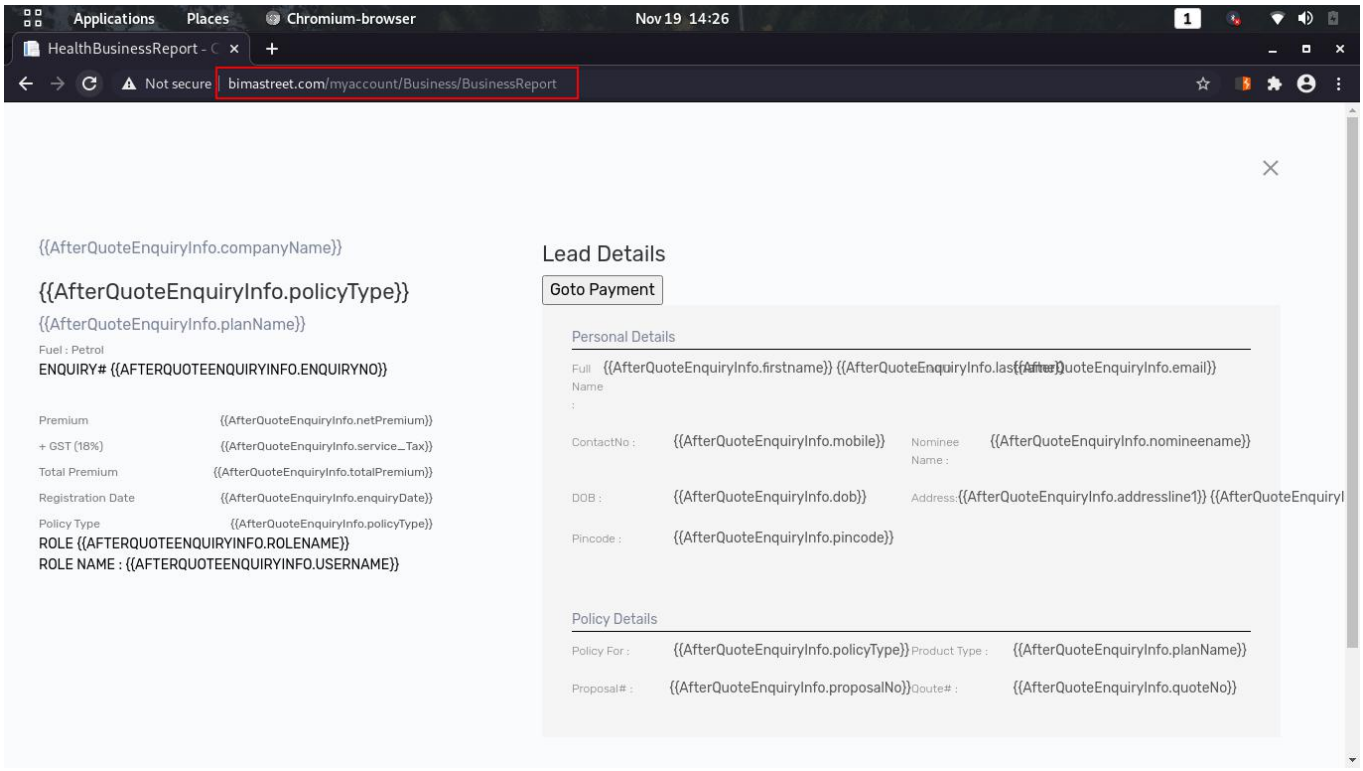


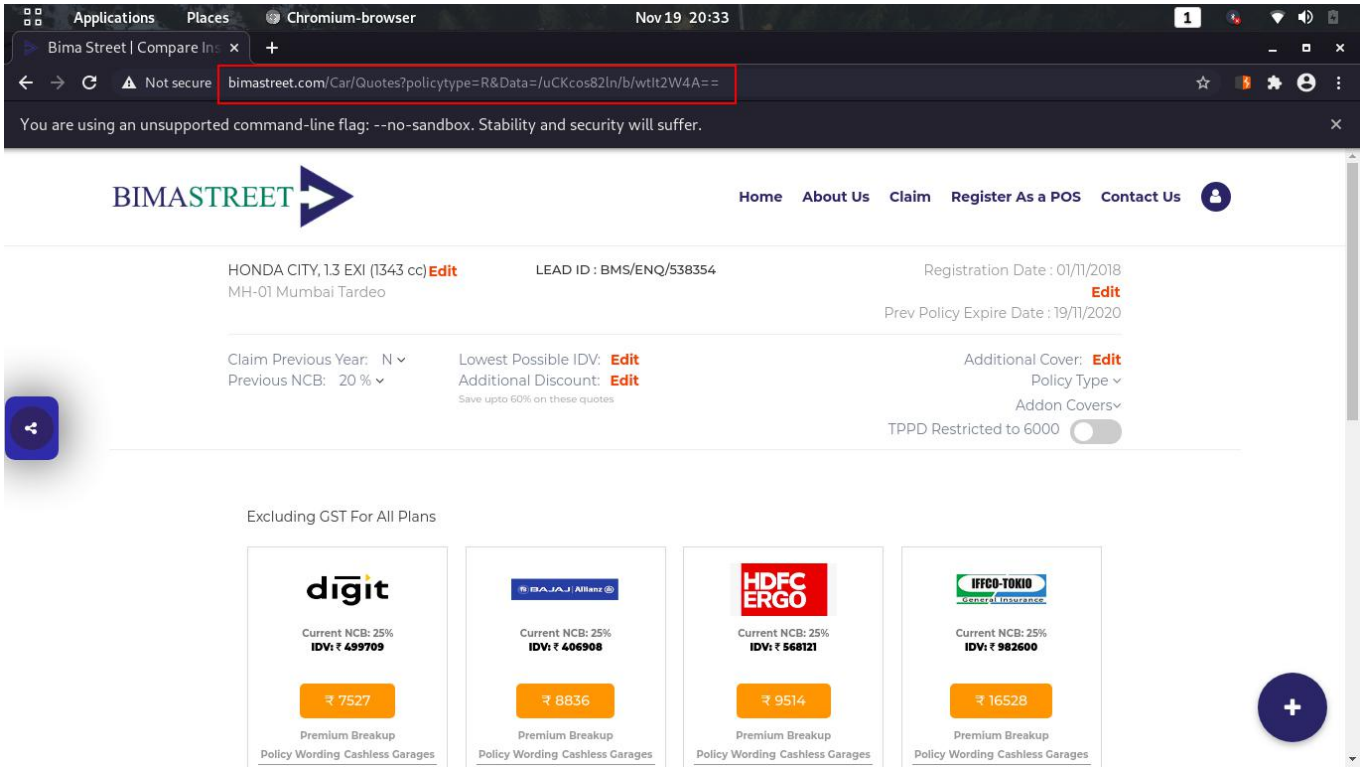












Recommendation:

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.

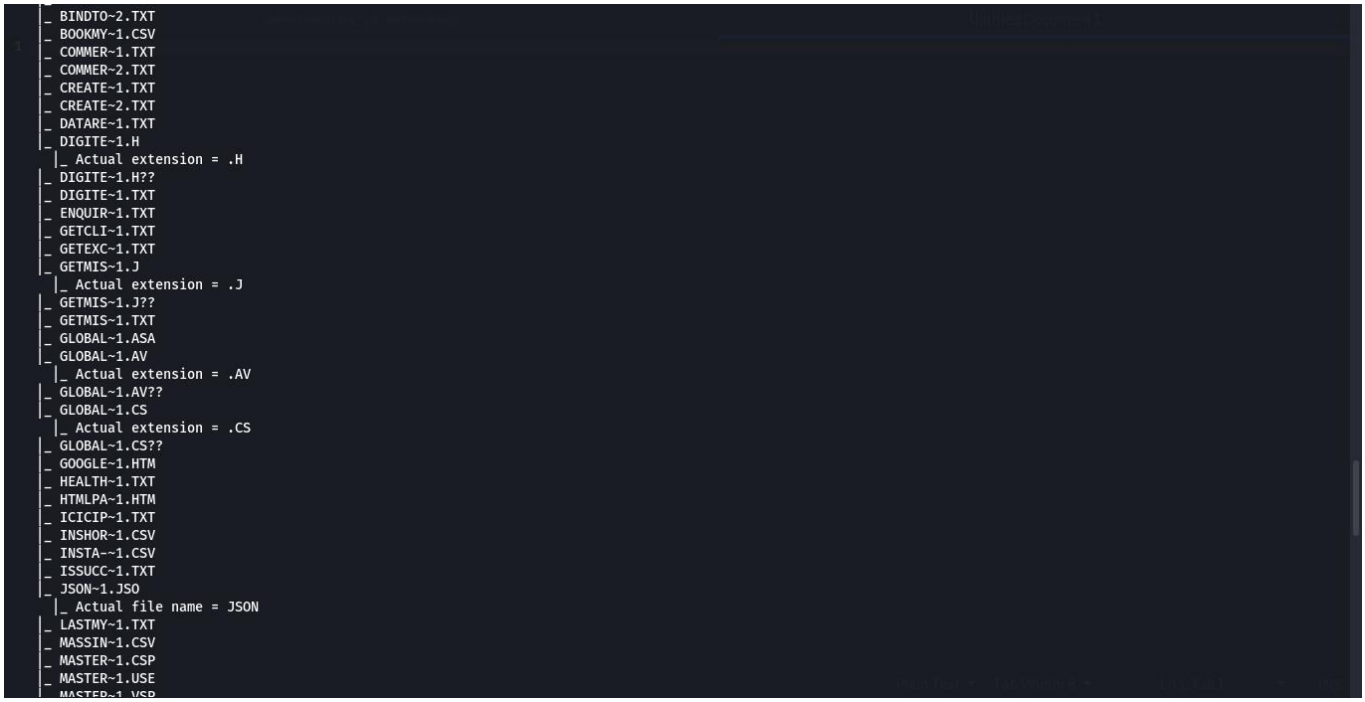
10.4 Tilde enumeration:

Name of Vulnerability	Tilde Enumeration
URL	https://www.bimastreet.com/
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:



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.

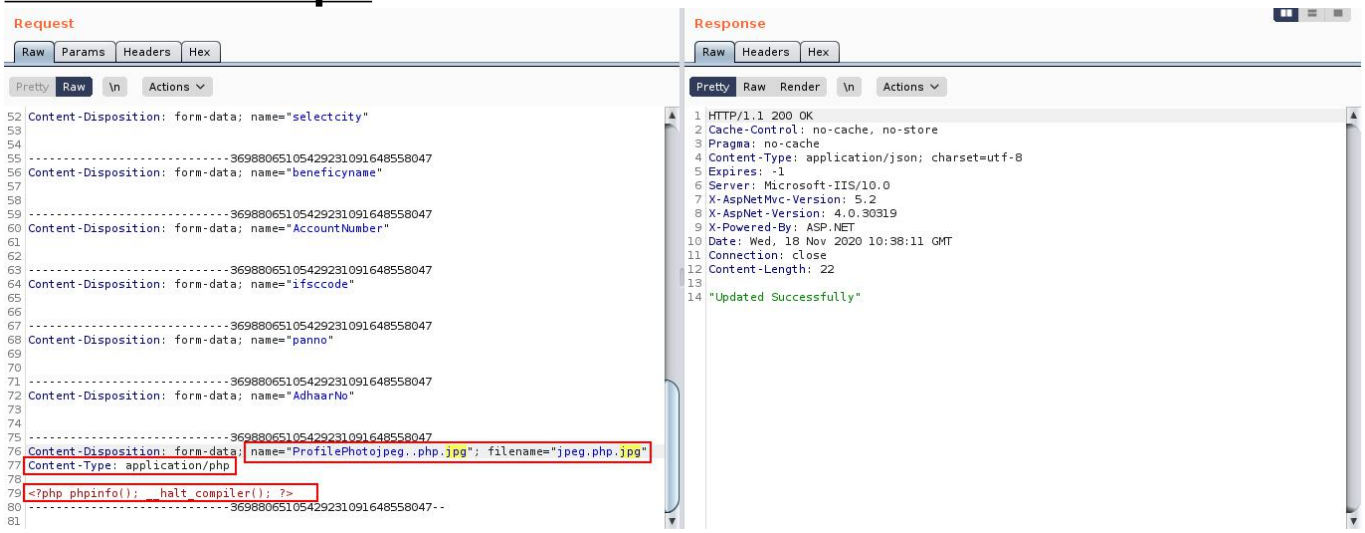
10.5 Malicious File Upload:

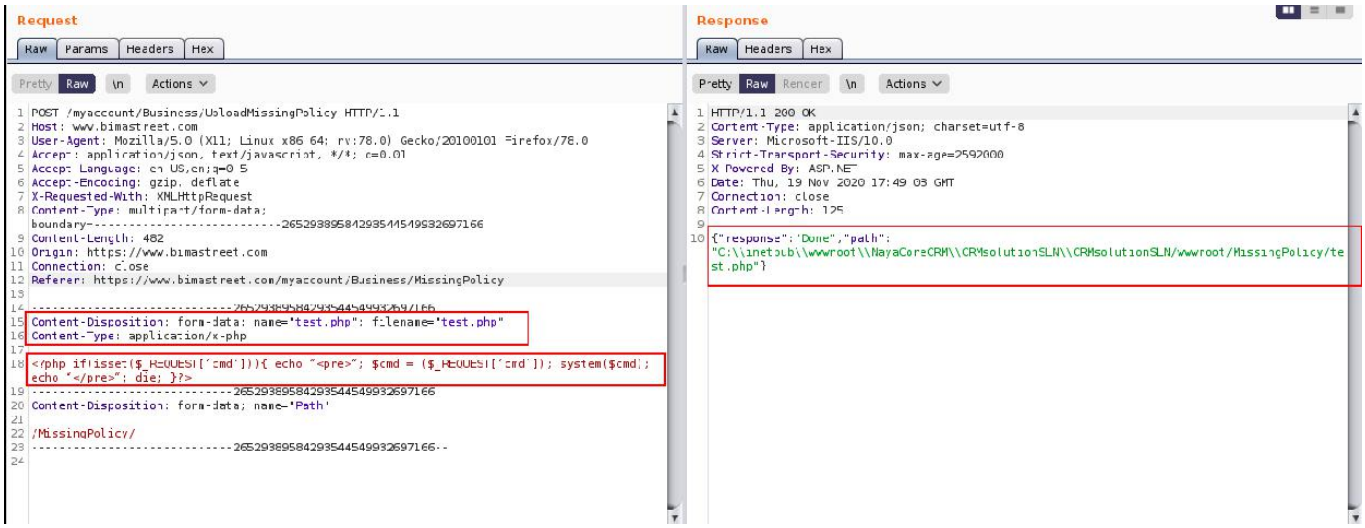
Name of Vulnerability	Malicious File Upload
URL	https://www.bimastreet.com/MyProfile/Updatepofile https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy
Risk	High

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:





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	https://www.bimastreet.com/feeds https://www.bimastreet.com/geo https://www.bimastreet.com/Admin/Home/LeadGrid
Risk	High

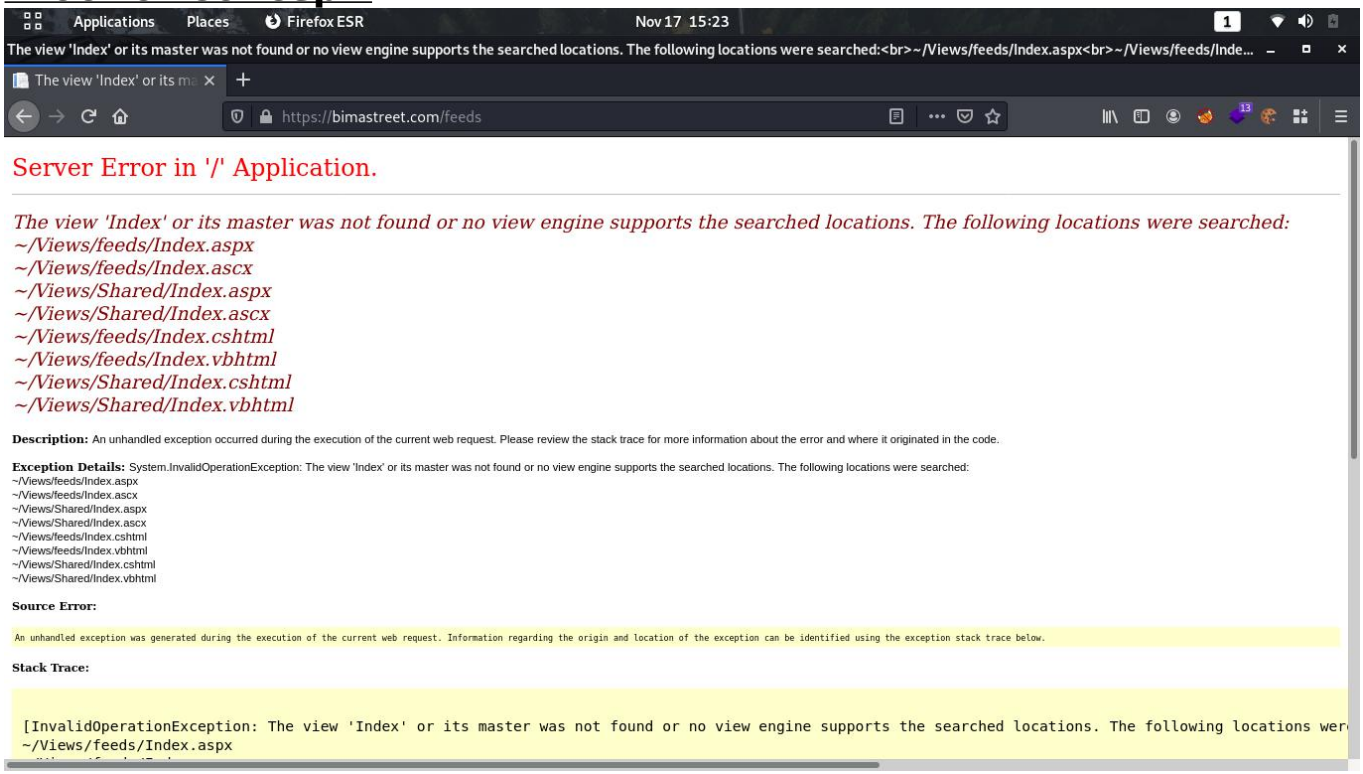
Description:

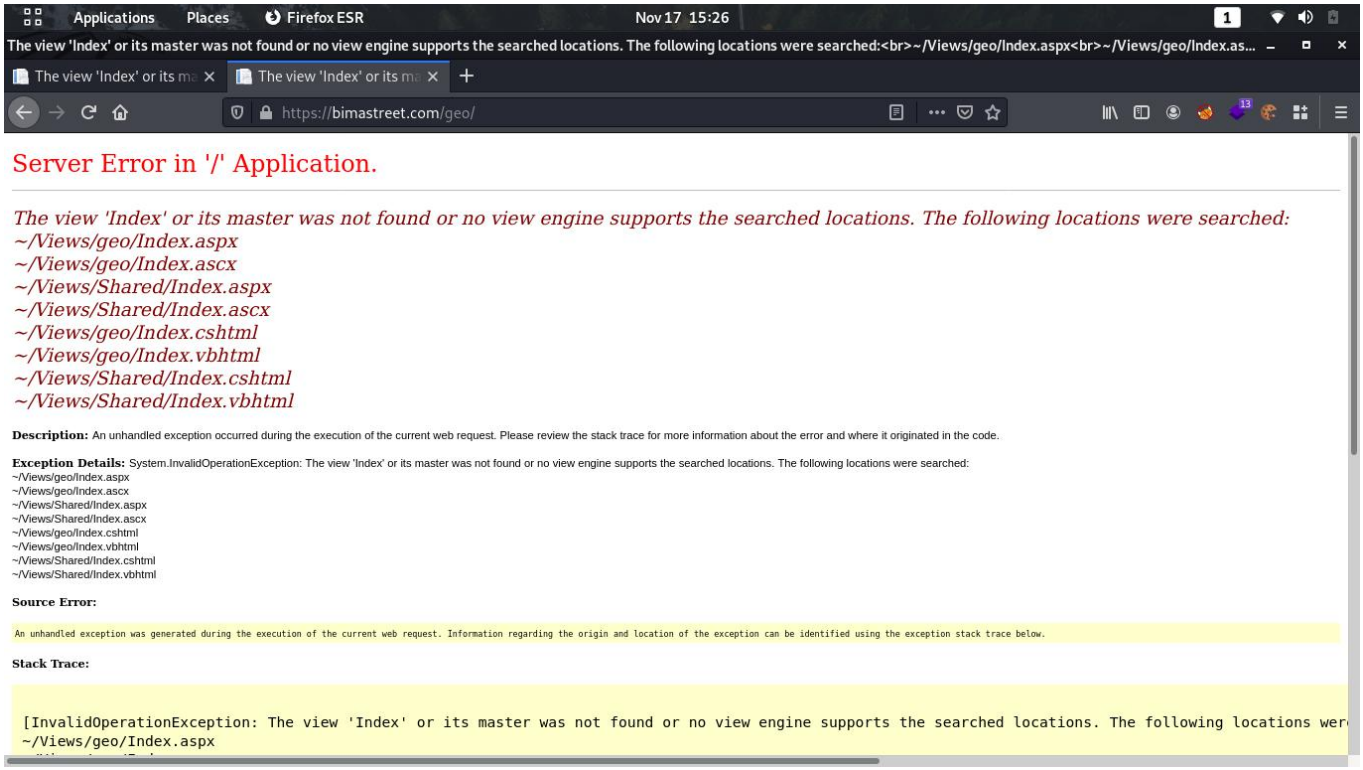
ASP.NET tracing is a debugging feature that is designed for use during development to help troubleshoot problems. It discloses sensitive information to users, and if enabled in production contexts may present a serious security threat.

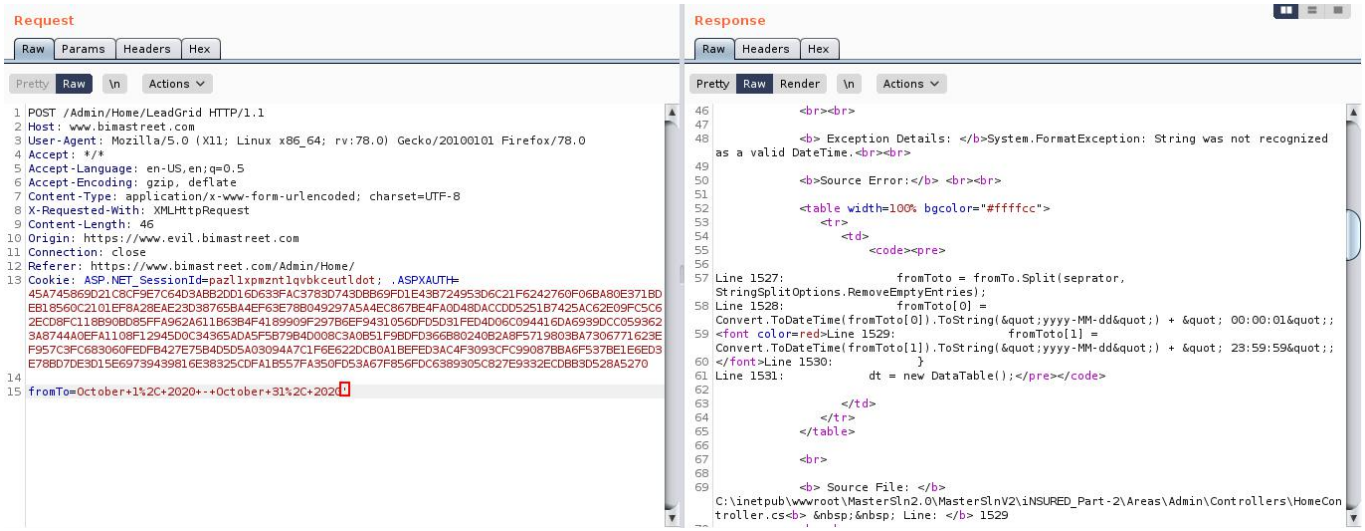
Application-level tracing enables any user to retrieve full details about recent requests to the application, including those of other users. This information typically includes session tokens and request parameters, which may enable an attacker to compromise other users and even take control of the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

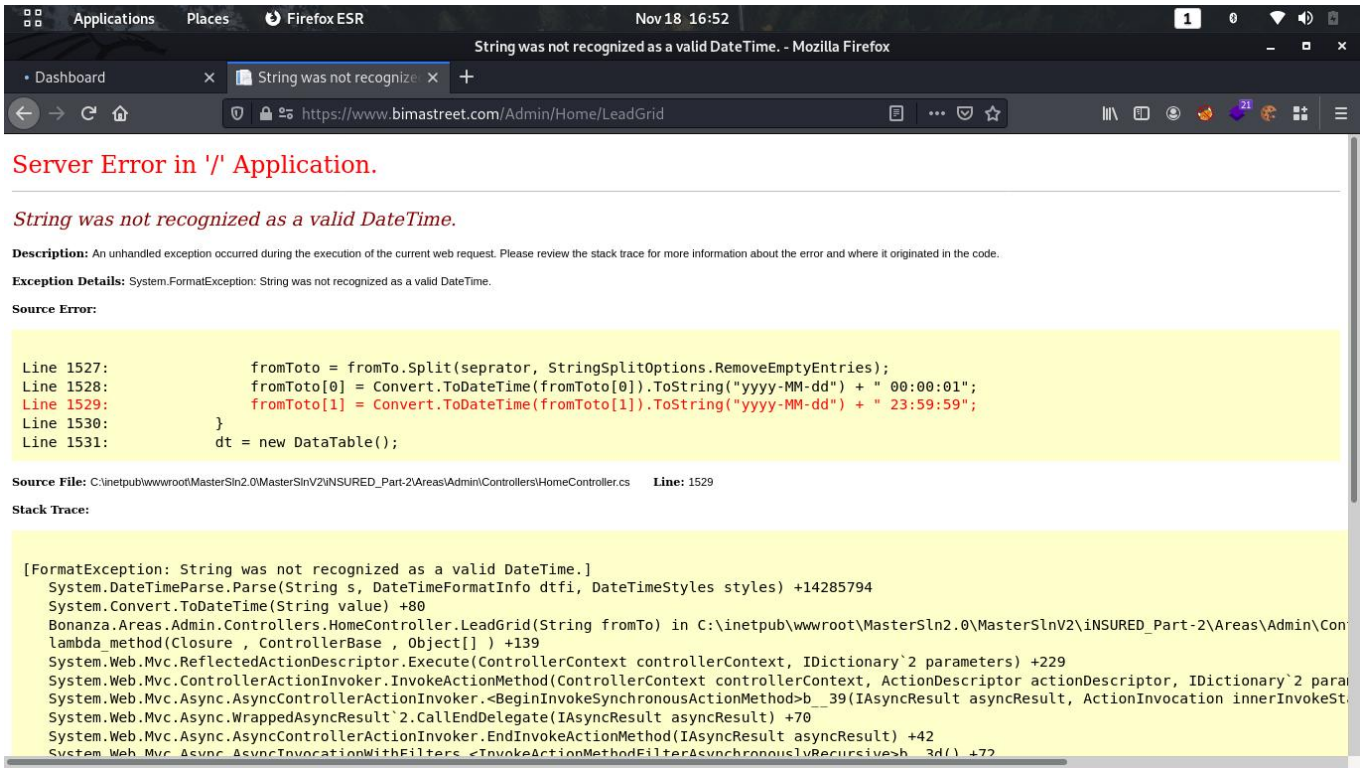
Page-level tracing returns the same information, but relating only to the current request. This may still contain sensitive data in session and server variables that would be of use to an attacker.

Proof of Concept:









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:

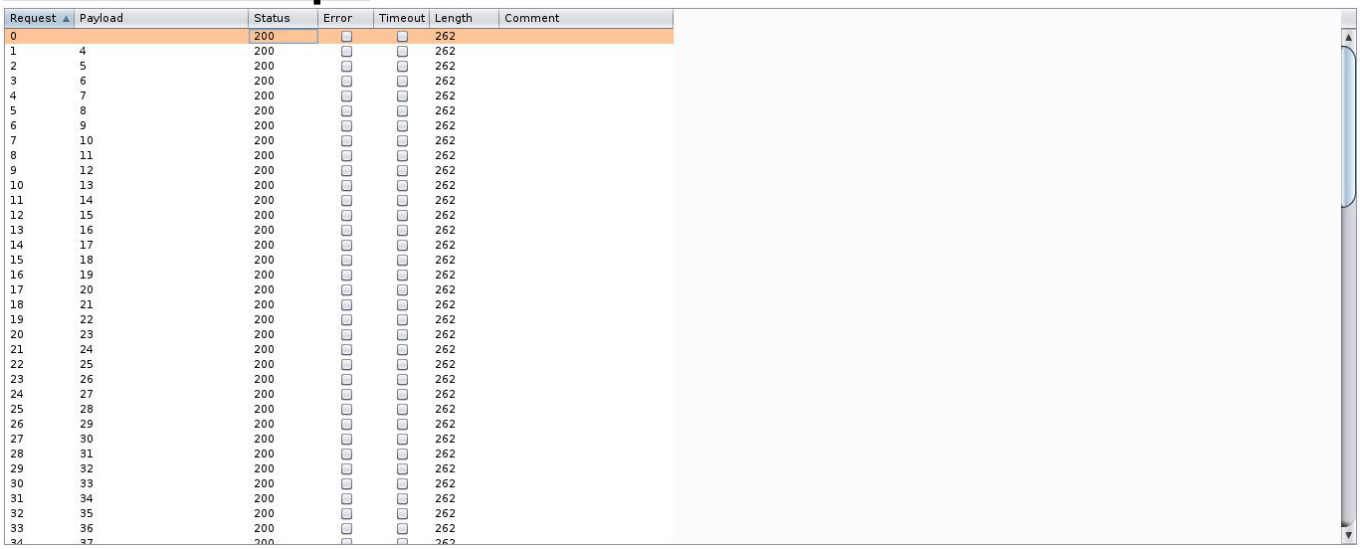
Name of Vulnerability	No Rate Limiting on Sensitive Endpoints
URL	https://www.bimastreet.com/myaccount/Account/CallCheck https://www.bimastreet.com/ProposalHealth/ShareEmail https://bimastreet.com/ProposalMotor/S

	endOTP?mobileno=8279329094
Risk	**High**

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	

Request | Response

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
POST /myaccount/Account/CallCheck HTTP/1.1
Host: www.bimastreet.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 640
Origin: https://www.bimastreet.com
Connection: close
Referer: https://www.bimastreet.com/myaccount/Setup/Mastervehiclesetup
Cookie: ASP.NET_SessionId=wm4d4qqdprtgunewwgzkkq2v

{"URL":"http://corecrmapi.stariengineering.com/api/Setup/AddManufacturer","PostString":
"{\"Token\":\"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbmlxdWVfbmFtZSI6IkJpbWEgU3RyZWV0Iiwicm9sZSI6IjEiLCJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9tb2JpbGVwaG9uZSI6Ik5VTEwiLCJlbWFpbCI6ImJtc0BnbWFpbC5jb20iLCJuYW1laWQiOiIzNSIsImh0dHA6Ly9zY2hlbWFzLmlpY3Jvc29mdC5jb20vd3MvMjAwOC8wNi9pZGVudGl0eS9jbGFpbXMvdXNlcmRhdGEiOiIyNDAyIiwibmJmIjoxNjA1Nzc0NzM4LCJleHAiOjE2MDU3NzgzMzgsImlhdCI6MTYwNTc3NDczOH0.MaQrVwhqogRdS8mpo-xdwtUvVi0Cq6QoL5Oc9CvPYGQ\",\"IsCar\":false,\"IsBike\":true,\"IsActive\":false,\"ManufacturerName\":\"test3\"}"}
```

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."
```

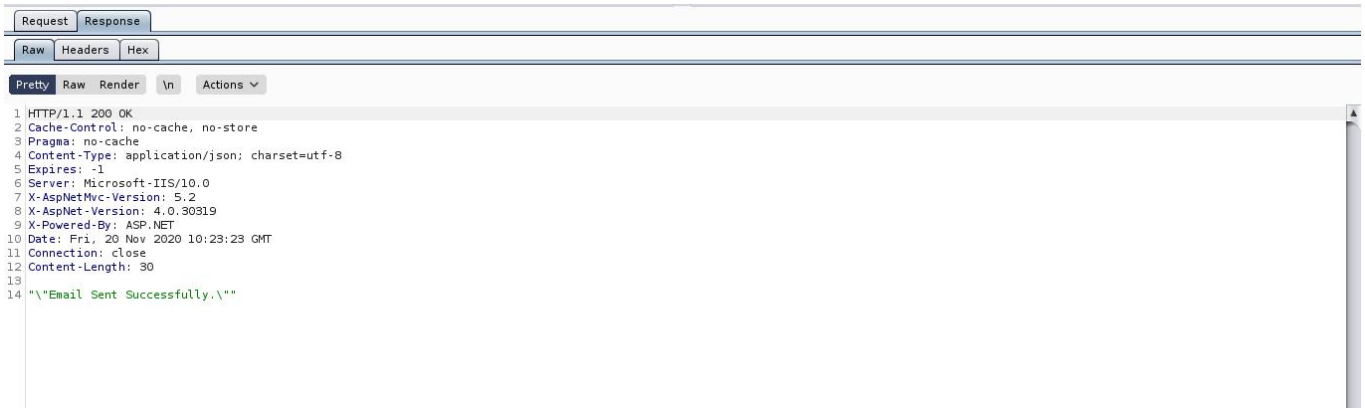
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			344	
1	87131	200			344	
2	87132	200			344	
3	87133	200			344	
4	87134	200			344	
7	87137	200			344	
8	87138	200			344	
9	87139	200			344	
11	87141	200			344	
12	87142	200			344	
13	87143	200			344	
15	87145	200			344	
18	87148	200			344	
19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

Request | Response

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /ProposalHealth/ShareEmail 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: 87131
10 Origin: https://www.bimastreet.com
11 Connection: close
12 Referer: https://www.bimastreet.com/ProposalHealth/GetFullDetails
13 Cookie: ASP.NET_SessionId=0mdldeOgwqrexgdbq1bwjnzs
14
15 model%5BClientURL%5D=www.bimastreet.com&model%5BEnquiryNo%5D=BMS%2FENQ%2F538581&model%5BToEmail%5D=robotmr786%40gmail.com&model%5BUrl%5D=
   https%3A%2F%2Fwww.bimastreet.com%2FProposalHealth%2FGetFullDetails%3Fenquiryno%3DBMS%2FENQ%2F538581&model%5BProposalReq%5D=
   %7B%26quot%3BSumInsured%26quot%3B%3A500000%2C%26quot%3BPolicyTerm%26quot%3B%3A1%2C%26quot%3BPinCode%26quot%3B%3A%26quot%3B201011%26quot%3B%2C%26quot%3BMobileNumber%26quot%3B%3A8279329094%2
   C%26quot%3BClientURL%26quot%3B%3A%26quot%3Bhttps%3A%2F%2Fwww.bimastreet.com%26quot%3B%2C%26quot%3BTierID%26quot%3B%3A0%2C%26quot%3BCompanyName%26quot%3B%3A%26quot%3BRaheja%26quot%3B%2C%26q
   uot%3BEnquiryNo%26quot%3B%3A%26quot%3BBMS%2FENQ%2F538581%26quot%3B%2C%26quot%3BProposerName%26quot%3B%3A%26quot%3BPOS+TEST%26quot%3B%2C%26quot%3BMarritalStatus%26quot%3B%3A%26quot%3BM%26qu
   ot%3B%2C%26quot%3BProposerEmail%26quot%3B%3A%26quot%3Bashutosh%40reconprolabs.com%26quot%3B%2C%26quot%3BFatherName%26quot%3B%3A%26quot%3BPOS+TEST%26quot%3B%2C%26quot%3BProposerOccupation%2
   6quot%3B%3A%26quot%3B2088~Employee~0052%26quot%3B%2C%26quot%3BproposerPhone%26quot%3B%3A8279329094%2C%26quot%3BProposerGender%26quot%3B%3A%26quot%3BM%26quot%3B%2C%26quot%3BproposerDob%26qu
   ot%3B%3A%26quot%3B11%2F22%2F1997%26quot%3B%2C%26quot%3BpanNumber%26quot%3B%3A%26quot%3B%26quot%3B%2C%26quot%3BgstTypeId%26quot%3B%3A%26quot%3B%26quot%3B%2C%26quot%3BgstIdNumber%26quot%3B%3
   A%26quot%3B%26quot%3B%2C%26quot%3BannualIncome%26quot%3B%3A500000%2C%26quot%3BHealthQuoteResponse%26quot%3B%3A%7B%26quot%3BPlanNo%26quot%3B%3A1%2C%26quot%3BCompanyID%26quot%3B%3A148%2C%26q
   uot%3BCompanyName%26quot%3B%3A%26quot%3BRaheja%26quot%3B%2C%26quot%3BKey%26quot%3B%3A%26quot%3B148-2_500000%26quot%3B%2C%26quot%3BSumInsured%26quot%3B%3A500000%2C%26quot%3BTotalPremium%26q
   uot%3B%3A2321%2C%26quot%3BBasePremium%26quot%3B%3A1966.949152542373%2C%26quot%3BPolicyTerm%26quot%3B%3A1%2C%26quot%3BPlanName%26quot%3B%3A%26quot%3BHealth+Qube+Super+saver%26quot%3B%2C%26q
   uot%3BPlanCode%26quot%3B%3Anull%2C%26quot%3BPinCode%26quot%3B%3A%26quot%3B201011%26quot%3B%2C%26quot%3BProductCode%26quot%3B%3A%26quot%3B1A%26quot%3B%2C%26quot%3BUrlLogo%26quot%3B%3A%26quo
   t%3Bhttps%3A%2F%2Fi.ibb.co%2FfNTkRPy%2FRaheja.png%26quot%3B%2C%26quot%3BAdult%26quot%3B%3A0%2C%26quot%3BChild%26quot%3B%3A0%2C%26quot%3BIsActive%26quot%3B%3Atrue%2C%26quot%3BEnquiryNo%26qu
   ot%3B%3A%26quot%3BBMS%2FENQ%2F538581%26quot%3B%2C%26quot%3BRequest%26quot%3B%3A%26quot%3B%7B%5C%26quot%3BClientCreation%5C%26quot%3B%3A%7B%5C%26quot%3Bsalutation%5C%26quot%3B%3A%5C%26quot%
   3BMr%5C%26quot%3B%2C%5C%26quot%3BfirstName%5C%26quot%3B%3A%5C%26quot%3BVishnu+%5C%26quot%3B%2C%5C%26quot%3BmiddleName%5C%26quot%3B%3A%5C%26quot%3B%5C%26quot%3B%2C%5C%26quot%3BlastName%5C%2
   6quot%3B%3A%5C%26quot%3BDixit%5C%26quot%3B%2C%5C%26quot%3BdateofBirth%5C%26quot%3B%3A%5C%26quot%3B11%2F20%2F1998%5C%26quot%3B%2C%5C%26quot%3Bgender%5C%26quot%3B%3A%5C%26quot%3BM%5C%26quot%
   3B%2C%5C%26quot%3BeducationalQualification%5C%26quot%3B%3A%5C%26quot%3B%5C%26quot%3B%2C%5C%26quot%3BpinCode%5C%26quot%3B%3A%5C%26quot%3B201011%5C%26quot%3B%2C%5C%26quot%3BuidNo%5C%26quot%3
```



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.

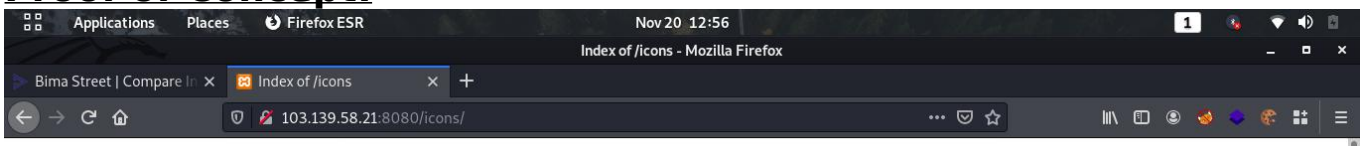
10.8 Directory Traversal:

Name of Vulnerability	Directory Traversal
URL	http://103.139.58.21:8080/img/ http://103.139.58.21:8080/icons/ http://103.139.58.21:8080/dashboard/docs/ http://103.139.58.21:8080/dashboard/images/ http://103.139.58.21:8080/dashboard/Images/ http://103.139.58.21:8080/dashboard/javascripts/ http://103.139.58.21:8080/dashboard/phpinfo.php http://103.139.58.21:8080/dashboard/stylesheets/
Risk	**High**

Description:

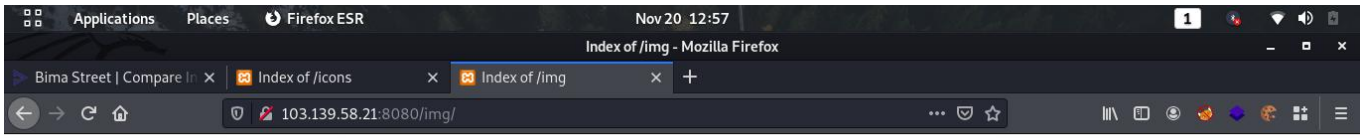
A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed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

Proof of Concept:



Index of /icons

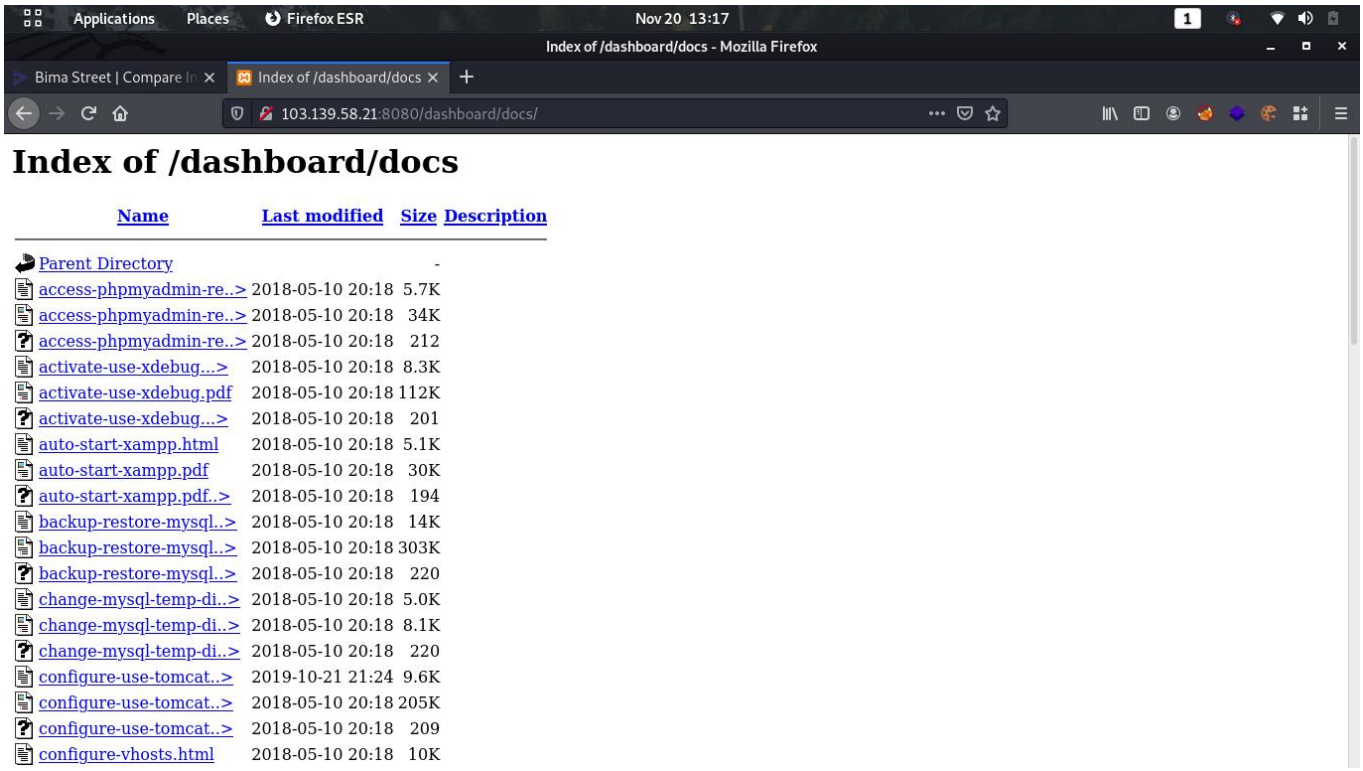
Name	Last modified	Size	Description
Parent Directory		-	
a.gif	2004-11-21 02:46	246	
a.png	2007-09-11 12:41	306	
alert.black.gif	2004-11-21 02:46	242	
alert.black.png	2007-09-11 12:41	293	
alert.red.gif	2004-11-21 02:46	247	
alert.red.png	2007-09-11 12:41	314	
apache_pb.gif	2013-05-04 20:22	4.4K	
apache_pb.png	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	



Index of /img

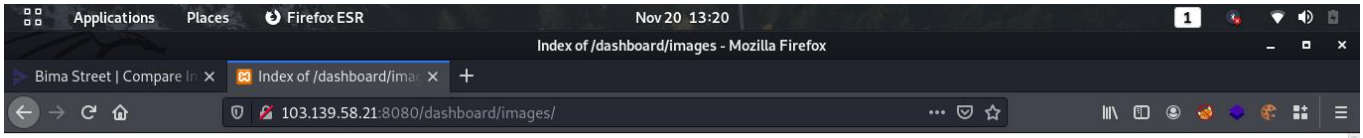
Name	Last modified	Size	Description
Parent Directory		-	
module_table_bottom.png	2019-08-27 19:32	751	
module_table_top.png	2019-08-27 19:32	337	

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



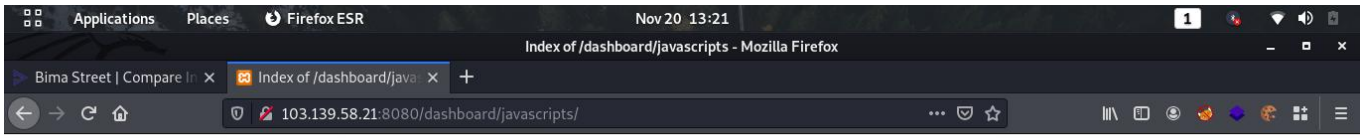
Index of /dashboard/docs

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



Index of /dashboard/images

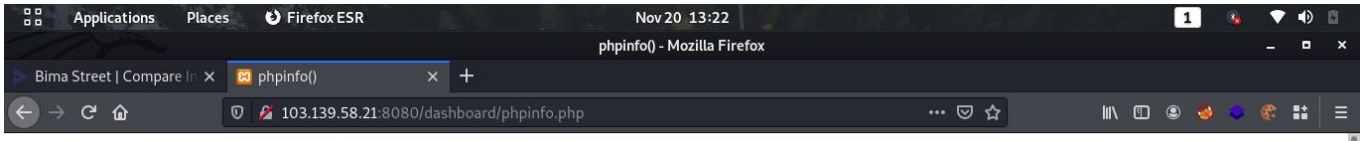
Name	Last modified	Size	Description
Parent Directory		-	
addons-video-thumb.png	2018-05-10 20:18	17K	
addons/	2020-07-20 10:50	-	
apple-logo.png	2018-05-10 20:18	1.5K	
background.png	2018-05-10 20:18	2.7K	
bitnami-xampp.png	2018-05-10 20:18	22K	
bitnami-xampp/	2020-07-20 10:50	-	
blog/	2020-07-20 10:50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



Index of /dashboard/javascripts

Name	Last modified	Size	Description
Parent Directory		-	
all.js	2018-05-10 20:18	184K	
modernizr.js	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



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	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

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.

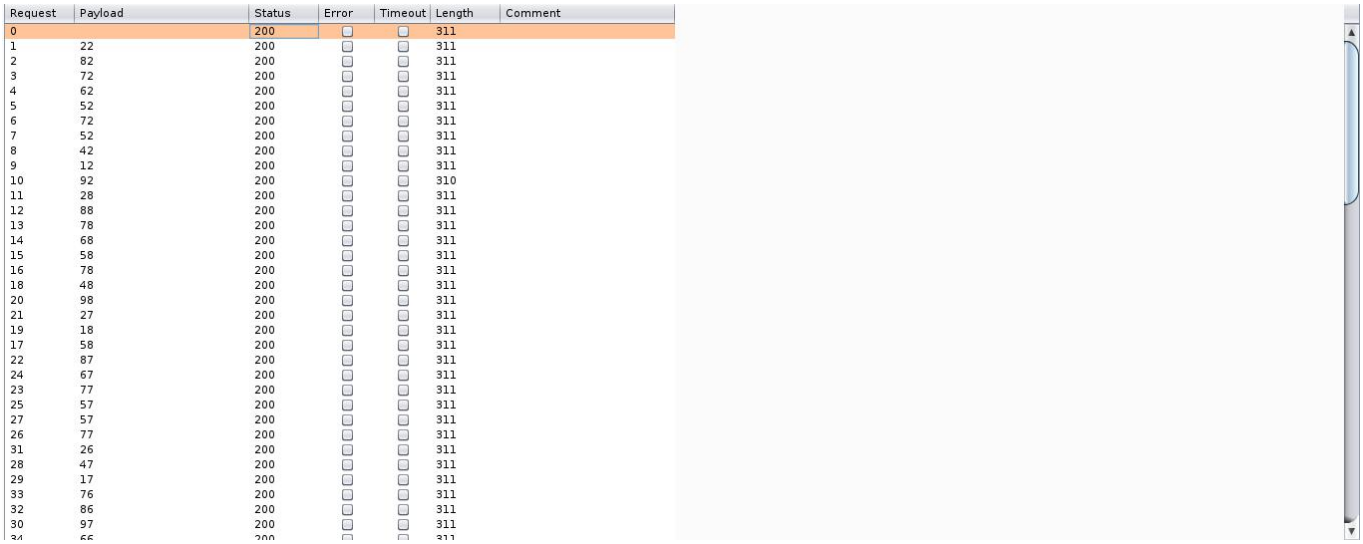
10.9 OTP Bypass through no rate limiting:

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

Description:

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

Proof of Concept:



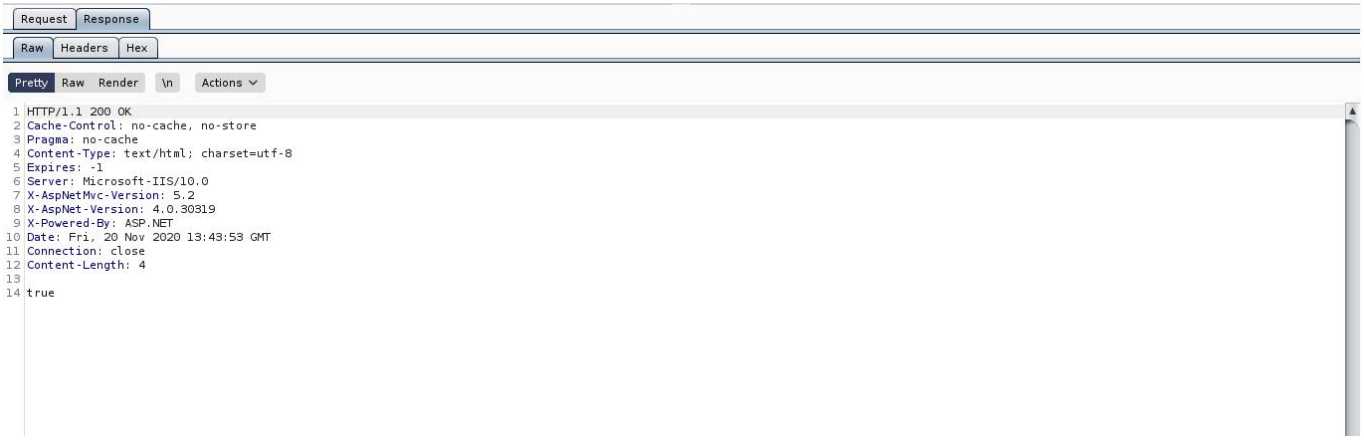
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			311	
1	22	200			311	
2	82	200			311	
3	72	200			311	
4	62	200			311	
5	52	200			311	
6	72	200			311	
7	52	200			311	
8	42	200			311	
9	12	200			311	
10	92	200			310	
11	28	200			311	
12	88	200			311	
13	78	200			311	
14	68	200			311	
15	58	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	

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=cqo5xllesvqmlybmaxlblpwa
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:

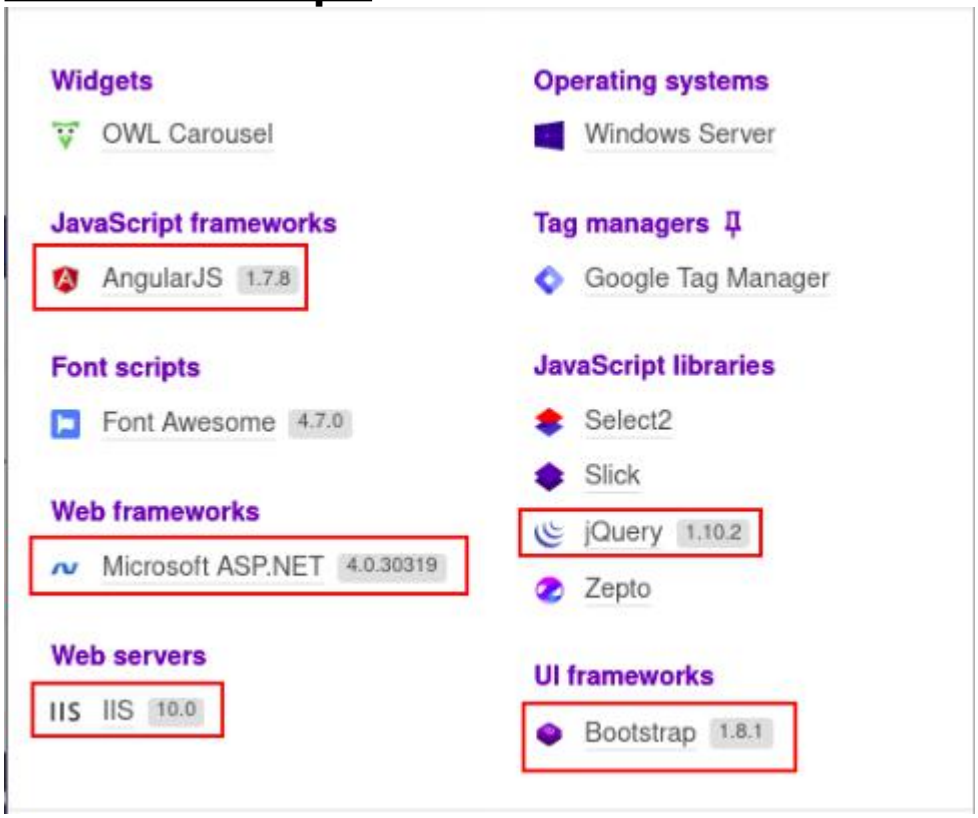
Name of Vulnerability	Using component with Known vulnerabilities

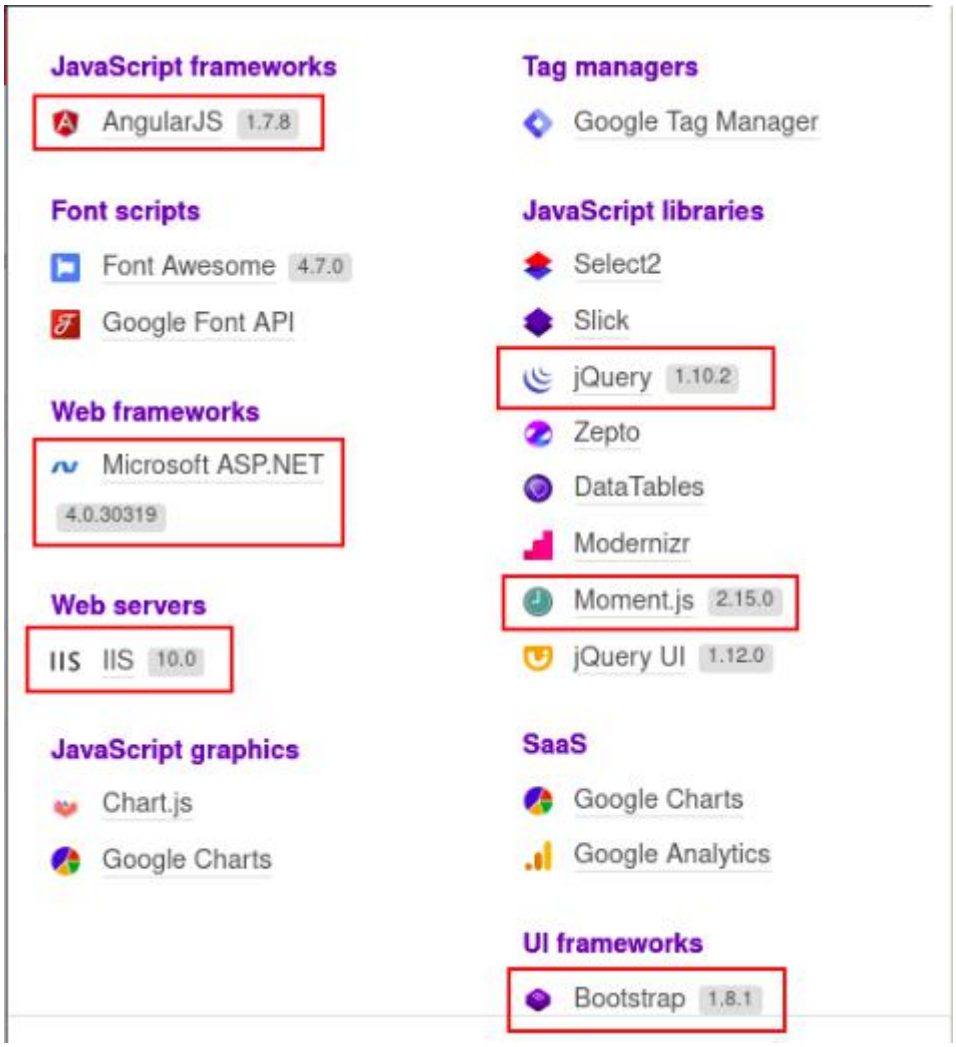
URL	https://www.bimastreet.com/
Risk	Medium

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:





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	https://www.bimastreet.com/
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:

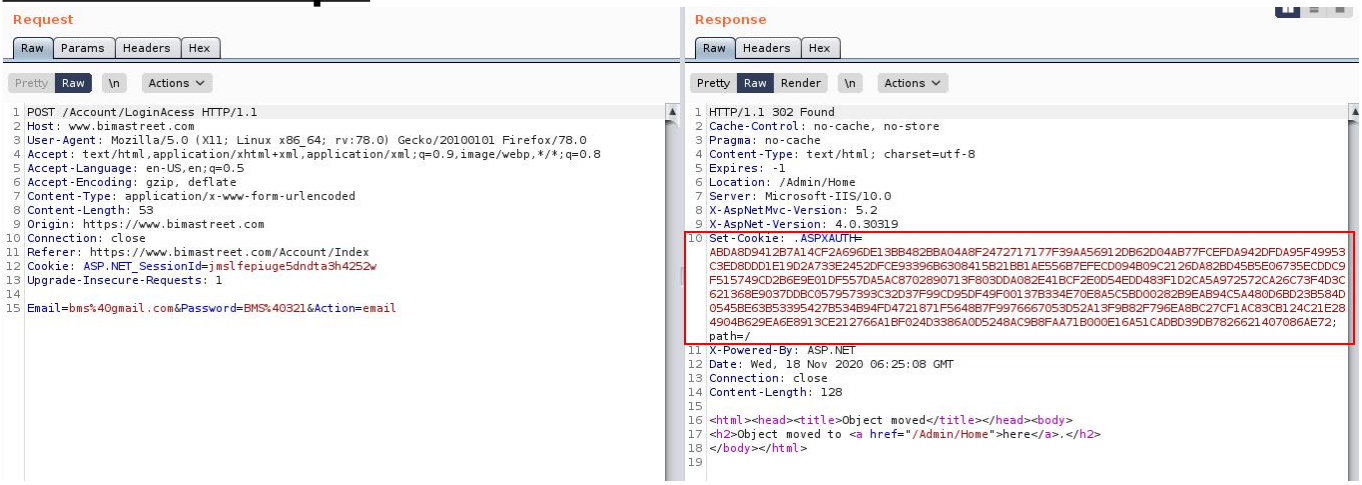
Name of Vulnerability	SSL Cookie without Secure flag and HTTPOnly Flag
URL	https://www.bimastreet.com/Account/Login Acess https://www.bimastreet.com/
Risk Level	Medium

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:



Recommendation:

Set the Secure flag and HttpOnly flag on these cookies.

10.13 Misconfigured Session Management:

Name of Vulnerability	Misconfigured Session Management
URL	https://bimastreet.com/myaccount/Account/CallCheck

Risk	Medium

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.

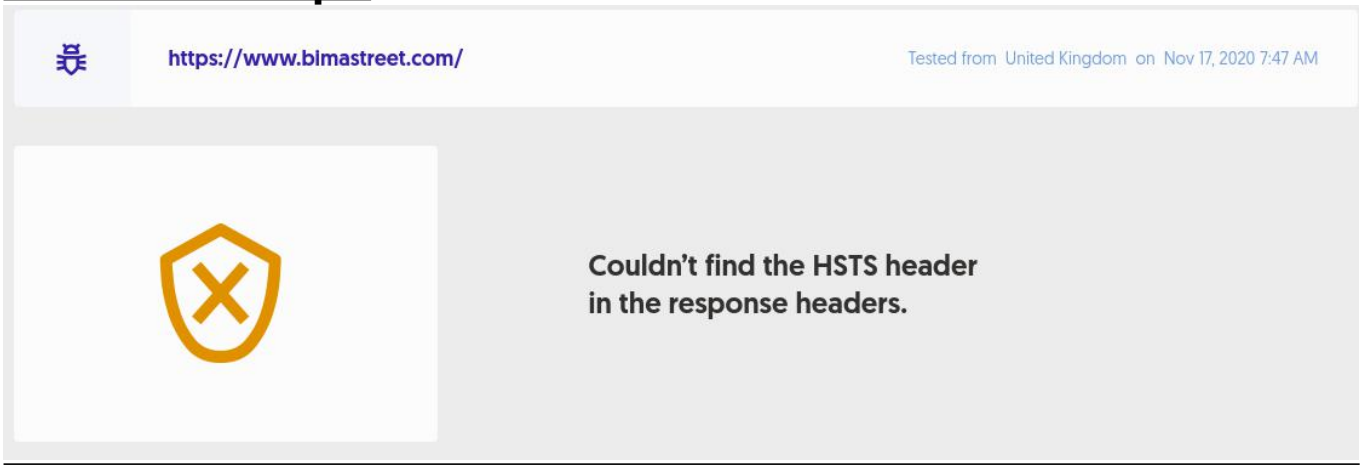
10.14 HTTP Strict-Transport-Security not Enforced:

Name of Vulnerability	HTTP Strict-Transport-Security not Enforced
URL	https://bimastreet.com
Risk	Medium

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:



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:

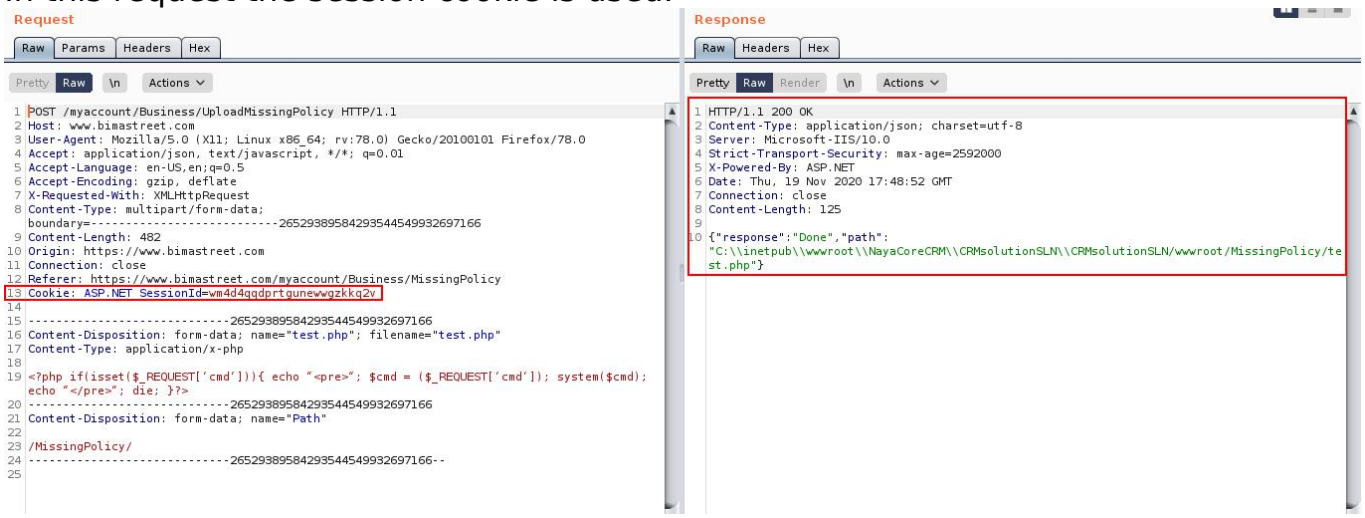
Name of Vulnerability	Cookie Misconfigurtion
URL	https://www.bimastreet.com/myaccount/Business/UploadMissingPolicy
Risk	Medium

Description:

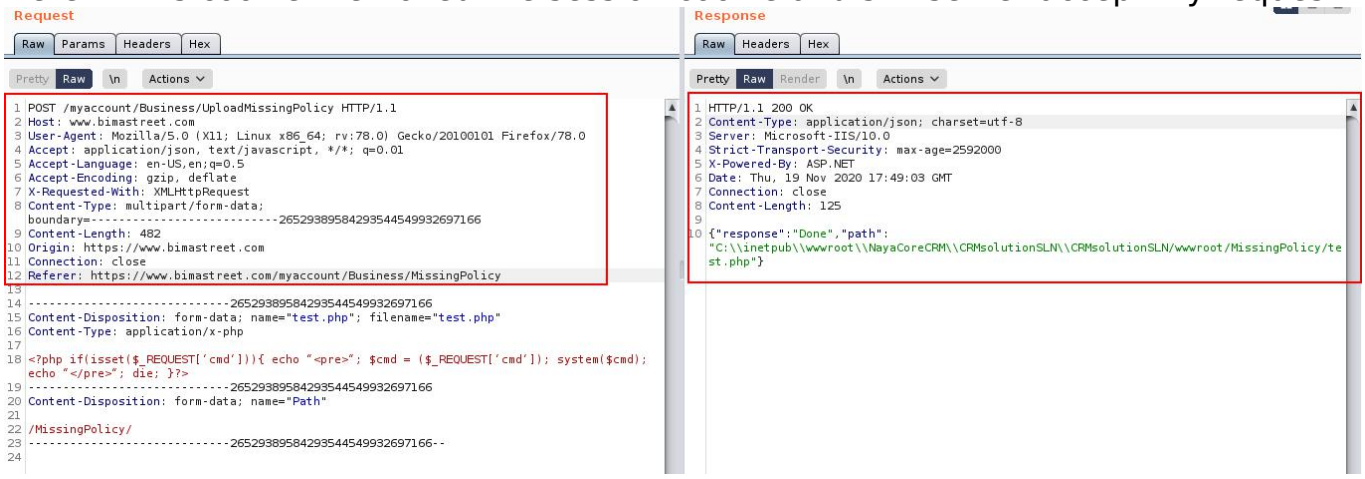
The user can perform any action without the session cookie because session cookie is not validated properly.

Proof of Concept:

In this request the session cookie is used.



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



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	https://www.bimastreet.com
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:

Recommendation:

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

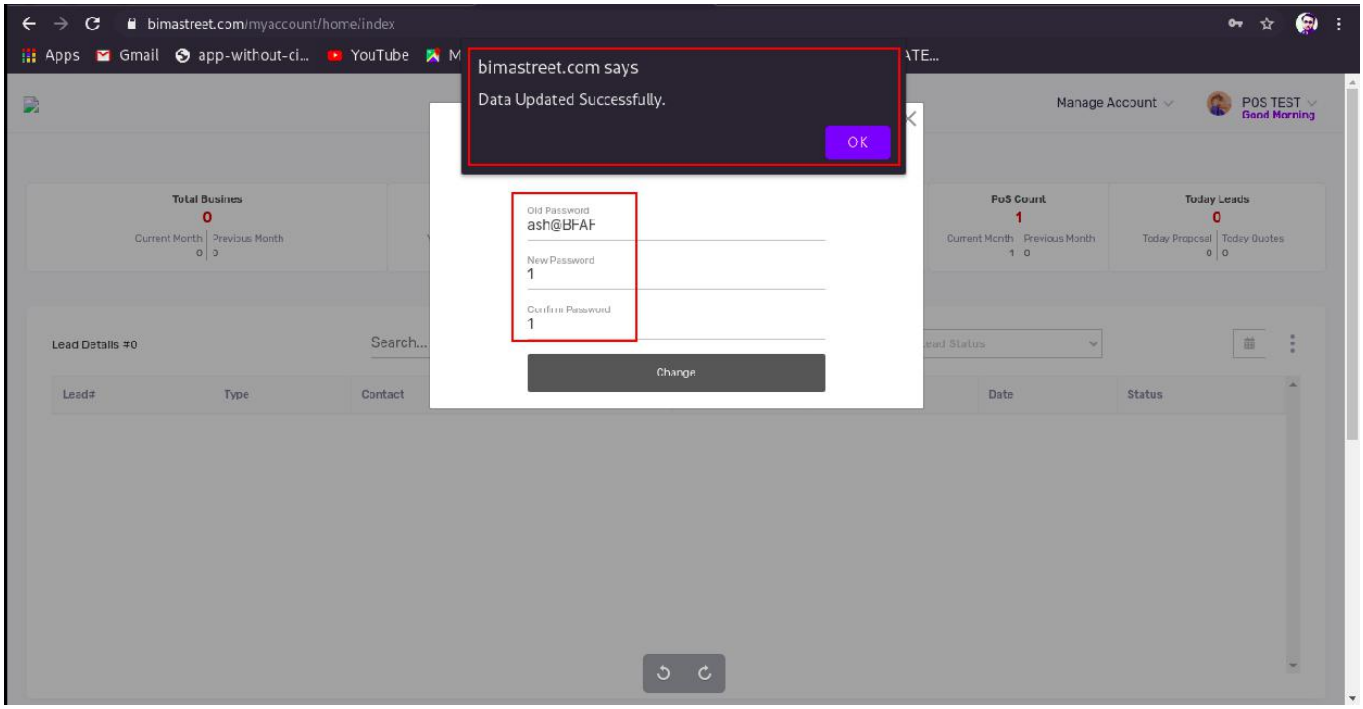
10.17 Weak Password Policy:

Name of Vulnerability	Weak Password Policy
URL	https://bimastreet.com/myaccount/Account/CallCheck
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.

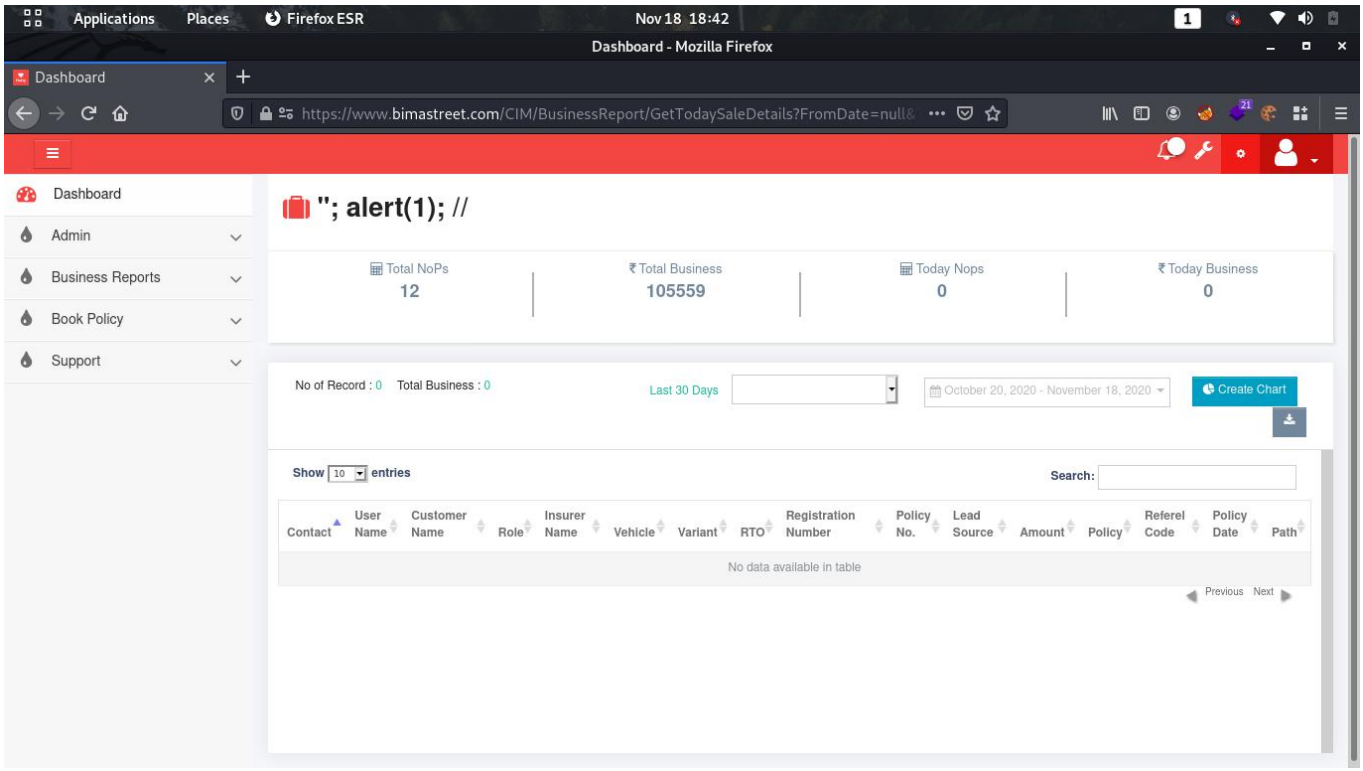
10.18 No Input Validation:

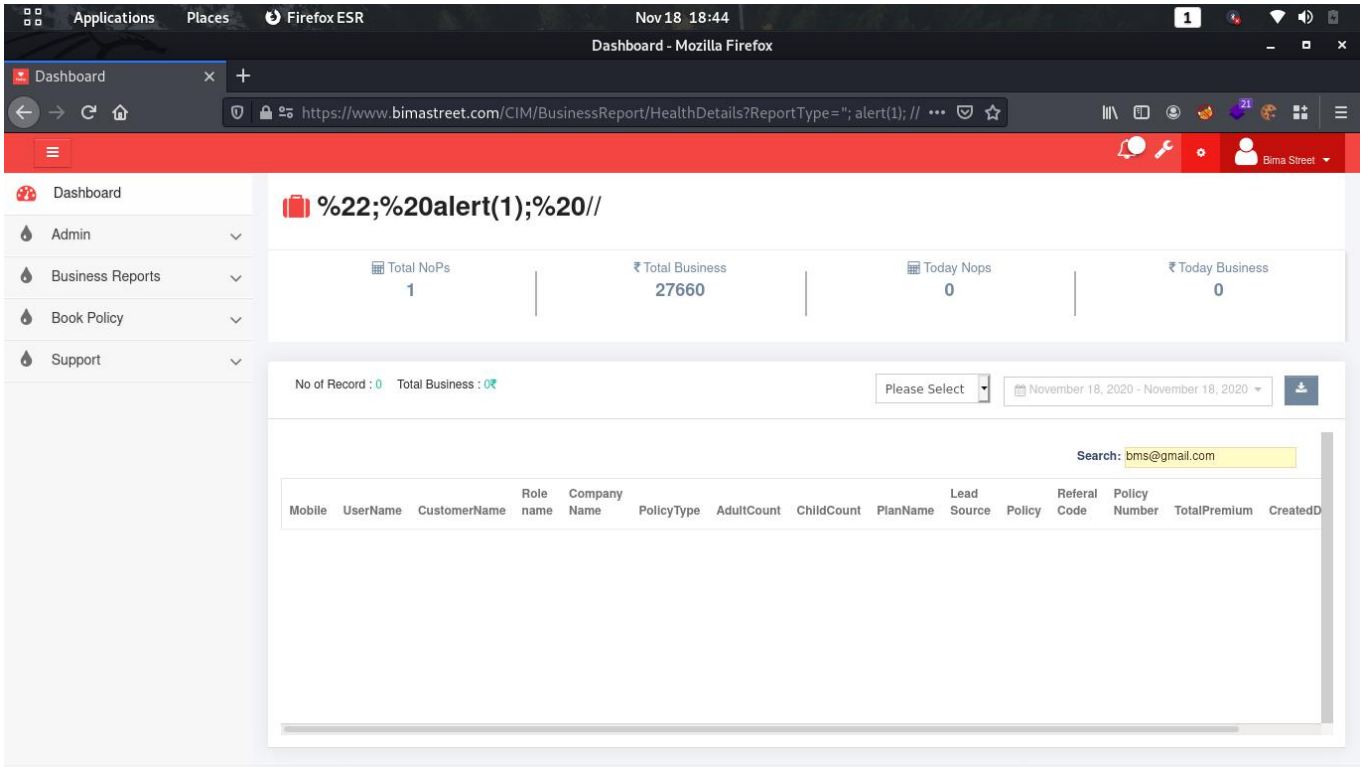
Name of Vulnerability	No Input Validation
URL	https://www.bimastreet.com/CIM/BusinessReport/GetTodaySaleDetails?FromDate=null&ToDate=null&ReportType="; alert(1); // https://www.bimastreet.com/CIM/BusinessReport/HealthDetails?ReportType=%22;%20alert(1);%20//
Risk Level	Low

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:





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.

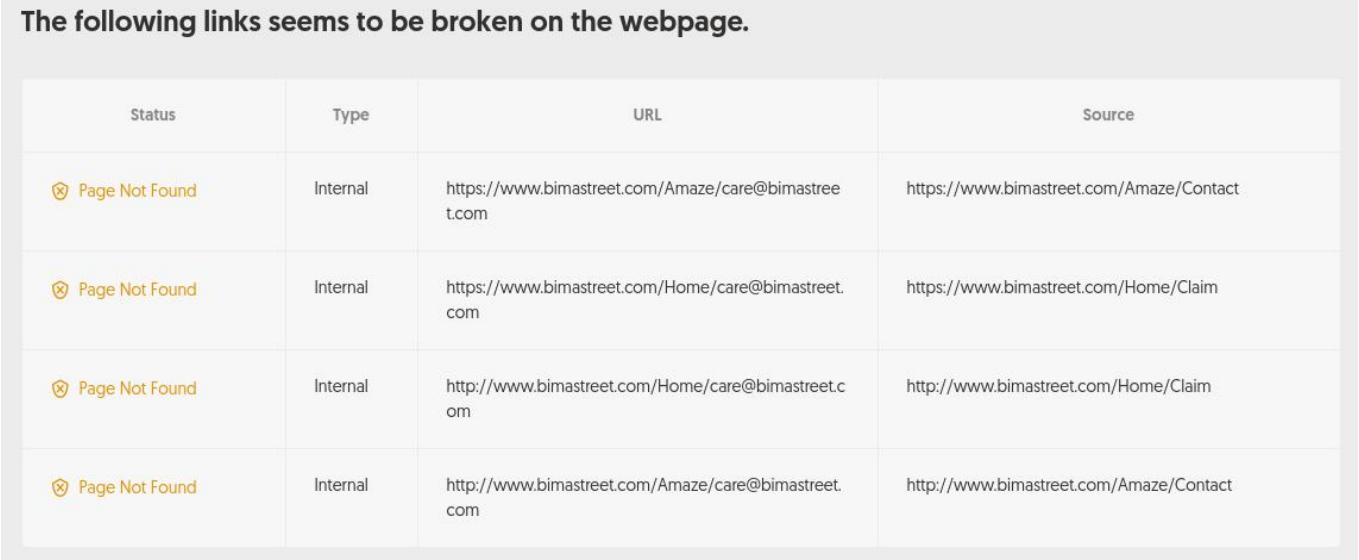
10.19 Broken Links:

Name of Vulnerability	Broken Links
URL	https://www.bimastreet.com/Amaze/care@bimastreet.com https://www.bimastreet.com/Home/care@bimastreet.com http://www.bimastreet.com/Home/care@bimastreet.com http://www.bimastreet.com/Amaze/care@bimastreet.com
Risk Level	Low

Description:

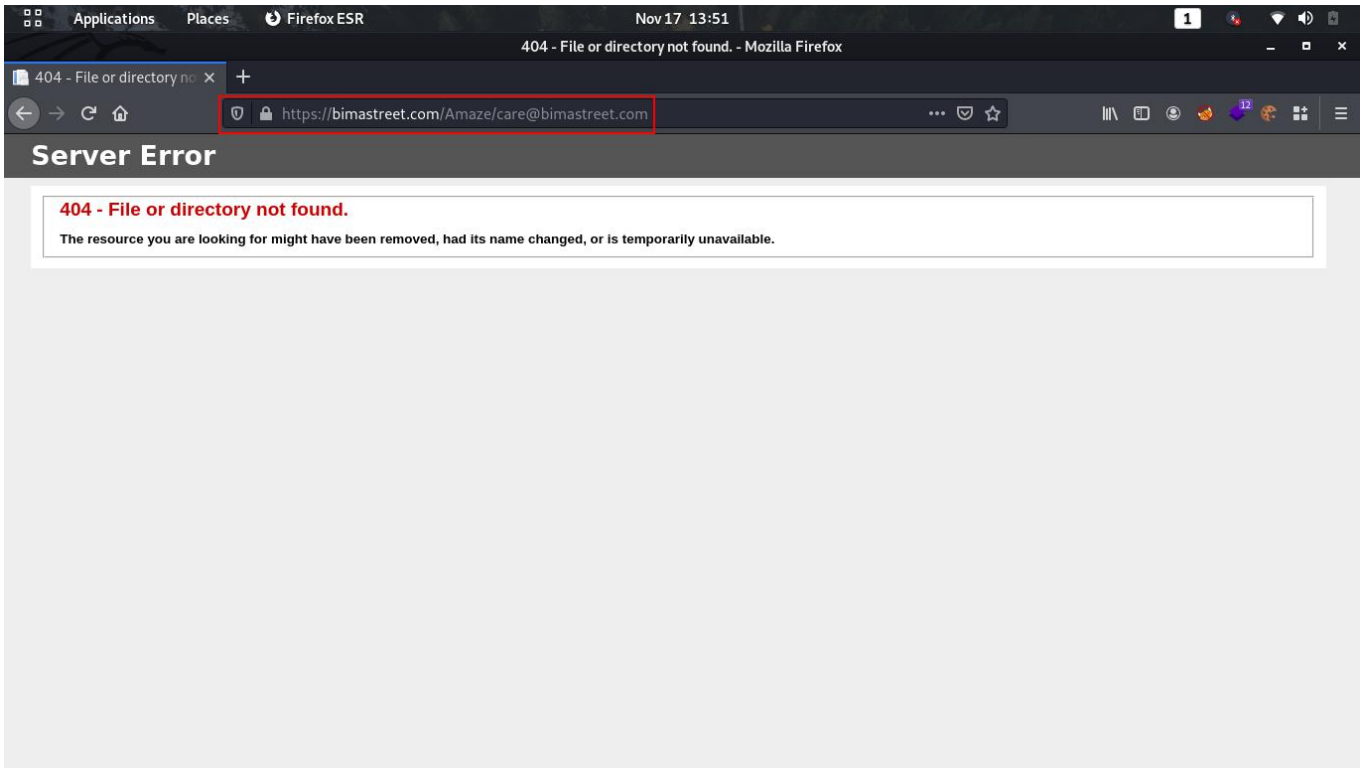
These links is provided in the dashboard but the links are not in use.

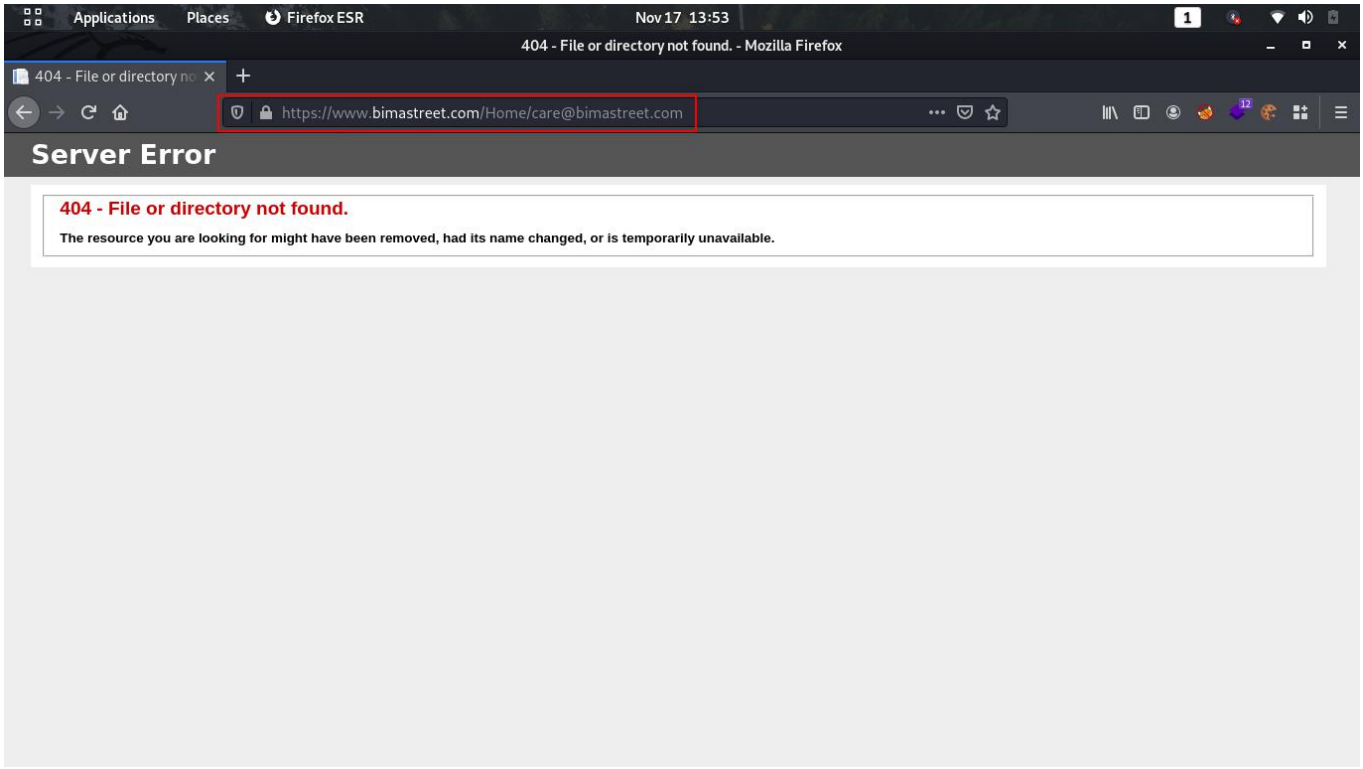
Proof of Concept:

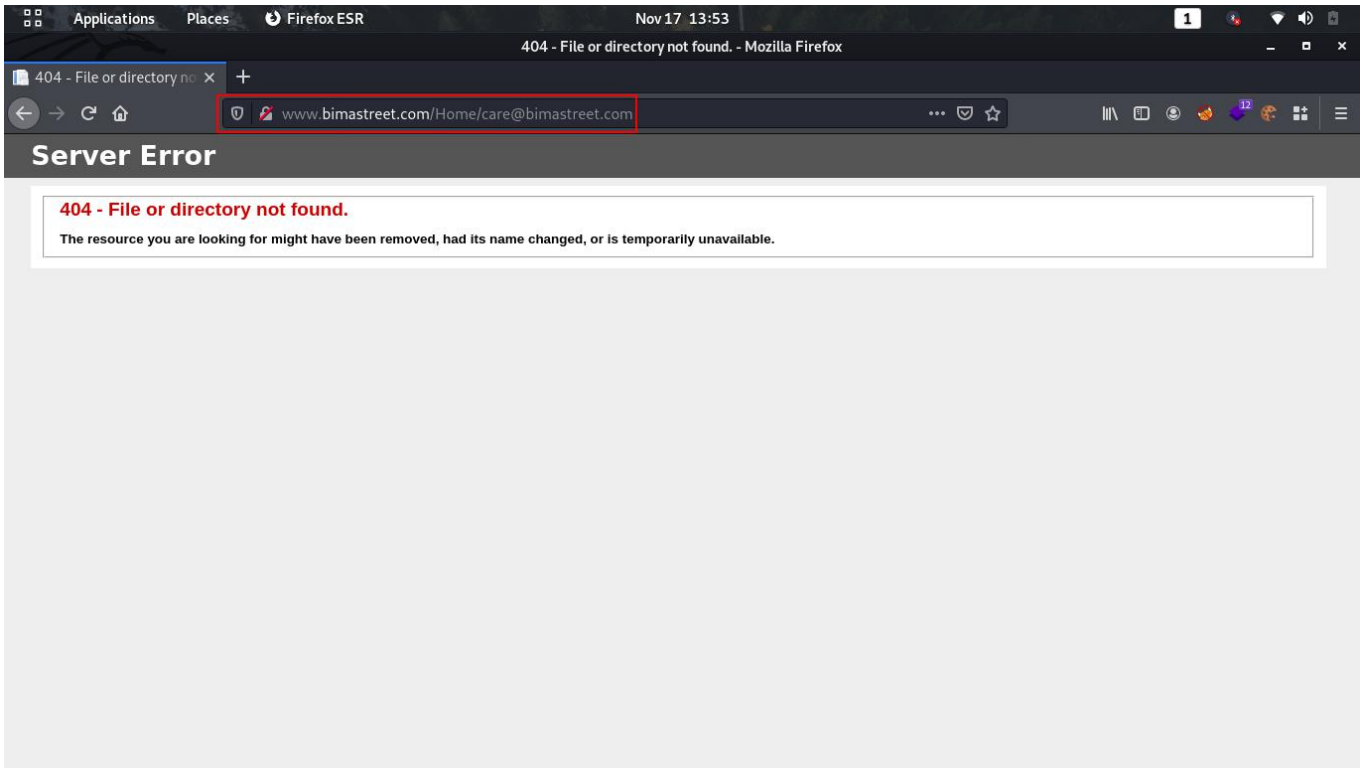


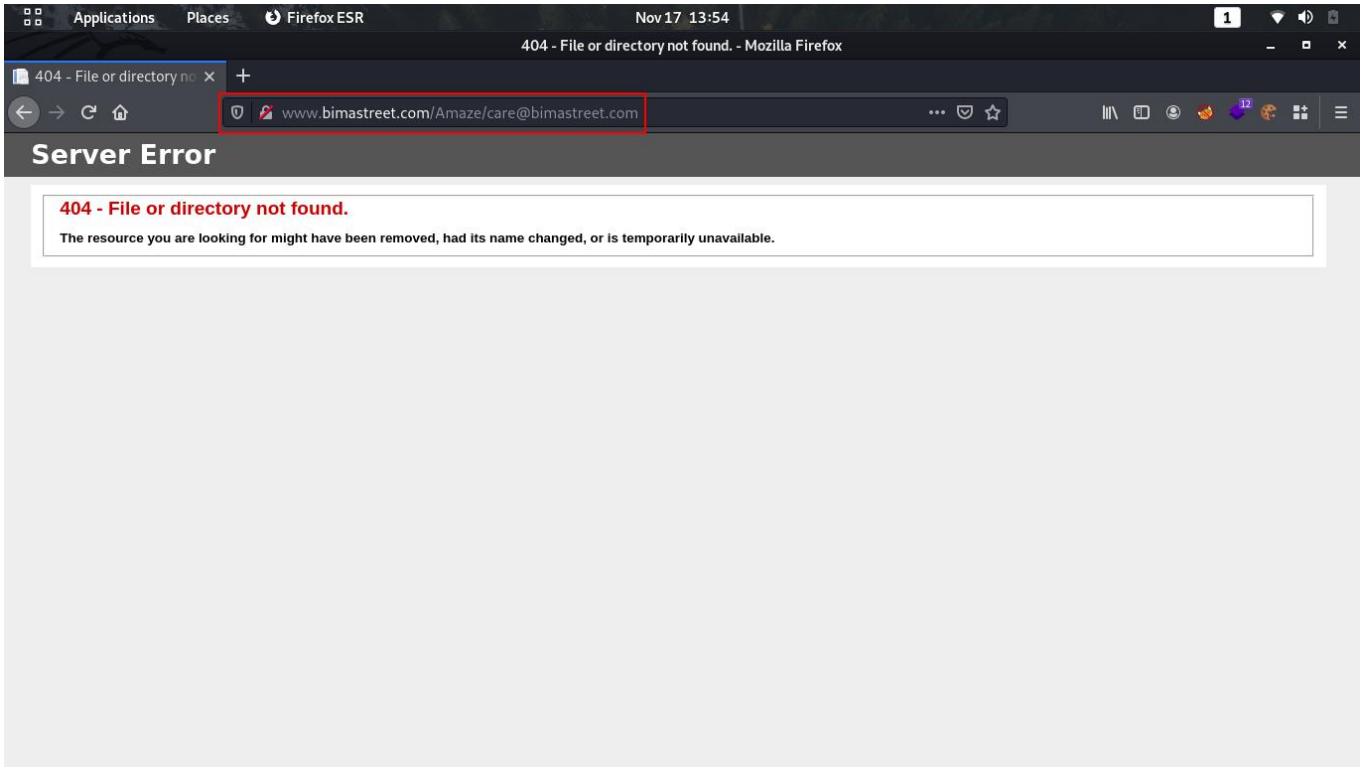
The following links seems to be broken on the webpage.

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.

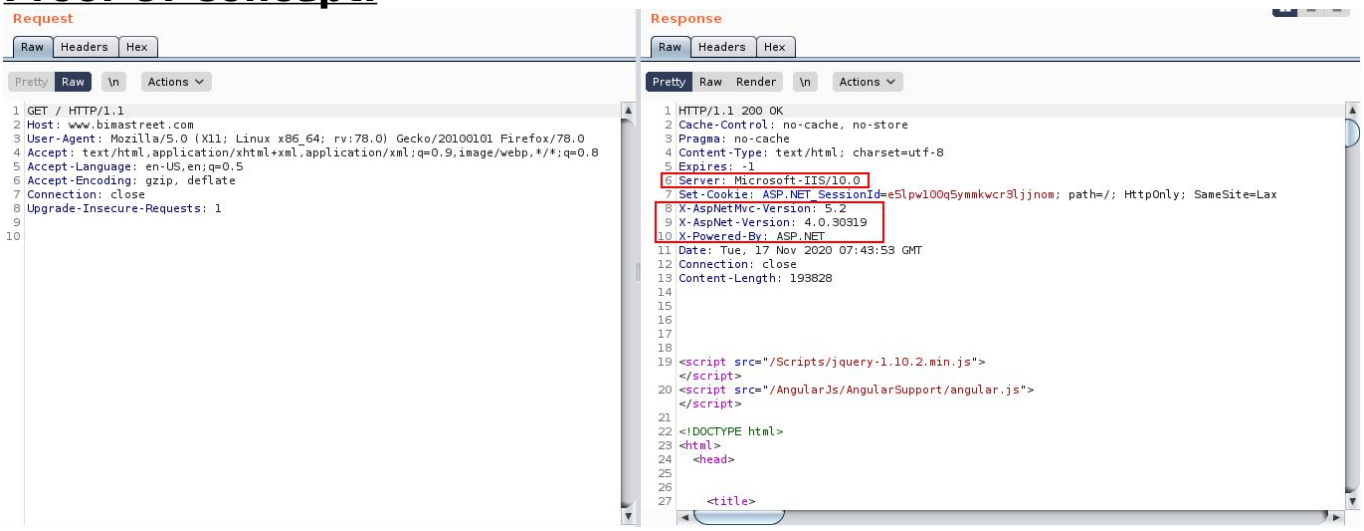
10.20 Banner Grabbing:

Name of Vulnerability	Banner Grabbing
URL	https://www.bimastreet.com/
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 Forbiden URL.

Proof Of Concept:



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	https://www.bimastreet.com/
Risk	Low

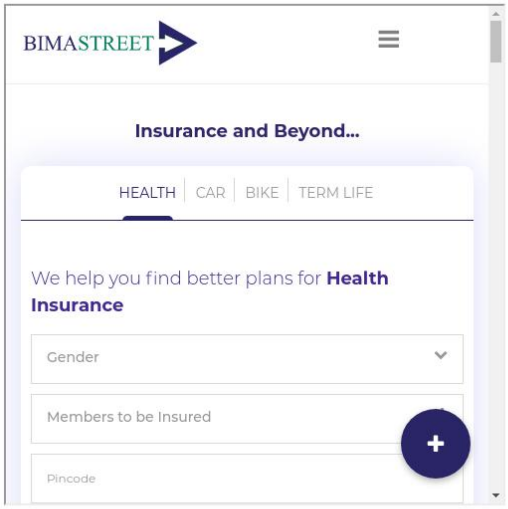
Description:

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!



Recommendation:

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

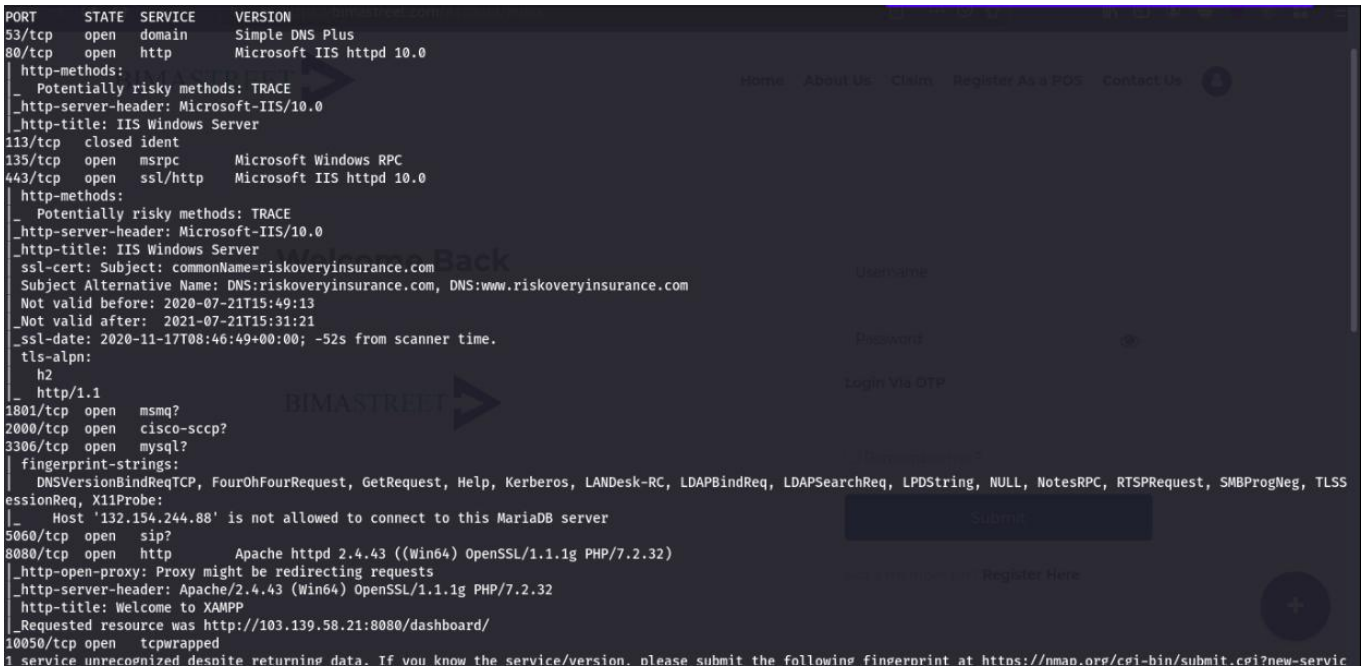
10.22 Various PORTS Open:

Name of Vulnerability	Various PORTS Open
URL	https://www.bimastreet.com/
Risk	Low

Description:

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

Proof of Concept:



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.