Web Security Audit Report of DITE.

https://49.206.243.85:8094/

30 October 2021

AAA Technologies P. Ltd
278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L & T Gate No. 6,
Powai, Andheri (East),
Mumbai 400 072, INDIA
Tel: + 91 22 28573815 / 16
Fax: + 91 22 40152501
info@aaatechnologies.co.in
www.aaatechnologies.co.in

AAA TECHNOLOGIES®
Accurate. Reliable. Innovative.

Document Reference

Item	Description
Document Title	Web Security Audit Report of DITE.
Client	AAA Technologies Ltd.
Report Number	1
Version No.	2.0
File Name	DITE Web application Security .docx
Type	Word Document
Status	Final

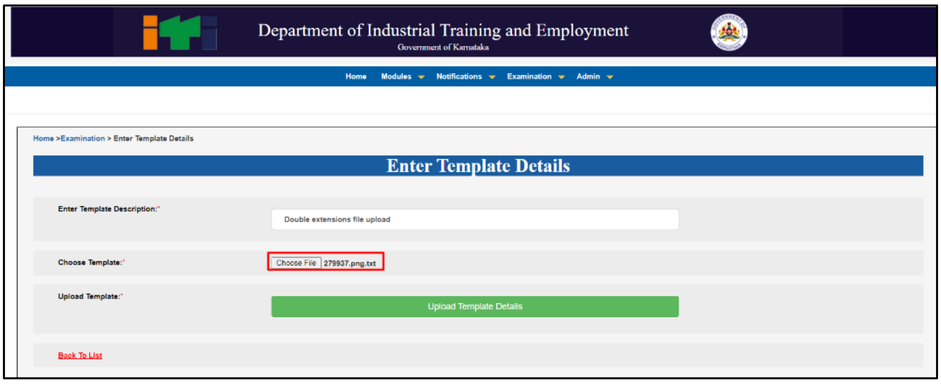
Document Control Status

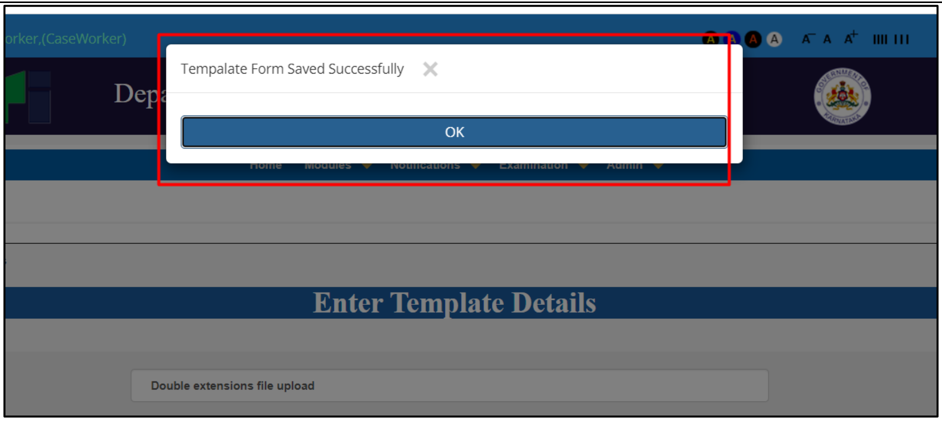
Change No.	Date	Prepared by
1.0	30/09/2021	AAA Technologies Private Limited

Table of Contents

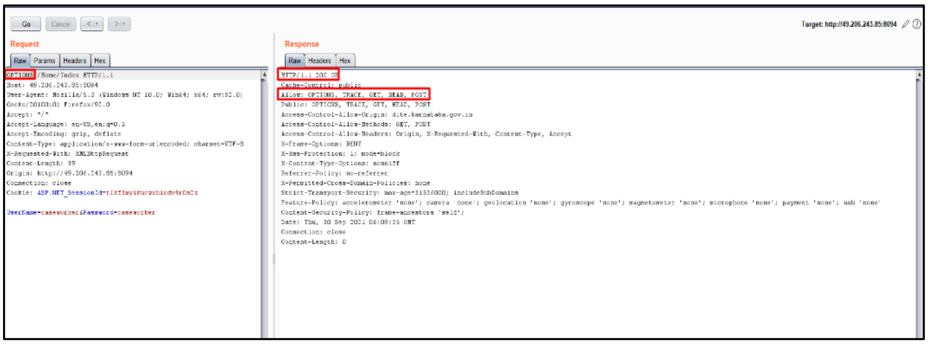
High

1. Malicious File Upload

Vulnerability Title: Malicious file upload is allowed in the application	
Risk	**High**
Abstract	It was observed that malicious file upload is possible in the application
Ease of Exploitation	Easy
Impact	An attacker could use this functionality to upload malicious executable files on the system. To test file upload capabilities.
Recommendations	Following things should be implemented in file upload module: 1 Inspect the content of uploaded files, and enforce a white list of accepted, non-executable content types. Additionally, enforce a blacklist of common executable formats, to hinder hybrid file attacks. 2 Enforce a white list of accepted, non-executable file extensions. 3 If uploaded files are downloaded by users, supply an accurate non-generic Content-type header, and also a Content-disposition header which specifies that browsers should handle the file as an attachment. 4 Enforce a size limit on uploaded files (max 8-10 MB); this can be implemented both within application code and in the web server's configuration. 5 Reject attempts to upload archive formats such as ZIP. 6 Multiple file extension like test.pdf.txt.php.jif.jpg should not be allowed for upload. 7 Proper checks to be put on Content type and MIME type as well.
Snapshot	 Department of Industrial Training and Employment Government of Karnataka Home Modules Notifications Examination Admin Home >Examination > Enter Template Details Upload Template Details Back To List Enter Template Details Enter Template Description:* Double extensions file upload Choose Template:* Choose File 279937.png.txt Upload Template:*

	 orker,(CaseWorker) Tempalate Form Saved Successfully OK Enter Template Details Double extensions file upload
Affected URLs	**throughout the application**

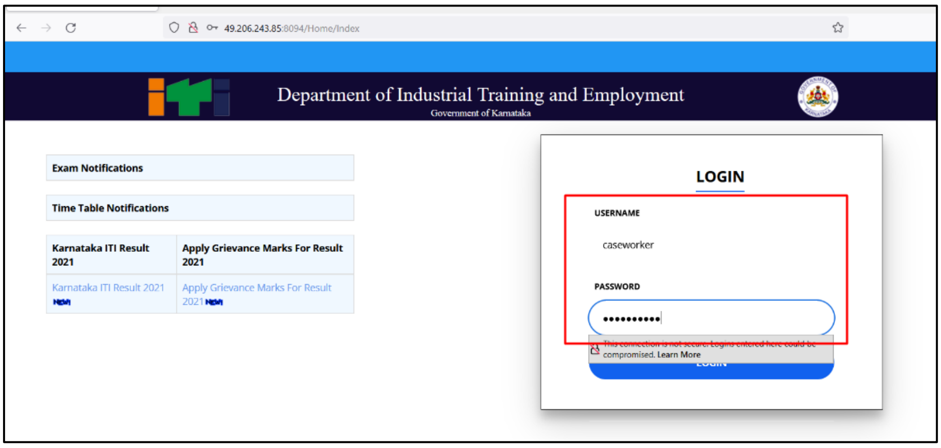
2. DANGEROUS HTTP METHOD ENABLED

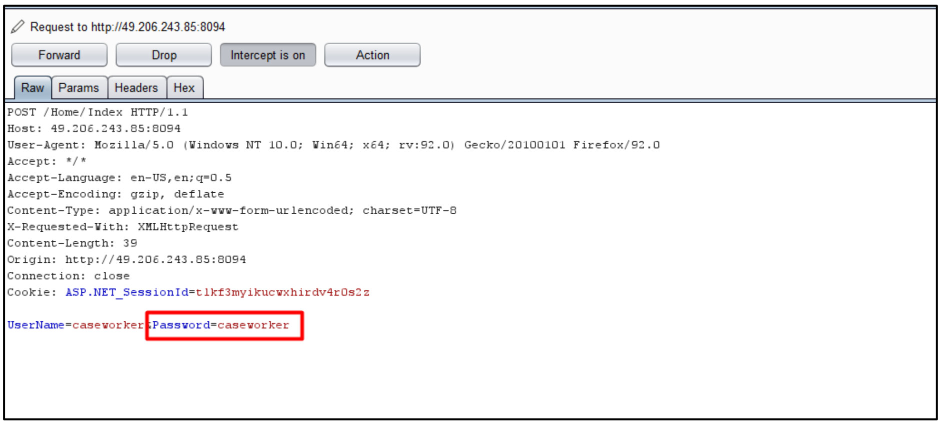
Vulnerability Title: Dangerous HTTP Methods Enabled	
Risk	**High**
Abstract	It was observed that Http options method is enabled on this web server.
Ease of Exploitation	Easy
Impact	It was observed that using the Options method may expose sensitive information that may help an malicious user to prepare more advanced attacks
Recommendations	It is recommended to disable OPTIONS and TRACE methods on the web server
Snapshot	
Affected Site	**Throughout the application**

```
OPTIONS /Home/Index HTTP/1.1
Host: 49.206.243.85:8094
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 39
Origin: http://49.206.243.85:8094
Connection: close
Cookie: ASP.NET_SessionId=t1Xf3myikucwxbirdv4rOs2z

UserName=caseworker&Password=caseworker
```

```
HTTP/1.1 200 OK
Cache-Control: public
Allow: OPTIONS, TRACE, GET, HEAD, POST
Public: OPTIONS, TRACE, GET, HEAD, POST
Access-Control-Allow-Origin: dite.karnataka.gov.in
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000; includeSubDomains
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
Content-Security-Policy: frame-ancestors 'self';
Date: Thu, 30 Sep 2021 06:09:35 GMT
Connection: close
Content-Length: 0
```

3. Password Travel in clear text

Vulnerability Title: password travel in clear text	
Risk	**High**
Abstract	The password between server and client is passed in clear text. It is possible for a malicious user to sniff into the network and access the application and password.
Ease of Exploitation	Easy
Impact	An attacker may be able to Sniff the password.
Recommendations	It is recommended to implement the hashing technique/algorithm used at login in the application. Password should be encrypted every time while being transmitted over the network. The solution is to implement: a) Salted SHA-512 technique in, authentication or login module b) SHA-512 hash technique in, change password and reset password Modules. The pre-requisite to this is that the backend database stores a SHA-512 hash of the password. (SHA-512hash is a cryptographic technique in which the actual value can never be recovered). Here is how the salted SHA-512technique works: When a client requests for the login page, the server generates a random number, the salt, and sends it to the client along with the page. A JavaScript code on the client computes the SHA-512 hash of the password entered by the user. It then concatenates the salt to the hash and re-computes the SHA-512hash. This result is then sent to the server. The server picks the hash of the password from its database, concatenates the salt and computes the SHA-512hash. If the user entered the correct password these two hashes should match. The server compares the two and if they match, the user is authenticated.
Snapshot	 49.206.243.85:8094/Home/Index Department of Industrial Training and Employment Government of Karnataka Exam Notifications Time Table Notifications Karnataka ITI Result 2021 · Apply Grievance Marks For Result 2021 Karnataka ITI Result 2021 NEW · Apply Grievance Marks For Result 2021 NEW LOGIN USERNAME caseworker PASSWORD •••••••••• This connection is not secure. Logins entered here could be compromised. Learn More LOGIN

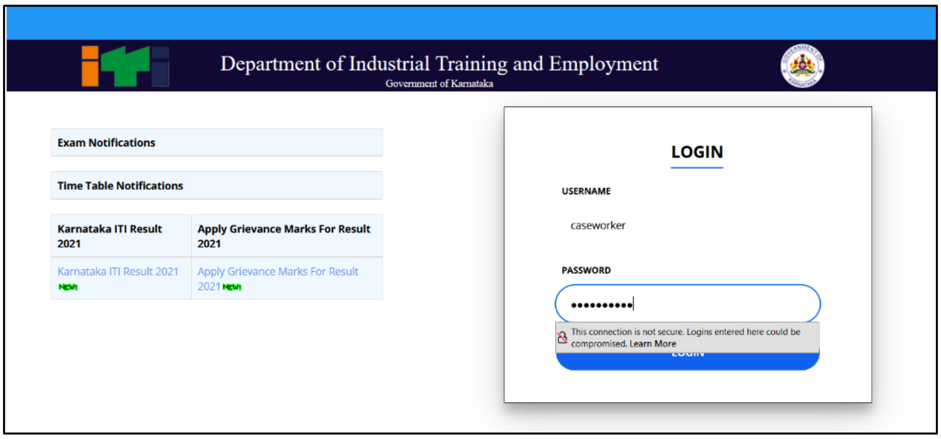
	 Request to http://49.206.243.85:8094 Forward Drop Intercept is on Action Raw Params Headers Hex POST /Home/Index HTTP/1.1 Host: 49.206.243.85:8094 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 39 Origin: http://49.206.243.85:8094 Connection: close Cookie: ASP.NET_SessionId=t1kf3myikucwxhirdv4r0s2z UserName=caseworker&Password=caseworker
Affected URLs	49.206.243.85:8094

Medium

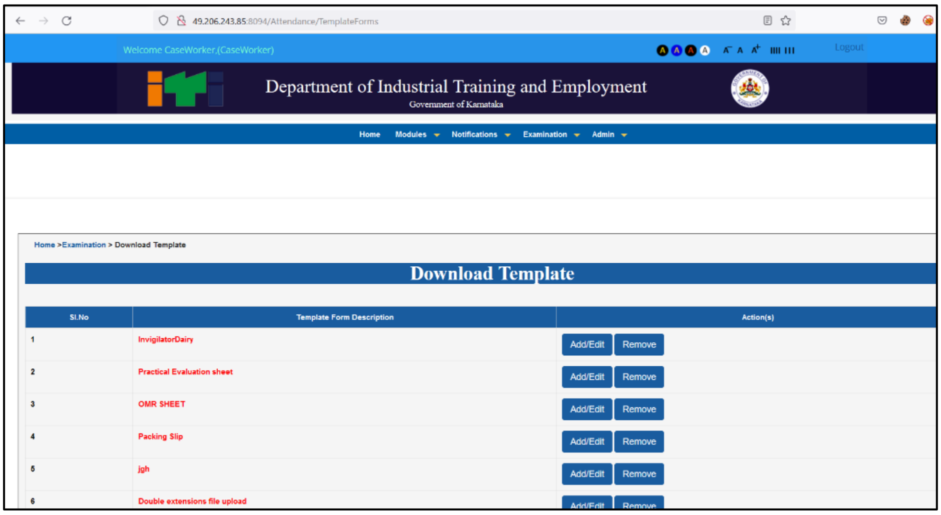
4. Audit Trail Not Implemented Properly

Vulnerability Title: Audit Trail is not implemented in properly	
Risk	**Medium**
Abstract	The application does not maintain the logout action and status of user activity where all user activities have to be logged.
Ease of Exploitation	Easy
Impact	In-case a malicious user tries to attack the application; the application will not be able to trace the attacker
Recommendations	An Audit trail should be incorporated in the application admin module, where all user activities have to be logged. Following points should be considered: • Audits are to be generated at the time of resource access and by the same routines accessing the resource • Information to be logged including the following: IP of the originating client, Date, Time, username if any in addition to other details to be logged in the web server. • These IP, date, time, session details, user details (NO password), referrer, process id to be logged in application logs. • To create audit • logs, use auto numbering so that every logged entry has a log number, which is not editable. Then if one audit entry is deleted a gap in the numbering sequence will appear. • Log entries are to be hashed/ signed so that changes to audit log can be detected. • Audit trails to answer the following • Logging of Authentication Process. Success and failed attempts. • Logging Authentication details and changes. • Software error and failures logged. • Should not be possible to retrieve confidential authentication information from these logs (including passwords) • Is it possible to uniquely identify both client host and user from these logs? • What level of information is logged by the application (read/write access, modification data, and copy/paste data) Are log files time sequential and can they positively identify the time of action?
Snapshot	N/A
Affected URLs	**throughout the application**

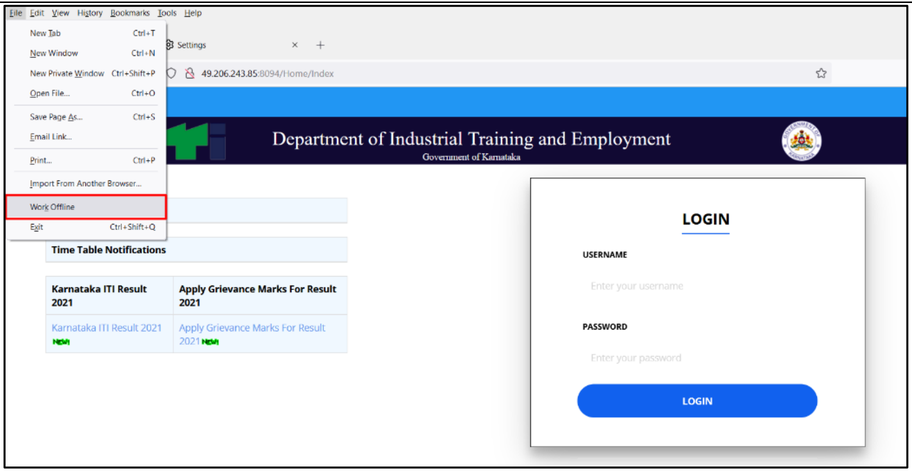
5. Page access Through Cache History

<table>
<tr><th colspan="2">Vulnerability Title: Page access through cache history</th></tr>
<tr><td>Risk</td><td><b>Medium</b></td></tr>
<tr><td>Abstract</td><td>It is possible to view the authenticated page from cache option of the browser.</td></tr>
<tr><td>Ease of Exploitation</td><td>Easy</td></tr>
<tr><td>Impact</td><td>An attacker can gain knowledge if discrepancies between the two pages the backup and original and can aid in more sophisticated attacks.</td></tr>
<tr><td>Recommendations</td><td>It is recommended to remove the Backup Pages from the Web Application</td></tr>
<tr><td>Snapshot</td><td>Step 1: Open URL and login with credentials and browse all the authenticated pages and then logout from the application as shown below:


Department of Industrial Training and Employment
Government of Karnataka
Exam Notifications
Time Table Notifications
Karnataka ITI Result 2021 | Apply Grievance Marks For Result 2021
Karnataka ITI Result 2021 NEW! | Apply Grievance Marks For Result 2021 NEW!
LOGIN
USERNAME
caseworker
PASSWORD
••••••••••
This connection is not secure. Logins entered here could be compromised. Learn More
LOGIN

Step 2:Enter in the web application as shown below:


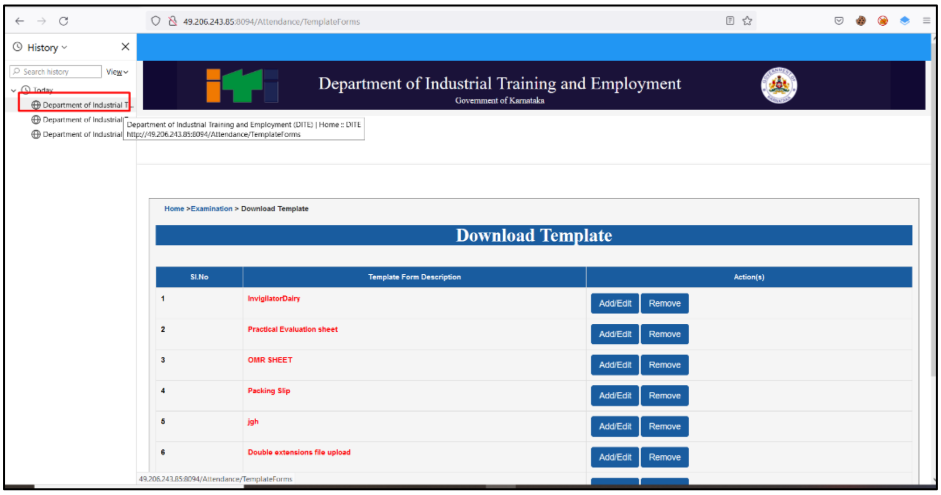
49.206.243.85:8094/Attendance/TemplateForms
Welcome CaseWorker,(CaseWorker)
Logout
Department of Industrial Training and Employment
Government of Karnataka
Home Modules Notifications Examination Admin
Home >Examination > Download Template
Download Template
<table>
<tr><th>Sl.No</th><th>Template Form Description</th><th>Action(s)</th></tr>
<tr><td>1</td><td>InvigilatorDairy</td><td>Add/Edit Remove</td></tr>
<tr><td>2</td><td>Practical Evaluation sheet</td><td>Add/Edit Remove</td></tr>
<tr><td>3</td><td>OMR SHEET</td><td>Add/Edit Remove</td></tr>
<tr><td>4</td><td>Packing Slip</td><td>Add/Edit Remove</td></tr>
<tr><td>5</td><td>jgh</td><td>Add/Edit Remove</td></tr>
<tr><td>6</td><td>Double extensions file upload</td><td>Add/Edit Remove</td></tr>
</table>
Step 3: Now open the browser and enable the Work offline mode as shown below:</td></tr>
</table>



Time Table Notifications

Karnataka ITI Result 2021	Apply Grievance Marks For Result 2021
Karnataka ITI Result 2021 New	Apply Grievance Marks For Result 2021 New

Step 4: From the browser's history, access the authenticated page one by one. It is clearly seen that the authenticated page is visible as shown below:


49.206.243.85:8094/Attendance/TemplateForms
History
Search history
View
Today
Department of Industrial T...
Department of Industrial
Department of Industrial
Department of Industrial Training and Employment
Government of Karnataka

Department of Industrial Training and Employment (DITE) | Home :: DITE
http://49.206.243.85:8094/Attendance/TemplateForms

Home >Examination > Download Template

Download Template

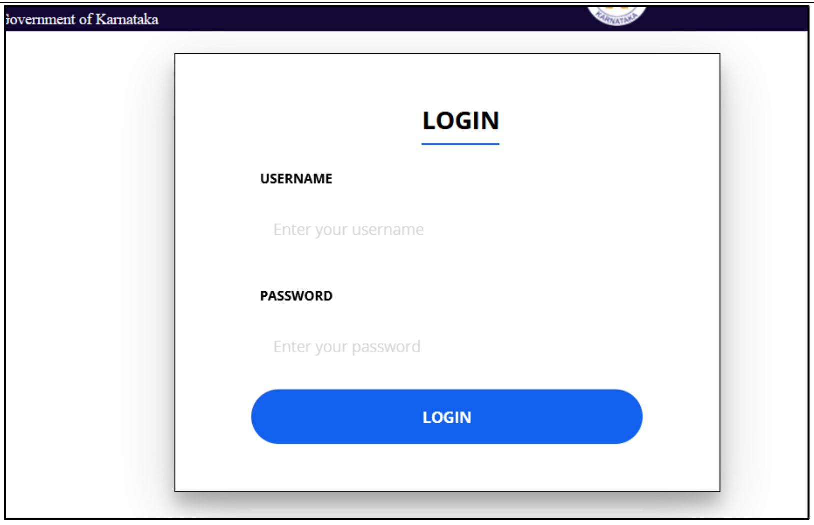
Sl.No	Template Form Description	Action(s)
1	InvigilatorDairy	Add/Edit Remove
2	Practical Evaluation sheet	Add/Edit Remove
3	OMR SHEET	Add/Edit Remove
4	Packing Slip	Add/Edit Remove
5	jgh	Add/Edit Remove
6	Double extensions file upload	Add/Edit Remove

49.206.243.85:8094/Attendance/TemplateForms

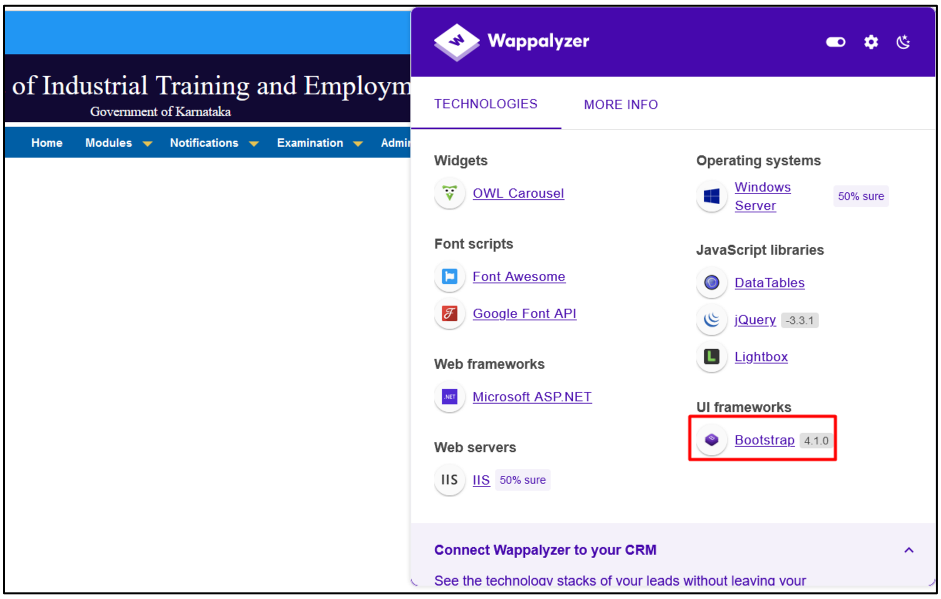
Affected URLs	**throughout the application**

6. Password Recovery Option Missing

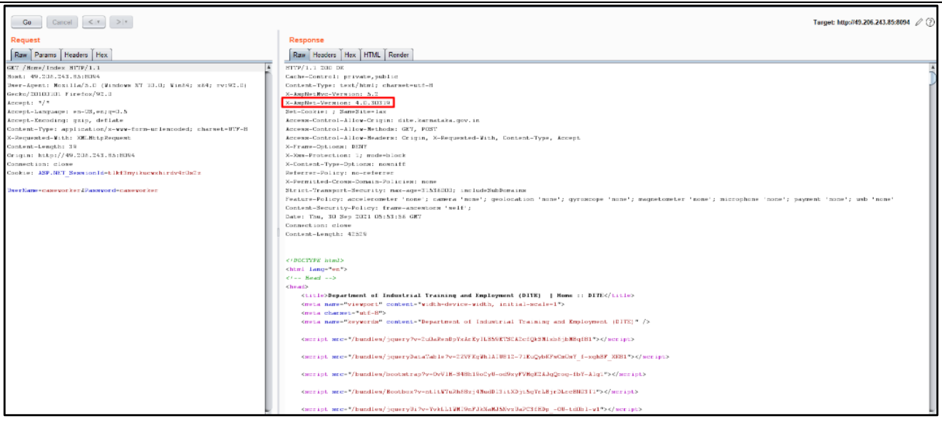
Vulnerability Title: Password Recovery Option is not working	
Risk	**Medium**
Abstract	It was observed that Password Recovery Option is not working in the application
Ease of Exploitation	Medium
Impact	User cannot change the password if the password is compromised.
Recommendations	Users may be required to retrieve their password. Users should be provided with a “forgot password” option through which user will retrieve their password whenever required. It is recommended that Forgot password should be enabled with the users email address. There are following conditions should be met in the forget password function: 1. Reset link should be sent to the user registered email address instead of password directly. 2. Reset Password link should get expired in 24 hours. 3. Reset Password link should not be reused again, once the link is used for reset password. 4. In the Reset Password page, Mandatory fields i.e. New password, Confirm Password and CAPTCHA field must present and should be validated at the client end. Server end validations are also mandatory. However, if the password retrieval is internal in the application then it is recommended to implement a hyperlink on login page resulting to a static page containing a message. “Please contact your site administrator at mail_id[at]domain[dot]com”. Please note that the email address in the message should not be a hyperlink.
Snapshot	

	 iovernment of Karnataka LOGIN USERNAME Enter your username PASSWORD Enter your password
Affected Site	**Login page**

7. Vulnerable Version of Bootstrap

Vulnerability Title: Vulnerable version of bootstrap is used in the application	
Risk	**Medium**
Abstract	Vulnerable version of bootstrap is used in the application.
Ease of Exploitation	Easy
Impact	Vulnerable version of bootstrap (4.1.0) is used in the application. Affected versions of this package are vulnerable to Cross-site Scripting (XSS) via the tooltip, collapse and scroll spy plugins.
Recommendations	It is recommended that application should use latest/Stable version of bootstrap.
Snapshot	 of Industrial Training and Employm Government of Karnataka Home Modules Notifications Examination Admi Wappalyzer TECHNOLOGIES MORE INFO Widgets: OWL Carousel Font scripts: Font Awesome, Google Font API Web frameworks: Microsoft ASP.NET Web servers: IIS 50% sure Operating systems: Windows Server 50% sure JavaScript libraries: DataTables, jQuery -3.3.1, Lightbox UI frameworks: Bootstrap 4.1.0 Connect Wappalyzer to your CRM See the technology stacks of your leads without leaving your
Affected URLs	**throughout the application**

8. Vulnerable Version of ASP.Net

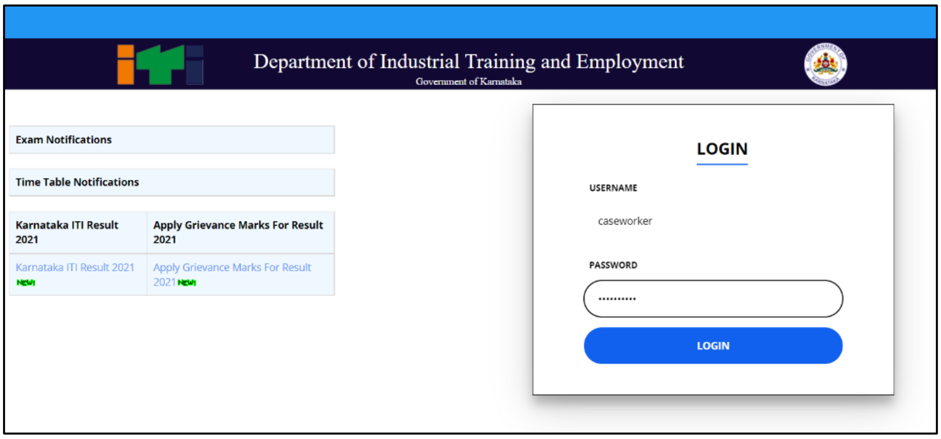
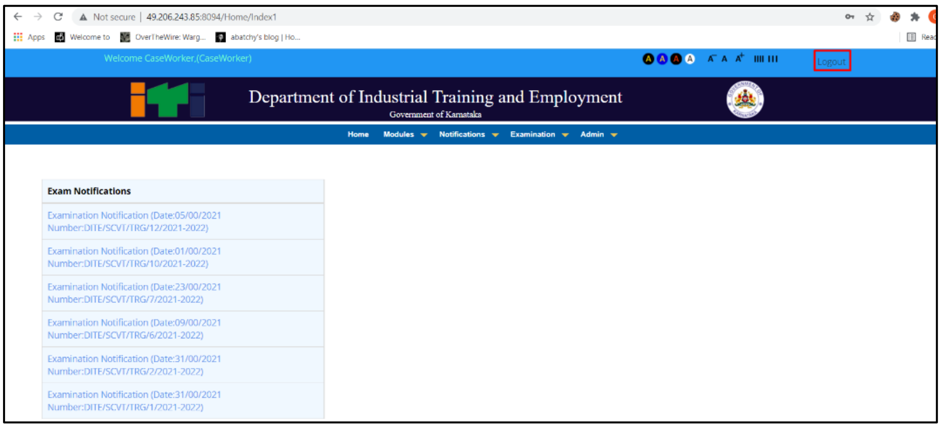
Vulnerability Title: Vulnerable version of ASP.Net is used in the application	
Risk	**Medium**
Abstract	Old Version of Asp.net is used in the application**.**
Ease of Exploitation	Easy
Impact	The strong name (SN) implementation in Microsoft .NET Framework 4.0.30319 relies on Cross-site scripting (XSS) vulnerability in ASP.NET in Microsoft .NET Framework allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka ".NET Elevation of Privilege Vulnerability.".
Recommendations	It is recommended that application should use latest/Stable version of ASP.
Snapshot	
Affected URLs	**Throughout the application**

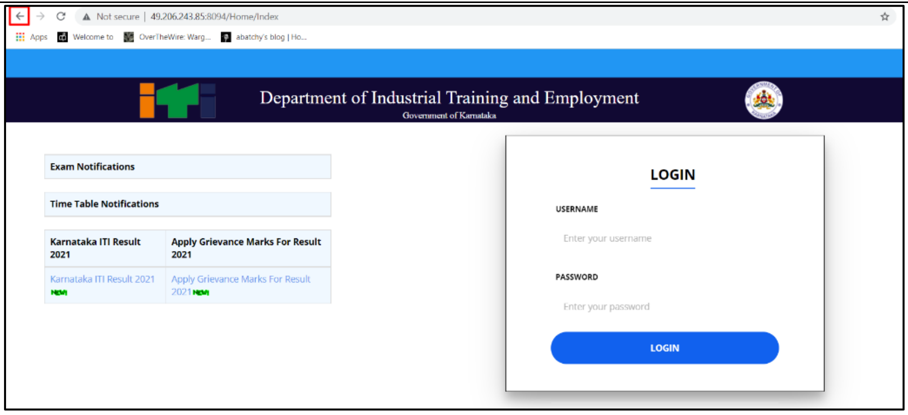
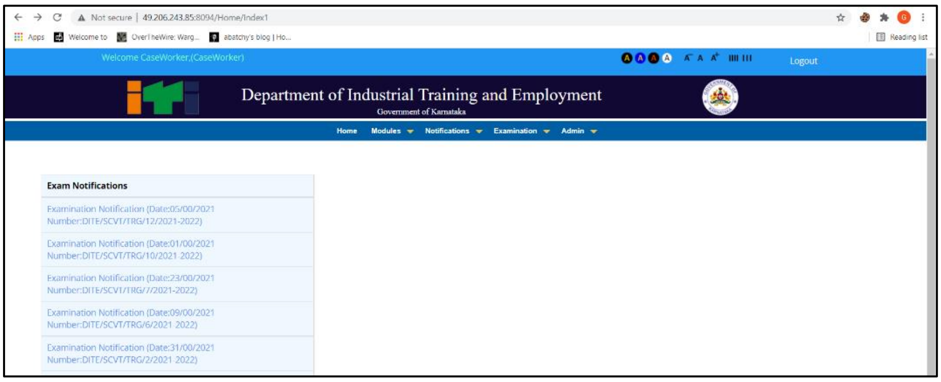
```
GET /Home/Index HTTP/1.1
Host: 49.206.243.85:8094
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 38
Origin: http://49.206.243.85:8094
Connection: close
Cookie: ASP.NET_SessionId=t1kt3myikucwxhirdv4r0s2z

UserName=caseworker&Password=caseworker
```

```
HTTP/1.1 200 OK
Cache-Control: private,public
Content-Type: text/html; charset=utf-8
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Set-Cookie: ; SameSite=lax
Access-Control-Allow-Origin: dite.karnataka.gov.in
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000; includeSubDomains
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
Content-Security-Policy: frame-ancestors 'self';
Date: Thu, 30 Sep 2021 05:53:56 GMT
Connection: close
Content-Length: 42528


<!DOCTYPE html>
<html lang="en">
<!-- Head -->
<head>
    <title>Department of Industrial Training and Employment (DITE)  | Home :: DITE</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8">
    <meta name="keywords" content="Department of Industrial Training and Employment (DITE)" />

    <script src="/bundles/jquery?v=2uDaRen0pYxAcEy1L859KTSCA2cfQk9MlxbSjbM8qfB1"></script>

    <script src="/bundles/jqueryDataTable?v=22VFKqWh1AI0812-71KuQybKFsCmOsY_f-xqhBF_XKB1"></script>

    <script src="/bundles/bootstrap?v=OvV1H-S48b19oCyU-od9xyFVHgK2AJqQroq-fbY-Alq1"></script>

    <script src="/bundles/Bootbox?v=ntltWTuRh68zj4NudD13itXDjt5qYrL8jrDLccBN03I1"></script>

    <script src="/bundles/jqueryUi?v=YvkLL1WMI9nFJkNaMJ5Nvz0aPC3fEDp_-OU-td0b1-w1"></script>
```

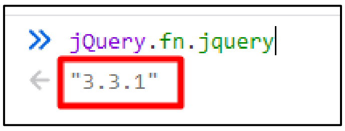
Low

9. Back Button Enabled

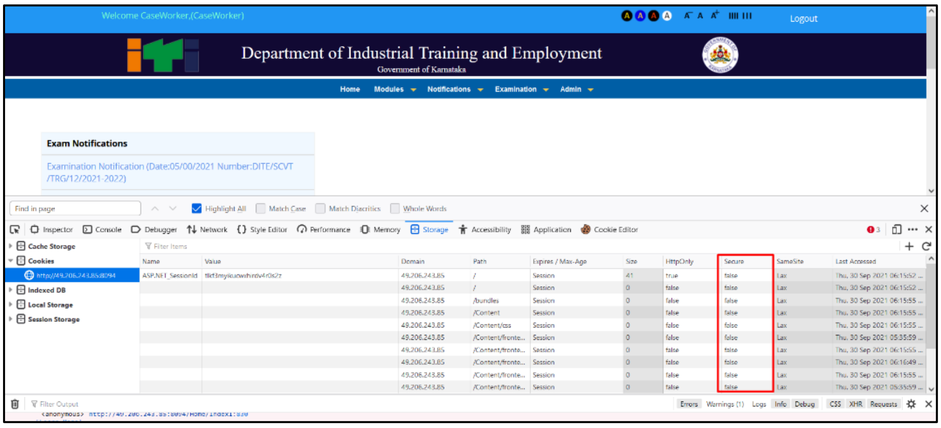
1) **Vulnerability Title: Back Button Enabled**	
Risk	**Low**
Abstract	It was observed that back button is enabled
CVE	-----
Ease of Exploitation	Easy
Impact	The back button on the browser display pages that the user visited recently.
Recommendations	It is recommended to disable back button on website.
Snapshot	Step 1 : Login in the web application  Department of Industrial Training and Employment Government of Karnataka Exam Notifications Time Table Notifications Karnataka ITI Result 2021 — Apply Grievance Marks For Result 2021 Karnataka ITI Result 2021 New — Apply Grievance Marks For Result 2021 New LOGIN USERNAME: caseworker PASSWORD: •••••••••• LOGIN Step 2 : Enter in the Web application  Not secure | 49.206.243.85:8094/Home/Index1 Welcome CaseWorker,(CaseWorker) Logout Department of Industrial Training and Employment Government of Karnataka Home Modules Notifications Examination Admin Exam Notifications Examination Notification (Date:05/00/2021 Number:DITE/SCVT/TRG/12/2021-2022) Examination Notification (Date:01/00/2021 Number:DITE/SCVT/TRG/10/2021-2022) Examination Notification (Date:23/00/2021 Number:DITE/SCVT/TRG/7/2021-2022) Examination Notification (Date:09/00/2021 Number:DITE/SCVT/TRG/6/2021-2022) Examination Notification (Date:31/00/2021 Number:DITE/SCVT/TRG/2/2021-2022) Examination Notification (Date:31/00/2021 Number:DITE/SCVT/TRG/1/2021-2022) Step 3 : logout the web application

	 Not secure | 49.206.243.85:8094/Home/Index Apps Welcome to OverTheWire: Warg... abatchy's blog | Ho... Department of Industrial Training and Employment Government of Karnataka Exam Notifications Time Table Notifications Karnataka ITI Result 2021 — Apply Grievance Marks For Result 2021 Karnataka ITI Result 2021 NEW! — Apply Grievance Marks For Result 2021 NEW! LOGIN USERNAME Enter your username PASSWORD Enter your password LOGIN Step 4 : After click the back button we enter in the website  Not secure | 49.206.243.85:8094/Home/Index1 Apps Welcome to OverTheWire: Warg... abatchy's blog | Ho... Reading list Welcome CaseWorker,(CaseWorker) Logout Department of Industrial Training and Employment Government of Karnataka Home Modules Notifications Examination Admin Exam Notifications Examination Notification (Date:05/00/2021 Number:DITE/SCVT/TRG/12/2021-2022) Examination Notification (Date:01/00/2021 Number:DITE/SCVT/TRG/10/2021-2022) Examination Notification (Date:23/00/2021 Number:DITE/SCVT/TRG/7/2021-2022) Examination Notification (Date:09/00/2021 Number:DITE/SCVT/TRG/6/2021-2022) Examination Notification (Date:31/00/2021 Number:DITE/SCVT/TRG/2/2021-2022)
Affected Site	**Throughout the application**

10. Vulnerable Version of jQuery

Vulnerability Title: Vulnerable version of jQuery is used in the application	
Risk	**Low**
Abstract	It was observed that this page is using an older version of jQuery that is vulnerable to a Cross Site Scripting vulnerability
Ease of Exploitation	Medium
Impact	An attacker can steal the cookies as well as the user session id
Recommendations	It is recommended to update to latest version of jQuery.
Snapshot	 ``>> jQuery.fn.jquery`` ``← "3.3.1"``
Affected URLs	**throughout the application**

11. Session Cookie without Secure Flag

Vulnerability Title: Session Cookie without Secure Flag	
Risk	**Low**
Abstract	It was observed that Session Cookie did not have Secure Flag Set.
Ease of Exploitation	Easy
Impact	This session 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 channels. This is an important security protection for session cookies.
Recommendations	It is recommended to set the Secure flag for this cookie.
Snapshot	
Affected Site	**Throughout the application**

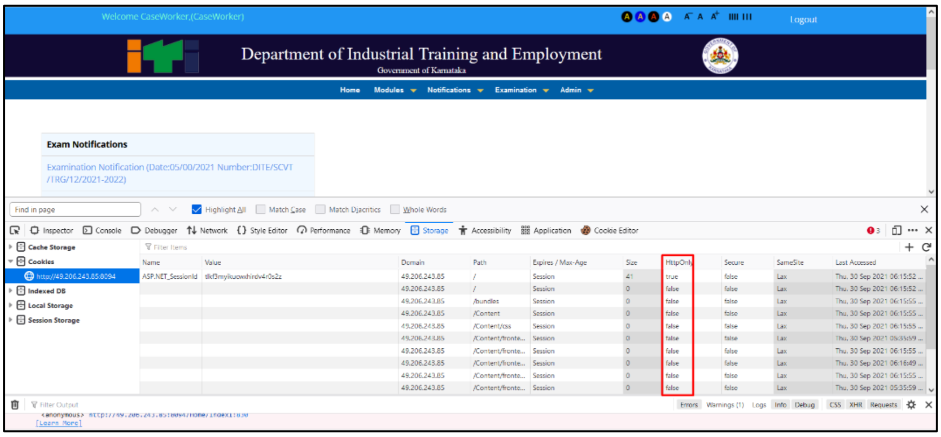
Exam Notifications

Examination Notification (Date:05/00/2021 Number:DITE/SCVT /TRG/12/2021-2022)

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ASP.NET_SessionId	tlkf3myikuowhirdv4r0s2z	49.206.243.85	/	Session	41	true	false	Lax	Thu, 30 Sep 2021 06:15:52 ...
		49.206.243.85	/	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:52 ...
		49.206.243.85	/bundles	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/css	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 05:35:59 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:16:49 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 05:35:59 ...

```
<anonymous> http://49.206.243.85:8094/Home/Index1:830
```

12. Session Cookie Without HTTP Only Flag

Vulnerability Title: Session Cookie without HTTP Only Flag	
Risk	**Low**
Abstract	It was observed that Session Cookie did not have HTTP Only Flag Set.
Ease of Exploitation	Easy
Impact	This session cookie does not have the HTTP Only flag set. When a cookie is set with the HTTP Only flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	It is recommended to set the HTTP Only flag for this cookie.
Snapshot	
Affected Site	**Throughout the application**

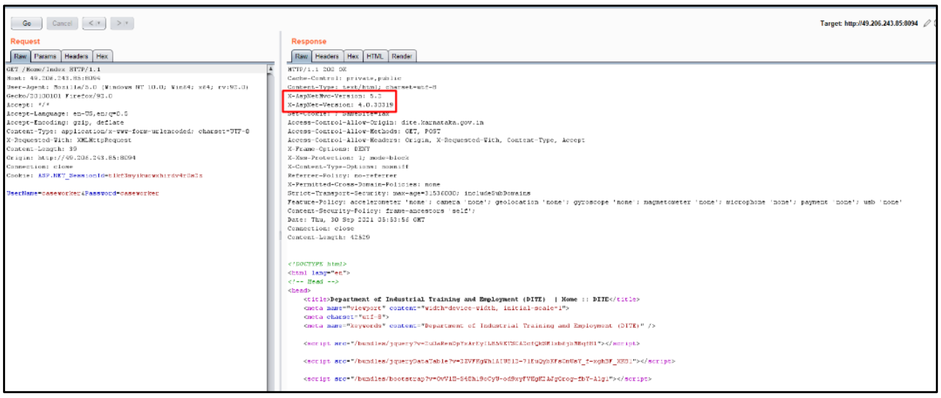
Exam Notifications

Examination Notification (Date:05/00/2021 Number:DITE/SCVT /TRG/12/2021-2022)

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ASP.NET_SessionId	tlkf3myikuowxhirdv4r0s2z	49.206.243.85	/	Session	41	true	false	Lax	Thu, 30 Sep 2021 06:15:52 ...
		49.206.243.85	/	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:52 ...
		49.206.243.85	/bundles	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/css	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 05:35:59 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:16:49 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 06:15:55 ...
		49.206.243.85	/Content/fronte...	Session	0	false	false	Lax	Thu, 30 Sep 2021 05:35:59 ...

```
<anonymous> http://49.206.243.85:8094/Home/Index1:830
[Learn More]
```

13. Webserver Informational Disclosure

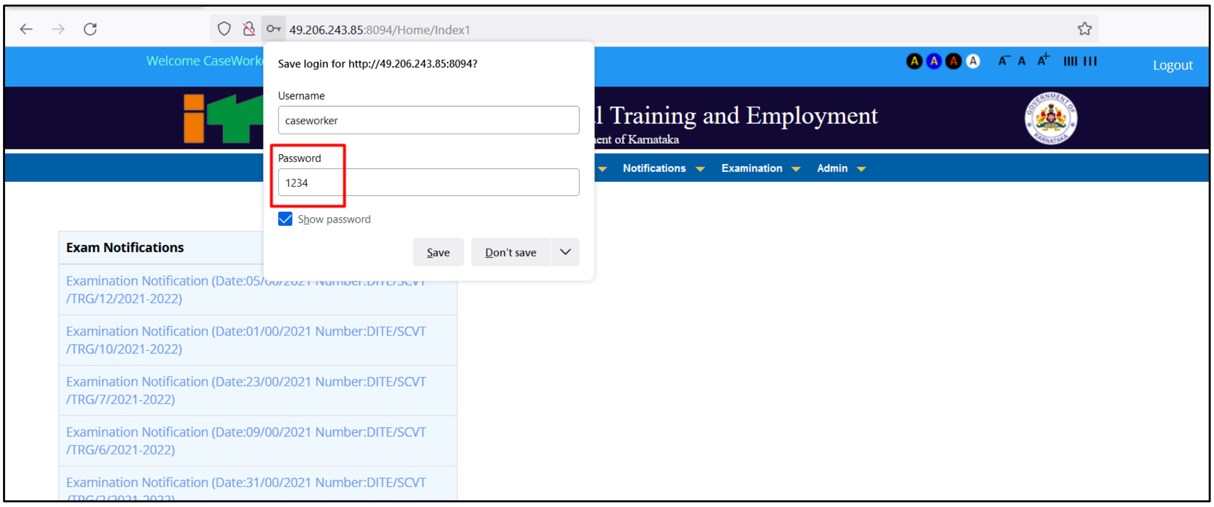
Vulnerability Title: Web Server Information Disclosure	
Risk	**Informational**
Abstract	Banner grabbing (application is displaying Server version and ASP.NET version which may help attacker to learn more about his target) is possible in the application.
Ease of Exploitation	Easy
Impact	Application is displaying Server version and ASP.NET version which may help attacker to learn more about his target.
Recommendations	Server and ASP.NET version should not be displayed to the end user.
Snapshot	
Affected URLs	**Throughout the application**

```
GET /Home/Index HTTP/1.1
Host: 49.206.243.85:8094
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 39
Origin: http://49.206.243.85:8094
Connection: close
Cookie: ASP.NET_SessionId=tlkf3myikucwxhirdv4r0s2z

UserName=caseworker&Password=caseworker
```

```
HTTP/1.1 200 OK
Cache-Control: private,public
Content-Type: text/html; charset=utf-8
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Set-Cookie: ; SameSite=lax
Access-Control-Allow-Origin: dite.karnataka.gov.in
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000; includeSubDomains
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
Content-Security-Policy: frame-ancestors 'self';
Date: Thu, 30 Sep 2021 05:53:56 GMT
Connection: close
Content-Length: 42529


<!DOCTYPE html>
<html lang="en">
<!-- Head -->
<head>
    <title>Department of Industrial Training and Employment (DITE)  | Home :: DITE</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8">
    <meta name="keywords" content="Department of Industrial Training and Employment (DITE)" />

    <script src="/bundles/jquery?v=2u0aRenDpYxArEyILB58KTSCASzfQkSMlxb8jbMNqfM1"></script>

    <script src="/bundles/jqueryDataTable?v=3ZVFKgWh1AIU013-71EuQybKFsOnUsY_f-xghBF_XK01"></script>

    <script src="/bundles/bootstrap?v=OvV1H-S48h19oCyU-od9xyFVEgK2AJgOrog-fbY-Alg1"></script>
```

INFORMATIONAL

1.Security Misconfiguration



49.206.243.85:8094/Home/Index1

Welcome CaseWork

Logout

l Training and Employment

ent of Karnataka

Save login for http://49.206.243.85:8094?

Username

caseworker

Password

1234

☑ Show password

Exam Notifications

Examination Notification (Date:05/00/2021 Number:DITE/SCVT /TRG/12/2021-2022)

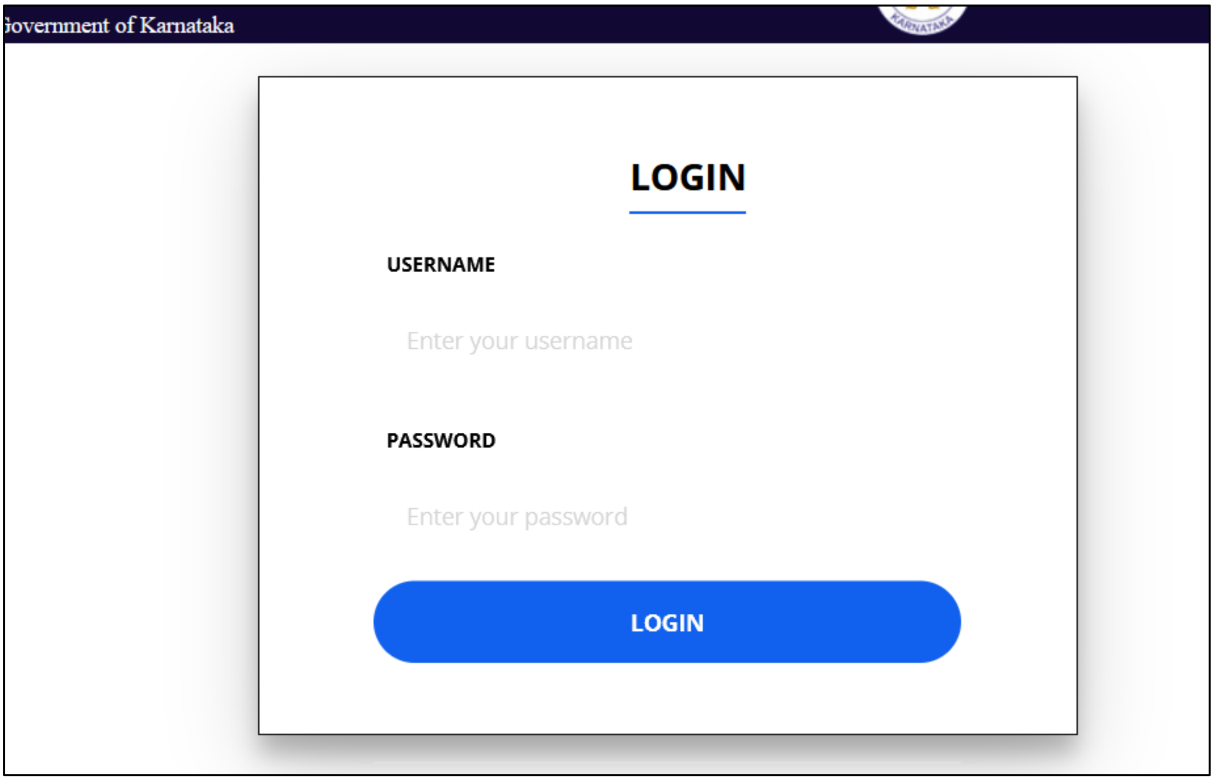
Examination Notification (Date:01/00/2021 Number:DITE/SCVT /TRG/10/2021-2022)

Examination Notification (Date:23/00/2021 Number:DITE/SCVT /TRG/7/2021-2022)

Examination Notification (Date:09/00/2021 Number:DITE/SCVT /TRG/6/2021-2022)

Examination Notification (Date:31/00/2021 Number:DITE/SCVT /TRG/2/2021-2022)

2. Captcha Not Implemented



Government of Karnataka

LOGIN

USERNAME

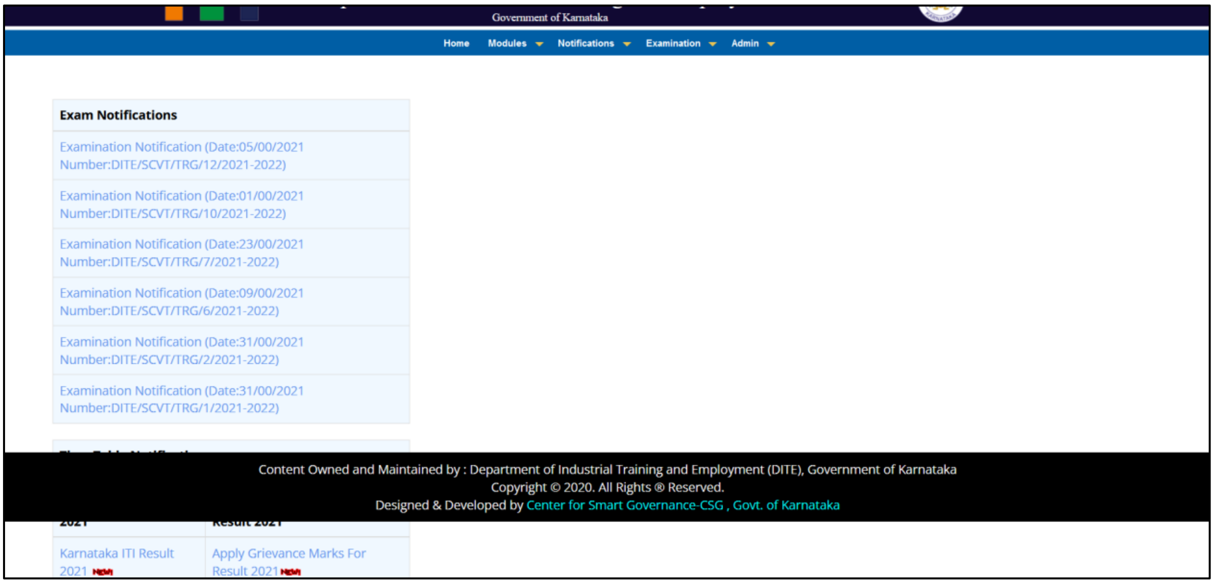
Enter your username

PASSWORD

Enter your password

LOGIN

3. UI Unstable



Government of Karnataka

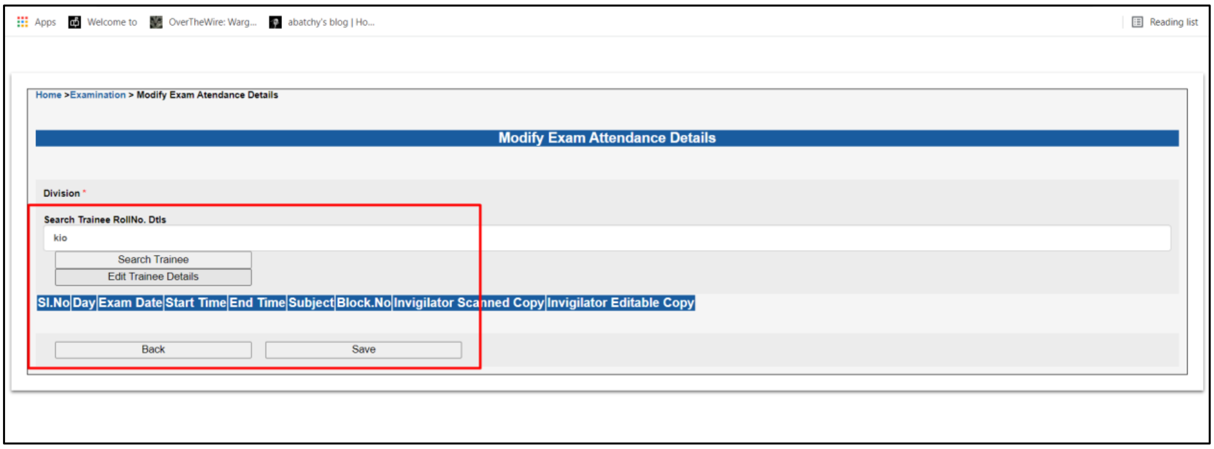
Exam Notifications

- Examination Notification (Date:05/00/2021 Number:DITE/SCVT/TRG/12/2021-2022)
- Examination Notification (Date:01/00/2021 Number:DITE/SCVT/TRG/10/2021-2022)
- Examination Notification (Date:23/00/2021 Number:DITE/SCVT/TRG/7/2021-2022)
- Examination Notification (Date:09/00/2021 Number:DITE/SCVT/TRG/6/2021-2022)
- Examination Notification (Date:31/00/2021 Number:DITE/SCVT/TRG/2/2021-2022)
- Examination Notification (Date:31/00/2021 Number:DITE/SCVT/TRG/1/2021-2022)

Content Owned and Maintained by : Department of Industrial Training and Employment (DITE), Government of Karnataka
Copyright © 2020. All Rights ® Reserved.
Designed & Developed by Center for Smart Governance-CSG , Govt. of Karnataka

2021	Result 2021
Karnataka ITI Result 2021 NEW	Apply Grievance Marks For Result 2021 NEW

4. Functionality Issue



Home >Examination > Modify Exam Atendance Details

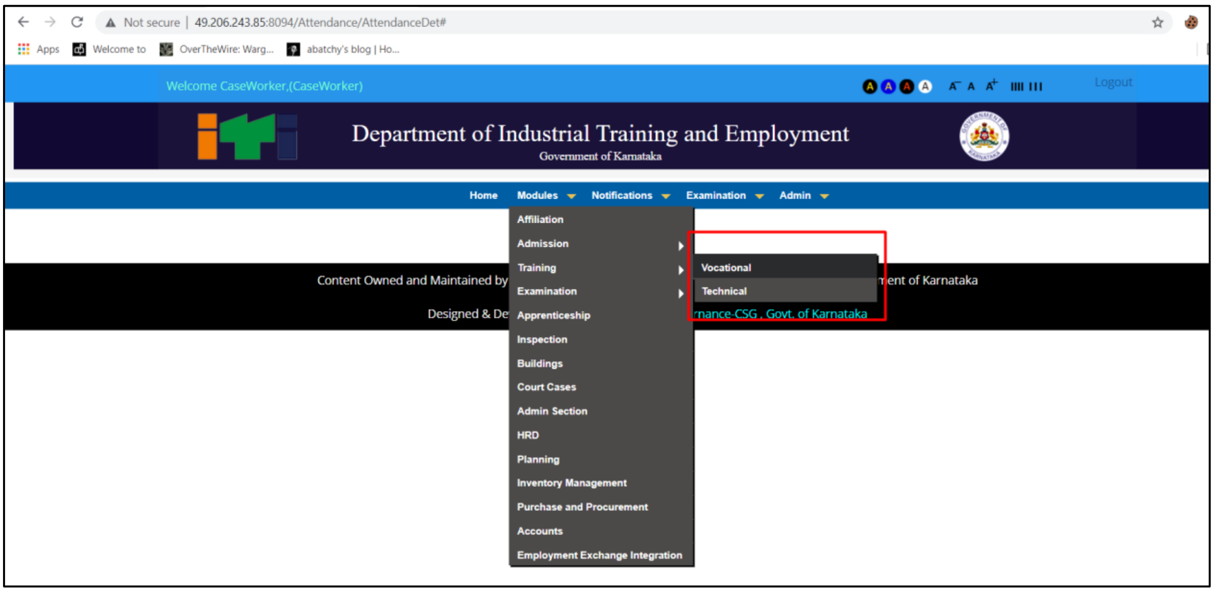
Modify Exam Attendance Details

Division *

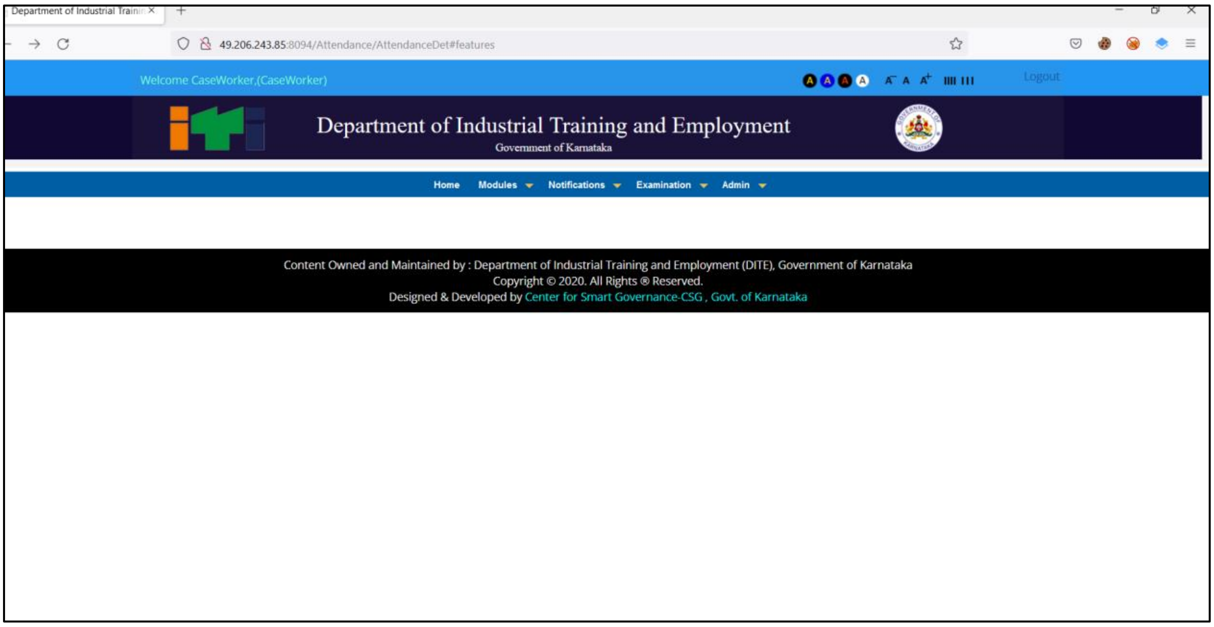
Search Trainee RollNo. Dtls

kio

Sl.No	Day	Exam Date	Start Time	End Time	Subject	Block.No	Invigilator Scanned Copy	Invigilator Editable Copy



5. Change Password Not Implemented



Department of Industrial Trainin
49.206.243.85:8094/Attendance/AttendanceDet#features
Welcome CaseWorker,(CaseWorker)
A A A A
A⁻ A A⁺
Logout
Home
Modules
Notifications
Examination
Admin

Department of Industrial Training and Employment
Government of Karnataka

Content Owned and Maintained by : Department of Industrial Training and Employment (DITE), Government of Karnataka
Copyright © 2020. All Rights ® Reserved.
Designed & Developed by Center for Smart Governance-CSG , Govt. of Karnataka