

~~SECRET~~

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No 1-5/2003 (NTISB-II)

Islamabad 3 March, 2021

Subject: Advisory - Prevention Against Exploitation of Website (Sindh Revenue Board) (Advisor No.8)

M(Admin IHR) ✓ Critical vulnerabilities have been identified in website of Sindh Revenue Board (<https://www.srb.gov.pk>) that may result in **database access and manipulation, exfiltration of sensitive data, remote take-over of users' sessions and website defacement**. Identified vulnerabilities (screenshots attached at Appex-I to Appex-XIII) are

A. S (Rev. Div.) as under:-

- a. SQL injection in database
- b. Citizen's Data Leakage
- c. Cross Site Scripting
- d. Unencrypted / plain text transfer of users' credentials
- e. Cross Site Request Forgery
- f. Microsoft IIS Tilde Directory Enumeration
- g. Internal IP Addresses and server-side paths disclosure
- h. Session cookies lacking secure flags
- i. Server / ASP Net version disclosure
- j. Stack traces and Error Messages on web pages
- k. Server-side technology stack documentation pages on public website

2. Impact of above-mentioned vulnerabilities and guidelines for prevention are attached at Appex -XIV for compliance.

3. For any query or reporting malware, please forward the same on following email addresses:-

asntisb2@cabinet.gov.pk

4. Forwarded for perusal and dissemination of information to all concerned and under command, please.

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

~~SECRET~~

327/4 R
FAX 0311-3800000
Revised 08 MAR 2021

Printed on Feb 11, 2024
The semaphore timeout period has been modified. An undefined procedure occurred during the execution of the program.

SQL INJECTION

Appex - I

2021-07-20 11:11:45.28 [Information] The semaphore timeout period has expired.
Description: An unhandled exception occurred during the execution of the current method. Please handle the start event for more information about this error, and its stack trace, if available.
Exception: System.ComponentModel.Win32Exception: The semaphore timeout period has expired
Source Error:
At [System.Threading.WaitHandle.WaitOne\(TimeSpan timeout\)](#)
at [System.Threading.WaitHandle.WaitOne\(\)](#)
at [System.Data.SqlClient.SqlInternalConnectionTds..ctor\(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, SqlCredential credential, Object providerInfo, String newPassword, Boolean integratedSecurity, SqlConnection connectionUser, SqlConnectionStringBuilder builder\)](#)
at [System.Data.SqlClient.SqlConnectionFactory.CreateConnection\(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object providerInfo, DbConnectionPool pool, DbConnection owningConnection, DbConnectionOptions userOptions\)](#)
at [System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection\(DbConnectionPool pool, DbConnectionOptions options, DbConnectionInternal oldConnection\)](#)
at [System.Data.ProviderBase.DbConnectionPool.CreateObject\(DbConnectionInternal connection, DbConnectionOptions options, DbConnectionInternal oldConnection\)](#)
at [System.Data.ProviderBase.DbConnectionPool.TryGetConnection\(DbConnectionInternal connection, DbConnectionOptions options, Int32 waitForTimeout, Boolean allowCreate, Boolean allowSync, DbConnectionInternal& connection, DbConnectionOptions& options\)](#)
at [System.Data.ProviderBase.DbConnectionFactory.TryGetConnection\(DbConnectionInternal connection, DbConnectionOptions options, Int32 waitForTimeout, Boolean allowCreate, Boolean allowSync, DbConnectionInternal& connection\)](#)
at [System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal\(DbConnection outerConnection, DbConnectionFactory connectionFactory, Boolean allowCreate, Boolean allowSync, DbConnectionOptions userOptions, DbConnectionInternal connection, DbConnectionOptions options\)](#)
at [System.Data.SqlClient.SqlConnection.TryOpen\(SqlConnectionString connection, SqlConnectionInternal connection, Boolean& willClose, Boolean checkConnection, Boolean& userOptions, Boolean& userWillClose\)](#)
at [System.Data.SqlClient.SqlConnection.Open\(\)](#)
at [System.Web.SessionState.SessionStateModule.OnPostAcquireRequestState\(Object source, EventArgs e\)](#) [Time=10ms]
[Information] The semaphore timeout period has expired.
System.Web.SessionState.SessionStateModule.OnPostAcquireRequestState(SqlSessionContainer conn, Exception e) >+26
System.Web.SessionState.SessionStateModule.OnPostAcquireRequestState(SqlSessionContainer conn, TimeSpan retryInterval) >+35
System.Web.SessionState.SessionStateModule.OnPostAcquireRequestState(SqlSessionContainer conn, TimeSpan retryInterval, String id, SessionStateItemData item, Object lockId, Boolean result) >+204
System.Web.SessionState.SessionStateModule.OnPreReleaseState(Object source, EventArgs e) >+20
System.Web.SessionState.SessionStateModule.OnEndRequest(Object source, EventArgs e) >+16
System.Web.SyncEventExecutionStep.System.Web.HttpApplication.EndRequestEventArgs+<EndRequest>g_1 >+19
System.Web.HttpApplication.OnEndRequest(IExecutionStep step) >+195
System.Web.HttpApplication.OnRequestEnd(IExecutionStep step, Boolean completedSynchronously) >+88

Server Error in '/' Application.

The semaphore timeout period has expired

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

Exception Details: System.ComponentModel.Win32Exception: The semaphore timeout period has expired

Source Error:

No source code is available for the current location

Stack Trace:

[Win32Exception (0x8000131904): The semaphore timeout period has expired]

[SqlException (0x80131904): A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that System.Data.SqlClient.SqlConnection.OnError(System.Data.SqlClient.SqlException) has been overridden.

[System.Data.SqlClient.SqlConnection.OnError(SqlException error, Boolean breakConnection, Object sender, String methodName)]
System.Data.ProviderBase.DbConnectionInternal.CreateWrapperConnection(DbConnection owningObject, DbConnectionPool pool, DbConnectionOptions options, DbConnectionPoolKey poolKey, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, Boolean isUserCancelled) +108
System.Data.ProviderBase.DbConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPool pool, DbConnectionPoolKey poolKey, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, Boolean isUserCancelled) +108
System.Data.ProviderBase.DbConnectionInternal.TryGetConnection(DbConnection outerConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, DbConnectionPool pool, DbConnectionPoolKey poolKey, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, Boolean isUserCancelled) +108
System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection outerConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, DbConnectionPool pool, DbConnectionPoolKey poolKey, DbConnectionOptions userOptions, Boolean isUserCancelled) +108
System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`1 retry) +282
System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry) +413
System.Data.SqlClient.SqlConnection.Open() +128
System.Web.SessionState.HttpSessionState.Connection_StartupPartitionInfo("WebApp", retryInterval) +138

[HttpSessionStateBase.OnSessionStart: unable to connect to SQL Server session database.]
System.Web.SessionState.SessionStateStore.OnEndConnection(DbConnection conn, Exception e) +248
System.Web.SessionState.SessionStateStore.CloseSession(DbPartitionInfo id, PartitionInfo timeout, TimeSpan retryInterval) +355
System.Web.SessionState.SessionStateStore.GetConnection(String id, SqlConnectionStringBuilder) +345
System.Web.SessionState.SessionStateStore.SetAndReleaseSessionDataItem(DbPartitionInfo id, String id, SessionStateStoreData item, Object lockId, Boolean newItem) +264
System.Web.SessionState.SessionStateStore.OnEndRequest(Object source, EventArgs eEventArgs) +89
System.Web.SessionState.SessionStateModule.OnEndRequest(Object source, EventArgs eEventArgs) +176

Printed on Feb 19, 2019 at 9:05:21 AM

CITIZENS' DATA LEAKAGE

**Sindh Revenue Board
Taxpayer Facilitation Portal**

User Guides

- How to e-Register
- How to e-Enroll
- How to e-File Return
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Bank
- ADC / e-Payment
- SWWFSCPWP User Guide

Downloads

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

(021) 111-778-000

Documents Required For Registration

- NTN Certificate
- CNIC
- Electricity Bill (Not Older than 1 month)
- Gas Bill (Not Older than 1 month)
- Bank Account Certificate (Not Older than 3 months) showing date of opening of the account or date showing the phone No., Fax No. & Email ID of the Bank branch
- Rent Agreement Ownership Property
- Land Head of the Business
- KFCP Acceptance Certificate with List of Director (WIA Form 25-A) along with List of Limited Companies
- Partnership Deed (or ACP)
- Customs License (for Customs Agents, Shipping Agents, Ship Changers & Public Bonded Warehouses)
- Tax Auditor License Permit (for Tax Auditors)
- KMC Department License Permit (for Security Agencies)
- Other License Permit Registration (as mentioned applicable to the business)

Send scanned copies of above listed documents in PDF format and E-mail at registration@srbsindh.gov.pk

SDTE Registration ID will be generated if the documents are complete.

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN	1234569	-	7
Taxpayer	Type INDIVIDUAL AOP COMPANY		
CNIC	42401-9156807-3		
Name	MCHAMMAD SAEED KHAN		
Reference	No.		

674802

Image Character

**Sindh Revenue Board
Taxpayer Facilitation Portal**

User Guides

- How to e-Register
- How to e-Enroll
- How to e-File Return
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Bank
- ADC / e-Payment
- SWWFSCPWP User Guide

Downloads

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

(021) 111-778-000

Documents Required For Registration

- NTN Certificate
- CNIC
- Electricity Bill (Not Older than 1 month)
- Gas Bill (Not Older than 1 month)
- Bank Account Certificate (Not Older than 3 months) showing date of opening of the account or date showing the phone No., Fax No. & Email ID of the Bank branch
- Rent Agreement Ownership Property
- Land Head of the Business
- KFCP Acceptance Certificate with List of Director (WIA Form 25-A) along with List of Limited Companies
- Partnership Deed (or ACP)
- Customs License (for Customs Agents, Shipping Agents, Ship Changers & Public Bonded Warehouses)
- Tax Auditor License Permit (for Tax Auditors)
- KMC Department License Permit (for Security Agencies)
- Other License Permit Registration (as mentioned applicable to the business)

Send scanned copies of above listed documents in PDF format and E-mail at registration@srbsindh.gov.pk

SDTE Registration ID will be generated if the documents are complete.

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN	1234569	-	5
Taxpayer	Type INDIVIDUAL AOP COMPANY		
CNIC	42401-5010687-9		
Name	ZZAT GUJ		
Reference	No.		

051811

Image Character

Sindh Revenue Board
Taxpayer Facilitation Portal

Home e-Registration e-Enrolment Search Taxpayers News FAQs Helpdesk & Support

User Guides

How to e-Register
How to e-Enrol
How to e-File Return
How to e-Pay Taxes
Who Should e-File Taxes
Op-Cit Debit Card
Internet Banking
ADC e-Payment
SWN/FSCPWP User Guide

Downloads

SRB Schedule-II
Sindh Sales Tax on Services
Act 2011
Sindh Sales Tax on Services
Rules 2011
Sales Tax Return Forms
Tax Payment Forms
Notification for Sales Tax on Services
NBP Authorised Branches

(021) 111-778-000

TAXPAYER REGISTRATION APPLICATION

Documents Required for Registration

- NTN/Cnic
- Cnic
- Exemptions (If Not Eligible, Please Select)
- On Behalf Of (If Not Selected)
- Bank Account Holder (For Account holder Abiding the PNC Act, No. A/c held in the Name of)
- New Address (Country, Town, District, State, Zip Code)
- Business Incorporation Certificate with Tax ID or Business Tax ID No. (If Not Available)
- Letter of Authorization (If Not Available)
- Customer License Permit (If Required)
- Business Department License Permit (For Service Providers)
- Other License Permit (From Environment Protection Authority)
- Self-employed Copy of Abatement Certificate (For Self-employed Individuals)
- Self-employed Tax Registration Certificate (For Self-employed Individuals)
- NOTE: Represented by authorized Signatory
Declarations are incorrect.

NTN [] 1234565 [] 2
Taxpayer Type INDIVIDUAL AOP COMPANY
CNIC [] 0101-39980617-7
Name C.RISHAD AHMAD KHAN
Reference []
Q No. []
049660

Image [] Character [] OK [] CLEAR []

TAXPAYER REGISTRATION APPLICATION

Documents Required for Registration

- NTN/Cnic
- Cnic
- Exemptions (If Not Eligible, Please Select)
- On Behalf Of (If Not Selected)
- Bank Account Holder (For Account holder Abiding the PNC Act, No. A/c held in the Name of)
- New Address (Country, Town, District, State, Zip Code)
- Business Incorporation Certificate with Tax ID or Business Tax ID No. (If Not Available)
- Letter of Authorization (If Not Available)
- Customer License Permit (If Required)
- Business Department License Permit (For Service Providers)
- Other License Permit (From Environment Protection Authority)
- Self-employed Copy of Abatement Certificate (For Self-employed Individuals)
- Self-employed Tax Registration Certificate (For Self-employed Individuals)
- NOTE: Represented by authorized Signatory
Declarations are incorrect.

NTN [] 1234563 [] 3
Taxpayer Type INDIVIDUAL AOP COMPANY
CNIC [] 02101-BBO2244-9
Name S.A.M. AHMED
Reference []
289538

Image [] Character [] OK [] CLEAR []

(021) 111-778-000

11, 202²

on Feb 11, 202²

eSRB.GOV.PK

Sindh Revenue Board
Taxpayer Facilitation Portal

Home e-Registration e-Enrolment e-Search Taxpayers News FAQs Helpdesk & Support

User Guides

- How to e-Register
- How to e-Enrol
- How to e-File Return
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Base
- ADC / e-Payment
- SWMFSCPWP User Guide

Downloads:

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

(021) 111-773-000

Documents Required for Registration

- NTN Certificate
- CNIC
- Bernoulli BC Date Order (not issued)
- Gas Bill (Not older than 6 months)
- Bank Account Certificate (Not older than 6 months) showing date of opening of the account and also showing the place No, Axis No, & account No of the Bank branch
- Business Approval Certificate (BAC)
- Letter Head of the Business
- SLCP Registration Certificate (Not older than 6 months) with Form 19 & 21 in case of Licensed Companies
- Partnership Deed (for AOP)
- Carrier License (for Carriers Agents, Shipping Agents, Ship Chas. & Public Goods Transporters)
- Port Authority License (from the Port Board)
- Haven Department License (from the Haven Agents)
- Other License (from the respective concerned authority applicable to the business)

Indicated copies of above said documents to be submitted and kept at a permanent address.

NOTE: Registration will not be permitted if the documents are incomplete.

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN Taxpayer Type INDIVIDUAL AOP COMPANY

CNIC Name RANA MOHAMMAD AHSEN K Reference No.

006430

Image Character OK CLEAR

eSRB.GOV.PK

Sindh Revenue Board
Taxpayer Facilitation Portal

Home e-Registration e-Enrolment e-Search Taxpayers News FAQs Helpdesk & Support

User Guides

- How to e-Register
- How to e-Enrol
- How to e-File Returns
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Base
- ADC / e-Payment
- SWMFSCPWP User Guide

Downloads:

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

(021) 111-778-000

Documents Required for Registration

- NTN Certificate
- CNIC
- Bernoulli BC Date Order (not issued)
- Gas Bill (Not older than 6 months)
- Bank Account Certificate (Not older than 6 months) showing date of opening of the account and also showing the place No, Axis No, & account No of the Bank branch
- Business Approval Certificate (BAC)
- Letter Head of the Business
- SLCP Registration Certificate (Not older than 6 months) with Form 19 & 21 in case of Licensed Companies
- Partnership Deed (for AOP)
- Carrier License (for Carriers Agents, Shipping Agents, Ship Chas. & Public Goods Transporters)
- Port Authority License (from the Port Board)
- Haven Department License (from the Haven Agents)
- Other License (from the respective concerned authority applicable to the business)

Indicated copies of above said documents to be submitted and kept at a permanent address.

NOTE: Registration will not be permitted if the documents are incomplete.

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN Taxpayer Type INDIVIDUAL AOP COMPANY

CNIC Name TANVEER IQBAL Reference No.

547454

Image Character OK CLEAR

PRINTED ON Feb 11, 2022

**Sindh Revenue Board
Taxpayer Facilitation Portal**

[Home](#) [e-Registration](#) [e-Enrolment](#) [Search Taxpayers](#) [News](#) [FAQs](#) [Helpdesk & Support](#)

User Guides

- How to e-Register
- How to e-Enrol
- How to e-File Return
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Base
- ADC / e-Payment
- SWIFSCPWP User Guide

Downloads

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

Documents Required For Registration

- NTN Certificate
- CNIC
- Electric Bill (Not Older than 6 months)
- Gas Bill (Not Older than 6 months)
- Bank Account Certificate (Not Older than 6 months) showing last 6 digits of the account and the details of the branch, IFC No. & name of the bank branch
- Business Registration Registry
- Letter Head of the Business
- SECP Incorporation Certificate with List of Directors (With Name & Date of Last Company Formation Date)
- Business License (For Current Agents, Shipping Agents, Rep, Chamber & Public Benefit Associations)
- Passport Department License (From the Service Agency)
- Other License (From the Service Agency)

Send scanned copies of above said documents in PDF format and Email at taxreg@srb.gov.pk

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN	1234567	-9
Taxpayer	Type	INDIVIDUAL AOP COMPANY
CNIC 51101-1967260-9		
Name MUHAMMAD UMER AZIZ		
Reference No.		
729778		
Image		
Character		
<input type="button" value="OK"/> <input type="button" value="CLEAR"/>		

PRINTED ON Feb 11, 2022

**Sindh Revenue Board
Taxpayer Facilitation Portal**

[Home](#) [e-Registration](#) [e-Enrolment](#) [Search Taxpayers](#) [News](#) [FAQs](#) [Helpdesk & Support](#)

User Guides

- How to e-Register
- How to e-Enrol
- How to e-File Return
- How to Pay Taxes
- Tax Calendar
- Who should e-File
- Direct Debit
- Internet Base
- ADC / e-Payment
- SWIFSCPWP User Guide

Downloads

- SRB Scheduled-II
- Sindh Sales Tax on Services Act, 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Forms
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

Documents Required For Registration

- NTN Certificate
- CNIC
- Electric Bill (Not Older than 6 months)
- Gas Bill (Not Older than 6 months)
- Bank Account Certificate (Not Older than 6 months) showing last 6 digits of the account and the details of the branch, IFC No. & name of the bank branch
- Business Registration Registry
- Letter Head of the Business
- SECP Incorporation Certificate with List of Directors (With Name & Date of Last Company Formation Date)
- Business License (For Current Agents, Shipping Agents, Rep, Chamber & Public Benefit Associations)
- Passport Department License (From the Service Agency)
- Other License (From the Service Agency)

Send scanned copies of above said documents in PDF format and Email at taxreg@srb.gov.pk

TAXPAYER REGISTRATION APPLICATION

SRB Registration, who already have NTN

NTN	1234567	-9
Taxpayer	Type	INDIVIDUAL AOP COMPANY
CNIC 51101-1967260-9		
Name MUHAMMAD UMER AZIZ		
Reference No.		
729778		
Image		
Character		
<input type="button" value="OK"/> <input type="button" value="CLEAR"/>		

← → C ▲ Not secure e.srb.gov.pk



Sindh Revenue Board Taxpayer Facilitation Portal

Home e-Registration e-Billing Search Taxpayers News FAQs Helpdesk & Support

User Guides

- How to e-Register
- How to e-Enrol
- How to e-Filing
- How to Pay Taxes
- Tax Calculation
- Who should e-File
- Return Details
- Interest Rate
- ADC/E-Payment
- SWF/FSCPWP User Guide

Downloads

- SRB Scheduled-II
- Sindh Sales Tax on Services Act 2011
- Sindh Sales Tax on Services Rules, 2011
- Sales Tax Return Form
- Tax Payment Forms
- Notification for Sales Tax on Services
- NBP Authorized Branches

Documents Required For Registration

- NTN Holder
- CNIC
- Business ID (NOC Letter from Head Office)
- Get Bill (Not Older than 3 months)
- Bank Account Certificate (Not older than three months of opening date and not due date) with phone No., fax No. & email ID of the Bank branch
- Bank Account Clearance Register
- Last Month's Business
- NAFIS Income Tax Filing with Last 3 Years (Folio No. 25 & 26) or Income Tax Filing Statement
- Partnership Deed (if AOP)
- Custom License (for Customs Agents, Shipping Lines, Ship Charters & Public Bodies Tax Exemptee)
- Few Authority Letters (Power of Attorney Letter)
- House Department License (from House Authority)
- Other License (from Exports & Imports Authority like ITC etc.)

Individuals required to attach self declaration or PGI (Printed and Signed) of a responsible person.

NOTE: Registration will be processed only after receiving the documents by postmaster.

TAXPAYER REGISTRATION APPLICATION

* SRB Registration, who already have NTN

NTN	1234568	7
Taxpayer	Type INDIVIDUAL AOP COMPANY	
CNIC	A2101-6835080-1	
Name	MUHAMMED NAWAZ ABBAS	
Reference	No.	

099405

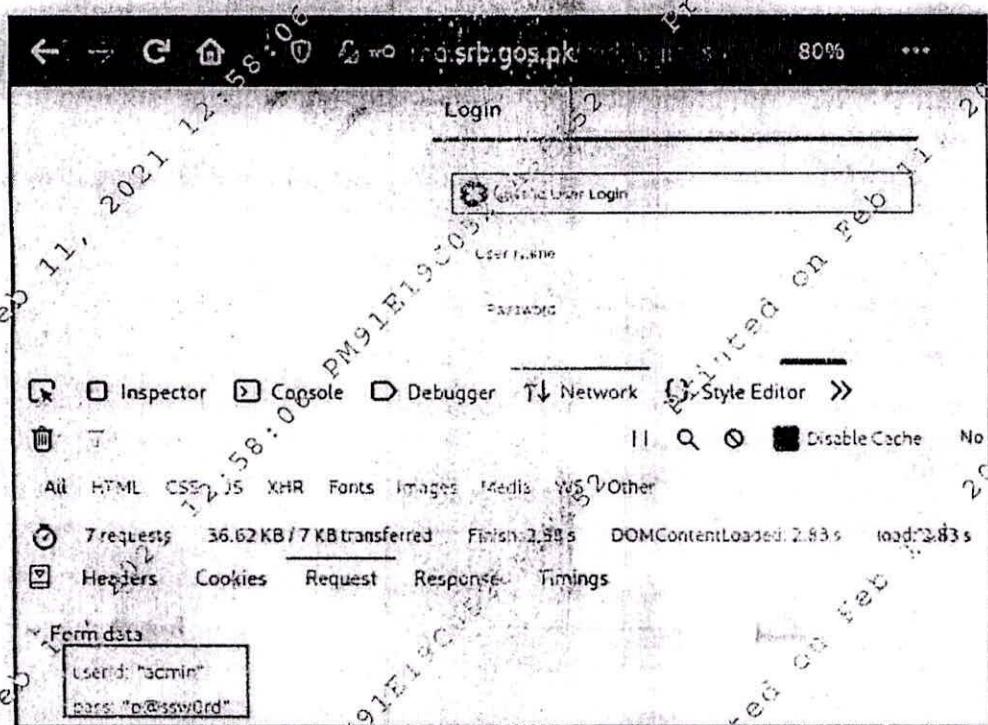
Image _____
Character _____

OK || CLEAR

(021) 111-770-000

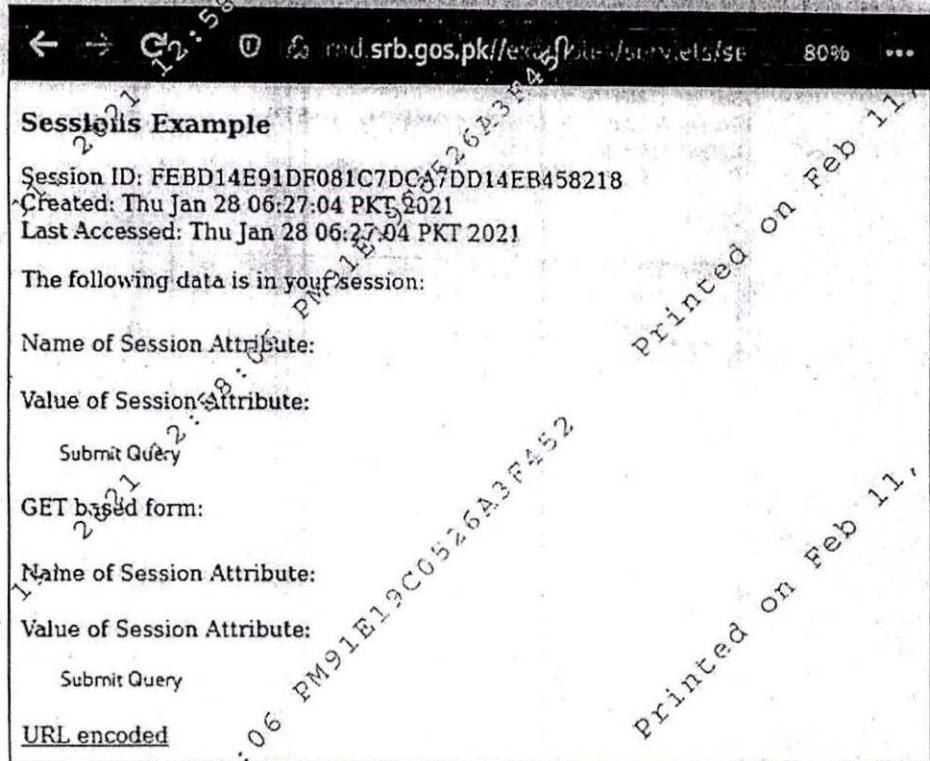
Append - IV

USERNAME / PASSWORD SENT IN PLAINTEXT



Appendix - V

APACHE TOMCAT VULNERABLE EXAMPLE SERVELET



CROSS SITE REQUEST FORGERY –

HTML FORM WITHOUT ANTI-CSRF TOKEN

Printed on Feb 11, 2021 12:58:06 PM91E12C0S26A3452
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2668
Date: Sat, 05 Dec 2020 22:05:47 GMT

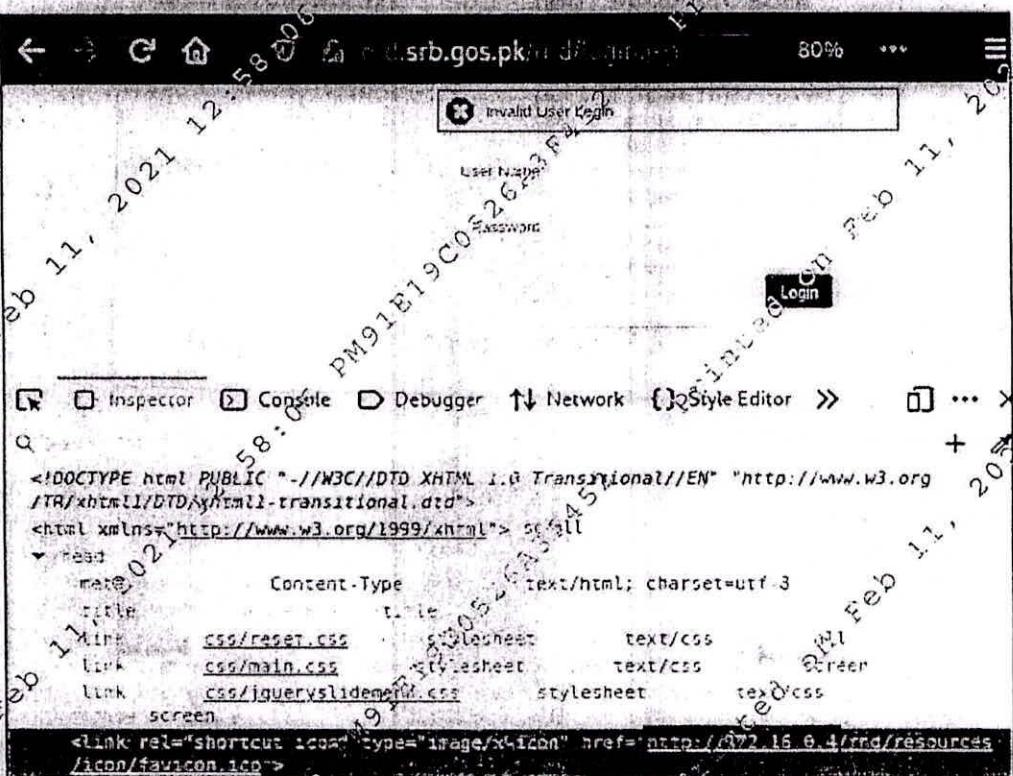
```
<html>
...
<form action="implicit-objects.jsp" method="GET">
    foo = <input type="text" name="foo" value="">
    <input type="submit">
</form>
```

Appex - VII

MICROSOFT IIS TILDE DIRECTORY ENUMERATION

```
OPTIONS /Registration//**/*/*?aspxerrorpath=/ HTTP/1.1
Cookie: ASP.NET_SessionId=cc021e19c0526a3e452
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Accept-Encoding: gzip,deflate
Host: e.srb.gos.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Connection: Keep-alive

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 05 Dec 2020 22:02:54 GMT
Content-Length: 245
```

INTERNAL IP ADDRESS AND SERVER-SIDE PATH DISCLOSURE

Appex -IX

SESSION COOKIE LACKING SECURE FLAG

Printed on Feb 11, 2021 12:58:06 PM 91E19C0526A3F452
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=87868F96678120CF0A326EDDA3A625A7; Path=/; HttpOnly
Location: http://www.srb.gov.pk/home/time.jsp
Content-Type: text/html; charset=ISO-8859-1
Date: Sat, 05 Dec 2020 21:58:50 GMT

Printed on Feb 11, 2024

Appendix X

SERVER PATH/ SERVER-SIDE INSTALLATION DIRECTORIES DISCLOSURE

A screenshot of a web browser displaying a Tomcat configuration file. The URL is `http://www.srb.gos.pk/docs/tomcat`. The page content shows the XML code for a context configuration:

```
<Context path="/mywebapp" docBase="/Users/theuser/mywebapp/src/main/webapp" >
    <Resources className="org.apache.naming.resources.VirtualDirContext"
        extraResourcePaths=
            "/WEB-INF/classes=/Users/theuser/mywebapp/target/classes" />
    <Loader className="org.apache.catalina.loader.VirtualWebappLoader"
        virtualClasspath="/Users/theuser/mywebapp/target/classes;
            /Users/theuser/.m2/repository/log4j/log4j/1.2.15/log4j-1.2.15.jar" />
    <Scanning scannableDirectories="true" />
</Context>
```

Below the code, a note reads:

Here is another example where the webapp serves pictures under /pictures and movies under /movies and also depends on another maven project mylib that would normally produce a jar to be packaged in WEB-INF/lib:

A screenshot of a web browser displaying a list of Tomcat configuration options. The URL is `http://www.srb.gos.pk/docs/virtual`. The page lists:

- 16) MBean Descriptor
- 17) Default Servlet
- 18) Clustering
- 19) Load Balancer

Below the list, notes say:

instilled, perhaps `/usr/local/tomcat`.

Also, this how-to uses Unix-style path separators and commands; if you're on Windows modify accordingly.

A screenshot of a web browser displaying a terminal command. The URL is `http://www.srb.gos.pk/docs/building`. The terminal window shows:

```
cd ${tomcat.source}
ant
```

Below the terminal window, a warning message reads:

WARNING: Running this command will download libraries required to build Tomcat to the `/usr/share/java` directory by default. On a

Append -XI

SERVER ASP.NET VERSION DISCLOSURE

```
GET /1.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: e.srb.gos.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Connection: Keep-alive

HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 05 Dec 2020 12:00:29 GMT
Content-Length: 7098
```

STACK TRACES AND ERROR MESSAGES ON PUBLIC WEBPAGES

Append -XIII

SERVER-SIDE TECH-STACK DOCUMENTATION PAGES

The screenshot shows the Apache Tomcat Manager App Home page. At the top, there's a logo of a cat and the text "Apache Tomcat 7 Version 7.0.56, Sep 26 2014". To the right, it says "The Apache Software Foundation" and provides a link to <http://www.apache.org>. Below this, there's a "Links" section with links to "Docs Home", "FAQ", and "User Comments". A "User Guide" section follows, containing links to "Introduction", "Configuring Manager App", and "Supported Manager Commands". A "Table of Contents" section is also present.

This screenshot shows a page from the Apache Tomcat documentation explaining the "MemoryRealm". It states that this realm is configured in the default SCALINA BASE/conf/server.xml file. It describes how it reads an XML-format file stored at SCALINA BASE/conf/tomcat-users.xml, which can be edited with any text editor. An example XML snippet is shown:

```
<user username="craigmc" password="secret" roles="standard,manager-script" />
```

This screenshot shows a page from the Apache Tomcat documentation about JDBCRealms. It explains that JDBCRealms are configured in the SCALINA BASE/conf/server.xml file. An example configuration for a MySQL database called "authority" is provided, showing how it connects to the database and maps users and roles to database tables:

```
<Realm className="org.apache.catalina.realm.JDBCRealm"
      driverName="org.gjt.mm.mysql.Driver"
      connectionURL="jdbc:mysql://localhost/authority?user=dbuser&password=dbpass"
      userTable="users" userNameCol="username" userCredCol="user_pass"
      userRoleTable="user_roles" roleMapCol="role_name"/>
```

GUIDELINES FOR PREVENTION AGAINST WEBSITE EXPLOITATION

1. Summary of identified vulnerabilities, impact and prevention mechanism are as under:-

Ser	Vulnerability	Detail	Remarks
a.	SQL Injection	Database of website is vulnerable to SQL Injection attack; allowing attacker to view, manipulate and delete any record(s) in database.	Append-I
b.	Citizens' Data Leakage	CNIC's and Name of citizens are easily brute-forced against bogus NTN numbers	Append-II
c.	Cross Site Scripting (XSS)	Attacker can hijack user sessions (including those of admin users) and manipulate content of web pages	Append-III
d.	Username and Password Sent in plaintext	Login / Registration pages are not using secure HTTPS protocol; therefore, user credentials can be intercepted in plaintext in case of man In The Middle (MITM) attack	Append-IV
e.	Cross Site Request Forgery (CSRF)	Attacker can perform unauthorized actions on behalf of victim user, such as change of passwords or access to otherwise restricted data.	Append-V
f.	Microsoft IIS Tilde Directory Enumeration	Files and folder names under web root are disclosed to attack.	Append-VI
g.	Internal IP Address Disclosure	Internal IP address is disclosed in webpage HTML	Append-VII
h.	Session Cookie lacking SECURE flag	Session cookie can be accessed on insecure channels (without SSUTLS)	Append-VIII
i.	Server Path Disclosure	Server paths are disclosed, giving away Valuable information about server, file system and installation directories	Append-IX
j.	Server and ASP.NET version Disclosure	HTML responses contain headers which disclose server version and ASP.NET version, providing valuable information to attacker to plan further attacks	Append-X

SECRET

k.	Stack Traces and Error Messages on Webpages	Stack traces pin point possible entry points, disclose server paths and technology stack of server	Appex-XI
l.	Server / Tech Documentation pages on Production	Unnecessary technical documentation is openly accessible, giving away important information about underlying server	Appex-XII

2. **Prevention against SQL Injection**

- a. **Input Validation.** Data that is received from external parties must be validated, such that only the value which passes the validation can be processed. It helps counteract any commands inserted in the input string.
- b. **Use of Parameterized Queries.** By employing parameterized queries, user input is automatically quoted and the user/attacker supplied input will not cause the change of the intent. This coding style helps mitigate an SQL injection attack.
- c. **Use of Stored Procedures.** Stored procedure can reduce the direct access to fractions of database, making it an essential asset of database security.
- d. **Escaping.** Always use character-escaping functions for user-supplied input provided by each database management system (**DBMS**). This is done to make sure the DBMS never confuses it with the SQL statement provided by the developer. For example, use the `mysql_real_escape_string()` in PHP to avoid characters that could lead to an unintended SQL command.
- e. **Avoiding Administrative Privileges.** Application must not be connected to the database using an account with root access. This should be done only if absolutely necessary since the attackers could gain access to the whole system.

3. **Prevention against Citizens Data Leakage.** Applications API's returning citizens data must be behind accessed control checks such as a strong authentication mechanism.

4. **Prevention Against Cross Site Scripting**

- a. **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.

SECRET

SECRET

- b. **Encode data on output.** At the point where user-controllable data is output in HTTP responses encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
 - c. **Use appropriate Response Headers.** To prevent XSS in HTTP responses that aren't intended to contain any HTML or Java Script, use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
 - d. **Content Security Policy.** Use Content Security Policy (CSP) to reduce the severity of any HTML or JavaScript, use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses.
5. **Prevention against Exploitation of Apache Tomcat Example Servlets.**
Example servlets must not be present / accessible on production server.
6. **Prevention against Unencrypted Transfer of User Credentials.** Transfer of usernames and passwords and other private / sensitive data must be encrypted using encryption protocol such as TLS 1.2 or TLS 1.3.
7. **Prevention Against Cross Site Request Forgery.** The recommended and that most widely used technique for preventing CSRF attacks is known as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well-designed anti-CSRF system involve the following attributes:-
- a. The Anti-CSRF token should be unique for each user session.
 - b. The session should automatically expire after a suitable amount of time.
 - c. The anti-CSRF token should be a cryptographically random value of significant length.
 - d. The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm.
 - e. The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent).
 - f. The server should reject the requested action if the anti-CSRF token fails validation.

SECRET

SECRET

8. **Prevention against Microsoft IIS Tilde Directory Enumeration.** Discard all web requests using the tilde character and add a registry key name NtfsDisable8dotNameCreation to HKLM\SYSTEM\CurrentControlSet\Control\FileSystem. Set the value of the key to 1 to mitigate all 8.3 name conventions on the server.
9. **Prevention against Internal IP Address Disclosure.** Prevent internal IP addresses from being displayed to users in any form.
10. **Prevention against Session Cookies Lacking Secure Tags.** Use Secure and Http Only flags with session cookies for their protection from attacks leading to session hijacking or session fixation.
11. **Prevention against Server-side Paths' Disclosure.** This is important as server-side paths provide information about underlying operation system, its file system, server-side technology and paths to sensitive data directories on server.
12. **Server and ASP.Net version Disclosure.** Disclosure of versions of server and other server-side technology must not be returned in HTTP responses as this information helps attacker during reconnaissance.
13. **Prevention against Stack Traces and Error Messages on Web Pages.** Properly configure the application to log errors to a file instead of displaying errors to the user.
14. **Prevention against Unnecessary Documentation Pages on Public Network.** Web server Must be upgraded to MS ISS V10.
15. **General Security Measures**
 - a. Upgrade OS and IIS webservers to latest version.
 - b. Website admin panel should only be accessible via white-listed IPs.
 - c. Complete analysis and penetration testing of application be carried out to identify potential threats on routine basis.
 - d. Compete website be deployed on inland servers including database and web infrastructure.
 - e. HTTPS protocol be used for communication between client and web server.
 - f. Application and database be installed on different machines with proper security hardening.
 - g. Sensitive data be stored in encrypted from with no direct public access.

SECRET

SECRET

- h. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.
- i. Up dated antivirus tools/ firewalls be used on both endpoints and servers to safeguard from potential threats.
- j. Enforce a strong password usage policy.
- k. Remote management services like RDP and SSH must be disabled in production environment.
- l. Deploy web application firewalls for protection against web attacks.
- m. Employ secure coding practices such as parameterized queries, proper input sanitization and validation to remove malicious scripts.
- n. Keep system and network devices up to date.
- o. Long retention policy must be devised for at least 3x months on separate device, for attacker's reconnaissance.

SECRET