Web Application Security Test Report

Indian Trade Portal

Test URL:

https://test.indiantradeportal.in/

https://test.indiantradeportal.in/20itp14/

July 21th, 2015

Interim-1

CyberQ Consulting Pvt. Ltd.

 # 622, DLF Tower A, Jasola,

New Delhi-44

INDIA

Main Switchboard: 011 41077560/1

Copyright Notice - Proprietary Information

Document Version Control			
Data Classification	CLASSIFIED		
Client Name	FIEO		
Document Title	Web Application Security Test Report		
Authors	Ashwini Srivastava		
Version	**Date of Issue**	**Issued by**	**Change Description**
1.0	21-07-2015	CyberQ Team	Initial Issue

Web Application Security Test Report

Presented by: Ashwini Srivastava

Application Testing Conducted On:

13-07-2015 to 21-07-2015

Table of Contents

1 Executive Summary

Purpose

CyberQ was asked to conduct a Web Application Security Test on the application provided by E2E Research Service Pvt Ltd. Details were provided to the extent mentioned in "Scope of Work". The testing was carried out from CyberQ Consulting Pvt. Ltd., New Delhi. The objective of this testing was to ensure the security of the network and web server from external threats through the web application.

The audit was carried on the staging URL: https://test.indiantradeportal.in/, https://test.indiantradeportal.in/20itp14/.
The scope of the project was limited to find out the vulnerable areas of the Web application. Exploiting the vulnerabilities was out of scope for the tests.

Authority

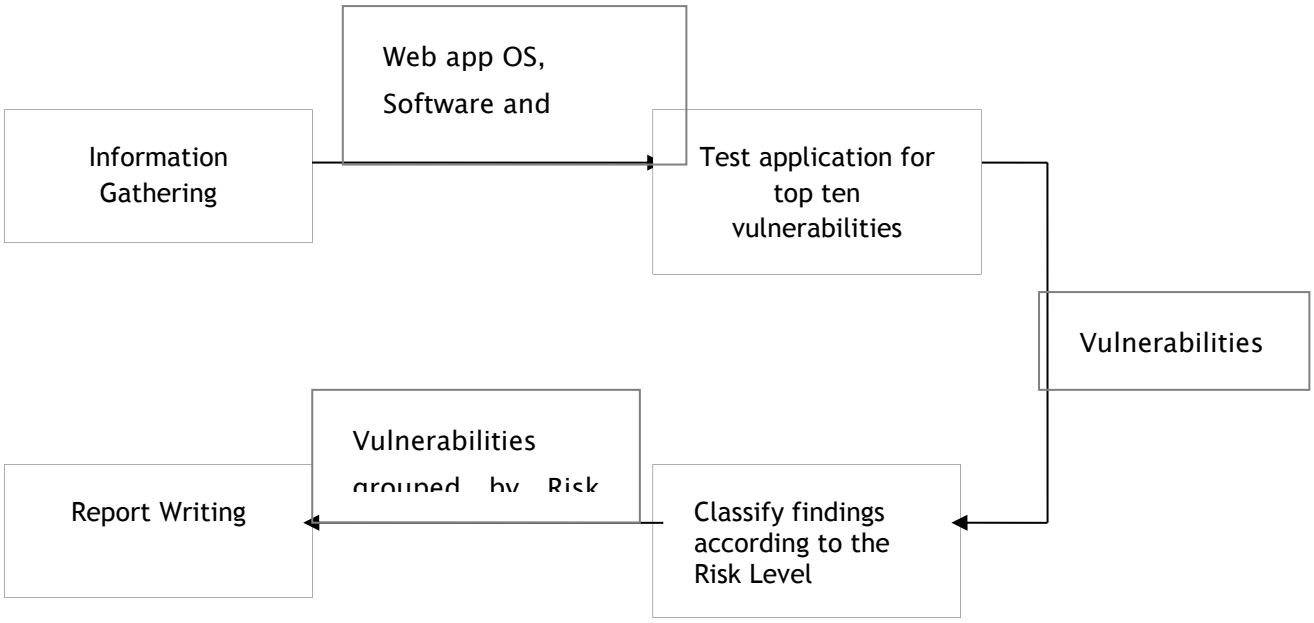
The Web Application Security Test was conducted under the authority of Mr.Chandra Nath Som of FIEO.

Auditor

Ashwini Srivastava

2 Methodology

The methodology applied in Web Application Security Testing is explained in the diagram below



Information Gathering: One of the first steps of this test is to identify the Web application environment, including the scripting language and Web server software in use, and the operating system of the target server. However, this step is generally omitted if the testing is limited to just the web application and not the host.

Test Application: While testing the application, we follow but are not limited to the OWASP standards. The top 10 vulnerabilities are tested for static and dynamic web sites. Our testing is done manually as well as using tools. An indicative list of tools is given in the section below.

After an exhaustive testing, the findings are compiled and classified according to a Risk Level of High, Medium or Low depending on the harm they may cause to the Web Application, server or to the network.

A Report is created highlighting the findings together with details for each finding.

3 Scope of Work

The audit was carried on the staging server URL: https://test.indiantradeportal.in/, https://test.indiantradeportal.in/20itp14/. The scope of the project was limited to find out the vulnerable areas of the Web application. Exploiting the vulnerabilities was out of scope for the tests.

4 Table of Findings

The following key findings support our assessment of the weaknesses associated with the application:-

Sl. No.	Severity	Vulnerability Description	Level-1	Interim-1
1	**High**	The password between server and client is being passed in clear text.	**Open**	**Closed**
2	**High**	No client or server side input validation has been implemented; This test successfully embedded a script in the response, which will be executed once the page is loaded in the user's browser. **Cross Site Scripting attack is possible**.	**Open**	**Open (Patch throughout the application)**
3	**High**	An .exe file can be uploaded. In this case it will be possible to upload unwanted self executing files to the server, which may be harmful for the server and the application. There should be a check on the file size as well. Also as this file upload feature is provided to general public anyone can knowingly or unknowingly upload a file infected by viruses and worms.	**Closed**	**Open (Patch throughout the application)**
4	**High**	Cross Site Request Forgery (CSRF) attack is possible Which forces a logged-on victim's browser to send a request to a vulnerable web application, which then performs the chosen action on behalf of the victim.	**Closed**	**Closed**
5	**Medium**	Improper Error Handling in the application.	**Open**	**Open (Patch throughout the application)**

Sl. No.	Severity	Vulnerability Description	Level-1	Interim-1
6	Medium	Server Errors are displayed to the user on giving invalid input.	Open	Open (Patch throughout the application)
7	Medium	Application allows to user to set very simple password. Password complexity is not implemented.	Open	Open
8	Medium	While changing password, there is no check on password history. This allows the user to change the password to his previous password.	Closed	Open
9	Medium	It is possible to view the sensitive information by fetching the page from the cache option of the browser.	Closed	Open (Patch throughout the application)
10	Medium	Http Only flag is not set.	Closed	Open
11	Medium	The Security answer between server and client is being passed in clear text.	Closed	Closed
12	Medium	The application has the provision for windows to remember the password to the application.	Closed	Closed
13	Medium	Application not terminating the session once directed to error page.	Open	Open (Patch throughout the application)

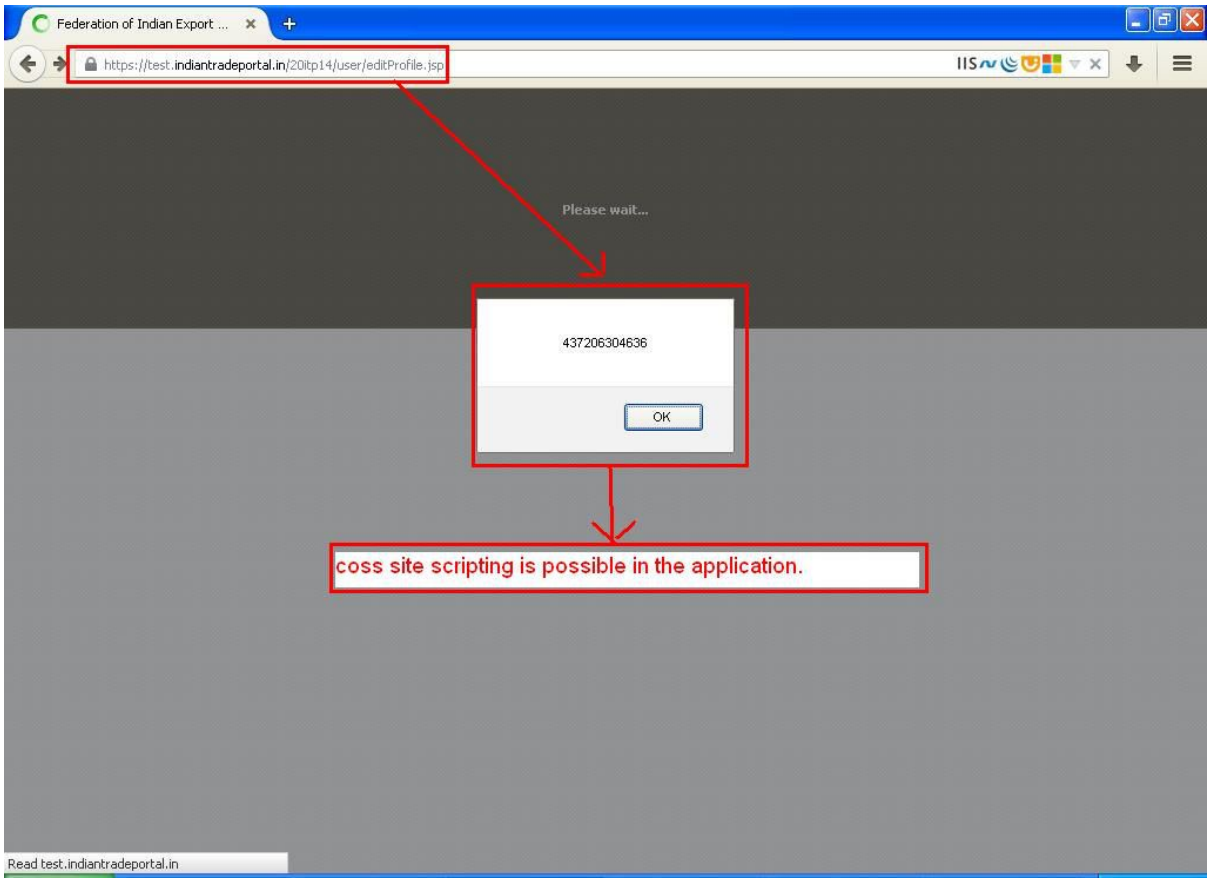
Sl. No.	Severity	Vulnerability Description	Level-1	Interim-1
14	Medium	Application has a provision to browse authenticated page through back button.	**Not Found**	**Open** **(Patch throughout the application)**
15	Medium	The Salt length is too short and not as per the NIC guidelines.	**Not Found**	**Open**
16	Medium	The salting processes is not as per the OWASP guidelines.	**Not Found**	**Open**
17	Medium	Session timeout is not implemented in application.	**Not Found**	**Open** **(Patch throughout the application)**

Finding No. 2

Description: No client or server side input validation has been implemented; this test successfully embedded a script in the response, which will be executed once the page is loaded in the user's browser. **Cross Site Scripting attack is possible.**

Recommendation: The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.

Screen shots/Evidence:



Finding No. 3

Description: An .exe file can be uploaded. In this case it will be possible to upload unwanted self executing files to the server, which may be harmful for the server and the application. There should be a check on the file size as well. Also as this file upload feature is provided to general public anyone can knowingly or unknowingly upload a file infected by viruses and worms.

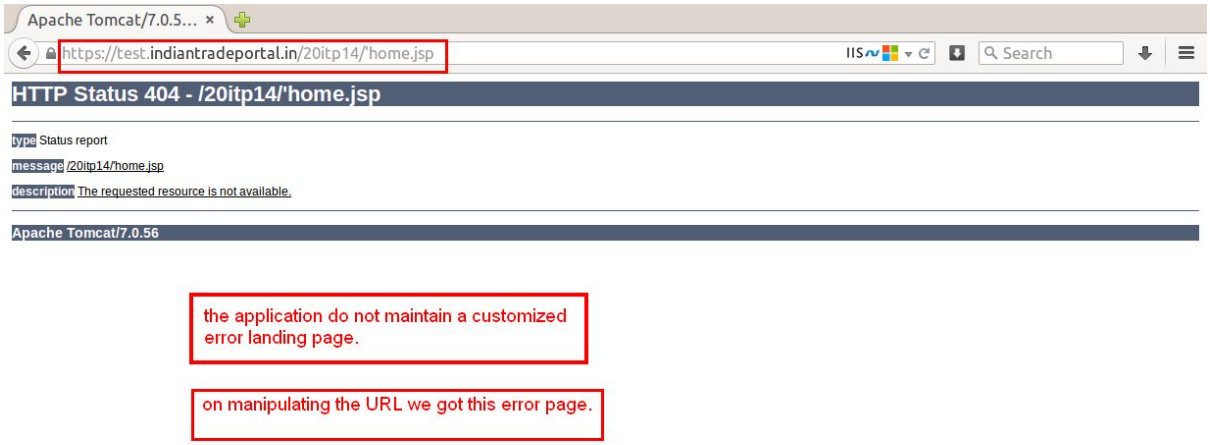
Recommendation: The application should not provide this facility of file upload to general public as the file upload feature is susceptible to many vulnerabilities and attacks. Only if it is extremely necessary this facility should be provided. In this case also the application should not allow any executable or malicious files to be uploaded into the database. The header information should be checked for to see the content and type of file. The file size should also be checked so that users do not upload large files which would eat up the server space.

Finding No. 5

Description: Improper error handling.

Recommendation: The application should validate input and trap all errors and give customized message to the user. Validation at the server end is mandatory.

Screen shots/Evidence:

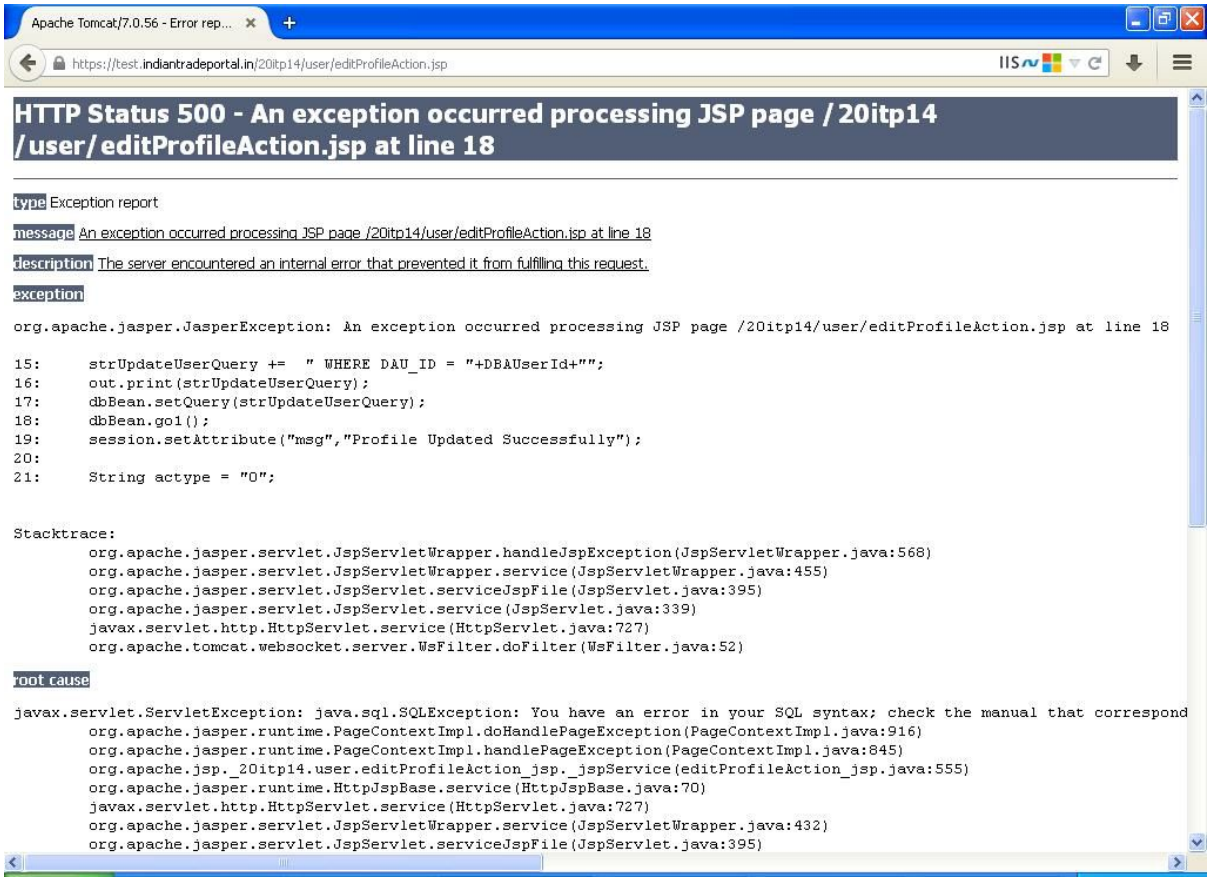


Finding No. 6

Description: Server error is displayed to the user.

Recommendation: The application must maintain a customized error page for manage the errors. so that if a user landed to the error page he/she may redirected to the customized error page.

Screen shots/Evidence:



Finding No. 7

Description: Improper Password complexity has been implemented in password policy. NO upper case check is implemented.

Recommendation: Passwords should have restrictions that require a minimum Size of 8 characters and complexity for the password. Complexity typically requires the use of minimum combinations of alphabetic, numeric, and/or non-alphanumeric characters in a user's password (e.g. one special character($,@,#,&),one upper case letter and one lower case letter and one number like Test@123).

Finding No. 8

Description: While changing password, there is no check on password history. This allows the user to change the password to his previous password. It accepts previous/old password as new password during the password change.

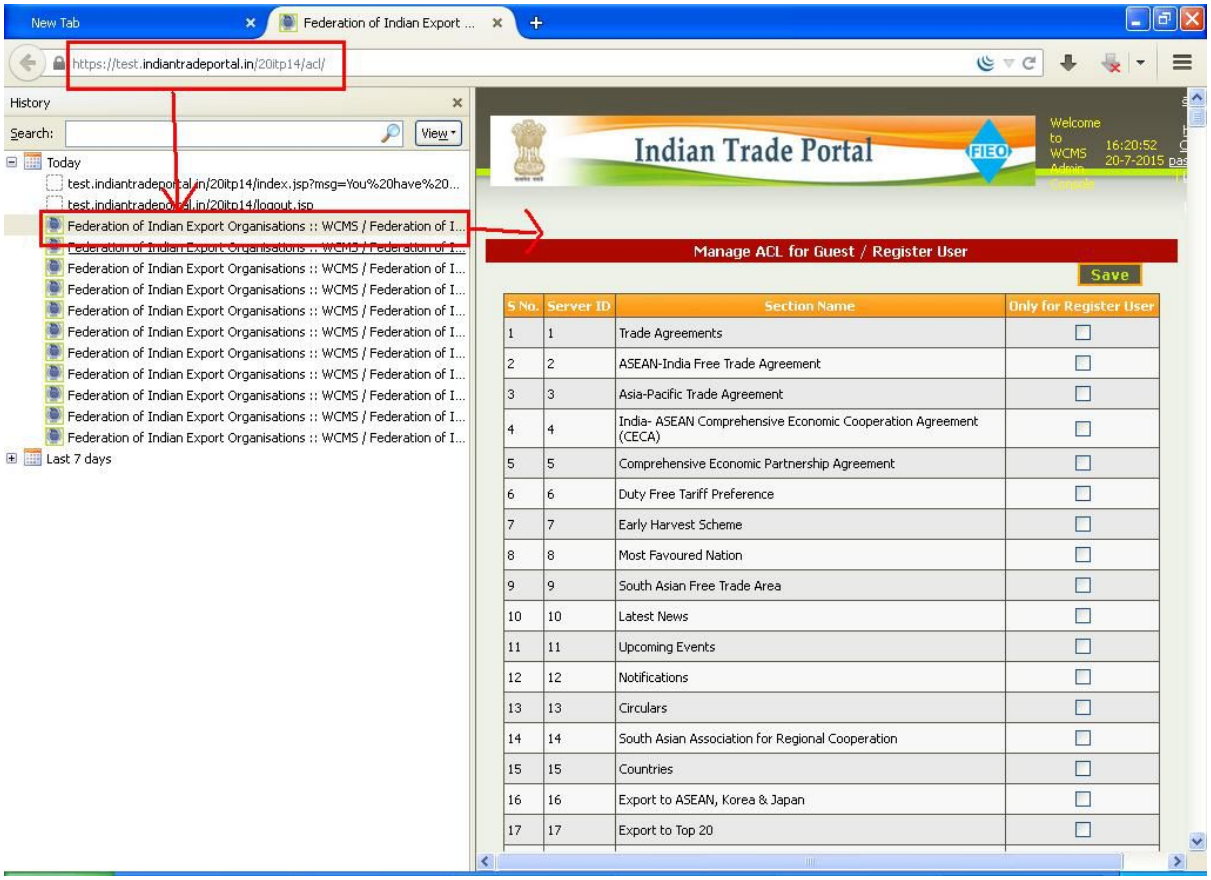
Recommendation: Users should be required to change their password periodically. Users should be prevented from reusing previous passwords. Password history should ideally be 3.

Finding No. 9

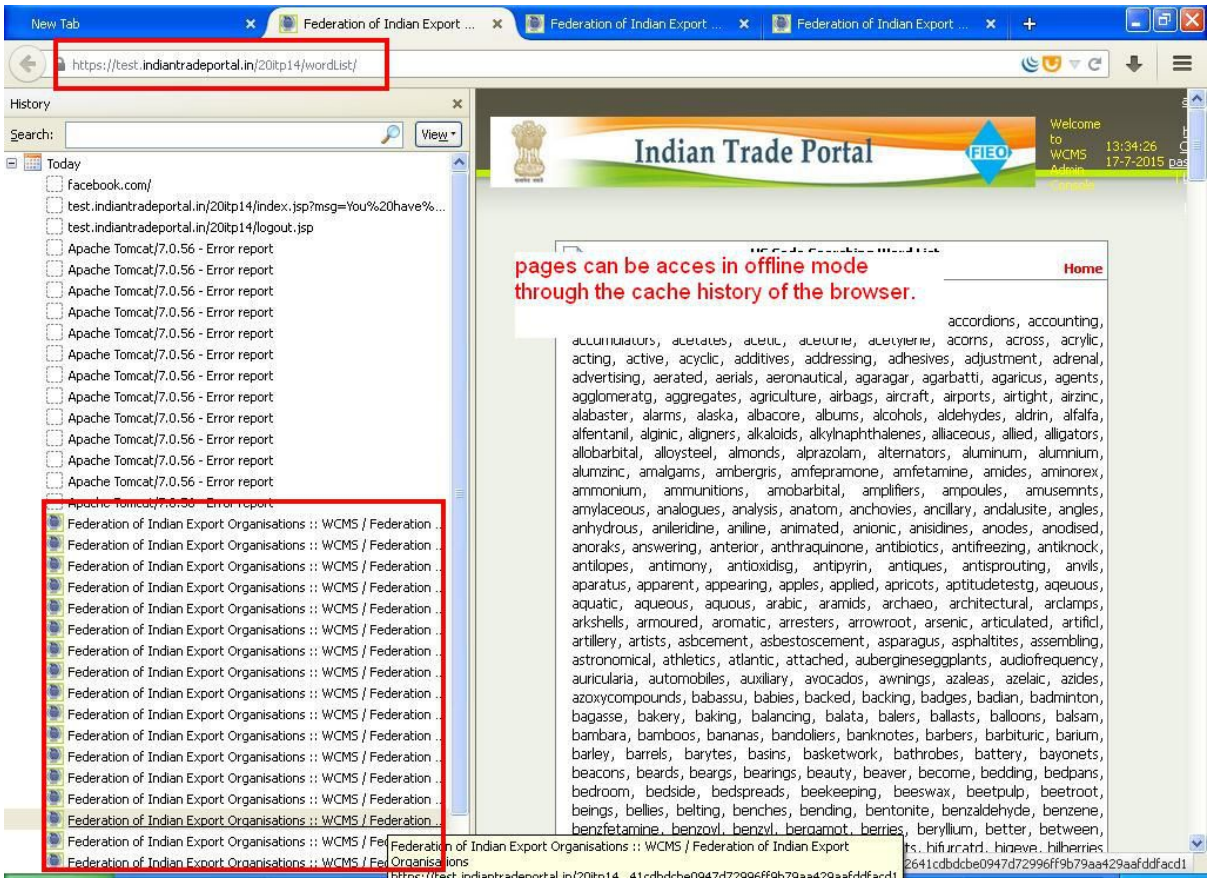
Description: It is possible to view the sensitive information by fetching the page from the cache option of the browser.

Recommendation: Cache for all pages should be cleared from server side, and also extra pages should be removed.

Screen shots/Evidence:



S No.	Server ID	Section Name	Only for Register User
1	1	Trade Agreements	☐
2	2	ASEAN-India Free Trade Agreement	☐
3	3	Asia-Pacific Trade Agreement	☐
4	4	India- ASEAN Comprehensive Economic Cooperation Agreement (CECA)	☐
5	5	Comprehensive Economic Partnership Agreement	☐
6	6	Duty Free Tariff Preference	☐
7	7	Early Harvest Scheme	☐
8	8	Most Favoured Nation	☐
9	9	South Asian Free Trade Area	☐
10	10	Latest News	☐
11	11	Upcoming Events	☐
12	12	Notifications	☐
13	13	Circulars	☐
14	14	South Asian Association for Regional Cooperation	☐
15	15	Countries	☐
16	16	Export to ASEAN, Korea & Japan	☐
17	17	Export to Top 20	☐

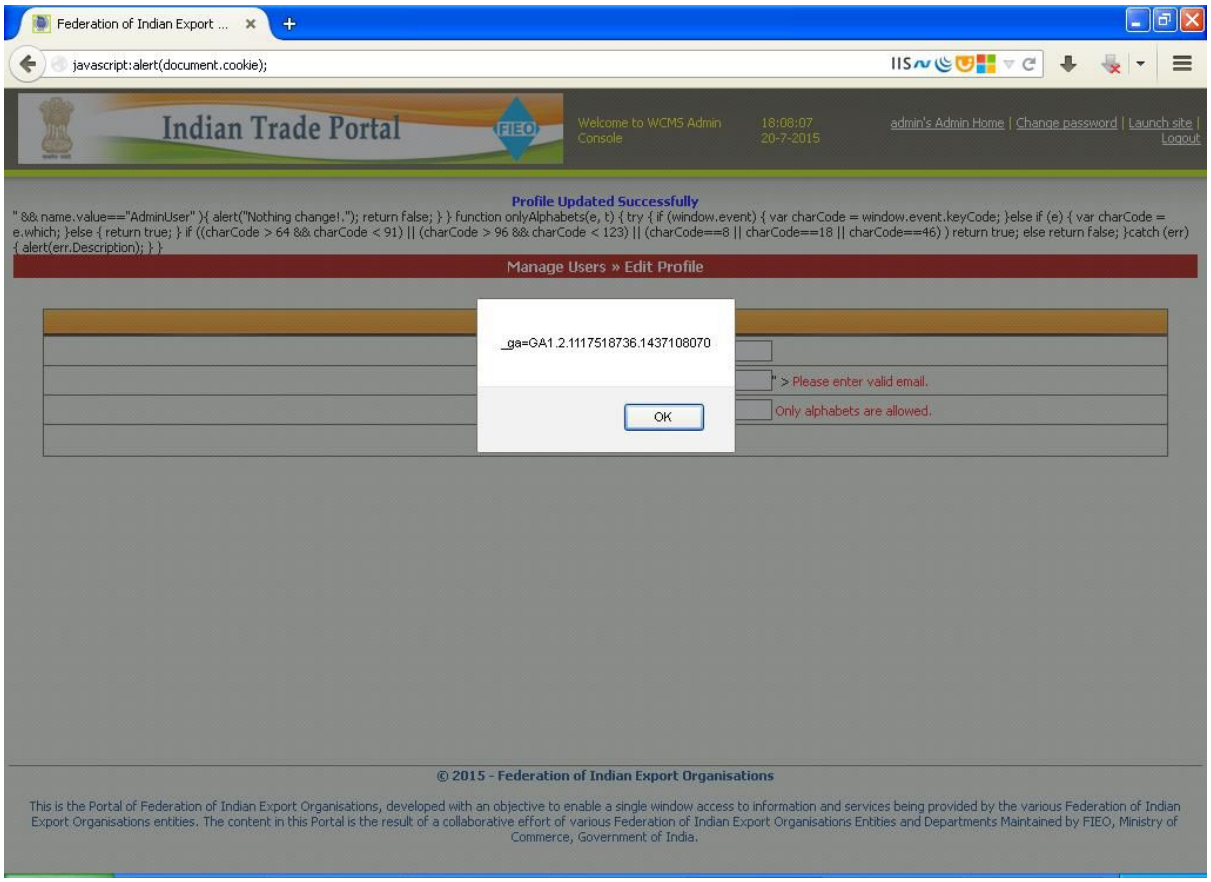

New Tab
Federation of Indian Export ...
https://test.indiantradeportal.in/20itp14/wordList/
History
Search:
View
Today
facebook.com/
test.indiantradeportal.in/20itp14/index.jsp?msg=You%20have%...
test.indiantradeportal.in/20itp14/logout.jsp
Apache Tomcat/7.0.56 - Error report
Federation of Indian Export Organisations :: WCMS / Federation ..
Indian Trade Portal
Welcome to WCMS
13:34:26
17-7-2015
pages can be acces in offline mode through the cache history of the browser.
Home
accordions, accounting, acting, active, acyclic, additives, addressing, adhesives, adjustment, adrenal, advertising, aerated, aerials, aeronautical, agaragar, agarbatti, agaricus, agents, agglomeratg, aggregates, agriculture, airbags, aircraft, airports, airtight, airzinc, alabaster, alarms, alaska, albacore, albums, alcohols, aldehydes, aldrin, alfalfa, alfentanil, alginic, aligners, alkaloids, alkylnaphthalenes, alliaceous, allied, alligators, allobarbital, alloysteel, almonds, alprazolam, alternators, aluminum, alumnium, alumzinc, amalgams, ambergris, amfepramone, amfetamine, amides, aminorex, ammonium, ammunitions, amobarbital, amplifiers, ampoules, amusemnts, amylaceous, analogues, analysis, anatom, anchovies, ancillary, andalusite, angles, anhydrous, anileridine, aniline, animated, anionic, anisidines, anodes, anodised, anoraks, answering, anterior, anthraquinone, antibiotics, antifreezing, antiknock, antilopes, antimony, antioxidisg, antipyrin, antiques, antisprouting, anvils, aparatus, apparent, appearing, apples, applied, apricots, aptitudetestg, aqeuous, aquatic, aqueous, aquous, arabic, aramids, archaeo, architectural, arclamps, arkshells, armoured, aromatic, arresters, arrowroot, arsenic, articulated, artificl, artillery, artists, asbcement, asbestoscement, asparagus, asphaltites, assembling, astronomical, athletics, atlantic, attached, auberginesegplants, audiofrequency, auricularia, automobiles, auxiliary, avocados, awnings, azaleas, azelaic, azides, azoxycompounds, babassu, babies, backed, backing, badges, badian, badminton, bagasse, bakery, baking, balancing, balata, balers, ballasts, balloons, balsam, bambara, bamboos, bananas, bandoliers, banknotes, barbers, barbituric, barium, barley, barrels, barytes, basins, basketwork, bathrobes, battery, bayonets, beacons, beards, beargs, bearings, beauty, beaver, become, bedding, bedpans, bedroom, bedside, bedspreads, beekeeping, beeswax, beetpulp, beetroot, beings, bellies, belting, benches, bending, bentonite, benzaldehyde, benzene, benzfetamine, benzoyl, benzyl, bergamot, berries, beryllium, better, between,
Federation of Indian Export Organisations :: WCMS / Federation of Indian Export Organisations

Finding No. 10

Description: Http Only flag is not set. It is possible to reveal sensitive information about the authenticated cookie of a user's session.

Recommendation: Set Http Only flag value to True in websites configuration file.

Screen shots/Evidence:

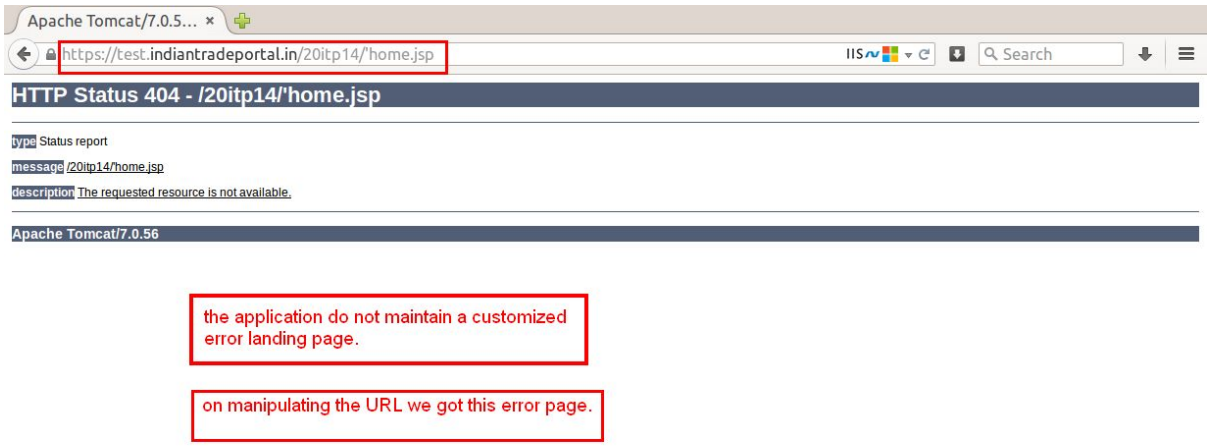


Finding No. 13

Description: Application not terminating the session once directed to error page.

Recommendation: Application must terminate its session on landing to a customized error page, user shall be asked again to enter the login credentials.

Screen shots/Evidence:

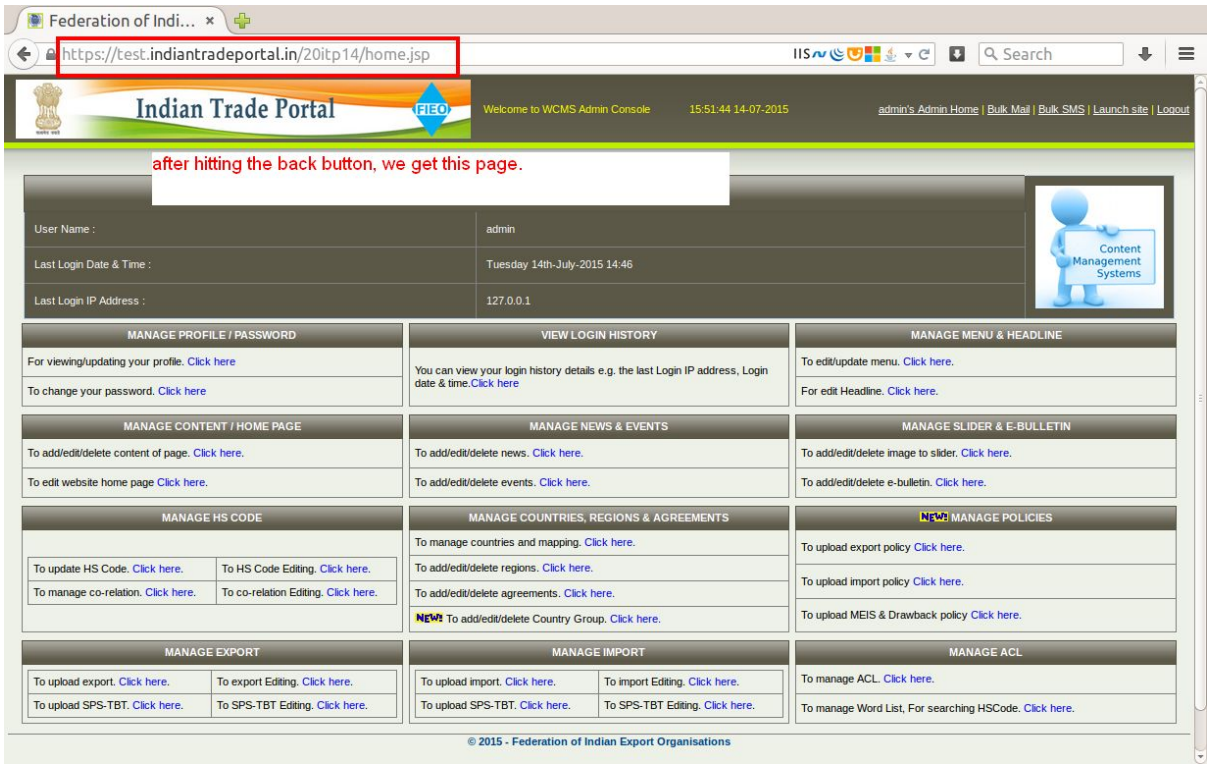


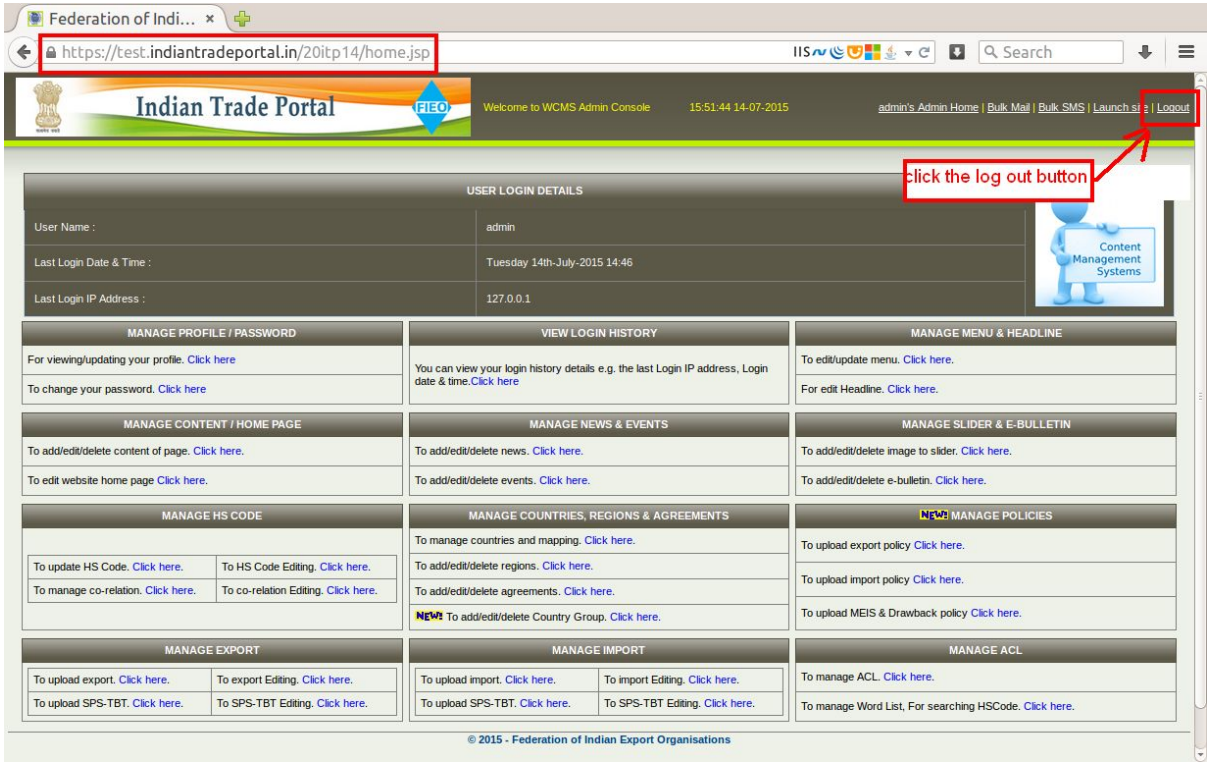
Finding No. 14

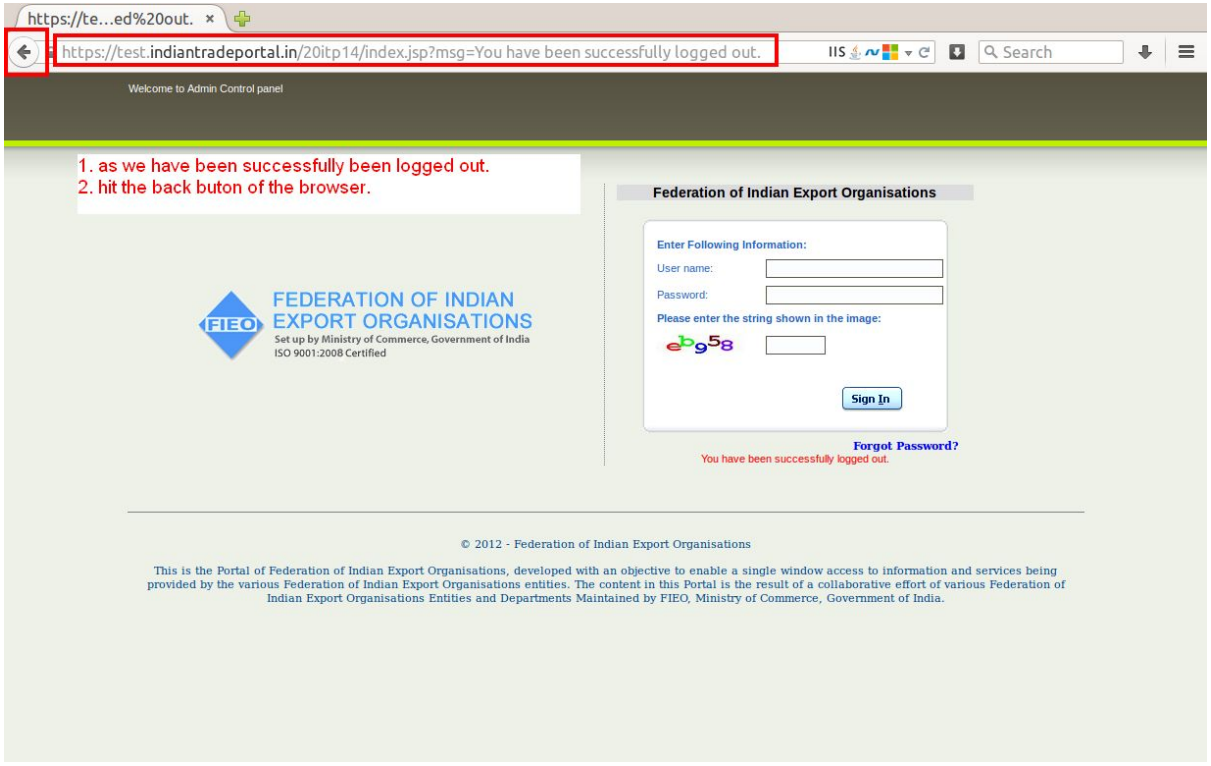
Description: Application has a provision to browse authenticated page through back button.

Recommendation: Back button should be disabled.

Screen shots/Evidence:




Federation of Indi...
https://test.indiantradeportal.in/20itp14/home.jsp
Search
Indian Trade Portal
Welcome to WCMS Admin Console
15:51:44 14-07-2015
admin's Admin Home | Bulk Mail | Bulk SMS | Launch site | Logout
click the log out button
USER LOGIN DETAILS
User Name : admin
Last Login Date & Time : Tuesday 14th-July-2015 14:46
Last Login IP Address : 127.0.0.1
Content Management Systems
MANAGE PROFILE / PASSWORD
For viewing/updating your profile. Click here
To change your password. Click here
VIEW LOGIN HISTORY
You can view your login history details e.g. the last Login IP address, Login date & time.Click here
MANAGE MENU & HEADLINE
To edit/update menu. Click here.
For edit Headline. Click here.
MANAGE CONTENT / HOME PAGE
To add/edit/delete content of page. Click here.
To edit website home page Click here.
MANAGE NEWS & EVENTS
To add/edit/delete news. Click here.
To add/edit/delete events. Click here.
MANAGE SLIDER & E-BULLETIN
To add/edit/delete image to slider. Click here.
To add/edit/delete e-bulletin. Click here.
MANAGE HS CODE
To update HS Code. Click here.
To HS Code Editing. Click here.
To manage co-relation. Click here.
To co-relation Editing. Click here.
MANAGE COUNTRIES, REGIONS & AGREEMENTS
To manage countries and mapping. Click here.
To add/edit/delete regions. Click here.
To add/edit/delete agreements. Click here.
NEW! To add/edit/delete Country Group. Click here.
NEW! MANAGE POLICIES
To upload export policy Click here.
To upload import policy Click here.
To upload MEIS & Drawback policy Click here.
MANAGE EXPORT
To upload export. Click here.
To export Editing. Click here.
To upload SPS-TBT. Click here.
To SPS-TBT Editing. Click here.
MANAGE IMPORT
To upload import. Click here.
To import Editing. Click here.
To upload SPS-TBT. Click here.
To SPS-TBT Editing. Click here.
MANAGE ACL
To manage ACL. Click here.
To manage Word List, For searching HSCode. Click here.
© 2015 - Federation of Indian Export Organisations

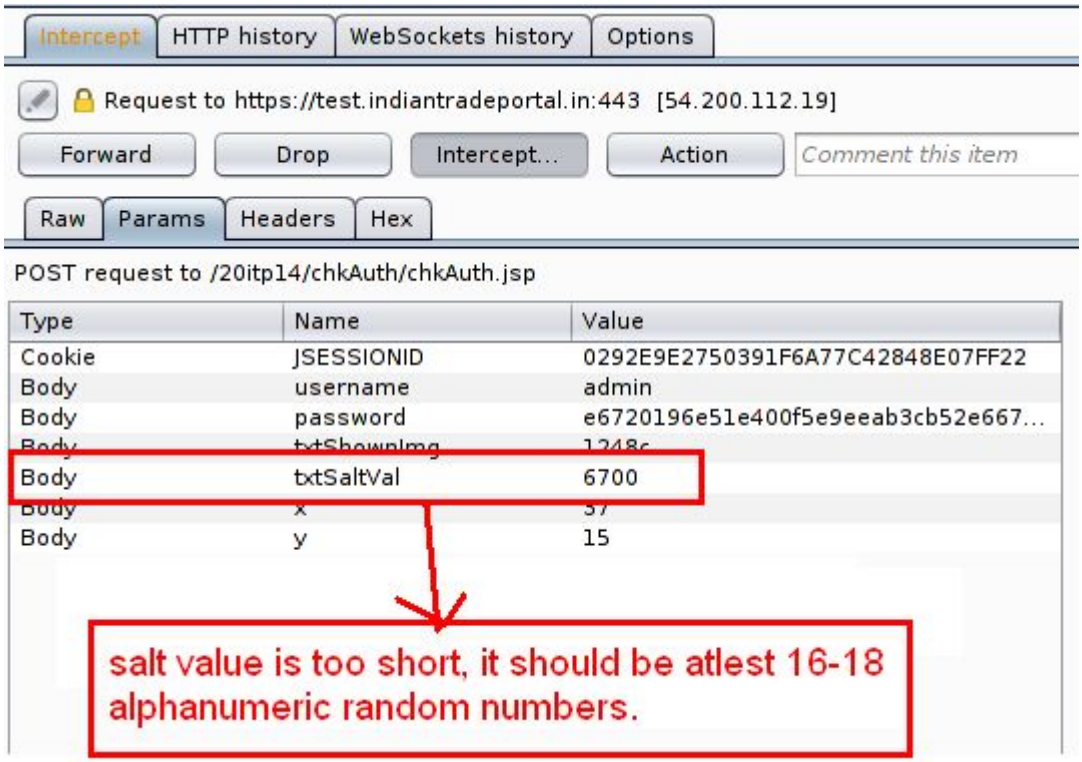

https://te...ed%20out.
https://test.indiantradeportal.in/20itp14/index.jsp?msg=You have been successfully logged out.
Search
Welcome to Admin Control panel
1. as we have been successfully been logged out.
2. hit the back buton of the browser.
FEDERATION OF INDIAN EXPORT ORGANISATIONS
Set up by Ministry of Commerce, Government of India
ISO 9001:2008 Certified
Federation of Indian Export Organisations
Enter Following Information:
User name:
Password:
Please enter the string shown in the image:
Sign In
Forgot Password?
You have been successfully logged out.
© 2012 - Federation of Indian Export Organisations
This is the Portal of Federation of Indian Export Organisations, developed with an objective to enable a single window access to information and services being provided by the various Federation of Indian Export Organisations entities. The content in this Portal is the result of a collaborative effort of various Federation of Indian Export Organisations Entities and Departments Maintained by FIEO, Ministry of Commerce, Government of India.

Finding No. 15

Description: The Salt length is too short and not as per the NIC guidelines.

Recommendation: Salt length must be at least 16-18 digits of length. It will be ideal that salt can be alpha numeric too.

Screen shots/Evidence:



Finding No. 16

Description: The salting processes is not as per the OWASP guidelines. What is actually happening that the password is converted into a MD5 hash, and the random number(salt) is converted to MD5 hash. These both the has are now been concatenate with a hyphen "-" symbol.

Recommendation:

The proper salting process is explained below step by step:

1. 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.

2. A JavaScript code on the client computes the hash of the password entered by the user.

3. It then concatenates the salt to the hash and then re-computes the hash.

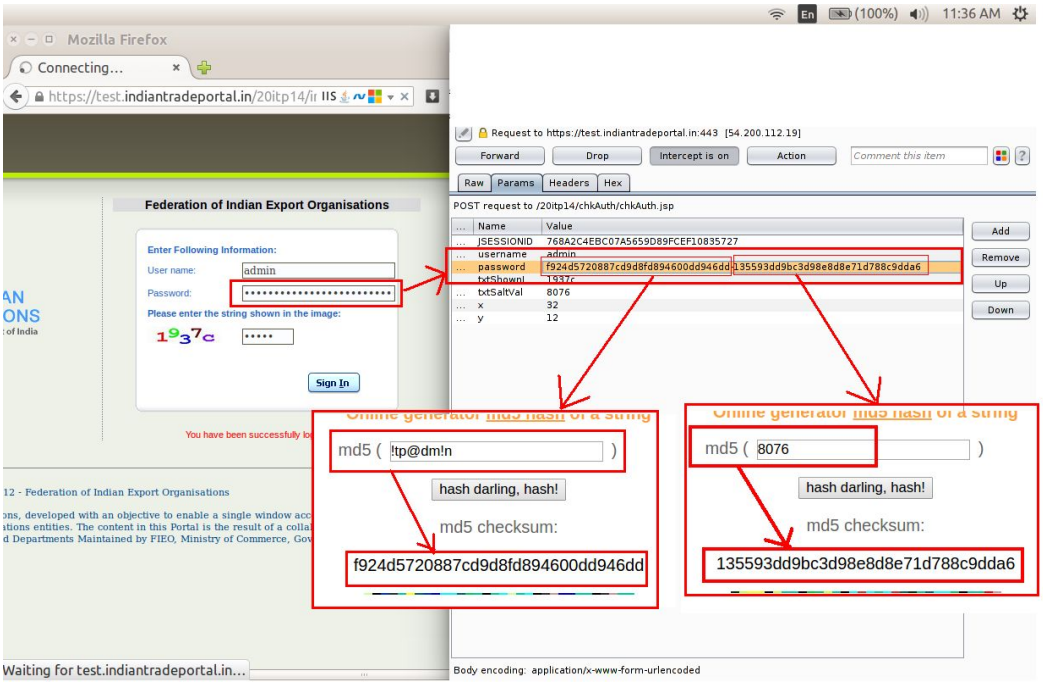
4. This result is then sent to the server.

5. The server picks the hash of the password from its database, concatenates the salt and computes the hash.

6. If the user entered the correct password these two hashes should match.

7. The server compares the two and if they match, the user is authenticated.

Screen shots/Evidence:



Finding No. 17

Description: Session timeout is not implemented in application.

Recommendation: Session timeout (ideally 15 minutes) should be implemented in application.