



**USAID**  
FROM THE AMERICAN PEOPLE

**BUSINESS CLIMATE  
REFORM**



# EVALUATION OF E-FILING SECURITY AND RECOMMENDATIONS

**DRAFT  
VERSION 1.0**

**15 June 2008**

This publication was produced for review by the United States Agency for International Development. It was prepared by Sadik Crnovrsanin, contract No AFP-I-00-04-00002-00, TO 3, managed by Chemonics International Inc. and submitted to USAID /Caucasus cognizant Technical officer John Hansen.

## **DISCLAIMER**

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

# CONTENTS

1. EXECUTIVE SUMMARY .....	3
2. BACKGROUND .....	3
3. CONTENTS.....	3
4. KEY BENEFITS.....	3
5. RECOMMENDATIONS .....	3
5.1 CONNECTION STRING & CONNECTION STRING USERS.....	3
5.2 INPUT VALIDATION.....	4
5.3 ORIGIN OF REQUEST VALIDATION .....	4
5.4 TOOLS AND EXTERNAL RECOURSES TO VALIDATE APPLICATION .....	5
5.5 SERVER CONFIGURATION .....	6
5.6 NETWORK CONFIGURATION .....	6
5.7 FRAMEWORK 3.5 .....	7
5.8 DATABASE LINK.....	7
5.9 SSL CERTIFICATION AUTHENTICATION .....	8
5.10 ONLY IE SUPPORT .....	8
5.11 CUSTOMS ERROR PAGES AND DEBUG MODE.....	8
5.12 SECONDARY SERVER, TEST SERVER.....	10
5.13 E-FILE MENU REORGANIZATION .....	10
6. CONCLUSION.....	11

# EXECUTIVE SUMMARY

The purpose of this document is to evaluate e-filing application and develop recommendations for improving functionality and security issues. The State Revenue Service (SRS) is currently implementing e-filing application and plans to make it a core for its e-services. In order to ensure effective and security operation of the system, a security audit of the web application has been performed. A set of recommendations are given to improve security and stability of the system. Recommendations will help establish a stable infrastructure that will be used as backbone for future e-government services.

## 1. Background

The USAID BCR project procured an e-filing web system which allowed SRS/MoF to provide better quality service to its taxpayers. This service is considered a great asset to taxpayers by providing the taxpayer with valuable services. The E-filing system makes it easier for businesses to submit tax declarations and review its tax balance sheet at any moment. The goal of the e-file service is to assist taxpayers with taxes and directly improve the business climate.

## 2. Contents

This document covers the following:

- a) Security Recommendations for e-filing system

## 3. Key Benefits

- Improve security aspect of e-filing
- Provide stable and safe infrastructure to be used for future e-services
- Provide safe and secure E-service portal

## 4. Recommendations

### 5.1 Connection String & connection string users

The e-filing application uses plain text connection strings which are stored in config global file. Unfortunately, the connection string is not encrypted, making it a high security risk. If the configuration file was ever exported or copied from server, accounts and passwords could be easily read. Priority: High.

**Recommendation 5.1.1:** Encrypt connection string used by web applications

At the time of review, about 8 old and unused connection strings were left over from previous version of software or testing. These old connection strings and referred accounts need to be removed. Only the production connection string should be present. Priority: High.

**Recommendation 5.1.2:** Remove old or unused connection strings.

The password used for connection strings was only 2 characters long. A stronger password with a mix of letters and alpha characters should be introduced. Also, a password for connection string accounts should be updated periodically. Priority: High.

**Recommendation 5.1.3:** Use stronger passwords for connecting string accounts.

**Recommendation 5.1.4:** Connection string passwords should be updated periodically.

The connection string accounts (user name: “TP”) should have very limited privileges on DB. During review of TP privileges on the Oracle database, it was noted that “TP” account had DBA (full database administrator) privileges. This in effect allowed this relatively public user name to delete, drop, or perform any administration level operation directly on database. Importantly, this account could have been used to grant privileges to other accounts, making it very hard to validate data integrity. Connection string accounts should have very limited privileges on the server. Priority: High.

**Recommendation 5.1.5:** The account used for connection string should only have SELECT and INSERT privileges on the Database (Connect, Select, Insert).

## 5.2 Input validation

During review of the e-filing application, it has been discovered that the system is predisposed to SQL injection attack. SQL injection attacks are considered a high risk for all web applications. The way it works is that user enters pure SQL code in one of the input boxes or parameters. Then if application is not validating inputs, the improper SQL functions will be inadvertently executed. This theoretically can allow users to delete or update data directly in the database. Hacking tools have been written to take advantage of these issues and cause problems with systems. Luckily, protection is very simple; all input boxes have to be validated to only accept alpha and number characters (abcd...ABCD...01234..). Characters (“!#\$’%^^&\*()-<>/) and keywords (update, insert, delete, drop) should be blocked and ignored. Priority: High.

**Recommendation 5.2.1:** Validate and ensure only clean data is executed by application.

**Recommendation 5.2.2:** Use tools to validate website (see 5.4 section)

## 5.3 Origin of request Validation

During review of the e-filing application and its source code, it was noted that the application does not check source of request. This goes together with SQL injection from 5.2 section of this document. All requests that come to the web server should have their requesting source information checked. Only requests originated by a validated server should be executed. This is important since parameters and data can

be extracted by special tools, manipulated and then sent back to server for execute. Priority: Medium.

**Recommendation 5.2.1:** Validate source of requests

#### **5.4 Tools and external recourses to validate application**

A great deal of resources and tools exist to help and improve security of web applications. It is highly recommended that tools be used periodically to ensure up to date security polices. Priority: High.

Security scanning tools should be used periodically to scan the entire site and check all security aspects of the webpage. Acunetic is commercial tool that is considered a standard tool for security scans. It provides a wide array of testing tools and is frequently updated.

**Recommendation 5.4.1:** The security scanner, Acunetix Web Vulnerability Scanner should be used periodically

There are also free security tools like SQL Inject Me that examine webpages and indicate problematic areas. This tool is actually an add-on to the Firefox browser and is highly recommended.

**Recommendation 5.4.2:** <http://www.securitycompass.com/> tools: (Exploit-Me and SQL Inject Me)

The US Department of Defense has the check list that is updated almost monthly that has detailed instructions on how to check and update your system to achieve maximum security. This list is a great source of information since it has step by step instructions on how to fix and what to look for. All federal agencies in the US are advised/required to use this check list.

**Recommendation 5.4.3:** Follow check list and recommendations from <http://iase.disa.mil/stigs/checklist/> Web Checklist IIS

Microsoft has its own security check list.

**Recommendation 5.4.4:** Check website against Microsoft security check list. <http://msdn2.microsoft.com/en-us/library/bb355989.aspx>

There are many books relating to the security of web applications on the subject of ASP.net and ISS web server. I personally like this book because of its real world examples:

**Recommendation 5.4.5:** The book: Professional ASP.NET Security, Membership, And Role Management is a great source of information.

## 5.5 Server configuration

During the first review, the e-filing application system was running on Windows 2000 server OS and on IIS server 5.0. These two software releases are considered old and not as secure as new Windows 2003 server and the IIS 6.0 server. Keep in mind that the IT department did start moving to system at the time this document was written.

**Recommendation 5.5.1:** Update to Windows server 2003

**Recommendation 5.5.2:** Update to IIS web server 6.0

**Recommendation 5.5.3:** Remove all default and unused options that are installed with IIS web server.

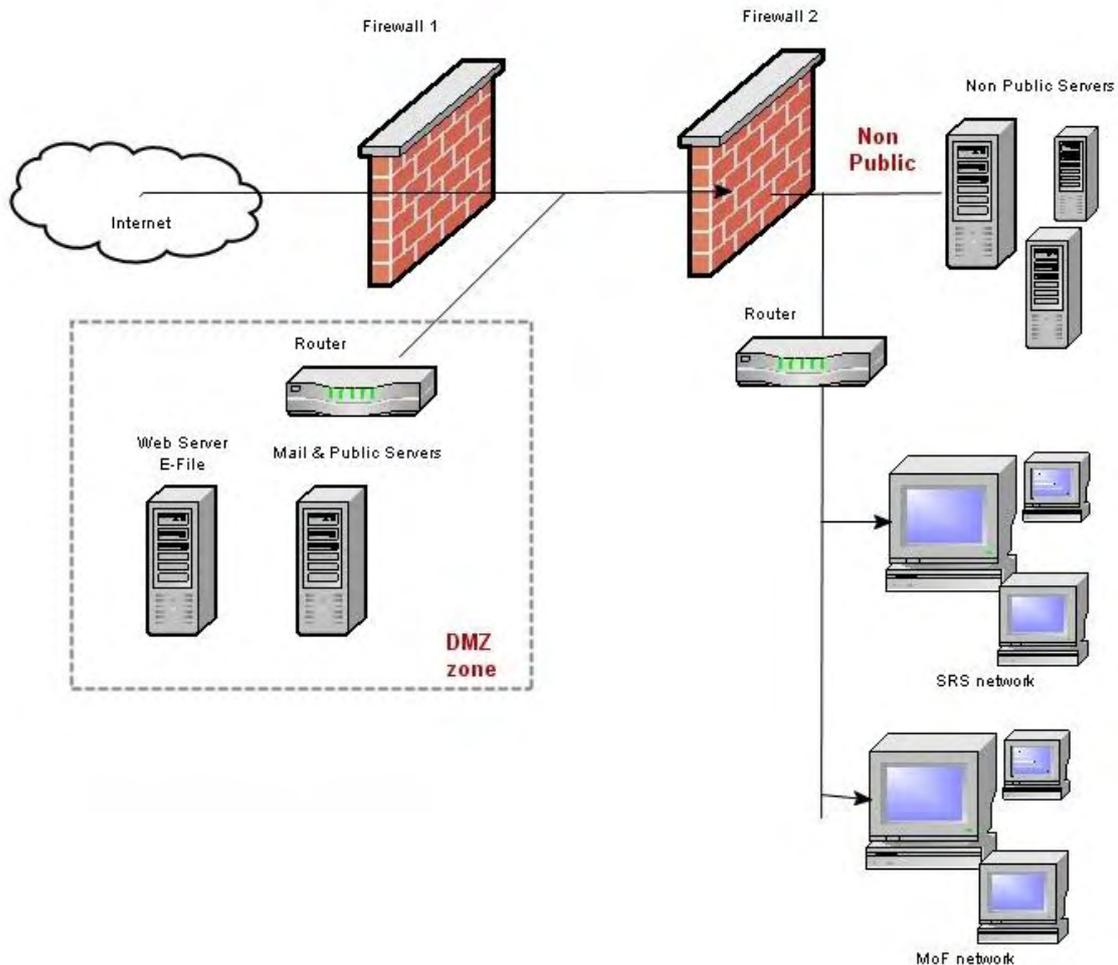
Since new security issues are found on almost a daily basis, Microsoft releases new Server Packs (SP) and patches it to its software periodically. It is crucial that the e-filing server has all of latest patches and SP installed on it. It is not recommended to enable Windows with an auto update option; instead every 60 days or so manually install the latest add-ons from the Microsoft webpage.

**Recommendation 5.5.4:** Periodically update the server with the latest Service Packs (SP) and patches.

## 5.6 Network configuration

Hosting any web server on the network is in itself considered risky activity. In most cases, companies simply outsource servers to data warehouse centers to minimize exposure of the company network. In a practical perspective, no system is secure enough and having a web server on the network is like leaving backdoor to be exploited. The recommendation would be to separate the web server from the rest of the network and place it in a De-Militarized Zone (DMZ) zone. Importantly, this means that servers in the DMZ zone will not be able to access any other part of network including “Non public” servers. New design of the network is illustrated below. Priority: High.

**Recommendation 5.6.1:** Move web servers to DMZ zone network



### 5.7 Framework 3.5

The current e-filing system runs on a 2.0.net framework. During development time this framework was considered a stable framework. Awhile back Microsoft released a new version called 3.5.net of the framework. This new version has few improvements relating to memory usage and security. Priority: Medium

**Recommendation 5.7.1:** Update current 2.0 framework to 3.5 framework

### 5.8 Database link

Currently the web database which holds web related data is linked to the main production server. This is considered a high risk security issue. If for whatever reason someone managed to take control over a web database, they could simply connect to the main production server and possibly create unforeseen problems. Actually, the web database should not know or indicate the path to any other servers on the network. Priority: High.

**Recommendation 5.8.1:** Remove link from web database to any server

It is not recommended for the web database to have any link or pointers to any servers. In other words, the web database and server should not be able to connect to any other server / data base. The main database server should connect to the web

database and extract/fetch data from the web server. Currently it is the other way around. This is done to guarantee damage containment. If the web database server gets compromised, then damage should be contained and unable to jump to other crucial servers. Priority: High.

**Recommendation 5.8.2:** Update data flow, main server (non public DB) should fetch data from the web server database in DMZ. (Chart 5.6)

### 5.9 SSL Certification Authentication

The current e-filing system uses 128 bit encryption and SSL certificate protocol. Unfortunately, at the time of review of E-file system, the SSL certificate was not “signed” by any SSL certificate authority. This is not a security risk but the e-filing application would look more professional if SSL certificate was signed by an official authority. It is recommended to get an SSL certificate from [www.VeriSign.com](http://www.VeriSign.com), which was one of the original pioneers. There are other SSL certificate authorities that charge less: [www.GoDaddySSL.com](http://www.GoDaddySSL.com), [www.DigiCert.com](http://www.DigiCert.com) or [www.rapidssl.com](http://www.rapidssl.com). Also, [www.instantssl.com](http://www.instantssl.com) does it for free (90 days). Priority: Medium

**Recommendation 5.9.1:** Acquire authentication of the E-filing SSL certificate from one of the SSL authorities.

**Recommendation 5.9.2:** Move from 128 to 256 bit encryption of SSL certificate.

### 5.10 Only IE support

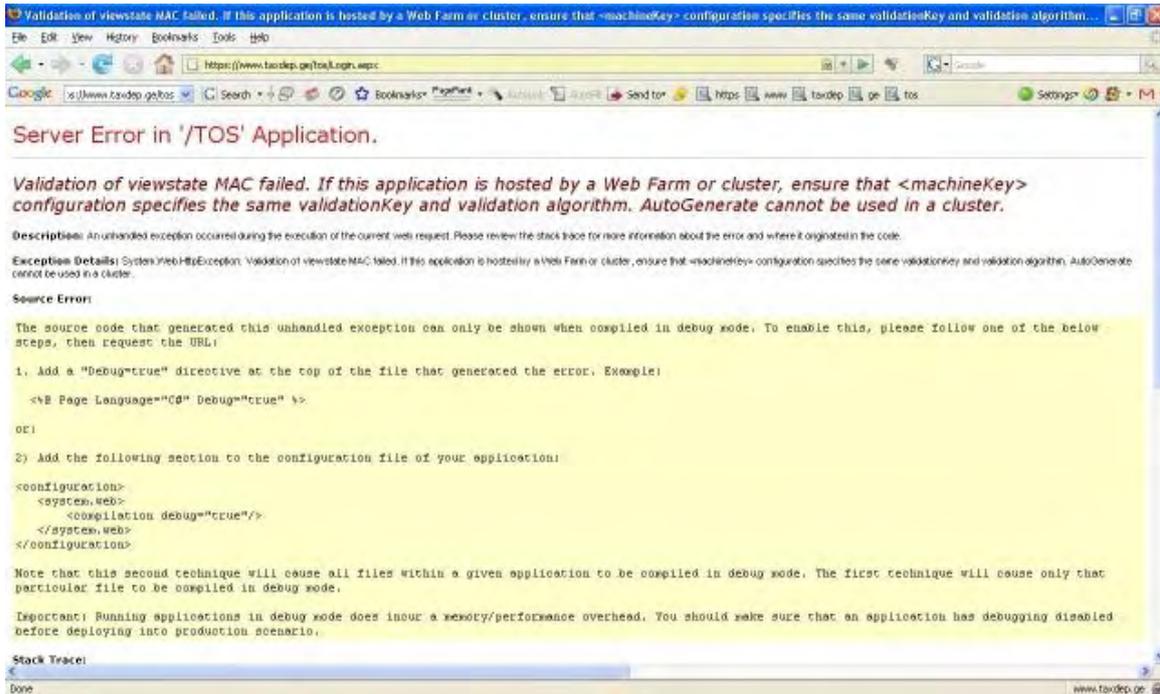
The current e-filing system only allows Internet Explorer (IE) users to log on the system. This is not security risk but it presents the e-filing application as a non profession system. Browsers like FireFox and Opera should be supported by e-filing system as well. Priority: Medium

**Recommendation 5.10.1:** Allow other browsers to use e-filing, not only IE.

### 5.11 Customs error pages and debug mode

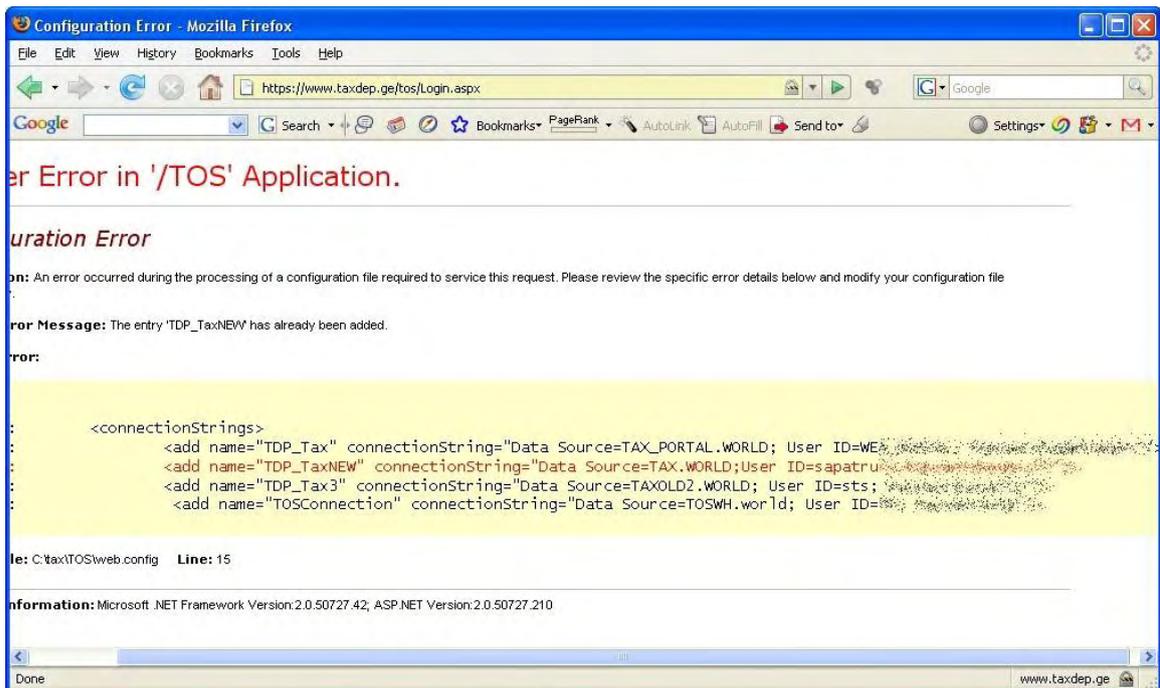
The current e-filing system only uses a default error page. The problem with default pages is that occasionally they show more information then recommended. There should be custom 500 server error pages that only states limited information. Priority: High

**Recommendation 5.11.1:** Create custom 500 Server error page



During audit of the e-file system, it was noted that debug mode on the server was set to show some information. At one stage, the debug mode was fully turned on, mostly likely by mistake. This was probably done during the software testing process and then forgotten. Priority: High

**Recommendation 5.11.1:** Disable all debug modes, use test server for testing (see 5.12)



### 5.12 Secondary server, test server

At this moment the main production server is also used for testing and development. This is not recommended as there should be an additional non-public server which should be used for testing and development. This server needs to be an exact copy of the public production server. This test environment should be used by ITs to test new modules of the e-file system without endangering the production server. Priority: Medium

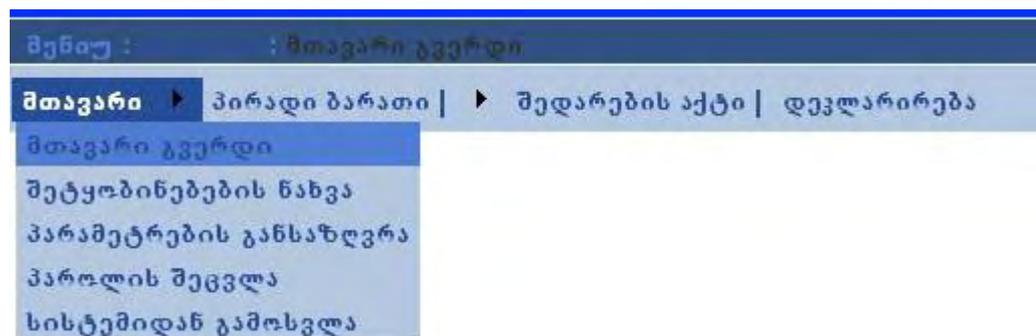
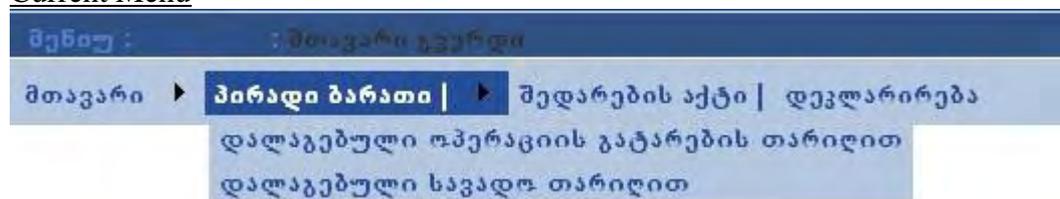
**Recommendation 5.12.1:** Setup non public test server for e-services

### 5.13 E-file menu reorganization

This in itself is not a security issues but should be considered very important for success of the E-filing system. Currently menus are bit overcomplicated and can discourage users from using the system. They should be organized in a more intuitive order. Priority: Medium

**Recommendation 5.13.1:** Restructure the page and menus.

#### Current Menu



#### New Menu structure

Root menu	Sub Menu
Main Page (Home)	-- jump to main page (show general info /news)
Tax Declarations	<ul style="list-style-type: none"> <li>• Submit New Declarations</li> <li>• Check Status of Declarations (e-filed)</li> <li>• List past E-File Declarations</li> <li>• Print Declarations (format for printing)</li> </ul>
Balance Sheet	<ul style="list-style-type: none"> <li>• Balance Sheet</li> <li>• List of Payments</li> <li>• List of Submitted declarations</li> <li>• News / updates</li> </ul>

User details	<ul style="list-style-type: none"> <li>• Reset Password</li> <li>• Change user details</li> </ul>
Log Out	-- Exit application

**How it should look to web user**

<b>Main Page (Home)</b>	<b>Tax Declarations</b>	<b>Balance Sheet</b>	<b>User Details</b>	<b>Log Out</b>
-------------------------	-------------------------	----------------------	---------------------	----------------

**Recommendation 5.13.2:** Main log on page should have a section to enter user name/password, remember lost password, register new user.



**ყურადღება!**

**ძველი WEB Portal გადამხდელებისათვის**

ძველ ვებ-პორტალზე შესვლის შემდეგ განხორციელდება თქვენი მომხმარებლის ავტომატური რეგისტრაცია ახალ პორტალზე ანუ

**1.** შევდივართ ძველ ვებ-პორტალზე (ვუთითებთ მომხმარებლის სახელს, პაროლს და ვაჭერთ ღილაკს „შესვლა“)

• პაროლის აღდგენა

**5. Conclusion**

The list of recommendations has been provided above; recommendations have been marked based on a priority scale. It is highly recommended that all recommendations are followed and addressed. These recommendations will help establish a stable infrastructure that will be used as a backbone for future e-government services.