Quality Assured

File Ref: north24parganas.gov.in-L2-31st August2010-AKSITServices-ver2.0.doc

Site Name:
North 24 Parganas.

Site URL:
http://north24parganas.gov.in

Test URL:
http://tempweb512.nic.in/

AKS Information Technology Services Pvt Ltd
E-52, Sector-3, NOIDA- 201301, INDIA
Telefax: + 91 120 4243669
Mobile: +91 9811943669

Web Site: www.aksitservices.co.in

Document Control

S.No.	Ver No.	Start Date	End Date	Prepared by	Approved by	Comments
1	2.0	27th August 2010	31st August 2010	Manikant Upadhyay (AKS IT Services)	Ashish Saxena (AKS IT Services)	Level2 Testing

Auditor: Manikant Upadhyay

Sign Off:

Contributions

S.No	Name	Role	Organization
1	Ms. Snigdha Acharya	Coordinator and Point of Contact	NIC
2	Mr. Manikant Upadhyay	Auditor	AKS IT SERVICES
3	Mr. Ashish Saxena	M.D	AKS IT SERVICES

Executive Summary

This report documents the findings of the web application security audit level-2 for the website "**http://tempweb512.nic.in/**". The objective of the test was to find out vulnerabilities that can be seen and compromised by malicious users. There is no business risk associated with the web application.

Summary of Findings

Table of Findings

Findings and Vulnerabilities description is tabulated below:

Finding No.	Vulnerability Description	Level I	Level II
1.	The application is vulnerable to session fixation	Open	Fixed
2.	The application is vulnerable to Insecure Communication	Open	Fixed
3.	The application is lacking in Account Lockout Policy	Open	Fixed
4.	The application does not generate audit trail or report for admin user & other user	Open	Fixed

The OWASP Top 12 for the website http://tempweb512.nic.in/

#	Vulnerabilities	Status (Safe/ Unsafe/NA)
1	Cross-Site Scripting (XSS) Flaws	Safe
2	Injection Flaws	Safe
3	Malicious File Execution	Safe
4	Insecure Direct Object Reference	Safe
5	CSRF	Safe
6	Information Leakage and Improper Error Handling	Safe
7	Broken Authentication and Session Management	Safe
8	Insecure Cryptographic Storage	Safe
9	Insecure Communications	Safe
10	Failure to Restrict URL access	Safe
11	Buffer Overflows	Safe
12	Denial of Service	Safe

STANDARD

Open Web Application Security Project (OWASP) standard was used for conduct of web application security audit of the application at **"http://tempweb512.nic.in/".** The OWASP Top Twelve represents a broad consensus about what are the most critical application security flaws. The following table summarizes the OWASP Top Twelve Most Critical Application Security Vulnerabilities:

A1	**Cross Site Scripting (XSS)**	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
A2	**Injection Flaws**	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3	**Malicious File Execution**	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.

A4	**Insecure Direct Object Reference**	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5	**Cross Site Request Forgery**	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6	**Information Leakage and Improper Error Handling**	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7	**Broken Authentication and Session Management**	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8	**Insecure Cryptographic Storage**	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9	**Insecure Communications**	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10	**Failure to Restrict URL Access**	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.
A11	**Buffer Overflows**	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
A12	**Denial of Service**	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

Site Structure

Contents of this section deleted for security reason.

Conclusion

1. Site may be considered safe for hosting with read permission:

Yes

2. SSl Deployment is suggested for further enhancing security on the following folder

   "http://tempweb512.nic.in/admin/"

   Authentication mechanism is being used in the given website at the following URL

   "http://tempweb512.nic.in/admin/secure/login.php"

3. Site needs to be audited for Application Vulnerability:

No