AKS IT SERVICES

Web Application Security Audit Report

Of

National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers

Testing URL
(https://katiyarprint.con/nppa/en)

March 2019
Version: 2.0

AKS Information Technology Services Pvt. Ltd
E-52, Sector-3, NOIDA- 201301, INDIA
Telephone: + 91 120 4545911
Fax: + 91 120 4243669
Website: www.aksitservices.co.in

Disclaimer

AKS IT Services shall assume no liability for any changes, omissions, or errors in this document. All the recommendations are provided on as is basis and are void of any warranty expressed or implied. AKS IT Services shall not liable for any damages financial or otherwise arising out of use/misuse of this report by any current employee of Akal information Systems or any member of general public.

Document Reference

Item	Description
Document Title:	Web Application Security Audit Report of National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers
Department:	Application Audit
Reference File:	Web_Application_Security_Audit_Report_v1.0_21.02.2019_ National Pharmaceutical Pricing Authority.pdf
Publish Date:	5th March 2019
Revision Date:	Nil

Author(s)			
Auditor			
Name	***Designation***	***Start Date***	***End Date***
Mr. Harish Vanjari	InfoSec Consultant	19th February 2019	5th March 2019
Prepared By			
Name	***Designation***	***End Date***	
Mr. Harish Vanjari	InfoSec Consultant	5th March 2019	
Reviewed by			
Name	***Designation***	***Date of Review***	
Mr. Yogendra Singh	Assistant Manager-Application Security	5th March 2019	
Approved by			
Name	***Designation***	***Date of Approval***	
Mr. Ashish Kumar Saxena	Managing Director	5th March 2019	

AKS IT SERVICES

Table of Contents

1. Executive Summary

As part of Web Application Testing proposal, AKS IT's security consultants conducted the Web Application Vulnerability Assessment of National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers to ensure that the deployment is free from any vulnerabilities and that the deployment adheres to the organization's security policies and procedures.

This was Level-2 testing and we found previously reported vulnerabilities were patched.

The key objective of this Web Application Testing was to identify whether any vulnerability exist in the Web Application and to exploit those that can be seen and compromised by malicious users. The objective of this testing was to ensure the security of the network and web server from external threats through the web application.

2. Scope

The scope of the assessment was limited to performing an Application Testing on the URL mentioned below:

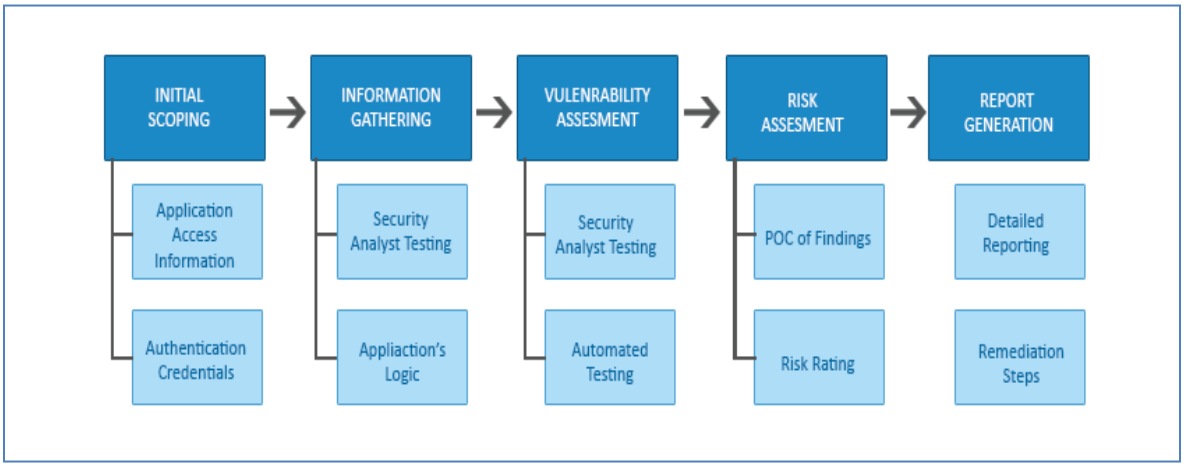
S. No.	Application Name	Application URL
1	National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers	https://katiyarprint.con/nppa/en

3. Methodology

Security Consultants at AKS IT Services used a combination of open source and commercial tools for conducting Vulnerability Assessment of the application.

A Vulnerability Assessment is a method of evaluating the security of an application by simulating an attack. The process involves an active analysis of the application for any weaknesses, functional flaws and vulnerabilities. Any security issues that are identified will be explained with an assessment of their impact, with a solution for their mitigation.

The OWASP Web Application Methodology is based on the 'black box' approach. The testing model consists of following phases:



4. Standard

Open Web Application Security Project (OWASP) standard was used for conduct of level II Web Application Vulnerability Assessment of National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers**.** The OWASP Top Ten represents a broad consensus about what are the most critical application security flaws. The following table summarizes the OWASP Top Ten Most Critical Application Security Vulnerabilities:

S. No.	Vulnerability & Description	Impact
A1	**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.	Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.
A2	**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.	Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.
A3	**Sensitive Date Exposure** 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.	For all sensitive data deserving encryption, do all of the following, at a minimum: 1. Ensure all sensitive data should be kept encrypted/hashed with a strong encryption/hashing algorithm within the database. 2. Ensure all keys and passwords are protected from unauthorized access.
A4	**XML External Entities (XXE)** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks. The business impact depends on the protection needs of all affected application and data.
A5	**Broke Access Control** Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized	The technical impact is attackers acting as users or administrators, or users using privileged functions, or

	users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly. Also, 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.	creating, accessing, updating or deleting every record. The business impact depends on the protection needs of the application and data.
A6	**Security Mis-Configuration** Security mis-configuration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code. Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.	Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.
A7	**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.	Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.
A8	**Insecure Deserialization** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.	The impact of deserialization flaws cannot be overstated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible. The business impact depends on the protection needs of the application and data.
A9	**Using Known Vulnerable Components** Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.	The full range of weaknesses is possible, including injection, broken access control, XSS, etc. The impact could be minimal, up to complete host takeover and data compromise.
A10	**Insufficient Logging and Monitoring** It is coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.	Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%.

5. Summary

5.1 Overall Summary of Findings

The table below provides summary of the vulnerabilities that were identified during the assessment.

Total Findings	High	Medium	Low
0	0	0	0

Table 1: Category Listing

The chart below, gives the overall summary of number of vulnerabilities discovered with their Risk Ratings. We Found zero (0) Vulnerability in final level of audit.

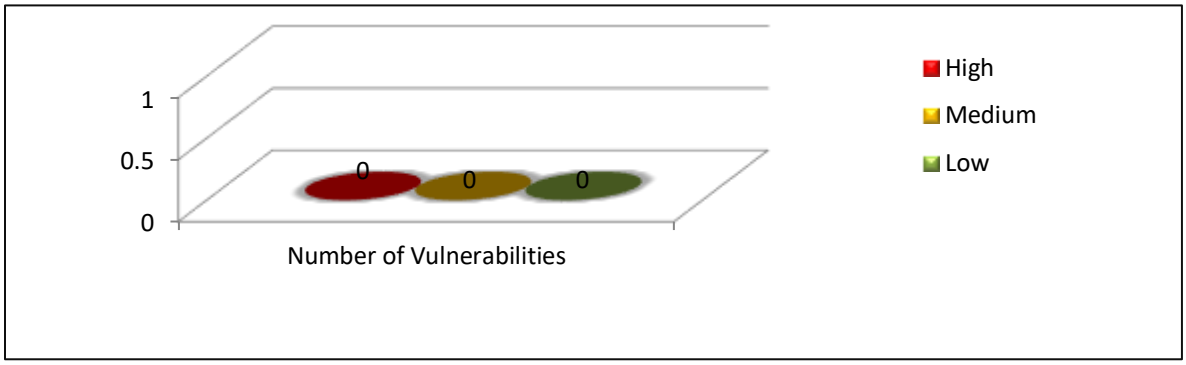


Figure 1: Vulnerabilities Summary

5.2 Key Findings

S. No.	Vulnerability Description	Level-I	Level-II
1.	HTML Injection	Open	**Closed**
2.	Broken Authentication	Open	**Closed**
3.	Sensitive Data Exposure	Open	**Closed**
4.	Broken Access Control	Open	**Closed**
5.	Security Misconfiguration	Open	**Closed**
6.	Using Known Vulnerable Components	Open	**Closed**
7.	Cross Site Request Forgery (CSRF)	Open	**Closed**
8.	Auto Fill Feature Enabled	Open	**Closed**
9.	HTTP Parameter Pollution	Open	**Closed**
10.	User Enumeration	Open	**Closed**
11.	Insecure Cookie Transmission	Open	**Closed**
12.	HSTS Header not Configured	Open	**Closed**

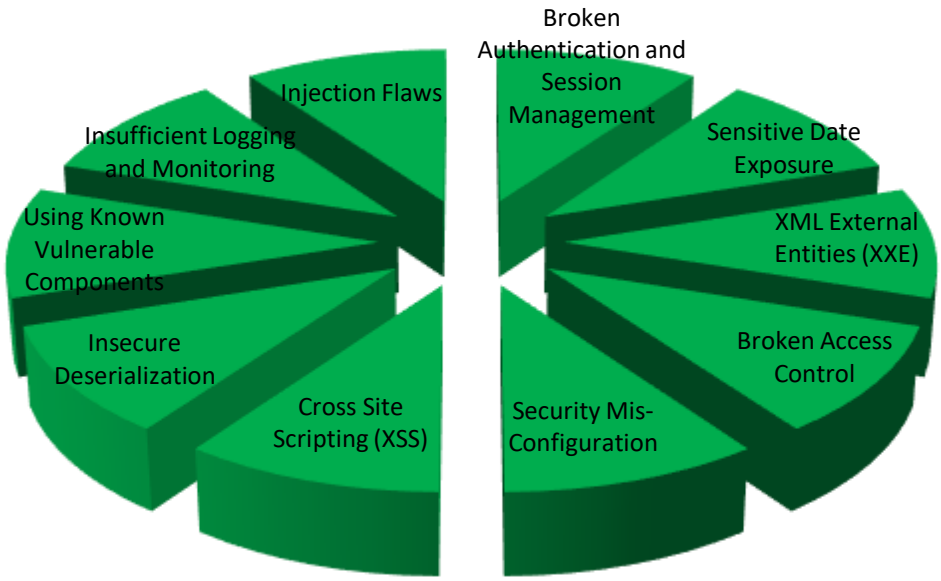
6. Application Security Observations based on OWASP Top 10

Status of Vulnerabilities

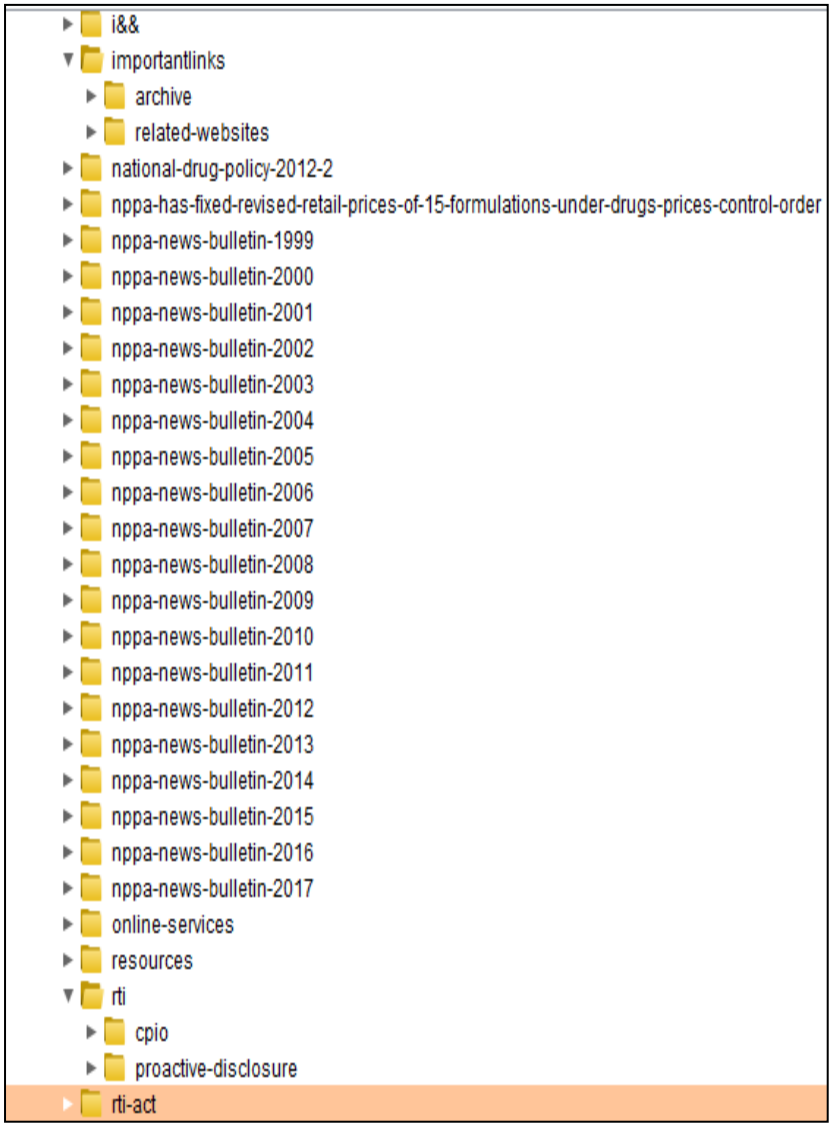
National Pharmaceutical Pricing Authority, Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers

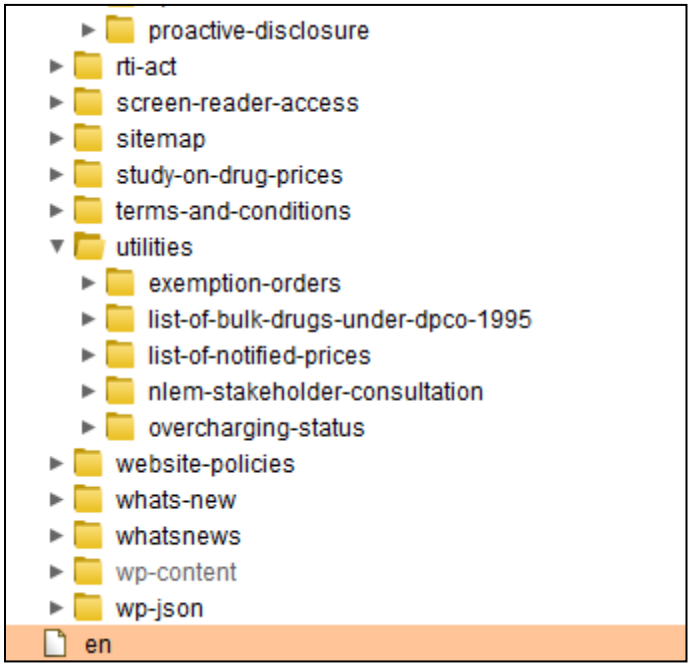
05/3/19

Red:Unsafe Green:Safe Orange: NA



7. Site Structure


i&&
importantlinks
archive
related-websites
national-drug-policy-2012-2
nppa-has-fixed-revised-retail-prices-of-15-formulations-under-drugs-prices-control-order
nppa-news-bulletin-1999
nppa-news-bulletin-2000
nppa-news-bulletin-2001
nppa-news-bulletin-2002
nppa-news-bulletin-2003
nppa-news-bulletin-2004
nppa-news-bulletin-2005
nppa-news-bulletin-2006
nppa-news-bulletin-2007
nppa-news-bulletin-2008
nppa-news-bulletin-2009
nppa-news-bulletin-2010
nppa-news-bulletin-2011
nppa-news-bulletin-2012
nppa-news-bulletin-2013
nppa-news-bulletin-2014
nppa-news-bulletin-2015
nppa-news-bulletin-2016
nppa-news-bulletin-2017
online-services
resources
rti
cpio
proactive-disclosure
rti-act


proactive-disclosure
rti-act
screen-reader-access
sitemap
study-on-drug-prices
terms-and-conditions
utilities
exemption-orders
list-of-bulk-drugs-under-dpco-1995
list-of-notified-prices
nlem-stakeholder-consultation
overcharging-status
website-policies
whats-new
whatsnews
wp-content
wp-json
en

Authenticated Link

- **http://katiyarprint.com/nppa/en/C0npane1/**

Tool Used

I. Burp Suite

II. Acunetix

Technical Risk

- In Production, any Framework running with older version should be upgraded with latest version, plug-in and add-on's.
- HTTP Parameter Pollution will be patch on the Production as per client justification mail
- Google Captcha is to be implemented on production

Conclusion

1. Web application may be considered safe for hosting with Read Only permission:

Yes

2. SSL Deployment is suggested on production server for further enhancing security.

3. Write permission should be granted only on the folder where the files are to be uploaded given at the following URL:

http://nppaindia.nic.in/wp-content/uploads/

4. Application needs to be audited for Application Vulnerability:

No

(Ashish Kumar Saxena)
Managing Director