CSE 3501

INFORMATION SECURITY ANALYSIS & AUDIT

Lab Assessment – 6

L9+L10 | PLBG04
Dr. Vimala Devi K

FALL SEMESTER 2021-22

by

SHARADINDU ADHIKARI

19BCE2105

sharadindu.adhikari2019@vitstudent.ac.in

November 23, 2021

SECURITY AUDIT REPORT OF PENETRATION TESTING

Prepared by

SHARADINDU ADHIKARI
Based on Use Case 9
ING Bank, Ukraine
For ISAA, Fall 2021

INTERNAL DOC
HIGHLY CLASSIFIED

Index

1. INTRODUCTION

A penetration test, also known as a pen test, is a simulated cyber attack against an organization's computer systems to check for exploitable vulnerabilities and determine whether unauthorized access or other malicious activity is possible. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF). A security vulnerability assessment identifies and reports them.

1.1. Background

A number of high-profile data security breaches have been recently reported within the media and have focused Government organisations on the need to have strong processes in place to protect their data which may be confidential or sensitive. These events, along with a number of reports into Government data handling and transit, have raised awareness and highlighted the need for organisations to review their existing information security arrangements to help ensure that robust security policies and practices are in place.

Furthermore, recent changes in legislation of Netherlands have enabled the Information Commissioner to issue strong warnings over the consequences of data losses including the ability to impose substantial penalties over any breach or loss. As a result, the Public Sector have identified the requirement for organisations to have strong Information Governance and Information Security controls in place to protect data held by the organisation and to assist in the compliance with the Data Protection Act 1998.

As a result of a recent cyber attack at the ING Group, Netherlands, the Council requested internal audit to undertake audit work for its Ukrainian Banking Division as well. ING Bank Ukraine is a full subsidiary of ING, a leading global financial institution with a strong European base. Its more than 63,000 employees offer retail and commercial banking services to over 32 million private, corporate and institutional clients in over 40 countries.

In preparing the audit plan, I have reviewed security policy, guidance and practices with an emphasis on access to and protection of electronic information and related practices, measures and tools.

1.2. Purpose

To conduct a comprehensive Information Systems and Security Audit of ING Bank's IT infrastructure and Communication Technology (ICT) including IT Governance. Bank seeks to have an external examination of the IT security.

- To ward off risks in the IT Domain and to appraise the findings thereof to the Management.
- To determine the effectiveness of planning and oversight of IT Activities.
- Evaluating adequacy of operating processes and internal controls.
- Determine adequacy of enterprise-wide compliance efforts relating to IT Policies and Internal Control Procedures.
- Identifying areas with deficient Internal Controls recommend corrective action to address deficiencies.

1.3. Objective

1.3.1. Application Black Box Penetration Testing.

Black box testing of the application includes, identifying and collecting all the possible application security vulnerabilities, from the front end of the application. This type of testing is suitable for all internal and business applications.

1.4. Testing Methodology

1. **Information Gathering**
    - Looking for information on publicly available resources
    - Inserting technical information provided by the organization
    - Non-intrusive scan to determine systems, servers and services
2. **Planning and Analysis**
    - Analysing the possible risks and vulnerabilities
    - Planning for a High Level Intense Penetration Test
    - Designing the overall testing approach
3. **Vulnerability Detection and Identification**
    - Searching for vulnerabilities on the resources
    - Enumerating known flaws, loopholes and mis-configurations
    - Manually probing the target, looking for vulnerabilities
4. **Attack or Active Penetration**
    - Customizing and using readymade exploits for a few known vulnerabilities
    - Building exploits for uncommon specific security loophole
    - Testing the exploits against vulnerabilities
    - Escalating the privileges to exploit higher roles, systems and services
5. **Reporting**
    - Executive Report for Top Management
    - Comprehensive Technical Report for Technical Personnel with solutions

1.5. Report and Compliance

The penetration testing report includes the following sections:

- Overall High-Level Summary and Recommendations (non-technical).
- Methodology walkthrough and detailed outline of steps taken.
- Each finding with included screenshots, walkthrough, sample code, etc.
- Any additional items that were not included.

This report can be used to support the regulatory and compliance requirements of:

- CERT-IN
- ISO 27001 ISMS
- PCI-DSS
- HIPAA
- GLBA

2. EXECUTIVE SUMMARY

A comprehensive security assessment of ING Bank has been conducted in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use. This assessment harnessed penetration testing and social engineering techniques to provide ING Bank's IT Management with an understanding of the risks and security posture of their corporate environment. The purpose was to point out security loopholes, business logic errors, and missing best security practices. The tests were carried out assuming the identity of an attacker or a malicious user but no harm was made to the functionality or working of the application/network.

2.1. Scope of Testing

The test scope for this engagement included three hosts on the bank's internal network, a business-critical web application, as well as an internally-developed mobile application.

In addition, The ING Group requested a wireless audit be performed against their bank's Wi-Fi infrastructure, to discover any insecure wireless protocols, unsecured networks, or related security issues. A social engineering assessment was also requested, to judge the responsiveness of company staff when facing a phishing attack.

Testing was performed from November 16 through November 21, 2021. Additional two days were utilized to produce the report. It was done using industry-standard penetration testing tools and frameworks.

2.2. Key findings

I have raised five priority 1 recommendations, fifteen priority 2 recommendations and four priority 3 recommendations, where I believe there is scope for improvement within the control environment. These are summarised below:

1. IT Security
Security of the Council's network as well as its data and information is dependent on appropriate IT security controls being defined and policies being implemented. I looked at various areas of IT security as set out in the scope of the audit and found that, although there are controls and policies in place, these should be enhanced to improve security and provide a greater level of protection. For example, I shall recommend that the network password controls be improved, greater audit logging and monitoring is performed, additional authentication is introduced for remote access, the requirement to perform a laptop asset audit to help ensure that the latest security controls have been employed on all portable PCs, similarly all mobile phones that have an email and data capability should have additional protection such as passwords and encryption enforced when issued as standard. In addition, we have also recommended that only approved Council issued encrypted USB devices be permitted.

2. Information Security and Governance
I've performed audit testing on the Information Security Policies, roles and responsibilities over Information, Data Classification and Asset Ownership. As a result of the audit, I've identified that currently Information Asset Owners have not been identified for Council information, that there is no process in place to identify and classify data according to its sensitivity. I've also identified that there is no formal records management process in place. The audit identified that although a data sharing

protocol is in place, this was created in 2001 and has not been reviewed for some time. In addition, I could not identify who had signed up to the protocol. Although the Council has a number of policies and procedures established for Information Security, these could benefit from consolidation into a single document covering all major areas of IT related security. I shall also recommend that the ownership of this document be formally assigned as the Information and data sharing protocols and agreements in place have not been reviewed for a long time to confirm validity and adequacy and since the departure of the Information Security Officer, there is currently no specific designated Security Officer in post. This role is currently performed by an IT officer who apart from this role and their other IT roles is also designated as the Records and Data Management officer.

3. Site Visits

As a result of the original information security incident, I've also visited three randomly selected sites within the bank. Some of the issues identified include records created on spreadsheets or databases that are not protected, records are retained longer than necessary, and access to files and folders is not restricted.

2.3. General Vulnerabilities' Summary

The table below includes the scope of the tests performed, as well as the overall results of penetration testing these environments.

Total	Critical	High	Medium	Low	Remarks
5	1	2	0	2	Scan 1 -C:0, H:2, M:1, L:0

Environment tested	Testing results
Internal Network	CRITICAL
Wireless Network	LOW
Web Application	HIGH
Mobile Application	HIGH
Social Engineering Exercises	LOW

3. TESTING

3.1. Overview

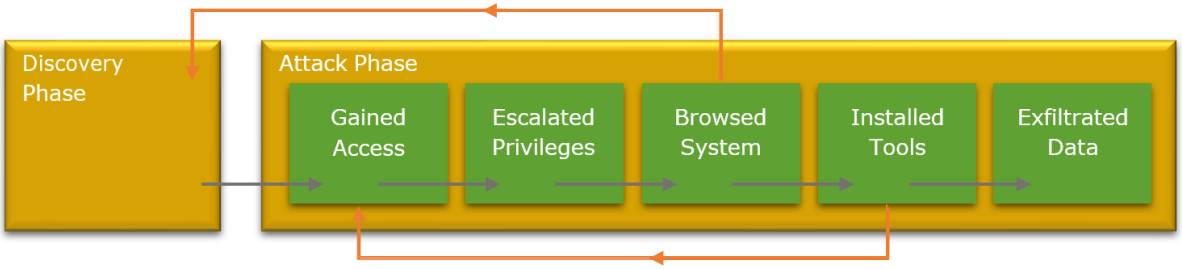
All testing was executed in several related phases.

- In the planning phase, the rules of engagement were identified, scope of testing and test windows were agreed upon, and testing goals were set.
- The discovery phase included automated vulnerability scanning along with manual testing to explore and understand the testing target and any vulnerabilities that could be detected by automated tools.

- The attack phase comprised efforts to exploit any vulnerabilities detected, and to synthesize knowledge gained about the environment, its technology, its users and its function into an escalation of privilege beyond that intended by the customer.
- The final phase recorded all findings in a manner that supports risk assessment and remediation by the customer. This included the writing of this report.

Additionally, the attack phase comprised several distinct steps, executed iteratively as information was discovered.

1. Gained access to the system or environment in a way that was not intended.
2. Escalated privileges to move from regular or anonymous user to a more privileged position.
3. Browsed to explore the newly accessed environment and identify useful assets and data.
4. Deployed tools to attack further from the newly gained vantage point.
5. Exfiltrated data.



3.2. Discovery & Reconnaissance

As the first step of this engagement, I've performed discovery and reconnaissance of the environment. This included performing network or application scans; reviewing the system, network or application architecture; or walking through a typical use case scenario for the environment. The results of discovery and reconnaissance determine vulnerable areas which may be exploited.

3.3. Validation & Exploitation

I've used the results of the reconnaissance efforts as a starting point for manual attempts to compromise the Confidentiality, Integrity and Availability (CIA) of the environment and the data contained therein.

The highest risk vulnerabilities identified were selectively chosen by the assessor for exploitation attempts. I may not have had time to exploit every vulnerability found, the assessor chose those vulnerabilities that provided the best chance to successfully compromise the systems in the time available.

3.4. Test Case' Artifacts

3.4.1 Server Misconfiguration

3.4.1.1. CMS is updated: Failed

CMS is not fully updated

Last checked: 7 hours 29 minutes ago (Check manually)

Drupal core

Drupal core 8.2.5

Recommended version: 8.3.7 (2017-Aug-16)

3.4.1.2. CMS Modules/Plugins/Addons updated: Failed

CMS modules are not fully updated.

ast checked: 7 hours 28 minutes ago (Check manually)

Jpdating modules and themes requires **FTP access** to your server. See the handbook for other update methods.

NAME	INSTALLED VERSION	RECOMMENDED VERSION
Blazy	8.x-1.0-rc1	8.x-1.0-rc2 (Release notes)
Colorbox	8.x-1.2	8.x-1.4 (Release notes)
Chaos tool suite (ctools)	8.x-3.0-beta1	8.x-3.0 (Release notes)
Field Formatter Class	8.x-1.0-rc2	8.x-1.0 (Release notes)
IMCE	8.x-1.4	8.x-1.6 (Release notes)
Libraries API	8.x-3.x-dev	8.x-3.x-dev (Release notes)

3.4.1.3. Server Version Disclosure: Passed

Server does not disclose the web server version information

3.4.1.4. Application Framework Version Disclosure: Passed

Application does not disclose the application framework version information

3.4.1.5. Clickjacking (X-Frame-Options): Passed

Server responds with "X-Frame-Options: SAMEORIGIN" header

3.4.1.6. XSS Protection: Passed

Server responds with "X-XSS-Protection" header

3.4.1.7. MIME Sniffing: Passed

Server responds with "X-Content-Type-Options: nosniff" header

3.4.1.8. Cache Poisoning: Passed

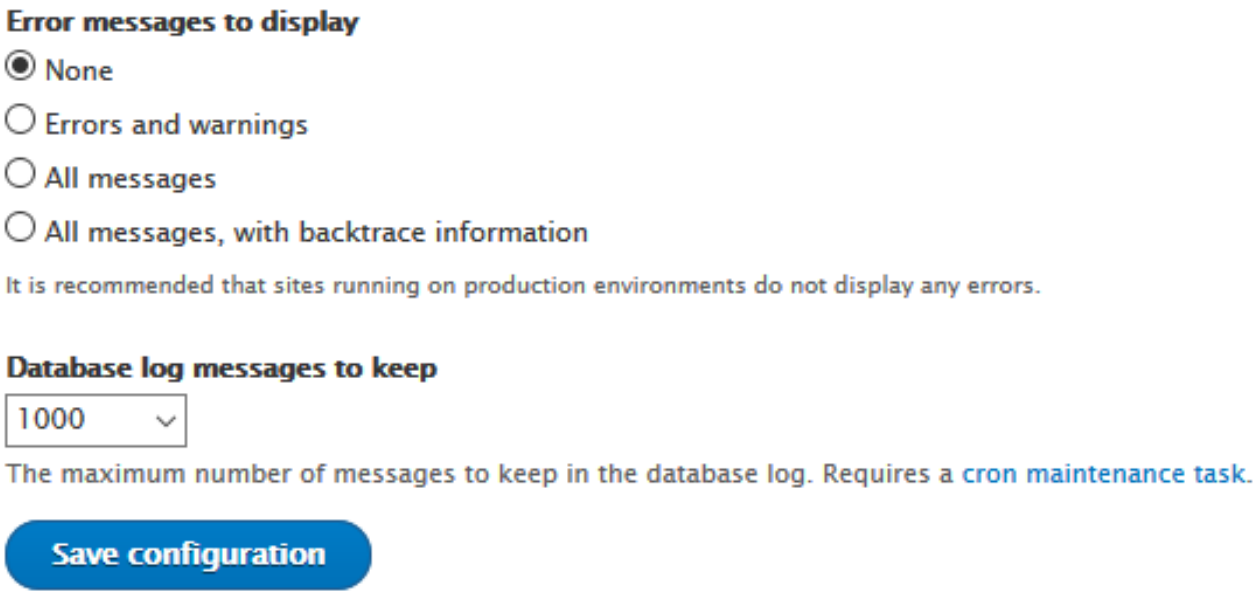
Server does not respond with "Cache-Control" header

3.4.1.9. Cross Origin Resource Sharing: Passed

Application does not allow all origins (*) for resource sharing, as the server does not respond with "Access-Control-Allow-Origin" header

3.4.1.10. Errors and Exceptions: Passed

Generic errors and messages are displayed to users, application does not reveal technical information in errors.



3.4.1.11. Strong Password Policy: Passed

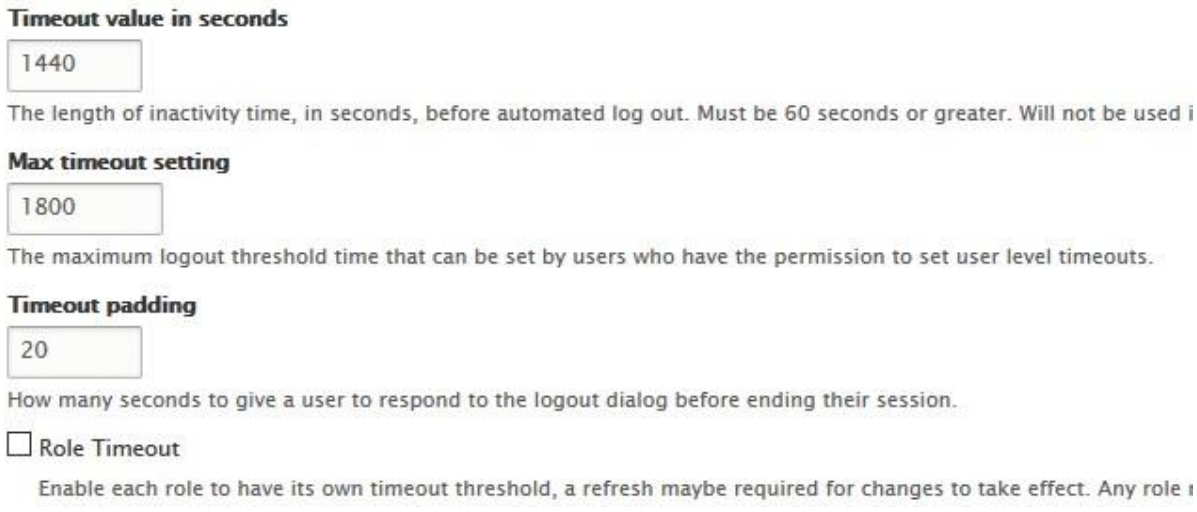
Application has configured strong password policy.

PLUGIN ID	SUMMARY
character_types	Minimum password character types: 4
password_policy_character_constraint	Password must contain 1 uppercase characters
password_policy_character_constraint	Password must contain 1 lowercase characters
password_policy_character_constraint	Password must contain 1 numeric characters
password_policy_character_constraint	Password must contain 1 special characters
password_policy_history_constraint	Number of allowed repeated passwords: 0
password_length	Password character length of at least 8
password_length	Password character length of at most 16
password_username	Password must not contain the user's username.

3.4.2. Session Management

3.4.2.1. Session Expiration: Passed

Application expires the session cookies after a pre-defined timeframe.



3.4.2.2. Concurrent Sessions: Passed

Application does not allow more than 1 active session.

Default maximum number of active sessions

1

The maximum number of active sessions a user can have. 0 implies unlimited sessions.

When the session limit is exceeded

- (•) Ask user which session to end.
- ( ) Automatically drop the oldest sessions.
- ( ) Prevent creating of any new sessions.

3.4.2.3. Cross Site Request Forgery: Passed

Application is able to defend against CSRF attacks.

3.5. Network Penetration Testing Results

Result Classification	
Vulnerabilities Found	Yes
Exploited – Denial of Service (DoS)	No
Exploited – Elevation of Privilege (EoP)	Yes
Exploited – Remote Code Execution (RCE)	Yes
Exploit Persistence Achieved	Yes
Sensitive Data Exfiltrated	Yes
Overall Risk	HIGH

3.6. Penetration Vulnerability Summary Table

#	Vulnerability Summary	Risk Level	Recommendations
1	Sun/Oracle GlassFish Server Authenticated Code Execution	CRITICAL	Ensure that the credentials protecting the Glassfish instance are suitably complex. Secure Admin can also be disabled on the instance to prevent remote access to the DAS.
2	Apache Struts REST Plugin with Dynamic Method Invocation Remote Code	HIGH	Disable Dynamic Method Invocation if possible.
3	Unauthenticated WebDAV Upload	MEDIUM	Require authentication to use the server's WebDAV functionality.

4	DistCC Daemon Command Execution	CRITICAL	Restrict access to the distccd service on UDP port 3632
5	Misconfigured "r" Services Vulnerability	CRITICAL	Disable the "r" services or edit the .rhosts file to prevent remote access
6	Samba "username map script" Command Execution	MEDIUM	Disable the "username map script" option in the smb.conf configuration file
7	Seattle Lab Mail 5.5 POP3 Buffer Overflow	HIGH	Upgrade SLMail or mitigate risk by restricting access to the service.

4. CONCLUSION

The ING Group suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on their banking if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate ING Bank's defenses
- Determining the impact of a security breach on:
  1. Confidentiality of the company's information.
  2. Internal infrastructure and availability of information systems.

These goals of the penetration test were met. A targeted attack against The ING Group can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the information systems. It is important to note that this collapse of the entire ING Group security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels. Appropriate efforts should be undertaken to introduce effective network segmentation, which could help mitigate the effect of cascading security failures throughout the ING Group infrastructure.

5. RECOMMENDATIONS

Employ security measures including two factor authentication (smart card), firewalls, intrusion detection prevention, dynamic monitoring and Virtual Private Network devices (VPN services use specialized hardware to build a private network capability over existing public network lines). VPN devices allow for a secure connection between two IT environments - workstation to server or server to server - by encrypting all traffic (data) over that connection.

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention.

I recommend the following:

5.1. General Recommendations

- Ensure that strong credentials are use everywhere in the organization.
- Establish trust boundaries.
- Implement and enforce implementation of change control across all systems.
- Implement a patch management program
- Conduct regular vulnerability assessments

5.2. IT Security

- Remote Access Controls
- Review of Access to Drives, Directories and Folders
- Laptop Management
- Security of Mobile Phones
- Password Controls
- Formal user administration and leavers process
- Audit Policy Settings and Logging
- Accounts with Non Expiry Passwords
- Use of USBs (Memory Sticks)
- Hardware Disposal Procedures
- Legal Banner

5.3. Information Security and Governance

- Records and Information Management
- Data Sharing Protocols
- IT Policies
- Security Officer Responsibility
- Information Owner and Classification
- Security of Laptops
- Use of Emails – Monitoring

5.4. Observations and Recommendations from Site Visits

- File and Database Protection
- Archiving of Records
- Recycle Bin on PCs
- Data Protection Training
- Confidentiality and Data Protection Statement
- Generic use of Email Account

6. LIMITATIONS

- Security issues that could potentially disrupt the Client environment were not fully tested.

  Security issues that could negatively disrupt and impact normal system operations, including Denial of Service (DoS) or buffer overflow attempts, were not fully tested as part of this assessment.

- Technical testing activities were limited to a finite time period.

  Testing was limited to a finite period of time. Malicious users may be able to discover and attempt additional security issues over a longer period of time or through other methods such as social engineering.

- Social Engineering
  Social Engineering attacks were not in scope for this assessment.

- Client-Side Attacks
  Client-side attacks were not in scope for this assessment.
