Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF COMPUTER STUDIES

FINAL REQUIREMENT IN ITEP 311 INFORMATION ASSURANCE AND SECURITY 1

PART I.

System/Website Security Exhibit Presentation Instructions

Objective

Present your system or website with a focus on its login security features, demonstrating how each aspect aligns with industry best practices. Judges will evaluate your exhibit based on five critical security criteria.

Login Security Checklist

Authentication
[ ] Use HTTPS on all login pages and endpoints
[ ] Enforce strong password policies (min length, complexity, no common passwords)
[ ] Implement Multi-Factor Authentication (MFA) (e.g., TOTP, SMS, hardware token)
[ ] Hash passwords securely using a modern algorithm (e.g., bcrypt, Argon2)
[ ] Use unique salts for each password hash
[ ] Disable password autocomplete on login forms
Brute-Force Protection
[ ] Limit login attempts per IP/user (rate limiting)
[ ] Account lockout after repeated failed attempts
[ ] Use CAPTCHA after several failed login attempts
[ ] Throttle response times for repeated failed logins Session Security
[ ] Use secure, HttpOnly cookies for session management
[ ] Set session timeouts and require re-authentication after inactivity
[ ] Regenerate session IDs after login
[ ] Invalidate sessions after logout or password change
Monitoring & Alerts
[ ] Log all login attempts, both successful and failed
[ ] Send email/SMS alerts for logins from new devices or locations
[ ] Provide user access logs in their account for review
[ ] Monitor for suspicious login patterns (e.g., geolocation anomalies)
Other Best Practices
[ ] Provide "forgot password" with secure reset tokens (expire after use/short time)
[ ] Avoid detailed error messages (e.g., don't reveal whether username or password is wrong)
[ ] Secure authentication APIs against abuse
[ ] Implement account recovery validation (e.g., email confirmation, challenge questions)

- Use a **demo account** for showing live features.
- Prepare **slides or infographics** highlighting each security component.
- Be ready to **answer technical questions** about how each security feature is implemented.

Login Security Evaluation Rubric (Total: 30 Points)

Category	Criteria	Points
1. Authentication	HTTPS is enforced on all login pages- Strong password policy is in place- Passwords are securely hashed with salt	___ / 6
2. Multi-Factor Auth (MFA)	MFA is implemented and required- Supports TOTP, SMS, or hardware token- Users can configure MFA options	___ / 6
3. Brute-force Protection	Login attempt limits or lockouts are in place- CAPTCHA after failed attempts- Throttling is implemented	___ / 6
4. Session Management	Sessions use secure, HttpOnly cookies- Session timeouts & ID regeneration- Sessions invalidated on logout or password change	___ / 6

Category	Criteria	Points
5. Monitoring & Alerts	Logs all login activity- Alerts users of new logins or anomalies- Offers visibility of recent logins	___ / 6

Scoring Guide

- **6 pts**: Fully implemented and well-documented
- **4 pts**: Partially implemented or missing some best practices
- **2 pts**: Minimal implementation or major gaps
- **0 pts**: Not implemented

Part II

IT Department Simulation: Build Your Secure Infrastructure

Objective

Students will take on roles within a simulated IT department to design and explain IT operations workflows, administrative responsibilities, and the importance of security policies in protecting an organization's digital assets.

Instructions:

1. Divide Students into Teams of 4–6. Research and define the following roles:
- IT Operations Engineer
- System Administrator
- Security Analyst
- Policy Manager
- Compliance Officer
- Help Desk Technician

2. Distribute the Scenario:

ex. Your university is launching a new online learning platform. Your IT team must build, operate, and secure this platform. Each team member must contribute based on their role to:
- Set up operations processes (e.g., monitoring, backup, patching)
- Define system administration tasks (e.g., account creation, access controls)
- Identify needed security policies (e.g., password policies, remote access rules)
- Explain how these policies protect users, systems, and data

3. Planning Phase:

Teams will:
- Outline each role's responsibilities
- Create a sample IT operations checklist (e.g., backup schedule, system monitoring)
- Write two critical security policies (e.g., Acceptable Use Policy, Data Retention Policy)
- Explain how their policies reduce risk and support daily operations

4. Presentation Phase (10–15 minutes):

Teams present:
- A brief explanation of their infrastructure setup
- How operations and admin duties are divided
- Their written policies and justifications

Student Worksheet Template:

Team Name:	
Scenario Summary:	
IT Operations Tasks:	
Administration Duties:	
Security Policies:	
Policy Purpose:	
Team Roles & Contributions:	

Lessons Learned:	

Criteria	Description	Points (0–6)
Clarity of Role Definitions	Roles and responsibilities (e.g., developer, security analyst, network admin) are clearly assigned and explained.	____
Realism of IT Operations	System reflects realistic IT workflows, including actual network, access controls, authentication, and incident handling.	____
Relevance of Security Policies	Demonstrates security policies appropriate to the system (e.g., password rules, access control, backup policy).	____
Team Collaboration	Team members contribute meaningfully; smooth coordination during setup and explanation; shared understanding of system goals.	____
Presentation Quality	Clear, engaging presentation; good visuals or demo; confident delivery; answers to judges' questions are well-informed and relevant.	____
	Total	/30