Hello everyone, Let's start a presentation

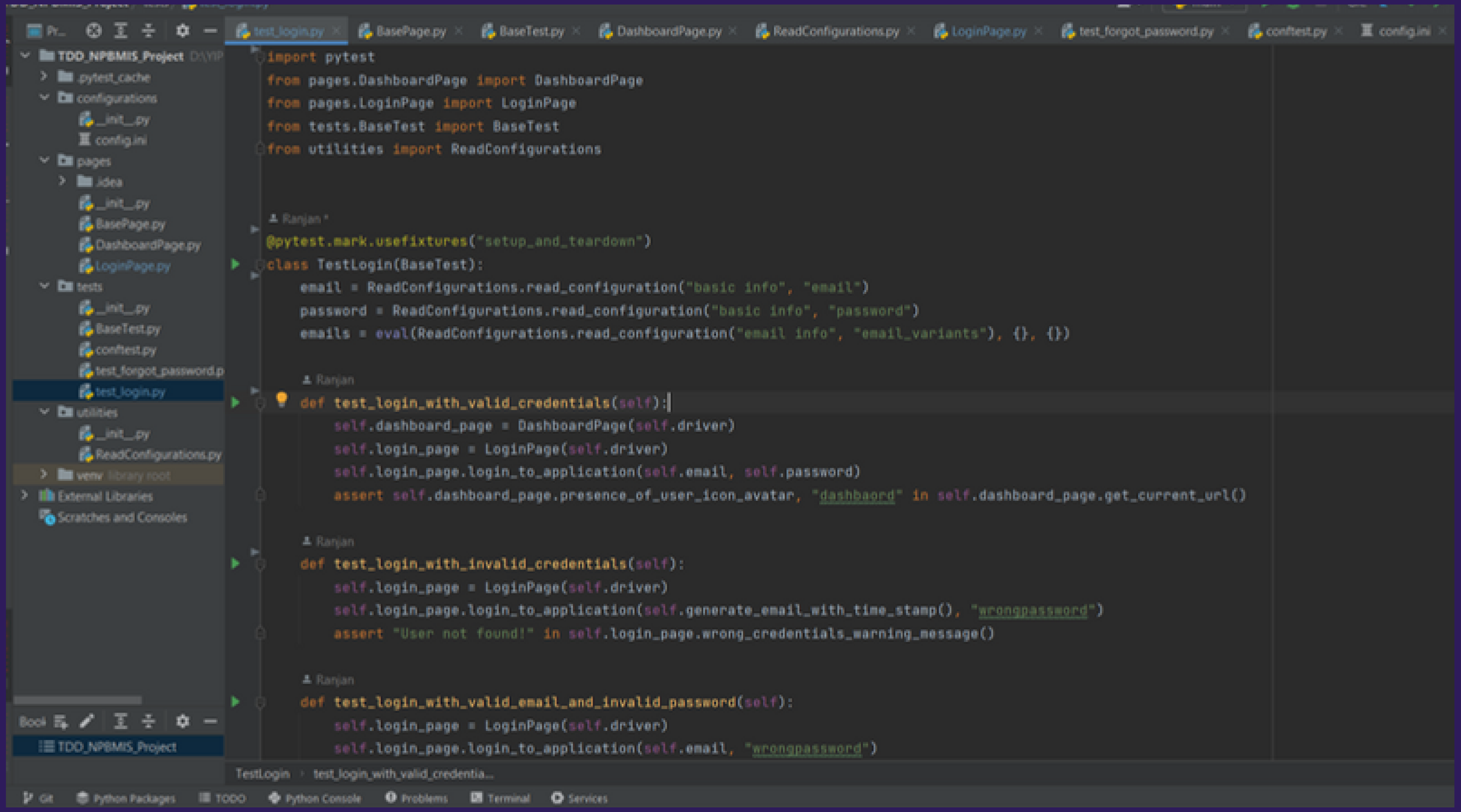
Title: 2nd Month Summary

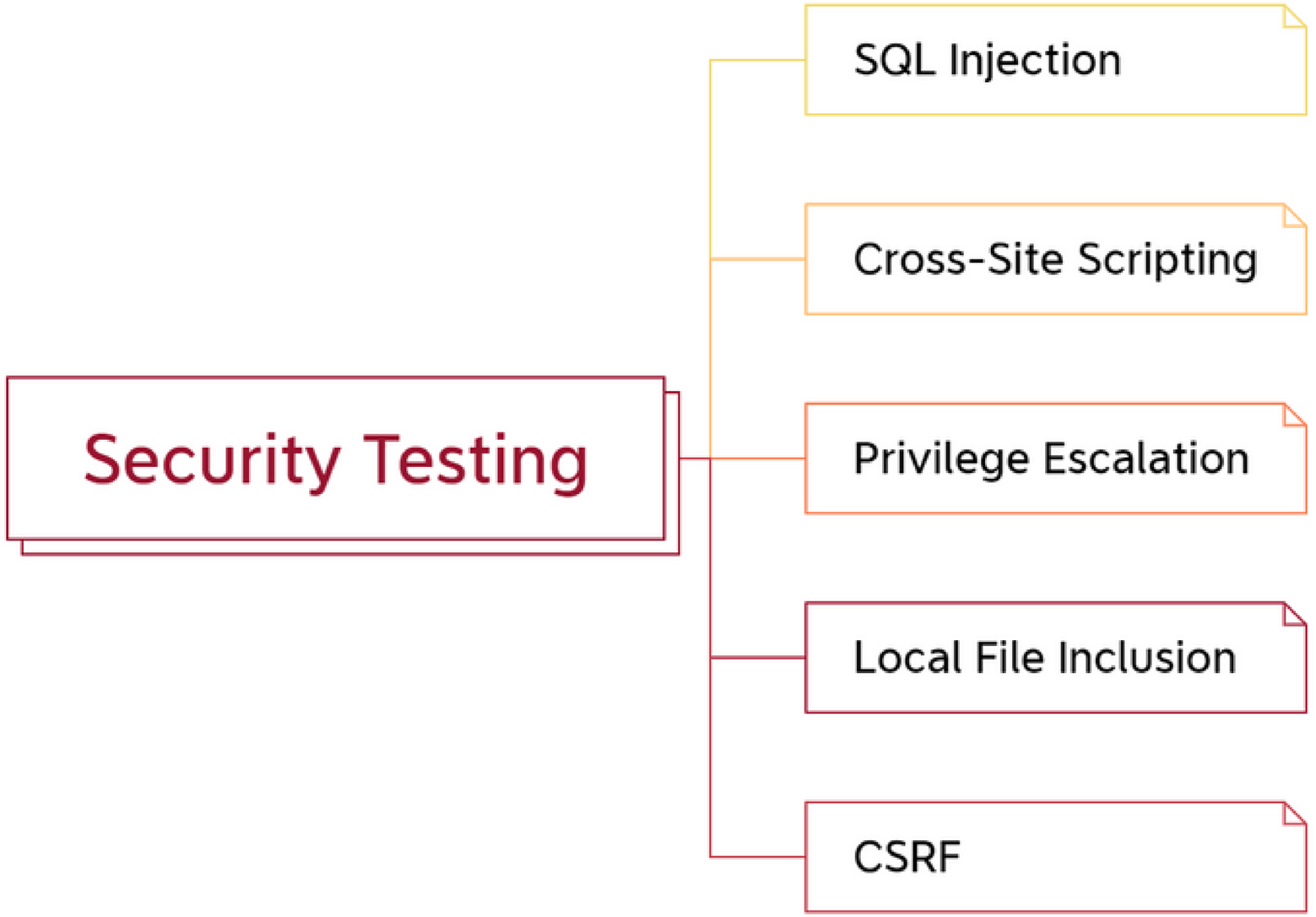
OverView

01.
Automation Testing

02.
Security Testing

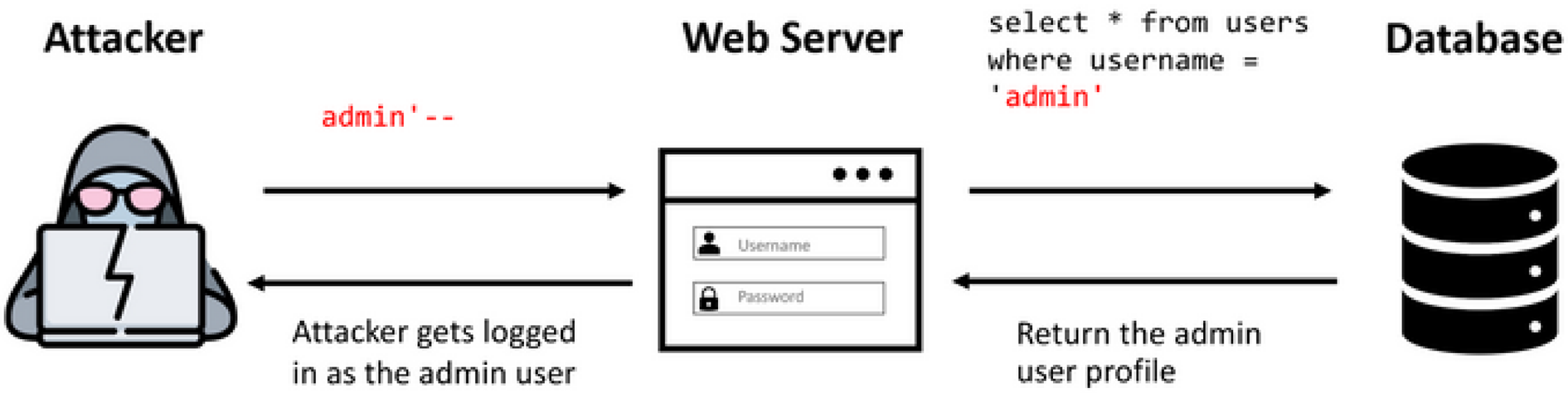
03.
Performance Testing


test_login.py
BasePage.py
BaseTest.py
DashboardPage.py
ReadConfigurations.py
LoginPage.py
test_forgot_password.py
conftest.py
config.ini
TDD_NPBMIS_Project
.pytest_cache
configurations
__init__.py
config.ini
pages
.idea
__init__.py
BasePage.py
DashboardPage.py
LoginPage.py
tests
__init__.py
BaseTest.py
conftest.py
test_forgot_password.p
test_login.py
utilities
__init__.py
ReadConfigurations.py
venv library root
External Libraries
Scratches and Consoles
TDD_NPBMIS_Project
import pytest
from pages.DashboardPage import DashboardPage
from pages.LoginPage import LoginPage
from tests.BaseTest import BaseTest
from utilities import ReadConfigurations
Ranjan *
@pytest.mark.usefixtures("setup_and_teardown")
class TestLogin(BaseTest):
email = ReadConfigurations.read_configuration("basic info", "email")
password = ReadConfigurations.read_configuration("basic info", "password")
emails = eval(ReadConfigurations.read_configuration("email info", "email_variants"), {}, {})
Ranjan
def test_login_with_valid_credentials(self):
self.dashboard_page = DashboardPage(self.driver)
self.login_page = LoginPage(self.driver)
self.login_page.login_to_application(self.email, self.password)
assert self.dashboard_page.presence_of_user_icon_avatar, "dashbaord" in self.dashboard_page.get_current_url()
Ranjan
def test_login_with_invalid_credentials(self):
self.login_page = LoginPage(self.driver)
self.login_page.login_to_application(self.generate_email_with_time_stamp(), "wrongpassword")
assert "User not found!" in self.login_page.wrong_credentials_warning_message()
Ranjan
def test_login_with_valid_email_and_invalid_password(self):
self.login_page = LoginPage(self.driver)
self.login_page.login_to_application(self.email, "wrongpassword")
TestLogin
test_login_with_valid_credentia...
Git
Python Packages
TODO
Python Console
Problems
Terminal
Services


Security Testing
SQL Injection
Cross-Site Scripting
Privilege Escalation
Local File Inclusion
CSRF

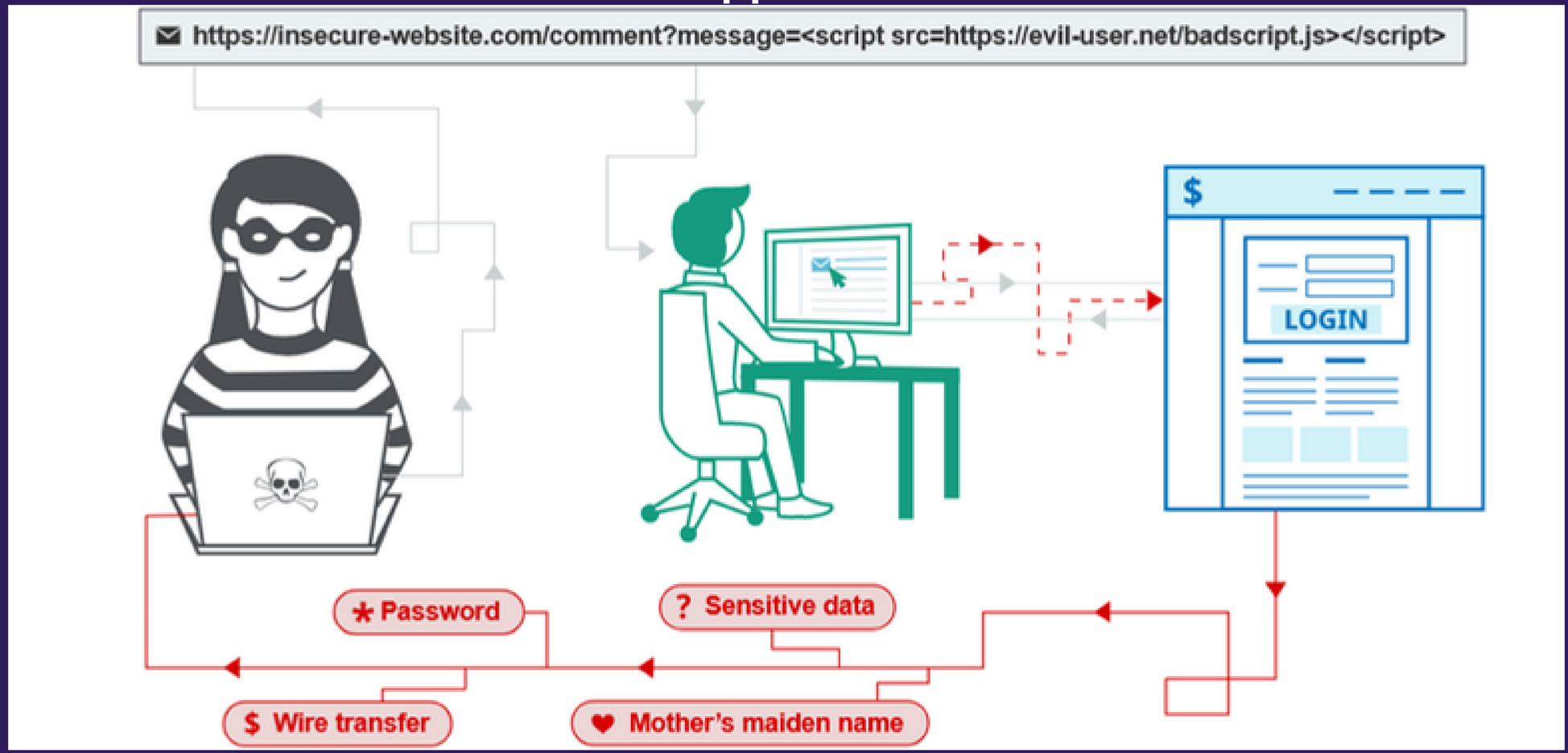
SQL Injection

- Vulnerability that consists of an attacker interfering with the SQL queries that an application makes to a database.

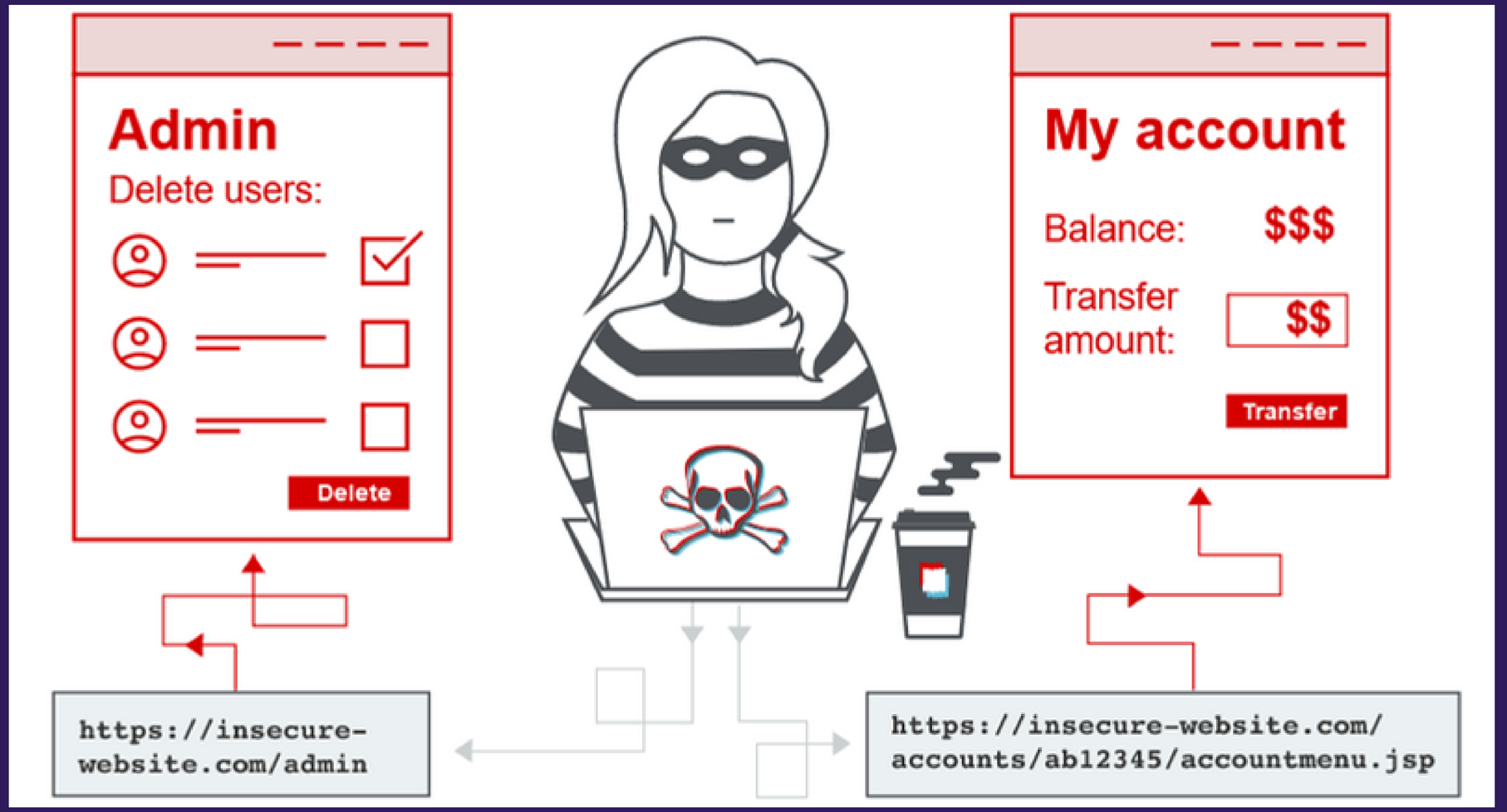


How does XSS work?

- XSS works by manipulating a vulnerable website so that it returns malicious JavaScript to users.
- When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the applicaiton



Broken Access Control




```
https://insecure-website.com/login/home.jsp?admin=true
https://insecure-website.com/login/home.jsp?role=1
```

Directory Traversal

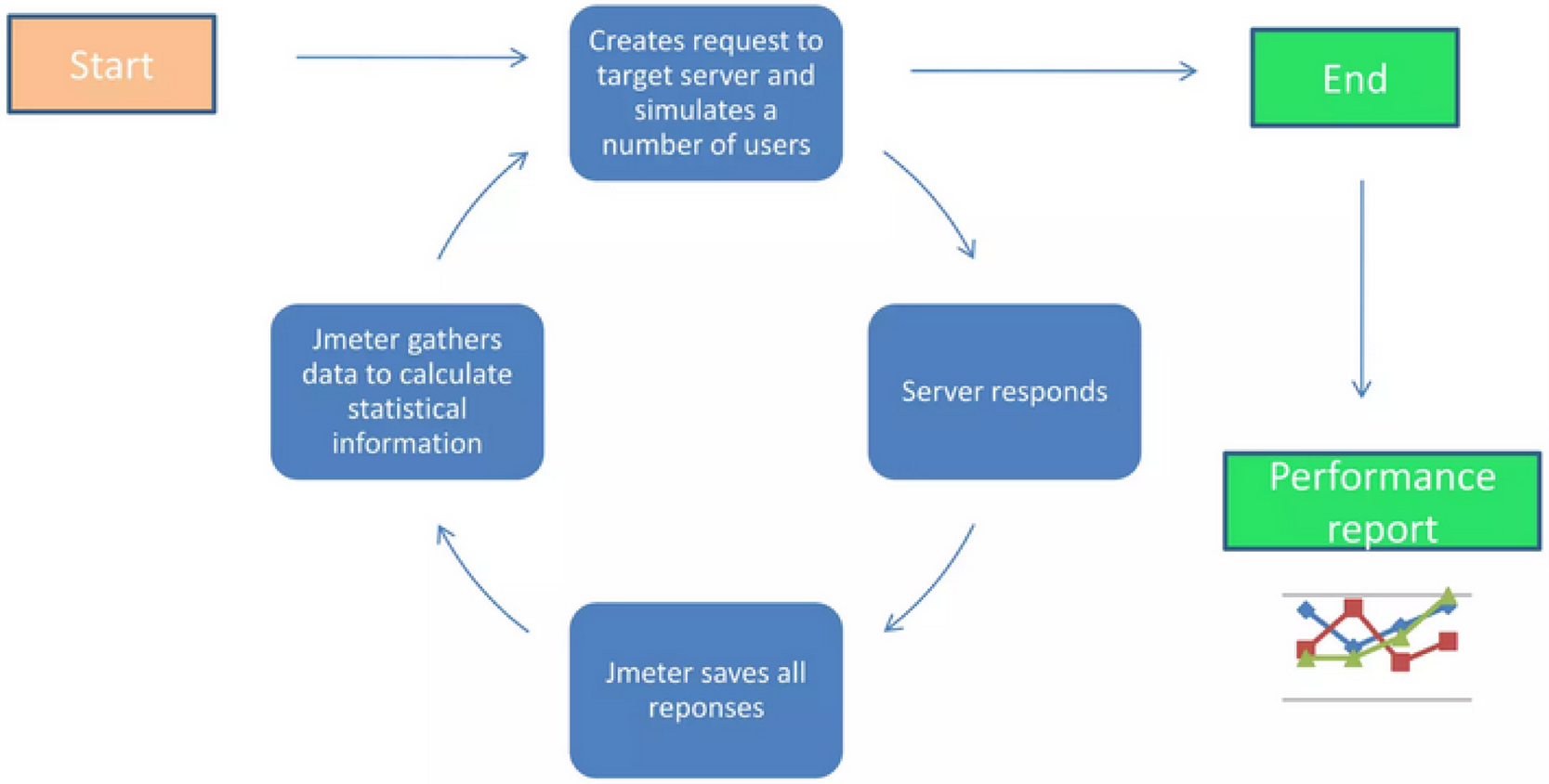
- **It exploits insufficient security validation or sanitization of user-supplied file names, such that characters representing "traverse to parent directory" are passed through to the operating system's file system API.**

Fun Facts!

Since 2011,Facebook Have spend 16 million dollars in bug bounty i.e 2.13 Arba in NRS

How jmeter work

Jmeter simulates a group of users sending requests to a target server , and returns statistics that show the performance of the target server/application through graphical diagrams. This is a basic description of how jmeter works.



Any Questions


Thank
You!