CSE 545 Project Presentation

Secure Banking System

Group 13

Atin Singhal (L)
Sriprashanth
Ayush Ray
Raj Buddhadev
Shivank Tiwari (DL)
Kangjian Ma
Uttam Das
Amitabh Das

Schedule

Part A
Security Requirements

Part B
Vulnerability Discussion

Security Requirements

- Public Key Certificates
- OTP (One-Time Password)
- Allow multiple users to use the system simultaneously
- Available 24x7
- Prevent Malicious Login Controls
- Session Management
- Must defend attacks on SBS
- Data masking & Hashing
- Sign-in History Function
- Hyperledger must capture all valid & approved transactions.

Security Implementations

- PKI is implemented to enforce the security of the application.
- Self signed certificate.
- OTP is implemented for multiple banking functionalities and forgot password function.
- The system is available 24x7 for user access- AWS.
- Preventing malicious logins by locking accounts after multiple incorrect login attempts.
- Session management- Enforcing one session per user & ending the session if it’s inactive for a few minutes.
- Login history is maintained.
- Fast response time (3-4 seconds)
- Hashing & salting is done for sensitive fields in the Database.
- Disabled copy/paste functionality, back buttons and other features to protect the site.
- Valid transactions are captured in Hyperledger.

Vulnerability Discussion

Valid Security Vulnerabilities

#	Issue	Reported by	Fix
1	XSS on login page input field	Karan Ajith, Prasoon Deva, Manjeshwar Ashish Padakannaya, Mojca Stampar	Limit input field by size and sanitize input.

Valid Functional Error

#	Issue	Reported by	Fix
1	Unexpected behaviour like logout or no response for transactions by new users. (Issue with deposit/ view/ transfer/ withdraw/ pay merchant)	Yashaswini Addada, Manav Bagai, Prasson Deva, Saumil Dixit, Yucheng Lu, Vasudev Sridhar, Manjeshwar Ashish Padakannaya, Sagar Parekh, Athul Pramod, Akshay Shah, Ankit Sharma, Yash Vijay, Mojca Stampar, Karthik Radhakrishnan, Nedumarandeepankarthik, Sagar Parekh	This is working fine for sample users we created. Faced some unexpected issues with new users after AWS deployment. Need to assign roles properly for new users created.

Valid Functional Error

#	Issue	Reported by	Fix
2	User is able to deposit same cheque multiple times/ User can deposit any cheque number.	Manjeshwar Ashish Padakannaya, Ankit Sharma, Yash Vijay, nedumarandeepankarthik	Generate cheque id randomly instead of sequential increment and update the same entry in the database when a cheque is deposited instead of creating a new entry.
3	Site shows improper error message/ Doesn't explain password criteria clearly/ Poor feedback/ Username gives error even though only alphabet are used.	Karan Ajith, Yucheng Lu, Sagar Parekh, Ankit Sharma	Fix error message to clearly explain the requirements. There is length requirement for most fields.

Valid Functional Error

#	Issue	Reported by	Fix
4	Unlock account request is not generated for merchant accounts.	Ankit Sharma, Yash Vijay	Add user role “merchant” in the query that picks accounts to be show in the tab.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
1	Some users may not have middle name which is made as compulsory for the registration/ When creating new employee, Address2 and middle name have to be populated, even though some people don’t have those.	Yasaswini Addada, Yucheng Lu, Mojca Stampar	Not a major flaw or a broken functionality. You can fill it with any character/ NA for testing purposes.
2	The users and employees are not able to request modification of their personal details.	Yasaswini Addada, Sagar Parekh	Design choice. You can schedule an appointment and an employee will help you with updation of the details.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
3	Cash requests are not shown in approval page for customers.	Yasaswini Addada	Not clear on what you're trying to say.
4	Multiple sessions can't be active for an account.	Yasaswini Addada	Not sure how this is a vulnerability. It's a design choice to improve security.
5	Session Management Error	Karan Ajith	You can't login as two different users simultaneously in the same browser.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
6	No 2FA for password change	Karan Ajith	Not a mandatory requirement.
7	Cookie Hijacking	Karan Ajith, Yash Vijay	We're enforcing HTTPS and using HTTPOnly for Cookies. Headers are encrypted when transmitting over the network. No evidence provided. Copying cookie/ session id from your own browser isn't classified as cookie hijacking.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
8	System logs show code errors in raw format	Karan Ajith	Logs can only be accessed by the Admin. No fixed log format was defined in the SRS. No exploitation shown.
9	Session continues even if the browser or tab is closed by the user	Prasoon Deva	Session invalidation time has been set to 5 minutes. Once you visit the homepage of bank, other sessions on the system are invalidated.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
10	Newly registered users can’t approve or decline transactions.	Prasoon Deva	The screenshot shown has no account listed under ‘To’ hence transaction can’t be approved or decline.
11	Can unlock an account different from which I clicked	Prasoon Deva	No screenshot or video evidence provided.
12	Server SSL certificate is not trusted	Prasoon Deva	It’s a self signed certificate. The project requirements deem this as valid.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
13	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for *excessive memory consumption* or *CPU usage*. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.	Prasoon Deva	No attacks shown. Can't assume attacks.
14	Open ssh port 22 on the server which is vulnerable to attack from the outside. Attacker can use brute force method to gain access	Prasoon Deva	Protected by Amazon GuardDuty. No attack shown.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
15	Improper Session Termination	Saumil Dixit	We're limiting one session per user from server side. If you try to process a request from the old session that you think is active, you'll find out requests won't be processed & you'll be redirected to login page.
16	Tier 1 or 2 employees can't view appointments of the day/ Unable to view scheduled appointments	Saumil Dixit, Lu Yucheng , Sagar Parekh, Yash Vijay, nedumarandeepankarthik, Manjeshwar Ashish Padakannaya	Appointments are shown only if scheduled for the same day. Also it's assigned to a random employee.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
17	Security Questions insufficient	Alyssa Goldstein	Security questions are old news. We're using OTP for verification where ever necessary.
18	I already register on account use SSN 000-00-0000, then I create another account also use this SSN number. I can register successful. However, one user only have one SSN number.	Yucheng Lu	Not possible. We have set SSN as UNIQUE in Database. No evidence provided.
19	Addresses are accepted even when no alphabets are entered. Takes an input which is entirely numbers./ Accepts 1 digit zip codes as input.	Yucheng Lu, Alyssa Goldstein	Not a requirement according to SRS to validate the address for correctness.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
20	I enter zip code as a 21 digit number (852811739134718371499), it's allowed. However, there is no zip code with so many digits. It may cause Fake user.	Yucheng Lu	The zip code field in DB is set as INT and the max input it can receive is 10 characters, 2147483647 to be precise. No evidence shown.
21	User can login without OTP	Yucheng Lu	Not a mandatory requirement
22	Login history time is incorrect. I login Apr.09, but login history show that 04-10	Yucheng Lu	Server time is logged, not user's local system time.
23	Search account function is not working about employee account.	Yucheng Lu	The field clearly states to enter account number but you are trying to input username.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
24	When the registration is completed, my mobile phone and email will not receive any activation code. This will cause the attacker to write a script for automatic registration. In this way, there will be an equivalent account waiting for the employee to activate, and the speed of the employee identifying and activating the account is much slower than the speed of the script.	Yucheng Lu	Many fields are set as unique for the form to be successfully submitted. No attack shown. Can't assume attacks.
25	One user can open multiple accounts of the same type	Manjeshwar Ashish Padakannaya, Ankit Sharma, Yash Vijay	SRS didn't say that users can't have multiple accounts of same type.
26	Employee creation sometimes errors out.	Manjeshwar Ashish Padakannaya	Unable to reproduce the issue.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
27	Admin can't create an employee/ No option to unlock employee accounts.	Manjeshwar Ashish Padakannaya, Ankit Sharma, Yash Vijay, karthik radhakrishnan neeragunda, nedumarandeepankarthik	All new accounts are locked and should be manually activated. Design choice to prevent misuse.
28	Regex validation failing for high school	Manjeshwar Ashish Padakannaya	It accepts only letters & numbers. ' ' (space) isn't satisfying the condition
29	Always says user present. Does not let me register. But when I go to forgot password it says if user present you will get an email. Never received any email.	Sagar Parekh	'User already exists in the DB' means username/ phone no./ email/ ssn were matching with any other user. Screenshots show same value of SSN for all your FAILED attempts.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
30	No option for new employee sign up.	Sagar Parekh	Employees can only be created by admin.
31	Calculator shows up when otp is asked.	Sagar Parekh, karthik radhakrishnan neeragunda	Design choice for virtual keyboard. Easiest way to restrict input to numbers.
32	For customers, Deposit/ Withdraw money does not wait for approval from the employees. Anyone can process any amount from their bank account like this	Sagar Parekh	This page was just added so you and others could easily add funds to check functionalities.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
33	No option to download logs.	Sagar Parekh	Not mandatory according to requirements. Design choice.
34	The form data (username and password) is visible in the console. / Sending password as plaintext	Athul Pramod, Vasudev Sridhar	Console is visible only to the user. No evidence of exploitation shown. HTTPS is enforced and Headers will be encrypted before transmission. Server-side encryption is done.
35	System crashed when typing random characters in the Amount field in the create, transaction for Tier 1 employees.	Athul Pramod	It's taking you to an error page. Error pages are common to make sure no unwanted information is displayed. Amount expects digits, not alphabets.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
36	The system is not imposing any limits on the number of wrong OTP attempts.	Athul Pramod, Akshay Shah, nedumarandeepankarthik	The OTP has a high entropy so it's not easy to guess. Also it's set to expire within a few minutes so brute-force is unlikely.
37	I am able to make an appointment for any day and the system does not show the availability of the employe while making the appointment. Also the system allows appointments during sundays thus not considering the availability of the employees.	Athul Pramod	Not a mandatory requirement. Each bank policy is different. Maybe employees can attend to customers over 'Zoom' in our case.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
38	Change Password: Can change the password for the user to the password previously used	Akshay Shah	Not a mandatory requirement. No exploitation shown.
39	No way to change the role of an employee.	Ankit Sharma, Yash Vijay	Couldn't find any such requirement. Admin can change the roles.
40	No user name or id is provided to tier 2 employees for unlocking locked accounts. / New Account Approval does not show employee details, hence just by account number you cannot know whose account is being unlocked.	Ankit Sharma, Yash Vijay	It's just the design followed to respect privacy of the user. No such requirement according to the SRS.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
41	Able to view the account number even before approval in Cashiers check page/ Unapproved accounts can be used for ordering cheques/ Accounts being reflected even when not approved	Ankit Sharma , Yash Vijay, nedumarandeepankarthik	The evidence just shows a list of accounts. No exploitation is shown. As accounts are not approved, it'll throw an error.
42	No schedule Appointment functionality available for Customer	Vasudev Sridhar	It's in the Service Requests link.
43	Not able to create account for customer. Account creation requires OTP. In order to receive OTP, email ID must be update.	Vasudev Sridhar	We don't require OTP for account creation.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
44	Transfer Funds Not Working - 2: When I transfer funds externally, the amount is not getting removed from account.	Yash Vijay	The screenshots show ‘to’ and ‘from’ account as same.
45	Not all provided users actually work.	Mojca Stampar	All credentials were tested before sharing Someone might’ve have changed them.
46	Every time you go back to main page from user account it logs you out	Mojca Stampar	That’s a good thing, you navigate away, it logs you out.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
47	Debit and credit for more than $1000 not asking for approval	karthik radhakrishnan neeragunda	No evidence shown. Unable to recreate issue.
48	Able to send money to individual when clicked on Merchant pay i.e account not validated as merchant or individual	nedumarandeepankarthik	No evidence provided.
49	Number of attempts is 5 but on the approval page it shows 4	nedumarandeepankarthik	No evidence provided.
50	Expects authorization for paying merchant(self authorization?)	nedumarandeepankarthik	No evidence shown. Also, not clear.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
51	On existing customer accounts, debit/credit doesn't get updated in transaction records	nedumarandeepankarthik	No evidence provided
52	DOB is accepting dates from future.	Yasaswini Addada, Alyssa Goldstein	No evidence shown. Unable to replicate.
53	Does not accept phone number in the specified format. [The phone number in screenshot is +1(129)-764-8376]	Alyssa Goldstein	The phone number you're trying is invalid. There's no US state area code that starts with 1xx.

Invalid Vulnerabilities

#	Issue	Reported by	Comment
54	An employee can use the portal even after an admin deletes the record.	Manjeshwar Ashish Padakannaya	Deleted employee can't change data, just has access to the dashboard that too until he logs out once (if he was logged in when he was deleted). After that he won't even be able to login.
55	Not able to update details of a customer/ employee. Username field is disabled.	Vasudev Sridhar	Username field is disabled for safety so users can’t change it. Unable to recreate the issue.

Summary

Valid Security Vulnerabilities: 1

Valid Functional Errors: 4

Invalid Vulnerabilities: 55

We tried our best to accommodate all the vulnerabilities reported. Just in case your issue isn't mentioned, let us know...

Thanks!