Looting Your Bank Savings

Using Digital India

Indrajeet Bhuyan

Dedicated to my parents

“*My parents gave me the courage and freedom to follow my heart.*”

Shameless self Promotion

- Just a common guy interested in security
- Contributed security to Samsung, HCL, Whatsapp, Photobucket, Digit, TVF and many more.
- Developed smallest possible (2kb) code which could crash Whatsapp
- Created wannasmile which was used to protect users from wannacry
- Helped Bollywood singer Papon recover his social accounts.
- Invited to speak at ToorCon, AndSec, GOS, BPM etc.
- Helped 2000+ people get started with cryptocurrency

Disclaimers

All the flaws demonstrated in the presentation are already reported by me or other security researchers and it got it.

No unfixed / unreported flaws will be discussed in this presentation

This presentation is only for educational purpose

8th November 2016

Two major announcements

Donald Trump Wins Election

PM announces Demonitization

Demonetization Effect

Long Queue in Banks

Cashless Economy

Pre- Demonitization

Easy bank account for all

Flaw 1 : Flaw in passbook printing machines

Passbook and its Use

- A Bank passbook is a small notebook.
- Contains your name, account number and certain other personal information about you
- Contains all the transactions both credit & debit that happened in your account right from the day of opening the account.

Passbook and its Use

- They are gradually becoming obsolete with the rise of online and mobile banking
- Internet connections and mobile networks are scarce or too expensive in India, hence passbook is still used successfully
- Keeps record of Entire Transactions

Government's step to increase bank users

- Indian government launched mega scheme 'Jan Dhan Yojana'
- On the inaugural day, 1.5 crore bank accounts were opened across the country
- Scheme launched at multiple places by 20 Chief Ministers

The Outcome

- 31 Crore+ or 310 million+ savings bank account till date
- More number of people opened bank accounts
- Transactions increased

How passbooks are updated ?

- Manually : By going to a bank
- Very slow and time consuming process

Introduction of Self Printing Machine

- The state bank of India launched an automatic passbook printer called 'Swayam'
- Soon all major banks followed the same
- Updates passbook with all transaction details automatically

Numbers of banks using Self printing machine

- The service was rolled out to more than 30,000 branches
- Other neighboring countries too use it now
- Some of the banks which rolled out their own versions of the Swayam service are :
  - Bank of Baroda
  - Union Bank
  - Bank of India
  - HDFC
  - Canara Bank
  - UCO
  - Central Bank of India etc.

Mechanism of Self printing machine

- Banks Paste barcodes in passbook
- When the user inserts the passbook, the barcode scanner inside the machine scans the barcode
- Printer prints the entire transaction details in the passbook

The flaw

- Only barcodes are used as authentication
- Account number is used as barcode data
- Account numbers are public and easy to get
- Barcodes can be easily spoofed
- Transaction and bank balance of any user can be viewed by making a barcode with the account number as its data

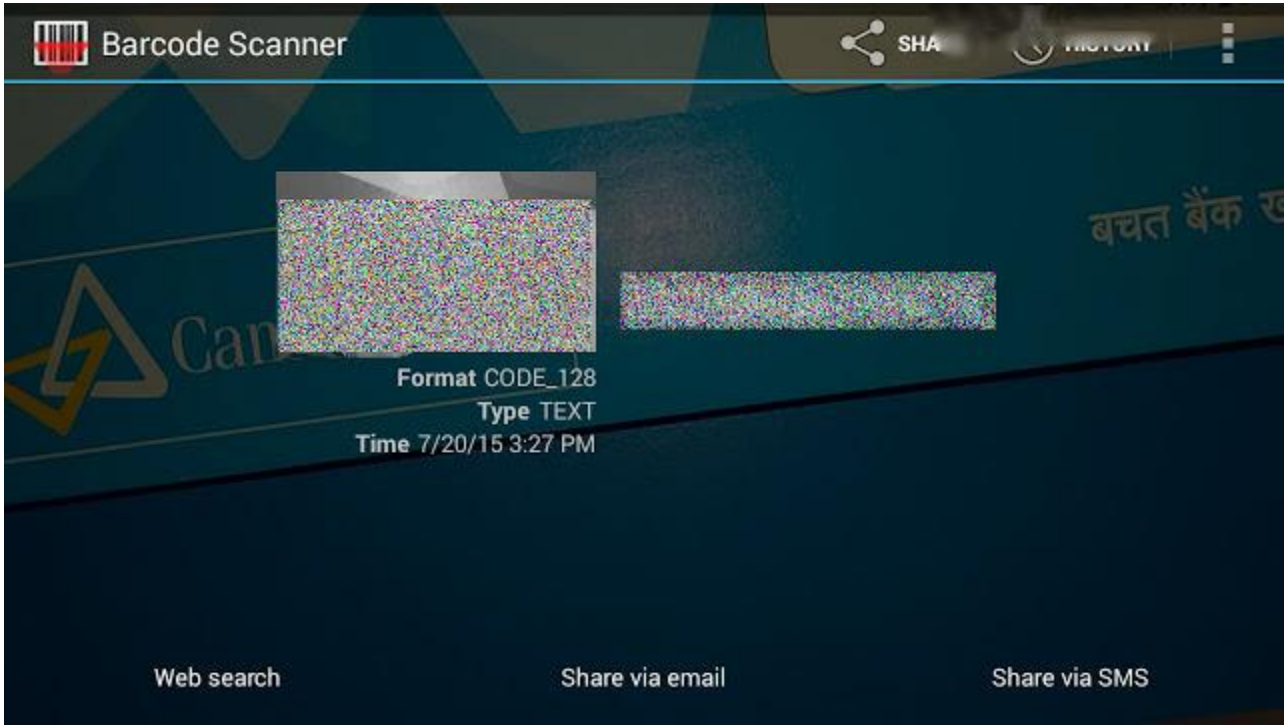
State Bank of India's approach

Barcode data is different from the account number

Other Banks' Approach

Account number used as barcode data

Other Banks' Approach

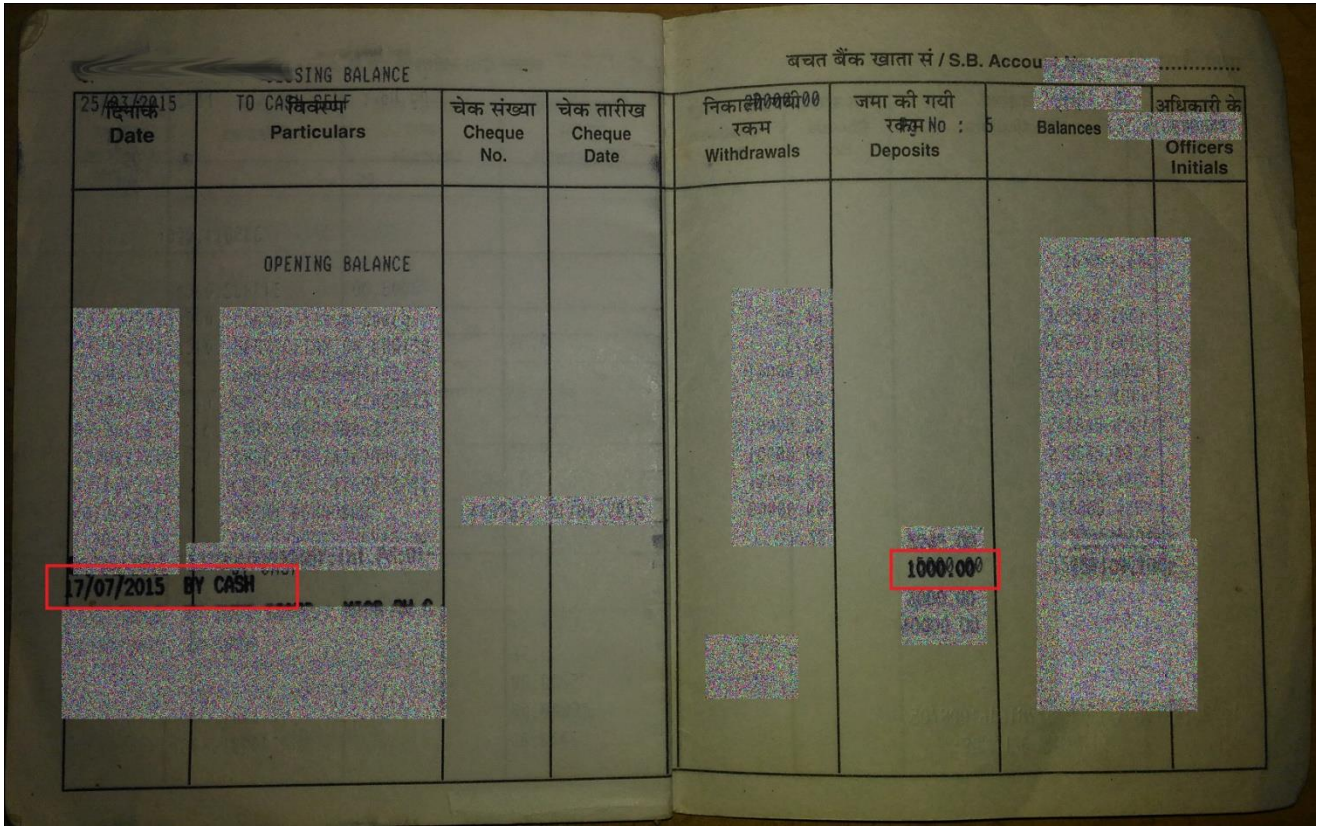


Account number used as barcode data

The Risk

Tool Demo

Practical


SING BALANCE
बचत बैंक खाता सं / S.B. Accou
दिनांक
Date
विवरण
Particulars
चेक संख्या
Cheque No.
चेक तारीख
Cheque Date
निकाली गयी रकम
Withdrawals
जमा की गयी रकम
Deposits
Balances
अधिकारी के
Officers Initials
OPENING BALANCE
17/07/2015 BY CASH
1000.00

The Solution

- Banks should add another level of authentication
- Which includes :
  - ATM Pin number
  - Biometrics
  - Swaping of ATM cards
  - SMS based OTP
  - Use of Separate Cards

Flaw 2 : Government Based wallet Flaw

Demonetization solution – Cashless Economy

Wallets by State Government

Toka Poisa E-Wallet Flaw

DEMO

Flaw 3 : BHIM Flaw

DDOS Flaw

Users were able to send Money to themselves

Risk : By creating a Tool which send money to itself in loop an attacker can take down the whole system.

Privacy Flaw

Attacker Can see the name of User using their registered phone number

Risk : A tool with random number can make a list of all users with their name and phone number

Flaw 4 : Credit / Debit Card Flaw

Question ?

What makes online transaction in India much secure than other countries ?

Answer !

Online transaction Security In india

Customers needs these information to carry out transaction

- 16 digit card number – (Static)
- Card expiry date – (Static)
- CVV – (Static)
- **OTP – (Dynamic)**

OTP Bypass

Step 1: Login to your SBI account

Step 2: After successfully login to your account go to "Payments/Transfers".

Step 3: Then in "Other Payments / Receipt" click on "Quick Transfer".

Step 4: After that choose account from which you have to transfer money.

Step 5: Click on OTP and confirm

Step 6 : Change the parameter "Smartotpflag=Y" to "Smartotpflag=N"

OTP Bypass

DEMO

Flaw 5 : Fetch Personal Information

Fetch Personal Information

Information which can be retrieved are :

- Account Username
- Account holder's Full Name
- Account Number
- IFSC Code
- Date of Birth
- Email ID
- Full Address

Fetch Personal Information

- In SBI, whenever an User forgets his password, he needs to submit a reset password form in the branch.
- The form is pre generated with details which an user can download in PDF form

Fetch Personal Information

To

The Branch Manager

State Bank Of India

[redacted] Branch

I am a registered USER of your Internet Banking Service - "OnlineSBI" for my our following Account (s).

My Reset profile password reference number is [redacted]

Applicant's Name : (Max. 25 characters) [redacted]

User Name(As recorded in Internet Banking) [redacted]

Applicant's Account number(s) [redacted]

I have forgotten the profile password and I request you to reset the same.

Date of Birth:16[redacted] Email Address: [redacted]nail.com

Address (as per bank's records)	Telephone No(s).
[redacted] Pin:700047	Office: Residence:00000000

I confirm having read and understood the document containing the "Terms of Service (Terms & Conditions) " governing the S

Fetch Personal Information

Download Link :

https://retail.onlinesbi.com/retail/resetProfilePwdFormDownloadPdf.htm?refNo=Pxxxxxx

Flaw 6 : Adhaar Based e-KYC Flaw

Aadhaar Based e-KYC Flaw

- Using this loophole anybody can use Aadhaar demographic authentication API by sending requests through NSDL servers and bypass the checks at place by UIDAI.

Aadhaar Based e-KYC Flaw

What is aadhaar API ?

UIDAI provides different APIs which can be used to perform various actions like authentication (demographic and biometric), e-KYC (know your customer), e-sign etc.

Aadhaar Based e-KYC Flaw

Authentication User Agencies (AUA)

Sub – Authentication User Agencies (SUA)

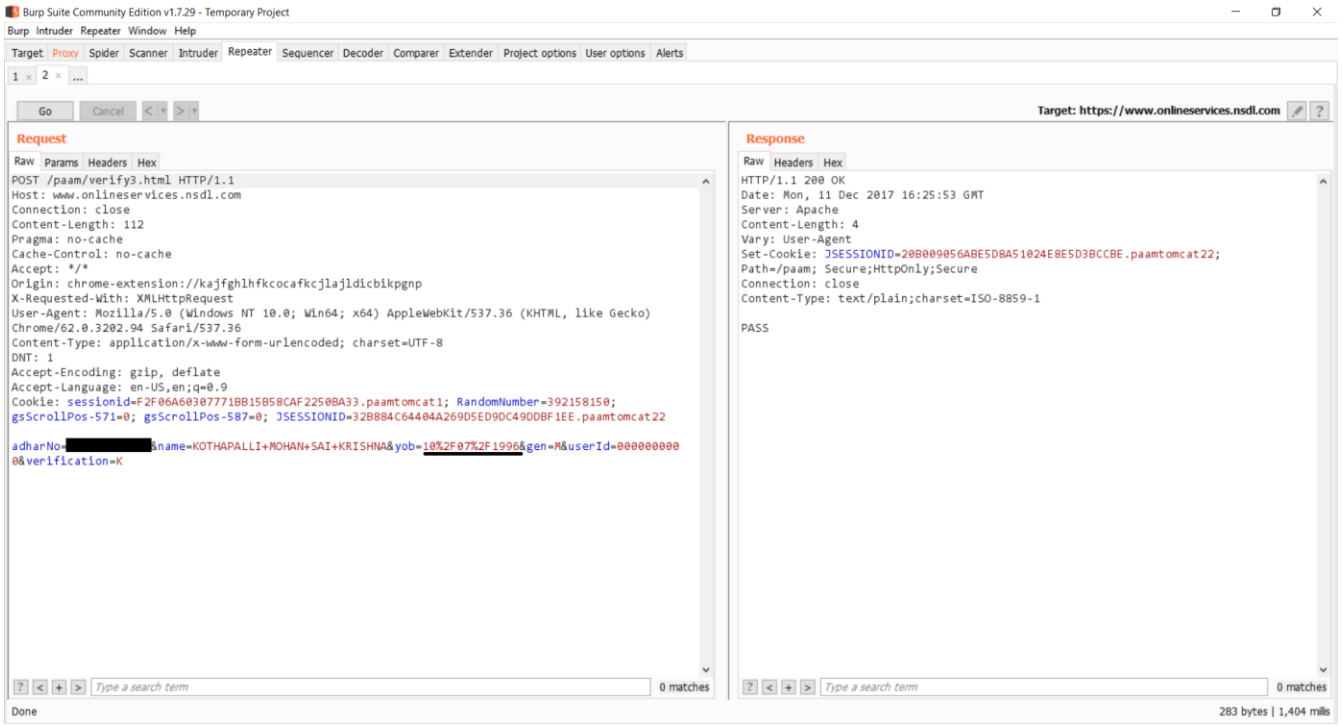
Aadhaar Based e-KYC Flaw

Aadhaar Based e-KYC Flaw

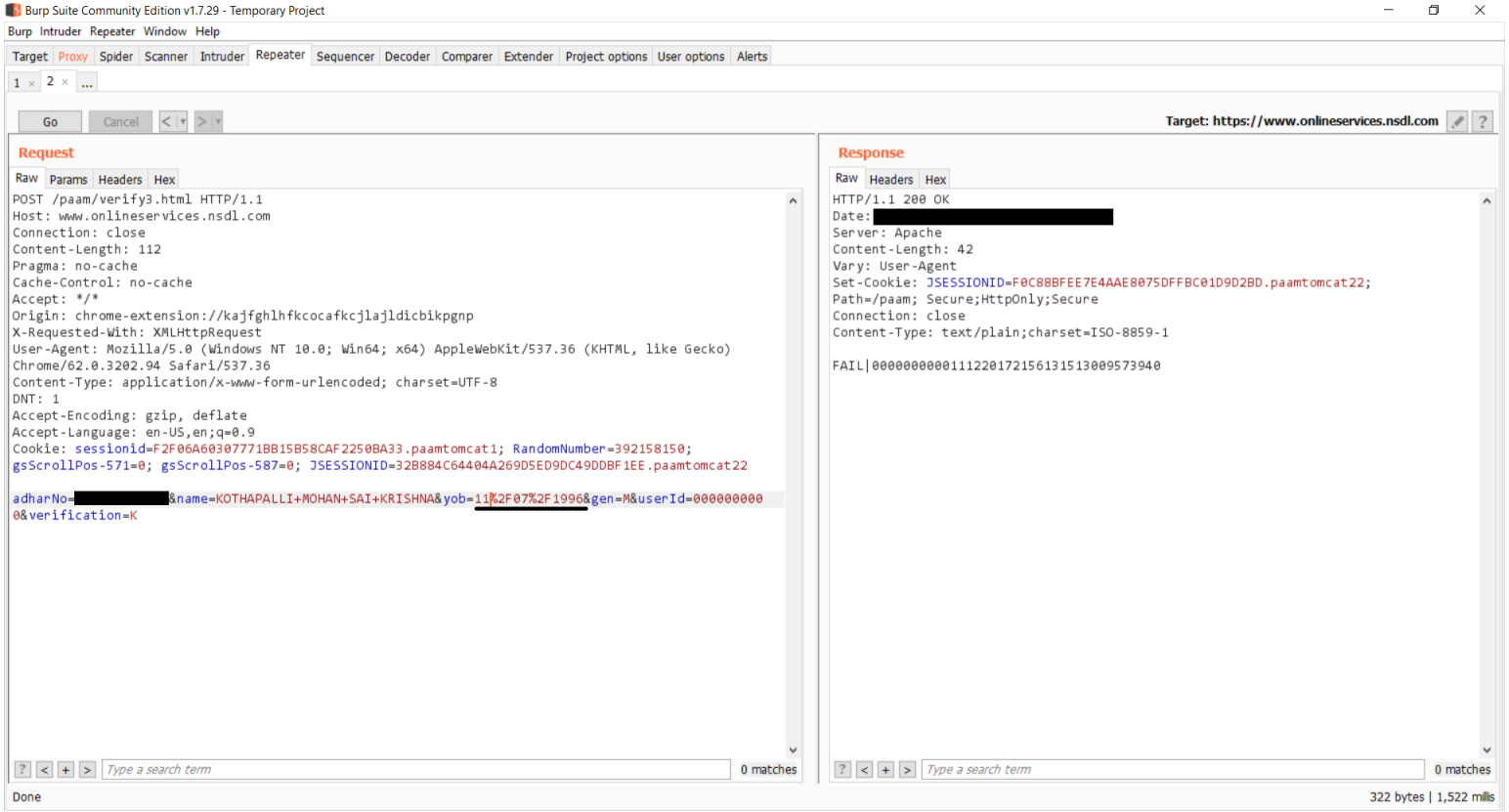
The Flaw

https://www.onlineservices.nsdl.com/paam/verify3.html
Content-Type:application/x-www-form-urlencoded; charset=UTF-8
Accept:*/*
X-Requested-
With:XMLHttpRequestadharNo=**********&name=****+****&yob=**%2F**%2F****&gen=*&userId=0000000000&verification=K

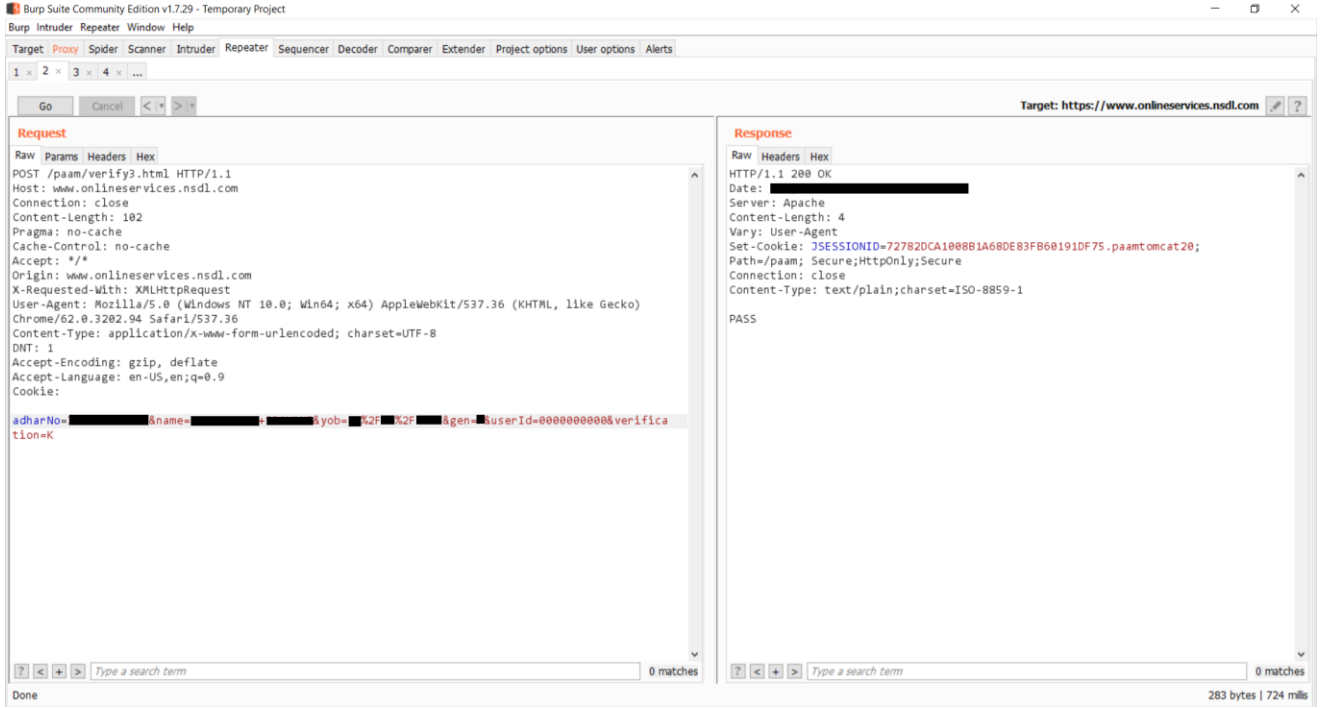
Aadhaar Based e-KYC Flaw



Aadhaar Based e-KYC Flaw



Aadhaar Based e-KYC Flaw



Connecting the Dots…

Connect with me

Facebook.com/indrajeet.bhuyan

Twitter.com/indrajeet_b

www.hackatrick.com

Thank You

*Special thanks to Hrishikesh Barman and Sai Krishna for their help and support