

DAT250

PROSJEKT - HØSTEN 2021

Prosjekt-
oppgaven

Project 1, Website security

Gruppenavn

Gruppe 15, AlphaBank

Gruppens
medlemmer

Navn

Studentnummer

Matias Ramsland

259150

Lukasz Pietkiewicz

253469

Chiran Pokhrel

259205

Jakub Mroz

260703

Konrad Jarczyk

242615

?contentsname?

Innhold	i
Introduction	iii
1 Threat model and site map	1
2 OWASP10	6
2.1 Problemstilling	6
2.2 Forslag til løsning	7
2.2.1 Kode for flow måling	7
2.2.2 Integrasjon ved Eulers forover metode	7
2.2.3 Integrasjon ved trapes metode	8
2.3 Verifikasjon	8
2.3.1 Verifikasjon del 1	9
2.3.2 Verifikasjon del 2, sinusfunksjonen	9
2.4 Integrasjonsmetoder i eksterne funksjoner	11

?CONTENTSNAME?

Bibliografi	11
--------------------	-----------

Introduction

The goal of the project was to create a secure banking application, resistant to OWASP TOP10 attacks.

Our application allows users to add money to their account, send it to a different user through a webpage. Visitors cannot use banking services. To become a user, a visitor must sign up for an account first.

The application is written in python with flask framework, and is using SQLAlchemy with Heroku addon resource Heroku-Postgresql as our database where we store our information.

?chaptername? 1

Threat model and site map

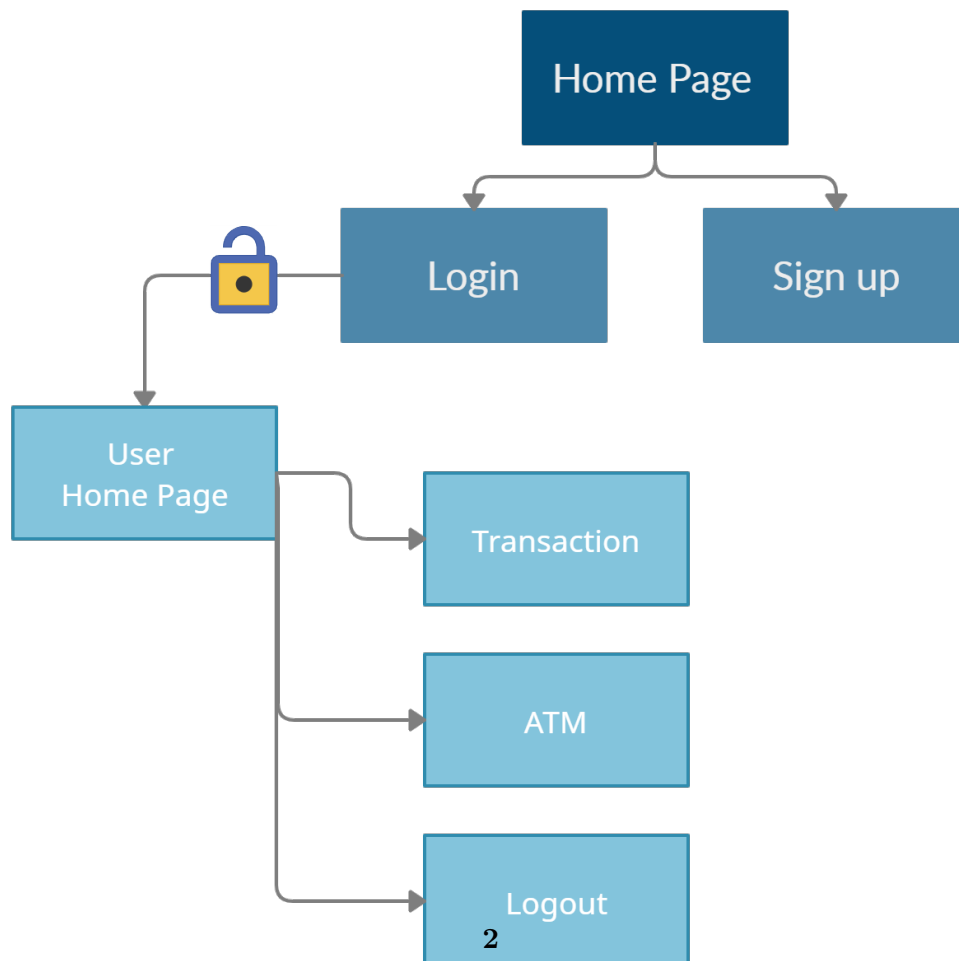


Fig. 1.1: Site map

Threat model and site map

A visitor can only see login and signup pages from the homepage. When an unlogged user tries to visit the URL of any other page, he gets redirected back to the homepage.

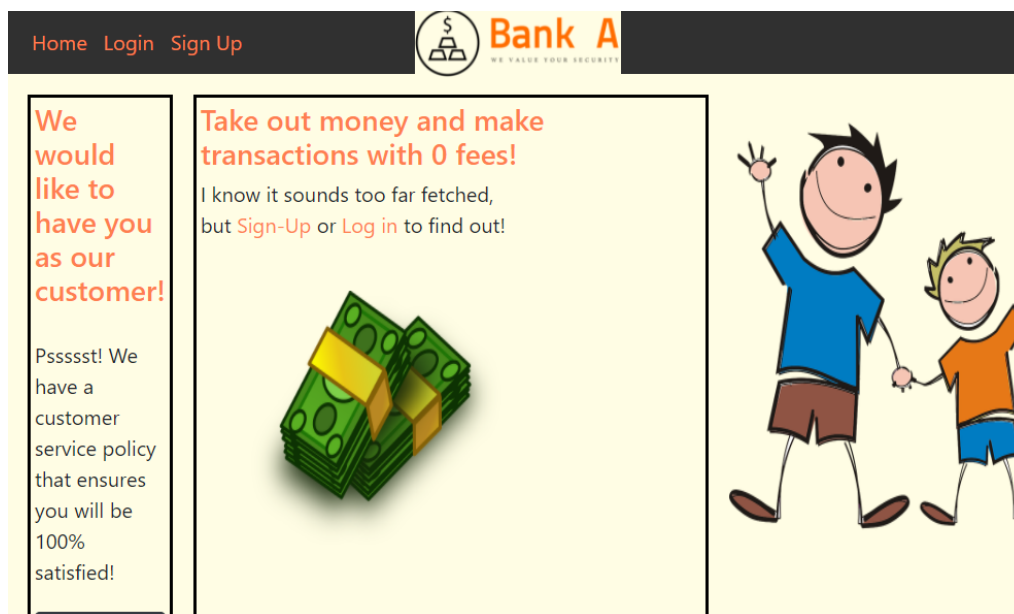


Fig. 1.2: Site landing page

After logging in, the user gets access to ATM and Transaction pages, also home-page changes to show the user's balance and transaction history.

Threat model and site map



Fig. 1.3: User homepage

The image shows the transaction page of Bank B. It has a dark navigation bar with links for Home, Transaction, ATM, and Logout, and the Bank B logo. The main heading is "Please choose amount and to which account you would like to transfer to". Below this, there are several input fields: "Choose your desired amount" with a sub-label "Amount"; "Username" with a sub-label "From which account? (Username)"; "Username" with a sub-label "To which account?"; and "Message" with a sub-label "Message to receiver". At the bottom, there is a large dark button labeled "Transfer Money".

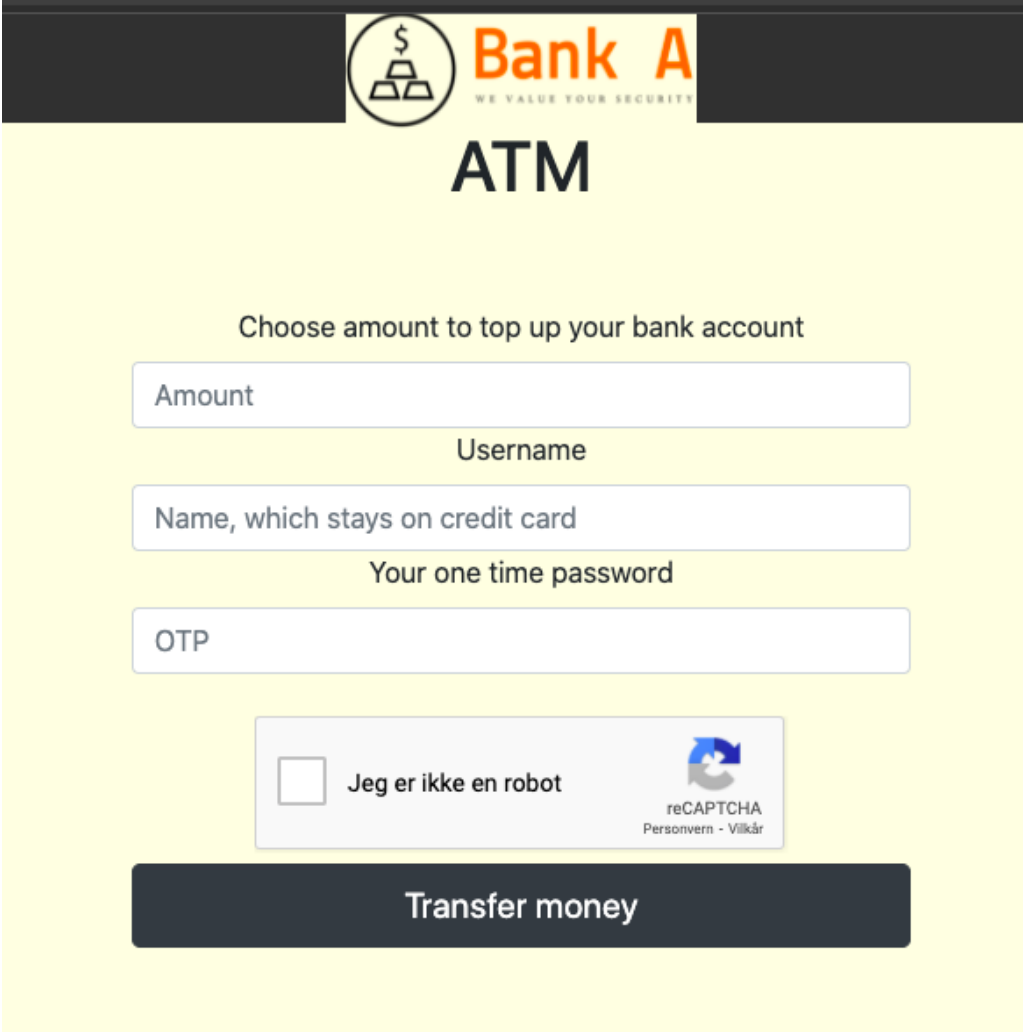
Fig. 1.4: Transaction page

To transfer cash from your own bank account in the Transaction page, the user

Threat model and site map

must know the username of the receiver, and in addition confirm his own. The user can also choose to send it with a message. This action must go through reCAPTCHA and 2FA authentication.

ATM service simulates depositing cash in a local ATM to fill your account. This page looks like this, and must also confirm/verify the name of the user, reCAPTCHA and 2FA authentication. The limit is set to 10 000kr to have realistic values. The ATM page looks like this:



The image shows a web page for 'Bank A' with a dark header bar. In the center of the header is a logo consisting of a circle with a dollar sign and three gold bars below it. To the right of the logo, the text 'Bank A' is written in orange, and below it, in smaller grey text, 'WE VALUE YOUR SECURITY'. Below the header, the word 'ATM' is displayed in large, bold, black letters. Underneath 'ATM', the text 'Choose amount to top up your bank account' is centered. This is followed by a series of input fields: 'Amount', 'Username', 'Name, which stays on credit card', and 'Your one time password'. Below these is an 'OTP' field. Further down is a reCAPTCHA box containing a checkbox, the text 'Jeg er ikke en robot', and the reCAPTCHA logo with the text 'reCAPTCHA Personvern - Villkår'. At the bottom of the page is a large, dark grey button with the text 'Transfer money' in white.

Fig. 1.5: ATM page

?chaptername? 2

OWASP10

2.1 Problemstilling

Problemstillingen i dette prosjektet har vært integrasjon i praktiske situasjoner. Ved numerisk integrasjon har vi tilgang bare til tidsseriesignalet, de vil si til data målt gjennom tid istedenfor å ha analytisk funksjon $f(x)$ som kan integreres ved å finne antiderivert.

Vi har lagt en simulasjon av «flow» i Matlab som skal være integrert. Simulert flow kan være både positiv og negativ, slik at vi kan måle økning eller reduksjon av den originale volumet. Simulasjon av flowsignalet har vi fått til ved å måle reflektert lys med lyssensoren og EV3 enheten fra Lego Mindstorm. Første måling er definert som ingen flow («nullflow»). Alle lysere verdier blir derfor positiv flow og mørkere verdier blir negativ flow.

Fig. 2.1: Ark brukt til simulasjon av flow

Vi har prøvd å oppnå målet ved å estimere arealet under flow ved å dele areal og summere det for å få anslag av arealet.

2.2 Forslag til løsning

2.2 Forslag til løsning

Vi lagrer verdi og tid fra hver måling vi får fra lyssensoren i to forskjellige vektorer Lys og Tid. Disse to vektorer blir indeksert med heltallet «k» som starter fra 1 og øker med 1 for hver ny måling. Lysverdi fra første måling Tid(1) blir definert som «nullflow» og blir trukket fra alle lysverdier. Data etter subtraksjon blir lagret i Flow vektoren som også er indeksert med k.

Etterpå blir flowsignalet integrert ved hjelp av Euler forover og Trapez metodene. Begge to metodene handler om å dele areal under grafen inni blokker som ligger mellom tidspunkt av målingene på x-aksen. Areal av alle blokker summeres til slutt slik at vi får estimat av totalt areal fra $x = 0$ til $x = k$

2.2.1 Kode for flow måling

Flow blir implementert til matlab slikt:

```
nullflow = Lys(1)
k = 1
while loop
    Flow(k) = Lys(k) - nullflow
    k = k + 1
end
```

Hvor Lys(k) er verdien vi får fra lyssensoren i måling nr k. På samme tid lagres tidspunkt av måling i egen vektor.

2.2.2 Integrasjon ved Eulers forover metode

I Euler forover metoden deles areal til rektangler som har tidsforskjell mellom to målingene som grunnflate og flowverdien som høyde.

2.3 Verifikasjon

$$\text{Volum}(k) = \text{Volum}(k - 1) + \text{Flow}(k) * \text{Tidsskritt}$$

Hvor Tidsskritt er tid mellom måling k og måling $(k - 1)$

$$\text{Tidsskritt} = \text{Tid}(k) - \text{Tid}(k - 1)$$

Formelen summerer forrige estimat av arealet med areal som kommer med ny flowmåling. Som du ser i figur 3 denne metoden tar ikke med trekanter som oppstår mellom grafen og rektangler, men estimatet blir mer nøyaktig med økt antall målinger i tidsintervallet.

2.2.3 Integrasjon ved trapes metode

Trapes metoden tar gjennomsnittet mellom to flowverdier og omgjør areal mellom to tidspunkt til trapes. Denne trapesen har 2 lysverdier som 2 parallelle sider og Tidsskritt som høyde. Areal av trapesen blir regnet ut med formel:

$$A = (a + b) * h / 2 \tag{2.1}$$

Etterpå blir areal av trapesen lagt til forrige estimat av arealet.

$$\text{volum}(k) = \text{volum}(k - 1) + (\text{flow}(k - 1) + \text{flow}(k)) * \text{Tidsskritt} / 2$$

Siden denne formelen bruker gjennomsnittet mellom to flowverdiene, blir det mindre feil i estimat når stor variasjon mellom nåværende og forrige måling av flow skjer.

2.3 Verifikasjon

Her verifiserer vi estimat av volum med kalkulasjon gjort for hånd mellom punkt utlest i flowsignalet og volum.

2.3 Verifikasjon

2.3.1 Verifikasjon del 1

Figur over viser at det er økning med 8 i tidsintervallet fra 9,028s til 11,57s

$$\begin{aligned}\text{Areal} &= \text{Lys} * \text{Tid}(\text{slutt}) - \text{Lys} * \text{Tid}(\text{start}) \\ \text{Areal} &= \text{Lys} * \text{Tidsskritt}\end{aligned}$$

$$\begin{aligned}\text{Tidsskritt} &= 11,57 - 9,028 = 2,542 \\ \text{Lys} &= 8 \\ \text{Areal} &= 8 * 2,542 = 20,336\end{aligned}$$

Dette stemmer med avlesning fra volumet:

$$\text{Stigning av volumet} = 19,25 - (-1,042) = 20,292$$

2.3.2 Verifikasjon del 2, sinusfunksjonen

Volum av sinusfunksjonen blir beregnet med formelen:

$$V(t) = \int a \sin(\omega t) dt \quad (2.2)$$

$$\omega = \text{vinkelfrekvens} \quad (2.3)$$

$$V(t) = -a(1/\omega) \cos(\omega t) + C \quad (2.4)$$

Hvor a står for amplituden og ω er vinkelfart. Konstanten C er volum ved Flow(1), altså 0.

2.3 Verifikasjon

$$\text{Topp1} = 8,154\text{s}$$

$$\text{Topp2} = 9,852\text{s}$$

$$\text{Bunn} = 8,981\text{s}$$

$$\text{Amplitude} = (\text{Ymax} - \text{Ymin}) / 2$$

$$\text{Amplitude} = (6 - (-8)) / 2$$

$$\text{Amplitude} = 7$$

$$\text{Vinkelfart} = 2\pi / \text{Tidsforskjellen mellom 2 topper}$$

$$\text{Vinkelfart} = 2\pi / (9,852\text{s} - 8,154\text{s}) = 2\pi / 1,698$$

$$\text{Vinkelfart} = 3,700 \text{ rad/s}$$

Volumet ved 1. toppen (tid = 8,154s) vil være:

$$\text{Volum}(8,154) = -7 * (1 / 3,700) * \cos(3,700 * 8,154)$$

$$\text{Volum}(8,154) = -0,60350$$

Volumet ved 2. toppen (tid = 9,852s) vil være:

$$\text{Volum}(9,852) = -7 * (1 / 3,700) * \cos(3,700 * 9,852)$$

$$\text{Volum}(9,852) = -0,60245$$

$\text{Volum}(8,154)$ og $\text{Volum}(9,852)$ er praktisk likt, det betyr altså at beregningene av vinkelfart stemmer.

Toppunkt og bunnpunkt i denne funksjonen skjer når cosinus er lik 1 eller -1.

Bunnpunkt skjer ved $\cos(t) = 1$, altså ved $t = 0$

$$\text{Volum}(0) = -7 * (1 / 3,700) * \cos(3,700 * 0)$$

$$\text{Volum}(0) = -1,89$$

Areal ved minimalpunkt I denne sinusfunksjonen er -1.88, men den er bare halvparten av «negativ» flow, som stopper mellom bunnpunkt og topppunkt. Derfor må vi gange areal som vi får i bunnpunkt med 2.

$$-1,89 * 2 = -3,78$$

Dette stemmer med data fra volumgrafene i figur 6:

$$35,83 - 32,1 = 3,73$$

Volumet har blitt mindre med 3,73, som er veldig nærme forventet 3,78.

2.4 Integrasjonsmetoder i eksterne funksjoner

2.4 Integrasjonsmetoder i eksterne funksjoner

Til slutt har vi lagret funksjoner i separate .mat filer slik at koden for integrering kan brukes i andre prosjekter.

Her er kallet til funksjoner EulerForward:

$$\text{volumEuler}(k) = \text{EulerForward}(\text{volum}(k-1), \text{flow}(k-1), \text{Ts}(k-1))$$

EulerForward trenger forrige areal estimat, forrige flowverdien og tidsskritt mellom aktuell og forrige måling.

Kallet til Trapesfunksjonen ses ut slik:

$$\text{volumTrapez}(k) = \text{Trapez}(\text{volum}(k-1), \text{flow}(k-1:k), \text{Ts}(k-1))$$

Trapez funksjonen trenger å vite nåværende flowverdien i tillegg til forrige areal estimat, forrige flowverdien og tidsskritt mellom aktuell og forrige måling.