Sikkerhet i Pindena Påmeldingssystem

Versjon: 6.1.0

Oppdatert: 23.09.2020

Innhold

1.Om dokumentet

Dette dokumentet beskriver hvordan sikkerhet er håndtert i Pindena Påmeldingssystem. Dokumentet beskriver nærmere sikkerhet både for klient og i koden. I tillegg til ekstra tjenester som e-post, servere, domene og personvern. Dette dokumentet er også som et vedlegg for Databehandleravtale.

2. Sikkerhet på klientsiden

Krypterte forbindelser og sikkerhet i programvaren på serversiden hjelper ikke hvis man har virus/trojanere eller andre sikkerhetshull på sin egen PC. Sikkerheten begynner på den siden brukeren sitter. Brukernavnet og passordet du mottar er personlig – ikke gi det til andre, og husk å endre passord etter du har logget inn.

3.Sikkerhetstiltak i koden

All programvare laget i Pindena-rammeverket har følgende sikkerhetstiltak:

3.1 Rollesikkerhet

Hver bruker kan ha null eller flere roller tilknyttet.
Rollene kontrollerer:

1. Hvilke maler brukerne kan se.
2. Hvilke menyelementer brukerne kan se.
3. Hvilke funksjoner brukerne kan utføre (klikk på knapper som endrer data etc).

3.2 Databasesikkerhet

Hver kunde har sine egne databasetabeller, som bare kundens installasjon har tilgang til.
Alle data lagres i klartekst i databasen bortsett fra passord som er kryptert.

3.3 Templatesikkerhet

Pindena Påmeldingssystem er mal-/templatebasert, og tilgang gis for hver enkelt template.

1. ”Nekt først-policy” på backend-maler. Hvis malen ikke har et definert sikkerhetsnivå har ingen tilgang til disse malene. Det er altså bevisste handlinger som må til for å tilgjengeliggjøre maler og tilgangsnivå til maler for de ønskede rollene.
2. Maler som ikke inngår i sikkerhetssystemet er som standard ikke tilgjengelige.
3. Maler i frontend har alle tilgang til, men for å utføre endringer uten pålogging så er det nødvendig med en unik ID.

3.4 Forebygge øktkapring (session hijacking)

3.4.1 Følgende er gjort for å forebygge øktkapring:

1. Session tidsavbrudd ved inaktivitet (session utløper etter en periode med inaktivitet selv om timeout ikke er nådd, og bruker blir logget ut). Antall timer er avhengig av ønsket sikkerhet. Kort utløpstid er mest sikkert.
2. Bytte av cookie-id ved pålogging for å hindre ”session fixation”.
3. Alle kunder med vårt domene har HTTPS. De med eget domene kan få HTTPS for en ekstra kostnad.

3.5 Forebygging av angrep

3.5.1 Følgende er gjort for å forebygge direkte angrep:

1. Vi bruker rammeverket Laravel som har innebygget beskyttelse mot tre typer angrep:
    a. ”SQL Injection attack”
    b. ”XSS attack” (Cross Site Scripting)
    c. “CSRF attack” (Cross-Site Request Forgery)
2. Validering av all input som skal lagres i databasen eller presenteres i en mal.
    a. All input blir konvertert til den minst sikkerhetskritiske datatypen som løser oppgaven.

b. Input i tallfelt blir konvertert til tall.
c. Input i datofelt blir konvertert til datoer.
d. Tekst som ikke skal ha formatering blir konvertert til ren tekst.
e. Siste utvei er lagring av HTML kode som vi prøver å unngå, men der vi må gjøre det blir det vasket mot svartelister for å hindre lagring av kode som kan gi sikkerhetsproblemer.

3.7 Logging

Logger brukes for sporing i tilfelle angrep. Følgende logger finnes:

1. Session-logg over brukersesjoner.
2. Logger for bruk.
3. Webserver-logg.
4. Google Analytics-logg.

Webserver logg slettes etter 14 dager.

3.8 Auditlogg

Pindena Påmeldingssystem har kraftig audit-funksjonalitet. Merk at dette genererer mye data. Audit-logging kan konfigureres på spesifikke felt i tabeller der det er av særskilt interesse å følge med på endringer.
Det som automatisk logges er:

1. Deltagerstatus
2. Betalingsstatus

Kunden kan også ønske hvilke felt som skal logges (fakturerbart).

Alle endringer i feltet blir logget og man har en historikk på alle verdier som har vært i feltet i tabellen og hvem som endret det og når de endret det.

4. E-post

Følgende tiltak er utført for å redusere risikoen for at utsendelser skal bli oppfattet som søppelpost:

1. Vår egen e-postadresse er lagt inn som en standard avsenderadresse, og kunder kan be om å endre dette om de ønsker.
2. Kunder har muligheten til å be om å sende e-poster fra egen konto i feks SendGrid, Mandrill, Mailgun og lignende epostklienter. Kunder som benytter seg av e-postklienter for utsendelse, bes følge råd om Whitelabel og andre sikre tiltak. Ved å sende fra andre klienter, så kan man se statistikk på utsendelser, samt velge egen avsenderadresse.
3. Vi anbefaler kunder om å ha færrest mulig bilder i e-post som et tiltak for å prøve å unngå spamfilter hos mottager.

5. Server

1. Pindena AS har retten til å flytte kunder mellom servere og leverandører; dette kan være nødvendig grunnet best ytelse for kunde. Med mindre annet er avtalt så kan kunder flyttes til servere som er lokalisert i andre EU/EØS land.
2. I Sverige har vi servere i Stockholm hos verdenskjente Amazon. I Norge så leier vi virtuelle servere av Webhuset AS som har sine datasentre i Oslo og Bergen. Webhuset sine servere bruker operativsystemet Debian 8 med automatisk oppdatering av sikkerhetspatcher.
3. Vi tar daglig backup av alle serverne, både filer og databaser.
4. Serverne overvåkes med Monit og varsler med både e-post og SMS ved feil.

6. Domene

Vi benytter Miss Hosting (tidligere ISP-huset) for domener. Miss Hosting holder til i Oslo.

7. Personvern

7.1 Tiltak:

1. Ingen deltagerinformasjon i kundens installasjon vil bli utgitt til tredjepart, eller brukt av Pindena.
2. Etter at en installasjon stenges, så skal den slettes etter 2 uker, med mindre annet er avtalt.
3. Innført SMS-verifisering på deltagerinformasjonsnivå.
4. Reservert felt for samtykke, med link til side for personvern.
5. La ansvarlig velge hvilke felt som er sensitiv og ikke.
6. Ansvarlig kan sette hvor lang tid informasjon skal være lagret etter aktivitetsslutt, og etter det vil det bli slettet fra Pindena Påmeldingssystem og så fra databasen.

7.2 Tiltak kunden bør gjøre overfor sine deltagere:

1. Be om godkjennelse til å innhente informasjon, ved å benytte “Samtykke” feltet med link til personvernerklæring.
2. Kun innhente informasjon som er godkjent.
3. Slette informasjonen etter en viss tid. Enten ved å slette deltager eller selve aktiviteten.
4. Slette informasjon om deltageren hvis den ønsker å bli slettet.
5. Sette opp innstillinger for å benytte Slette funksjoner for deltagerdata og sensitiv deltagerdata.
6. Si ifra til Pindena om tidligere aktiviteter skal slettes fra databasen (fakturerbart om man ikke gjør det selv).

8. Diverse

- “Min side” kan benyttes for at deltagere kan logge inn, og se hvilke aktiviteter de har deltatt i og blitt invitert til. Her kan de laste ned vedlegg som er aktuelle for aktiviteten, som: faktura, QR-kode, kursbevis og billett.
- Ved bruk av tredjeparts selskap på eget initiativ og ønske (som betalingsløsninger, e-postklienter og lignende), så er ansvaret mye til kunden selv, da Pindena ikke har valgt ut dette som egne underleverandører.
- I forbindelse med Pindena sine underleverandører, så er det opprettet Databehandleravtaler med disse. Om kunden ønsker kan de tilsendes.