Sikkerhet i Pindena Påmeldingssystem

Versjon: 5.0.0
Oppdatert: 05.09.2018

Telefon: +47 33 80 65 00
Web: www.pindena.no
E-post: post@pindena.no

Innhold

Om dokumentet

Dette dokumentet beskriver hvordan sikkerhet er håndtert i Pindena Påmeldingssystem.

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.

Sikkerhetstiltak i koden

All programvare laget i Pindena-rammeverket har følgende sikkerhetstiltak:

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).
4. Hvilke databasetabeller du kan lese/skrive/oppdatere/slette.

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.

Fallback-sikkerhet

Uavhengig av rolle søker en fallback-sikkerhetsmodell å minimere skade dersom en ekstern bruker har fått en rolle han ikke skulle hatt.

Pindena er oppdelt i to grensesnitt:

1. Frontend. Alle har tilgang som standard.
2. Backend. Krever pålogging. En bruker får kun full tilgang til backend hvis den har blitt lagt til som en bruker. Det betyr at hvis en kunde prøver å logge inn med en intern rolletilgang som er gitt ved en feil, vil de bli stoppet med mindre denne brukeren er spesifikt knyttet til malen/funksjonen.

Templatesikkerhet

Pindena 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.

Forebygge øktkapring (session hijacking)

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 potensielt farlige tegn fjernes fra alle felt og variabler der de ikke er tillatt å bruke. Dette gjør session hijacking med Javascript umulig.
4. Alle kunder med vårt domene har HTTPS. De med eget domene kan få HTTPS for en ekstra kostnad.
5. Session utløper umiddelbart hvis man prøver å bruke den fra en annen IP-adresse, en annen nettleser eller en annen protokoll enn den ble opprettet fra.

Forebygging av angrep

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. Forhindre lagring av svartelistet kode i input elementer (for eksempel kjørbare Javascript er umulig å lagre).
    b. All input blir konvertert til den minst sikkerhetskritiske datatypen som løser oppgaven.
    c. Input i tallfelt blir konvertert til tall.
    d. Input i datofelt blir konvertert til datoer.
    e. Tekst som ikke skal ha formatering blir konvertert til ren tekst.
    f. 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. Alle potensielt usikre tegn fjernes fra alle felt og variabler ihht. konvensjoner på variabelnavn og sikkerhetsoppsett før lagring av data i databasen eller presentasjon av data i en mal.

Logging

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

1. Logger forsøk på tilgang til maler som man ikke har tilgang til.
2. Session-logg over brukersesjoner.
3. Logger for sider som ikke finnes.
4. Logger for bruk.
5. Webserver-logg.
6. Google Analytics-logg i de tilfellene kundene ønsker det.

Loggene slettes etter 3 måneder.

Auditlogg

Pindena har kraftig audit-funksjonalitet. Denne kan skrus på etter kundens ønske. 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 logges er:

1. Databasetabell
2. Feltnavn
3. Bruker-id
4. Innhold
5. Tidspunkt

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

Audit-logger slettes etter 4 måneder.

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 vår SendGrid konto, eller opprette konto i SendGrid, og lignende klienter, selv.
3. Kunder som benytter seg av epostklienter for utsendelse, bes følge råd om Whitelabel og andre sikre tiltak.
4. Vi ber kunder om å ha færrest mulig bilder i e-post.

Server

Tiltak:

1. Vi leier virtuelle servere av Webhuset AS som har sine datasentre i Norge (Oslo og Bergen).
2. Serverne 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.

Domene

Vi benytter ISP-huset for domener. ISP-huset holder til i Drammen.

Personvern

Tiltak:

1. Ingen informasjon i kunde sin installasjon vil bli utgitt til tredjepart, eller brukt av Pindena på noen annen måte.
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.

Tiltak som skal innføres:

1. La ansvarlig velge hvilke felt som er sensitiv og ikke.
2. Ansvarlig kan sette hvor lang tid informasjon skal være lagret etter aktivitetsslutt, og etter det vil det bli slettet fra Pindena og så fra databasen.

Tiltak kunden bør gjøre overfor sine deltagere:

1. Be om godkjennelse til å innhente informasjon.
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. Si ifra til Pindena om tidligere aktiviteter skal slettes.