

zahtjevi iz pitanja i odgovora

1. penetraciono testiranje dovoljno da povežemo neki od alata za penetraciono testiranje
2. Webshop mora da ima punu kontrolu nad svim mogućim tokovima i da omogući puno testiranje svih mogućih funkcionalnosti, praktično CRUD i front ya to ya sve objekte u webshopu
3. Šifrovanje osjetljivih podataka u bazama mora da se uradi
4. Na frontu pspa kontrola načina plaćanja ya dati webshop
5. U banci može da se kreira nalog (novi klijent)
6. U banci admin panel koji prikazuje sve transakcije (PCI DSS)
7. Veb-prodavnica treba da vodi računa o izvršenim transakcijama i da sadrži spisak kupljenih proizvoda.
8. QR kod

psp front

- registracije webshopa
- biranje dozvoljenih metoda plaćanja

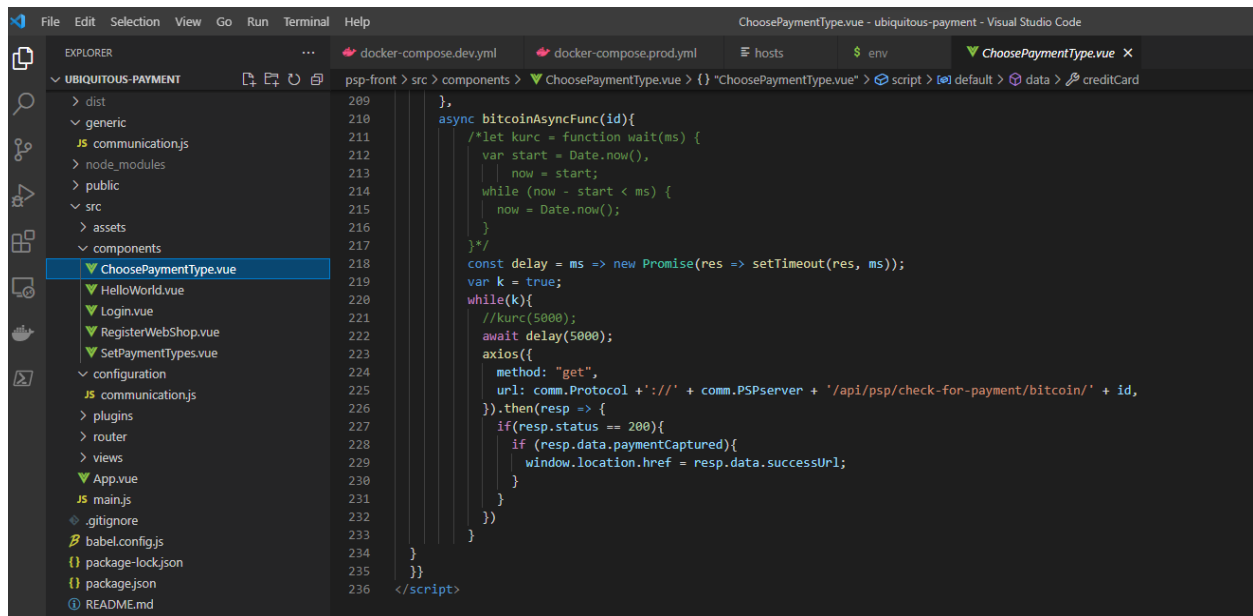
Sif:

- Pan(bank+pcc)
- Cvc(bank+pcc)
- secret(bank)
- Merch id(webshop)
- Merch secret(webshop)

PCI DSS

- Hashovati secret u banci
- Zaštita kartičnih podataka dok se skladište i dok su u transportu; 1.aes u bazi 2. Https tls/ssl
- Minimalna količina skladištenih podataka, podatke ya autentifikaciju ne čuvati posle autorizacije
- Prvih 6 i posljednjih 4 su max koliko smije da se prikaye
- Šifrovanje ključeva ključeva, životni vijek njih meeeeh
- Owasp top 10 (pass, xss, sqli ....)
- Auto logout?
- Deaktivirati naloge ako su neaktivni
- Provjere za lozinke, ne sme da se poklapa sa starim lozinkama
- Blame usera (user id u logovima)
- Logovi (na nivou dokaza)
- Čuvati logove od godinu dana, a tri mjeseca lako dostupna
- Periodično skeniranje mreže ya ynačajne promjene (nmap portovi recimo)
- Penetraciono testiranje (ponasati se kao napadac)
- CDE? Neki obod, kritične tačke

- Hash nad konfiguracijama



```
209 },
210 async bitcoinAsyncFunc(id){
211   /*let kunc = function wait(ms) {
212     var start = Date.now(),
213         now = start;
214     while (now - start < ms) {
215       now = Date.now();
216     }
217   }*/
218   const delay = ms => new Promise(res => setTimeout(res, ms));
219   var k = true;
220   while(k){
221     //kunc(5000);
222     await delay(5000);
223     axios({
224       method: "get",
225       url: comm.Protocol + '://' + comm.PSPserver + '/api/psp/check-for-payment/bitcoin/' + id,
226     }).then(resp => {
227       if(resp.status == 200){
228         if (resp.data.paymentCaptured){
229           window.location.href = resp.data.successUrl;
230         }
231       }
232     })
233   }
234 }
235 }}
236 </script>
```

## TESTIRANJE

U skripti Napraviti drugog prodavca u okviru webshopa koji prodaje drvenu stolicu za 12e i prihvata samo placanje qrcodom. Taj prodavac ima racun u bank2. Potrebno je banka1 i banka2 da imaju po jednog kupca kod sebe, da mozemo kupovati sa obje banke bilo koji proizvod (jer je jedan prodavac u jednoj, a drugi u drugoj banci)