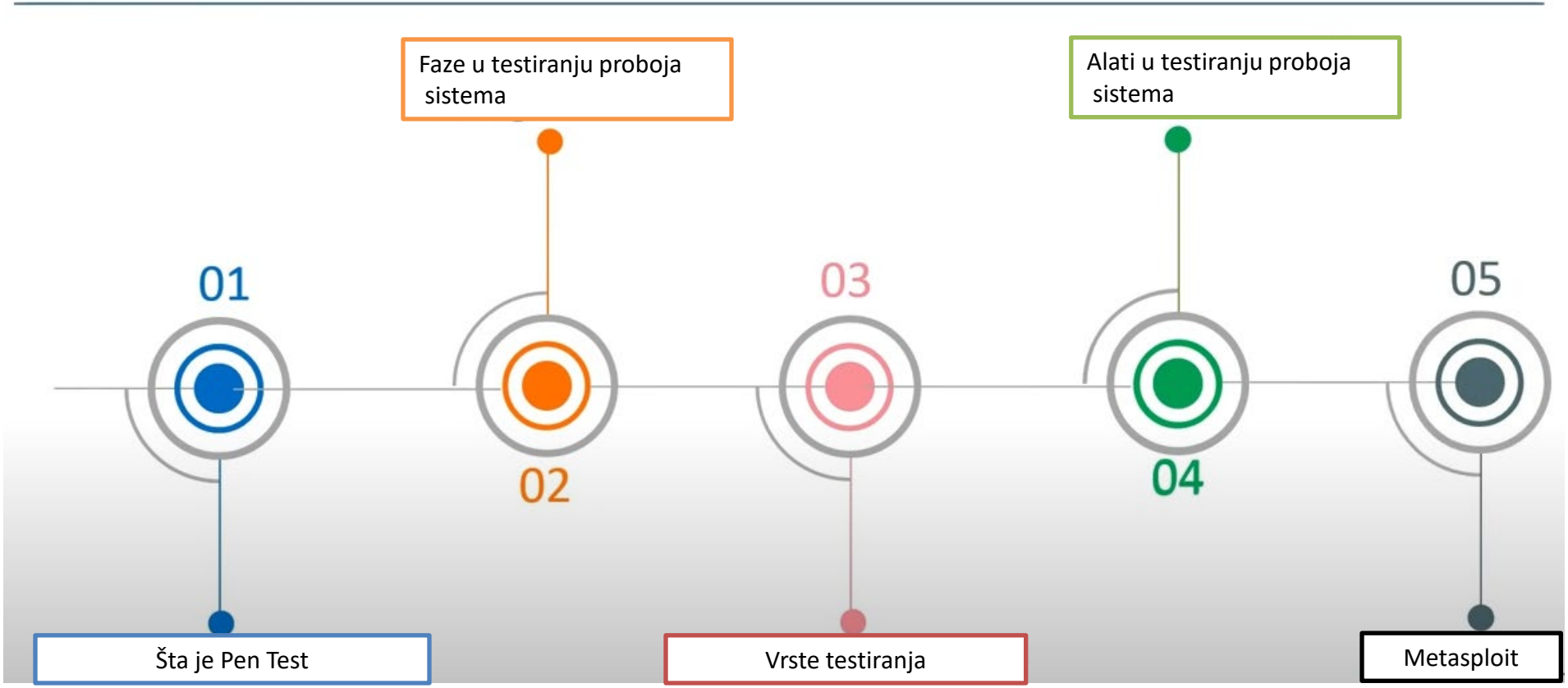
TESTIRANJE PROBOJNOSTI SISTEMA

Predavač: dr Dušan Stefanović

Pen Testing

Pen test je simulirani *cyber security* napad radi provere i procene bezbednosti IT sistema

Proaktivni načini testiranja web aplikacija izvršavanjem napada koji su slični stvarnim napadima



TESTIRANJE PROBOJNOSTI INFORMACIONOG SISTEMA

Simulirani sajber napad

Na informacioni sistem, mrežu, aplikaciju ili uređaj

Identifikovanje i testiranje ranjivosti

Koje bi potencijalni napadać mogao da iskoristi

Procena ranjivosti

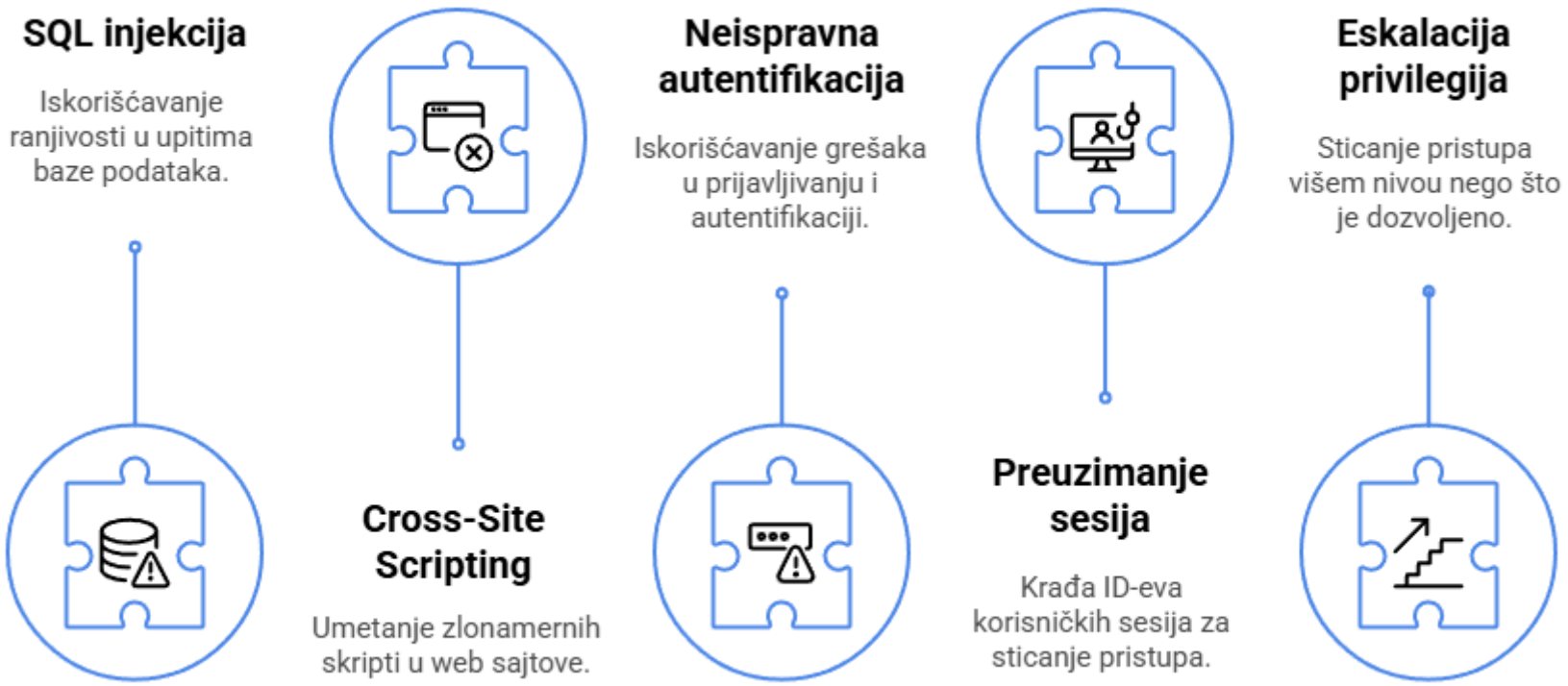
Pen testovi procenjuju ranjivosti u sistemima.

Proaktivna provera bezbednosti

Cilj je predupredititi realne pretnje i napade

TESTIRANJE WEB APLIKACIJA

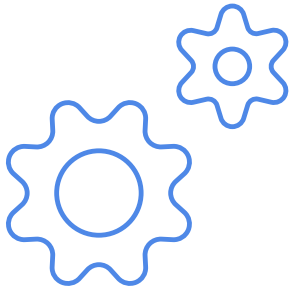
Test probojnosti kod Web aplikacija uključuje **izvršavanje napada koji oponašaju realne metode napadača** (hakera)



SVRHA TESTIRANJA PROBOJNOSTI INFORMACIONOG SISTEMA

Identifikovanje slabosti

Prepoznavanje ranjivosti pre nego što ih napadači iskoriste.



Unapređenje bezbednosti

Poboljšanje bezbednosnih mera kako bi sprečio potencijalne povrede.

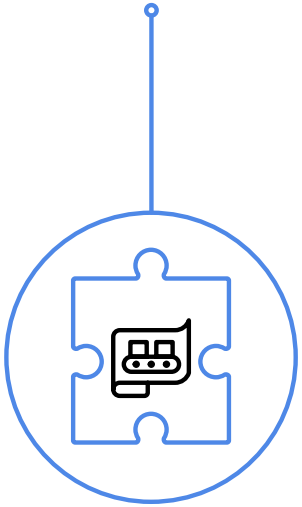
Usklađivanje sa standardima

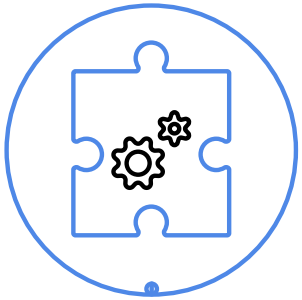
Usklađivanje sa bezbednosnim standardima i regulativama(npr. ISO 27001, PCI-DSS).

IZVORI RANJIVOSTI U INFORMACIONIM SISTEMIMA

Dizajn sistema

Nedostatak autentifikacije ili kontrole pristupa



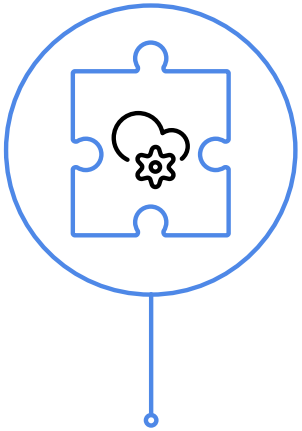


Loša konfiguracija

Pogrešna ili podrazumevana podešavanja (otvoreni portovi, nešifrovana komunikacija, default lozinke)

Nebezbedna mreža

Korišćenje nezaštićenih mrežnih protokola, nedostatak enkripcije, loša segmentacija mreže i ranjivosti u rutiranju ili bežičnim mrežama

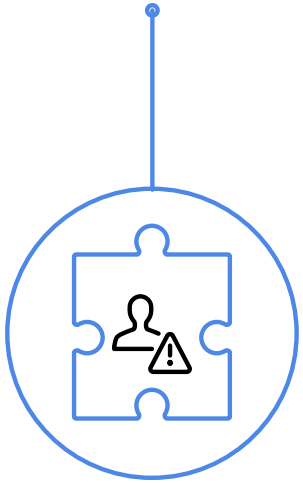


Složenost sistema

Oslanjanje na raznovrsne tehnologije povećava površinu napada.

Ljudska greška

Deljenje lozinki, klik na phishing linkove, loše upravljanje i korisničkim privilegijama



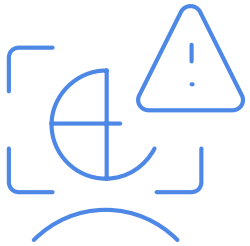
TERMINOLOGIJA U TESTIRANJU BEZBEDNOSTI

Etičko hakovanje

Profesionalac koji identifikuje nedostatke u sistemu, pomažući vlasnicima da otklone ranjivosti.

Penetraciono testiranje

Identifikuje ranjivosti sistema i određuje mogućnost eksploatacije, regulisano ugovorom.



Procena ranjivosti

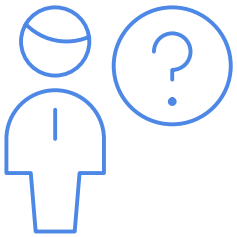
Izveštaj koji opisuje ranjivosti sistema, sortirane prema stepenu rizika.

Provera bezbednosti

Sistemska procedura za merenje stanja sistema u odnosu na standarde, pružajući izveštaje o usklađenosti.

VRSTE TESTIRANJA PREMA STEPENU INFORMISANOSTI TESTERA

TESTIRANJE CRNE KUTIJE (BLACK BOX TESTING)



Informacije o testeru

Tester nema informacije o unutrašnjem radu sistema.

Spoljni napadač

Simulira spoljneg napadača koji pronalazi ranjivosti samo na osnovu spoljnih informacija

Realistična simulacija

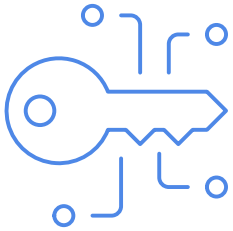
Koristi se za realističnu simulaciju spoljašnjih napada.

Cilj

Otkriti kako sistem reaguje na nepoznate ulaze bez prethodnog znanja o unutrašnjosti sistema.

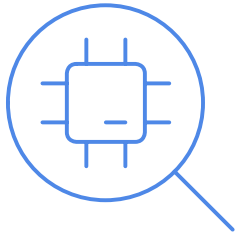
VRSTE TESTIRANJA PREMA STEPENU INFORMISANOSTI TESTERA

TESTIRANJE BELE KUTIJE (WHITE BOX TESTING)



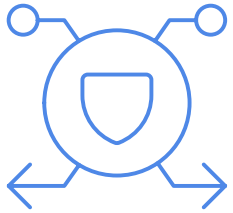
Potpun pristup informacijama

Tester poseduje kompletnu informaciju o sistemu, uključujući izvorni kod, konfiguracije, mrežne dijagrame, privilegovani pristup.



Dubinska analiza ranjivosti

Omogućava dubinsko ispitivanje ranjivosti, čak i onih koje je teško pronaći.



Interne slabosti

Koristi se za proveru internih bezbednosnih propusta i logičkih

Cilj

Iscrpna analiza sistema sa maksimalnim znanjem i pristupom.

VRSTE TESTIRANJA PREMA STEPENU INFORMISANOSTI TESTERA

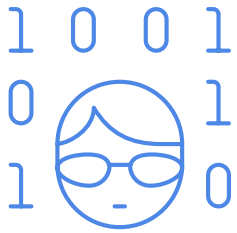
TESTIRANJE SIVE KUTIJE (GREY BOX TESTING)

Kombinovan pristup

Kombinuje pristupe crne i bele kutije.

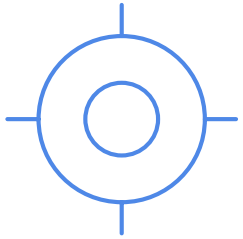
Ograničene informacije

Tester poseduje delimične informacije o sistemu, ne potpune.



Simulacija napadača

Simulira napadača sa ograničenim pristupnim privilegijama.



Cilj

Ocena bezbednosti sistema iz perspektive korisnika sa ograničenim pristupom.

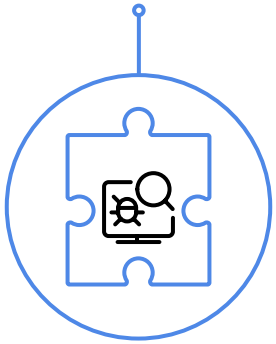
CILJ TESTIRANJA PROBOJA SISTEMA

Otkrivanje ranjivosti sistema

Identifikuje tehničke slabosti koje bi mogle biti iskorišćene od strane napadača.

Provera osoblja na bezbedonosne pretnje

Simulira socijalni inženjering da bi se ocenila otpornost zaposlenih.



Testiranje osoblja na primeni bezbedonosnih procedura

Proverava usklađenost zaposlenih sa bezbednosnim politikama (npr. upravljanje lozinkama, zaštita podataka, reagovanje na sumnjive aktivnosti).

FAZE U SPROVOĐENJU PEN TESTA

Faza 1

Sakupljanje što više informacija o meti napada

Faza 2

Identifikovanje ranjivosti u sistemu skeniranjem sistema

Faza 3

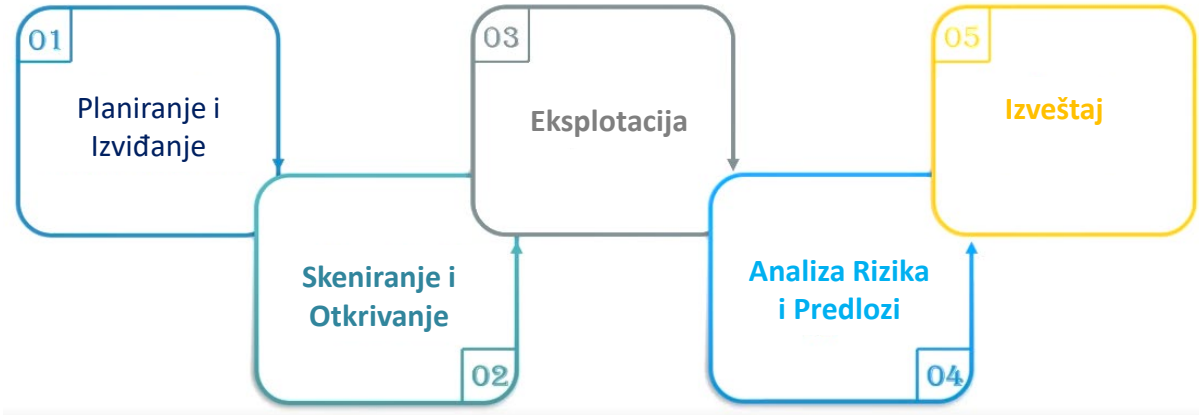
Eksplotacija – sprovođenje napada na uočene ranjivosti u sistemu

Faza 4

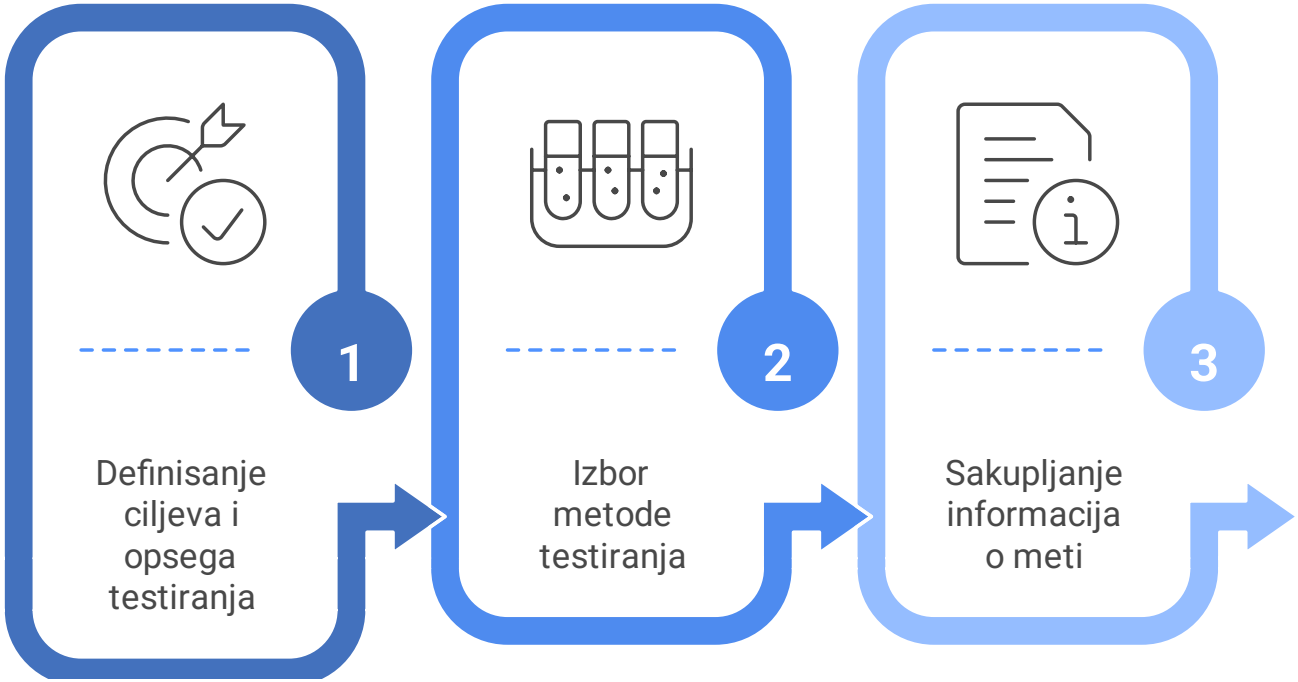
Analiza svake ranjivosti i njen uticaj na bezbednost sistema

Faza 5

Detaljan izveštaj koji sumira rezultate testiranja



PLANIRANJE



Jasno se određuje šta se testira (npr. web aplikacija, mrežna infrastruktura) i koji su ciljevi testa (npr. otkrivanje kritičnih ranjivosti, test otpornosti na napade).

Određuje se pristup:
Black Box – bez ikakvih internih informacija
White Box – sa potpunim uvidom
Gray Box – delimičan uvid u sistem

Prikupljaju se javno dostupne informacije o cilju (npr. IP adrese, detalji vezani za domen, Email, opis mrežne topologije, vrsta sistema koja je izabrana za metu)

SKENIRANJE

Interakcija sa metom

Napadač stupa u interakciju sa metom kako bi započeo proces identifikacije ranjivosti u konfiguraciji servera, mrežnoj infrastrukturi i aplikaciji

Skeniranje mreže i servisa

Specijalizovani alati se koriste za prikupljanje informacija o deljenim folderima, otvorenim portovima i servisima koji se izvršavaju.

Statičko skeniranje web aplikacije

Analiza koda bez izvršavanja se koristi za otkrivanje ranjivih biblioteka, pogrešno implementirane funkcije i slabosti u implementacionoj logici.

Dinamičko skeniranje web aplikacije

Izvršavanje aplikacije u realnom vremenu sa prosleđivanjem različitih ulaznih parametara kako bi se pratilo ponašanje aplikacije u cilju detektovanja anomalija i nepredviđene reakcije na ulaze ((npr. XSS, SQLi))

EKSPLOATACIJA

Cilj ove faze je da se proveri da li se prethodno otkrivene ranjivosti **mogu praktično iskoristiti** za kompromitaciju sistema, aplikacije ili mreže.

Izvršavanje napada

Izvođenje specifičnih napada na osnovu prikupljenih informacija

Dobijanje neovlašćenog pristupa

Uspešno prodiranje u sistem

Eskalacija privilegija

Povećanje nivoa pristupa u sistemu

Eksfiltracija podataka

Izvlačenje osetljivih informacija iz sistema

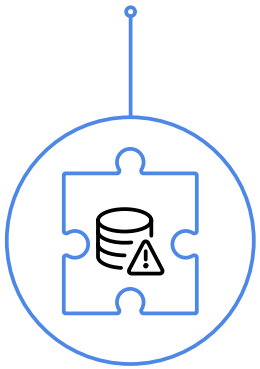
Narušavanje funkcionalnosti sistema

Važno je da se napad izvede kontrolisano i bez nanošenja trajne štete sistemu.

TEHNIKE U EKSPLOATACIJI SISTEMA

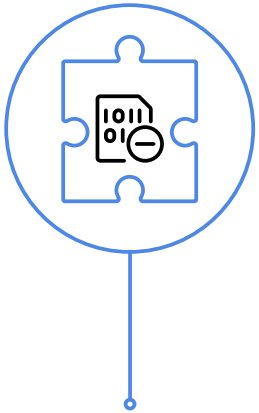
SQL injekcija

Ubrizgavanje zlonamernih SQL naredbi da bi se pristupilo bazama podataka.



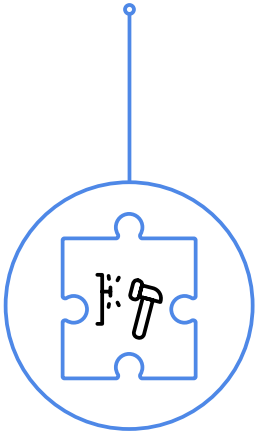
Prelivanje bafera

Iskorišćavanje grešaka u memoriji za izvršavanje proizvoljnog koda.



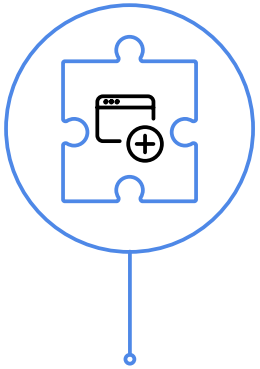
Brute Force

Pokušaji pogađanja lozinki automatskim alatima.



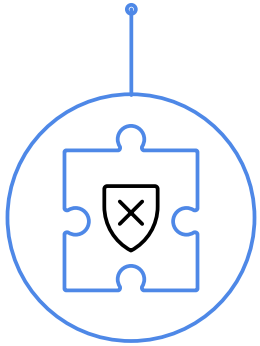
Cross-Site Scripting

Ubacivanje zlonamernog JavaScript koda u web aplikacije.



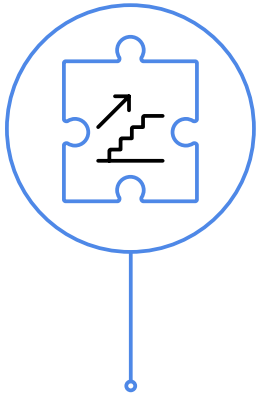
Iskorišćavanje javno poznatih ranjivosti

Korišćenje javno poznatih ranjivosti, kao što su Log4Shell.



Eskalacija privilegija

Dobijanje viših nivoa pristupa nego što je inicijalno dozvoljeno.



ANALIZA RIZIKA I PREDLOZI
- Dokumentacija napada -

Rezultati napada

Konkretni rezultati napada se dokumentuju(screenshot-ovi, logovi, shell pristupi, izlazi komandi).

Prilozi

Prilozi služe kao dokaz o kompromitaciji sistema. Ovo uključuje kompromitaciju aplikacije ili mreže.

ANALIZA RIZIKA I PREDLOZI
- Kategorizacija rizika -

Svi identifikovani bezbednosni propusti se klasifikuju po nivou rizika:

Kritični rizik

Direktna kompromitacija sistema sa potpunim pristupom.

Visok rizik

Visok uticaj na bezbednost, zahteva ispunjenje specifičnih uslova za eksploataciju.

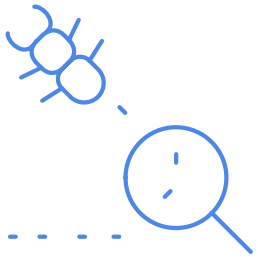
Srednji rizik

Potencijalna pretnja koja zahteva više koraka. Može se iskoristiti u kombinaciji sa drugim ranjivostima.

Nizak rizik

Nizak rizik, obično bez direktnog uticaja. Pretežno informativnog karaktera.

ANALIZA RIZIKA I PREDLOZI
- Izveštavanje klijenta -



Opis ranjivosti

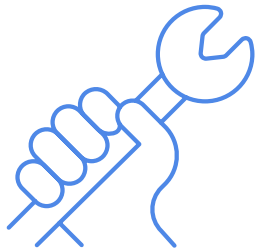
Detaljno objašnjenje sigurnosne greške.

Nivo rizika

Ocena ozbiljnosti identifikovane ranjivosti.

Dokaz

Dokaz koncepta koji demonstrira ranjivost.



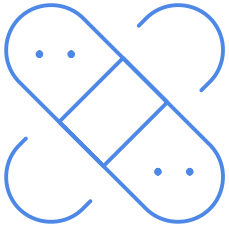
Predlog za rešavanje

Preporučeni koraci za ispravku sigurnosnog problema

ANALIZA RIZIKA I PREDLOZI
- Korektivne mere-

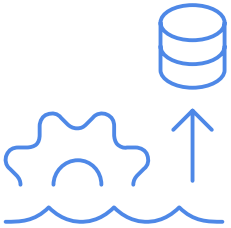
Preporuke za unapređenje bezbednosti

Izrada preporuka za unapređenje bezbednosti sistema.



Patch-ovanje

Primena potrebnih zakrpa za rešavanje ranjivosti.



Promena konfiguracije

Modifikovanje podešavanja za poboljšanje bezbednosnog stava.

Dodatne kontrole

Uvođenje dodatnih bezbednosnih mera kao što je WAF.

FINALNI IZVEŠTAJ

Otkrivene ranjivosti u sistemu

Detaljan spisak, tehnički opisi i klasifikacija ranjivosti prema nivou rizika.

Eksploatacija otkrivenih ranjivosti

Dokaz o mogućnosti iskorišćavanja ranjivosti kroz simulirane napade.

Izveštaj o sprovedenim testovima

Metodologija testiranja i korišćeni alati sa granicama testiranja.

Predlog za otklanjanje ranjivosti

Korektivne mere i preporučene politike za svaku ranjivost.