Intelsentrix

UAB "Pavyzdine imone"

Įsilaužimo testavimo ataskaita

Web, API, mobile aplikacijų, kodo ir tinklo saugumo vertinimas

PARENGĖ
Mantas Sabeckis, MB "Otterly"

VERTINIMO PERIODAS
2026-06-01 - 2026-06-08

ATASKAITOS DATA
2026-06-08

Turinys

Pranešimas ir kontaktai

Pranešimas

Dokumente pateikiama informacija turi būti laikoma konfidencialia, kai ji naudojama realiame projekte, nes joje gali būti sistemos architektūros, pažeidžiamumų ir atkūrimo žingsnių.

Saugumo vertinimas yra skirtas konkrečiam laiko momentui. Radiniai ir rekomendacijos atspindi vertinimo metu surinktą informaciją, sutartą apimtį ir turėtas prieigas. Tai negarantuoja, kad po vertinimo sistemoje neatsiras naujų pažeidžiamumų.

Visi testavimo veiksmai realiame projekte turi būti atliekami tik gavus aiškų užsakovo leidimą, sutartus testavimo langus ir patvirtintą apimtį. Jei atliekamas pakartotinis testavimas, jo rezultatai pateikiami atskirame taisymo statuso skyriuje.

Kontaktai

Vardas	Pareigos	Kontaktai
Mantas Sabeckis	Saugumo testavimo vadovas	info@otterly.lt
Jonas Jonaitis	Generalinis direktorius	jonas.jonaitis@pavyzdys.lt
Joana Jonaitienė	Techninė vadovė	joana.jonaitiene@pavyzdys.lt

Rezultatų santrauka

Apžvalga

UAB "Pavyzdine imone" užsakė Manto Sabeckio, MB "Otterly", atliekamą web aplikacijų, API, mobiliųjų aplikacijų, kodo ir tinklo saugumo vertinimą. Vertinimo tikslas buvo patikrinti sutartoje apimtyje esančias sistemas iš realaus užpuoliko perspektyvos ir nustatyti, ar per aplikacijas, API, mobilias aplikacijas, kodą ar palaikančią infrastruktūrą būtų galima gauti neteisėtą prieigą prie sistemų, duomenų ar jautrių funkcijų.

Vertinimas atliktas mišriu metodu: web, API, mobile ir tinklo dalims taikytas ribotos informacijos, tikslais paremtas testavimas, o kodo daliai - whitebox peržiūra su sutarta prieiga prie repozitorijos arba kodo failų. Tokia kombinacija leido vertinti tiek išorėje matomus atakos scenarijus, tiek vidinę autentifikacijos, autorizacijos, duomenų apdorojimo, konfigūracijų ir kitų jautrių funkcijų logiką.

Šio vertinimo rezultatai parodo, kokiu mastu sutartoje apimtyje esančios sistemos galėtų būti paveiktos saugumo spragų. Visi radiniai dokumente klasifikuojami pagal techninį išnaudojamumą, poveikį verslui ir taisymo prioritetą, kad užsakovo komanda galėtų aiškiai planuoti tolimesnius veiksmus.

Darbų apimtis

Sritis	Apimtis	Pastabos
Web	1 klientų portalas, 1 CRM sistema, 1 administravimo panelė	Blackbox ir autentifikuotas testavimas
API	1 REST API, 42 endpointai, 4 naudotojų rolės	OWASP API Security Top 10 scenarijai
Mobile	1 iOS ir 1 Android aplikacija	Statinė ir dinaminė aplikacijos analizė
Kodas	3 kodo repozitorijos: CRM, Dashboard, admin	Whitebox peržiūra pagal sutartą kodo apimtį
Tinklas	10 išorinių IP adresų, 23 vidiniai IP adresai	Išorinio ir vidinio tinklo mazgų testavimas

Naudoti įrankiai

Kategorija	Įrankiai
Web / API	Burp Suite Professional, Acunetix, ffuf, sqlmap, asmeniniai skriptai
Tinklas	Nmap, nuclei ir Nessus
Mobile	MobSF, Frida, apktool, proxy įrankiai
Kodas	Semgrep, Gitleaks, Trufflehog

Rezultatų vertinimo metodika

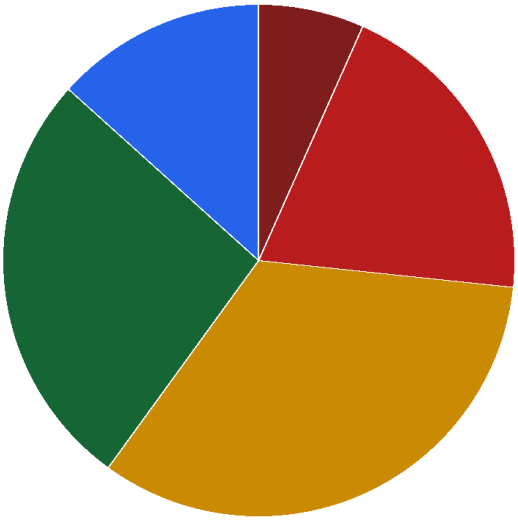
Radiniai vertinami ir prioritizuojami pagal kontekstą: techninį išnaudojamumą, poveikį verslui, paveiktų duomenų jautrumą, pasiekiamumą, turimas prieigas ir realaus atakos scenarijaus tikimybę. Pradiniam sunkumo lygiui nustatyti naudojama CVSS skaičiuoklė, o galutinis prioritetas koreguojamas pagal sutartą sistemos apimtį ir praktinį išnaudojimo scenarijų.

Rizika	Aprašymas
Kritinė	Radinys kelia tiesioginę ir neatidėliotiną riziką kritinėms sistemoms, jautriems duomenims, infrastruktūrai, kodui arba verslo operacijoms. Išnaudojimas gali lemti visišką sistemos, aplikacijos, API, paskyros, serverio ar tinklo segmento kompromitavimą, reikšmingą duomenų praradimą, veiklos sutrikdymą arba reputacinę žalą. Tokiems radiniams reikalingas neatidėliotinas dėmesys ir taisymas.
Aukšta	Radinys gali lemti neteisėtą prieigą prie sistemų, aplikacijų, API, tinklo mazgų, kodo artefaktų arba konfidencialių duomenų. Į šį lygį patenka radiniai, kurie gali sudaryti sąlygas privilegijų eskalavimui, nuotoliniam kodo vykdymui, reikšmingam duomenų atskleidimui, jautrių funkcijų piktnaudžiavimui arba svarbiam atitikties pažeidimui. Tokie radiniai turi būti taisomi aukštu prioritetu.
Vidutinė	Radinys dažniausiai nesukuria tiesioginio ir pilno kompromitavimo vienas pats, tačiau gali būti sujungtas su kitais pažeidžiamumais, konfigūracijos trūkumais ar silpna prieigos kontrole. Tokia kombinacija gali padėti pasiekti sistemas, hostus, aplikacijas, API, vidinius tinklo resursus arba konfidencialius duomenis. Šiuos radinius verta taisyti laiku, kad nebūtų sukurtas stipresnis atakos scenarijus.
Žema	Radinys turi ribotą tiesioginį poveikį, tačiau gali atskleisti techninę, konfigūracinę, verslo logikos arba infrastruktūros informaciją, kuri padeda pasiruošti tolimesnei atakai. Taip pat tai gali būti procesas, kontrolė ar saugumo praktika, kurią pagerinus sumažėja bendra rizika. Tokius radinius verta taisyti po kritinių, aukštų ir vidutinių radinių.
Informacinė	Radinys paprastai nėra savarankiška pažeidžiamumo rizika, tačiau veikia kaip rekomendacija, padedanti pagerinti sistemos, kodo, tinklo arba proceso saugumo brandą. Kai kuriais atvejais tokia informacija gali padėti užpuolikui geriau suprasti aplikacijos logiką, API struktūrą, infrastruktūrą ar naudojamas technologijas. Šiuos punktus verta peržiūrėti po aukštesnio prioriteto radinių sutvarkymo.

Radinių santrauka

Pagal sunkumą

Iš viso: 15



Kritinė	1 (7%)
Aukšta	3 (20%)
Vidutinė	5 (33%)
Žema	4 (27%)
Informacinė	2 (13%)

Pagal sritį

Iš viso: 15

API	3 (20%)
WEB	3 (20%)
MOBILE	3 (20%)
CODE	3 (20%)
NETWORK	3 (20%)

Saugumo rizikos

- Neteisėta prieiga prie kitų naudotojų arba organizacijų duomenų dėl prieigos kontrolės trūkumų.
- Galimas jautrių duomenų nuskaitymas arba duomenų bazės veikimo trikdymas per injection tipo pažeidžiamumus.
- Padidėjusi pradinės prieigos prie infrastruktūros rizika dėl pažeidžiamų VPN paslaugų arba per plačiai pasiekiamų administravimo sąsajų.
- Sesijų, tokenų arba prisijungimų perėmimas dėl silpno sesijų valdymo ir mobilios aplikacijos saugojimo trūkumų.
- Dėl nesaugių kodo sprendimų arba netinkamos konfigūracijos gali būti atskleisti slapti raktai, silpnai apsaugotos jautrios funkcijos arba sudarytos sąlygos tolimesniam sistemos kompromitavimui.

Aukšto lygio rekomendacijos

- Sustiprinti autorizacijos ir objektų nuosavybės patikras serverio pusėje, kad naudotojai galėtų pasiekti tik jiems priklausančius duomenis ir funkcijas.
- Sutvarkyti injection rizikas: validuoti įvestis, naudoti saugias užklausų konstravimo praktikas ir peržiūrėti jautrių endpointų duomenų apdorojimą.
- Sumažinti išorinį atakos paviršių: apriboti administravimo servisų pasiekiamumą, atnaujinti pažeidžiamas paslaugas, įjungti MFA ir reguliariai peržiūrėti viešus bei vidinius tinklo mazgus.
- Sustiprinti sesijų, tokenų ir prisijungimų apsaugą: naudoti saugų saugojimą, trumpesnį galiojimą, rotaciją ir serverio pusės sesijų anuliavimą.
- Peržiūrėti kodo ir konfigūracijų valdymą: pašalinti slaptus raktus iš kodo, naudoti saugią konfigūracijų saugyklą ir įtraukti jautrių funkcijų peržiūrą į release procesą.

Išvada

Bendra vertinimo rizika yra kritinė, nes identifikuotas SQL injekcijos radinys gali lemti jautrių duomenų nuskaitymą arba duomenų bazės veikimo trikdymą, o kiti aukšti ir vidutiniai radiniai didina neteisėtos prieigos, jautrių funkcijų piktnaudžiavimo ir tolimesnių atakos scenarijų riziką. Norint sumažinti šią riziką, rekomenduojama vadovautis aukščiau pateiktomis rekomendacijomis, pirmiausia taisyti kritinius ir aukštus radinius, o po pataisymų atlikti pakartotinį testavimą.

Detalūs radiniai

R-01 [API] Laiko pagrindu patvirtinama SQL injekcija API paieškoje

Paveikta sritis: Dashboard API, /api/v1/search

Rizika: Kritinė

CVSS balas: 8.8

Santrauka

API priima vartotojo perduodamą paieškos parametrą ir perduoda jį į duomenų bazės užklausą be pakankamos parametrizacijos. Testo metu pavyko patvirtinti laiko pagrindu veikiančią SQL injekciją naudojant saugų testą.

Poveikis

Užpuolikas gali bandyti skaityti jautrius duomenis, išgauti duomenų bazės struktūros informaciją arba sukelti papildomą sistemos apkrovimą. Realus poveikis priklauso nuo duomenų bazės naudotojo teisių ir papildomų kontrolės priemonių.

Atkūrimo žingsniai

1. Prisijungti prie testinės API aplinkos su įprasto naudotojo teisėmis.
2. Išsiųsti POST užklausą į paieškos endpointą su specialiai suformuotu parametru.

```
POST /api/v1/search
{
  "query": "test' AND 1=(SELECT 1 FROM pg_sleep(5))--",
  "page": 1
}
```

3. Palyginti įprastą užklausą ir užklausą su uždelstu atsaku.
4. Patvirtinti, kad atsako laikas padidėja pagal pateiktą uždelsimą, o tai rodo SQL užklausos įvykdymą.

Rekomendacija

Visas duomenų bazės užklausas perrašyti naudojant parametrizuotas užklausas arba ORM saugius parametrus. Papildomai riboti įvesties formatą, peržiūrėti panašius endpointus ir pridėti regresinius testus.

R-02 [WEB] Autorizacijos apėjimas administravimo funkcijoje

Paveikta sritis: Administravimo panelė

Rizika: Aukšta

CVSS balas: 8.8

Santrauka

Administravimo funkcija patikrina, ar naudotojas yra prisijungęs, tačiau nepakankamai tikrina konkrečios rolės arba teisės turėjimą. Dėl to žemesnių teisių naudotojas gali pasiekti veiksmus, kurie turėtų būti leidžiami tik administratoriui.

Pažeistos vietos

- PATCH /admin/users/{user_id}/role
- POST /admin/users/{user_id}/disable
- DELETE /admin/users/{user_id}
- POST /admin/organizations/{organization_id}/settings
- GET /admin/audit-log/export

Poveikis

Galimas duomenų keitimas, vartotojų valdymas, konfigūracijų modifikavimas arba kiti verslui jautrūs veiksmai be tinkamo leidimo.

Atkūrimo žingsniai

1. Prisijungti kaip naudotojas su administratoriaus teisėmis.
2. Perimti administratoriaus veiksmui skirtą HTTP užklausą.

```
PATCH /admin/users/{user_id}/role
Authorization: Bearer <low_privileged_user_token>

{
  "role": "admin"
}
```

3. Pakartoti užklausą su žemesnių teisių naudotojo sesija.
4. Patvirtinti, kad sistema leidžia atlikti veiksmą nepaisant trūkstamos rolės.

Rekomendacija

Visuose jautriuose veiksmuose tikrinti ne tik autentifikaciją, bet ir konkrečias teises serverio pusėje. Įvesti centralizuotą autorizacijos sluoksnį ir testus kiekvienai rolei.

R-03 [NETWORK] Viešai pasiekiama VPN paslauga su žinomu pažeidžiamumu

Paveikta sritis: VPN Gateway, vpn.example.lt:443

Rizika: Aukšta

CVSS balas: 8.8

Santrauka

Išoriniame perimetre aptikta VPN paslauga, kurios versija siejama su viešai žinomu aukštos rizikos pažeidžiamumu. Paslauga pasiekiama iš interneto ir neturi papildomo IP ribojimo.

Poveikis

Sėkmingai išnaudojus pažeidžiamumą užpuolikas gali gauti pradinę prieigą arba sukurti sąlygas tolimesniam judėjimui vidiniame tinkle. Rizika priklauso nuo konkretaus pažeidžiamumo išnaudojimo sąlygų ir papildomų apsaugos priemonių.

Atkūrimo žingsniai

1. Atlikti išorinio perimetro portų ir servisų skenavimą.
2. Identifikuoti VPN paslaugos produktą ir versiją.

```
vpn.example.lt:443
Service: ExampleVPN Gateway
Detected version: ExampleVPN Gateway 8.2.1
```

3. Sulyginti versiją su viešomis CVE duomenų bazėmis ir gamintojo saugumo pranešimais.
4. Patikrinti, ar paslauga pasiekiama be IP allowlist arba papildomos apsaugos.

Rekomendacija

Skubiai atnaujinti VPN komponentą, apriboti prieigą pagal IP, įjungti MFA, peržiūrėti paskutinius prisijungimus ir patikrinti, ar nėra kompromitavimo požymių.

R-04 [API] Prieigos kontrolės pažeidimas leidžia pasiekti kito naudotojo įrašus

Paveikta sritis: User Documents API, /api/v1/users/{id}/documents

Rizika: Aukšta

CVSS balas: 8.1

Santrauka

API endpointai leidžia keisti objekto identifikatorių ir ne visada patikrina, ar objektas priklauso prisijungusiam naudotojui. Tai atitinka IDOR / broken access control scenarijų.

Poveikis

Užpuolikas gali pasiekti arba pakeisti kitų naudotojų įrašus, užsakymus, failus, mokėjimo informaciją arba kitus jautrius objektus.

Atkūrimo žingsniai

1. Prisijungti kaip naudotojas A ir gauti savo objekto identifikatorių.
2. Prisijungti kaip naudotojas B arba naudoti kitą žinomą objekto ID.

```
GET /api/v1/users/{other_user_id}/documents
Authorization: Bearer <user_a_token>
```

3. Pakeisti objekto ID užklausoje ir stebėti, ar API grąžina arba pakeičia svetimus duomenis.

Rekomendacija

Kiekviename endpointo veiksme tikrinti objekto nuosavybę ir leidimus serverio pusėje. Atskirti globalius ID nuo naudotojui pasiekiamų objektų sąrašų ir pridėti neigiamus autorizacijos testus.

R-05 [WEB] Nesaugus failų įkėlimas leidžia talpinti pavojingus failus

Paveikta sritis: Failų įkėlimo funkcijos

Rizika: Vidutinė

CVSS balas: 6.1

Santrauka

Failų įkėlimo funkcija nepakankamai tikrina failo tipą, turinį ir pavadinimą. Kai kurie įkėlimo endpointai leidžia pateikti pavojingus plėtinius arba manipuliuoti failo keliu.

Pažeistos vietos

- POST /api/v1/files/upload
- POST /api/v1/profile/avatar
- POST /api/v1/messages/{message_id}/attachments
- PUT /api/v1/files/{file_id}
- GET /uploads/{filename}

Poveikis

Sistema gali būti naudojama nepageidaujamų failų talpinimui, phishing scenarijams, saugyklos užteršimui arba ribotai kelio manipuliacijai, jei nėra papildomų kontrolės priemonių.

Atkūrimo žingsniai

1. Į failų įkėlimo funkciją pateikti failą su pavojingu plėtiniu.
2. Pakeisti failo pavadinimą į reikšmę su specialiais simboliais arba kelio sekomis.

```
POST /api/v1/files/upload
filename=../sample.html
content-type=text/html
```

3. Patikrinti, ar serveris priima failą ir grąžina viešai pasiekiamą nuorodą.

Rekomendacija

Naudoti leidžiamų plėtinių ir MIME tipų sąrašą, tikrinti failo turinį, generuoti saugius pavadinimus, saugoti failus ne web root direktorijoje ir apriboti viešą prieigą.

R-06 [WEB] Stored XSS profilio URL lauke

Paveikta sritis: Profilio URL laukas ir administravimo peržiūros puslapis

Rizika: Vidutinė

CVSS balas: 6.1

Santrauka

Serveris leidžia išsaugoti profilio URL reikšmę su javascript schema, o administravimo peržiūros puslapyje ši reikšmė atvaizduojama kaip aktyvi nuoroda be pakankamos serverio pusės validacijos. Testavimo metu pavyko patvirtinti stored XSS scenarijų administravimo panelėje.

Poveikis

Užpuolikas gali išsaugoti kenkėjišką profilio nuorodą, kuri įvykdoma administratoriui peržiūrint naudotojo profilį. Priklausomai nuo sesijos apsaugos ir naršyklės kontrolės priemonių, tai gali leisti atlikti veiksmus administratoriaus naršyklės kontekste arba pavogti jautrią informaciją iš puslapio.

Atkūrimo žingsniai

1. Prisijungti kaip įprastas naudotojas ir atnaujinti profilio URL lauką per API.
2. Pateikti javascript schema paremtą reikšmę profilio URL lauke.

```
PATCH /api/v1/profile
{
  "website_url": "javascript:alert(document.domain)"
}
```

3. Prisijungti prie administravimo panelės ir atidaryti naudotojo profilio peržiūros puslapį.
4. Patvirtinti, kad naršyklėje įvykdomas pateiktas JavaScript kodas.

Rekomendacija

Validuoti URL serverio pusėje ir leisti tik aiškiai apibrėžtas schemas, pvz., HTTPS. Administravimo panelėje visas naudotojo pateiktas reikšmes atvaizduoti su kontekstui tinkamu escaping ir nenaudoti pavojingų schemų aktyvioms nuorodoms.

R-07 [CODE] AWS prieigos raktas aptiktas kodo repozitorijoje

Paveikta sritis: Backend repozitorija

Rizika: Vidutinė

CVSS balas: 5.9

Santrauka

Kodo repozitorijoje aptiktas AWS Access Key ID, prasidedantis prefiksu AKIA. Testavimo metu nebuvo atliekamas rakto aktyvumo ar teisių validavimas, tačiau tokio tipo reikšmė kode rodo galimą cloud prieigos rakto nutekėjimą.

Poveikis

Jei susijęs slaptasis raktas yra aktyvus ir turi reikšmingas teises, užpuolikas galėtų pasiekti AWS resursus, skaityti arba keisti duomenis, kurti papildomus resursus arba sukelti finansinę žalą. Rizika vertinama kaip vidutinė, nes raktas aptiktas privačioje repozitorijoje, o ne viešai pasiekiamame kode. Realus poveikis priklauso nuo rakto aktyvumo, IAM teisių ir papildomų AWS kontrolės priemonių.

Atkūrimo žingsniai

1. Atlikti repozitorijos ir git istorijos peržiūrą su secrets aptikimo įrankiais.
2. Identifikuoti AWS Access Key ID reikšmę, prasidedančią AKIA prefiksu.

```
AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
```

3. Patikrinti, kuriame faile ir commite reikšmė buvo įkelta.
4. Patikrinti, ar ta pati reikšmė nėra naudojama CI/CD konfigūracijoje arba aplinkos failuose.

Rekomendacija

Nedelsiant patikrinti rakto aktyvumą AWS IAM aplinkoje, rotuoti arba panaikinti paveiktą raktą, peržiūrėti jo naudojimo istoriją CloudTrail žurnaluose ir pašalinti reikšmę iš repozitorijos bei jos istorijos. Papildomai įdiegti pre-commit ir CI secrets patikras.

R-08 [MOBILE] Sesijos duomenys saugomi išorinėje įrenginio saugykloje

Paveikta sritis: Mobilios aplikacijos SD card saugykla

Rizika: Vidutinė

CVSS balas: 5.5

Santrauka

Mobilioji aplikacija išsaugo sesijos duomenis išorinėje įrenginio saugykloje, kuri gali būti pasiekiama plačiau nei privati aplikacijos saugykla. Testavimo metu sesijos failas aptiktas SD card tipo saugyklos kelyje.

Poveikis

Jei įrenginys kompromituotas, prijungtas prie nepatikimos aplinkos arba kita aplikacija turi prieigą prie išorinės saugyklos, sesijos duomenys gali būti nuskaityti ir panaudoti tolimesnei paskyros analizei ar perėmimo bandymams.

Atkūrimo žingsniai

1. Prisijungti prie mobilios aplikacijos testiniame įrenginyje.
2. Patikrinti išorinės saugyklos katalogus ir aplikacijos sukurtus failus.

```
/sdcard/Android/data/com.example.app/files/session.json
{
  "session_token": "eyJhbGciOiJIUzI1NiIs..."
}
```

3. Identifikuoti SD card tipo saugykloje išsaugotus sesijos duomenis.

Rekomendacija

Sesijos duomenis saugoti tik privačioje aplikacijos saugykloje arba platformos saugioje saugykloje, nenaudoti išorinės SD card tipo saugyklos jautriems duomenims ir išvalyti sesijos failus atsijungus.

R-09 [CODE] Sesija neanuliuojama serverio pusėje atsijungus

Paveikta sritis: AuthService atsijungimo funkcija

Rizika: Vidutinė

CVSS balas: 5.3

Santrauka

Atsijungimo funkcija pašalina kliento pusės slapuką arba tokeną, tačiau serverio pusėje sesija išlieka aktyvi iki numatyto galiojimo pabaigos.

Poveikis

Jei sesijos tokenas pavagiamas, užpuolikas gali tęsti prisijungusio naudotojo veiksmus net po to, kai naudotojas atsijungia.

Atkūrimo žingsniai

1. Prisijungti ir išsisaugoti sesijos slapuko arba tokeno reikšmę.
2. Atsijungti per aplikacijos funkciją.

```
GET /api/v1/me
Cookie: session=<old_session_after_logout>
```

3. Pakartoti autentifikuotą API užklausą naudojant seną sesijos reikšmę.
4. Patvirtinti, kad serveris vis dar priima seną sesiją.

Rekomendacija

Atsijungimo metu anuliuoti sesiją serverio pusėje, trumpinti sesijos galiojimą, įdiegti refresh token rotaciją ir numatyti kompromituotų sesijų atšaukimo mechanizmą.

R-10 [API] Nepakankamas užklausų ribojimas jautriuose endpointuose

Paveikta sritis: Auth API, /login ir /verify-code

Rizika: Žema

CVSS balas: 3.5

Santrauka

Keli API endpointai priima daug kartotinių užklausų iš tos pačios sesijos arba IP adreso be efektyvaus rate limiting mechanizmo.

Poveikis

Radinys pats savaime nesuteikia neteisėtos prieigos, tačiau gali palengvinti automatizuotus bandymus, vienkartinių kodų spėjimą, el. laiškų siuntimo piktnaudžiavimą arba papildomą infrastruktūros apkrovą.

Atkūrimo žingsniai

1. Pasirinkti jautrų endpointą, pvz., prisijungimą arba kodo validaciją.
2. Išsiųsti seriją užklausų per trumpą laiką.
3. Patikrinti, ar sistema pradeda riboti bandymus arba grąžina apsaugos atsaką.

Rekomendacija

Įdiegti IP, paskyros ir endpointo lygio ribojimus, progresyvų cooldown, audit logs ir įspėjimus apie anomalijas.

R-11 [CODE] Slaptažodžiai saugomi atviru tekstu

Paveikta sritis: AuthService legacy importo funkcija

Rizika: Žema

CVSS balas: 3.3

Santrauka

Kodo peržiūros metu nustatyta, kad legacy importo funkcija laikinai išsaugo pradinius slaptažodžius atviru tekstu. Funkcija nėra tiesiogiai pasiekiama iš interneto, tačiau tokia praktika didina riziką incidento, klaidingos konfigūracijos arba atsarginių kopijų nutekėjimo atveju.

Poveikis

Jei šie duomenys būtų išsaugoti produkcinėje bazėje, loguose arba atsarginėse kopijose, ribotas naudotojų kiekis galėtų būti paveiktas. Rizika vertinama kaip žema dėl ribotos apimties ir papildomų sąlygų, reikalingų realiam išnaudojimui.

Atkūrimo žingsniai

1. Peržiūrėti legacy naudotojų importo funkciją ir su ja susijusį duomenų modelį.
2. Patikrinti, ar pradinis slaptažodis prieš saugojimą perduodamas per saugų hashing mechanizmą.

```
legacy_import.initial_password = "DemoSlaptazodis123"
```

3. Patvirtinti, kad importo lentelėje slaptažodžio reikšmė išlieka perskaitoma.

Rekomendacija

Pašalinti atviru tekstu saugomų slaptažodžių lauką, pradinius slaptažodžius generuoti tik vienkartiniam perdavimui, o visus saugomus slaptažodžius apdoroti su bcrypt, Argon2id arba kitu slaptažodžiams skirtu algoritmu.

R-12 [NETWORK] Atviras administravimo servisas be papildomos prieigos kontrolės

Paveikta sritis: Administravimo portalas, admin.example.lt

Rizika: Žema

CVSS balas: 3.1

Santrauka

Viešame internete pasiekiamas administravimo prisijungimo puslapis. Testavimo metu nebuvo patvirtintas autentifikacijos apėjimas ar kitas tiesioginis išnaudojimo scenarijus, tačiau toks pasiekiamumas didina išorinį atakos paviršių.

Poveikis

Radinys pats savaime nesuteikia prieigos prie sistemos, tačiau administravimo sąsaja gali tapti papildomu taikiniu slaptažodžių spėjimui, socialinės inžinerijos scenarijams arba ateityje atsirasiantiems produkto pažeidžiamumams.

Atkūrimo žingsniai

1. Atlikti subdomenų ir portų skenavimą.
2. Identifikuoti administravimo panelę pagal HTTP atsakymus ir pavadinimą.

```
https://admin.example.lt/login
```

3. Patikrinti, ar servisas pasiekiamas iš viešo interneto be IP ribojimų.

Rekomendacija

Administravimo servisą perkelti už VPN arba IP allowlist, įjungti MFA, riboti prisijungimų bandymus ir stebėti anomalius prisijungimus.

R-13 [MOBILE] Debug funkcijos paliktos produkcinėje mobilios aplikacijos versijoje

Paveikta sritis: Mobile aplikacijos release build

Rizika: Žema

CVSS balas: 3.1

Santrauka

Produkcinėje aplikacijos versijoje aptikti debug nustatymai arba diagnostikos funkcijos, kurios neturėtų būti aktyvios galutiniame build'e.

Poveikis

Tai gali palengvinti aplikacijos analizę, informacijos rinkimą arba vidinės logikos supratimą, ypač kartu su kitomis mobilios aplikacijos spragomis.

Atkūrimo žingsniai

1. Gauti produkcinį APK failą iš testavimo apimtyje sutartos aplikacijos versijos.
2. Išpakuoti APK ir peržiūrėti AndroidManifest.xml failą.

```
$ apktool d app-release.apk -o app-release
$ grep -n 'android:debuggable' app-release/AndroidManifest.xml
<application android:debuggable="true" ...>
```

3. Patvirtinti, kad application elemente nustatyta android:debuggable reikšmė yra true.

Rekomendacija

Išjungti debug nustatymus produkciniuose build'uose, atskirti debug ir release konfigūracijas ir CI/CD metu tikrinti build saugumo parametrus.

R-14 [MOBILE] Nėra certificate pinning jautriai API komunikacijai

Paveikta sritis: Mobile API komunikacija, api.example.lt

Rizika: Informacinė

Santrauka

Mobilioji aplikacija pasitiki įrenginio sertifikatų saugykla ir nenaudoja certificate pinning jautrioms API užklausoms. Testinėje aplinkoje tai leidžia perimti ir analizuoti srautą naudojant vartotojo įdiegtą sertifikatą.

Poveikis

Tai yra papildomos apsaugos rekomendacija jautriai mobile API komunikacijai. Radinys pats savaime nesuteikia prieigos prie sistemos ir paprastai reikalauja papildomų sąlygų, todėl vertinamas kaip informacinis.

Atkūrimo žingsniai

1. Į testinį įrenginį įdiegti proxy sertifikatą.
2. Nukreipti aplikacijos srautą per testavimo proxy.
3. Patikrinti, ar aplikacija leidžia sėkmingai vykdyti API užklausas per tarpinį proxy.

Rekomendacija

Jautriems API domenams įdiegti certificate pinning, numatyti saugų pin rotacijos procesą ir testuoti, kad pinning neveiktų debug build logikos pagrindu produkcinėje versijoje.

R-15 [NETWORK] TLS konfigūracijos trūkumai išoriniuose servisuose

Paveikta sritis: Vieši web ir API servisai

Rizika: Informacinė

Santrauka

Dalis išorinių servisų palaiko pasenusius TLS nustatymus arba neturi vienodai pritaikytų saugumo antraščių.

Poveikis

Tai nėra tiesiogiai išnaudojamas radinys šiame vertinime, tačiau konfigūracijos suvienodinimas pagerintų bendrą transporto sluoksnio saugumo kokybę ir sumažintų riziką specifinėse papildomų sąlygų reikalaujančiose situacijose.

Atkūrimo žingsniai

1. Atlikti TLS ir saugumo antraščių skenavimą išoriniams domenams.
2. Palyginti rezultatus su organizacijos standartu ir viešomis gerosiomis praktikomis.
3. Patikrinti, ar trūkumai kartojasi keliuose servisuose.

Rekomendacija

Suvienodinti TLS politiką, įjungti HSTS, išjungti pasenusius protokolus ir cipher suites, o pakeitimus patikrinti visose aplinkose.

Taisymo ir pakartotinio testavimo ataskaita

Ši dalis naudojama pataisymų planavimui ir pakartotiniam testavimui. Ji parodo radinių prioritetą, taisymo būseną ir sujungtas rizikas, kurias galima taisyti kaip bendras technines problemas.

Taisymo darbų suvestinė

ID	Tipas	Rizika	CVSS	Prior.	Būsena	Retest
R-01	API	**Kritinė**	8.8	**P1**	Atviras	Neatliktas
R-02	Web	**Aukšta**	8.8	**P2**	Atviras	Neatliktas
R-03	Tinklas	**Aukšta**	8.8	**P2**	Atviras	Neatliktas
R-04	API	**Aukšta**	8.1	**P2**	Atviras	Neatliktas
R-05	Web	**Vidutinė**	6.1	**P3**	Atviras	Neatliktas
R-06	Web	**Vidutinė**	6.1	**P3**	Atviras	Neatliktas
R-07	Kodas	**Vidutinė**	5.9	**P3**	Atviras	Neatliktas
R-08	Mobile	**Vidutinė**	5.5	**P3**	Atviras	Neatliktas
R-09	Kodas	**Vidutinė**	5.3	**P3**	Atviras	Neatliktas
R-10	API	**Žema**	3.5	**P4**	Atviras	Neatliktas
R-11	Kodas	**Žema**	3.3	**P4**	Atviras	Neatliktas
R-12	Tinklas	**Žema**	3.1	**P4**	Atviras	Neatliktas
R-13	Mobile	**Žema**	3.1	**P4**	Atviras	Neatliktas
R-14	Mobile	**Informacinė**	-	**P4**	Atviras	Neatliktas
R-15	Tinklas	**Informacinė**	-	**P4**	Atviras	Neatliktas

Prioritetų logika

Prioritetas	Taikoma	Rekomenduojamas veiksmas
P1	**Kritinė rizika**	Taisyti nedelsiant ir pakartotinai patikrinti pirmu prioritetu.
P2	**Aukšta rizika**	Planuoti taisymą artimiausiame release arba sprinto cikle.
P3	**Vidutinė rizika**	Įtraukti į saugumo backlog ir pataisyti pagal produkto riziką.
P4	**Žema / informacinė rizika**	Spręsti kaip hardening, techninės skolos arba proceso gerinimo darbus.

Detalus taisymo planas

Prior.	Bendra rizika	Kaip taisyti
P1	SQL injekcija ir duomenų bazės užklausų sauga Susiję: R-01	Perrašyti pažeidžiamas užklausas naudojant parametrizuotas užklausas arba ORM saugius parametrus. Peržiūrėti panašius paieškos ir filtravimo endpointus, pridėti regresinius testus ir riboti duomenų bazės naudotojo teises.
P2	Autorizacija, ACL ir objektų nuosavybė Susiję: R-02, R-04	Įdiegti centralizuotą autorizacijos sluoksnį, tikrinti konkrečias teises serverio pusėje ir kiekviename endpointo veiksme validuoti objekto priklausymą naudotojui arba organizacijai. Pridėti neigiamus testus kiekvienai rolei.
P2	Išorinis perimetras ir administravimo pasiekiamumas Susiję: R-03, R-12	Atnaujinti VPN komponentą, apriboti prieigą pagal IP arba VPN, įjungti MFA ir perkelti administravimo sąsajas už papildomos prieigos kontrolės. Peržiūrėti prisijungimų žurnalus ir reguliariai tikrinti viešą atakos paviršių.
P3	Naudotojo įvestis, failai ir XSS Susiję: R-05, R-06	Failams taikyti leidžiamų tipų sąrašą, tikrinti turinį, generuoti saugius pavadinimus ir saugoti failus ne web root direktorijoje. URL ir kitą naudotojo įvestį validuoti serverio pusėje, o administravimo panelėje atvaizduoti su kontekstui tinkamu escaping.
P3	Sesijos, slaptažodžiai ir jautrūs duomenys Susiję: R-08, R-09, R-11	Sesijos duomenis laikyti tik saugioje platformos arba privačioje aplikacijos saugykloje, atsijungimo metu anuliuoti sesijas serverio pusėje ir pašalinti atviru tekstu saugomų slaptažodžių laukus. Taikyti trumpesnį sesijų galiojimą ir saugų tokenų rotacijos procesą.
P3	Cloud prieigos raktų valdymas Susiję: R-07	Patikrinti AWS rakto aktyvumą, rotuoti arba panaikinti paveiktą raktą, peržiūrėti CloudTrail žurnalus ir pašalinti reikšmę iš repozitorijos istorijos. Įdiegti pre-commit ir CI secrets patikras bei naudoti secrets manager.
P4	Automatizuotų užklausų ribojimas Susiję: R-10	Įdiegti IP, paskyros ir endpointo lygio ribojimus, progresyvų cooldown, audit logs ir įspėjimus apie anomalijas. Ribojimus testuoti taip, kad nebūtų blokuojamas teisėtas naudotojų darbas.
P4	Mobile release hardening Susiję: R-13, R-14	Išjungti debug nustatymus produkciniuose build'uose ir CI/CD metu tikrinti release konfigūraciją. Certificate pinning vertinti kaip papildomą apsaugą jautriai API komunikacijai, ypač aplikacijoms su jautriais duomenimis.
P4	TLS ir transporto sluoksnio hardening Susiję: R-15	Suvienodinti TLS politiką, įjungti HSTS, išjungti pasenusius protokolus ir cipher suites, o pakeitimus patikrinti visose aplinkose.