4.6 security threat model

مدل تهدیدات امنیتی - ProDecks
نسخه: 1.0
تاریخ: 1403/11/16
وضعیت: MVP - تحلیل شده

فصل ۱: مرور کلی امنیت

هدف این سند .۱.۱

.و تعریف کنترل‌های لازم برای کاهش ریسک ProDecks شناسایی و تحلیل تهدیدات امنیتی احتمالی علیه سیستم

محدوده تحلیل .۱.۲

• شامل فرانت‌اند، بک‌اند و پایگاه داده ProDecks کل سیستم
• کلیه کاربران: اعضا، مدیران، مهمانان
• کلیه داده‌ها: کاربری، پروژه‌ای، مالی

مفروضات امنیتی .۱.۳

• زیرساخت میزبانی امن است
• توسعه‌دهندگان آموزش امنیتی دیده‌اند
• به‌روزرسانی‌های امنیتی به موقع اعمال می‌شوند

فصل ۲: دارایی‌های حیاتی

داده‌های حساس .۲.۱

• اطلاعات هویتی کاربران (ایمیل، نام، ...)
• داده‌های احراز هویت (رمز عبور، توکن‌ها hash)
• داده‌های پروژه (Spaces، Decks، کارت‌ها)
• داده‌های تحلیلی و رفتاری کاربران
• لاگ‌های سیستم

قابلیت‌های حیاتی .۲.۲

• سیستم احراز هویت
• سیستم دسترسی و مجوزها

سیستم پرداخت (آینده) •
و بازیابی backup سیستم •

زیرساخت حیاتی ۲.۳.

سرورهای پایگاه داده •
application سرورهای •
شبکه و ارتباطات •
backup سیستم‌های •

فصل ۳: پروفایل تهدید

مهاجمان بالقوه ۳.۱.

۱. هکر انفرادی (Script Kiddie)
انگیزه: شهرت، چالش •
سطح مهارت: پایین •
منابع: محدود •
احتمال: متوسط •

۲. هکر سازمان‌یافته
انگیزه: مالی، جاسوسی •
سطح مهارت: بالا •
منابع: زیاد •
احتمال: کم •

۳. کاربر مخرب داخلی
انگیزه: انتقام، سود شخصی •
سطح مهارت: متوسط •
منابع: دسترسی مجاز •
احتمال: کم •

۴. رقیب تجاری
انگیزه: کسب مزیت رقابتی •
سطح مهارت: بالا •
منابع: متوسط •
احتمال: کم •

۵. تهدیدات دولتی
انگیزه: نظارت، کنترل •
سطح مهارت: بسیار بالا •
منابع: بسیار زیاد •
احتمال: بسیار کم •

فصل ۴: سطوح حمله

سطح ۱: حمله از طریق اینترنت ۴.۱.

• Attack Vector: اینترنت عمومی
• دارایی‌های در معرض: سرورهای front-facing
• تهدیدات: DDoS، اسکن پورت، brute force

سطح ۲: حمله از طریق برنامه کاربردی ۴.۲.

• Attack Vector: APIهای وب، فرم‌ها
• دارایی‌های در معرض: application logic
• تهدیدات: SQL Injection، XSS، CSRF

سطح ۳: حمله از طریق احراز هویت ۴.۳.

• Attack Vector: سیستم login، توکن‌ها
• دارایی‌های در معرض: حساب کاربری
• تهدیدات: credential stuffing، session hijacking

سطح ۴: حمله از طریق داده‌ها ۴.۴.

• Attack Vector: uploadها، داده‌های ورودی
• دارایی‌های در معرض: پایگاه داده
• تهدیدات: data corruption، data theft

سطح ۵: حمله از طریق insider ۴.۵.

• Attack Vector: دسترسی داخلی
• دارایی‌های در معرض: تمام سیستم
• تهدیدات: data exfiltration، sabotage

فصل ۵: سناریوهای تهدید

سناریو ۱: سرقت اطلاعات کاربران ۵.۱.

.تهدید: حمله‌گر به پایگاه داده دسترسی پیدا می‌کند و اطلاعات کاربران را سرقت می‌کند
دارایی: اطلاعات کاربران
مهاجم: هکر سازمان‌یافته
احتمال: متوسط
تأثیر: بالا
کنترل‌ها: رمزنگاری داده، access control، monitoring

سناریو ۲: اختلال در سرویس ۵.۲.

.باعث از کار افتادن سرویس می‌شود DDoS تهدید: حمله
دارایی: دسترسی پذیری سرویس
مهاجم: هکر انفرادی
احتمال: بالا
تأثیر: متوسط
کنترل‌ها: DDoS protection، load balancing، auto-scaling

سناریو ۳: دسترسی غیرمجاز ۵.۳.

.تهدید: کاربری با دسترسی محدود، به داده‌های دیگر کاربران دسترسی پیدا می‌کند
دارایی: محرمانگی داده‌ها
مهاجم: کاربر داخلی
احتمال: متوسط
تأثیر: بالا
کنترل‌ها: authorization checks، audit logging

سناریو ۴: تزریق کد ۵.۴.

.تزریق می‌کند input fields تهدید: حمله‌گر کد مخرب را از طریق
دارایی: integrity سیستم
مهاجم: هکر انفرادی
احتمال: متوسط
تأثیر: بالا
کنترل‌ها: input validation، output escaping، WAF

سناریو ۵: سرقت session ۵.۵.

.کاربر را سرقت کرده و به حساب او دسترسی پیدا می‌کند session تهدید: حمله‌گر
دارایی: حساب کاربری
مهاجم: هکر انفرادی
احتمال: متوسط
تأثیر: متوسط
کنترل‌ها: secure session management، HTTPS، CSRF tokens

فصل ۶: کنترل‌های امنیتی

کنترل‌های پیشگیرانه ۶.۱.

۱. احراز هویت قوی
- رمز عبور پیچیده اجباری
- محدودیت تلاش برای ورود

• 2FA (در آینده)

۲. کنترل دسترسی

• Role-Based Access Control (RBAC)
• Least Privilege Principle
• Segregation of Duties

۳. امنیت برنامه

• Input Validation
• Output Encoding
• Prepared Statements

۴. رمزنگاری

• برای تمام ارتباطات HTTPS
• رمزنگاری داده‌های حساس
• مدیریت امن کلیدها

۶.۲. کنترل‌های تشخیصی

۱. مانیتورینگ

• لاگ‌گیری فعالیت‌های مهم
• Real-time monitoring
• Alerting برای فعالیت‌های مشکوک

۲. Audit Logging

• لاگ تمام تغییرات مهم
• نگهداری لاگ‌ها به مدت ۱ سال
• تحلیل دوره‌ای لاگ‌ها

۳. سیستم تشخیص نفوذ

• Network IDS
• Host-based IDS
• Application-level monitoring

۶.۳. کنترل‌های اصلاحی

۱. Incident Response Plan

• فرآیند پاسخ به حوادث
• تیم پاسخ‌گویی
• communication plan

۲. Backup و Recovery

• backup روزانه
• recovery تست دوره‌ای
• disaster recovery plan

۳. Patch Management

• به‌روزرسانی منظم

• vulnerability scanning
• emergency patching

فصل ۷: امنیت برنامه کاربردی

امنیت احراز هویت ۷.۱.

• استفاده از bcrypt برای hash کردن رمز عبور
• session management امن
• جلوگیری از session fixation
• timeout خودکار session

امنیت authorization ۷.۲.

• بررسی مجوز در هر سطح
• پیش‌فرض: deny all
• context-aware authorization

امنیت داده‌های ورودی ۷.۳.

• validation در client و server
• sanitization قبل از پردازش
• محدودیت حجم و نوع input

امنیت ارتباطات ۷.۴.

• TLS 1.2+ برای تمام ارتباطات
• HSTS implementation
• certificate management

فصل ۸: امنیت زیرساخت

امنیت شبکه ۸.۱.

• فایروال برای تمام سرورها
• segmentation شبکه
• DDoS protection

امنیت سرورها ۸.۲.

• hardening سیستم عامل
• به‌روزرسانی منظم
• minimum installed software

امنیت پایگاه داده ۸.۳.

• encrypted connections

• encrypted data at rest
• access control دقیق

۸.۴. امنیت cloud

• secure configuration
• monitoring cloud resources
• backup در cloud

فصل ۹: مدیریت کلیدها و رمزنگاری

۹.۱. Key Management Policy

• جداسازی محیط‌ها (development, staging, production)
• دوره‌ای کلیدها rotation
• secure storage کلیدها

۹.۲. رمزنگاری داده‌ها

• داده‌های حساس در حال انتقال: TLS
• داده‌های حساس در حال ذخیره: AES-256
• رمز عبور: bcrypt hash

۹.۳. Certificate Management

• استفاده از certificates معتبر
• monitoring expiration dates
• automatic renewal

فصل ۱۰: لاگ‌گیری و مانیتورینگ

۱۰.۱. لاگ‌های امنیتی

• لاگ تمام تلاش‌های ورود
• لاگ تغییرات مهم داده‌ها
• لاگ فعالیت‌های مدیریتی
• لاگ خطاهای سیستم

۱۰.۲. مانیتورینگ real-time

• monitoring uptime
• monitoring performance
• فعالیت‌های مشکوک monitoring

۱۰.۳. Alerting

• برای فعالیت‌های غیرعادی alert

• برای خطاهای امنیتی alert
• escalation procedures

فصل ۱۱: مدیریت حوادث امنیتی

تیم پاسخ‌گویی ۱۱.۱.

• Incident Response Team (IRT)
• نقش‌ها و مسئولیت‌ها
• contact information

فرآیند پاسخ ۱۱.۲.

(Detection) تشخیص ۱.
(Containment) مهار ۲.
(Eradication) ریشه‌یابی ۳.
(Recovery) بازیابی ۴.
(Lessons Learned) یادگیری ۵.

۱۱.۳. communication plan

• ارتباط با کاربران
• ارتباط با regulatory bodies
• ارتباط با رسانه‌ها

فصل ۱۲: انطباق و استانداردها

استانداردهای پیاده‌سازی شده ۱۲.۱.

• OWASP Top 10
• ISO 27001 guidelines
• GDPR principles (برای کاربران اروپایی)

انطباق قانونی ۱۲.۲.

• قوانین حریم خصوصی ایران
• قوانین بین‌المللی (در صورت لزوم)

بررسی‌های انطباق ۱۲.۳.

• بررسی‌های داخلی فصلانه
• external audits سالانه
• continuous compliance monitoring

فصل ۱۳: تست امنیت

۱۳.۱. انواع تست امنیت

- Vulnerability Scanning ماهانه
- Penetration Testing شش‌ماهه
- Code Review امنیتی
- Security Training

۱۳.۲. Security Testing Tools

- OWASP ZAP برای dynamic testing
- SonarQube برای static analysis
- NMAP برای network scanning

۱۳.۳. Bug Bounty Program (آینده)

- برنامه پاداش برای گزارش آسیب‌پذیری
- scope و قوانین
- reward amounts

فصل ۱۴: آموزش امنیتی

۱۴.۱. آموزش تیم توسعه

- Secure Coding Training
- Security Awareness
- Incident Response Training

۱۴.۲. آموزش کاربران

- Security Best Practices
- Phishing Awareness
- Password Management

۱۴.۳. مستندات امنیتی

- Security Guidelines
- Incident Response Playbooks
- Security Policies

فصل ۱۵: ارزیابی ریسک

۱۵.۱. روش ارزیابی ریسک

Risk = Probability × Impact

Probability Levels:
- Very High (۵): بیش از ۱ بار در ماه
- High (۴): ۱ بار در ماه

• Medium (۳): بار در سال ۱
• Low (۲): بار در ۲ سال ۱
• Very Low (۱): کمتر از ۱ بار در ۲ سال

Impact Levels:
• Critical (۵): از دست رفتن کامل کسب‌وکار
• High (۴): آسیب مالی جدی
• Medium (۳): آسیب متوسط
• Low (۲): آسیب جزئی
• Very Low (۱): آسیب ناچیز

۱۵.۲. Risk Matrix

Impact ۱	۲	۳	۴	۵
Probability				
۵	۵		۱۰	۱۵	۲۰	۲۵	
۴	۴		۸	۱۲	۱۶	۲۰	
۳	۳		۶	۹	۱۲	۱۵	
۲	۲		۴	۶	۸	۱۰	
۱	۱		۲	۳	۴	۵	

Risk Rating:
• ۱-۵: Low (Accept)
• ۶-۱۲: Medium (Mitigate)
• ۱۳-۲۵: High (Avoid/Transfer)

فصل ۱۶: برنامه کاهش ریسک

۱۶.۱. ریسک‌های High

۱. ریسک: نقض داده‌های کاربران
• Score: ۲۰
• استراتژی: Mitigate
• اقدامات: encryption، access control، monitoring

۲. ریسک: از کار افتادن سرویس
• Score: ۱۶
• استراتژی: Mitigate
• اقدامات: redundancy، DDoS protection

۱۶.۲. ریسک‌های Medium

۱. ریسک: brute force attacks
• Score: ۱۲

• استراتژی: Mitigate
• اقدامات: rate limiting، account lockout

۲. ریسک: XSS attacks
• Score: ۹
• استراتژی: Mitigate
• اقدامات: input validation، output encoding

۱۶.۳. ریسک‌های Low

۱. ریسک: information disclosure through error messages
• Score: ۴
• استراتژی: Accept
• اقدامات: generic error messages

فصل ۱۷: برنامه بهبود امنیت

۱۷.۱. Short-term (ماه ۳)

• پیاده‌سازی WAF
• سرورها security hardening
• افزایش monitoring

۱۷.۲. Medium-term (ماه ۶)

• پیاده‌سازی 2FA
• security awareness training
• external penetration test

۱۷.۳. Long-term (ماه ۱۲)

• پیاده‌سازی SIEM
• bug bounty program
• ISO 27001 certification

فصل ۱۸: نتیجه‌گیری

مدل تهدید ProDecks یک رویکرد نظام‌مند برای شناسایی، تحلیل و کاهش ریسک‌های امنیتی ارائه می‌دهد.
با پیاده‌سازی کنترل‌های پیشگیرانه، تشخیصی و اصلاحی، سیستم در برابر تهدیدات متعدد محافظت می‌شود.
برنامه کاهش ریسک و بهبود مستمر تضمین می‌کند که امنیت سیستم همگام با رشد آن توسعه می‌یابد.

ضمیمه‌ها

ضمیمه ۱: نقشه کامل تهدیدات

ضمیمه ۲: ماتریس ریسک کامل

ضمیمه ۳: Security Control Catalog

ضمیمه ۴: Incident Response Playbooks

تهیه‌کنندگان:

تیم امنیت ProDecks

حامد کوهی (مدیر امنیت)

مشاوران امنیتی
