

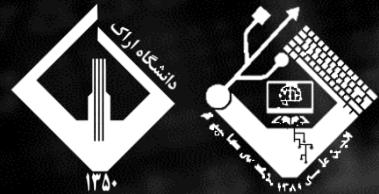
Hackers & Hunters

هکرها و شکارچیان

آشنایی با رشته هانت (شکار) در امنیت

کیان درفش دار

مهر ۱۴۰۳



۱۱:۰۰	فیلم خوش آمدگویی
بخش اول	شاخه‌ها و زیرشاخه‌های اصلی امنیت
بخش دوم	معیارها و سازمان‌های جهانی امنیت
بخش سوم	چگونگی تکامل رشته باگ بانتی
آنتراک	
بخش چهارم	زمینه‌های فعالیت و پلتفرم‌های شکار
بخش پنجم	پیش نیازها و نقشه راه شکارچی شدن
۱۲:۱۵	پرسش و پاسخ

شاخه‌های اصلی امنیت

چرا زمینه‌های مختلفی در امنیت سایبری داریم؟

۶. استراتژی‌های دفاع در مقابل حمله
(تشخیص و کاهش آسیب)

۷. تحقیق و توسعه
(آسیب پذیری‌های جدید)

۸. آموزش و پرورش
(آموزش‌های جدید و مدارک بیشتر)

۱. انواع مختلفی از تهدید‌ها و حملات
(malware, phishing, social engineering, and etc.)

۲. توانایی‌های خاص
(technical skills and knowledge)

۳. قانون‌گذاری و رعایت قوانین
(HIPPA , PCI DSS)

۴. پیچیدگی تکنولوژی‌ها
(IOT , mobile applications and etc.)

۵. مدیریت ریسک
(بانک و مغازه فست‌فود)

شاخه‌های اصلی امنیت

۲. امنیت اپلیکیشن

حافظت از دستگاه و برنامه در مقابل تهدید‌ها.
(کد نویسی امن و متدهای تشخیص آسیب پذیری)



۱. امنیت شبکه

محافظت از دسترسی، یکپارچگی و محرومگی شبکه و اطلاعات.
(فایروال، سیستم تشخیص نفوذ و VPN ها)



شاخه‌های اصلی امنیت

۳. امنیت اطلاعات

مقابله با دسترسی غیرمجاز و تغییرات داده ها.
(رمزگاری داده، کنترل دسترسی ها و رعایت قوانین)



۴. امنیت پایانه

امن سازی دستگاه های پایانه یا دستگاه های کاربران مانند کامپیوترها، موبایل ها، تبلت ها و
(آنتی ویروس و سیستم EDR)

شاخه‌های اصلی امنیت

۶. واکنش به حادثه

آمادگی برای تشخیص و پاسخ به حوادث سایبری
(مدیریت حادثه، تحقیق و پروسه بازیابی)



۵. امنیت ابر

اطمینان از امن بودن محیط‌های رایانش ابری و دیتای درون آن‌ها
(خصوصی بودن داده‌ها، انطباق و تنظیمات ایمن)



شاخه‌های اصلی امنیت

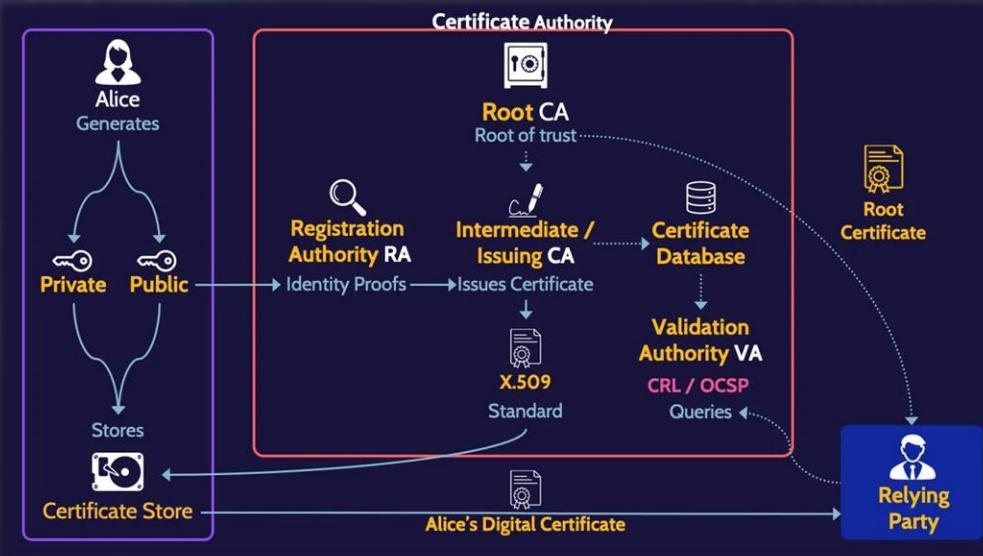
۸. هوش تهدید

جمع‌آوری و آنالیز اطلاعات در مورد تهدید و آسیب‌پذیری‌ها برای پیش‌بینی و کاهش حملات.
(دفاع‌های پیشگیرانه)



۷. معماری و مهندسی امنیت

تمرکز روی طراحی و ارتقاء فریمورک‌های امنیت
(مدیریت ریسک و کنترل‌های امنیتی)



شاخه‌های اصلی امنیت

۱. انطباق و مدیریت ریسک

چک کردن سازمان‌ها برای رعایت کردن قوانین، استانداردها (GDPR, HIPAA, etc)، مقررات و مدیریت ریسک در برابر تهدیدها



۹. مدیریت هویت و دسترسی (IAM)

آیا افراد درست دسترسی موردنظر از منابع تکنولوژی‌ها را دارند؟
(احراز هویت، مجوزها و اصلی بودن هویت)



شاخه‌های اصلی امنیت

۱۲. تست نفوذ و هک قانونمند

سیستم‌های تسته آسیب‌پذیری‌ها از دیدگاه هکر
تا از ضعف‌ها پیشگیری شود.



Forensics . ۱۱

جمع‌آوری شواهد و مدارک از حوادث امنیتی و نفوذ‌ها،
معمولاً در زمینه‌های قانونی استفاده می‌شود.



شاخه‌های اصلی امنیت

۱۳. آموزش آگاهی از امنیت

آموزش کارمندان و کاربران با بهترین تمرین‌ها برای
جلوگیری از حملات مهندسی اجتماعی و ارتقاء
فرهنگ امنیت در سازمان‌ها



معیارها و سازمانهای جهانی امنیت

NIST

National Institute of Standards
and Technology

PCI SSC

Payment Card Industry
Security Standards Council

MITRE
Corporation

CIA Triad

Confidentiality, Integrity, and
Availability

CVSS

Common Vulnerability
Scoring System

CVE

Common Vulnerabilities and
Exposures



معیارها و سازمان‌های جهانی امنیت

NIST

National Institute of
Standards and Technology



انتشار فریمورک امنیتی

Identify, Protect, Detect, Respond, and Recover.

انتشارات خاص (special Publications)

انتشار مطالب در زمینه‌های مختلف امنیت

انتشار فریمورک مدیریت ریسک

Identify, Protect, Detect, Respond, and Recover.

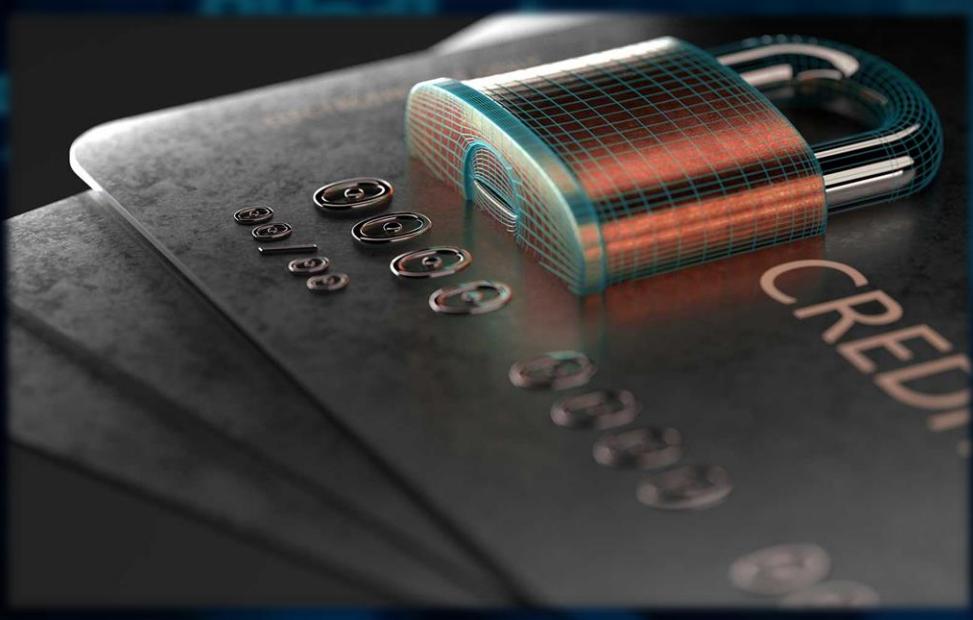
اجام تحقیقات بر تکنولوژی‌های جدید
و ترکیب تکنولوژی‌ها

(کامپیوتر کوانتمی، بلاکچین، رایانش ابری و...)

معیارها و سازمان‌های جهانی امنیت

PCI SSC

Payment Card Industry
Security Standards Council



تأسیس ۲۰۰۶

Visa, Master Card, American Express, etc.

ارتقاء استاندارد های امنیتی
برای کارت های پرداخت
تایید، پردازش، نگهداری و انتقال داده

هماهنگی و انطباق بخش پرداخت و کارت های
پرداخت سازمان ها برای اطمینان از امنیت

معیارها و سازمان‌های جهانی امنیت

MITRE Corporation



فعالیت در زمینه‌های مختلف با دولت آمریکا
آنالیز سیستم‌های مجتمع در سازمان دفاع، امنیت سایبری، سلامت و...

ATT&CK

بر پایه دانشی از تاکتیک‌ها، تکنیک‌ها و رویه‌های
مورد استفاده دشمنان در امنیت سایبری
(مناسب برای ارتقاء امنیت و مورد استفاده متخصصان)

متخصص در مهندسی سیستم، توسعه نرم‌افزار و
مشاوره تکنیکال

معیارها و سازمان‌های جهانی امنیت

CIA Triad

محرمانگی

CONFIDENTIALITY

یکپارچگی

2
INTEGRITY

دسترسی

3
AVAILABILITY

معیارها و سازمان‌های جهانی امنیت

CVSS

Common Vulnerability
Scoring System

فریمورک تعیین شدت آسیب پذیری

با توجه به میزان حساسیت داده، مقدار نشت اطلاعاتی، میزان عملکرد و پیچیدگی لازم برای رخداد آسیب پذیری و نحوه اتفاق افتادن برای قربانی، این فریمورک یا معیار عددی به ما میدهد که شدت را مشخص میکند.

CVSS v2.0

2007

پارامتر کمتر، پایه‌ای، مدل ساده و محدود در تعیین ریسک

CVSS v3.0

2015

دقیق‌تر و ساده‌تر، پارامترهای بیشتر، تعیین بهتر ریسک و تأثیرگذاری

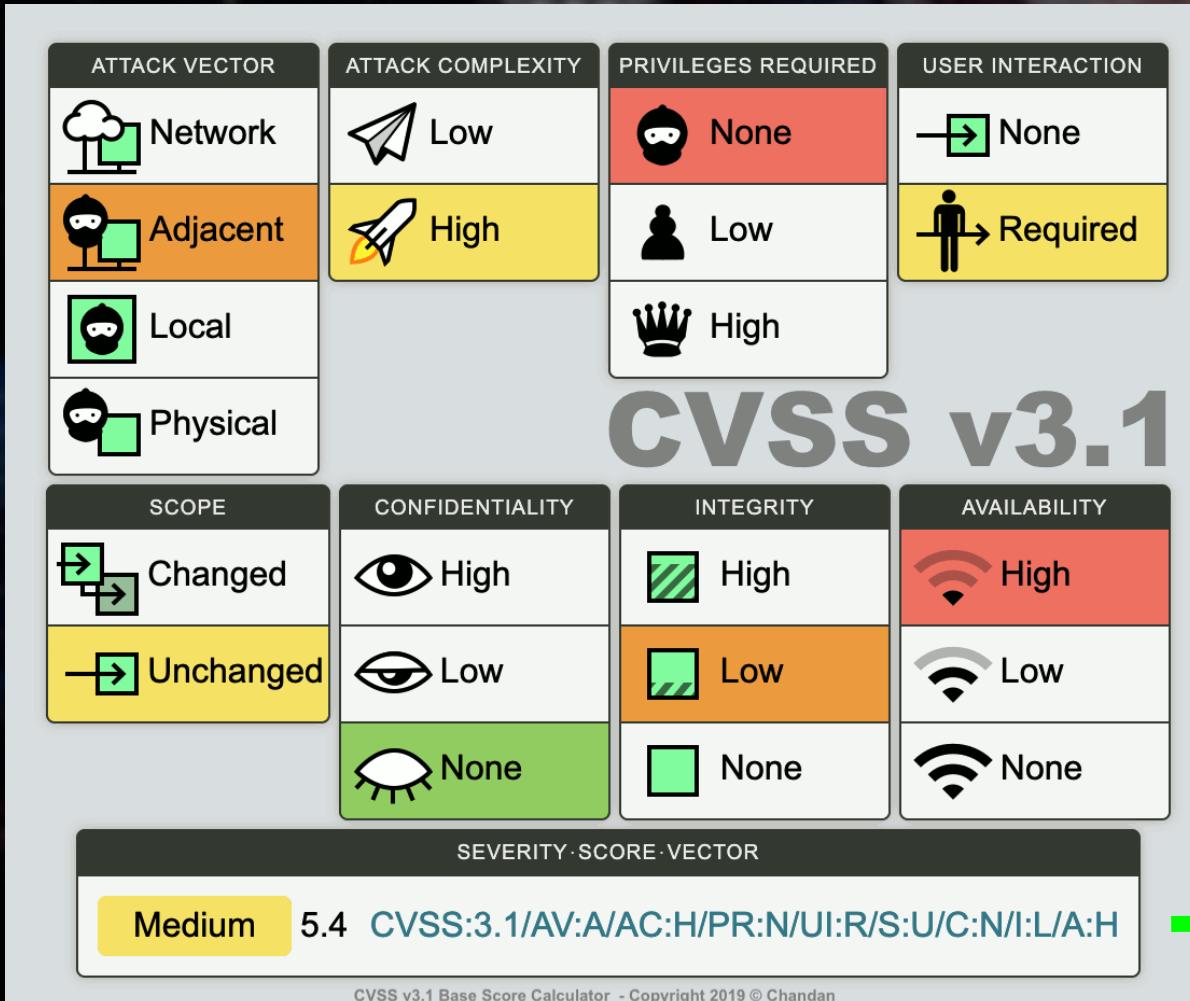
CVSS v3.1

2019

بر اساس ورژن ۳.۰، تغییرات کوچکی برای وضوح و جلوگیری از برداشت نادرست. بهبود نتایج قابل اجرا و کاهش اهمیت ریسک.

معیارها و سازمان‌های جهانی امنیت

CVSS



CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

معیارها و سازمان‌های جهانی امنیت

CVE

Common Vulnerabilities
and Exposures

سیستم استاندارد برای شناسایی آسیب‌پذیری در نرم‌افزار و سخت‌افزار

شناسه مشخص، اطلاعات منتشر شده و قابل دسترس،
استانداردسازی شده و دارای جامعه خاص

کاری از شرکت **MITRE** و سهامداران مختلف
مدیریت آسیب‌پذیری، اطلاعات تهدید و قابلیت همکاری

CVE-2024-0451

AI ChatBot for WordPress

WPBot The AI ChatBot plugin for
WordPress is vulnerable to
unauthorized access of data.

تکامل باگ بانتی و شکار

Bug Bounty & Hunt



از شکل‌گیری تا آینده...

تکامل باگ بانتی و شکار

Bug Bounty & Hunt



آنtrap

SYSTEM
HACKED



زمینه های فعالیت

۱. تست نرم افزار
۲. تست وب اپلیکیشن
۳. تست موبایل اپلیکیشن
۴. امنیت شبکه
۵. برنامه های آزاد باگ بانگ
۶. تست بازی
۷. تیم قرمز، هک قانونمند
۸. امنیت سخت افزار

پلتفرم های شکار

1. HackerOne

hackerone

2. Bugcrowd

bugcrowd

See
Security
Differently

3. Intigriti



INTIGRITI

BUG BOUNTY

پلتفرم های شکار

بخش های یک برنامه

قانون گذاری

Scope

Rewards

تحریم ها

دامنه ها و ساب دامنه ها

میزان پاداش ها بر اساس
هر آسیب پذیری

حملات غیر قانونی

دامنه های حساس

جوایز خاص
(امتیاز، تخفیف و کالا)

شرایط خاص

باق های قابل قبول

STEP 01

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed
do eiusmod tempor incididunt ut
labore et dolore magna aliqua.



STEP 02

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed
do eiusmod tempor incididunt ut
labore et dolore magna aliqua.



STEP 03

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed
do eiusmod tempor incididunt ut
labore et dolore,

نقشه راه

STEP 04

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed
do eiusmod tempor incididunt ut
labore et dolore magna aliqua. Ut
enim.



STEP 05

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed
do eiusmod tempor incididunt ut
labore et dolore magna aliqua.

