The second law of Hacker Metaverse

1) All assets in Metaverse are software and code
2) Vulnerability is the most important digital assets
3) Vulnerability is Native NFT
4) The hacker law is the first innovation all over the world.

参赛项目：元宇宙第二定律

1)元宇宙所有资产本质都是软件代码

2) 系统漏洞是重要的数字资产

3)系统漏洞是天然的NFT资产

4) 黑客三定律是全世界首次创新发现

The hacker law of Metaverse

The First Law of Hacking (Von Neumann) Neumann, the father of modern computing).

Information security vulnerability is the vulnerability of information technology, information products and information systems in the process of demand, design, implementation, configuration and operation, intentionally or unintentionally, these vulnerabilities exist in different forms in all levels and links of information systems, and can be exploited by malicious subjects, thus affecting the normal operation of information systems and their services.

The Second Law of Hacking : (He-Jun Xu paper published in June 2021)

The market value of an information security vulnerability = 5 × the average monthly salary of the developer who generated the security vulnerability × the security level of the vulnerability.

The Third Law of Hacking: (Paper by He-Jun Xu, published in June 2021)

The market economic value of an information system vulnerability can be referred to the market economic value of the labor of the developer of that information system.Translated with www.DeepL.com/Translator (free version)

元宇宙黑客三定律

黑客第一定律 （冯.诺伊曼 现代计算机之父）：
信息安全漏洞是信息技术，信息产品和信息系统在需求，设计，实现，配置，运行的过程中，有意或者无意产生的脆弱性，这些脆弱性以不同形式存在于信息系统各个层次和环节中，能够被恶意主题所利用，从而影响信息系统及其服务的正常运行。

黑客第二定律 ： （徐鹤军 论文发表于2021年6月发表）
信息安全漏洞的市场价值 = 5 × 产生该安全漏洞开发人员的月平均工资 × 漏洞的安全等级。

黑客第三定律 ： （徐鹤军 论文发表于2021年6月发表）
信息系统漏洞的市场经济价值可以参考该信息系统开发人员劳动力的市场经济价值。

Newton’s law vs. Hacker law

The first law : **Inertia**

The First Law: The Eternal Law ofVulnerability

Second Law : **Force**

Second Law: Law of Value Valuation

Third Law : **Action & Reaction**

Third Law: Law of Value Symmetry

Newton law vs. Hacker Law

- 第一定律 惯性定律
- 第二定律 作用力定律
- 第三定律 反作用力定律

- 第一定律：漏洞永恒定律
- 第二定律： 价值估值定律
- 第三定律：价值对称定律

The second law of hacker Metaverse

- The market Value of Vulnerability (VoV)=
- 5 (Pareto Principle/ 2:8 principle)
- * average month salary who make this vulnerability (AvS)
- * the score level which evaluated by security administration (Impact Score)

元宇宙第二定律

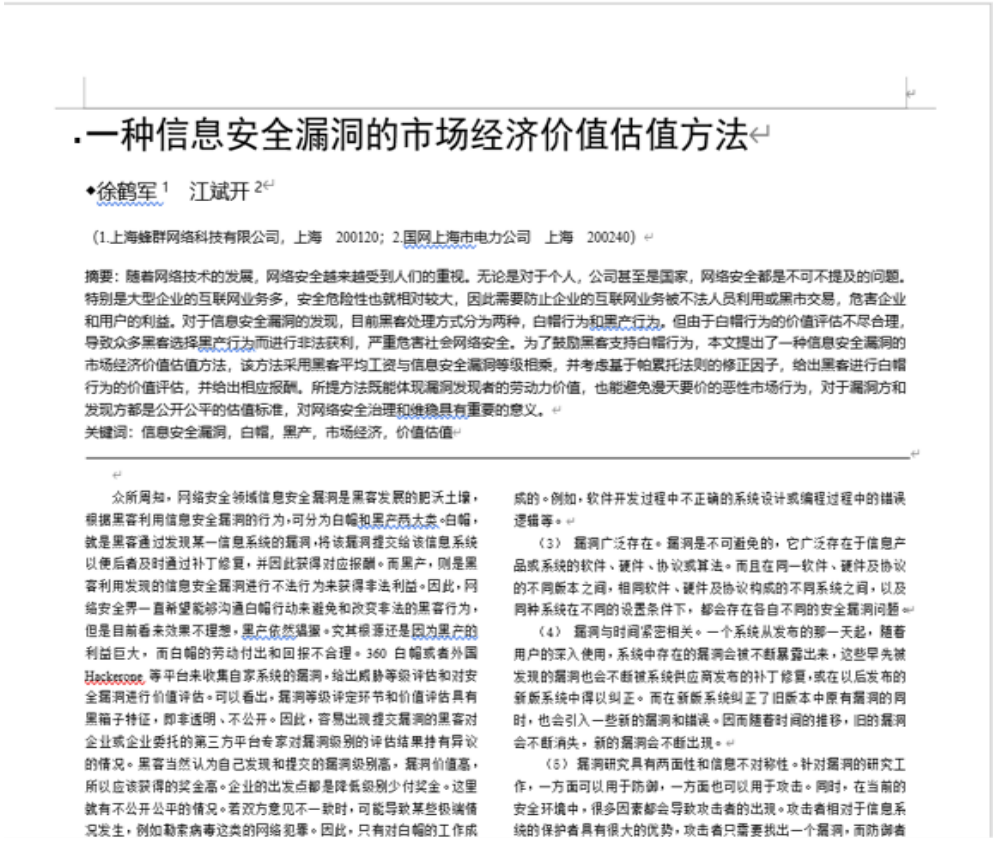
信息安全漏洞的市场价值 (VoV)=

5 （经济学帕累托原则/ 2:8 原则）

× 产生该安全漏洞开发人员的月平均工资（AvS)

× 漏洞的安全等级(Impact Score)

The research paper



一种信息安全漏洞的市场经济价值估值方法

徐鹤军[1] 江斌开[2]

(1.上海蜂群网络科技有限公司，上海 200120；2.国网上海市电力公司 上海 200240)

摘要：随着网络技术的发展，网络安全越来越受到人们的重视。无论是对于个人，公司甚至是国家，网络安全都是不可不提及的问题。特别是大型企业的互联网业务多，安全危险性也就相对较大，因此需要防止企业的互联网业务被不法人员利用或黑市交易，危害企业和用户的利益。对于信息安全漏洞的发现，目前黑客处理方式分为两种，白帽行为和黑产行为。但由于白帽行为的价值评估不尽合理，导致众多黑客选择黑产行为而进行非法获利，严重危害社会网络安全。为了鼓励黑客支持白帽行为，本文提出了一种信息安全漏洞的市场经济价值估值方法，该方法采用黑客平均工资与信息安全漏洞等级相乘，并考虑基于帕累托法则的修正因子，给出黑客进行白帽行为的价值评估，并给出相应报酬。所提方法既能体现漏洞发现者的劳动力价值，也能避免漫天要价的恶性市场行为，对于漏洞方和发现方都是公开公平的估值标准，对网络安全治理和维稳具有重要的意义。

关键词：信息安全漏洞，白帽，黑产，市场经济，价值估值

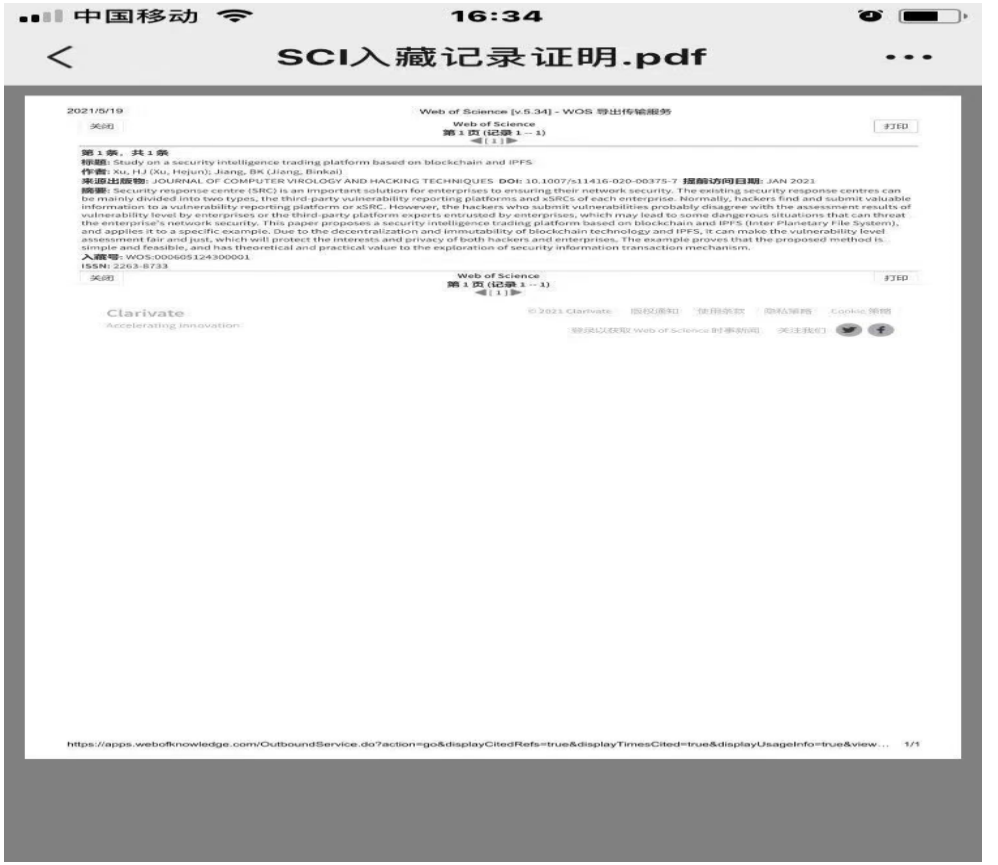
众所周知，网络安全领域信息安全漏洞是黑客发展的肥沃土壤，根据黑客利用信息安全漏洞的行为，可分为白帽和黑产两大类。白帽，就是黑客通过发现某一信息系统的漏洞，将该漏洞提交给该信息系统以便后者及时通过补丁修复，并因此获得对应报酬。而黑产，则是黑客利用发现的信息安全漏洞进行不法行为来获得非法利益。因此，网络安全界一直希望能够沟通白帽行动来避免和改变非法的黑客行为，但是目前看来效果不理想，黑产依然猖獗。究其根源还是因为黑产的利益巨大，而白帽的劳动付出和回报不合理。360 白帽或者外国 Hackerone 等平台来收集自家系统的漏洞，给出威胁等级评估和对安全漏洞进行价值评估。可以看出，漏洞等级评定环节和价值评估具有黑箱子特征，即非透明、不公开。因此，容易出现提交漏洞的黑客对企业或企业委托的第三方平台专家对漏洞级别的评估结果持有异议的情况。黑客当然认为自己发现和提交的漏洞级别高，漏洞价值高，所以应该获得的奖金高。企业的出发点都是降低级别少付奖金。这里就有不公开公平的情况。若双方意见不一致时，可能导致某些极端情况发生，例如勒索病毒这类的网络犯事。因此，只有对白帽的工作成

成的。例如，软件开发过程中不正确的系统设计或编程过程中的错误逻辑等。

（3） 漏洞广泛存在。漏洞是不可避免的，它广泛存在于信息产品或系统的软件、硬件、协议或算法。而且在同一软件、硬件及协议的不同版本之间，相同软件、硬件及协议构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

（4） 漏洞与时间紧密相关。一个系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞会被不断暴露出来，这些早先被发现的漏洞也会不断被系统供应商发布的补丁修复，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中原有漏洞的同时，也会引入一些新的漏洞和错误。因而随着时间的推移，旧的漏洞会不断消失，新的漏洞会不断出现。

（5） 漏洞研究具有两面性和信息不对称性。针对漏洞的研究工作，一方面可以用于防御，一方面也可以用于攻击。同时，在当前的安全环境中，很多因素都会导致攻击者的出现。攻击者相对于信息系统的保护者具有很大的优势，攻击者只需要找出一个漏洞，而防御者



Impact Score from NVD

- National Vulnerability Database
- The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
- CVE-2020-5320 - Dell EMC OpenManage Enterprise (OME) versions prior to 3.2 and OpenManage Enterprise-Modular (OME-M) versions prior to 1.10.00 contain a SQL injection vulnerability.

漏洞威胁等级评分来自 NVD

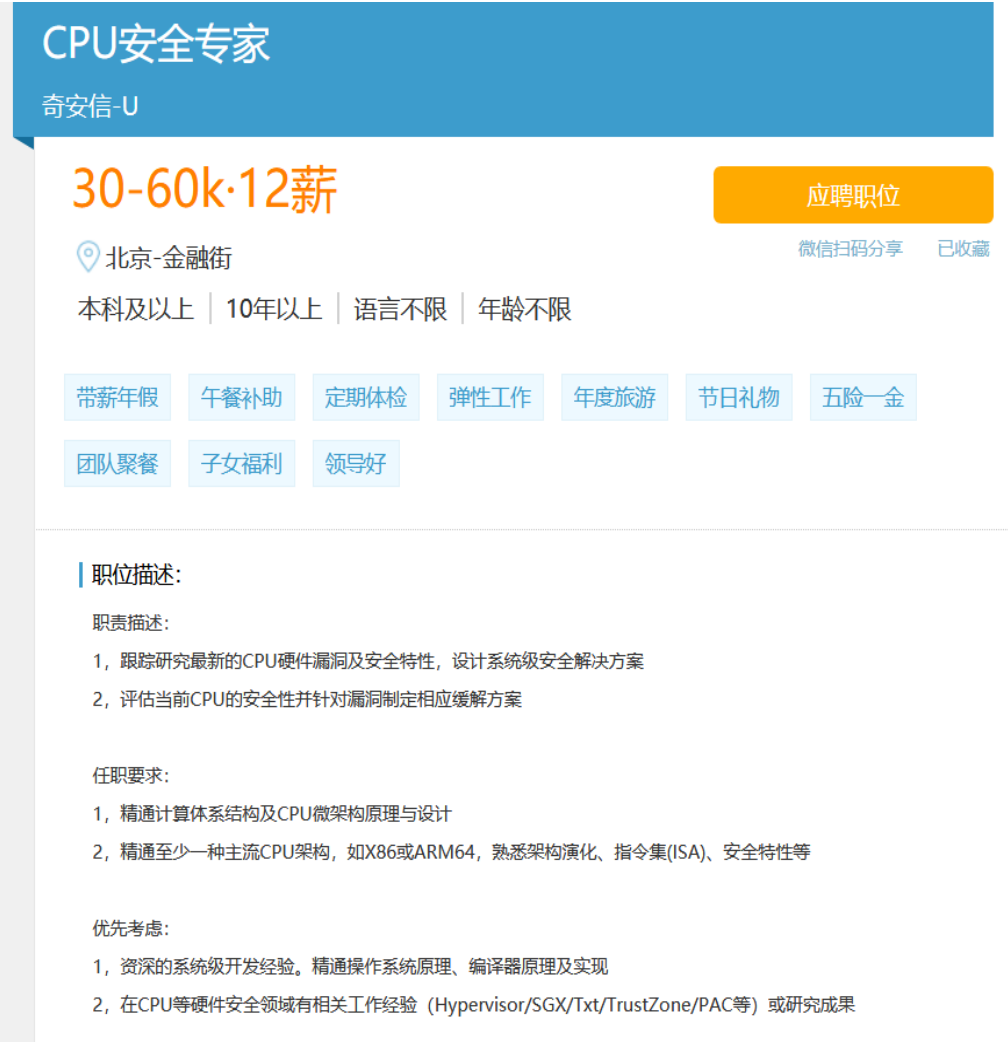
国家漏洞数据库

NVD是美国政府基于标准的漏洞管理数据库，使用安全内容自动化协议（SCAP）表示。这些数据能够实现漏洞管理、安全测量和合规性的自动化。NVD包括安全检查表参考、安全相关软件缺陷、错误配置、产品名称和影响指标的数据库。

CVE-2020-5320 - Dell EMC OpenManage Enterprise（OME）3.2之前的版本和OpenManage Enterprise-Modular（OME-M）1.10.00之前的版本包含一个SQL注入漏洞。

Valuation of Baidu's vulnerability = 5 × 45,000 × 4 = 900,000 RMB

Baidu Rust SGX SDK Security Vulnerability CNNVD Number: CNNVD-202001-091
Hazard Level: Ultra Critical CVE Number: CVE-2020-5499
Vulnerability Type: Other
Release Date: 2020-01-04
Threat Type: Remote
Updated: 2020-01-16 Manufacturer.
Vulnerability Source.



CPU安全专家

奇安信-U

30-60k·12薪

应聘职位

北京-金融街

微信扫码分享 已收藏

本科及以上 | 10年以上 | 语言不限 | 年龄不限

带薪年假 午餐补助 定期体检 弹性工作 年度旅游 节日礼物 五险一金 团队聚餐 子女福利 领导好

职位描述:

职责描述:

1，跟踪研究最新的CPU硬件漏洞及安全特性，设计系统级安全解决方案

2，评估当前CPU的安全性并针对漏洞制定相应缓解方案

任职要求:

1，精通计算体系结构及CPU微架构原理与设计

2，精通至少一种主流CPU架构，如X86或ARM64，熟悉架构演化、指令集(ISA)、安全特性等

优先考虑:

1，资深的系统级开发经验。精通操作系统原理、编译器原理及实现

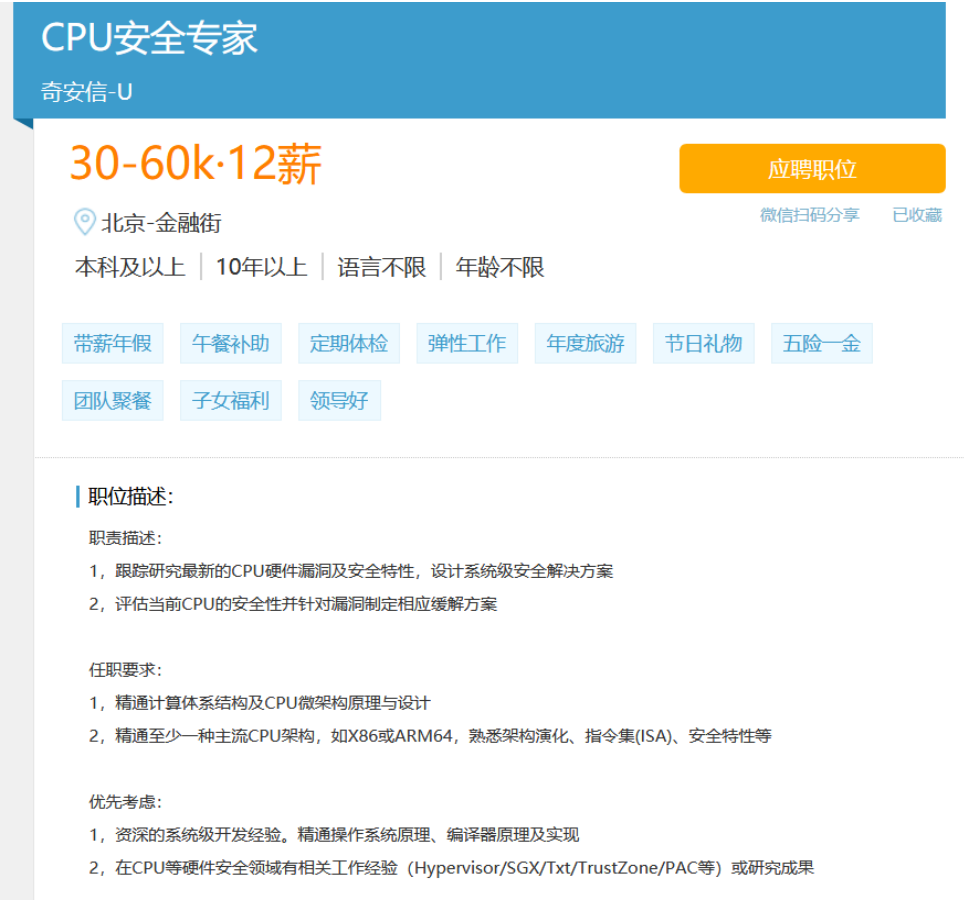
2，在CPU等硬件安全领域有相关工作经验（Hypervisor/SGX/Txt/TrustZone/PAC等）或研究成果

百度公司漏洞的价值评估 = 5 ×45，000 × 4 = 900，000 RMB

Baidu Rust SGX SDK 安全漏洞

- CNNVD编号：CNNVD-202001-091
- 危害等级： 超危

- CVE编号： CVE-2020-5499
- 漏洞类型： 其他
- 发布时间： 2020-01-04
- 威胁类型： 远程
- 更新时间： 2020-01-16
- 厂　　商：
- 漏洞来源：



Demo：Vulnerabitlity impact score from external adapter in Chainlink

- Vulnerability score from NVD ()
- Every vulnerability is indexed by unique CVE ID
- Tech Stack: Ethereum+xDai+Arbitrum+Chainlink+Swarm/Filecoin

演示：漏洞威胁评分来自Chainlink外部适配器

来自NVD的漏洞评分

每个漏洞都是由唯一 CVE ID来索引的

技术栈。以太坊+xDai+Arbitrum+Chainlink+Swarm/Filecoin

Smart contract is NFT type

- Software code is digit asset in Metaverse
- Smart contract is software code
- The address of Smart Contract is unique and native NFT id
- Vulnerability PoC code can be saved into smart contract
- Smart contract can be exchanged as NFT

智能合约是NFT资产

软件代码是Metaverse中的数字资产
智能合约是软件代码
智能合约的地址是唯一的，并且是天然NFT ID
漏洞PoC代码保存在智能合约中
智能合约可以作为NFT进行交换

Blockchain 4.0 Stack

App Dockerfile	App code Repos	Tracked App
SmartContract	P2P based Source CodeVersionControl	ContainerPlatform
BlockChain Platform	P2P File system / IPFS	Container/Docker

Collect and control vulnerability,rule the metaverse

收集和挖掘漏洞，统治元宇宙。