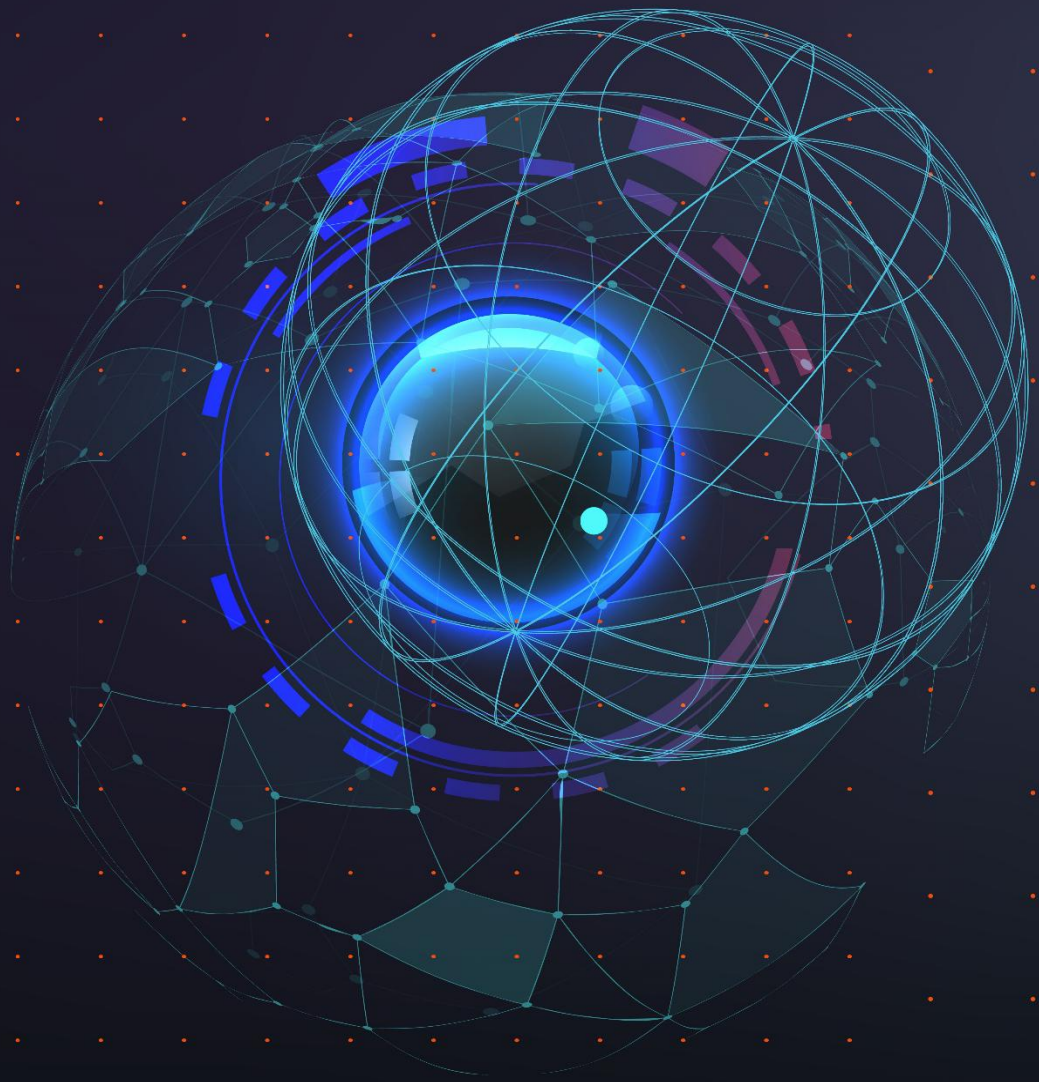


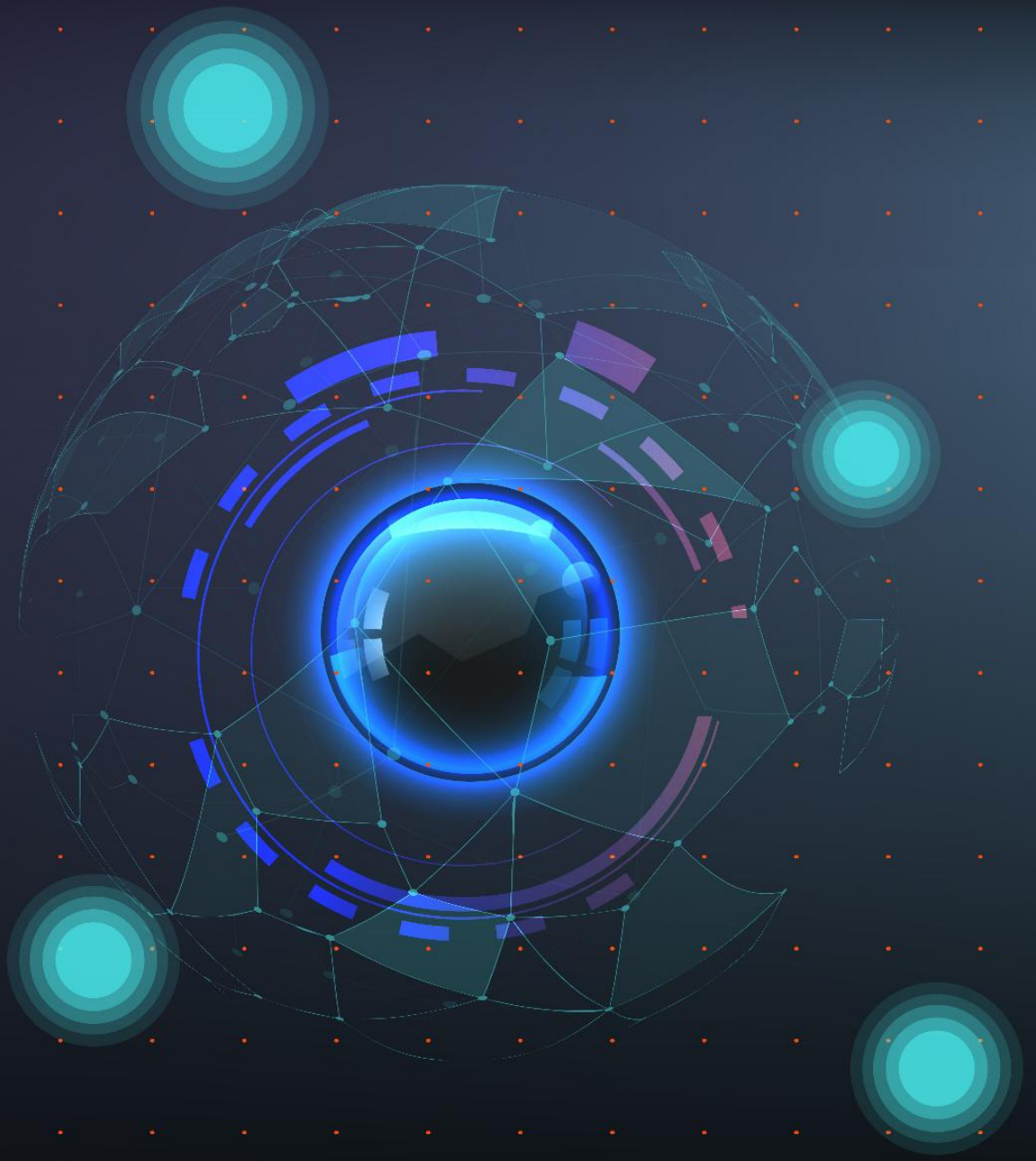
Onebel系统分析与设计

演讲：林章

目录

THE PART ONE 第一部分

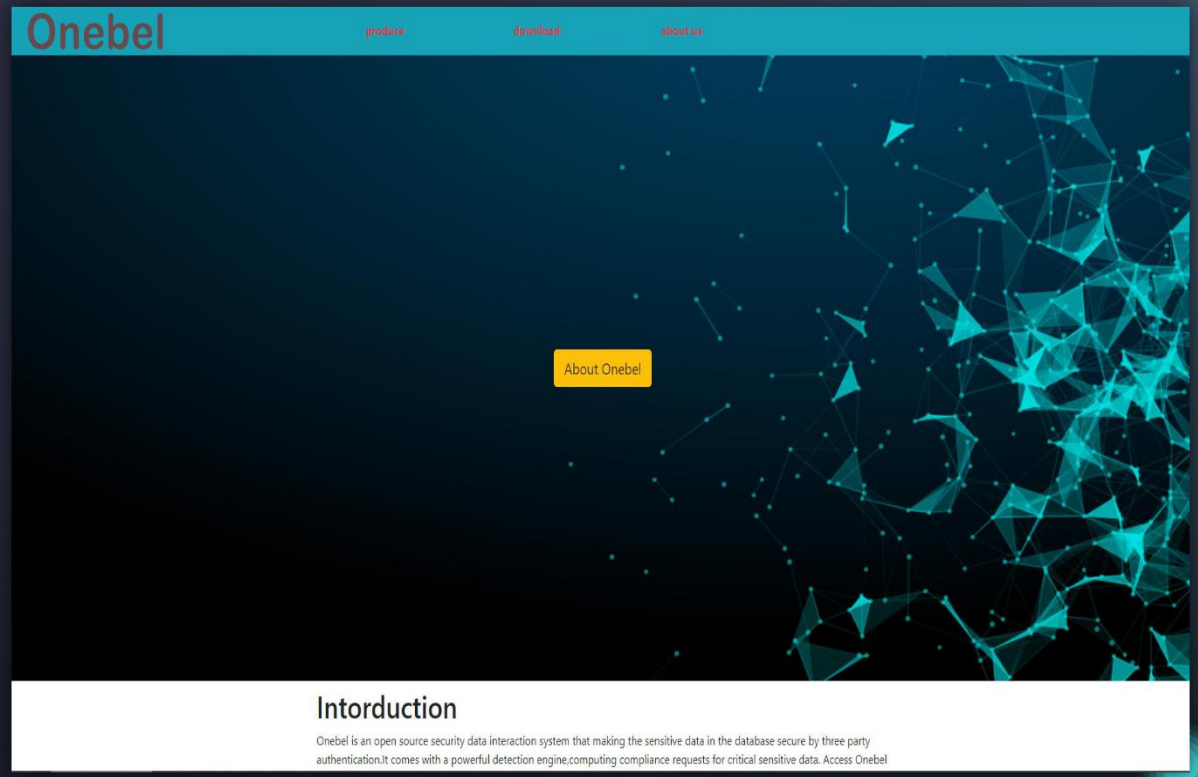
——什么是Onebel?



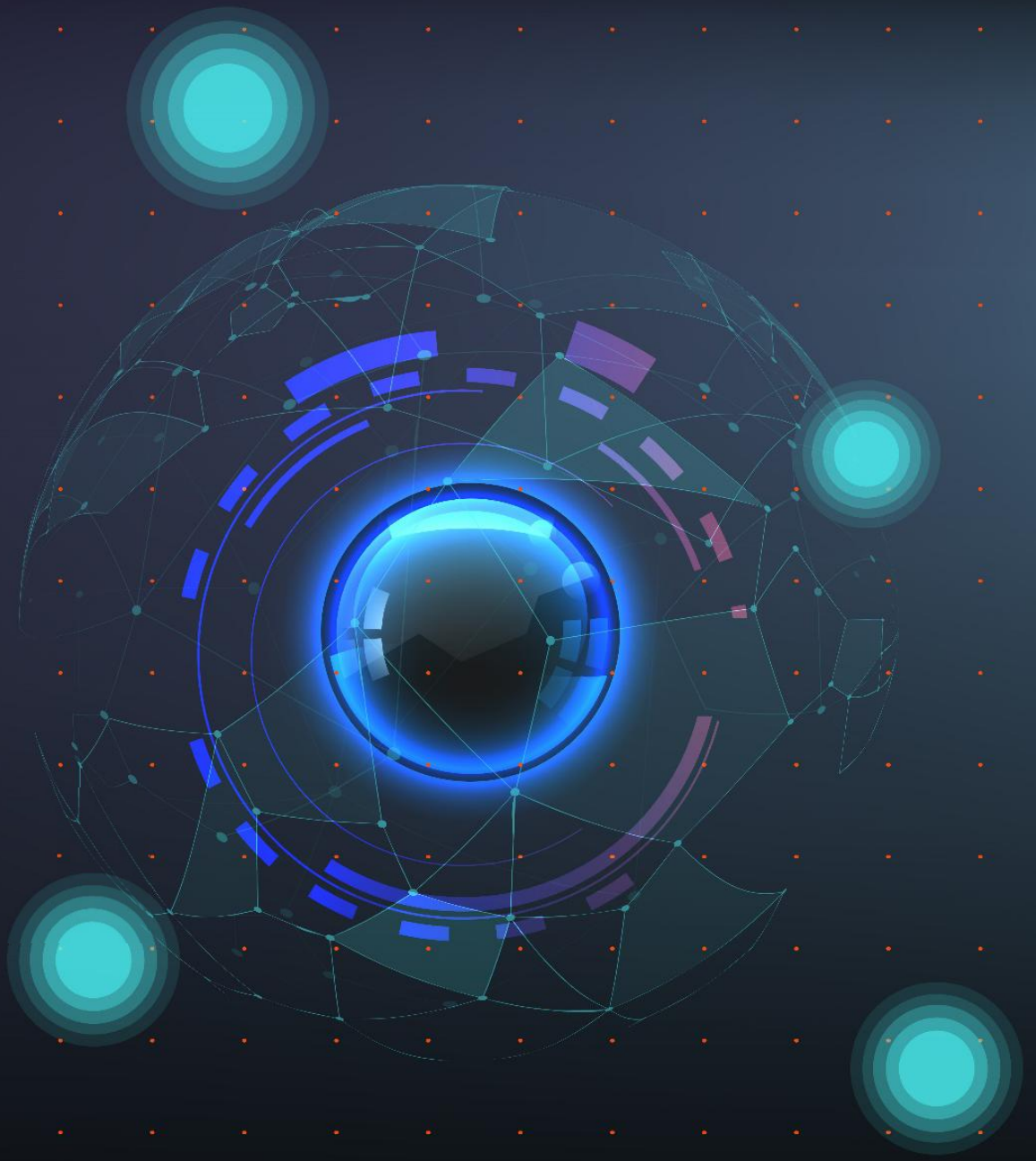
概念：什么是Onebel

Onebel是一个的数据存储系统，通过分离核心数据储存的方式，保证了数据安全性。通过第三方的参数保证了数据安全

通过强大的风控引擎，能够有效的防止核心数据受到黑客攻击。系统适用于中型互联网电商平台，或者SSO系统、支付系统



THE PART TWO
第二部分
——需求分析



原始需求分析

部分敏感数据或数据库的配置信息储存在主服务器上，将导致主服务被攻击后关键信息泄漏，数据的规范储存和核心功能系统与主系统分离成为了一种安全需求

在中大型互联网公司，登陆和支付系统剥离出主系统已经成为主流。在剥离系统后，新的子系统配合上Onebel可以进一步提高系统的安全性

举个例子

结果 消息

	name1	pass	email	site	salt	other	id	text
45	lihui	e10adc3949ba59abbe56e057f20f883e	527290476@qq.com	八度网络	NULL	NULL	363792470	NULL
46	lihui	a281c6facaa1642d65821000a01376f5	250427656@qq.com	新51CTO	f3bded	220.1...	369385314	NULL
47	lihui	a281c6facaa1642d65821000a01376f5	250427656@qq.com	新51cto	f3bded	220.1...	372668671	NULL
48	lihui	lihuip1p2	peterok_304306766@qq.com	万业网	NULL	李辉:...	375943109	NULL
49	lihui	b04b8454525865988d2e527f4a07e0dc	anconghuifei@163.com	Sorry	259310	NULL	382274360	NULL
50	lihui	ba0b8cce8301c357c2b5341aa60d692b	805312926@qq.com	Sorry	NULL	NULL	382691993	NULL
51	lihui	a543fbe522d59eaa86361b967fd8da44	NULL	Sorry	NULL	NULL	382956139	NULL
52	lihui	e10adc3949ba59abbe56e057f20f883e	ni31415926@163.com	多玩YY	NULL	123456	387361458	NULL
53	lihui	e10adc3949ba59abbe56e057f20f883e	ni31415926@163.com	多玩YY	NULL	123456	391884440	NULL
54	lihui	f23acb74e794c925e91c6339cb2a4938	41494341@qq.com	吹友吧	813293	NULL	398974303	NULL
55	lihui	ebd66d6af9187745	wobenfeiyang1987@yaho...	tpy100	NULL	15176...	415408453	姓...
56	lihui	c5f0438806166d1ddc2818ad02f21144	qq865230809@163.com	hk1433	19e...	NULL	423770015	NULL

原始需求分析


密文: e10adc3949ba59abbe56e057f20f883e
类型: 自动
[帮助]
查询
加密
查询结果:
123456
[添加备注]


密文: a281c6facaa1642d65821000a01376f5
类型: 自动
[帮助]
查询
加密
查询结果:
已查到,这是一条付费记录。请点击购买
(点击购买才扣费，并立即显示解密结果和加密类型。本站数据量全球第一，成功率全球第一，支持多种类型，许多密码只有本站才可以查询)
[添加备注]


密文: b04b8454525865988d2e527f4a07e0dc
类型: 自动
[帮助]
查询
加密
查询结果:
未查到
已加入本站后台解密，请等待最多5天，如果解密成功将自动给你发送邮件通知，否则表示解密失败。请注意本站实时查询已经非常强大，实时查询未查到则后台解密成功的希望并不大
[不知道密文类型？]
[添加备注]

Onebel的作用

将敏感数据储存在Onebel可以在主数据库发生泄漏的时候守住用户的核心利益

假设泄漏了用户的用户名和hash，通过md5(pass.salt)的方式加密，如果将salt储存在Onebel中，假定salt仅为6位数（10数字+26字母+9个特殊字符），个人PC验证一个账户单个密码的有效性需要81亿次，对比一个密码的hash结果就需要187.5天，有效的防止了密码泄漏后用户被发起指定攻击。对撞hash的成本>识别验证码撞库成本，导致了数据库泄漏后黑客只有hash，没有salt，很难撞出密码，也不会去主动撞出密码

而Onebel不仅仅可以运用于SSO salt的储存中，更可以用于支付系统的关键数据储存中

软件需求分析&技术可行性分析

对于Onebel的数据储存，由于是敏感数据，所以技术上有以下要点：

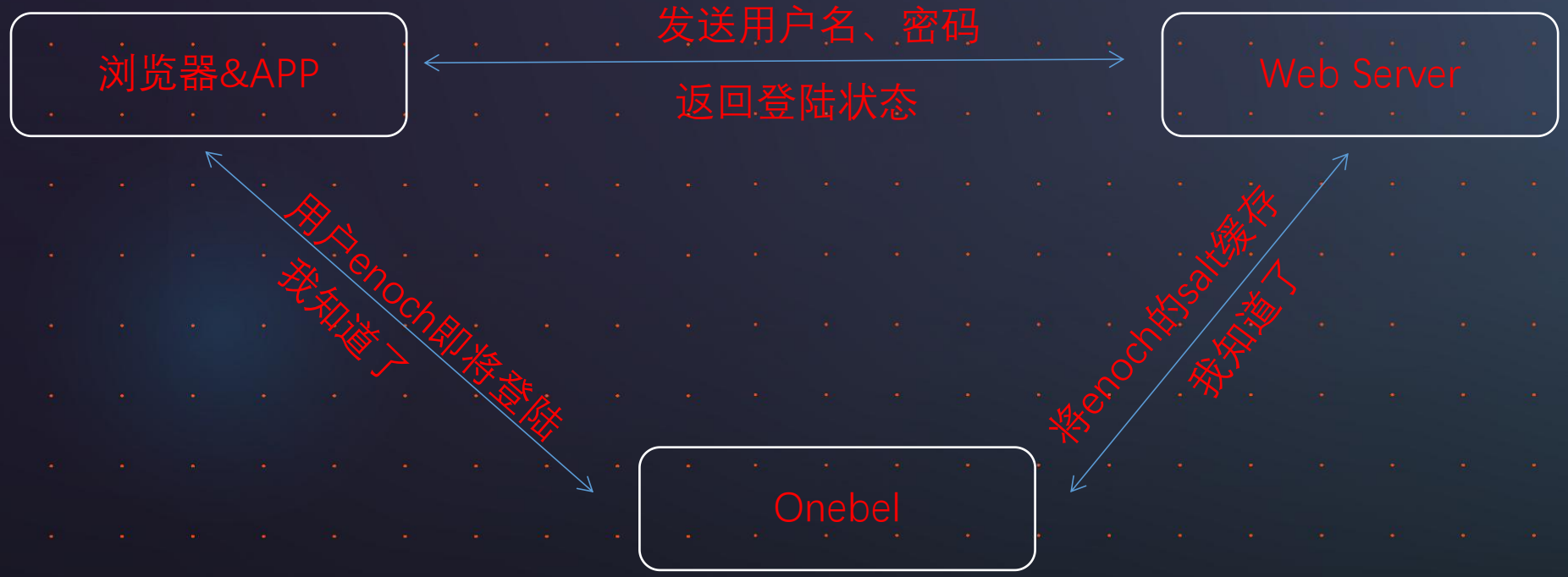
1. Onebel的数据可以读取，但是不能被黑客一下子扒光；

   不能是Onebel与Web Server二者之间进行通讯

2. Onebel的数据不能影响网页的加载速率；

   需要用户预请求和服务器预缓存

模型图


浏览器&APP
发送用户名、密码
返回登陆状态
Web Server
用户enoch即将登陆
我知道了
将enoch的salt缓存
我知道了
Onebel

风控引擎

如果黑客在网页的前端不断的请求用户名，要求Onebel将所有用户的salt发送给服务器怎么办？

1.Onebel将设计一个强大的风险控制引擎，计算网页、APP前端传来的设备指纹，包括但不仅限于：IP、浏览器头、MAC地址、DEVID、内网IP。通过这些参数，一个黑客要获取走所有的用户salt需要大量伪造IP地址等信息

2.风控引擎将设置超频报警，超频验证等，一但超过频率的请求Onebel数据，Onebel将要求前端进行用户真实身份校验

Onebel.js

为什么不会影响网页的加载速率呢？

1. Onebel. js会在用户输入用户名后马上告知Onebel该用户要登陆了，在这之后Onebel会在用户输入完密码之前就把数据缓存到SSO服务器

2. Onebel会在cookie中储存用户名信息，即便用户采用了记住密码，也能在点击登陆时完成缓存

3. 这种操作降低了SSO服务器登陆所需时间

Onebel宏图

■ SSO登陆
· 储存salt

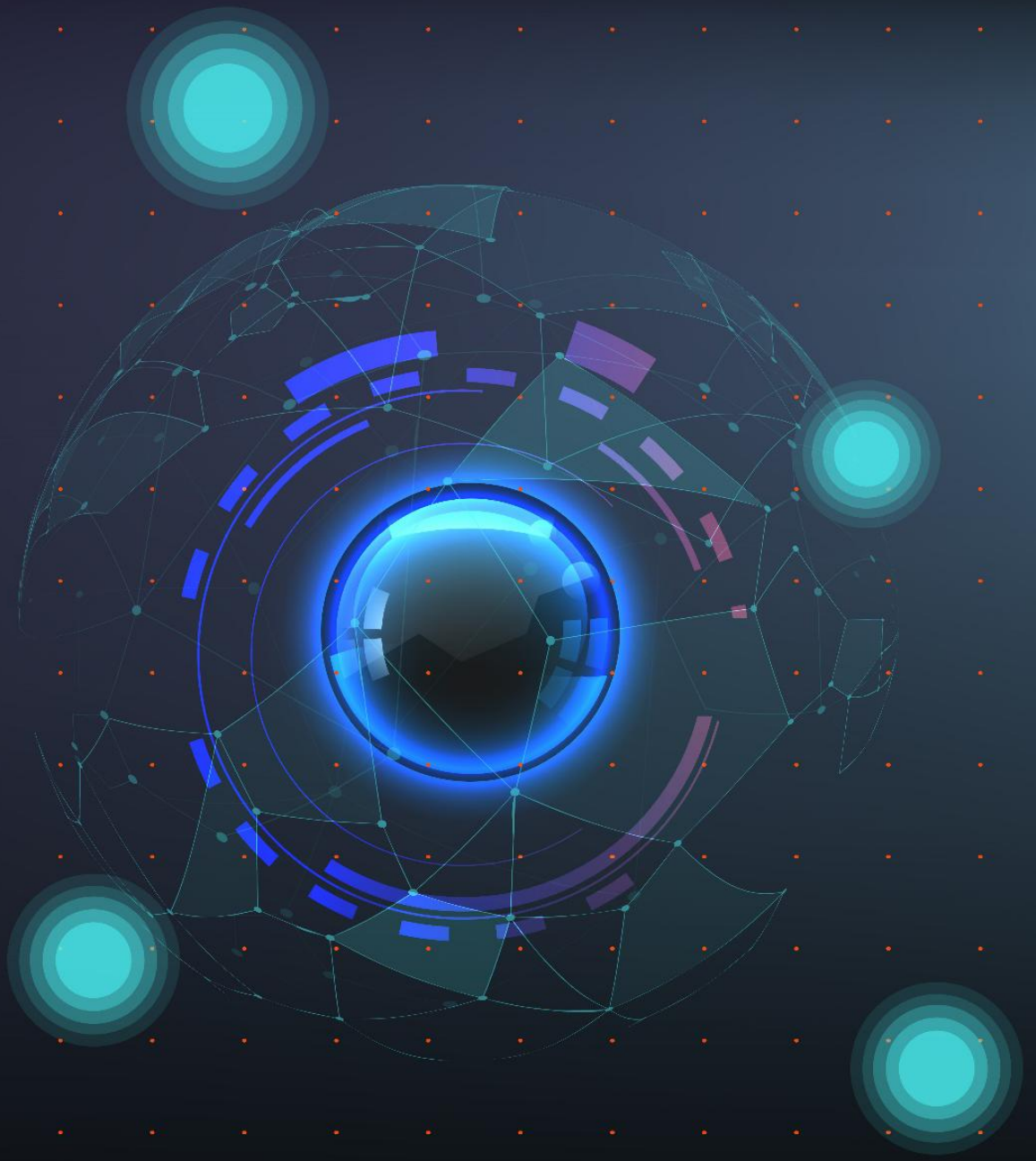
■ 支付系统
· 储存收获地址
· 储存银行卡信息

■ 用户系统
· 储存密保问题答案
· 储存用户身份证信息
· 储存用户注册信息

■认证系统
· 储存身份证信息
· 储存照片信息
· 储存认证指纹

■ 区块链
· 智能合约

THE PART THREE
第三部分
——开发计划



Onebel的基本架构

现实需求

ONEBEL的基本架构

前端?

Onebel服务器?

Web Server?

Onebel的基本架构

1.前端

Onebel.js基于原生JavaScript进行开发

2.Onebel服务器

风控引擎基于python

数据存储将选用nosql

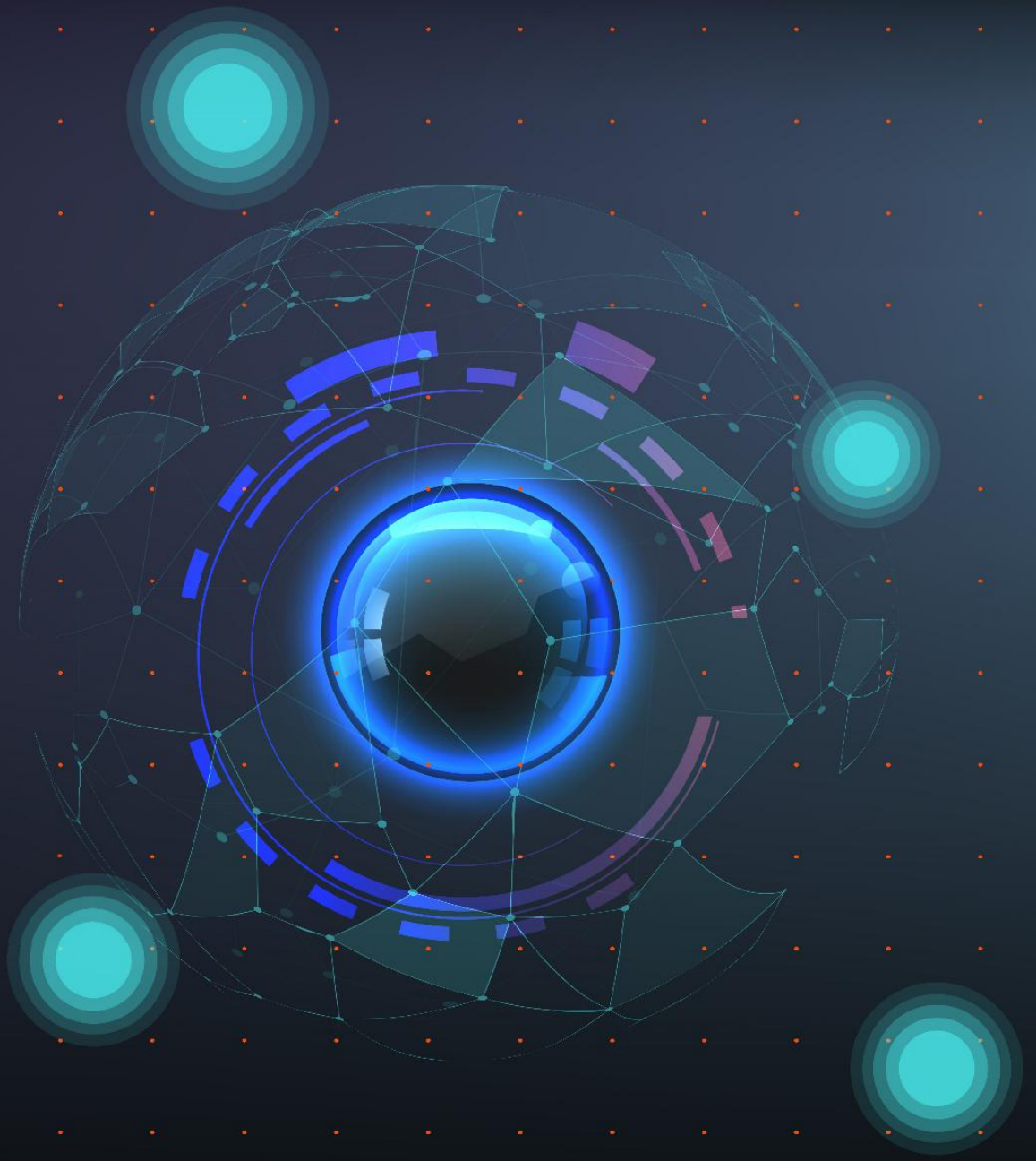
web api将基于python的web.py进行开发

3.Web Server

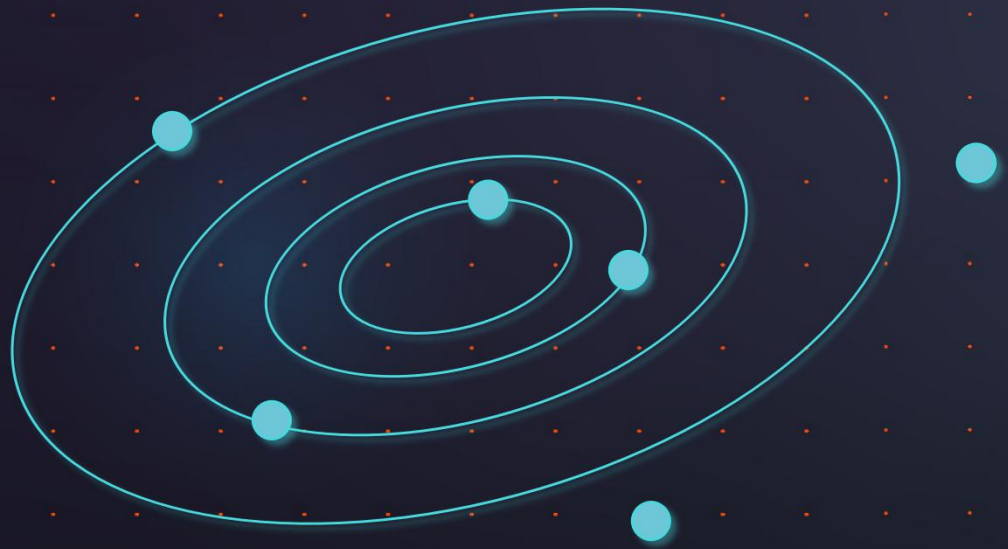
开发者根据自己的服务对接Onebel

Onebel将提供bash脚本检测并定期清理日志文件（如果需要日志进行分析，日志文件需要转发到第三方），自动销毁缓存的信息

THE PART FOUR
第四部分
——开源计划



Onebel的开源计划

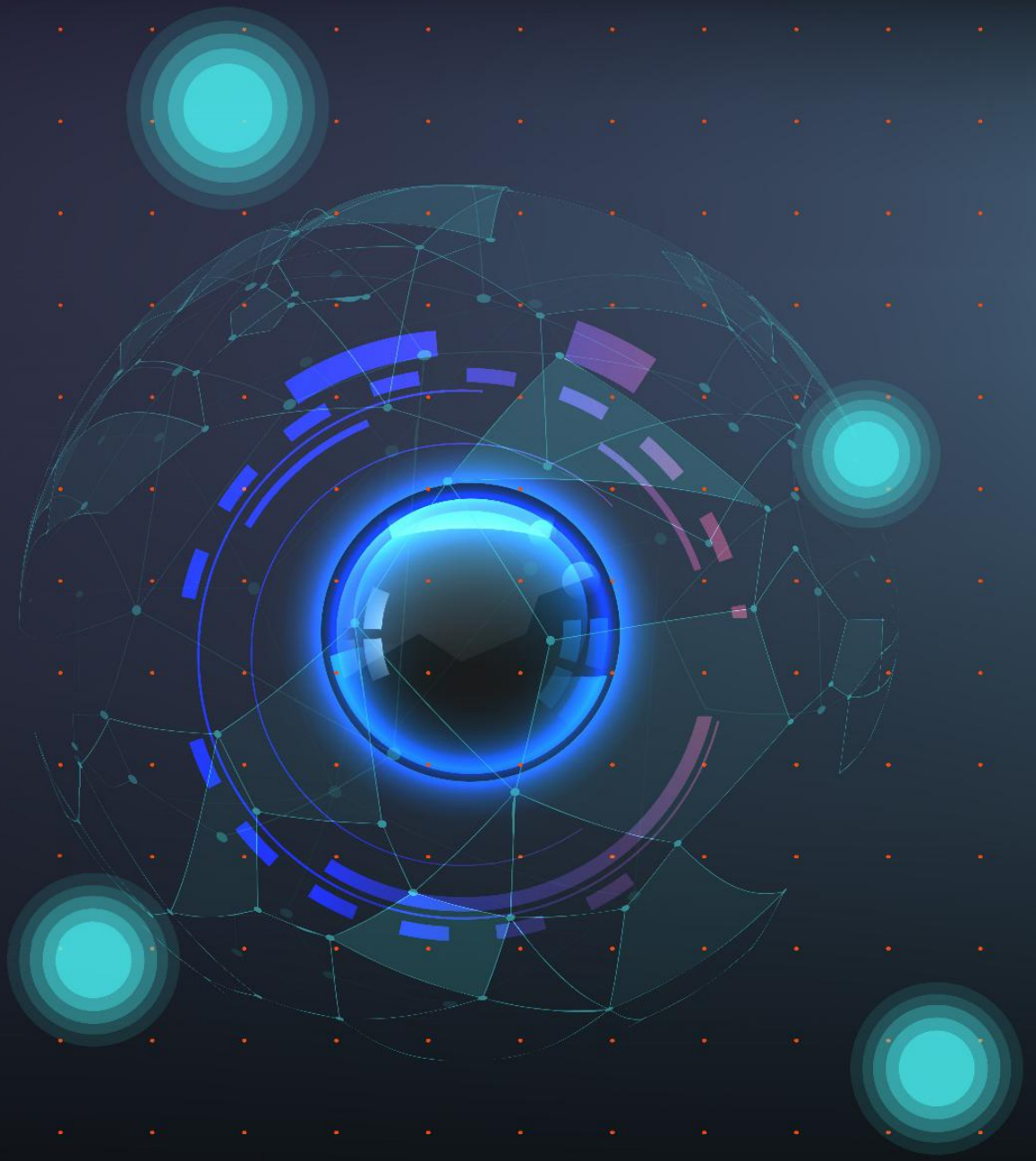


Onebel将是一个庞大的数据安全系统，它将广泛运用于大数据的关键存储中，这样一个庞大的项目唯有开源才能推进项目的进行

该系统的代码将发布到github上，并且在官网更新项目进程和文档 http://www.onebel.org

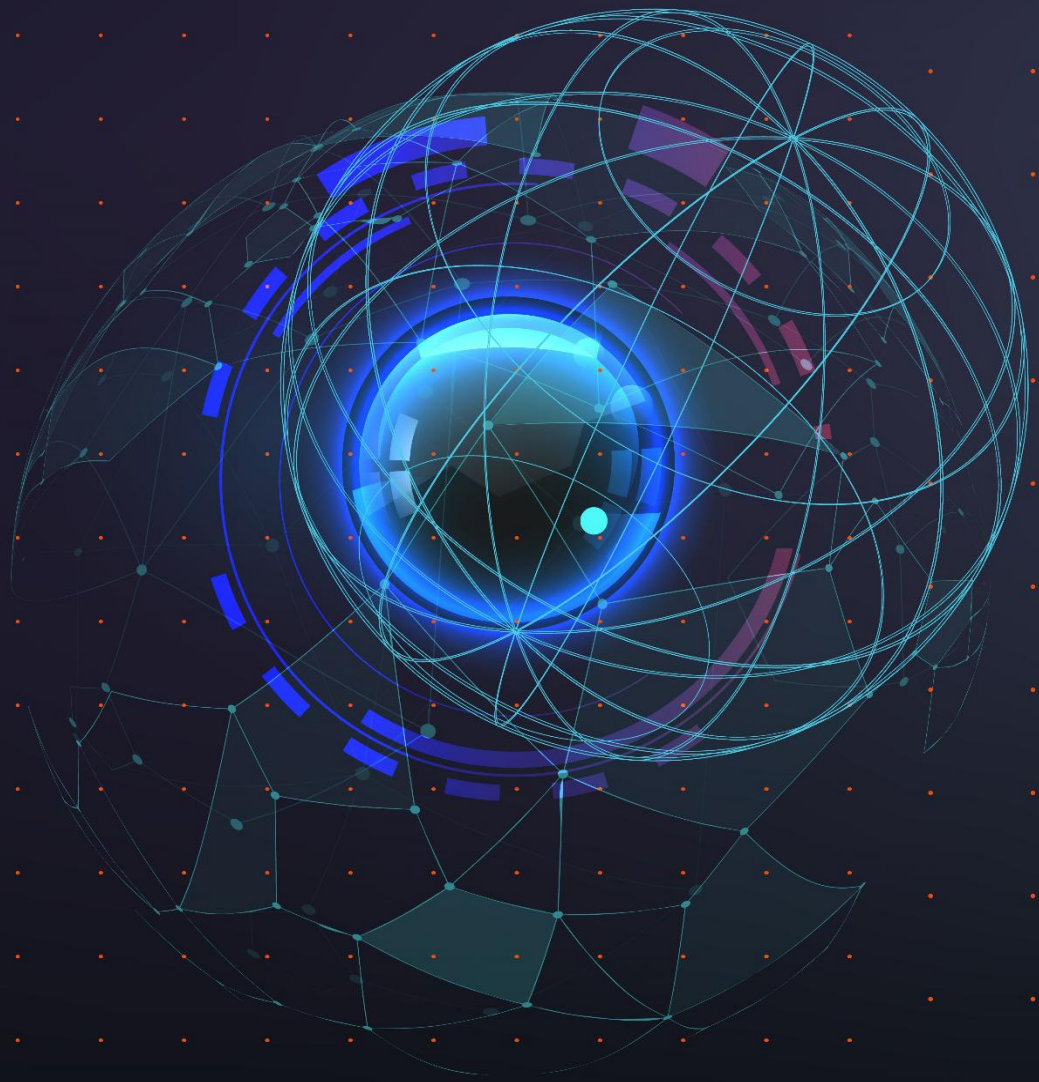
THE PART FIVE
第五部分

——致敬linus



为什么是Onebel

托瓦兹利用个人时间及器材创造出了这套当今全球最流行的操作系统内核之一。而他的毕业设计就是linux操作系统，所以我的毕业设计将不是一个商用系统，是一个开源的项目，他将维护网络安全和个人信息安全



感谢聆听
THAKS

INTELLIGENT FACTORY SYSTEM SOLUTION

演讲：林章