

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»**

Факультет безопасности информационных технологий

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

“Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей”

Выполнил:

Студент гр. Р32141

Полуянов Александр Михайлович

Проверила:

Коржук Виктория Михайловна

Санкт-Петербург

2023 г.

Цель работы:

получить знания и навыки работы с различными базами данных угроз и уязвимостей. Работа индивидуальная.

Объекты:

1. Обязательный материал для ознакомления:
 - 1.1. <https://habr.com/ru/company/pt/blog/266485/>
 - 1.2. <https://habr.com/ru/company/ic-dv/blog/453756/>
 - 1.3. [https://xakep.ru/2009/05/15/48221/#toc01.](https://xakep.ru/2009/05/15/48221/#toc01)
 - 1.4. <https://habr.com/ru/company/xakep/blog/305262/>
2. БД угроз и уязвимостей (описываем 5 БД и прикладываем пару скриншотов):
 - 2.1. ФСТЭК
 - 2.2. Vulners
 - 2.3. CVE (NVD)
 - 2.4. cert/cc
 - 2.5. secunia
 - 2.6. exploit in
 - 2.7. X-Force
 - 2.8. SecurityFocus
 - 2.9. CNNVD
 - 2.10. JVN
 - 2.11. <https://www.exploit-db.com>
3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

Ход работы:

БД угроз и уязвимостей:

1) ФСТЭК

Аббревиатура расшифровывается как Федеральная служба по техническому и экспортному контролю. Это крупнейшая и наиболее значимая база уязвимостей на русском языке. Банк угроз ФСТЭК содержит, помимо названия и кода угрозы, её краткое описание, вероятные источники, объекты воздействия и, конечно, последствия, которые повлечёт за собой реализация угрозы.

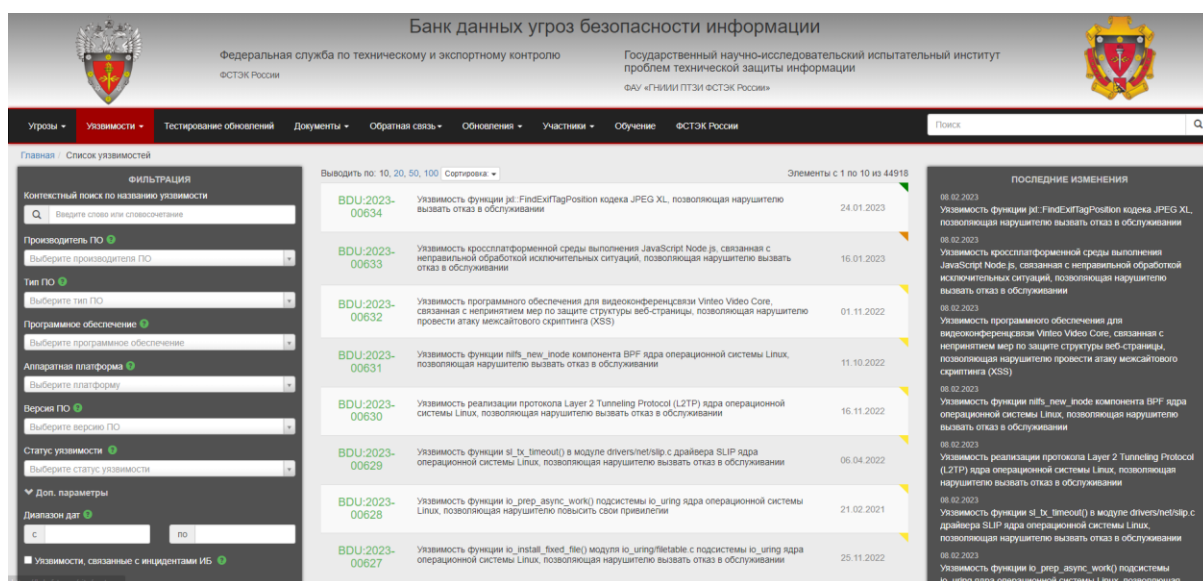


Рисунок 1 - Список уязвимостей по данным ФСТЭК

2) Vulners

Vulners — это очень большая и непрерывно обновляемая база данных ИБ-контента. Сайт позволяет искать уязвимости, эксплойты, патчи, результаты bug bounty так же, как обычный поисковик ищет сайты. Vulners агрегирует и представляет в удобном виде шесть основных типов данных: популярные базы уязвимостей, вендорские бюллетени безопасности, эксплойты из Exploit-DB и Metasploit, Nessus-плагины

для детекта уязвимостей, дисклозы багов с сайтов bug bounty программ, публикации на тематических ресурсах.

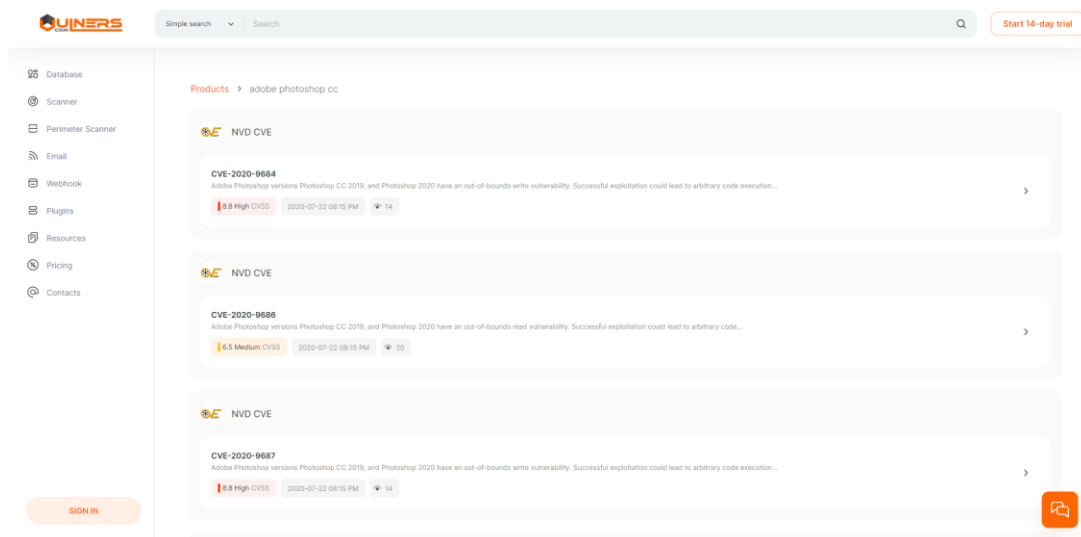


Рисунок 2 - Пример поиска уязвимостей в программе Adobe Photoshop

3) **CERT Coordination Center (CERT/CC)**

Наряду с проведением независимых исследований и решением различных задач по обеспечению безопасности глобальной информационной инфраструктуры, эта организация обеспечивает централизованный сбор сведений обо всех уязвимостях в различных информационных системах и поддержание актуальной базы знаний об уязвимостях в информационных системах. Сведения о вновь выявляемых уязвимостях, вредоносных программах и способах нарушения информационной безопасности рассылаются по электронной почте: подписчиками этого бюллетеня являются более 161000 специалистов во всем мире.

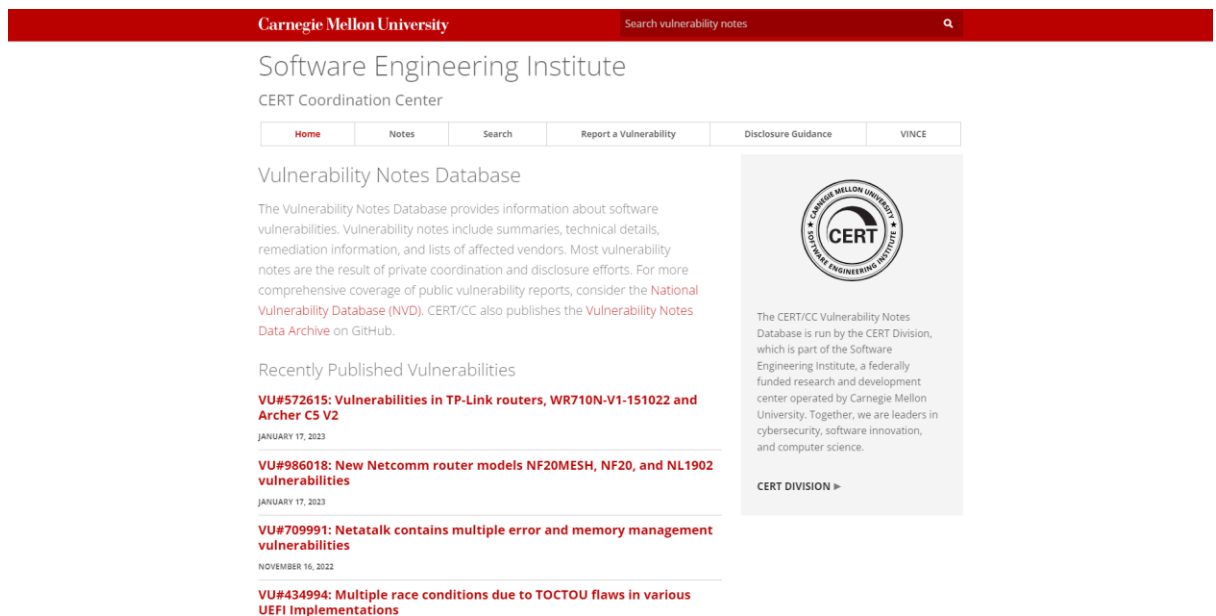


Рисунок 3 - Вид главной страницы сайта CERT/CC

4) Secunia

Secunia - датская компания, специализирующаяся на компьютерной и сетевой безопасности. Наибольшую известность приобрела благодаря своим тестам на наличие уязвимостей. Эти тесты прошли более 12400 программных продуктов и ОС.

15 сентября 2015 года компания Flexera Software объявила о приобретении компании Secunia. Условия сделки не разглашаются.

По мнению Питера Колстеда (Peter Colsted), CEO компании Secunia, приобретение позволит предприятиям "проактивно противостоять кибер-угрозам безопасности в рамках своей основной деятельности по управлению использованием приложений".

Multiple ways to consume Secunia Research

Secunia delivers software security research that provides reliable, curated and actionable vulnerability intelligence. Organizations can expect to receive standardized, validated and enriched vulnerability research on a specific version of a software product. Secunia Research supports four solutions:



Software Vulnerability Research

Software Vulnerability Research utilizes Secunia Research to drive awareness of vulnerabilities matching your specified criteria

[LEARN MORE >](#)



Software Vulnerability Manager

Software Vulnerability Manager uses Secunia Research data to identify, prioritize and patch known vulnerable software detected in your environment

[LEARN MORE >](#)



Data Platform

Data Platform leverages Secunia Research to provide high-level insights based on major or minor versions of software in your normalized inventory

[LEARN MORE >](#)



Flexera One

Flexera One utilizes Secunia Research (alongside public NVD data) to provide more granular matching of build-level versions of software in your normalized inventory within its IT Asset Management and IT Visibility solutions

[LEARN MORE >](#)

Рисунок 4 - Описание Secunia с сайта flexera.com

5) Exploit Data Base

База данных Exploit — это архив публичных эксплойтов и соответствующего уязвимого программного обеспечения, разработанный для использования тестировщиками проникновения и исследователями уязвимостей. Его цель — служить наиболее полным набором эксплойтов, шелкодека и документов, собранных с помощью прямых представлений, списков рассылки и других общедоступных источников, и представлять их в свободно доступной и простой для навигации базе данных. База данных Exploit — это хранилище эксплойтов и доказательств концепций, а не советов, что делает его ценным ресурсом для тех, кто нуждается в действительных данных сразу.

Date	D	A	V	Title	Type	Platform	Author
2022-11-11				SmartRG Router SR510n 2.6.13 - Remote Code Execution	Remote	Hardware	Yerodin Richards
2022-11-11				CVAT 2.0 - Server Side Request Forgery	WebApps	Python	Emir Polat
2022-11-11				IoTTransfer V4 - Unquoted Service Path	Local	Windows	BLAY ABU SAFIAN
2022-11-11				AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal	Remote	Hardware	Jens Regel
2022-11-11				MSNSwitch Firmware MNT.2408 - Remote Code Execution	Remote	Hardware	Eli Fulkerson
2022-11-11				Open Web Analytics 1.7.3 - Remote Code Execution	WebApps	PHP	Jacob Ebben
2022-10-17				Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	ABDO10
2022-10-06				Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi	WebApps	PHP	Rizacan Tufan
2022-09-23				Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)	WebApps	PHP	Ashkan Moghaddas

Рисунок 5 - Список эксплойтов с официального сайта

1. Оцените уязвимости по базовым метрикам для ситуации при следующих условиях:

а) атака высокой сложности будет проводится на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению целостности высокого уровня. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.

Главная | Калькулятор CVSS V3
Вектор CVSS v3: (AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N)

Базовые метрики **4.8**

Базовая оценка (BS): **4.8**

Вектор атаки (AV):
☐ Сетевой (N) ☐ Смежная сеть (A) ☐ Локальный (L) ☒ Физический (P)

Сложность атаки (AC):
☒ Высокая (H) ☐ Низкая (L)

Уровень привилегий (PR):
☐ Высокий (H) ☒ Низкий (L) ☐ Не требуется (N)

Взаимодействие с пользователем (UI):
☐ Требуется (R) ☒ Не требуется (N)

Влияние на другие компоненты системы (S):
☐ Не оказывает (U) ☒ Оказывает (C)

Влияние на конфиденциальность (C):
☒ Не оказывает (N) ☐ Низкое (L) ☐ Высокое (H)

Влияние на целостность (I):
☐ Не оказывает (N) ☐ Низкое (L) ☒ Высокое (H)

Влияние на доступность (A):
☒ Не оказывает (N) ☐ Низкое (L) ☐ Высокое (H)

Рис 6. Оценка по базовым метрикам

Базовая оценка (BS): **4.8**

Вектор CVSS v3: (AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N)

2. Оцените уязвимости по временным метрикам для ситуации при следующих условиях:

в) Предполагается, что есть PoC-код для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

Главная / Калькулятор CVSS V3

Вектор CVSS v3: (AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:X/RC:C)

Базовые метрики	4.8	AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N
Временные метрики	4.6	E:P/RL:X/RC:C

Временная оценка (TS): 4.6

Доступность средств эксплуатации (E):

Не определено (X)	Высокая (H)	Есть сценарий (F)	Есть PoC-код (P)	Теоретическая (U)
-------------------	-------------	-------------------	-------------------------	-------------------

Доступность средств устранения (RL):

Не определено (X)	Недоступно (U)	Рекомендации (W)	Временное (T)	Официальное (O)
--------------------------	----------------	------------------	---------------	-----------------

Степень доверия к информации об уязвимости (RC):

Не определено (X)	Подтверждена (C)	Достоверные отчеты (R)	Отчеты (U)
-------------------	-------------------------	------------------------	------------

Рисунок 7 - Оценка по временным метрикам

Временная оценка (TS): **4.6**

3. Оцените уязвимости по контекстным метрикам для ситуации при следующих условиях:

е) К уровню обеспечения КЦД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака неопределенной сложности на сетевой уровень системы. Уровень привилегий в данном случае - низкий, взаимодействия с пользователем не происходит. Также оказывается влияние на другие компоненты системы.

Вектор CVSS v3 (AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:X/RC:CCR:H/IR:H/AR:H/MAV:N/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L)

Базовые метрики 24

Временные метрики 15

Контекстные метрики 7

AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:X/RC:CCR:H/IR:H/AR:H/MAV:N/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L

Контекстная оценка (ES): 7

Требования к конфиденциальности (CR):

Не определено (X)

Низкое (L)

Среднее (M)

Высокое (H)

Требования к целостности (IR):

Не определено (X)

Низкое (L)

Среднее (M)

Высокое (H)

Требования к доступности (AR):

Не определено (X)

Низкое (L)

Среднее (M)

Высокое (H)

Вектор атаки (корр.) (MAV):

Не определено (X)

Сетевой (N)

Смешанная сеть (A)

Локальный (L)

Физический (P)

Сложность атаки (корр.) (MAC):

Не определено (X)

Высокая (H)

Низкая (L)

Уровень привилегий (корр.) (MPR):

Не определено (X)

Высокий (H)

Низкий (L)

Не требуется (N)

Взаимодействие с пользователем (корр.) (MUI):

Не определено (X)

Требуется (R)

Не требуется (N)

Влияние на другие компоненты системы (корр.) (MS):

Не определено (X)

Не оказывает (U)

Оказывает (C)

Влияние на конфиденциальность (корр.) (MC):

Не определено (X)

Не оказывает (N)

Низкое (L)

Высокое (H)

Влияние на целостность (корр.) (MI):

Не определено (X)

Не оказывает (N)

Низкое (L)

Высокое (H)

Влияние на доступность (корр.) (MA):

Не определено (X)

Не оказывает (N)

Низкое (L)

Высокое (H)

Рисунок 8 - Оценка по контекстным метрикам

Контекстная оценка (ES): 7

Вектор CVSS v3:

(AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:X/RC:CCR:H/IR:H/AR:H/MAV:N/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L)

Вывод:

В ходе работы мною были изучены различные базы данных уязвимостей и получены навыки по работе с ними. Во второй части лабораторной работы получен опыт работы с калькулятором CVSS v3.