

**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. N3253

Пастухова А.А.



Проверил:

Якимова С.А.

Санкт-Петербург

2022г.

Цель работы: получить знания и навыки работы с различными базами данных угроз и уязвимостей.

Ход работы:

1. CVE (Common Vulnerabilities and Exposures)

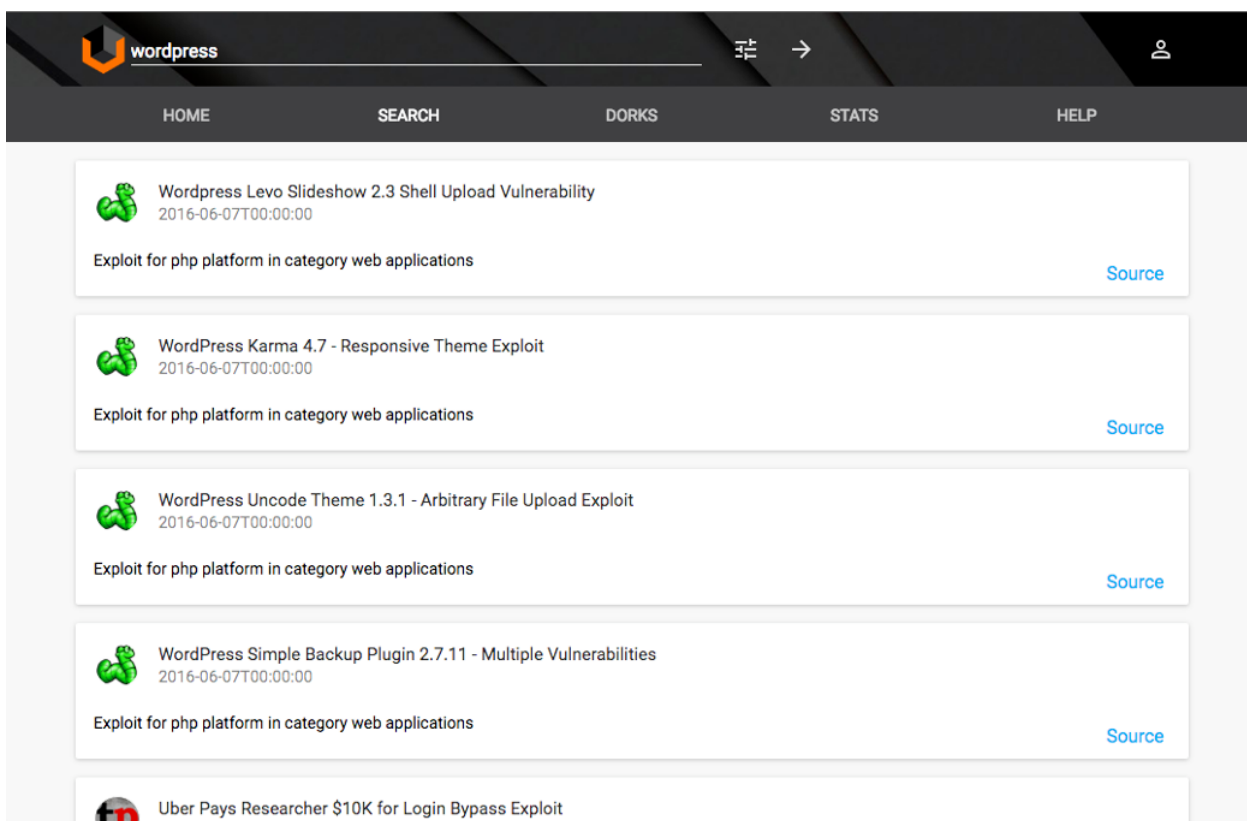
Так называемый "словарь" известных уязвимостей, имеющий строгую характеристику по описательным критериям. Полностью CVE можно отыскать в Национальной Базе Уязвимостей США (National Vulnerability Database). Общий вид записи CVE выглядит примерно так: CVE ID, Reference и Description, ID записывается с указанием кода и порядкового номера. В поле Reference записываются различного рода ссылки на патчи, рекомендательного рода документы или комментарии разработчика. Description отвечает за описание самой уязвимости.

The screenshot displays the CVE-2016-9637 entry on the NVD website. The page includes a navigation bar with links like 'CVE List', 'CNA's', 'WG's', 'Board', 'About', and 'News & Blog'. A prominent notice states: 'Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)'. Below this, the CVE ID 'CVE-2016-9637' is listed with a link to 'Learn more at National Vulnerability Database (NVD)'. The description states: 'The (1) ioport_read and (2) ioport_write functions in Xen, when qemu is used as a device model within Xen, might allow local x86 HVM guest OS administrators to gain qemu process privileges via vectors involving an out-of-range ioport access.' A list of references is provided, including links to security focus, xenbits, support.citrix.com, gentoo.org, debian.org, redhat.com, and securitytracker.com. The assigning CNA is listed as MITRE Corporation, and the date record created is 20161123.

2. Vulners

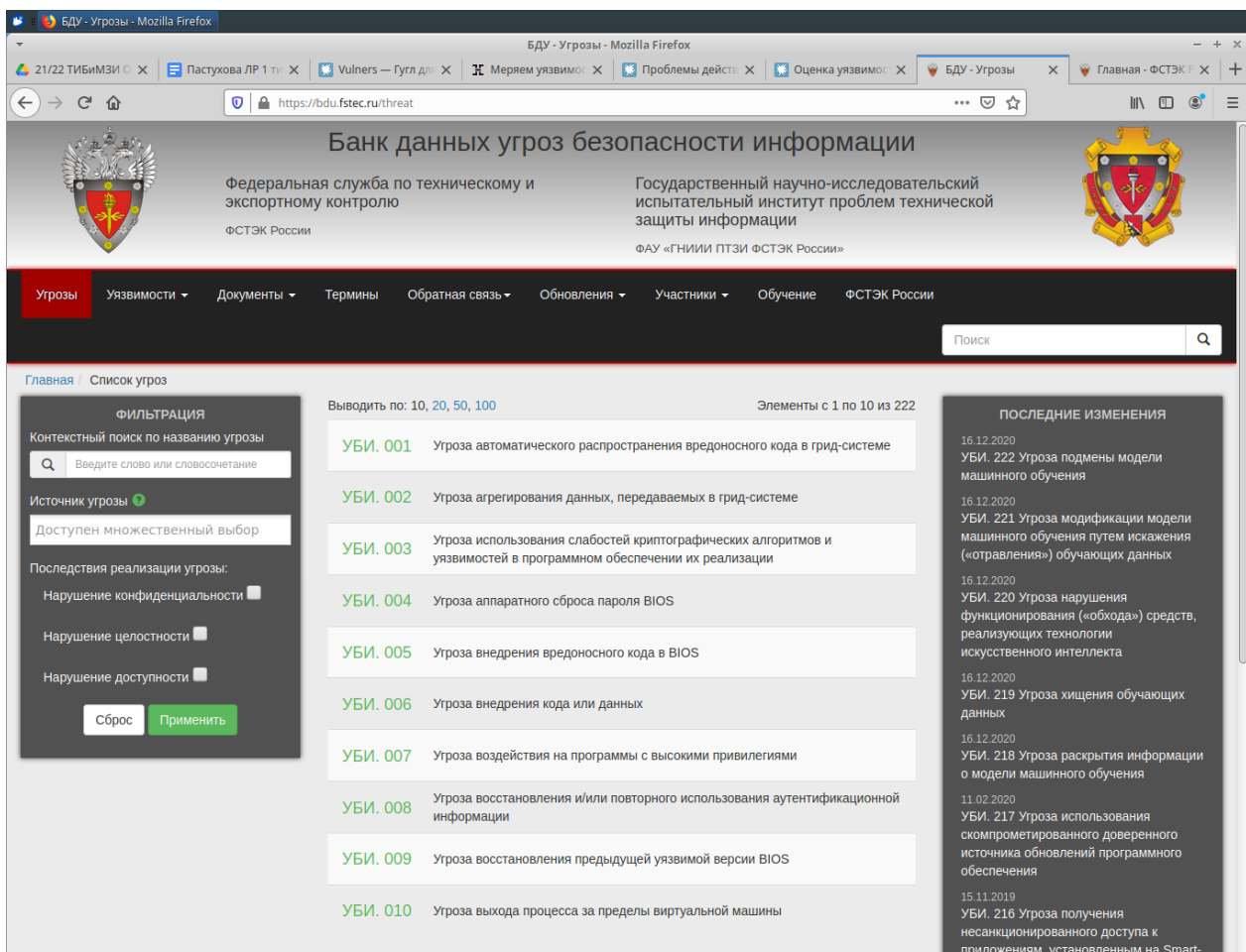
Очень большая и непрерывно обновляемая база данных ИБ-контента. Он агрегирует и представляет в удобном виде шесть основных типов данных: популярные базы уязвимостей, вендорские бюллетени безопасности, эксплойты из Exploit-DB и Metasploit, Nessus-плагины для детекта

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



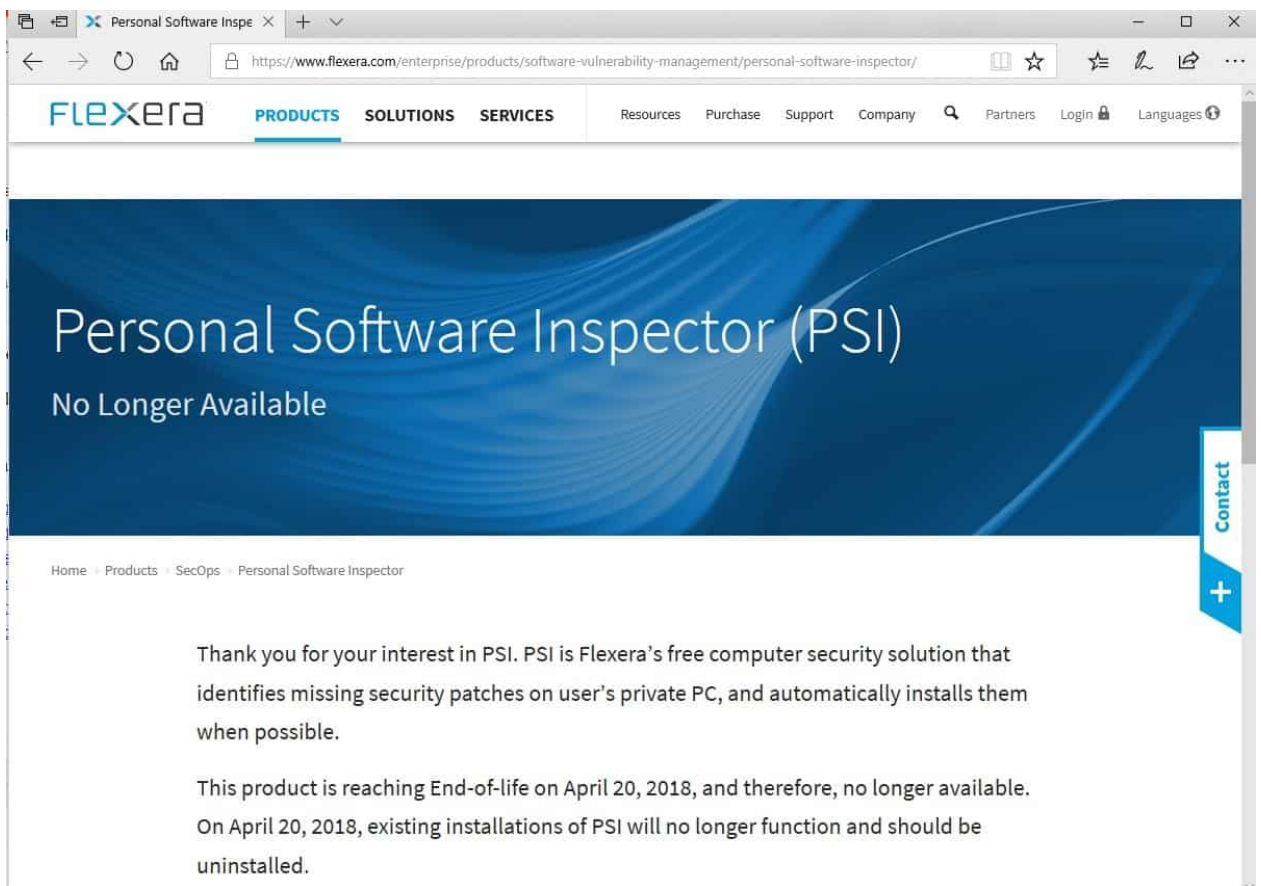
3. ФСТЭК

Федеральная служба по техническому и экспортному контролю. База данных содержит перечень угроз и уязвимостей программного обеспечения, согласно законодательству РФ. Список постоянно пополняется и обновляется.



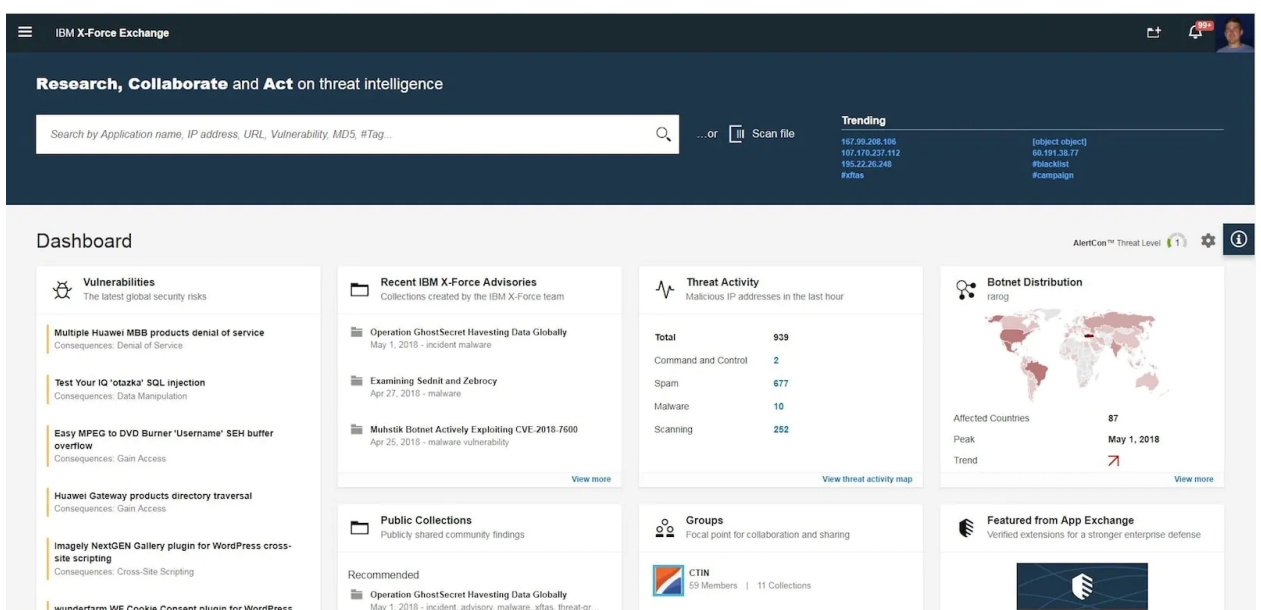
4. Secunia

Датская компания, специализирующаяся на компьютерной и сетевой безопасности. Наиболее известна своими тестами на наличие уязвимостей, которые прошли более 12,400 программных продуктов и операционных систем. Подписка платная.



5. X-Force

Облачная платформа для обмена аналитическими данными об угрозах, которая позволяет быстро исследовать новейшие угрозы безопасности, собирать практически полезные аналитические данные и сотрудничать с коллегами. Кроме всего прочего также описывает материальный ущерб, который может повлечь за собой угроза эксплуатации.



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

е) атака высокой сложности будет проводится на сетевой уровень системы, при этом не оказывается влияние на другие компоненты системы. Атака приводит к нарушению конфиденциальности и целостности высокого уровня, доступности низкого уровня. При этом требуется взаимодействие с пользователем, уровень привилегий - низкий.

The screenshot shows the BDU - CVSS v3 Calculator interface in a Mozilla Firefox browser. The page title is "БДУ - CVSS v3 Calculator - Mozilla Firefox". The URL is "https://bdu.fstec.ru/calculator". The page header includes the logo of the Federal Security Service of Russia (ФСБ России) and the text "экспортному контролю" and "испытательный институт проблем технической защиты информации". The main navigation bar includes links for "Угрозы", "Уязвимости", "Документы", "Термины", "Обратная связь", "Обновления", "Участники", "Обучение", and "ФСБ России". The search bar contains the text "Поиск". The main content area shows the "Базовые метрики" section with a "Базовая оценка (BS): 6.7". The "Вектор атаки (AV)" is set to "Сетевой (N)". The "Сложность атаки (AC)" is set to "Высокая (H)". The "Уровень привилегий (PR)" is set to "Низкий (L)". The "Взаимодействие с пользователем (UI)" is set to "Требуется (R)". The "Влияние на другие компоненты системы (S)" is set to "Не оказывает (U)". The "Влияние на конфиденциальность (C)" is set to "Высокое (H)". The "Влияние на целостность (I)" is set to "Высокое (H)". The "Влияние на доступность (A)" is set to "Низкое (L)".

Метрика	Значение
Базовая оценка (BS)	6.7
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Высокая (H)
Уровень привилегий (PR)	Низкий (L)
Взаимодействие с пользователем (UI)	Требуется (R)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Низкое (L)

Результат 6.7

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

е) Предполагается, что есть сценарий для средств эксплуатации, есть рекомендации для средств устранения, а информация об уязвимостях получена из достоверных отчетов.

Результат 6.1

БДУ - CVSS v3 Calculator - Mozilla Firefox

https://bdu.fstec.ru/cal3

Угрозы **Уязвимости** Документы Термины Обратная связь Обновления Участники Обучение ФСТЭК России

Поиск

Контекстные метрики 6.7 CR:H/IR:H/AR:H/MAV:N/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L

Контекстная оценка (ES): 6.7

Требования к конфиденциальности (CR):

Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)
-------------------	------------	-------------	-------------

Требования к целостности (IR):

Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)
-------------------	------------	-------------	-------------

Требования к доступности (AR):

Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)
-------------------	------------	-------------	-------------

Вектор атаки (корр.) (MAV):

Не определено (X)	Сетевой (N)	Смежная 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)	Низкие (L)	Высокие (H)
-------------------	------------------	------------	-------------

Влияние на целостность (корр.) (MI):

Не определено (X)	Не оказывает (N)	Низкие (L)	Высокие (H)
-------------------	------------------	------------	-------------

Влияние на доступность (корр.) (MA):

Не определено (X)	Не оказывает (N)	Низкие (L)	Высокие (H)
-------------------	------------------	------------	-------------

Вывод: я получила знания и навыки работы с различными базами данных угроз и уязвимостей. Также изучила материалы касательно метрик и калькулятора CVSS v3, посчитала базовые, временные и контекстные метрики для гипотетической ситуации.