

Внешний аудит безопасности корпоративных сетей

Лекция 1. Введение

Crypto
Kantiana



Семён Новосёлов

2021



БФУ имени
И. Канта

Содержимое курса

- оценка безопасности компьютерных сетей
- разбор сетевых атак, уязвимостей, способов их поиска и эксплуатации
- изучение основных инструментов: **metasploit**, **nmap**, **wireshark** и др.
- практическая направленность

Основные понятия

- **Уязвимость** — недостаток в системе, ведущий к нарушению её безопасности. Например, позволяет:
 - выполнить произвольный код
 - получить несанкционированный доступ к информации
- **Эксплойт** — программа, которая использует уязвимость для проведения атаки на систему
- **Аудит** — процесс оценки безопасности системы (санкционированный)

Стадии сетевой атаки

- **Сбор информации**
 - информация о ПО и его версиях, доменах
- **Анализ уязвимостей**
 - поиск по базам известных уязвимостей и эксплойтов
 - самостоятельное нахождение уязвимостей в ПО
- **Эксплуатация**
 - разработка/выбор эксплойта и его использование
- **Постэксплуатация**
 - выполнение вредоносной нагрузки (рассылка спама, сбор личной информации)
 - эскалация привилегий, продвижение по сети дальше
- **Подготовка отчёта (при аудите)**

Базы с уязвимостями (CVE/NVD)

- CVE
 - классификатор уязвимостей в конкретных программах и их компонентах
 - уязвимостям назначаются уникальные номера
 - содержит список ссылок с информацией о уязвимостях
- NVD
 - собирает воедино информацию из различных классификаторов и баз (CPE/CWE/CVE и др.)
 - <https://nvd.nist.gov/vuln/search>
 - Доступна для свободного скачивания в формате JSON (<https://nvd.nist.gov/vuln/data-feeds>)

Пример. Список уязвимостей в Chrome. 1/3

Q Search Results (Refine)

Sort results by: Publish Date Descending Sort

Search)

Search Parameters:

- Results Type: Overview
- Keyword (text search): chrome
- Search Type: Search All

There are 2,602 matching records.
Displaying matches 1 through 20.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2021-21116	Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. Published: январь 08, 2021; 2:15:15 PM -0500	V3.1: 8.8 HIGH V2.0: 6.8 MEDIUM
CVE-2021-21115	User after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. Published: январь 08, 2021; 2:15:15 PM -0500	V3.1: 9.6 CRITICAL V2.0: 6.8 MEDIUM
CVE-2021-21114	Use after free in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. Published: январь 08, 2021; 2:15:15 PM -0500	V3.1: 8.8 HIGH V2.0: 6.8 MEDIUM

← → ↺

🔒 nvd.nist.gov/vuln/detail/CVE-2021-21116

☆ ABP NEW

⚙️ 👤

 CVE-2021-21116 Detail

Current Description

Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

Краткое описание уязвимости

Base Score: 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка опасности

Пример. Список уязвимостей в Chrome. 2/3

Hyperlink	Resource
https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html	Release Notes Vendor Advisory
https://crbug.com/1151069	Permissions Required Vendor Advisory
https://security.gentoo.org/glsa/202101-05	Third Party Advisory

Список ссылок с дополнительной информацией об уязвимости

CWE-ID	CWE Name	Source
CWE-787	Out-of-bounds Write	 NIST

Класс уязвимости

Пример. Список уязвимостей в Chrome. 3/3

 cpe:2.3:a:google:chrome:*:*:*:*:*	Up to
Show Matching CPE(s)▼	(excluding)
	87.0.4280.141

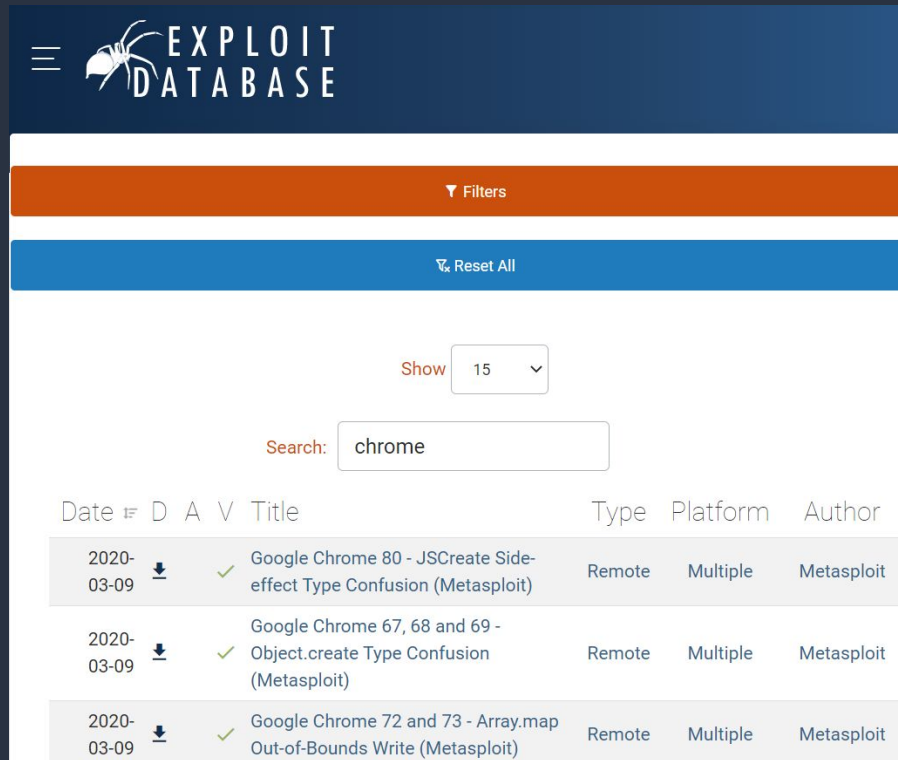
Информация об уязвимых версиях

- Аналогичным образом можно проверить по базе любое программное обеспечение или его компоненты

Базы эксплойтов

База от Offensive Security:

- www.exploit-db.com
- **SearchSploit** - утилита для поиска по базе
- большинство эксплойтов Proof-of-Concept (PoC)



The screenshot shows the Exploit Database website interface. At the top is the logo with a spider icon and the text "EXPLOIT DATABASE". Below the logo is a navigation bar with "Filters" and "Reset All" buttons. A search bar contains the text "chrome". Below the search bar is a table of search results. The table has columns: Date, D (Download), A (Add), V (Vote), Title, Type, Platform, and Author. Three results are visible, all dated 2020-03-09 and authored by Metasploit.

Date	D	A	V	Title	Type	Platform	Author
2020-03-09	↓	✓		Google Chrome 80 - JSCreate Side-effect Type Confusion (Metasploit)	Remote	Multiple	Metasploit
2020-03-09	↓	✓		Google Chrome 67, 68 and 69 - Object.create Type Confusion (Metasploit)	Remote	Multiple	Metasploit
2020-03-09	↓	✓		Google Chrome 72 and 73 - Array.map Out-of-Bounds Write (Metasploit)	Remote	Multiple	Metasploit

Вероятность успеха атаки

- Многие коммерческие компании работают по принципу “работает - не трогай”
- ПО может не обновляться годами
- Даже низкоквалифицированный хакер может взломать такую систему, используя уже готовые эксплойты к известным уязвимостям
- При этом проверить сеть можно общедоступными сканерами уязвимостей, например **OpenVAS**

Виды уязвимостей

- **OWASP Top 10**: самые опасные классы уязвимостей сайтов
- **CWE** - наиболее полная общая база/классификатор видов уязвимостей

OWASP Top 10 2017

- A1: **Injection**
- A2: **Broken Authentication**
- A3: **Sensitive Data Exposure**
- A4: **XML External Entities (XXE)**
- A5: **Broken Access Control**
- A6: **Security Misconfiguration**
- A7: **Cross Site Scripting (XSS)**
- A8: **Insecure Deserialization**
- A9: **Using Components with Known Vulnerabilities**
- A10: **Insufficient Logging & Monitoring**

База слабостей (CWE)

- база слабостей для сортировки уязвимостей по классам
- содержит подробное описание слабостей с примерами

← → ↻ <https://cwe.mitre.org/top25>    

The CWE Top 25

Below is a brief listing of the weaknesses in the 2020 CWE Top 25, including the overall score of each.

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
[11]	CWE-190	Integer Overflow or Wraparound	15.81
[12]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67
[13]	CWE-476	NULL Pointer Dereference	8.35
[14]	CWE-287	Improper Authentication	8.17
[15]	CWE-434	Unrestricted Upload of File with Dangerous Type	7.38
[16]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.95
[17]	CWE-94	Improper Control of Generation of Code ('Code Injection')	6.53

Список самых опасных уязвимостей по версии разработчиков CWE

Пример: внедрение кода (CWE-94)

← → ↺ cwe.mitre.org/data/definitions/94.html ☆ ABP NEW ⚙️ 👤



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

CWE TOP 25 Most Dangerous Software Weaknesses

Home > CWE List > CWE- Individual Dictionary Definition (4.3) ID Lookup: Go

Home | About | CWE List | Scoring | Community

CWE-94: Improper Control of Generation of Code ('Code Injection')

Weakness ID: 94 Status: Draft
Abstraction: Base
Structure: Simple

Presentation Filter: Complete ▾

Description

The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Extended Description

When software allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended control flow of the software. Such an alteration could lead to arbitrary code execution.

Example 1

This example attempts to write user messages to a message file and allow users to view them.

Example Language: PHP (bad code)

```
$MessageFile = "cwe-94/messages.out";
if ($_GET["action"] == "NewMessage") {
    $name = $_GET["name"];
    $message = $_GET["message"];
    $handle = fopen($MessageFile, "a+");
    fwrite($handle, "<b>$name</b> says '$message'<hr>\n");
    fclose($handle);
    echo "Message Saved!<p>\n";
}
else if ($_GET["action"] == "ViewMessages") {
    include($MessageFile);
}
```

While the programmer intends for the MessageFile to only include data, an attacker can provide a message such as:

(attack code)

```
name=h4x0r
message=%3C?php%20system(%22/bin/ls%20-l%22);?%3E
```

which will decode to the following:

(attack code)

```
<?php system("/bin/ls -l");?>
```

The programmer thought they were just including the contents of a regular data file, but PHP parsed it and executed the code. Now, this code is executed any time people view messages.

Notice that XSS (CWE-79) is also possible in this situation.

Инструментарий

- Metasploit
 - система тестового вторжения
- Nmap
 - сетевой сканер
- Wireshark/Tcpdump
 - анализатор сетевого трафика
- Kali Linux
 - дистрибутив с инструментами для тестирования безопасности

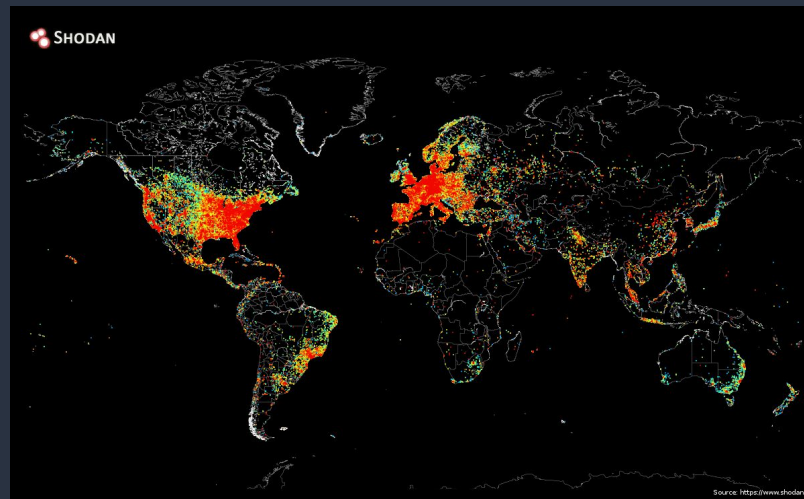
Поисковые системы

- Google Dorks

- поисковые запросы для нахождения уязвимостей и приватной информации на сайтах
- база: <https://www.exploit-db.com/google-hacking-database>

- Shodan

специализированная поисковая система для нахождения устройств (IoT), подключенных к сети



Ping-карта интернета

Машины для тренировки



HackTheBox

- список машин с уязвимостями (платные/бесплатные)
- есть сортировка по уровню сложности
- для регистрации нужно взломать их сайт
- www.hackthebox.eu



VulnHub

- виртуальные машины с уязвимостями
- www.vulnhub.com

Программы Bug Bounty

Плата за найденные уязвимости

HackerOne

- платформа для сообщений об уязвимостях и оплаты за них
- собрана вся информация по программам со всего мира
- из российских компаний: Mail.ru, Ozon, Yandex, VK

Program	Launch date ↓	Reports resolved ↓	Bounties minimum ↓	Bounties average ↓
 Verizon Media Managed	02 / 2014	6730	\$50	\$400-\$500
 Mail.ru	04 / 2014	3955	\$100	\$250-\$300
 AT&T Managed	07 / 2019	3802	\$100	\$300
 Uber Managed	12 / 2014	1579	\$500	\$500-\$750
 Twitter	05 / 2014	1250	\$280	\$560
 Slack	02 / 2014	1138	\$100	\$500
 Magento Managed	01 / 2019	1120	\$100	\$320-\$690
 Starbucks Managed	05 / 2016	1079	\$100	\$250-\$375
 Shopify	04 / 2015	1032	\$500	\$500

Список активных программ

<https://hackerone.com/directory/programs>

Пример программы. 1/2



Mail.ru
Building the Internet since 1998

<https://corp.mail.ru> · [@mailru](#)

Reports resolved	Assets in scope	Average bounty
3956	18	\$250-\$300

[Submit report](#)

Bug Bounty Program
Launched on Apr 2014

Bounty splitting enabled ?

- <https://hackerone.com/mailru>
- на данный момент выплачено 124 миллиона руб.

Пример программы. 2/2

Больше всего платят за:

- удаленное выполнение кода
- SQL-инъекции
- доступ и манипуляции с локальными файлами в обход ограничений

Mail.ru authentication center, mail, messaging, cloud services, portal, content and news projects:

Vulnerability	Main Scope	MCS	ICQ	Content
Remote code execution (RCE)	\$35000	\$25000	\$15000	\$20000
Injections (SQLi or equivalent)	\$25000	\$20000	\$10000	\$10000
Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions	\$25000	\$20000	\$10000	\$10000
RCE in standalone isolated / virtualized single-purpose process (e.g. image conversion)	\$5000	\$15000	\$5000	\$5000
SSRF, non-blind (with ability to read reply text), except dedicated proxies	\$10000	\$15000	\$5000	\$7500
SSRF, blind, except dedicated proxies	\$2000	\$2000	\$2000	\$1500



Правовые вопросы

- Не проводите тестирование на безопасность без разрешения
 - наказуемо по **статье 272 УК РФ**
- Для тренировки используйте спец. машины
- Программы поиска уязвимостей Bug Bounty
 - внимательно читайте описание программ, там есть область допустимого (Scope)
- Разработка и распространение эксплойтов
 - PoC-эксплойты разрешены
 - Остальное: на грани **статьи 273 УК РФ**

Курсы/сертификаты

1. Offensive Security Certified Professional (OSCP)

- один из наиболее известных сертификатов
- практическая направленность, сложный экзамен
- дорогая цена

2. Hacker101

- бесплатный видеокурс
- <https://youtube.com/playlist?list=PLxhvVyxYRviZd1oEA9nmnilY3PhVrt4nj>

Литература и ссылки

- Яворски П. - Ловушка для багов. Полевое руководство по веб-хакингу (2020)
 - Яворски П. - Основы веб-хакинга (2016)
 - Эрикссон Д. - Хакинг: искусство эксплойта. 2 изд. (2018)
 - Курс по Metasploit:
 - <https://www.offensive-security.com/metasploit-unleashed/>
 - Журнал Хакер:
 - <https://xakep.ru/>
- опыт работы автора на HackerOne

