Основы построения защищенных компьютерных сетей

Лекция 1. Введение

Семён Новосёлов

2022

БФУ имени И. Канта

О чём курс?

- изучение средств защиты сетей, в отличии от курса ВАБКС по пентесту
- разбор сетевых атак, уязвимостей, методов защиты от них
- изучение основных инструментов: metasploit, nmap, wireshark, iptables, snort и др.

Страница курса:
https://crypto-kantiana.com/semyon.novoselov/teaching/netsec_2022/

Содержимое курса

1. Сетевые атаки.
2. Анализ трафика. Wireshark
3. Межсетевые экраны. Iptables
4. Системы обнаружения и предотвращения вторжений. Snort
5. Криптографические протоколы. TLS
6. Виртуальные частные сети. OpenVPN
7. Безопасность беспроводных сетей. Aircrack
8. ...

Основные понятия

- Уязвимость — недостаток в системе, ведущий к нарушению её безопасности. Например, позволяет:
  - выполнить произвольный код
  - вытянуть приватную информацию
- Эксплойт — программа, которая использует уязвимость для проведения атаки на систему
- Пентест — процесс оценки безопасности системы (санкционированный)

Стадии сетевой атаки

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

Базы уязвимостей 1/2. CVE

 Common Vulnerabilities and Exposures (cve.mitre.org)

Классификатор уязвимостей в программах и их компонентах.

- уязвимости регистрируются с уникальным номером и списком ссылок с доп. информацией

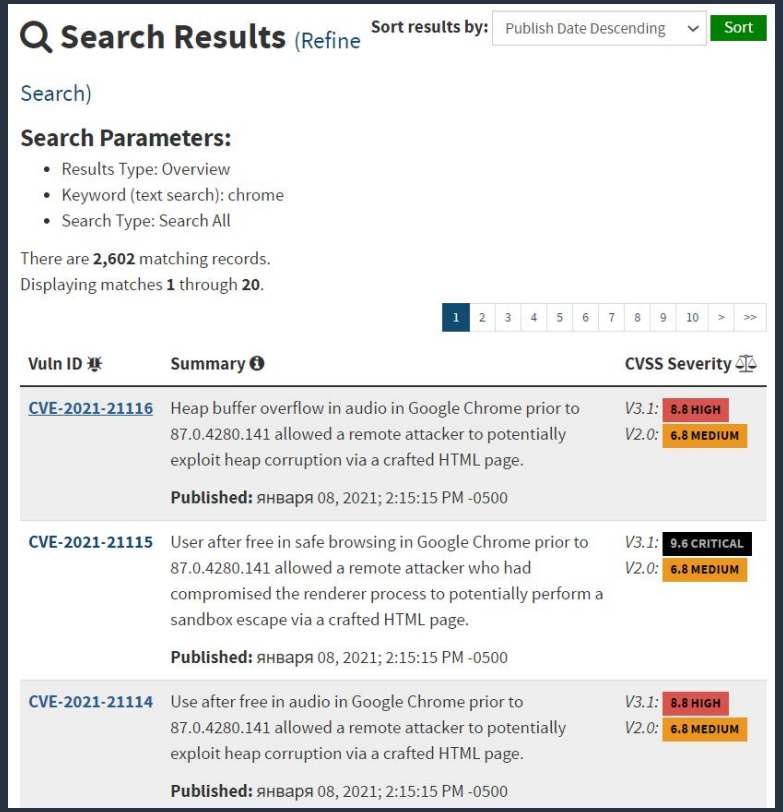
Базы уязвимостей 2/2. NVD

Собирает воедино информацию из различных классификаторов и баз (CPE/CWE/CVE и др.)

Поиск: https://nvd.nist.gov/vuln/search

Автоматизация: База NVD доступна для загрузки (формат JSON) и использования в инструментах безопасности https://nvd.nist.gov/vuln/data-feeds

Пример. Список уязвимостей в Chrome. 1/3



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

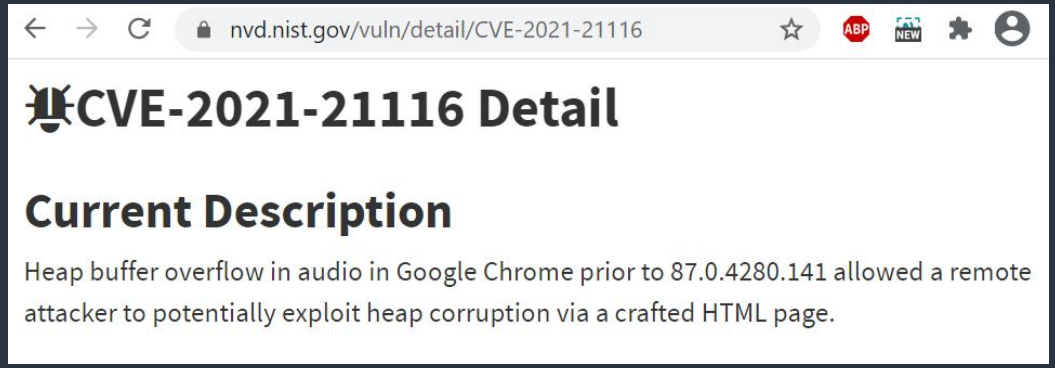
Search Parameters:

- 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:** января 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:** января 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:** января 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

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

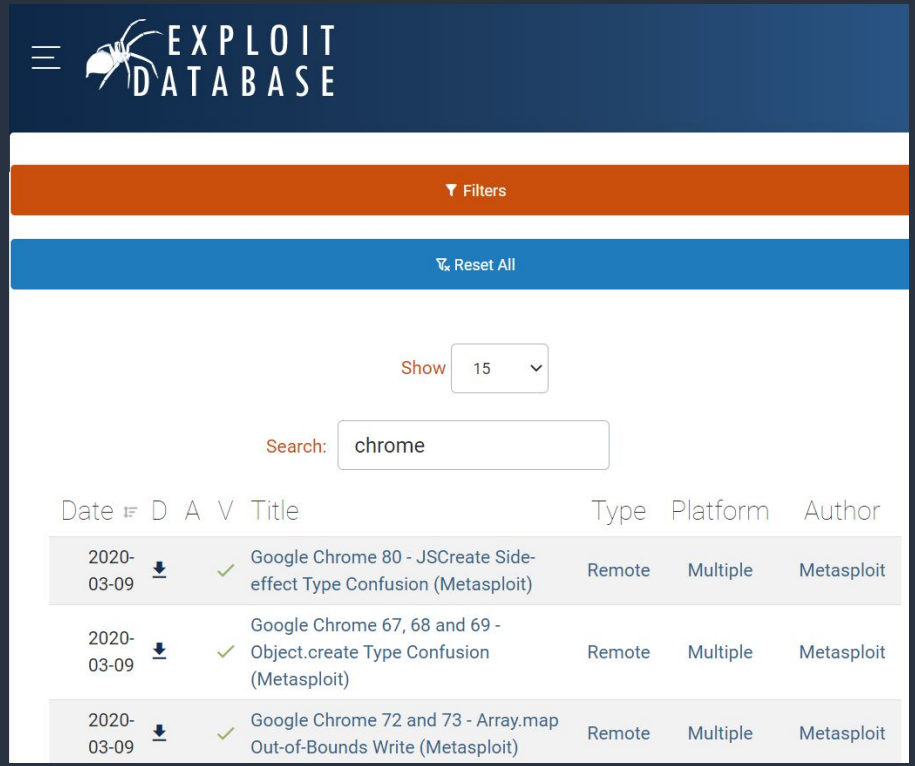
Информация об уязвимых версиях

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

Базы эксплойтов

База от Offensive Security:

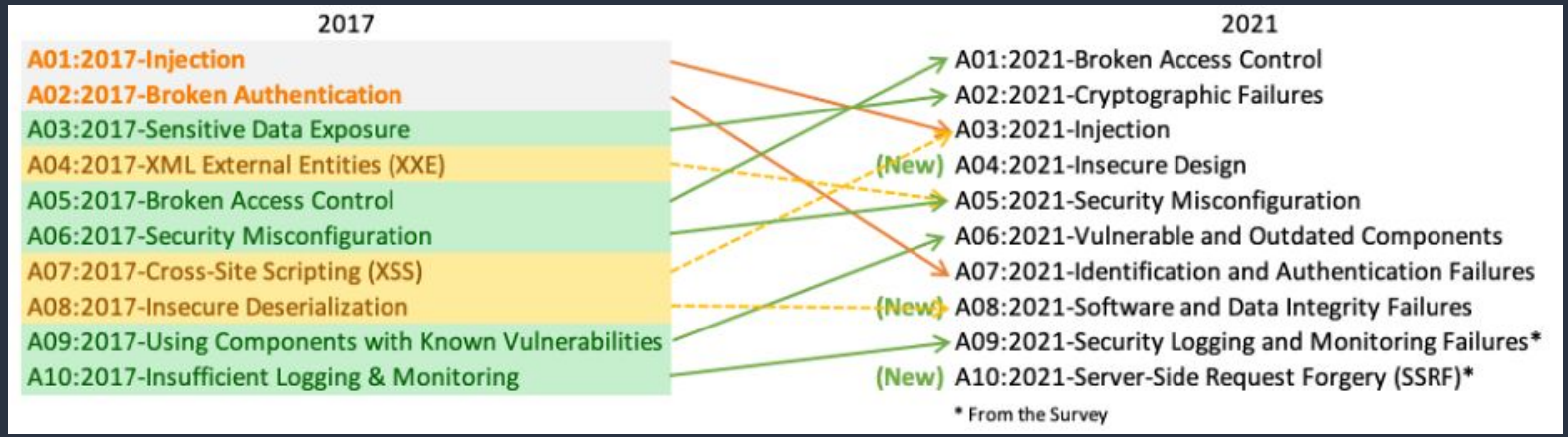
- www.exploit-db.com
- SearchSploit - утилита для поиска по базе
- большинство экплойтов Proof-of-Concept (PoC)



Вероятность успеха атаки готовыми эксплойтами

- многие коммерческие компании работают по принципу “работает - не трогай”
- ПО может не обновляться годами
- не требуется большой квалификации для взлома таких систем
- могут использоваться готовые эксплойты к известным уязвимостям
- проверить сеть можно общедоступными сканерами уязвимостей, например OpenVAS

Виды уязвимостей



Источник: https://owasp.org/www-project-top-ten/

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

База слабостей (CWE)

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

Список самых опасных уязвимостей по версии CWE

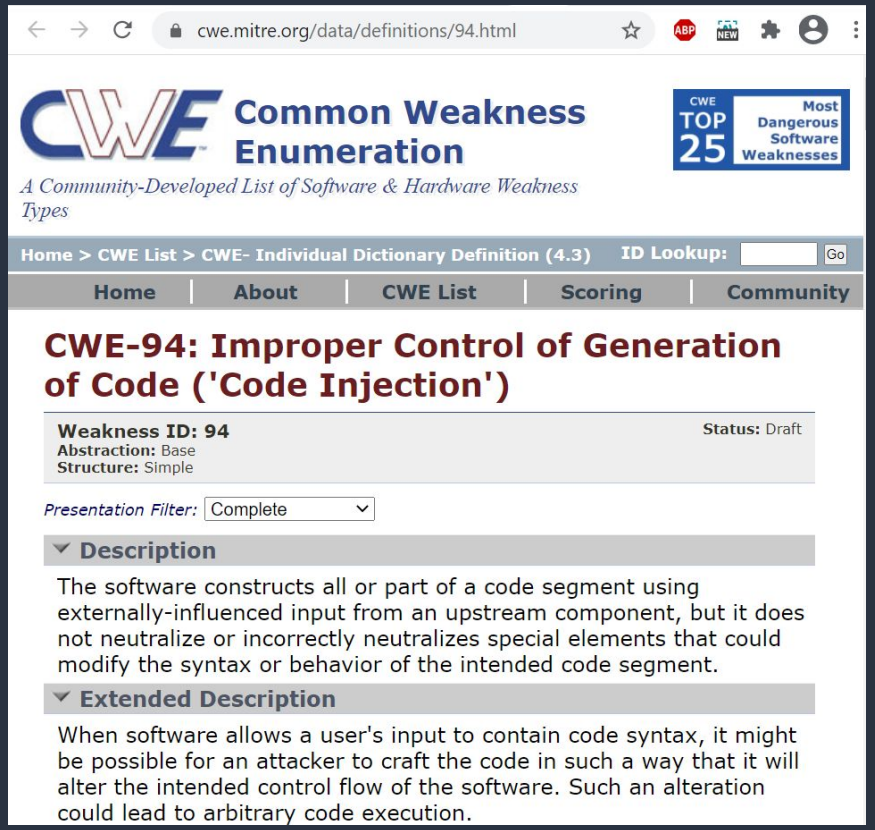
The CWE Top 25

Below is a list of the weaknesses in the 2022 CWE Top 25, including the overall score of each. The KEV Count (CVEs) shows the number of CVE-2020/CVE-2021 Records from the CISA KEV list that were mapped to the given weakness.

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

Источник: https://cwe.mitre.org/top25/

Пример: внедрение кода (CWE-94)



cwe.mitre.org/data/definitions/94.html

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

Nmap — сетевой сканер
https://nmap.org/

Wireshark — анализатор сетевого трафика
https://www.wireshark.org/

Metasploit — система тестового вторжения
https://www.metasploit.com/

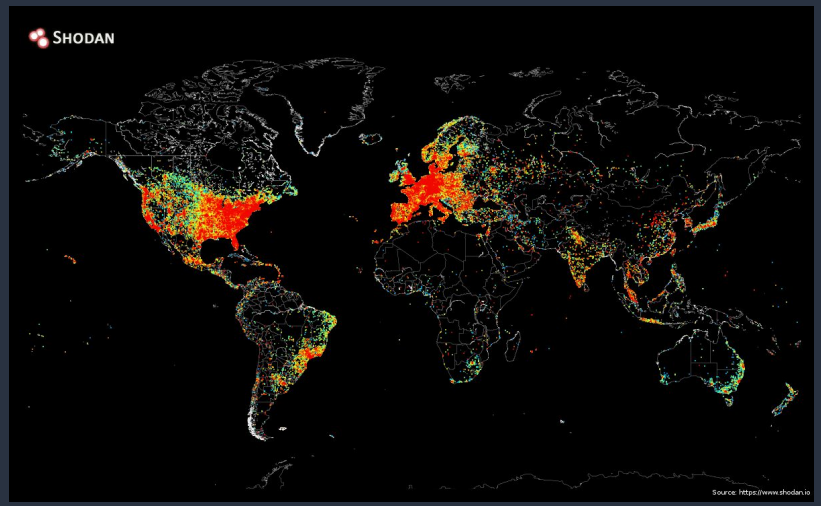
Kali Linux — дистрибутив с инструментами для тестирования безопасности
https://www.kali.org/

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

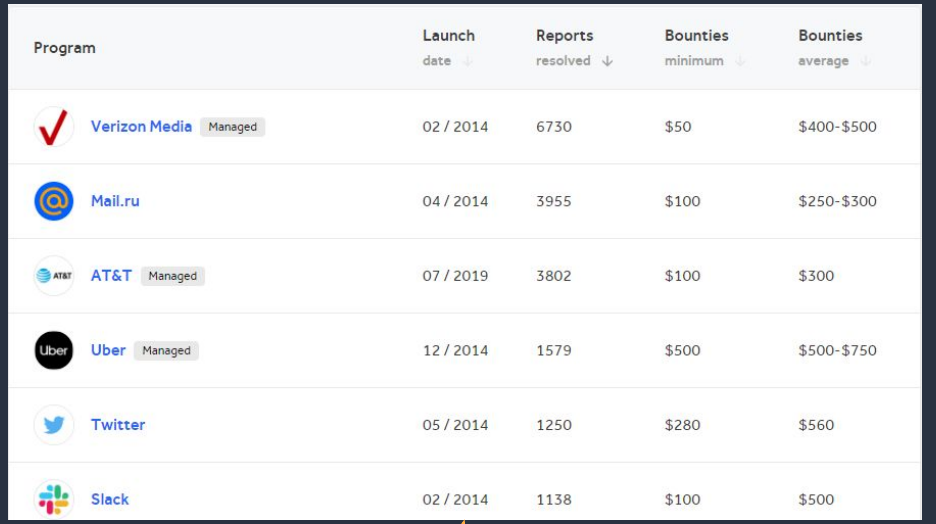
Программы Bug Bounty

Плата за найденные уязвимости

hackerone

Платформа HackerOne

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



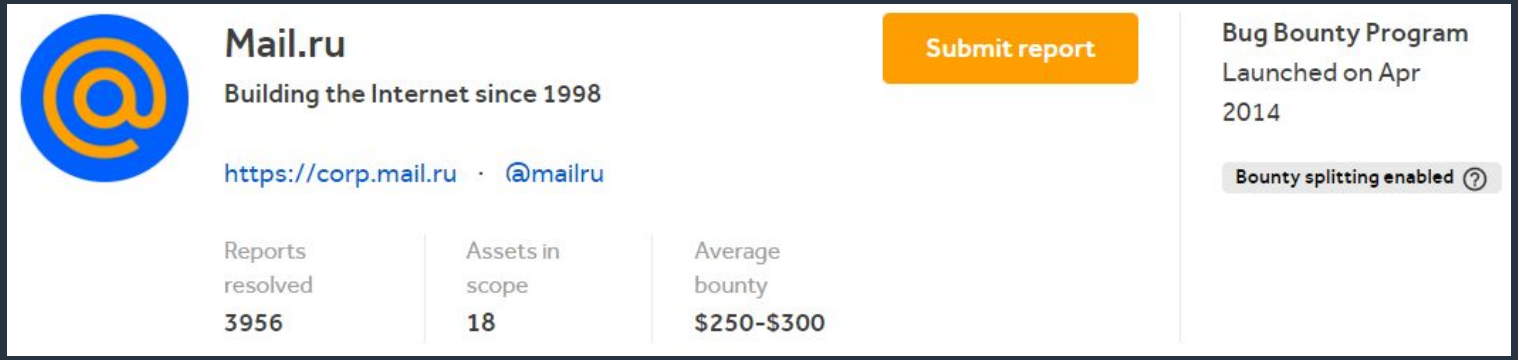
Program	Launch date	Reports resolved	Bounties minimum	Bounties average
Verizon Media Managed	02 / 2014	6730	$50	$400-$500
Mail.ru	04 / 2014	3955	$100	$250-$300
AT&T Managed	07 / 2019	3802	$100	$300
Uber Managed	12 / 2014	1579	$500	$500-$750
Twitter	05 / 2014	1250	$280	$560
Slack	02 / 2014	1138	$100	$500

Список активных программ
https://hackerone.com/directory/programs

Состояние в данный момент

- В настоящее время выплаты разработчикам из России и Белоруссии недоступны.
- Аналог от Positive Technologies: https://bugbounty.standoff365.com/
- У компаний есть свои страницы, например: Yandex: https://yandex.ru/bugbounty/index

Пример программы. 1/2



- https://hackerone.com/mailru
- выплачено более 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)

опыт работы автора на HackerOne

- Эриксон Д. - Хакинг: искусство эксплойта. 2 изд. (2018)
- Курс по Metasploit:
  - https://www.offensive-security.com/metasploit-unleashed/
- Журнал Хакер:
  - https://xakep.ru/