

Основы построения защищенных компьютерных сетей

Лекция 1. Введение



Семён Новосёлов

2026

БФУ
ИМЕНИ И. КАНТА

О чём курс?

- изучение средств **защиты** сетей
- разбор сетевых атак, уязвимостей, методов защиты от них
- изучение основных инструментов:
metasploit, nmap, wireshark, iptables, snort и др.
- пентест тоже будет и некоторые задания в формате **ctf**

Страница курса:

crypto-kantiana.com/semyon.novoselov/teaching/netsec_2026



Порядок работы

Формат: лекции + сдача лабораторных работ

- после лекций выкладываются лабораторные работы
- срок сдачи: 2 недели с даты публикации задания
- сдача: **флаг** и/или **отчёт** в lms.kantiana.ru + устная защита
- за пределами срока сдачи работы защищаются с низким приоритетом и не более 2 шт. за раз

Зачёт: сдать 90% лабораторных

- будет примерно 15 лабораторных ⇒ 12 сдать

Политика в отношении ИИ

- допустимо использование любых инструментов при выполнении заданий
- но если студент **не разобрался в теме** задания и заметно применение нейросетей, то он рискует получить на дом:
 - a. продвинутое задание, которое трудно решить даже с нейросетями
 - b. вопрос исследовательского класса, на который у ИИ ответа нет

Содержимое курса

1. Введение
2. Базовые сетевые протоколы и их безопасность
3. Сетевые атаки
4. Сетевые сканеры. **Nmap**
5. Системы текстового вторжения. **Metasploit**
6. Анализ трафика. **Wireshark**
7. Уязвимости Web-приложений
8. Межсетевые экраны. **Iptables**
9. Системы обнаружения и предотвращения вторжений. **Snort**
10. Криптографические протоколы. **TLS**
11. Виртуальные частные сети. **OpenVPN**
12. Безопасность беспроводных сетей. **Aircrack**
13. Песочницы. **AppArmor**

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 (www.cve.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

NVD Vulnerability Search

For a phrase search, use " "

cpe:2.3:*google:chrome:*:*:*:*:*:* Vendor: google Product: chrome

Items per page: 25 1-25 of 6503

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2026-9999	✖	May 28, 2026	Chrome	Inappropriate implementation in ANGLE in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)
CVE-2026-9998	✖	May 28, 2026	Chrome	Integer overflow in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
CVE-2026-9997	✖	May 28, 2026	Chrome	Use after free in Input in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
CVE-2026-9996	✖	May 28, 2026	Chrome	Out of bounds read in WebRTC in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)

nvd.nist.gov/vuln/detail/cve-2026-9999

CVE-2026-9999 Detail

Description

Inappropriate implementation in ANGLE in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

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

URL	Source(s)	Tag(s)
https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html 	Chrome	Vendor Advisory
https://issues.chromium.org/issues/513364480 	Chrome	Permissions Required

Список ссылок с дополнительной информацией об уязвимости

CWE-ID	CWE Name	Source
CWE-269	Improper Privilege Management	 CISA-ADP

Класс уязвимости

Пример. Список уязвимостей в Chrome. 3/3

Vendor	Product	Versions
Google	Chrome	Affected 148.0.7778.216 < 148.0.7778.216

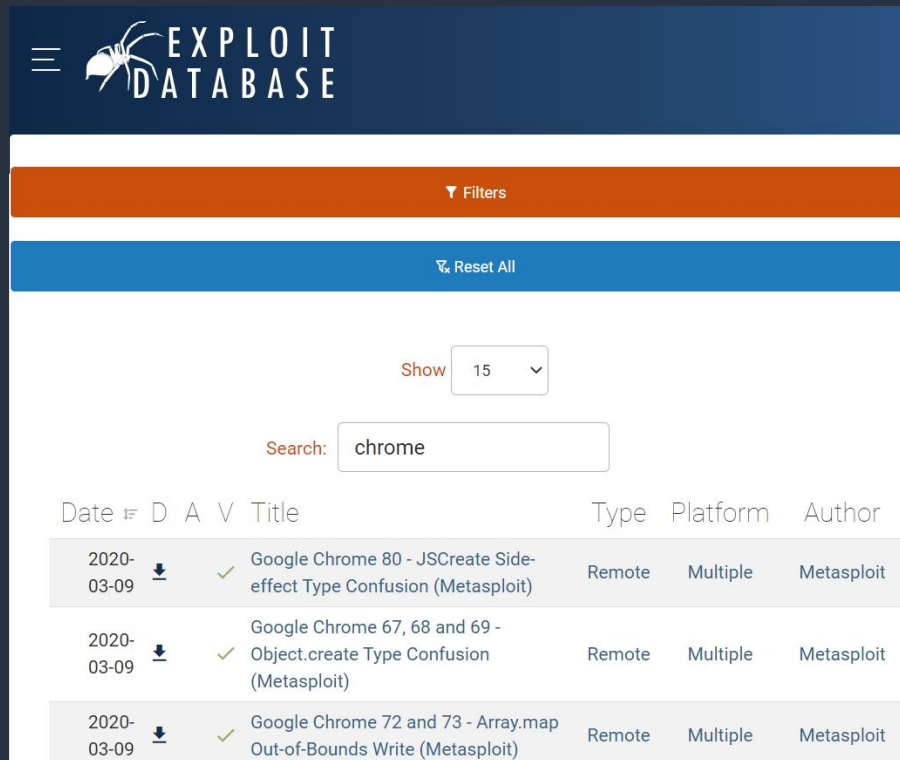
Информация об уязвимых версиях

- 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)



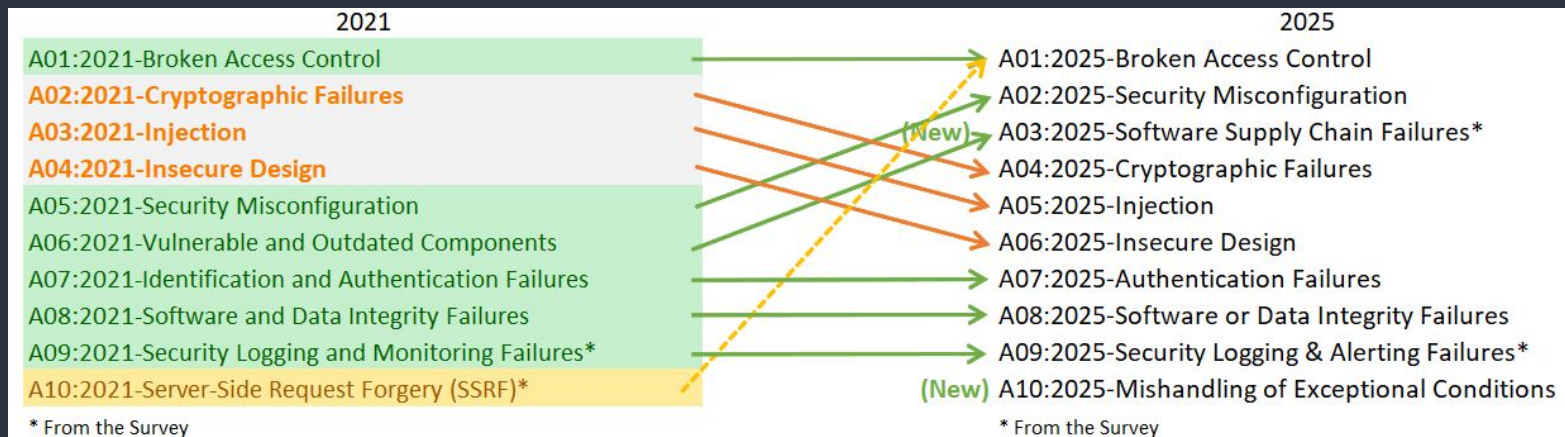
The screenshot displays the Exploit Database website interface. At the top, there is a dark blue header with the 'EXPLOIT DATABASE' logo and a hamburger menu icon. Below the header, there are two horizontal bars: an orange one with a 'Filters' button and a blue one with a 'Reset All' button. The main content area has a search bar with the text 'chrome' and a 'Show 15' dropdown menu. Below the search bar, there is a table of search results.

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 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 MITRE

2025 CWE Top 25

Rank	ID	Name	Score	CVEs in KEV
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	60.38	7
2	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28.72	4
3	CWE-352	Cross-Site Request Forgery (CSRF)	13.64	0
4	CWE-862	Missing Authorization	13.28	0
5	CWE-787	Out-of-bounds Write	12.68	12
6	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	8.99	10
7	CWE-416	Use After Free	8.47	14
8	CWE-125	Out-of-bounds Read	7.88	3
9	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7.85	20
10	CWE-94	Improper Control of Generation of Code ('Code Injection')	7.57	7
11	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	6.96	0
12	CWE-434	Unrestricted Upload of File with Dangerous Type	6.87	4
13	CWE-476	NULL Pointer Dereference	6.41	0
14	CWE-121	Stack-based Buffer Overflow	5.75	4
15	CWE-502	Deserialization of Untrusted Data	5.23	11
16	CWE-122	Heap-based Buffer Overflow	5.21	6
17	CWE-863	Incorrect Authorization	4.14	4
18	CWE-20	Improper Input Validation	4.09	2
19	CWE-284	Improper Access Control	4.07	1
20	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	4.01	1
21	CWE-306	Missing Authentication for Critical Function	3.47	11
22	CWE-918	Server-Side Request Forgery (SSRF)	3.36	0
23	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.15	2
24	CWE-639	Authorization Bypass Through User-Controlled Key	2.62	0
25	CWE-770	Allocation of Resources Without Limits or Throttling	2.54	0

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

Пример: внедрение кода (CWE-94)

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

CWE 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:

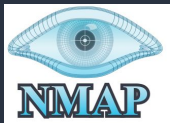
(attack code)

```
<?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/>

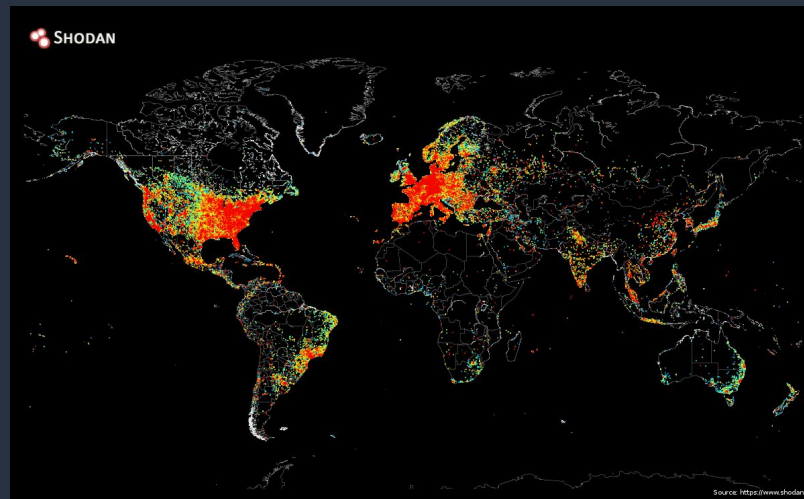
Поисковые системы

- 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

Shodan 1/2. Пример

 SHODAN

Explore

Downloads

Pricing 

city:"Kaliningrad"



TOTAL RESULTS

51,211

TOP PORTS

80	6,086
8291	3,420
161	2,200
2000	2,163
6881	2,146

More...

TOP ORGANIZATIONS

TIS Dialog LLC	15,192
OJSC Rostelecom North-West	8,293
Cloudflare London, LLC	5,132
OJSC North-West Telecom	3,283
PJSC MegaFon	2,241

More...

TOP PRODUCTS

nginx	3,297
MikroTik Winbox	3,087
MikroTik bandwidth-test server	2,152
CloudFlare	1,965

 View Report

 Browse Images

 View on Map

 Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Direct IP access not allowed | Cloudflare 

5.182.85.235
Cloudflare London, LLC
 Russian Federation, Kaliningrad

HTTP/1.1 403 Forbidden
Date: Tue, 02 Sep 2025 14:07:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 6235
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=...

91.109.143.185 

ppp91-109-143-185.tis-dialog.ru
TIS Dialog LLC
 Russian Federation, Kaliningrad

HTTP/1.1 404 Not Found
Date: TUE SEP 02 16:06:39 2025
Server: cwmv server
Connection: close
Content-Length: 14
Content-Type: text/plain; charset=ISO-8859-1

5.11.78.215

ppp5-11-78-215.tis-dialog.ru
TIS Dialog LLC
 Russian Federation, Kaliningrad

Recursion: enabled

DSL-2640U 

178.68.57.22
OJSC Rostelecom North-West
 Russian Federation, Kaliningrad

 HTTP/1.0 200 OK
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Content-type: text/html
Expires: Tue, 02 Jan 2000 01:00:00 GMT
Last-Modified: Thu, 01 Jan 1970 03:34:17 GMT
Set-Cookie: user_ip=224.11.19.144

[www.shodan.io/search?
query=city:Kaliningrad](https://www.shodan.io/search?query=city:Kaliningrad)



Shodan 2/2. Другие фильтры

Filters Cheat Sheet

Shodan currently crawls nearly 4,000 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites
net	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255
org	Name of the organization that owns the IP space	Devices at Google
port	Port number for the service that is running	SSH servers
product	Name of the software that is powering the service	Samsung Smart TVs
screenshot.label	Label that describes the content of the image	Screenshots of Industrial Control Systems
state	U.S. State	Devices in Texas

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



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>
- https://bugbounty.standoff365.com/programs/mail_vk
- выплачено более 22 миллиона руб. на Standoff365

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)
 - Эриксон 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

