2025

# Топ-10 инструментов пентестера для тестирования веб-приложений

ЭТОТ ГАЙД — ВАШ КРАТКИЙ ПУТЕВОДИТЕЛЬ ПО ИНСТРУМЕНТАМ, КОТОРЫЕ ИСПОЛЬЗУЮТ ПРОФЕССИОНАЛЫ В ПЕНТЕСТЕ. ПРИМЕНЯЙТЕ ТОЛЬКО НА ЛЕГАЛЬНЫХ ПРОЕКТАХ!

АКАДЕМИЯ КОДЕБАЙ | CODEBY ACADEMY

*Бонус для студентов бесплатного курса WASA от Codeby*

# Оглавление



# Сравнение ТОП-10 инструментов

| **Инструмент** | **Возможности** | **Сложность** | **Лицензия** |
|---|---|---|---|
| Burp Suite | Анализ трафика, сканирование, эксплуатация | Средняя | Платная/Бесплатная |
| OWASP ZAP | Сканирование уязвимостей, автоматизация атак | Средняя | Бесплатная |
| SQLMap | Автоматизация SQL-инъекций | Средняя | Бесплатная |
| Nmap | Сканирование сети, поиск уязвимых сервисов | Низкая | Бесплатная |
| Metasploit | Эксплуатация уязвимостей, полезные нагрузки | Высокая | Бесплатная/Платная |
| Wfuzz | Подбор параметров, перебор директорий | Низкая | Бесплатная |
| Dirb/Dirbuster | Поиск скрытых файлов и директорий | Низкая | Бесплатная |
| John the Ripper | Взлом паролей по хешам | Средняя | Бесплатная |
| Nikto | Сканирование на устаревшее ПО и уязвимости | Низкая | Бесплатная |
| Hydra | Брутфорс логинов (FTP, SSH, веб-формы) | Средняя | Бесплатная |

## 1. Burp Suite

**Для чего**: Перехват и анализ трафика, сканирование уязвимостей, автоматизация атак.
**Ссылка**: portswigger.net/burp
**Пример**:

- Перехватывайте запросы к сайту через **Proxy** → меняйте параметры (например, cookie) для проверки на XSS.
- Используйте **Intruder** для подбора паролей или эксплуатации SQLi.

---

## 2. OWASP ZAP

**Для чего**: Бесплатная альтернатива Burp Suite, сканирование уязвимостей, автоматическое тестирование.
**Ссылка**: owasp.org/zap
**Пример**:

- Запустите автоматическое сканирование сайта через **Quick Start** → анализируйте отчеты на наличие XSS и CSRF.

---

## 3. SQLMap

**Для чего**: Автоматизация эксплуатации SQL-инъекций.
**Ссылка**: sqlmap.org
**Пример**:

```bash
sqlmap -u "https://example.com/page?id=1" --dbs  # Поиск баз данных
sqlmap -u "https://example.com/page?id=1" -D db_name --tables  # Поиск таблиц
```

---

## 4. Nmap

**Для чего**: Сканирование сети, поиск открытых портов и уязвимых сервисов.
**Ссылка**: nmap.org
**Пример**:

```bash
nmap -sV -p 80,443 example.com  # Проверка версий сервисов на портах 80 и 443
nmap --script vuln example.com  # Поиск известных уязвимостей
```

---

## 5. Metasploit Framework

**Для чего**: Эксплуатация уязвимостей, создание полезных нагрузок.
**Ссылка**: metasploit.com
**Пример**:

```bash
msfconsole
use exploit/unix/ftp/proftpd_modcopy_exec  # Пример эксплойта для ProFTPD
set RHOSTS target_ip
exploit
```

---

## 6. Wfuzz

**Для чего**: Подбор параметров (логины, директории, API-эндпоинты).
**Ссылка**: wfuzz.io
**Пример**:

```bash
wfuzz -c -z file,wordlist.txt --hc 404 https://example.com/FUZZ  # Поиск скрытых директорий
```

---

## 7. Dirb/Dirbuster

**Для чего**: Поиск скрытых файлов и директорий на веб-сервере.
**Ссылка**: tools.kali.org
**Пример**:

```bash
dirb https://example.com /usr/share/wordlists/common.txt
```

---

## 8. John the Ripper

**Для чего**: Взлом хешей паролей.
**Ссылка**: openwall.com/john
**Пример**:

```bash
john --format=raw-md5 --wordlist=rockyou.txt hashes.txt  # Подбор MD5-хешей
```

---

## 9. Nikto

**Для чего**: Сканирование веб-серверов на устаревшее ПО и базовые уязвимости.
**Ссылка**: cirt.net/nikto2
**Пример**:

```bash
nikto -h example.com -ssl  # Проверка HTTPS-сайта
```

---

## 10. Hydra

**Для чего**: Брутфорс логинов (FTP, SSH, веб-формы).
**Ссылка**: github.com/vanhauser-thc/thc-hydra
**Пример**:

```bash
hydra -l admin -P passwords.txt example.com http-post-form "/login.php:user=^USER^&pass=^PASS^:Invalid password"
```

---

## Советы по легальному использованию

1. **Всегда тестируйте только те системы, где у вас есть письменное разрешение**. Несанкционированные действия могут быть расценены как преступление.
2. **Проводите тестирование аккуратно и осторожно**. Не наносите реальный ущерб системам и данным заказчика.
3. **Соблюдайте конфиденциальность**. Не разглашайте информацию о выявленных уязвимостях без согласования.
4. **Действуйте в рамках закона и этических норм**. Помните, что ваша цель- помочь, а не причинить вред.
5. Начните с **Burp Suite** или **ZAP** для анализа веб-приложений.
6. Для автоматизации атак используйте **SQLMap** и **Metasploit**.
7. Проверяйте результаты через отчеты (например, в **OWASP ZAP**).

## Карьерный путь пентестера

Профессия пентестера (специалиста по тестированию на проникновение) входит в топ-10 самых высокооплачиваемых и востребованных в ИТ-отрасли. По данным hh.ru, средняя зарплата специалистов в этой области составляет:

- Junior (2-3 года опыта): от 150 000 руб.
- Middle (3-5 лет опыта): от 250 000 руб.
- Senior (от 5 лет опыта): от 350 000 руб.

### Этап 1: Фундаментальная подготовка (0-2 года)

- Получение базового образования в IT или информационной безопасности
- Освоение сетевых технологий и основ программирования
- Получение начальных сертификатов (WASA, WAPT)
- Работа системным администратором или специалистом техподдержки

### Этап 2: Junior Penetration Tester (2-3 года)

- Изучение основных инструментов пентеста
- Получение специализированных сертификатов (CEH, OSCP, ADPTi)
- Участие в CTF-соревнованиях
- Работа в команде под руководством опытных пентестеров

### Этап 3: Middle Penetration Tester (3-5 лет)

- Специализация на конкретных направлениях (веб, мобильные приложения, IoT)
- Самостоятельное проведение тестирований
- Активное участие в bug bounty программах
- Получение продвинутых сертификатов (GPEN, GWAPT)

### Этап 4: Senior Penetration Tester (5-7 лет)

- Проведение комплексных пентестов крупных систем
- Менторство junior-специалистов
- Разработка методологий тестирования
- Выступления на профильных конференциях

### Этап 5: Lead/Principal Penetration Tester (7+ лет)

- Руководство Red Team или Purple Team
- Проведение аудитов безопасности критической инфраструктуры
- Консультирование по вопросам построения безопасности
- Участие в разработке отраслевых стандартов

### Ключевые факторы успеха:

- Постоянное самообразование и отслеживание новых угроз
- Развитие soft skills и навыков коммуникации
- Создание профессионального портфолио и репутации
- Нетворкинг в профессиональном сообществе

## Преимущества курса "WAPT" от Codeby Academy

- 100% практический курс с 65+ заданиями и 16 экзаменационными кейсами
- Опытные преподаватели- действующие пентестеры, победители CTF-соревнований
- Поддержка и консультации от кураторов на протяжении всего обучения
- Получение Удостоверения о повышении квалификации или Сертификата
- Гарантия возврата средств в течение 14 дней, если курс вам не подойдет

## Отзывы выпускников

---

*"Благодаря курсу я смог значительно прокачать свои навыки в пентестинге. Теперь я уверенно применяю изученные техники на реальных проектах."*

Александр, Middle Pentester

*"Курс дал мне глубокое понимание не только инструментов, но и методологии тестирования. Я научился структурированно подходить к пентесту."*

Ольга, Junior Pentester

*"Практические задания и разбор реальных кейсов помогли мне быстро освоить все тонкости профессии. Теперь я чувствую себя готовым к любым вызовам."*

Иван, Senior Pentester

---

## В платном курсе **«WAPT»** вы научитесь:

1. Комплексному тестированию веб-приложений
2. Работе с продвинутыми техниками взлома
   - Изучите SQL Injection, XSS, CSRF, PHP injection и Server Side Template injection
3. Решению сложных практических задач
4. Работе с профессиональными инструментами
5. Построению карьеры в сфере ИБ
   - Получите актуальные знания от практикующих специалистов и победителей CTF
   - Освоите методики, применяемые в реальных проектах и bug bounty программах

---

*«Хотите научиться применять эти инструменты в реальных кейсах? Записывайтесь на курс **WAPT — тестирование веб-приложений на проникновение**!»*

***ЗАПИСАТЬСЯ НА WAPT***