0.1 Front matter

title: “Индивидуальный проект этап 4” subtitle: “Основы информационной безопасности” author: “Пинега Белла Александровна”

0.2 Generic otions

lang: ru-RU toc-title: “Содержание”

0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs: english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9 ## Biblatex biblatex: true biblio-style: “gost-numeric” biblatexoptions: - parentracker=true - backend=biber - hyperref=auto - language=auto - autolang=other* - citestyle=gost-numeric ## Pandoc-crossref LaTeX customization figureTitle: “Рис.” tableTitle: “Таблица” listingTitle: “Листинг” lofTitle: “Список иллюстраций” lotTitle: “Список таблиц” lolTitle: “Листинги” ## Misc options indent: true header-includes: -

keep figures where there are in the text

- # keep figures where there are in the text

1 Цель работы

Научиться основным способам тестирования веб приложений

2 Задание

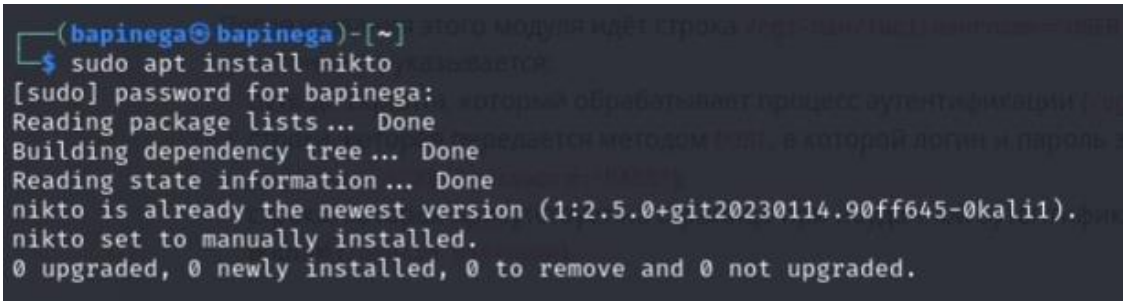
nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

3 Теоретическое введение

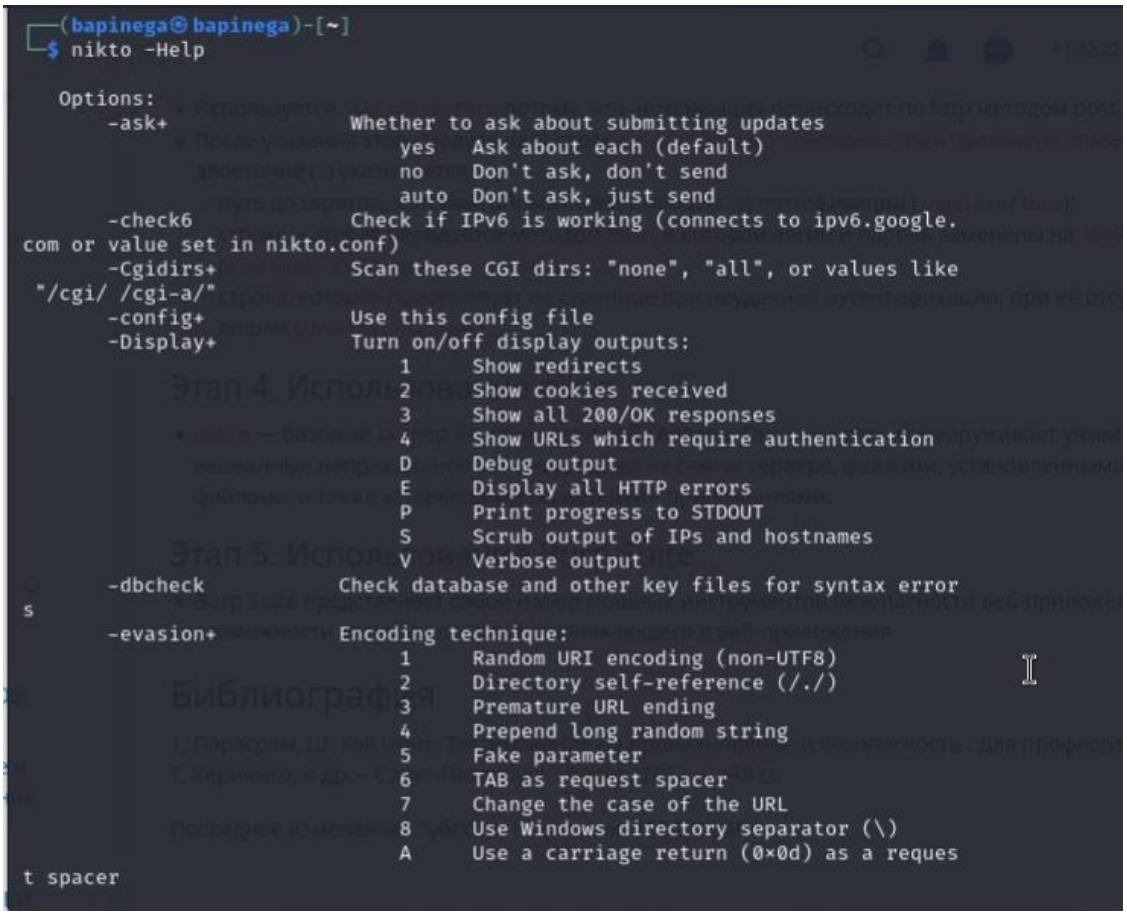
Ищутся уязвимости в специально предназначенном для этого веб приложении под названием Damn Vulnerable Web Application (DVWA). Назначение DVWA — попрактиковаться в некоторых самых распространённых веб уязвимостях. Предлагается попробовать и обнаружить так много уязвимостей, как сможете.

4 Выполнение лабораторной работы

1. Установлю nikto



2. Познакомлюсь с nikto



3. Выполню сканирование SSL и порта 443

```
┌──(bapinega㉿bapinega)-[~]
└─$ nikto -h pbs.org -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 54.225.198.196, 54.225.206.152
+ Target IP:          54.225.198.196
+ Target Hostname:    pbs.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.pbs.org
                   Ciphers:  ECDHE-ECDSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-03-07 22:48:40 (GMT3)
---------------------------------------------------------------------------
+ Server: openresty
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozil
la.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-158-80.ec2.internal.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: http
s://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type. See: https://www.netsparker.co
m/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.pbs.org/
```

4. Сканирую ip-адрес

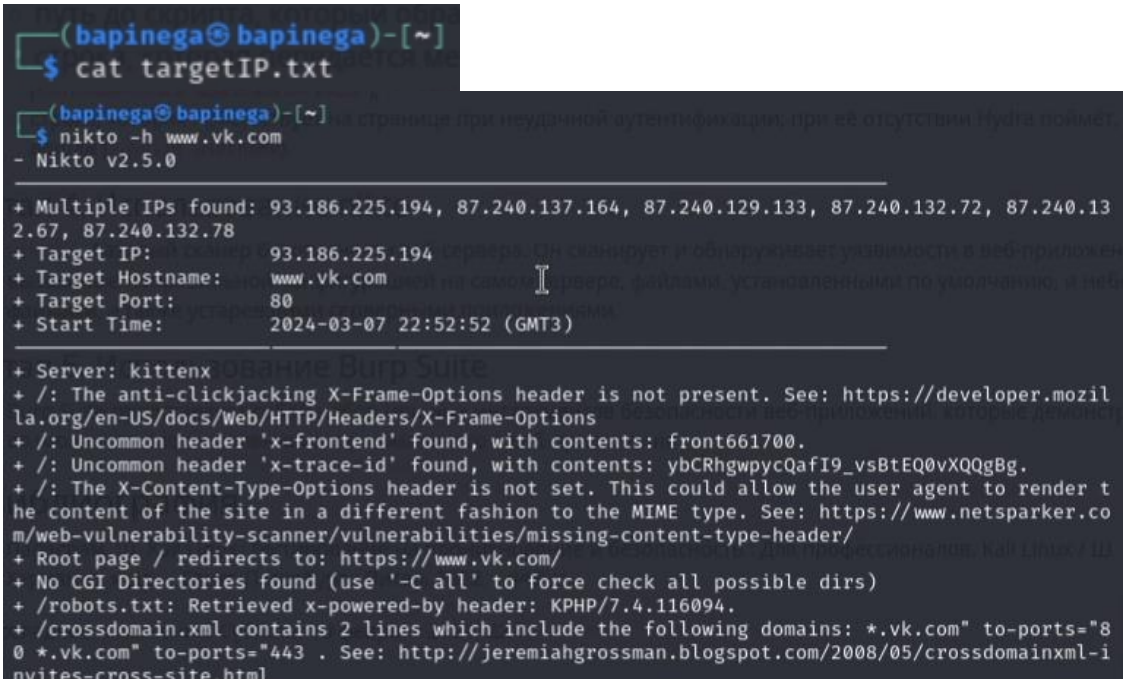
```
┌──(bapinega㉿bapinega)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fef6:7276  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:f6:72:76  txqueuelen 1000  (Ethernet)
        RX packets 37504  bytes 44892800 (42.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14396  bytes 1672351 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2034  bytes 121820 (118.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2034  bytes 121820 (118.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(bapinega㉿bapinega)-[~]
└─$ ipcalc 192.168.0.48
```

5. Чтобы отправить все хосты в nikto и увидеть все ip-адреса проделаем следующее:

```
┌──(bapinega㉿bapinega)-[~]
└─$ cat nullbyte.txt | awk '/Up${print $2}' | cat >> targetIP.txt
awk: cmd. line:1: /Up${print $2}
awk: cmd. line:1:  ^ unterminated regexp
cat: nullbyte.txt: No such file or directory
```



5 Выводы

Я познакомилась с nikto

Список литературы