
Front matter

lang: ru-RU

title: Индивидуальный проект 4

subtitle: Основы информационной безопасности

author:

- Пинега Б.А.

institute:

- Российский университет дружбы народов, Москва, Россия

i18n babel

babel-lang: russian

babel-otherlangs: english

Formatting pdf

toc: false

toc-title: Содержание

slide_level: 2

aspectratio: 169

section-titles: true

theme: metropolis

header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- '\makeatother'

Докладчик

- * Пинега Белла Александровна

- * Студентка НБИБд-02-22

- * Российский университет дружбы народов

...

.....

Цель работы

Научиться основным способам тестирования веб приложений

Устанавливаю nikto

```
(bapinega@bapinega)-[~]
$ sudo apt install nikto
[sudo] password for bapinega:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

{#fig:001 width=70%}

Познакомлюсь с nikto

```
(bapinega@bapinega)-[~]
$ nikto -Help

Options:
  -ask+          Whether to ask about submitting updates
                  yes    Ask about each (default)
                  no    Don't ask, don't send
                  auto   Don't ask, just send
  -check6        Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/" "/cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1      Show redirects
                  2      Show cookies received
                  3      Show all 200/OK responses
                  4      Show URLs which require authentication
                  D      Debug output
                  E      Display all HTTP errors
                  P      Print progress to STDOUT
                  S      Scrub output of IPs and hostnames
                  V      Verbose output
  -dbcheck       Check database and other key files for syntax error
  -evasion+      Encoding technique:
                  1      Random URI encoding (non-UTF8)
                  2      Directory self-reference (../)
                  3      Premature URL ending
                  4      Prepend long random string
                  5      Fake parameter
                  6      TAB as request spacer
                  7      Change the case of the URL
                  8      Use Windows directory separator (\)
                  A      Use a carriage return (0x0d) as a request spacer
```

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: 4. 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.mozilla.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: https://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 the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.pbs.org/
```

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:fe6:7276 prefixlen 64 scopeid 0x20<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 0x10<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
```

{#fig:005 width=40%}

Выводы

Я познакомилась с nikto

...