

0.1 Front matter

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

0.2 Generic options

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: - parenttracker=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. 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.
```

2. 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
```

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.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/
```

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 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
```

5. Чтобы отправить все хосты в nikto и увидеть все ip-адреса сделаем 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
```

```

(bapinega@bapinega)-[~]
$ cat targetIP.txt

(bapinega@bapinega)-[~]
$ nikto -h www.vk.com
- Nikto v2.5.0

+ Multiple IPs found: 93.186.225.194, 87.240.137.164, 87.240.129.133, 87.240.132.72, 87.240.132.67, 87.240.132.78
+ Target IP: 93.186.225.194
+ Target Hostname: www.vk.com
+ Target Port: 80
+ Start Time: 2024-03-07 22:52:52 (GMT3)

+ Server: kittenx
+ /: 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-frontend' found, with contents: front661700.
+ /: Uncommon header 'x-trace-id' found, with contents: ybCRhgwpYcQafI9_vsBtEQ0vXQqBg.
+ /: 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.vk.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Retrieved x-powered-by header: KPHP/7.4.116094.
+ /crossdomain.xml contains 2 lines which include the following domains: *.vk.com" to-ports="80 *.vk.com" to-ports="443 . See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html

```

5 Выводы

Я познакомилась с nikto

Список литературы