

## 0.1 Front matter

title: "Индивидуальный проект этап 2" 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

Установите DVWA в гостевую систему к Kali Linux.

Репозиторий: <https://github.com/digininja/DVWA>.

Некоторые из уязвимостей веб приложений, который содержит DVWA:

Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.

Исполнение (внедрение) команд: Выполнение команд уровня операционной

системы.

Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.

Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.

SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение.

Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер.

Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS.

Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

Невозможный – этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.

Высокий – это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.

Средний – этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу.

Низкий – этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

### 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. Я настроила гостевую систему.

2. Затем я установила DVWA в гостевую систему к Kali Linux.

```
(bapinega@bapinega)-[~]
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
--2024-03-07 15:58:44 https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16688 (16K) [text/plain]
Saving to: 'Install-DVWA.sh'

Install-DVWA.sh      100%[=====>] 16.30K  --.-KB/s   in 0.01s
2024-03-07 15:58:44 (1.47 MB/s) - 'Install-DVWA.sh' saved [16688/16688]

(bapinega@bapinega)-[~]
$ chmod +x Install-DVWA.sh

(bapinega@bapinega)-[~]
$ sudo ./Install-DVWA.sh
[sudo] password for bapinega:

./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
php !Está instalado!
./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
php-mysql !Está instalado!
./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
php-gd no está instalado. Instalándolo ahora...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package php-gd
./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
libapache2-mod-php !Está instalado!
./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
git !Está instalado!
./Install-DVWA.sh: line 8: [: C.: syntax error: invalid arithmetic operator (error token is ".")
Descargando DVWA desde GitHub...
Cloning into '/var/www/html/DVWA' ...
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (35/35), done.
Receiving objects: 7% (315/4494)
```

## 5 Выводы

Я установила DVWA в гостевую систему к Kali Linux.

## Список литературы