Федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
Факультет информационных систем и безопасности
Кафедра комплексной защиты информации

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: Разработка утилиты для обфускации веб-приложений

направление подготовки 10.03.01 «Информационная безопасность»

Научный руководитель: Митюшин Д.А.

Автор ВКР: Медведев Е.В.

Актуальность

На сегодняшний день существует большое количество уязвимостей веб-приложений, которые могут привести не только к сбою работы сервисов, но и к несанкционированному просмотру и копированию исходных кодов и данных.

Цели и задачи

Цель: разработать утилиту для обфускации веб-приложений и их отдельных частей.

Задачи:

- ознакомиться с термином “обфускация”;
- рассмотреть языки программирования и утилиты обфускации кода для них;
- разработать утилиту для обфускации.

Структура

Первая глава:

- Определение термина “обфускация”
- Анализ уязвимости, при которой возможен доступ к исходным файлам веб-приложения

Вторая глава:

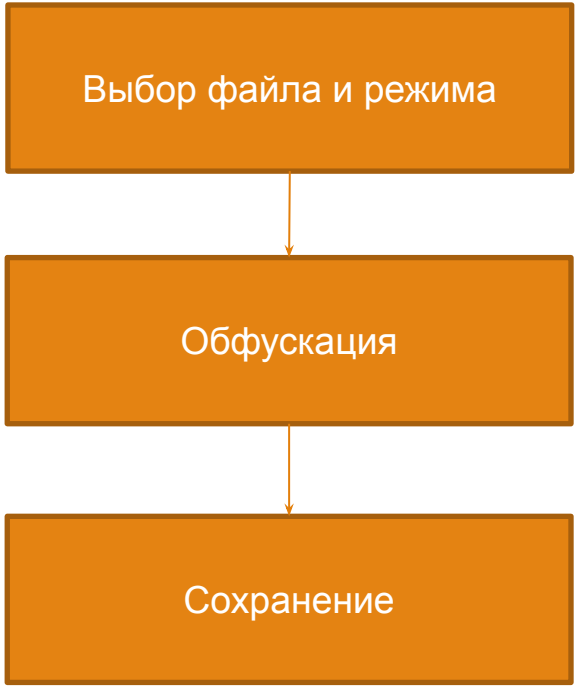
- Анализ языков программирования
- Анализ средств для обфускации рассмотренных языков программирования

Третья глава:

- Описание функций и принципов работы утилиты
- Примеры использования утилиты

Алгоритм работы утилиты

- выбор исходного файла и режима обработки
- выполнение выбранного режима
- сохранение результата в новый файл



Использование утилиты

Входные параметры: input_file.php -m, где

input_file.php – входной файл; **-m** – режим работы утилиты.

Режимы работы:

- -v – замена имен переменных;
- -f – удаление переноса строк и табуляции;
- -c – замена имен классов и переменных;
- -s – преобразование SQL-запросов;
- -a – применение всех режимов.

Результат: выходной файл с именем input_file**_obfuscated**.php.

Примеры. Исходный код

```php
<?php
class Like{
    public static function get_user_like($link, $id, $uid){
        $id = (int)$id;
        $uid = (int)$uid;
        $id = $link->real_escape_string($id);
        $uid = $link->real_escape_string($uid);
        $query="SELECT * FROM `story_likes` WHERE `user_id`='$uid' AND
        `story_id`='$id'";
        $result = $link->query($query);
        if(!$result) die('Неизвестная ошибка.');
        $num = $result->num_rows;
        if($num==0){
            return false;
        }
        else{
            return true;
        }
    }
}
```

Примеры. Режим -v

```php
<?php
class Like{
    public static function get_user_like($l11111111111, $l1111111111111111111,
     $l111111111111111){
        $l1111111111111111111 = (int)$l1111111111111111111;
        $l111111111111111 = (int)$l111111111111111;
        $l1111111111111111111 = $l11111111111->real_escape_string(
        $l1111111111111111111);
        $l111111111111111 = $l11111111111->real_escape_string($l111111111111111);
        $l1111111111111111111="SELECT * FROM `story_likes` WHERE `user_id`='
        $l111111111111111' AND `story_id`='$l1111111111111111111'";
        $l111111111111111 = $l11111111111->query($l1111111111111111111);
        if(!$l111111111111111) die('Неизвестная ошибка.');
        $l1111111111111111111 = $l111111111111111->num_rows;
        if($l1111111111111111111==0){
            return false;
        }
        else{
            return true;
        }
    }
}
```

Примеры. Режим -f

```
1  <?php
2  class Like{public static function get_user_like($link, $id, $uid){$id = (int)
   $id;$uid = (int)$uid;$id = $link->real_escape_string($id);$uid = $link->
   real_escape_string($uid);$query="SELECT * FROM `story_likes` WHERE
   `user_id`='$uid' AND `story_id`='$id'";$result = $link->query($query);if(!
   $result) die('Неизвестная ошибка.');$num = $result->num_rows;if($num==0){
   return false;}else{return true;}}}
```

Примеры. Режим -c

```php
<?php
class lllllllllllllllll{
    public static function lllll($link, $id, $uid){
        $id = (int)$id;
        $uid = (int)$uid;
        $id = $link->real_escape_string($id);
        $uid = $link->real_escape_string($uid);
        $query="SELECT * FROM `story_likes` WHERE `user_id`='$uid' AND
        `story_id`='$id'";
        $result = $link->query($query);
        if(!$result) die('Неизвестная ошибка.');
        $num = $result->num_rows;
        if($num==0){
            return false;
        }
        else{
            return true;
        }
    }
}
```

Примеры. Режим -s

```php
<?php
class Like{
    public static function get_user_like($link, $id, $uid){
        $id = (int)$id;
        $uid = (int)$uid;
        $id = $link->real_escape_string($id);
        $uid = $link->real_escape_string($uid);
        $query=base64_decode(
        "IlNFTEVDVCAqIEZST00gYHN0b3J5X2xpa2VzYCBXSEVSRSBgdXNlcl9pZGA9JyR1aWQnI
        EFORCBgc3RvcnlfaWRgPSckaWQnIg==");
        $result = $link->query($query);
        if(!$result) die('Неизвестная ошибка.');
        $num = $result->num_rows;
        if($num==0){
            return false;
        }
        else{
            return true;
        }
    }
}
```

Примеры. Режим -a

```
1  <?php
2  class lllllllllllll{public static function lllllllllllllllllll(
   $l11111111111, $llllllll, $l111111111111111){$llllllll = (int)$llllllll;
   $l111111111111111 = (int)$l111111111111111;$llllllll = $l11111111111->
   real_escape_string($llllllll);$l111111111111111 = $l11111111111->
   real_escape_string($l111111111111111);$l111111111111111=base64_decode(
   "IlNFTEVDVCAqIEZST00gYHN0b3J5X2xpa2VzYCBXSEVSRSBgdXNlcl9pZGA9JyR1aWQnIEFORCBgc
   3RvcnlfaWRgPSckaWQnIg==");$lllllllllllllll = $l11111111111->query(
   $lllllllllllllll);if(!$lllllllllllllll) die('Неизвестная ошибка.');
   $llllllllll = $lllllllllllllll->num_rows;if($llllllllll==0){return false;}
   else{return true;}}}
```

Уникальность

- Генерация псевдослучайных последовательностей символов для преобразования имен переменных, функций и классов;
- Преобразование SQL-запросов;
- Скорость работы.

Заключение

В результате работы были решены все поставленные задачи и получены следующие результаты:

- Изучен термин “обфускация”, а также термины, относящиеся к обфускации;
- Проанализированы языки программирования и средства обфускации для них;
- Разработана утилита для обфускации PHP кода.