세션관리

세션

Http는 한번의 요청과 응답만으로 통신을 처리하기에 과거에 수행한 통신 내용을 기억하지 않는 무 상태 프로토콜이다. 이런 한계를 극복하기 위해 세션이라는 논리적 연결을 통한 인증절차를 이용 사용자들의 요청을 구별한다.

세션상태 유지기법

1. 히든필드

<input type=”hidden” name=”var” value=”data”>

1. URL다시쓰기

URL주소에 세션을 유지시키기 위한 값을 붙이는 방법

-변조의 위험성을 가지고 있음.

1. 쿠키

-세션쿠키

쿠키발급시 메모리에만 상주하기 때문에 웹 브라우저 종료시에 해당 값은 함께 삭제된다. 별도의 만료시간을 통해 특정시간만 해당 쿠키 값이 유효 할 수 있도록 설정할 수 있다.

-영속적인 쿠키

디스크에 보관하기에 웹 브라우저, PC의 종료에 관계없이 유지된다. xss취약점이 있을 경우 사용자의 쿠키정보가 외부로 유출될 수 있다는 취약점이 있다.

-HttpOnly쿠키

외부 유출을 막기위한 쿠키

-Secure 쿠키

HTTPS상에서만 사용되며 사용자->서버 쿠키는 항상 암호화 되기에 쿠키노출 등의 위험성을 줄여준다.

-Third-party 쿠키

여러 도메인을 구분하기 위해 사용되며 사용자가 어느 사이트를 통해 유입되었는지 등을 추적하기 위한 용도로 사용할 수 있다.

1. 세션

세션이란 클라이언트와 서버 간의 활성화된 접속을 의미한다.

히든필드 변조

관리자만 이용가능한 공지사항 게시판을 히든 필드 변조를 통해 관리자권한으로 글을 쓸 수 있는 취약점을 이용함. 소스보기를 통해

<input type=hidden name=”writer” value=”guest”>

If name<> “master11” then 이런 구절을 확인 하고 관리자 계정이 master11이라는 것을 알 수 있고 이후 히든필드값을 master11로 변경하여 공격가능

쿠키변조

Cooxie 툴을 이용하여 쿠키 값을 확인하고 해당 값을 다른 계정으로 변조하여 타인의 권한을 획득 할 수 있다.

쿠키가로채기

1. xss코드 삽입 2.피해자 클릭 3.세션탈취 4.피해자의 세션을 이용한 세션하이재킹

가입정보 변조

프록시 도구로 회원가입, 회원정보 수정 계정 값을 가로채어 계정 값 등을 훔침.

관리자 페이지 접근 우회

관리자 페이지를 알고 있고, 관리자 페이지 접근제어를 스크립트로 할 때 가능한 것.

게시판 글 작성자 이름 변조

일반적으로 인증후 작성시에 자동으로 삽입하는 구성이 있는데

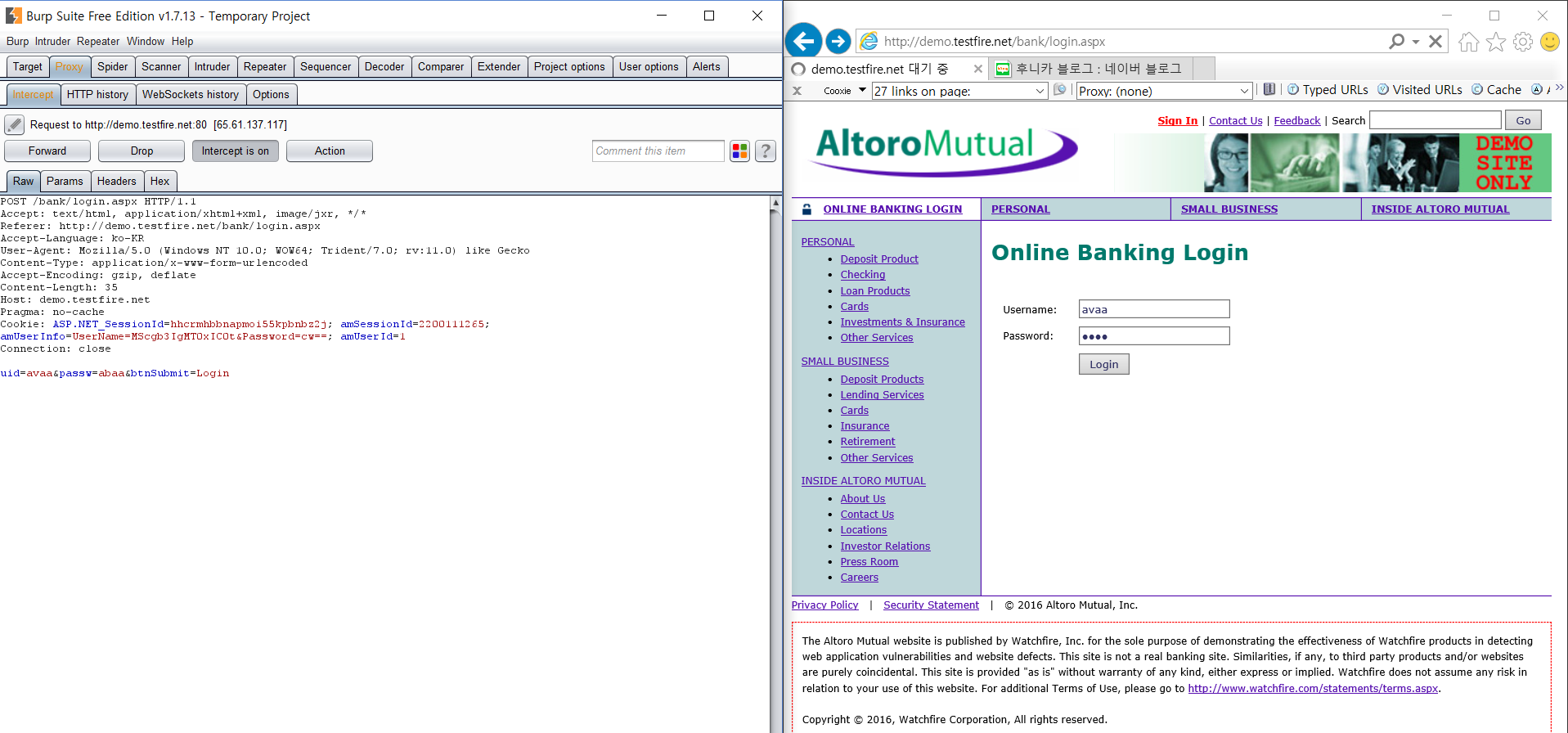
수정불가 설정 시 <readonly>태그를 이용해서 막아놨다면 프록시 도구를 이용하여 태그를 삭제, 이름을 변조 할 수 있다.

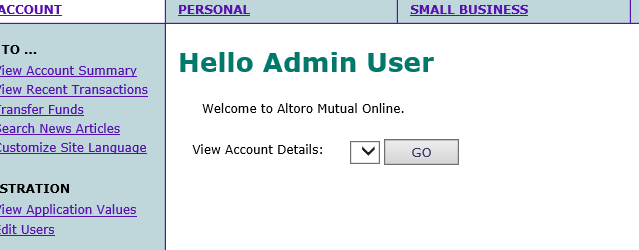
쿠키종류에 따른 취약성 테스트

모의실습

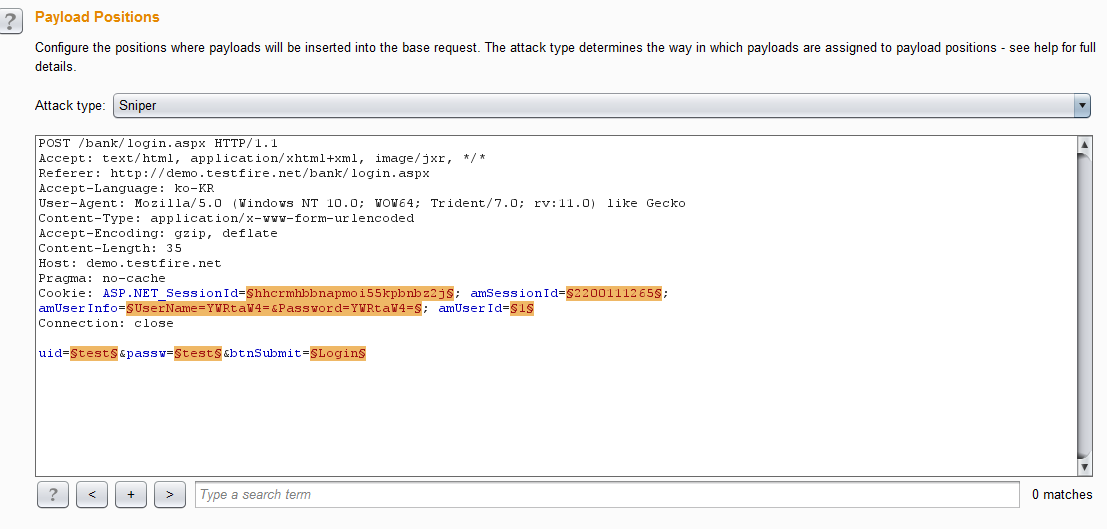
SQL injection 을 통한 인증 우회와 웹 폼에 추측된 계정과 암호를 전송 시켜 취약한 계정과 암호를 찾는 HTTP BruteForce 공격실습

BruteForce공격은 사전적인 단어들로 구성된 아이디와 패스워드 리스트를 가지고 계속적으로 로그인을 시도하는 것이다.





성공시 문자열 Hello Admin User



Intruder 화면 – Clear 후 Attack type 변경

