

Analysis FireFox

Brute Force Attack

Plug-in FireForce

Date : 10. 3. 30

Test : Windows 7 Localhost

Written by incle 천영철

E-mail : incle@stgsecurity.com

URL : <http://incle.org>

개요

Firefox 전용 플러그인 중 Brute Force 공격이 가능한 FireForce 에 대해 알아봄에 로컬 호스트에 직접 로그인 폼을 작성하여 어떤 논리로 공격이 성립되는지 확인하여 본다.

시나리오

특정 페이지 에서의 Brute Force 공격 가능성 입증

상세내역

Firefox는 Get & POST 방식을 사용하는 로그인 폼에서 사전 방식을 통해 Brute Force 공격을 행 할 수 있는 아주 간단한 틀이며 http://www.scr.t.ch/pages_en/fireforce.html 에서 구할 수 있다. 지금부터 말하는 모든 이야기는 Firefox 에서 가능한 이야기이다.



그림 1 Fireforce 다운

위의 링크를 클릭하면 다음과 같은 링크 페이지를 확인 할 수 있는데 Firefox 를 사용한 상태에서 해당 링크를 클릭하게 되면 Plug-IN 형태로 Firefox 부가기능이 설치된다.



그림 2 링크 클릭

다음과 같이 로그인 폼을 확인 할 수 있다.

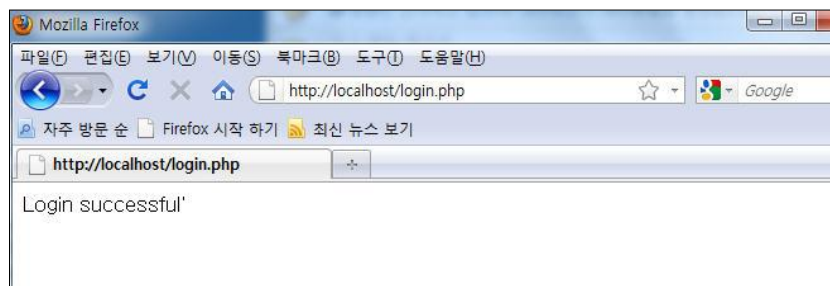
이는 그저 페이지의 Brute-Force 공격이 가능한것인지를 테스트 해봄이지 그것 외 다른의미를 가지지는 않는다.



그림 5 로그인 테스트 페이지

위의 페이지의 기본적인 기능은 다음과 같다.

올바르지 않은 ID 및 패스워드를 대입하였을 시 Login failed 가 요청되고 올바른 ID 및 Password 가 요청되면 Login Successful 이 나타나게 된다.



다음과 같이 @ DICTIONARY는 항상 삽입 되어야 하며 일종의 플래그 역할을 한다.
 밑의 화면처림의 진행한다.

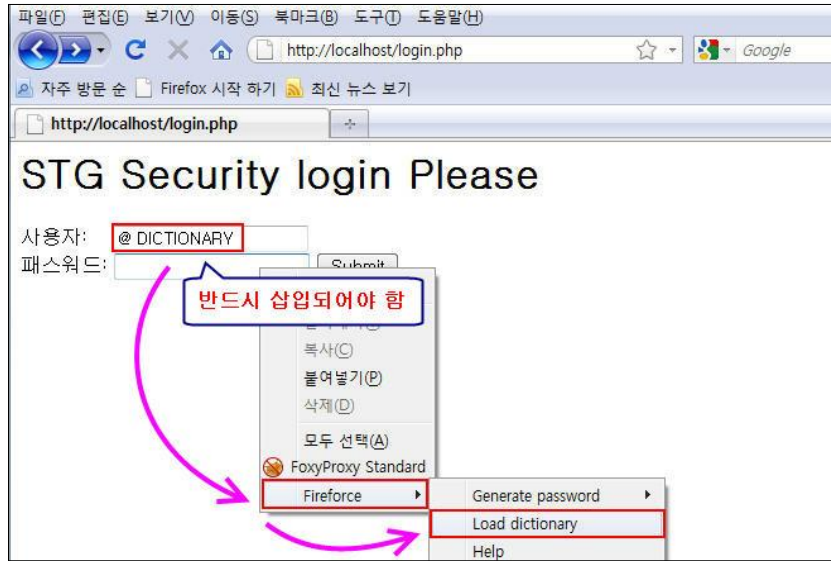


그림 6 특정 구문 삽입

COMMON_PASSWORDS.TXT 를 삽입한다.

Common_passwords	Common_username
Admin	Root
Asdf	asdf
1234	Girl
123456	Stg
0100	admin

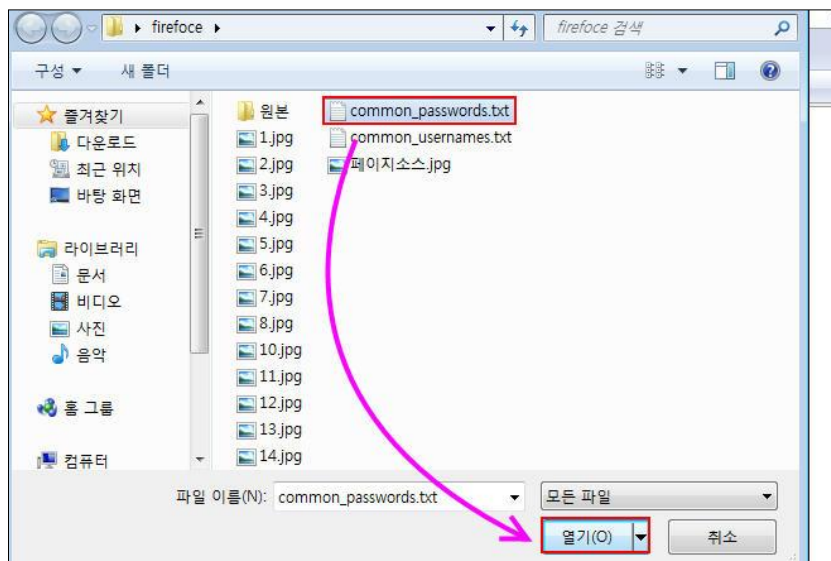


그림 7 Select common_passwords

다음과 같이 계속 진행한다.

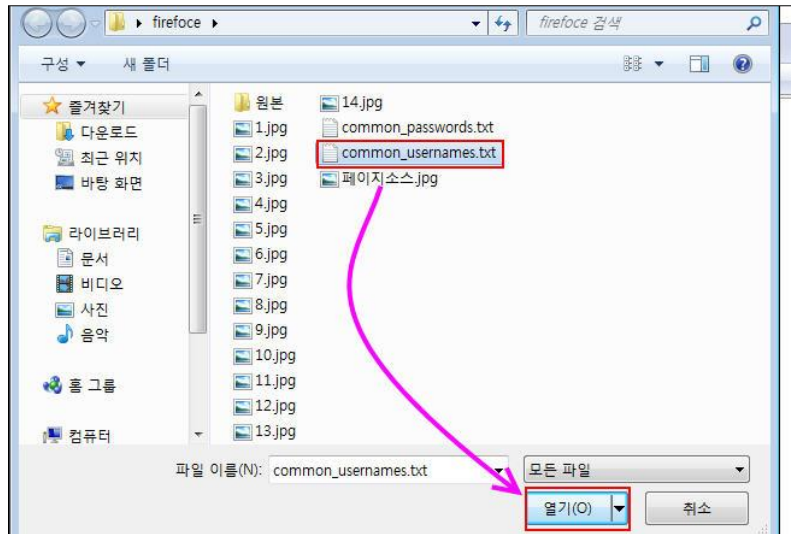


그림 8 Select common_usernames

이 툴의 가장 특징적인 부분은 인증시 실패된 에러 메시지로 패스워드를 추측해낸다.

만약 로그인 페이지 코딩 시 failed 의 에러메세지를 처리하지 않았다면 여기에서 failed 를 입력하여도 아무 소용이 없다.



그림 9 failed 입력

몇번의 인증을 요청할 것인지에 대해 물어본다 디폴트가 500이며 500번 인증을 요청시 약 10초 정도의 시간이 소요된다



그림 10 Request Number 입력

정상적으로 Brute Force 공격이 성공하였다.

이는 곧 특정 로그인 페이지의 에러메세지를 통해 충분히 Brute Force 공격이 가능하다는 것을 직접 확인해낸 것이다.



그림 11 공격 성공

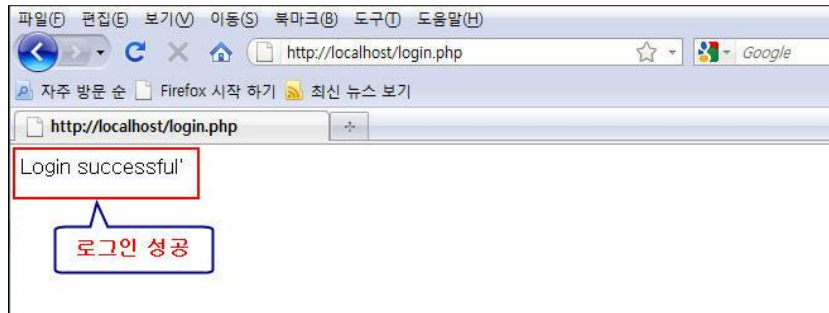


그림 12 로그인 성공

마치면서

공부를 게을리 해서 인지 정보에 눈이 어두워서 인지 이러한 툴이 존재하고 있다는 것에 놀랐고 또 하나는 특정 에러페이지의 문자열을 판단으로 Brute Force 공격이 가능하다는 것에 한번 더 놀랐습니다.

이러한 플러그인이 어떻게 만들어졌는지는 소스코드가 공개되어있지 않아 확인할 방법은 없었으나 분명한 것은 또 하나의 정보를 얻었다는 것에 있습니다.

실제 많이 쓰이는 툴이며 유저명과 패스워드 사전 파일을 직접 컨트롤 할 수 있다는 것에 큰 장점이 있네요. 기존의 정형화 되어 있던 Brute force 툴과는 다르게 가볍구요.

분석할 때 가장 곤란했던 부분은 역시 제 무지함에 있었습니다. 에러페이지 문자열을 토대로 공격한다는 것을 몰랐던 터라 에러페이지를 다르게 만들어놓았거나 다른 문자열을 집어넣었을 때 공격이 성공하지 않아 많은 어려움을 겪었습니다.

여러가지 경험으로 아주 많은 안전 진단을 시도하는 PT전문 컨설턴트들에게 많은 도움이 되었으면 합니다.

저희 STG 시큐리티 에서는 늘 기존의 기법이든 최신기법이든 항상 전문 기술적인 분석을 하고 있으며 이를 생활화 하고 있습니다.

이상 문서를 마칩니다.