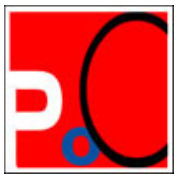
Web Proxy와 Paros, Odysseus 사용법



By poc@securityproof.net

차 례

1. web proxy란 무엇인가?

이 글에서는 해킹과 보안의 관점에서 웹 프록시 프로그램들을 소개할 것이다. 소개할 프로그램은 **Paros**[1]와 **Odysseus**[2]이며, 이미 많이들 사용하고 있지만 아직 정확한 사용법을 알지 못해 그 기능을 제대로 활용하지 못하고 있는 경우도 있다. Paros는 기능의 다양성 때문에, Odysseus는 사용의 용이성 때문에 선택하였으며, 둘 다 오픈 프로그램이라는 장점이 있다.

일반적으로 웹 클라이언트(보통 IE나 Fire Fox와 같은 웹 브라우저)는 POST나 GET 등의 방식을 통해 데이터를 웹 서버로 보내며(request), 웹 서버는 클라이언트의 요청을 처리하여 그 결과를 웹 클라이언트로 보내준다(response). 이때 웹 클라이언트에서 데이터를 보내면 그 데이터는 특별한 수정 없이 웹 서버로 보내진다. 웹 서버에서 처리한 결과를 클라이언트에 보낼 때도 마찬가지다.

Web client → Web server (request)

Web client ← Web server (response)

우리가 지금 다루려고 하는 웹 프록시는 웹 클라이언트와 웹 서버 사이에 위치한다. 웹 프록시가 중간에 위치하여 웹 클라이언트에서 보내지는 데이터를 웹 프록시가 받아 웹 서버로 중개한다. 웹 서버에서 웹 클라이언트로 보낸 데이터도 마찬가지로 웹 프록시를 거치게 된다.

Web client → Web proxy 프로그램 → Web server

Web client ← Web proxy 프로그램 ← Web server

웹 프록시 프로그램을 해킹과 보안의 관점에서 다루는 것은 웹 프록시 프로그램에서 웹 서버로 보내지는 데이터를 수정하여 보낼 수 있기 때문이다. 정상적인 상태에서는 데이터 릴레이 과정에서 데이터를 수정할 수 없다. 그러나 웹 프록시 프로그램을 사용하면 웹 서버로 데이터가 전달되기 전에 웹 클라이언트를 이용해 보내진 데이터를 수정할 수 있고, 수정된 데이터를 서버에 전달하게 된다.

---

[1] http://www.parosproxy.org

[2] http://www.bindshell.net/tools/odysseus

이는 보안의 입장에서 보면 큰 문제가 아닐 수 없다. 웹 프록시를 이용하여 웹 클라이언트에서 전달된 데이터를 웹 서버로 보내지기 전에 수정하는 한가지 예를 들어보자. Hackthissite[3]의 웹 해킹 레벨 10 문제를 보자. 이 문제는 인증 우회 관련 문제이며, 웹 프록시를 이용해 풀 수 있는 문제이다.

****

Level 10

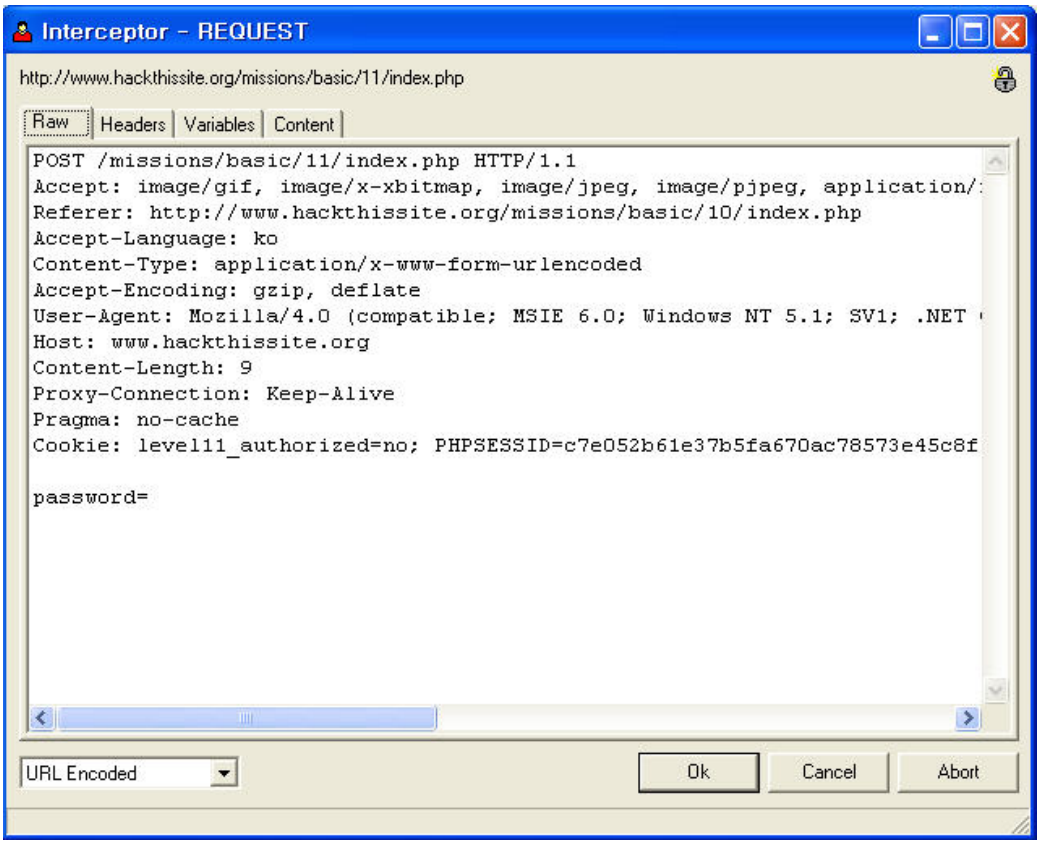
Network Security Sam has decided to hardcode the password into the script. He also started to use cookies to detect if the user is authorized to advance to the next level. When you enter the correct password, it sets you to authorized, and if you enter an incorrect password, it sets you to unauthorized.

password:

submit

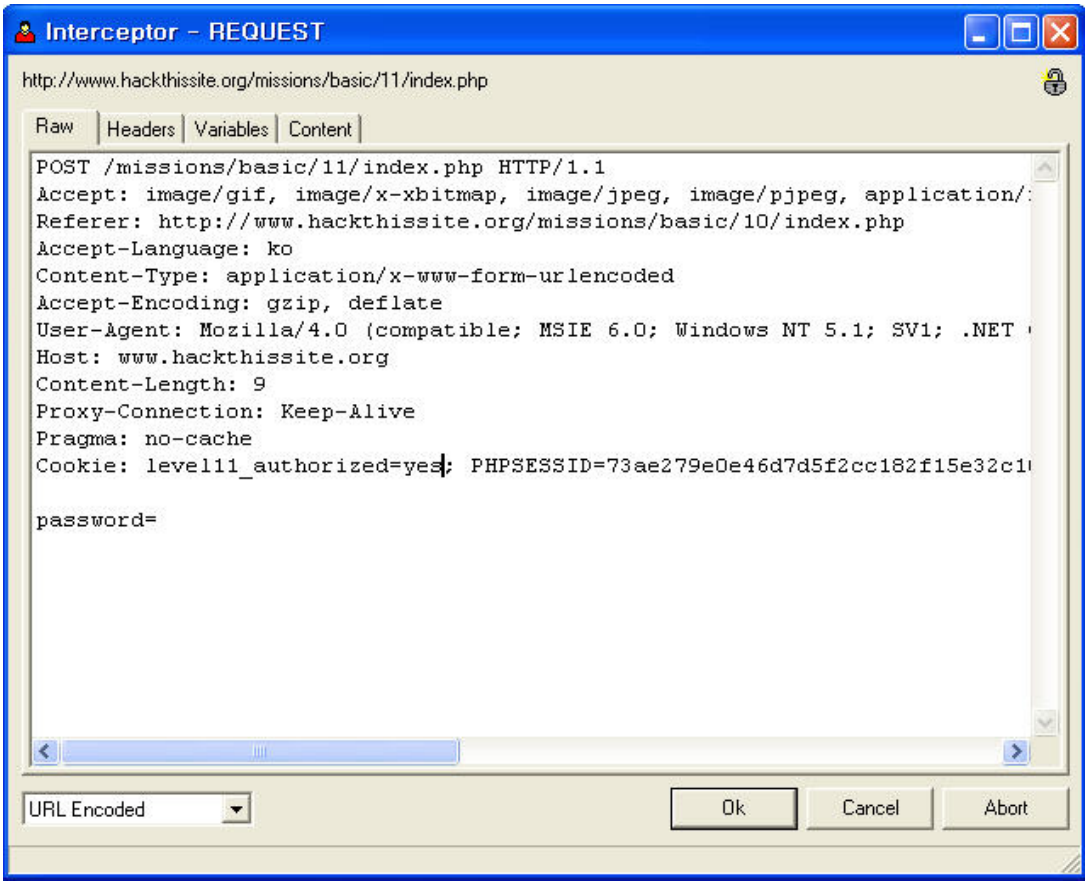
****

이 문제는 cookie를 조작하는 문제이다. 여기서는 Odysseus를 사용할 것이다. 자세한 사용법은 나중에 설명할 것이다. 먼저 submit 버튼을 누르면 다음과 같은 창이 뜬다.



[3] http://www.hackthissite.org/

위의 결과는 웹 클라이언트에 웹 서버로 보낸 데이터이다. 이 데이터를 웹 프록시가 중간에서 임시로 받은 것이다. 이 데이터를 수정 없이 웹 서버로 보낼 수도 있지만 해커는 데이터의 조작을 위해 웹 서버로 보내질 데이터를 수정할 수 있다. 웹 서버로 보내질 데이터 중에서는 인증 관련 내용이 나오는데, Cookie: level11_authorized=no; 이 부분을 다음과 같이 Cookie: level11_authorized=yes;로 수정하여 웹 서버로 보낸다. 그러면 레벨11로 로그인하게 되는 것이다.



그리고 Ok 버튼을 눌러 데이터를 서버로 보낸다. 데이터가 서버에 보내지면 다음과 같이 성공했다는 메시지가 떤다.

웹 프록시 프로그램을 이용하면 쇼핑몰 가격 조작 등 다양한 웹 해킹이 가능하다. 이 글은 웹 해킹을 직접 다루는 것이 아니라 웹 프록시 프로그램을 소개하는 것이 주 목적이다. 따라서 여기서 위의 문제 풀이 과정을 자세하게 설명하지는 않을 것이다. 그리고 알아본 hackthissite의 문제는 아주 기본적인 수준의 문제라서 별도의 설명이 필요하지 않을 것이다.

중요한 것은 웹 프록시 프로그램을 이용해 웹 서버로 전달되는 인증 관련 정보 등을 포함하여 각종 데이터를 수정 및 조작할 수 있다는 것이다.

2. Paros 소개

Paros는 웹 어플리케이션의 보안을 점검하기 위해 사용하는 웹 프록시 툴이다. 무료로 사용할 있으며, Java로 만들어졌다. 그래서 Paros를 제대로 사용하기 위해서는 Jave JRE 또는 JDK 1.4.2 또는 그 이상 버전이 설치되어 있어야 한다. Paros를 이용하여 쿠키와 form field를 포함하여 서버와 클라이언트 사이의 HTTP와 HTTPS 데이터를 가로챌 수 있고, 수정될 수 있다.

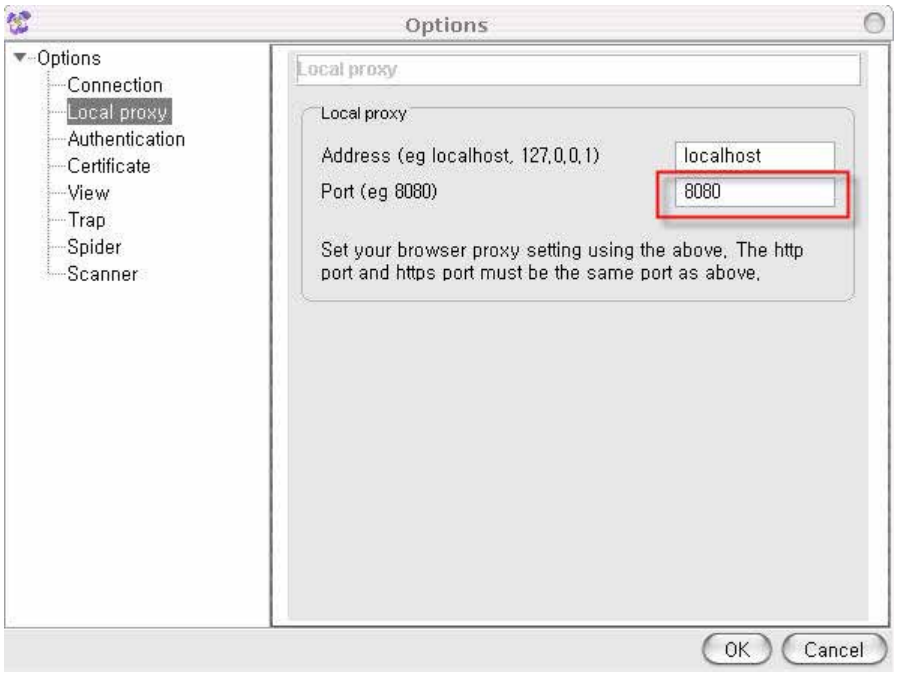
2-1. 설치 및 기본 설정

1. **Java Run Time Enviroment (JRE)** 최신 버전이 설치되어 있는지 확인한다. 설치되어 있지 않다면 http://java.sun.com/javase/downloads/index.jsp로 가서 다운받아 설치한다.

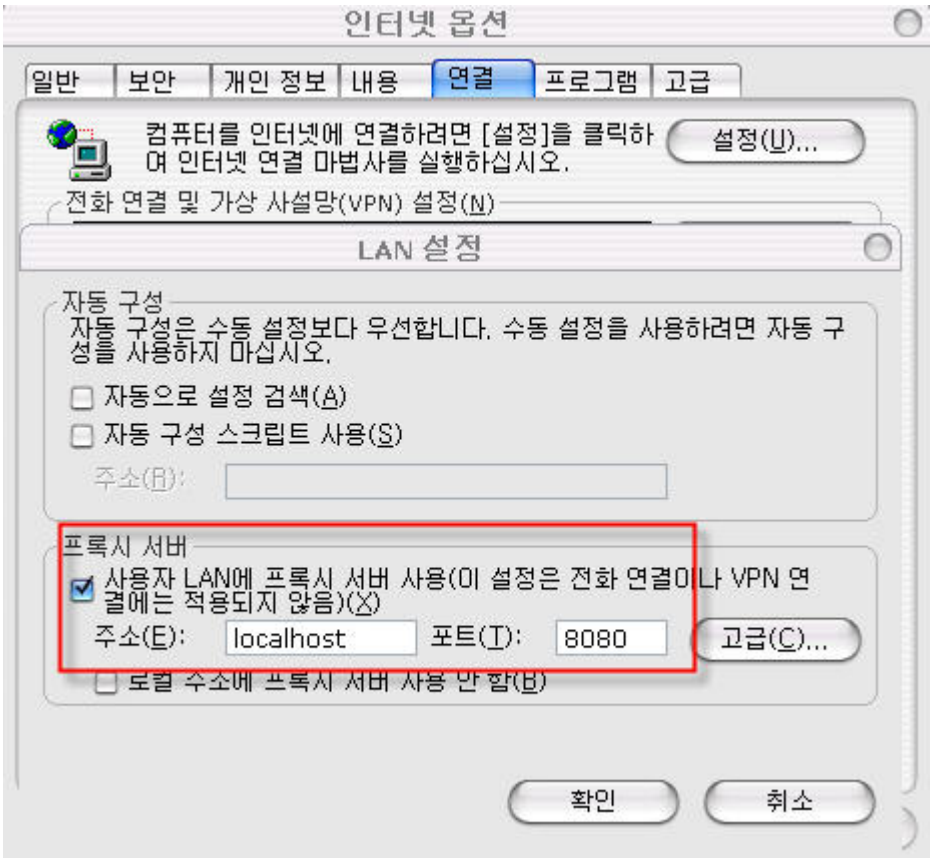
2. **Paros**를 http://www.parosproxy.org/download.shtml에서 다운받아 설치한다.

3. Windows용의 경우 설치 프로그램의 명령을 따른다. 설치가 완료되면 바탕화면에 shortcut가 생성된다. UNIX 또는 다른 플랫폼의 경우 새로운 디렉토리에 압축을 풀고, .jar 파일을 클릭하거나 명령 프롬프트에 'javaw -jar paros.jar'를 타이핑하여 실행한다. 개인 Unix 사용자의 경우 root만 사용할 수 있도록 퍼미션을 조정한다.

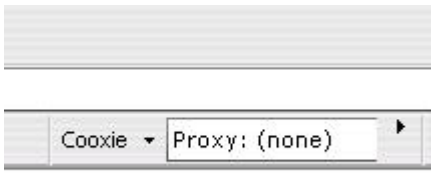
4. 이제 **Paros**를 설정해야 한다. Paros는 두 개의 포트를 사용한다. 프록시 연결을 위해서 8080을, 내부 SSL 핸들링을 위해서 8443을 사용한다. 그래서 Paros를 사용할 때는 이 두 포트가 다른 어플리케이션에 의해 사용되지 않도록 해야 한다. 물론 "Tools"의 "Options" 태그를 누른 후 Local proxy 섹션의 Port(eg 8080) 부분을 눌러 기본 포트를 변경할 수 있다.



5. IE 와 같은 웹 브라우저를 열고, LAN 설정을 다음과 같이 한다.

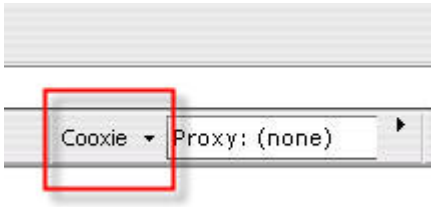


8443 포트는 Paros 그 자체에 의해 사용되는 것이며, 웹 브라우저가 사용할 것은 아니다. 그래서 이 부분에 대해서는 신경 쓸 필요가 없다. 웹 브라우저의 LAN 설정을 이렇게 설정하는 것은 번거로울 수 있다. 그래서 이 번거로움을 피하기 위해 사용할 수 있는 툴이 있다. 그 툴은 Cooxie 툴바이다. Cooxie toolbar는 http://www.diodia.com/cooxietoolbar.htm에서 다운받을 수 있다. Cooxie 툴바를 설치하면 웹 브라우저에 다음과 같이 표시된다.

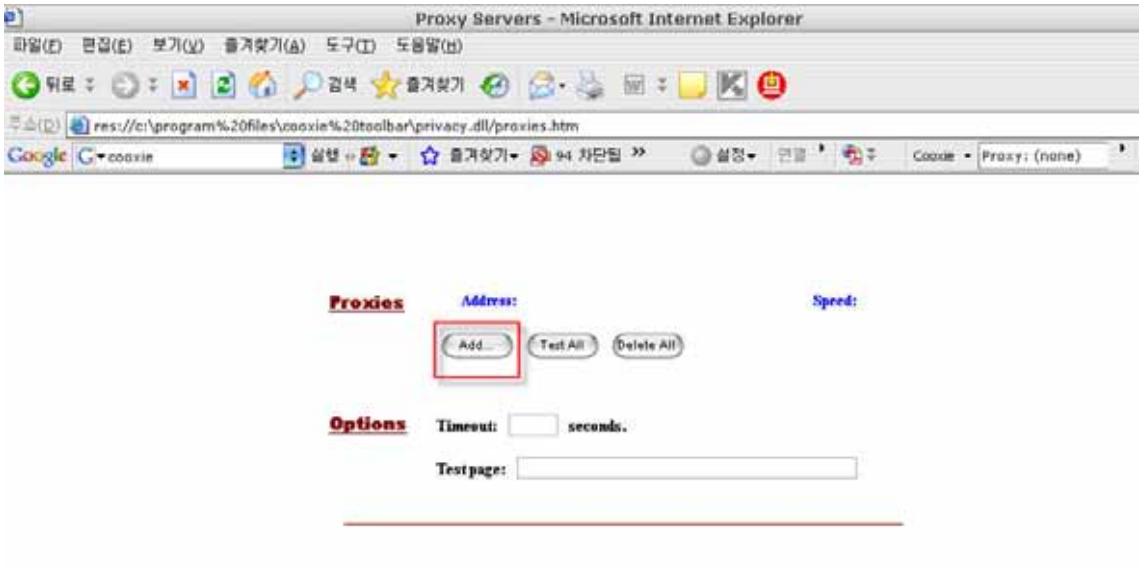


이를 잘 이용하면 웹 브라우저의 LAN 설정을 이용할 필요가 없다. 다음은 Cooxie Toolbar를 이용한 프록시 서버를 위한 포트 설정 과정이다.

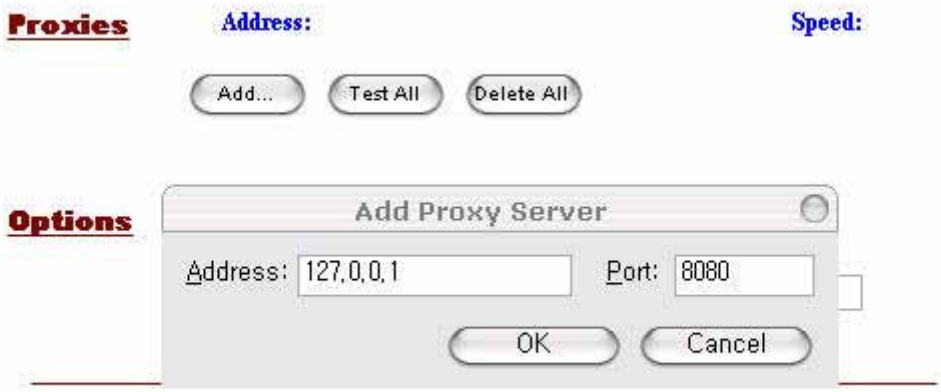
먼저 다음 Cooxie 부분을 클릭한다.



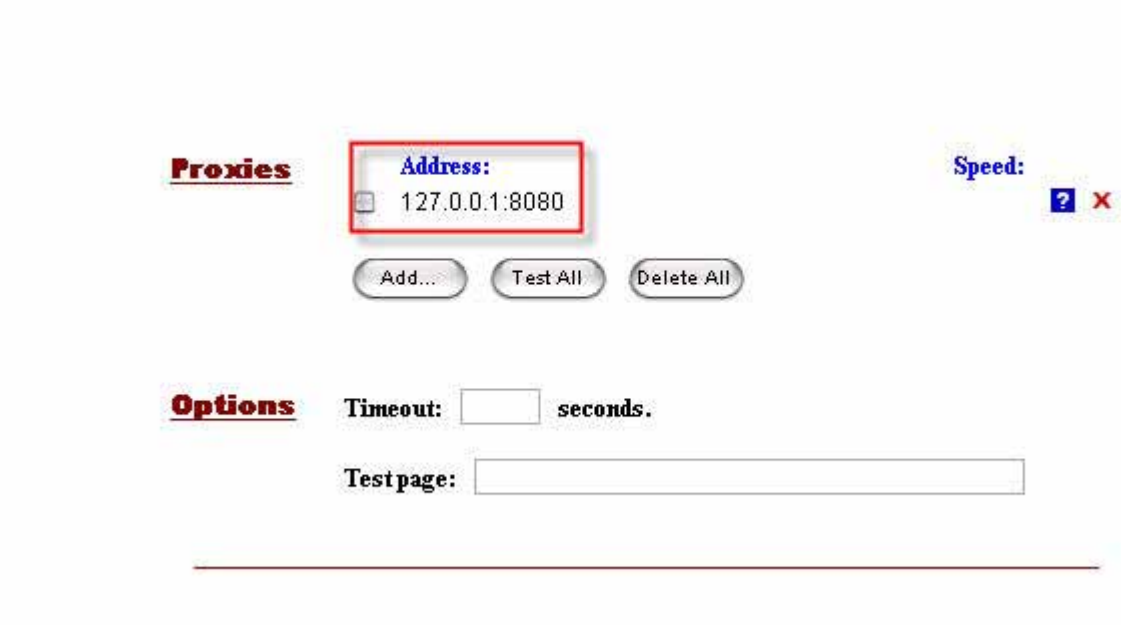
클릭하면 Proxy Servers를 클릭한다. 그럼 다음과 같은 화면이 나타난다.



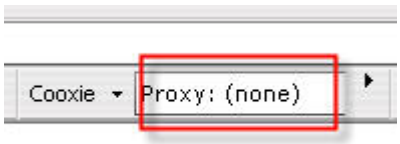
여기서 Add를 클릭한 후 다음과 같이 설정한 후 OK를 클릭한다. Local proxy 섹션의 Port를 8080에서 다른 것으로 수정하였다면 그 번호를 입력하면 된다.



설정을 하면 다음과 같이 나온다.



그런 후 체크한 부분에서 Proxy: 127.0.0.1:8080를 선택한다. Proxy:(none) 상태는 웹 프록시 프로그램을 사용하지 않는 경우이다.



6. 만약 PC가 방화벽 이면에서 실행되고 있어서 사전에 정의된 프록시를 거쳐 인터넷에 접근할 수 있다면 Paros에서 프록시 설정을 변경할 필요가 없다. 이것은 4번 단계에서 이미 살펴본 것이다.

이제 설치 및 기본 설정이 모두 끝났다.

2-2. Paros의 기능

Spider 기능

Spider는 웹 사이트를 크롤링(crawling, crawl이란 단어는 '천천히 움직이다'[4] 라는 뜻을 가지고 있는데, 여기서는 타깃이 되고 있는 사이트를 전체를 조사하며 다니는 것을 의미한다)해서 가능한 많은 URL 링크를 수집하는 것이다. 이 기능을 이용하면 직접 확인하기 전 짧은 시간 내에 웹

[4] *Oxford Quick Reference Dictionary*

사이트의 링크 계층 구조를 더 잘 이해할 수 있다. 그러나 이 글을 작성하고 있는 현재 버전 3.2.13에서는 Spider 기능을 제대로 사용할 수가 없었다. 아직 베타 단계에서 벗어나지 못한 것 같다. Spider에는 다음과 같은 기능이 있다

* 주어진 URL에 기반을 둔 HTTP와 HTTPS 웹 사이트를 크롤링
* cookie 지원
* Option 탭의 ProxyChain 필더에 설정되어 있는 proxy chaining 지원

  (Skip 필더는 spider 기능에 아무런 영향을 미치지 않음)
* 최근 스캐닝에 대해 해당 웹 사이트의 계층 구조에 자동으로 URL 링크를 추가

그러나 단순한 spider 기능이기 때문에 다음과 같은 한계가 있다:

* 유효하지 않은 인증으로 SSL이 지원되는 웹사이트는 크롤링이 안된다.
* 멀티 쓰레드 기능이 지원되지 않는다.
* HTML에 'malformed' URL은 인식될 수 없다. 또한 자바스크립트로 생성된 URL은 이 spider 기능을 이용해서 찾을 수 없다. 하지만 이런 URL은 수작업으로 통해서 찾아내고, 계층구조에 추가하면 된다.

Scanner 기능

scanner 기능은 웹 사이트 계층구조에 기반을 둔 서버를 스캐닝하는 것으로써, 서버 설정에 문제가 있는지 여부를 점검할 수 있다. 이 기능이 Paros에 추가된 것은 일반적인 웹 스캐너들의 크롤링 엔진으로는 어떤 URL 경로들의 경우 발견하거나 점검할 수 없다는 것이 밝혀졌기 때문이다. 예를 들어, 어떤 URL 링크들은 유효한 로그온 후에만 볼 수 있다. 자동 웹 스캐너는 경로들을 찾아내지 못하거나 서버 정보를 노출시킬 수 있는 백업 파일(.bak)들이 존재하는지 여부를 체크할 수 없을지도 모른다. 이 기능을 사용하기 위해 웹 사이트를 먼저 탐색할 필요가 있다. 어떤 웹 사이트에 로그온하고 탐색을 한 후 웹 사이트 계층구조가 자동적으로 Paros에 의해 만들어질 것이다. 그런 다음 다음과 같은 것을 할 수 있다:

* 만약 계층 구조에 있는 모든 웹 사이트들을 스캐닝하고자 한다면 Anaylse의 "Scan All"를 클릭
* 계층구조 트리의 한 웹 사이트를 스캐닝하고자 원한다면 tree panel에 있는 그 사이트를 오른쪽 마우스를 클릭한 후 "Scan selected Node"를 클릭

현재 Paros는 다음과 같은 점검 기능을 가지고 있다:
* HTTP PUT 허용 여부 – PUT 옵션이 서버 디렉토리에서 가능한지 점검

* Directory index가능 여부 – 서버 디렉토리들을 브라우징 가능한지 점검
* 오래된 파일 존재 여부 – 쓸모 없는 파일들이 존재하는지 점검
* Cross-site scripting – XSS이 request 파라미터에 허용되어 있는지 점검
* websphere 서버에 디폴트 파일들 존재 여부 - websphere 서버에 디폴트 파일들이 존재하는지 점검

위의 모든 점검 기능은 웹 사이트 계층 구조 트리에 있는 URL에 기초를 두고 있다. 이것은 스캐너가 각 URL에 대해 각각의 취약점에 대해 점검한다는 것을 의미한다. 이것은 웹 사이트의 계층구조에 대한 고려가 없는 blink scanning과 비교되는 점이기도 하다.

Filter 기능

filter 기능을 사용하는 것은 다음과 같은 목적이 있다:

* HTTP 메시지에 미리 정의된 패턴들을 탐지하고 알려주며, 그래서 모든 HTTP 메시지를 trap할 필요가 없고, 원하는 패턴만 찾아보면 된다.
* 흥미로운 부분의 정보, 예를 들어 cookie의 정보를 로깅한다.

Filter가 서버와 Paros 사이를 오가는 각 HTTP(S) 메시지를 가로채어 분석하기 때문에 모든 필터 기능을 활성화시키는 것은 proxy의 속도를 떨어뜨릴 수 있다. 그래서 필요한 필터 기능만 켜두는 것이 좋다.(기본적으로 LogCookie 필터가 활성화되어 있다.)

현재 Paros는 다음과 같은 filter 기능을 가지고 있다:

* LogCookie: 브라우저에서 서버로 보내진 모든 받아들인 쿠키들을 로깅
* LogGetQuery: 브라우저에서 보내진 모든 HTTP(S)의 GET 질의를 로깅한다. ‘get.xls’라는 로그 파일이 Paros 프로그램 디렉토리에 저장된다.
* LogPostQuery: 브라우저에서 보내진 모든 HTTP(S)의 POST 질의를 로깅한다. ‘post.xls’라는 로그 파일이 Paros 프로그램 디렉토리에 저장된다.
* CookieDetectFilter: HTTP response의 “Set-Cookie” 시도를 알리고, 수정할 수 있게 한다.
* IfModifiedSinceFilter: HTTP request의 'If−Modified−Since' & 'If−None−Match' 헤더 필더들을 제거한다. 이것은 ‘HTTP 304 not modified’ 대신 ‘HTTP 200 OK’ response를 저장하는데 사용될 수 있다.

HTTP request와 response Trapping 기능

Paros는 HTTP(S) request/response들을 trap(‘trap’이란 단어는 덫으로 가두는 것을 의미하는데,

여기서는 웹 클라이언트가 웹 서버로 보낸 데이터를 임시로 '가두고' 데이터 수정을 가능하게 해준다는 의미가 있다.)하여 직접 수정할 수 있다. Paros를 통해 전달되는 모든 HTTP와 HTTPS 데이터는 trap되어 수정될 수 있다. 이 기능은 웹 해킹에서 아주 중요한 부분이다. Paros를 이용해 데이터를 조작하여 웹 서버에 보낼 수 있다. 이와 같은 기능을 Odysseus를 이용해 hackthissite의 웹 해킹 문제를 풀어본 것을 통해 이미 알아보았지만, Paros의 이 기능에 대해서는 뒤에서 별도로 살펴볼 것이다.

1. Trap Request

   "Trap"의 "Trap Request" 체크 박스에 체크를 하면 모든 request들은 trap된다. Header/Body의 텍스트 부분의 내용을 수정할 수 있으며, 그런 다음 Continue 버튼을 클릭한다. "Tabular View" 버튼이 있는데, 이 버튼은 "Trap Request"에 체크가 되어 있을 경우에만 사용될 수 있다. 그리고 "Body" 텍스트 부분에 텍스트가 있는데, 이것은 편집을 쉽게 하기 위해 HTTP POST request를 테이블 form으로 변환하기 위해 사용된다. 파라미터들을 수정한 후에는 "Original View" 버튼을 클릭하여 업데이트된 request로 이전 스크린으로 돌아갈 수 있다.

2. Trap Response

   "Trap" 탭의 "Trap Response"를 체크하면 모든 response가 trap된다. Header/Body 텍스트 부분의 내용을 수정할 수 있으며, "Continue" 버튼을 클릭하여 더 실행한다. 여기서 "Tabular View" 버튼은 소용 없다. "Tabular View"는 HTTP(S) POST 요청을 trap할 때만 유용하다.

기타 다른 기능들

앞에서 언급된 주 기능들 이외에도, Paros에는 몇 가지 기능들이 있다:

* 클라이언트 인증 지원 - 어떤 웹 어플리케이션들은 클라이언트 인증을 요구한다. 많은 man-in-the-middle 프록시들은 이런 상황에서는 작동할 수 없다. 왜냐하면 handshaking 또는 로그온을 위한 인증을 저장할 수 없기 때문이다. 필요한 클라이언트 인증 정보를 handshaking 또는 로그온 바로 직전에 Paros로 가져옴으로써 클라이언트 인증을 요구하는 웹 어플리케이션들의 HTTP 데이터를 가로채 수정할 수 있다. 이 기능을 사용하기 위해 Tools -> Options -> Certificate 순으로 이동하여 User Client Certificate 부분을 체크한다.

* 이동 중인 HTTP request와 response를 로깅한다. Response 시간도 역시 기록된다.

* Base64, SHA1 및 MD5를 포함하여 다른 인코딩/해쉬 포맷으로 데이터를 변환한다. 이 기능은 웹 보안을 위해 점점 많은 사이트들이 웹 방화벽을 도입하여 특정 공격 문자열에 대한 필터링을 하고

있는 상황에서 유용한 기능이다. 예를 들어, 공격에 사용되는 특정 태그를 인코딩하여 사용하며 기본적인 필터링의 경우 우회할 수 있게 된다. 또한 로깅 과정에서 이루어지는 특정 signature 분석 및 탐지를 우회하여 웹 방화벽 같은 것을 무력화시킬 수 있다. 물론 이를 위해 다른 제3의 인코딩/디코딩 툴을 사용해도 상관없지만, 필요한 기능이 가까이에 있다는 것은 좋은 일이다. 보안의 입장에서는 인코딩된 문자열까지도 탐지하여 필터링할 수 있어야 한다. 이 기능을 사용하기 위해서는 Tools -> Encoder/Hash를 클릭하면 변환을 위한 별도의 창이 떤다. 이것을 이용하면 우리가 자주 사용하는 암호 인코딩/디코딩을 할 수 있다.

이상에서 Paros의 다양한 기능을 살펴보았다. 앞에서 설명된 것을 그냥 눈으로 머리로 받아들이지 말고 직접 테스트 해보는 것이 이해를 위해 가장 좋다. 모든 기능에 대해 테스트를 하면서도 불법적인 행위를 하지 않기 위해 워 게임 사이트를 대상으로 테스트를 해보는 것은 좋은 생각이다. 보안 전문가들은 보안을 목적으로 자신이 관리하는 사이트를 테스트할 수 있을 것이다.

앞에서는 웹 프록시 프로그램 Odysseus를 이용한 인증 우회 방법을 간단하게 알아보았는데, 이제 Paros를 이용해 데이터를 조작하는 방법에 대해 알아보도록 하겠다. 테스트는 워 게임 사이트인 hackthissite에서 실시되었다.

2-3. Paros를 이용한 웹 해킹의 예

다음은 hackthissite의 Realistic Missions 레벨 1 문제이다. 이런 종류의 문제는 실제 웹 해킹에서 인증 우회와 더불어 웹 프록시 프로그램이 가장 많이 사용되는 분야 중의 하나일 것이다.

****

From: HeavyMetalRyan

Message: Hey man, I need a big favor from you. Remember that website I showed you once before? Uncle Arnold's Band Review Page? Well, a long time ago I made a $500 bet with a friend that my band would be at the top of the list by the end of the year. Well, as you already know, two of my band members have died in a horrendous car accident... but this asshole still insists that the bet is on!
I know you're good with computers and stuff, so I was wondering, is there any way for you to hack this website and make my band on the top of the list? My band is Raging Inferno. Thanks a lot, man!

Welcome to Uncle Arnold's Local Band Review Page!

These are some bands that play in the chicago suburban area. Please contribute your own ratings as well.

Imposing Republic
Imposing Republic is a rock band that incorporates a bit of everything that is good. Good music and good lyrics make this band awesome.
The average rating of this band is 23.107846155906. How would you rate it?

1 vote!

Three Spins Five
A merry mix of brass instruments, bongos, a turn table, and various other sounds and composed in such a unique and melodic way. Tip top, I give it a A.
The average rating of this band is 4.794992435452. How would you rate it?

1 vote!

The Flag of Nothing
A young punk band consisting of idealistic but underdeveloped theories about how money should be distributed within our country. It is good to see that they are trying to mix a message with their music, but the tunes suck. I give it a C
The average rating of this band is 3.6064935510428. How would you rate it?

1 vote!

Killing Mr. A.P.E.
A hip hop group of five people who recently moved in from the city and wants to "be representin'" in the suburban areas. The music is can barely be considered music at all but they seem to have a way of livening the crowds. I give it a D.
The average rating of this band is 2.6534181307877. How would you rate it?

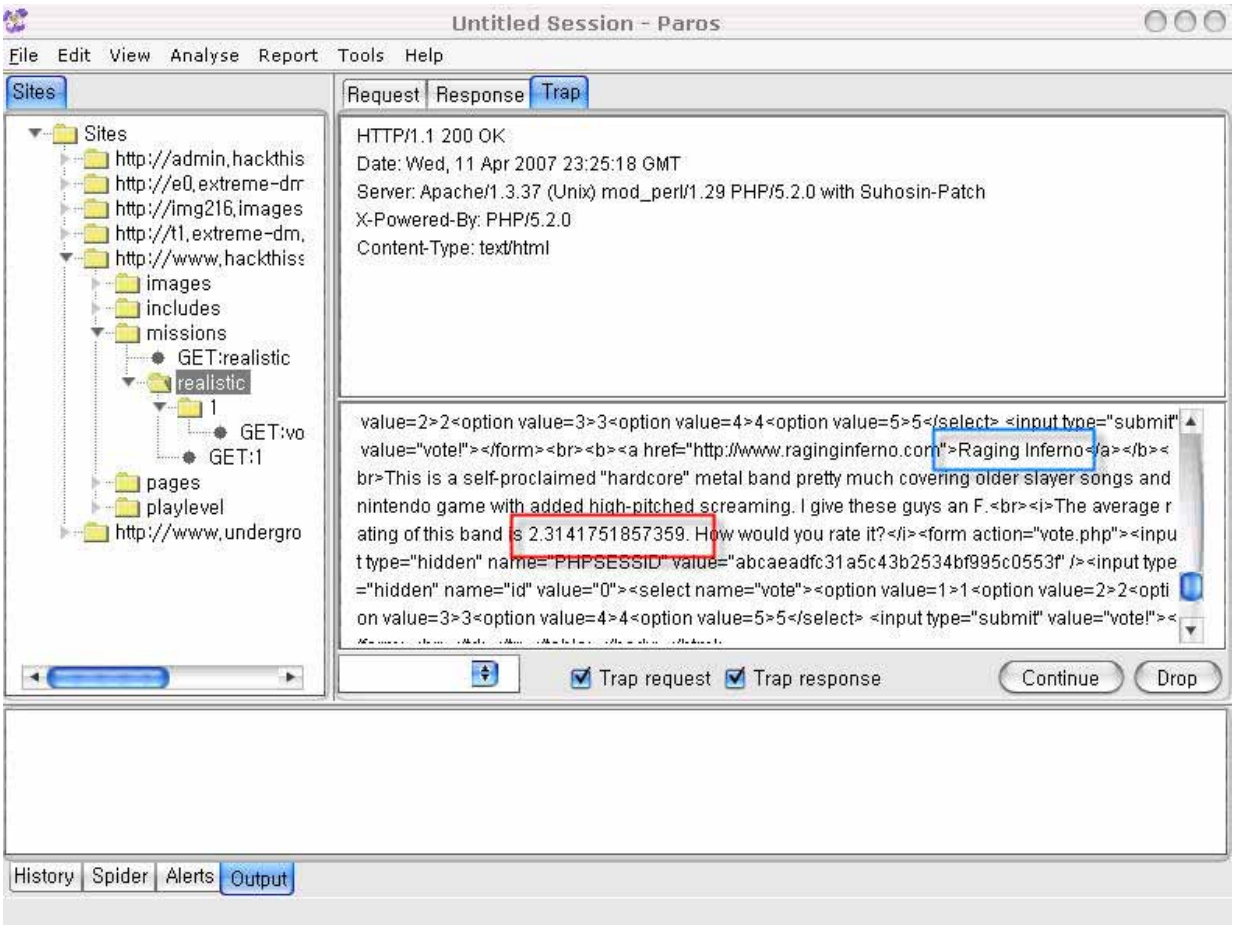
1 vote!

Raging Inferno
This is a self-proclaimed "hardcore" metal band pretty much covering older slayer songs and nintendo game with added high-pitched screaming. I give these guys an F.
The average rating of this band is 2.3141751857359. How would you rate it?

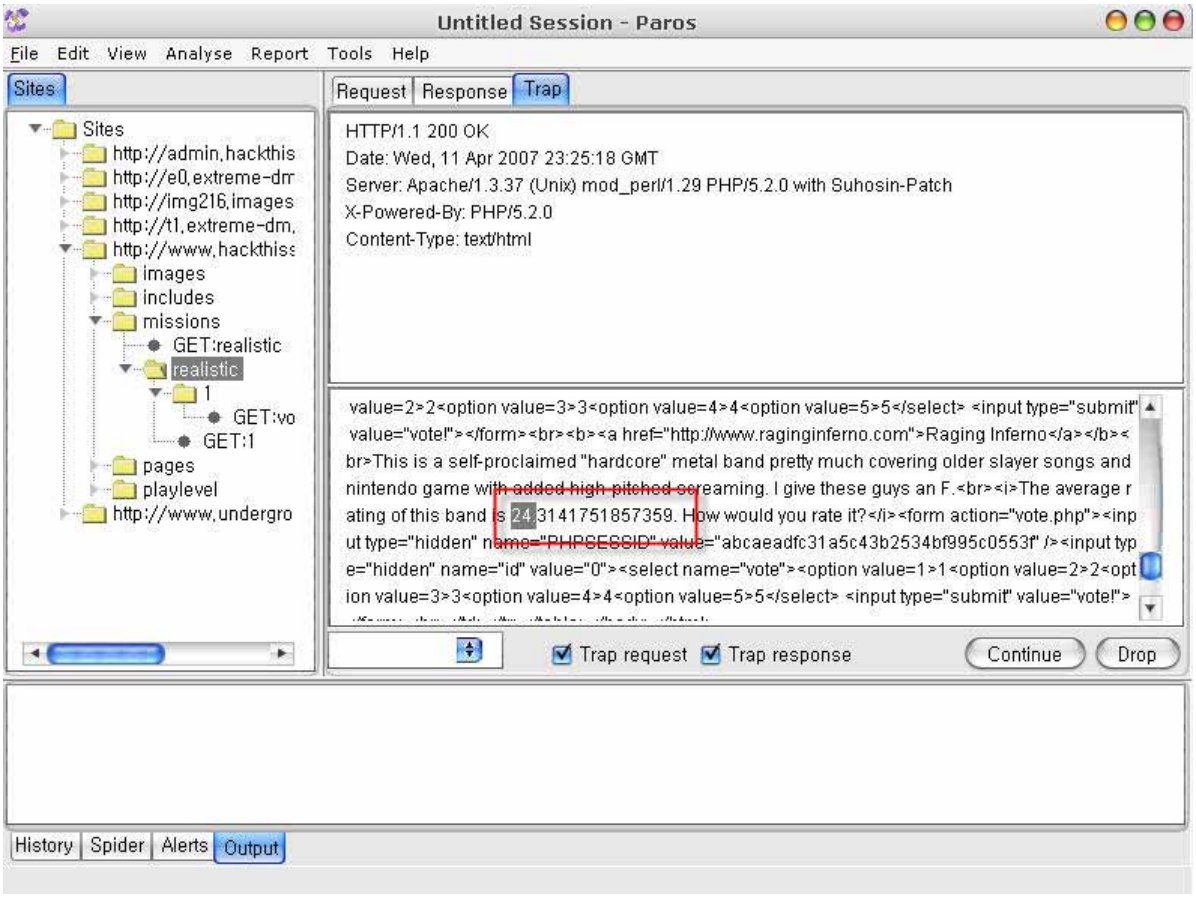
1 vote!

****

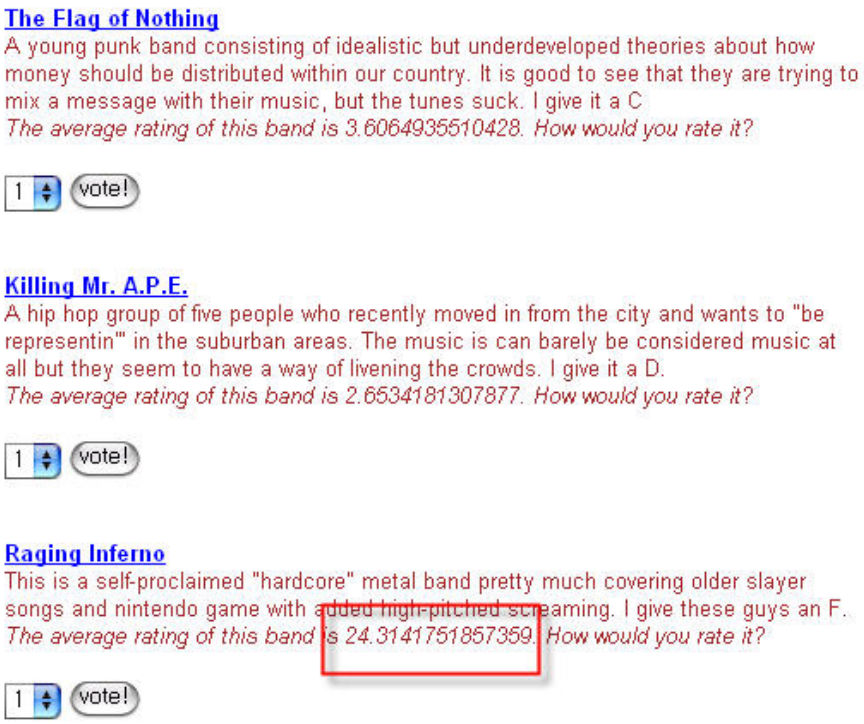
이 문제는 현재 꼴찌인 **Raging Inferno**의 순위를 투표를 통해 1위로 올리는 것이다. 정상적인 경우라면 한번밖에 투표를 할 수 없고, 투표 시 점수도 1점밖에 줄 수 없다. 그러나 웹 프록시를 거치면 투표할 수 있는 점수가 1점에 국한되지 않는다. 웹 클라이언트에서는 직접 데이터를 조작할 수 없지만 웹 프록시 프로그램에서는 데이터를 조작할 수 있기 때문이다. 먼저 Paros를 실행하면 다음과 같이 원래의 데이터 값 *2.3141751857359*가 trap 되어 있다.



이 문제의 미션은 Raging Inferno의 순위를 1위로 만드는 것이다. 현재 1위의 값은 **Imposing Republic**의 *23.107846155906*이다. 그렇다면 **Raging Inferno**의 값을 **Imposing Republic**의 값보다 많게 만들면 된다. Trap된 **Raging Inferno**의 값을 다음과 같이 *24.3141751857359*로 수정하였다.



그런 다음 Continue 버튼을 클릭하면 수정된 값이 서버로 전달된다. 조작된 값에 대한 점검 정책이 없는 서버의 경우 조작된 값을 그대로 받아들이게 된다. 그 결과를 보면 다음과 같다.



Raging Inferno의 값이 *24.3141751857359*로 수정되었고, 미션에 성공했다. 이 과정을 다음과 같이 간단하게 도식화할 수 있다. 먼저 웹 프록시를 사용하지 않을 경우에는 다음과 같이 1이 더해진 값이 전달된다.

Web client	→	**Web server**
2*.3141751857359*		***3****.3141751857359*
(원래의 값)		(서버에 전달된 값)

그러나 웹 프록시의 trap 기능을 이용해 원래의 데이터를 가둔 후 그 값을 수정하여 서버로 post하면 다음과 같이 값이 전달된다.

Web client	→	**Web proxy 프로그램**	→	**Web server**
2*.3141751857359*		***24****.3141751857359*로 수정		***24****.3141751857359*
(원래의 값)		(수정된 값)		(최종 전달된 값)

좀더 정확하게 순서를 말하면 다음과 같다.

① 최초의 값 ***2****.3141751857359*
② 웹 클라이언트에서 vote! 버튼을 클릭하면 ***2****.3141751857359*이 서버로 post됨
③ 웹 프록시에서 ***2****.3141751857359*을 trap함
④ 웹 프록시에서 trap된 값 ***2****.3141751857359*을 ***24****.3141751857359*로 수정
⑤ 서버로 수정된 값 ***24****.3141751857359*을 서버로 전달
⑥ 미션 완료

3. Odysseus 소개

Odysseus를 소개하는 것은 앞에서 말했지만 사용의 용이성 때문이다. 최근에는 Telemachus와 함께 사용할 수 있게 되었다. Paros처럼 다양한 기능은 없지만 로그인 우회 및 데이터 조작 등에 사용될 수 있다. Odysseus는 별도의 랜 설정 없이 바로 사용 가능하다는 장점이 있다.

3-1. 설치 및 기본 사용 방법

1. Odysseus를 http://www.bindshell.net/tools/odysseus에서 다운받아 설치한다. 설치 과정에서 특별하게 어려운 부분은 전혀 없다.

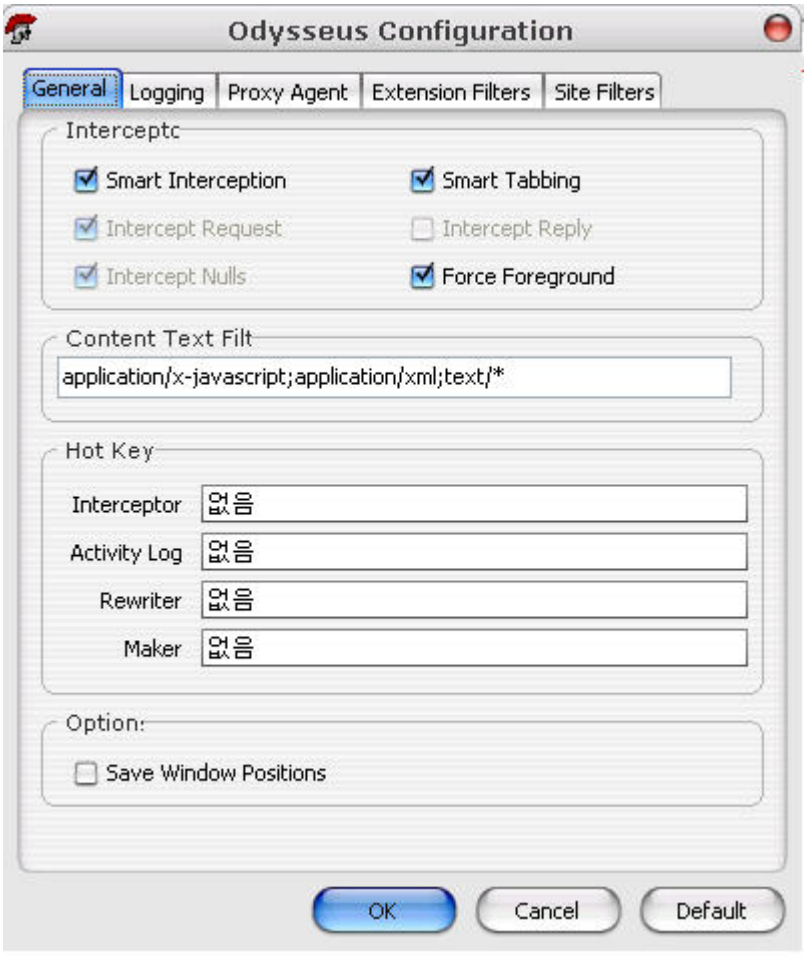
2. Odysseus를 실행한다. 실행을 한 후 오른쪽 하단에 있는 Odysseus를 오른쪽 마우스 클릭한다.

3. 기본적인 설정 상태에서 Odysseus를 사용하려면, IE Proxy Setting 중에서 None과 Odysseus 중에서 Odysseus를 설정한다.

4. 다시 오른쪽 하단에 있는 Odysseus를 오른쪽 마우스 클릭한다.

5. Interceptor를 체크한다. 그러면 Odysseus를 사용할 준비가 된 것이며, Telemachus[5]를 실행하여 같이 사용하면 된다. 준비가 되었다면 Odysseus의 색깔이 녹색으로 변한다.

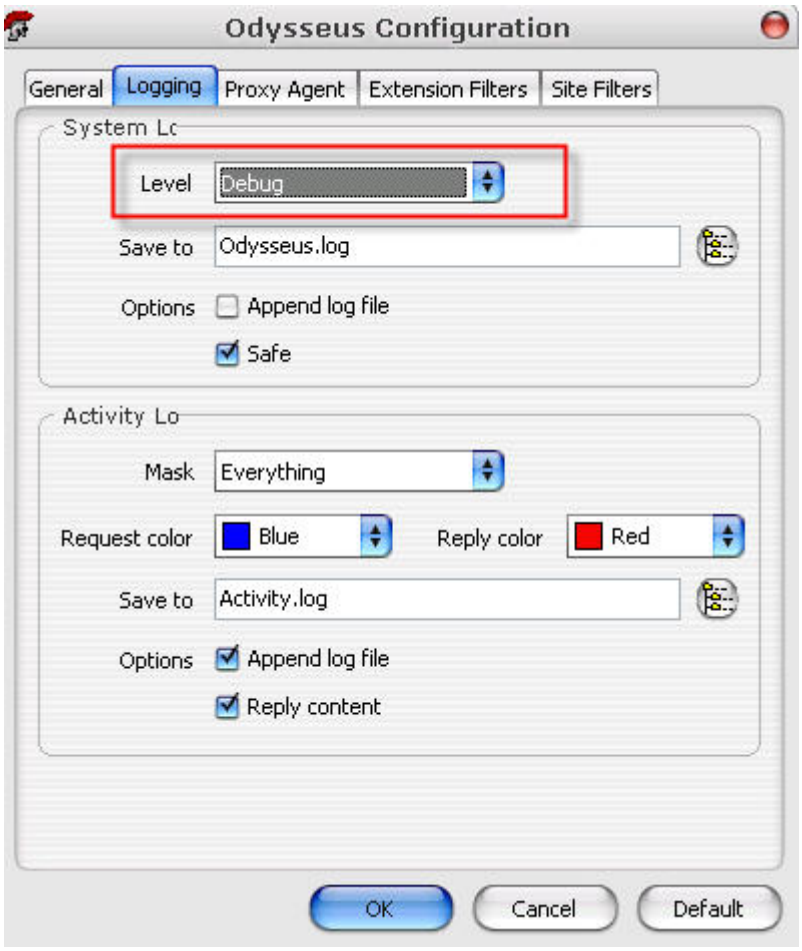
6. 그러나 기본 설정 이외의 기능을 사용하기 위해서는 Configuration을 클릭한다. **General** 부분은 다음과 같다.



[5] http://www.bindshell.net/tools/telemachus

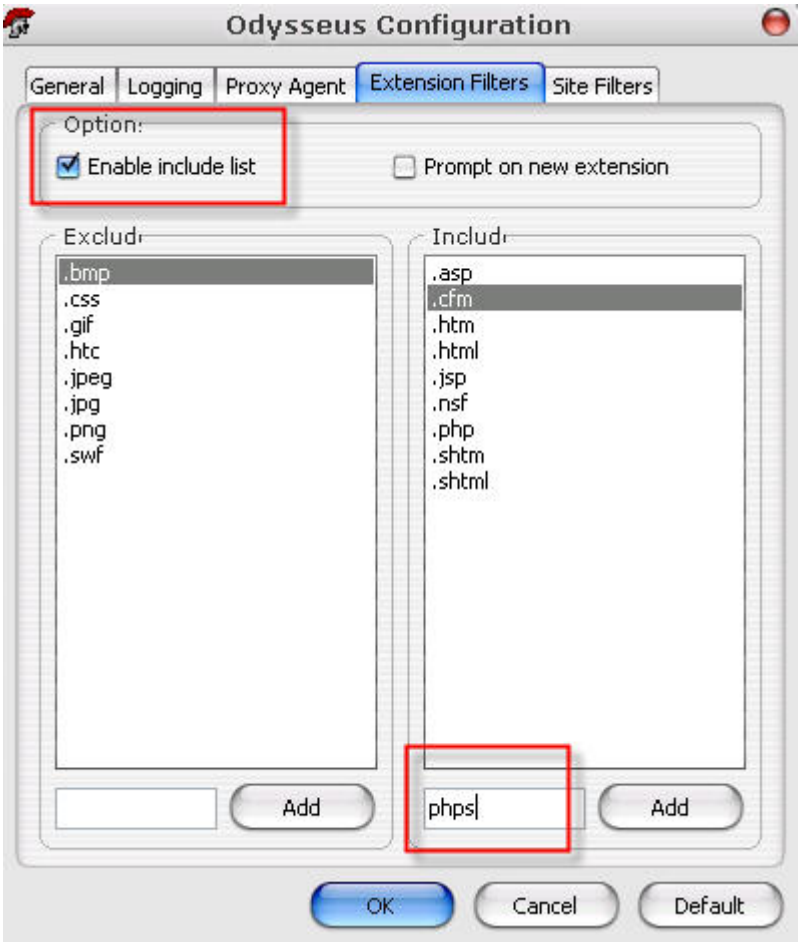
기본적으로는 Smart Interception은 체크가 되어 있지 않지만, 전체 기능을 다 사용하기 위해 여기서는 체크한다.

Logging 부분에서 몇 가지 선택할 Level이 있다. 디폴트는 Debug이다. Insane 옵션은 소켓 커뮤니케이션 문제를 디버깅하기 위해 주로 사용되며, 모든 소켓 stream으로부터 오는 데이터를 로깅한다. Diabolical 옵션은 OpenSSL locking call을 디버깅하는데 사용된다. 이 레벨은 목적에 따라 선택하여 사용하면 되는데, 일반적으로 웹 해킹에서는 디폴트 상태인 Debug를 사용하면 된다.



Proxy Agent 부분에서는 Odysseus가 사용하는 포트를 설정할 수 있는데, 기본 포트는 50000번이다. 다른 부분은 특별히 사용할 것이 없다.

다음 부분은 **Extension Filters**인데, 여기서는 필터링할 파일의 확장자를 지정할 수 있다. Exclude는 배제하기 위한 것이며, Include는 포함시키기 위한 것이다. Include 부분에 파일 확장자를 추가하기 위해서는 Enable include list 부분을 체크한 후 다음과 같이 파일을 추가한다. 그런 다음 Add를 클릭하면 된다.



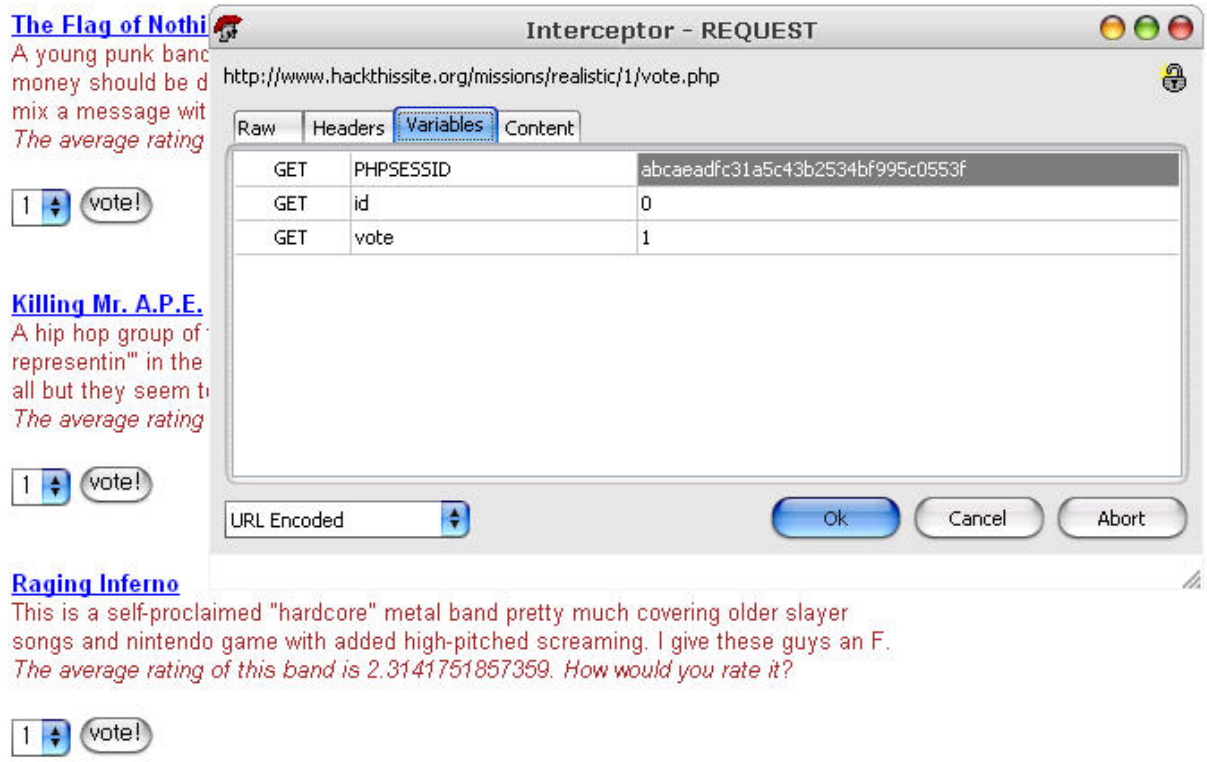
다음으로 설정할 부분은 **Site Filters**인데, 이 부분에 별도로 추가할 필요는 없을 것이다. 필터링 없이 전체 사이트를 점검하는 것이 중요하기 때문이다.

3-2. Odysseus를 이용한 웹 해킹의 예

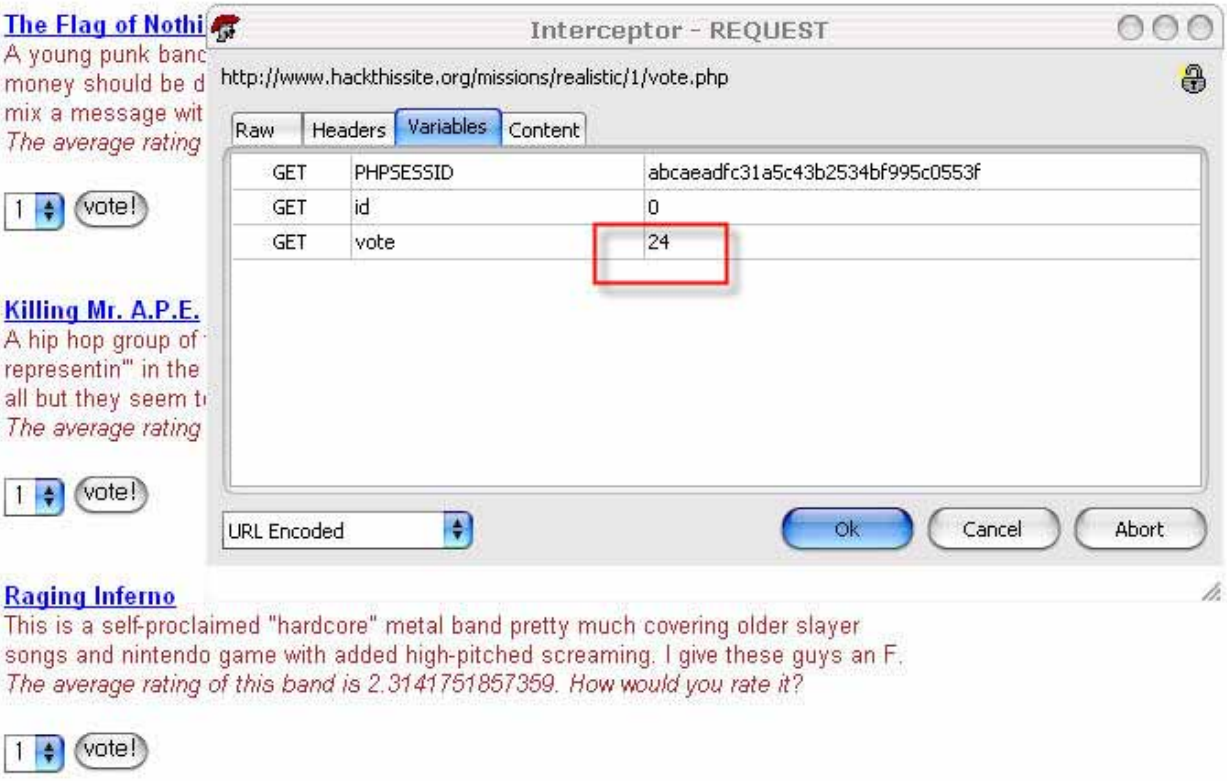
Odysseus의 사용법은 앞에서 Paros를 이용해 풀었던 hackthissite의 Realistic Missions 레벨 1 문제 풀이를 통해 설명하고자 한다. 문제에 대한 설명은 이미 앞에서 했으므로 여기서는 문제 자체에 대한 설명은 없이 문제 풀이 과정을 그대로 보여주는 방식을 선택하도록 하겠다. 웹 클라이언트에서 데이터를 post하고, 그런 다음 웹 프록시 프로그램을 거친 후, 웹 서버로 데이터가 전달되는 과정은 앞에서 Paros를 이용해 문제를 풀었던 6단계와 동일하다.

먼저 문제 풀이 사이트로 가서 로그인을 하고, 문제 풀이 페이지로 이동한다. 그런 다음 Odysseus를 실행한다. 여기서 Odysseus의 설정은 모든 부분이 디폴트 상태로 설정된 상태이다. IE Proxy Setting 부분에서 Odysseus를 선택하고, 다시 Interceptor를 체크한다. 이제 Odysseus를 사용할 준비가 되었다.

이제 Raging Inferno 부분에서 vote!를 클릭한다. 그러면 다음과 같이 Odysseus의 창이 뜬다.



여기서 vote 부분의 값 1을 24로 다음과 같이 수정한다. 24로 수정하는 이유는 Paros 설명 부분에서 설명하였다. 그런 다음 OK를 클릭하면 조작된 데이터가 서버로 전달된다.



서버에서 조작된 값을 보내면 다음과 같이 성공했다는 메시지를 볼 수 있다.

Paros를 이용하던 Odysseus를 이용하던 그 과정은 같다. 두 프로그램의 기능에서 차이가 있지만 핵심 기능에서는 별 차이가 없다. 자신에게 편하고, 상황에 맞는 프로그램을 선택하여 사용하면 된다. 그리고 웹 프록시 프로그램에는 이 두 개 이외에도 더 있다. 따라서 자신에게 가장 필요한 웹 프록시 프로그램을 선택하는 것은 자신의 취향과 상황에 달려있는 셈이다.