



To be Red Team/Penetrate Tool Review

Fiddler를 활용한 웹 모의해킹

NELpos 2016.06.13 15:07

" 이 포스트는 이런 분에게 추천합니다. "

- Fiddler를 처음 사용하시는 분
- Fiddler를 웹 모의해킹 진단에 활용하고 싶으신 분
- 웹 디버깅을 위해 사용하시는 분(단, 해킹 위주의 기능 설명이 많음)

단, 해당 포스트에 나와있는 내용을 바탕으로 절대로 허가받지 않는 사이트에 웹 모의해킹을 시도하지 말아주세요. 해당 게시글에 노출되어 있는 URL에 웹 공격 및 스캔 시도를 하지 말아주세요.

1. 글쓰기에 앞서

올해 진행된 Codegate를 비롯하여 고객사에서 웹 모의해킹 진단을 할때는 항상 burp suite를 활용하여 진단을 하였다. 그러다가 우연히 Fiddler를 알게 되었는데 이 프로그램 역시 별도의 프록시 설정 없이도 웹 모의해킹 진단이 가능하였고 Burp Suite와는 다른 또다른 매력에 빠질 수 있는 툴이었다. Fiddler와 burp suite를 적절하게 활용한다면 웹 모의해킹을 조금더 효율적으로 가능하다는 것도 확인할 수 있었다.

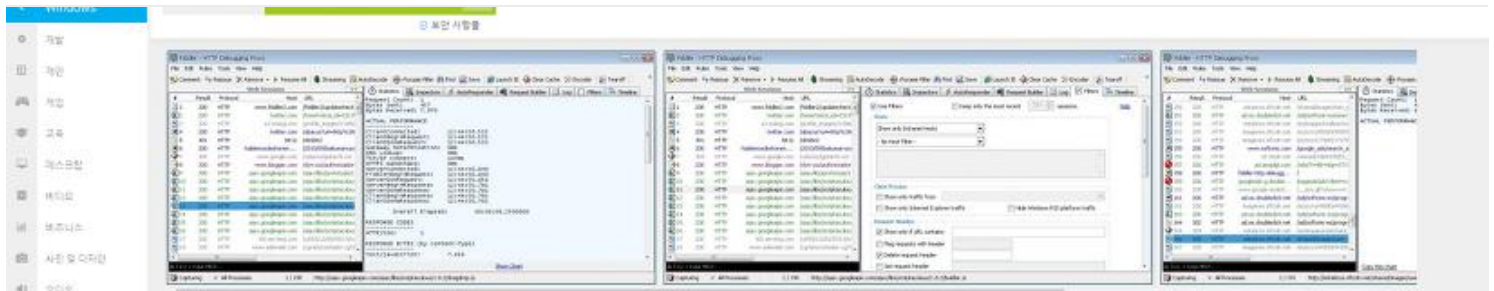
2. 피들러 다운로드

<https://fiddler.kr.uptodown.com/windows>

NELpos

당신의 친구가 해커라면?

CATEGORY



피들러(Fiddler)는 프록시 역할을 하면서 사용자의 컴퓨터와 인터넷 사이 일어나는 여러 HTTP 트래픽 문제를 다변경합니다.

여러 탭으로 나뉘어 있는 프로그래밍의 인터페이스는 사용자가 빠르고 쉽게 방문한 기록이 있는 모든 서버에의 통계에 접근할 수 있도록 합니다. '갑작스럽게' 불리기도 하는 이 기능 덕분에 모든 요청(request)의 콘텐츠를 확인해 특정 대담(response)을 해당 포맷으로 보낼 수 있습니다.

더욱 흥미로운 기능으로는 구체적인 HTTP 세션 트랜스미션을 확인할 수 있는 능력을 이용해 중요치 않은 트래픽과 타임바에 필터링을 설정해 시간을 절약하는 기능입니다.

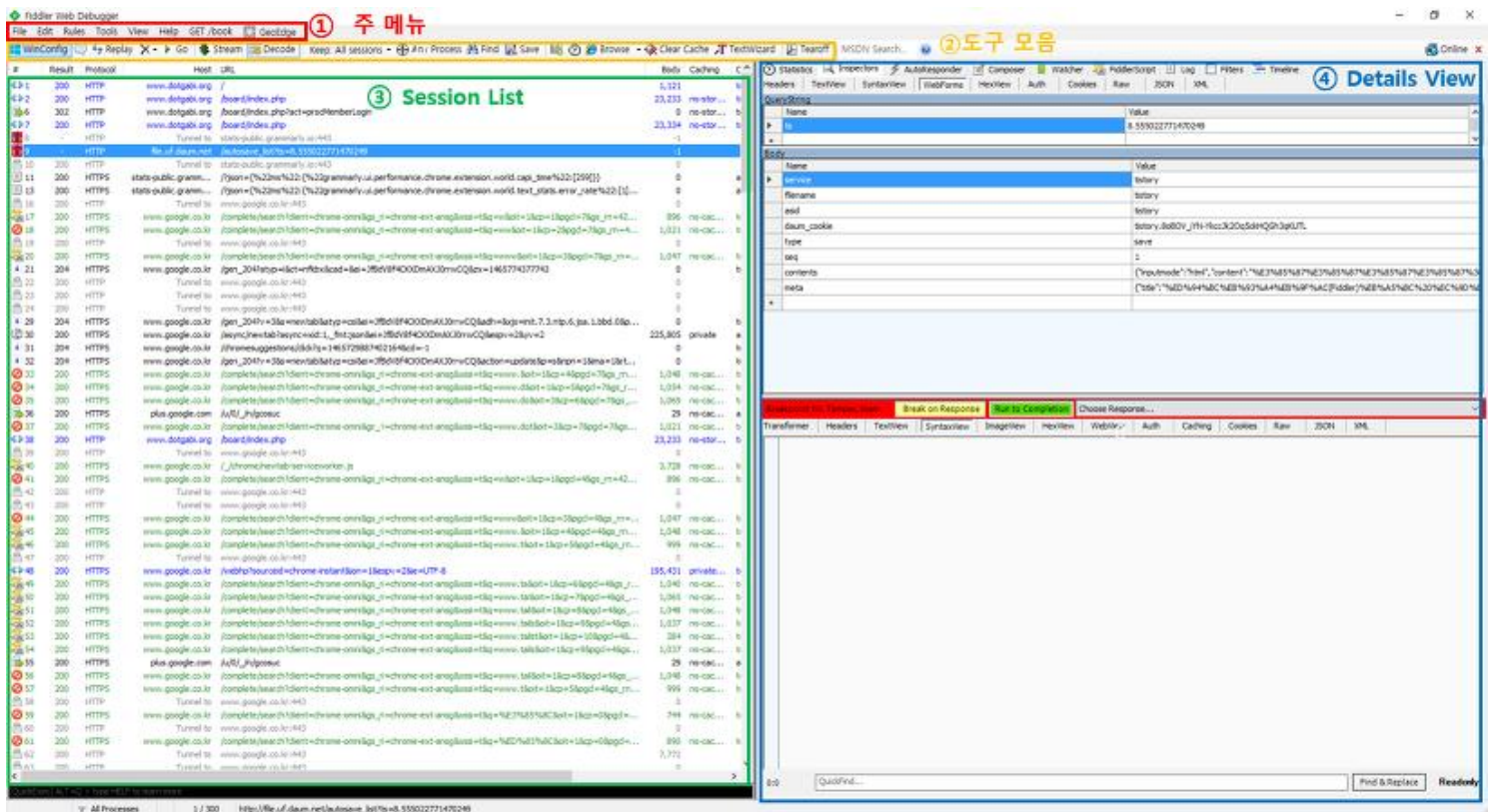
START DOWNLOAD

3 steps to Fast Package Tracking

1. Click to Begin
2. Download App
3. Track Packages Free - Instantly

3. 피들러 주요 기능 살펴보기

피들러(Fiddler)를 실행시켜보면 아래 그림과 같은 창이 뜨게 된다. 틀기능을 간략하게 분류해보면 4가지로 분류할 수 있다.



① 주 메뉴: File, Edit, Rules, Tools, View, Help, GET/book, Decade, WinConfig, Replay, Go, Stream, Decode, Keep All Sessions, Show in Process, Find, Save, Browse, Clear Cache, TextWizard, Test, NSDN Search, 도구 모음, Online

② 도구 모음: Statistics, Inspectors, AutoResponder, Composer, Watcher, FiddlerScript, Log, Filters, Timeline

③ Session List: Table view showing HTTP sessions with columns for Result, Protocol, Host, URL, Size, Cache, and C.

④ Details View: Right-hand pane showing details for a selected session, including Headers, Body, and meta information.

① 주메뉴, ②도구 모음, ③Session List, ④Details View



NELpos

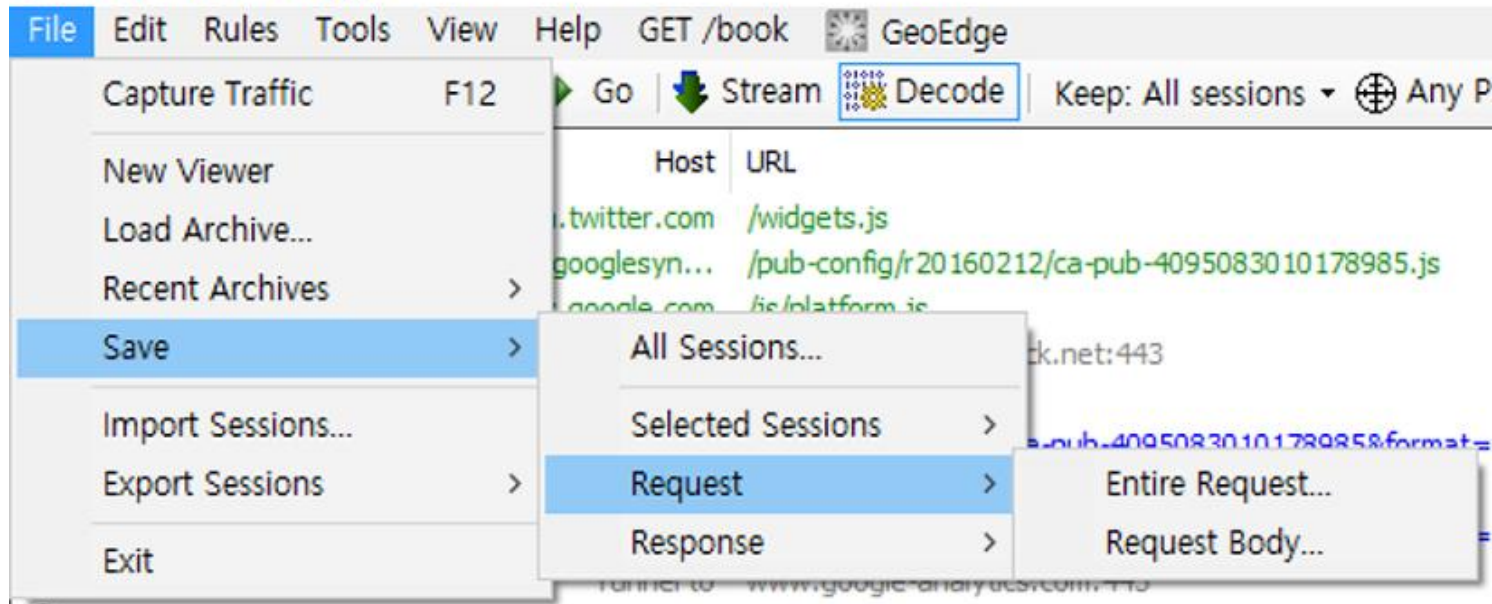
당신의 친구가 해커라면?

CATEGORY

3-1. 주메뉴

3-1-1. File

Fiddler Web Debugger

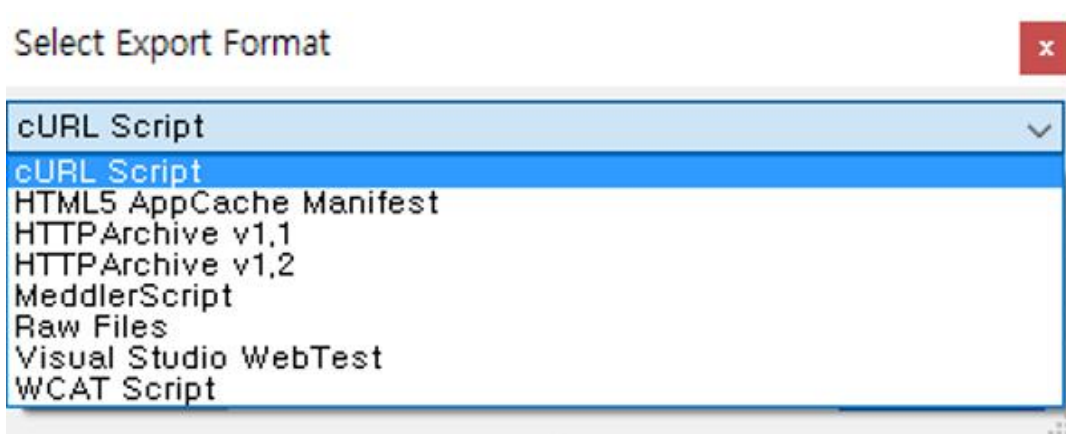


1) Capture Traffic : 트래픽 캡처할때 사용된다.

2) Load Archive : 저장된 세션을 불러온다.

3) Save : 캡처된 세션을 저장한다. 다양한 옵션 제공(모든 세션 저장, 선택된 세션 저장, Request만 저장 Response만 저장)

4) Export Session : 세션 추출이 기능, 추출 저장 형태는 아래 그림과 같이 다양한 형태 지원



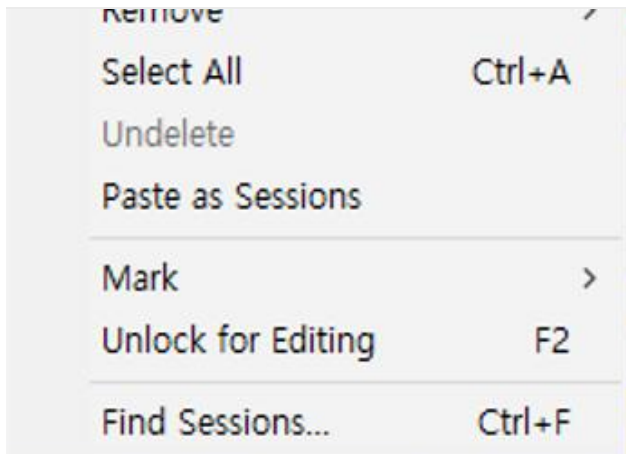
3-1-2. Edit



NELpos

당신의 친구가 해커라면?

CATEGORY



- 1) Copy : 세션 복사
- 2) Remove : 세션 제거
- 3) Select All : 모든 세션 선택
- 4) Mark : 세션 마킹 (중앙 줄 굵기, 색깔 변경 등), 웹 모의해킹 진행시 체크가 필요한 세션 마킹시 유용

483 200 HTTP ifyourfriendishacker... /admin/entry/post/getDaumCookie.php
 484 200 HTTP file.uf.daum.net /hostname.xml?1465779214780_host_9

5) Find Sessions(Ctrl + F) : 원하는 세션을 찾게 해준다.

필자가 생각하기에는 마킹보다는 이 기능이 자신이 모의해킹을 진행하는 사이트를 구별 표시하기에 더 유용한 것 같다.

예를 들어 www.dotgabi.org 사이트를 표시하기 위해서 검색어에 'www.dotgabi.org'를 넣게 되면 아래와 같이 음영색으로 표시되서 한 눈에 알아보기 쉽다.

40	200	HTTPS	clients1.google.com	/tbproxy/af/query?client=Google%20Chrome	28	private	t
41	304	HTTPS	ssl.google-analytics...	/ga.js	0	Expires...	t
42	200	HTTP	www.dotgabi.org	/	1,121		t
43	200	HTTP	www.dotgabi.org	/board/index.php	23,233	no-stor...	t
44	302	HTTP	www.dotgabi.org	/board/index.php?act=procMemberLogin	0	no-stor...	t
45	200	HTTP	www.dotgabi.org	/board/index.php	23,334	no-stor...	t
46	0	HTTP	Tunnel to	stats-public.grammarly.io:443	0		
47	0	HTTP	file.uf.daum.net	/autosave_list?ts=8.555022771470249	0		
48	200	HTTP	Tunnel to	stats-public.grammarly.io:443	730		

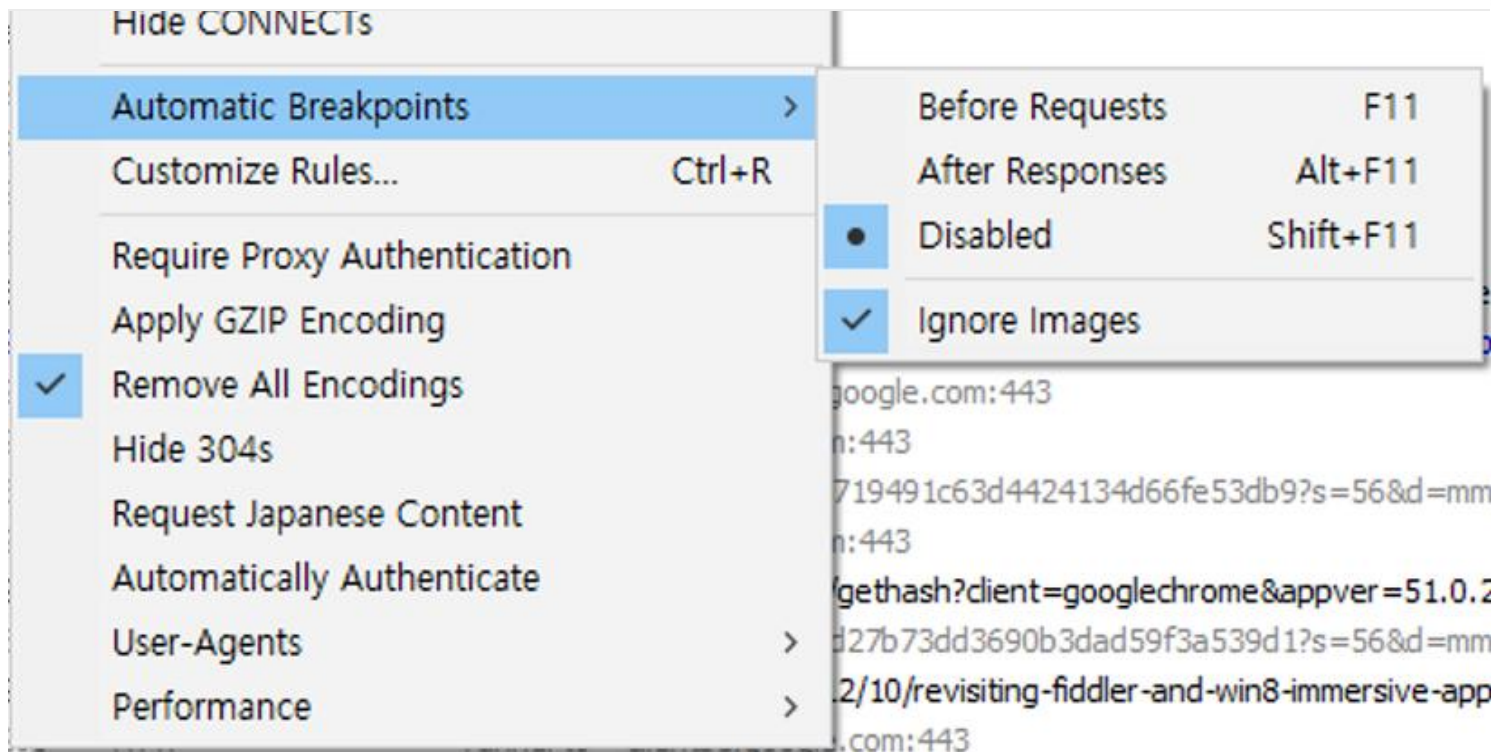
3-1-3. Rules



NELpos

당신의 친구가 해커라면?

CATEGORY



1) Hide Image Requests : 이미지 요청 숨기기

2) Automatic Breakpoints : 수동 브레이크 설정

- **Before Requests** : Request 요청 전에 breakpoint 설정, 웹 Request 변조시 사용

- **After Responses** : Response 응답 전에 breakpoint 설정, 웹 Response 변조시 사용

3) Customize Rules : 사용자가 Script를 개발하여 필요한 Rules 적용 가능



NELpos

당신의 친구가 해커라면?

CATEGORY

```

public static RulesOption("Request &Japanese Content")
var m_Japanese: Boolean = false;

// Automatic Authentication
public static RulesOption("Automatically Authenticate")
BindPref("fiddlerscript.rules.AutoAuth")
var m_AutoAuth: Boolean = false;

// Cause Fiddler to override the User-Agent header with one of the defined values
// The page http://browserscope.org/browse?category=selectors&ua=Mobile%20Safari is a good place to find updated versions:
RulesString("User-Agents", true)
BindPref("fiddlerscript.ephemeral.UserAgentString")
RulesStringValue(0, "Netscape 4.3", "Mozilla/3.0 (Win95; I)")
RulesStringValue(1, "WinPhone8.1", "Mozilla/5.0 (Mobile; Windows Phone 8.1; Android 4.0; ARM; Trident/7.0; Touch; rv:11.0; Windows NT 6.1; en-US) AppleWebKit/533.21.1 (KHTML, like Gecko) IPhone/810.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Safari/600.1.4")
RulesStringValue(2, "Safari5 (Win7)", "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11) AppleWebKit/601.1.56 (KHTML, like Gecko) Version/8.0.2 Safari/601.1.56")
RulesStringValue(3, "Safari9 (Mac)", "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11) AppleWebKit/601.1.56 (KHTML, like Gecko) Version/8.0.2 Safari/601.1.56")
RulesStringValue(4, "iPad", "Mozilla/5.0 (iPad; CPU OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Safari/600.1.4")
RulesStringValue(5, "iPhone6", "Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Safari/600.1.4")
RulesStringValue(6, "IE 16 (XPSP2)", "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)")
RulesStringValue(7, "IE 47 (Vista)", "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1)")
RulesStringValue(8, "IE 8 (Win2k3 x64)", "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; WOW64; Trident/4.0)")
RulesStringValue(9, "IE 48 (Win7)", "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)")
RulesStringValue(10, "IE 9 (Win7)", "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)")
RulesStringValue(11, "IE 10 (Win8)", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)")
RulesStringValue(12, "IE 11 (Surface2)", "Mozilla/5.0 (Windows NT 6.3; ARM; Trident/7.0; Touch; rv:11.0) like Gecko")
RulesStringValue(13, "IE 11 (Win8.1)", "Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko")
RulesStringValue(14, "Edge (Win10)", "Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/14.14263.0.0")
RulesStringValue(15, "Opera", "Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.17")
RulesStringValue(16, "Firefox 3.6", "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.7) Gecko/20100625 Firefox/3.6")
RulesStringValue(17, "Firefox 43", "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0")
RulesStringValue(18, "Firefox Phone", "Mozilla/5.0 (Mobile; rv:18.0) Gecko/18.0 Firefox/18.0")
RulesStringValue(19, "Firefox (Mac)", "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0) Gecko/20100101 Firefox/24.0")
RulesStringValue(20, "Chrome (Win)", "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36")
RulesStringValue(21, "Chrome (Android)", "Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36")
RulesStringValue(22, "ChromeBook", "Mozilla/5.0 (X11; CrOS x86_64 6680.52.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36")
RulesStringValue(23, "GoogleBot Crawler", "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)")
RulesStringValue(24, "Kindle Fire (Silk)", "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-us; Silk/1.0.22.78_100133;")
RulesStringValue(25, "CUSTOM...", "%CUSTOM%")
public static var sUA: String = null;

```

3-1-4. Tools

Tools View Help GET /book GeoEdge

Fiddler Options...

WinINET Options...

Clear WinINET Cache Ctrl+Shift+X

Clear WinINET Cookies

TextWizard... Ctrl+E

Compare Sessions Ctrl+W

Reset Script

Sandbox

View IE Cache

Win8 Loopback Exemptions

HOSTS...

New Session Clipboard...

1) **Fiddler Options**: 포트 설정, 프록시 설정, HTTPS 설정, 글씨크기 설정, 연결 도구 설정등이 가능하다.



NELpos

당신의 친구가 해커라면?

CATEGORY

Fiddler Options

General HTTPS Connections Gateway Appearance Extensions Performance Tools

Fiddler can debug traffic from any application that accepts a HTTP Proxy. All WinINET traffic is routed through Fiddler when "File > Capture Traffic" is checked. [Learn more...](#)

Fiddler listens on port:

[Copy Browser Proxy Configuration URL](#)

☐ Capture FTP requests

☐ Allow remote computers to connect

☒ Reuse client connections

☒ Reuse server connections

☒ Act as system proxy on startup

☒ Monitor all connections ☐ Use PAC Script

☐ DefaultLAN

☐ [REDACTED]

Bypass Fiddler for URLs that start with:

[Help](#) Note: Changes may not take effect until Fiddler is restarted.

- Gateway : 프록시 설정 기능, Burp와 같이 사용시 Manual Proxy Configuration에 아이피, 포트를 넣어주면 된다.

(Allow remote computers to connect를 체크해주게 되면 안드로이드나 아이폰 프록시 설정을 통해 분석이 가능하다)



NELpos

당신의 친구가 해커라면?

CATEGORY

By default, Fiddler "chains" to the system's default proxy (Client -> Fiddler -> Gateway -> Web). These settings allow you to override that behavior.

- ☒ Use System Proxy (recommended)
☐ Automatically Detect Proxy using WPAD
☐ Manual Proxy Configuration:

☐ No Proxy

Show Current Gateway Info

Help

Note: Changes may not take effect until Fiddler is restarted.

OK

Cancel

- Appearance : 글자 크기 설정
- Extensions : 확장 dll 등록
- Tools : TextEditor 연결 설정, Script Editor 연결 설정, diff 툴 연결 툴 경로 설정

2) WinINET Options : 인터넷 설정 옵션창 열기

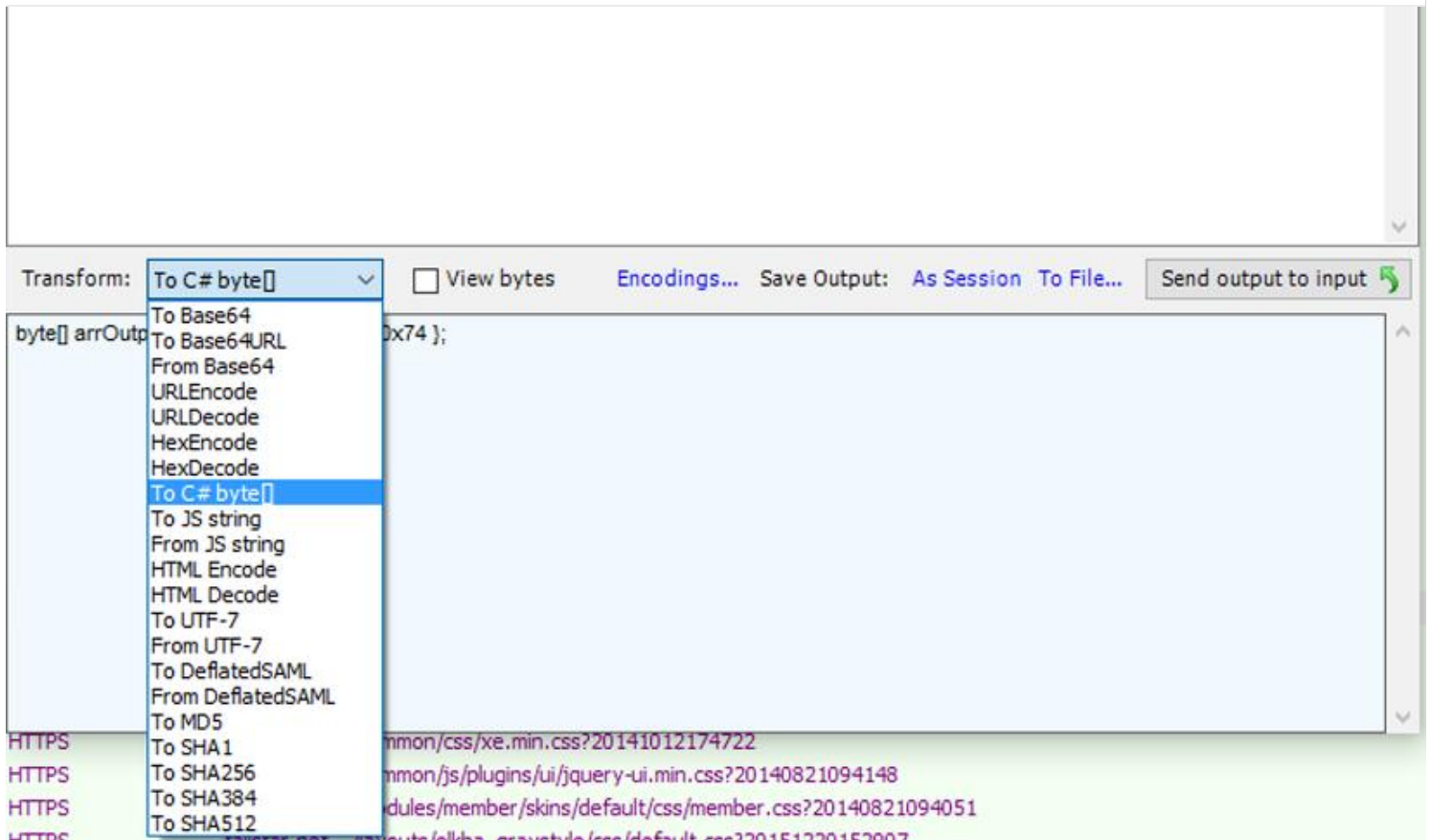
3) TextWizard : 인코딩/디코딩(한글 지원), C#byte, JSSTRING 문자열 변환등



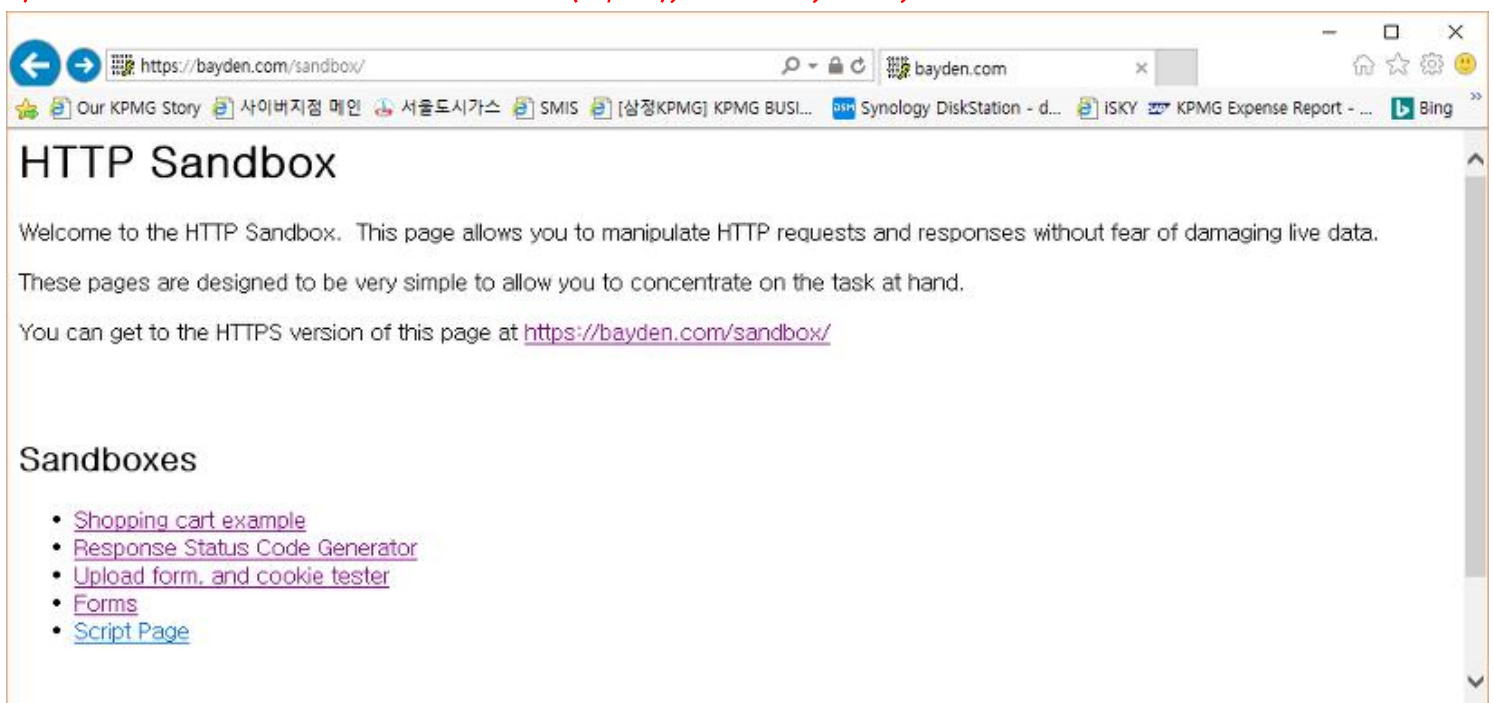
NELpos

당신의 친구가 해커라면?

CATEGORY



4) Sandbox : 개발자의 디버깅 편의를 위해 일부 폼(ID/PW), 결제 사이트, 업로드, 쿠키등 테스트 페이지 사이트 제공





NELpos

당신의 친구가 해커라면?

CATEGORY

Headers:

```

Connection: Keep-Alive
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR
Cookie: ASPSESSIONIDAUTB0BRC=LGFJGLPCDHFECLBHFBEJBGH
Host: bayden.com
Referer: https://bayden.com/sandbox/
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
DNT: 1
  
```

1_	2_	3_	4_
찾아보기...			
Go			

5) Win8 Loopback Exceptions : 윈8에서 루프백을 하는 프로그램들의 캡처 여부를 선택할 수 있다. 기본으로 Internet Explorer, Microsoft Edge가 설정되어 있으며 추가적으로 캡처를 원하는 어플리케이션이 있으면 해당 프로그램을 체크를 해주면 된다

AppContainer Loopback Exemption Utility
— □ ×

For security and reliability reasons, Windows blocks "Immersive" apps from sending network traffic to the local computer. This utility enables removal of this restriction for debugging purposes.

Refresh

Exempt All

Exempt None

Save Changes

[Learn more...](#)

DisplayName	Description	Package	AC Name	AC SID	AC User(s)	Binaries
<input type="checkbox"/> 3D Builder	3D Builder	Micros...	Microso...	S-1-15-2-3995...	hmjung	(None)
<input type="checkbox"/> @C:\Windows\Win...	@C:\Windows\Wi...	(No Pa...	winstor...	S-1-15-2-2608...	Everyone	C:\Windows\System32\...
<input type="checkbox"/> Assigned Access Loc...	Launches above lo...	Micros...	Microso...	S-1-15-2-2705...	hmjung	\\?\C:\Windows\System...
<input type="checkbox"/> CheckPoint.VPN	CheckPoint.VPN	Check...	CheckP...	S-1-15-2-3676...	Everyone	(None)
<input type="checkbox"/> Groove 음악	Groove 음악	Micros...	Microso...	S-1-15-2-3132...	hmjung	(None)
<input type="checkbox"/> JuniperNetworks.Jun...	JuniperNetworks.J...	Juniper...	Juniper...	S-1-15-2-4137...	Everyone	(None)
<input type="checkbox"/> MSN 건강	HealthAndFitness	Micros...	microso...	S-1-15-2-1138...	hmjung	C:\WINDOWS\system32...
<input type="checkbox"/> MSN 금융	MSN 금융	Micros...	Microso...	S-1-15-2-3492...	hmjung	(None)
<input type="checkbox"/> MSN 날씨	MSN 날씨	Micros...	Microso...	S-1-15-2-2040...	hmjung	(None)
<input type="checkbox"/> MSN 뉴스	MSN 뉴스	Micros...	Microso...	S-1-15-2-5081...	hmjung	(None)

Refreshed AppContainer information at 오전 8:22:25.

3-2. 도구 모음

도구 모음의 각 메뉴마다 주요 기능을 하단 요약된 그림을 참고 바란다.

**NELpos**

당신의 친구가 해커라면?

CATEGORY



3-3 Session List

캡처된 세션 리스트를 보여준다.

NELpos

당신의 친구가 해커라면?

CATEGORY

45	200	HTTP	www.dotgabi.org	/board/index.php	23,334	no-stor...	text/html; c...	chrome...	[#7]
69	200	HTTP	www.dotgabi.org	/board/index.php	23,233	no-stor...	text/html; c...	chrome...	[#38]
510	200	HTTP	group1.maggie.dau...	/maggie/opencounter/Open.do?service...	0			chrome...	
3...	200	HTTP	ir-na.amazon-adsys...	/e/jr?o=1&t=baydensystems&l=w00	42	no-cache	image/gif	chrome...	
4...	200	HTTPS	js.dntry.com	/antenna2.js?0_4201_130207489_6979...	17,495	public, ...	text/javasc...		
1...	200	HTTP	Tunnel to	ad.doubleclick.net:443	0				
1...	200	HTTP	localhost	/Screenshot_10-52-29.jpg	345,095		image/jpeg		
1...	408	HTTPS	watson.telemetry....	/Telemetry.Request	512	no-cac...	text/html; c...	verfaul...	
1...	200	HTTP	www.dotgabi.org	/board/index.php	23,233	no-stor...	text/html; c...	chrome...	
1...	200	HTTP	Tunnel to	nexus.officeapps.live.com:443	0			csisync...	
1...	201	HTTPS	nexus.officeapps.li...	/nexus/upload/%7b99E10300-E4B2-420...	0	no-cac...		csisync...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	200	HTTPS	docs.google.com	/fe/rpc/s/config?oid=u523d2b2259015...	398	private...	application/...	chrome...	
1...	200	HTTPS	docs.google.com	/fe/rpc/s/offline/docs?oid=u523d2b225...	170	private...	application/...	chrome...	
1...	200	HTTP	Tunnel to	roaming.officeapps.live.com:443	0			excel:5...	
1...	200	HTTPS	roaming.officeapps....	/rs/RoamingSoapService.svc	712	private	text/xml; c...	excel:5...	
1...	200	HTTP	Tunnel to	nexus.officeapps.live.com:443	0			powerp...	
1...	201	HTTPS	nexus.officeapps.li...	/nexus/upload/%7b9BD66F06-5AE5-4A...	0	no-cac...		powerp...	
1...	200	HTTP	Tunnel to	clients4.google.com:443	0			chrome...	
1...	304	HTTPS	clients4.google.com	/chrome-variations/seed?osname=win	0			chrome...	
1...	302	HTTPS	docs.google.com	/offline/cacheupdate?al=1&oid=u523d...	248	no-cac...	text/html; c...	chrome...	
1...	200	HTTP	Tunnel to	logins.daum.net:443	0			chrome...	
1...	200	HTTPS	logins.daum.net	/accounts/auth.gif?dummy=146578451...	807	no-cac...		chrome...	
1...	200	HTTPS	docs.google.com	/offline/offline/manifest	725	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	stats-public.gramm...	/?json={%22c%22:{%22grammarly.ui...	0		application/...	chrome...	
1...	200	HTTP	Tunnel to	drive.google.com:443	0			chrome...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	200	HTTP	Tunnel to	docs.google.com:443	0			chrome...	
1...	302	HTTPS	docs.google.com	/spreadsheets/offline/cacheupdate?oid...	321	no-cac...	text/html; c...	chrome...	
1...	302	HTTPS	docs.google.com	/document/offline/cacheupdate?oid=u...	296	no-cac...	text/html; c...	chrome...	
1...	302	HTTPS	docs.google.com	/document/offline/cacheupdate?oid=u...	283	no-cac...	text/html; c...	chrome...	
1...	302	HTTPS	docs.google.com	/drawings/offline/cacheupdate?oid=u5...	317	no-cac...	text/html; c...	chrome...	
1...	302	HTTPS	docs.google.com	/presentation/offline/cacheupdate?oid...	321	no-cac...	text/html; c...	chrome...	
1...	302	HTTPS	drive.google.com	/docdist/offline/cacheupdater?oid=u523...	277	no-cac...	text/html; c...	chrome...	
1...	200	HTTPS	docs.google.com	/document/offline/manifest?oid=u523d...	12,179	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	docs.google.com	/document/offline/manifest?oid=u523d...	12,251	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	docs.google.com	/drawings/offline/manifest?oid=u523d2...	8,052	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	docs.google.com	/presentation/offline/manifest?oid=u52...	12,101	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	docs.google.com	/spreadsheets/offline/manifest?oid=u5...	19,050	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	drive.google.com	/docdist/offline/cacheupdater?oid=u523...	290	no-cac...	text/html; c...	chrome...	
1...	200	HTTP	Tunnel to	felog.grammarly.io:443	0			chrome...	
1...	200	HTTP	Tunnel to	ssl.gstatic.com:443	0			chrome...	
1...	302	HTTPS	drive.google.com	/drive/offline/cacheupdate?authuser=0	232	private...	text/html; c...	chrome...	
1...	200	HTTPS	docs.google.com	/offline/common/manifest?oid=u523d2...	837	no-cac...	text/cache-...	chrome...	
1...	200	HTTPS	drive.google.com	/drive/offline/manifest?oid=u523d2b22...	13,291	no-cac...	text/cache-...	chrome...	
1...	302	HTTPS	docs.google.com	/offline/cacheupdate?al=1&oid=u523d...	248	no-cac...	text/html; c...	chrome...	
1...	200	HTTPS	docs.google.com	/offline/offline/manifest	725	no-cac...	text/cache-...	chrome...	

각 세션을 클릭하게 되면 우측 Detail list에서 상세 정보를 볼 수 있다.

Session List를 보게 되면 각 세션별로 아이콘이 표시되어 있어 어떤 유형의 세션인지 확인이 가능하다. 자주쓰는 세션 유형아이콘을 분류해 보면 아래 그림과 같다.



NELpos

당신의 친구가 해커라면?

CATEGORY

**Request BreakPoint(Intercept)****Response BreakPoint (Intercept)****Response(Https)****Text File****JS File****json File****Session Error**

예를 들어 파라미터 변조를 위해 Request에 breakpoint가 건 경우 해당 세션 아이콘은 세번째 이미지:(Request BreakPoint)로 표시되어 있다.

또한 피들러의 세션 리스트 하단 바를 활용하면 조금더 피들러를 효율적으로 사용 가능하다.

	59	200	HTTPS	www.google.co.kr	/complete/search?client=chrome-omni&gs_r
	60	200	HTTP	Tunnel to	www.google.co.kr:443
	61	200	HTTPS	www.google.co.kr	/complete/search?client=chrome-omni&gs_r
	62	200	HTTP	Tunnel to	www.google.co.kr:443
	63	200	HTTP	Tunnel to	www.google.co.kr:443

[QuickExec] ALT+Q > type HELP to learn more

All Processes
1 / 300
http://file.uf.daum.net/autosave_list?t

하단바의 구체적인 기능을 살펴보면 아래와 같다.



1) Capturing

- 클릭으로 캡처 활성화/비활성화 가능

2) Automatic BreakPoint

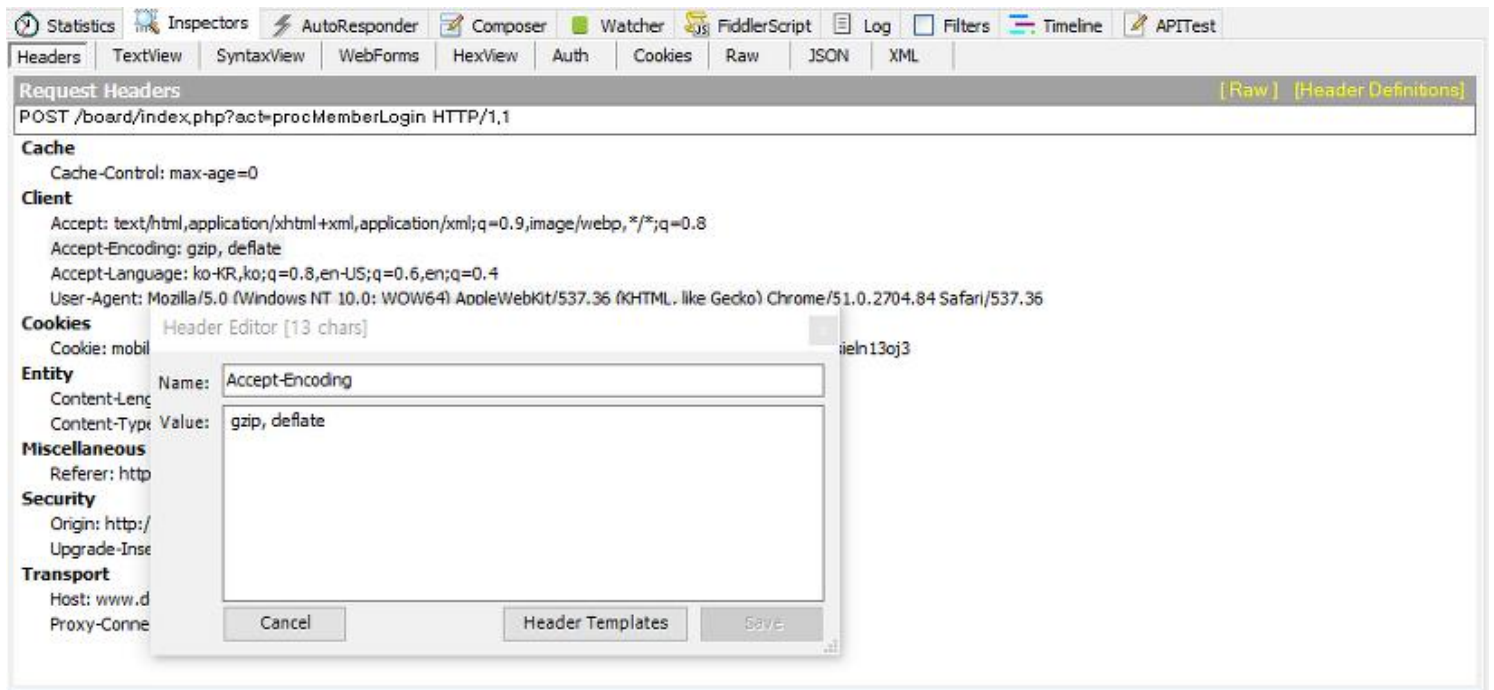
- 한번 클릭 → Before Request(Request Intercept)
- 두번 클릭 → After Responses(Response Intercept)

3-4 Detail list

Detail List에서는 웹 모의해킹 진단시 사용되는 기능 위주로 작성하였다.

3-4-1. Inspectors

- 1) Headers : 헤더 정보를 표시한다. 우측 클릭을 통해 edit Header 선택하면 헤더 value 수정이 가능하다.



- 2) TextView/SyntaxView : 텍스트형태와 Syntax형태로 보여준다.

- 3) HexView : 16진수 형태로 보여준다. 덮어쓰기가 가능해 Hex 수정이 가능하다. 단 burp Suite에 있는 byte 추가 기능은 없으므로 Raw 메뉴에서 텍스트를 추가한 다음 HexView에서 해당 텍스트를 수정해주는 형태로 사용이 가능하다.



NELpos

당신의 친구가 해커라면?

CATEGORY

00000105	87 69 6E 64 6F 77 73 20 4E 84 20 31 30 2E 30 3E 20 87 4F 87 36 34 29 20 41 70 70 6C 68	Windows NT 10.0; WOW64) Apple
00000122	57 65 62 4B 69 74 2F 35 33 37 2E 33 36 20 28 4B 48 54 4D 4C 2C 20 6C 69 6B 65 20 47 65	WebKit/537.36 (KHTML, like Ge
0000013F	63 68 6F 29 20 43 68 72 6F 6D 65 2F 35 31 2E 30 2E 32 37 30 34 2E 38 34 20 53 61 66 61	cko) Chrome/51.0.2704.84 Safa
0000015C	72 69 2F 35 33 37 2E 33 36 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C	ri/537.36..Content-Type: appl
00000179	69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63 60 64 65 64	ication/x-www-form-urlencoded
00000196	0D 0A 41 63 63 65 70 74 3A 20 74 65 78 74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74 69	..Accept: text/html,application
000001B3	6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 61 70 61 6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B	on/xhtml+xml,application/xml;
000001D0	71 3D 30 2E 39 2C 69 6D 61 67 65 2F 77 65 62 70 2C 2A 2F 2A 3B 71 3D 30 2E 38 0D 0A 52	q=0.9,image/webp,*/*;q=0.8..R
000001ED	65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 77 77 77 2E 64 6F 74 67 61 62 69 2E 6F 72	eferer: http://www.dotgabi.or
0000020A	67 2F 62 6F 61 72 64 2F 69 6E 64 65 78 2E 70 68 70 0D 0A 41 63 63 65 70 74 2D 45 6E 63	g/board/index.php..Accept-Enc
00000227	6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 41 63 63 65 70 74 2D	oding: gzip, deflate..Accept-
00000244	4C 61 6E 67 75 61 67 65 3A 20 6B 6F 2D 4B 52 2C 6B 6F 3B 71 3D 30 2E 38 2C 65 6E 2D 55	Language: ko-KR,ko;q=0.8,en-U
00000261	53 38 71 3D 30 2E 36 2C 65 6E 3B 71 3D 30 2E 34 0D 0A 43 6F 68 69 65 3A 20 6D 6F 62	S;q=0.6,en;q=0.4..Cookie: mob
0000027E	69 6C 65 3D 66 61 6C 73 65 3B 20 75 73 65 72 2D 61 67 65 6E 74 3D 31 64 61 64 32 33 33	ile=false; user-agent=ldad233
0000029B	31 64 30 61 33 61 64 31 38 36 37 31 30 63 65 64 33 34 35 38 36 66 66 35 30 3B 20 50 48	id0a3ad186710ced34586ff50; PH
000002B8	50 53 45 53 53 49 44 3D 74 68 63 6A 6A 66 72 37 30 68 33 63 6C 66 61 75 73 69 65 6C 6E	PSID=thcjfr70h3clfausieln
000002D5	31 33 6F 6A 33 0D 0A 0A 65 72 72 6F 72 5F 72 65 74 75 72 6E 5F 75 72 6C 3D 25 32 46	13oj3....error_return_url=%2F
000002F2	62 6F 61 72 64 25 32 46 69 6E 64 65 78 2E 70 68 70 26 6D 69 64 3D 48 6F 6D 65 26 76 69	board%2Findex.php&mid=Home&vi
0000030F	64 3D 26 72 75 6C 65 73 65 74 3D 25 34 30 6C 6F 67 69 6E 26 61 63 74 3D 70 72 6F 63 4D	d=ruleset=%40login&act=procM
0000032C	65 6D 62 65 72 4C 6F 67 69 6E 26 73 75 63 63 65 73 73 5F 72 65 74 75 72 6E 5F 75 72 6C	emberLogin&success_return_url
00000349	3D 25 32 46 62 6F 61 72 64 25 32 46 69 6E 64 65 78 2E 70 68 70 26 78 65 5F 76 61 6C 69	=%2Fboard%2Findex.php&xe_vali
00000366	64 61 74 6F 72 5F 69 64 3D 77 69 64 67 65 74 73 25 32 46 6C 6F 67 69 6E 5F 69 6E 66 6F	dator_id=widgets%2Flogin_info
00000383	25 32 46 73 68 69 6E 73 25 32 46 64 65 66 61 75 6C 74 25 32 46 6C 6F 67 69 6E 5F 66 6F	%2Fskins%2Fdefault%2Flogin_fo
000003A0	72 6D 25 32 46 31 26 75 73 65 72 5F 69 64 3D 74 65 73 74 26 70 61 73 73 77 6F 72 64 3D	rm%2Fuser_id=test&password=
000003BD	31 32 33 31 64 32 33	1231k23

227 [0xe3] of body

Overwrite

4) Raw : Request Data 전체 확인 및 수정이 가능하다. 여기서 Cookie 및 파라미터 수정이 가능하다.

Statistics Inspectors AutoResponder Composer Watcher FiddlerScript Log Filters Timeline APITest

Headers Text View Syntax View WebForms Hex View Auth Cookies Raw JSON XML

```

POST http://www.dotgabi.org/board/index.php?act=procMemberLogin HTTP/1.1
Host: www.dotgabi.org
Proxy-Connection: keep-alive
Content-Length: 230
Cache-Control: max-age=0
Origin: http://www.dotgabi.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.dotgabi.org/board/index.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: mobile=false; user-agent=ldad233id0a3ad186710ced34586ff50; PHPSESSID=thcjfr70h3clfausieln13oj3

error_return_url=%2Fboard%2Findex.php&mid=Home&vid=&ruleset=%40login&act=procMemberLogin&success_return_url=%2Fboard%2Findex.php&xe_vali
  
```

Find... (press Ctrl+Enter to highlight all) View in Notepad

5) JSON/XML : JSON과 XML 데이터 정보 확인이 가능하다.

3-4-2. Composer

Composer 기능을 이용하면 원하는 세션을 드래그하여 Request를 가져온 후 수정이 가능하다. 수정 후에 Execute 버튼을 누르면 세션이 전송된다.

NELpos

당신의 친구가 해커라면?

CATEGORY

The screenshot displays the Fiddler web proxy interface. On the left, a list of intercepted HTTP requests is shown, including various GET and POST requests to domains like 'api.devicem...' and 'state public.g...'. A red arrow points to a specific request in the list, labeled '채널 선택 후 드래그' (After channel selection, drag). The right pane shows the details of the selected request, including the request body which contains a large block of Base64-encoded data. The interface also shows the 'Host' field as 'file://daum.net' and the 'Content-Type' as 'application/javascript'.

3-4-3. Watcher

Watcher는 수집된 URL 정보를 바탕으로 해당 페이지의 위험도를 표시해준다. 관련 위험에 대한 Reference 사이트도 URL로 제공하고 있고 위험도 기준으로 필터해서 확인도 가능하다.



NELpos

당신의 친구가 해커라면?

CATEGORY

Severity	Session ID	Type	URL
High	218	Insecure SSLv2 was allowed	tpc.google syndication.com
High	220	Insecure SSLv2 was allowed	cm.g.doubleclick.net
High	228	Insecure SSLv2 was allowed	accounts.google.com
High	232	Insecure SSLv2 was allowed	fonts.gstatic.com
High	235	Information leak in HTTP referer	https://s0.2mdn.net/879366/html_inpage_rendering_lib_200_126.js
High	233	Insecure SSLv2 was allowed	ssl.gstatic.com
High	235	Insecure SSLv2 was allowed	s0.2mdn.net
High	240	User controllable cookie (potential cookie poisoning attack)	https://syndication.twitter.com/widgets/timelines/557822563553132545?callback=__twtr.callbacks.tl_i0
High	241	Information leak in HTTP referer	https://pagead2.google syndication.com/pagead/js/ldar.js
High	242	Information leak in HTTP referer	https://s0.2mdn.net/ads/rtchmedia/studio/pv2/37546815/20150806110853152/index.html?e=69&render
High	256	Information leak in HTTP referer	https://js.dntry.com/antenna2.js?0_4201_130207489_69795830
High	256	Insecure SSLv2 was allowed	js.dntry.com
High	257	Insecure SSLv2 was allowed	fonts.googleapis.com
High	263	Information leak in HTTP referer	https://log.dntry.com/redir/178951/0/4201/130207489/69795830/349876/0/0/0/1.ver?at=i&d=imp&ec
High	264	Information leak in HTTP referer	https://log.dntry.com/384551/0/4201/130207489/69795830/349876/0/0/0/1.ver?at=ol&d=Load&ddl=C
High	266	User controllable HTML element attribute (potential XSS)	https://tailstar.net/index.php?mid=main&act=dispMemberLoginForm
High	268	Information leak in HTTP referer	https://log.dntry.com/163845/0/4201/130207489/69795830/349876/0/0/0/1.ver?at=p&d=Post&ta=na
High	291	Insecure SSLv2 was allowed	ajax.googleapis.com
High	303	User controllable HTML element attribute (potential XSS)	https://apis.google.com/u/0/se/0/_/+1/fastbutton?useapi=1&size=small&hl=ko&origin=https%3A%2F%2F
High	314	Information leak in HTTP referer	https://www.google.com/ads/measurements/3?chid=11h37-c8-BL-DC-ENR0M4V6-P4lke0C-0uY6a

Export Findings Export Method: ☐ AutoScroll

Reference: <http://websecuritytool.codeplex.com/wikipage?title=Checks#information-disclosure-in-http-referer>

The HTTP Header in the following request may have leaked a potentially sensitive parameter to another domain:

https://log.dntry.com/redir/178951/0/4201/130207489/69795830/349876/0/0/0/1.ver?
at=i&d=imp&echo=&sz=na&jf=1&jt=3&jsv=4.5.0&oc=ADO&nc=0&num=0&sr=1920x1080x24&tz=-9&url=http%3A%2F%2Ftailstar.net%2F

The potentially sensitive parameter(s) identified were:

1) A(n) 'credit card number' seems to have been found with the value:

ca-pub-4095083010178985

Casaba Watcher Web Security Tool v1.5.8, Copyright © 2010 [Casaba Security, LLC](http://casaba-security.com). All rights reserved.

3-4-4. log

프로그램 로그 확인이 가능하다.

3-4-5. filter

특정 URL을 필터 걸어 해당 URL에 대한 세션만 확인이 가능하게 할 수 있다.

아래 그림은 www.dotgabi.org url을 필터를 걸었더니 해당 url과 관련된 세션만 캡처 되는것을 알 수 있다.

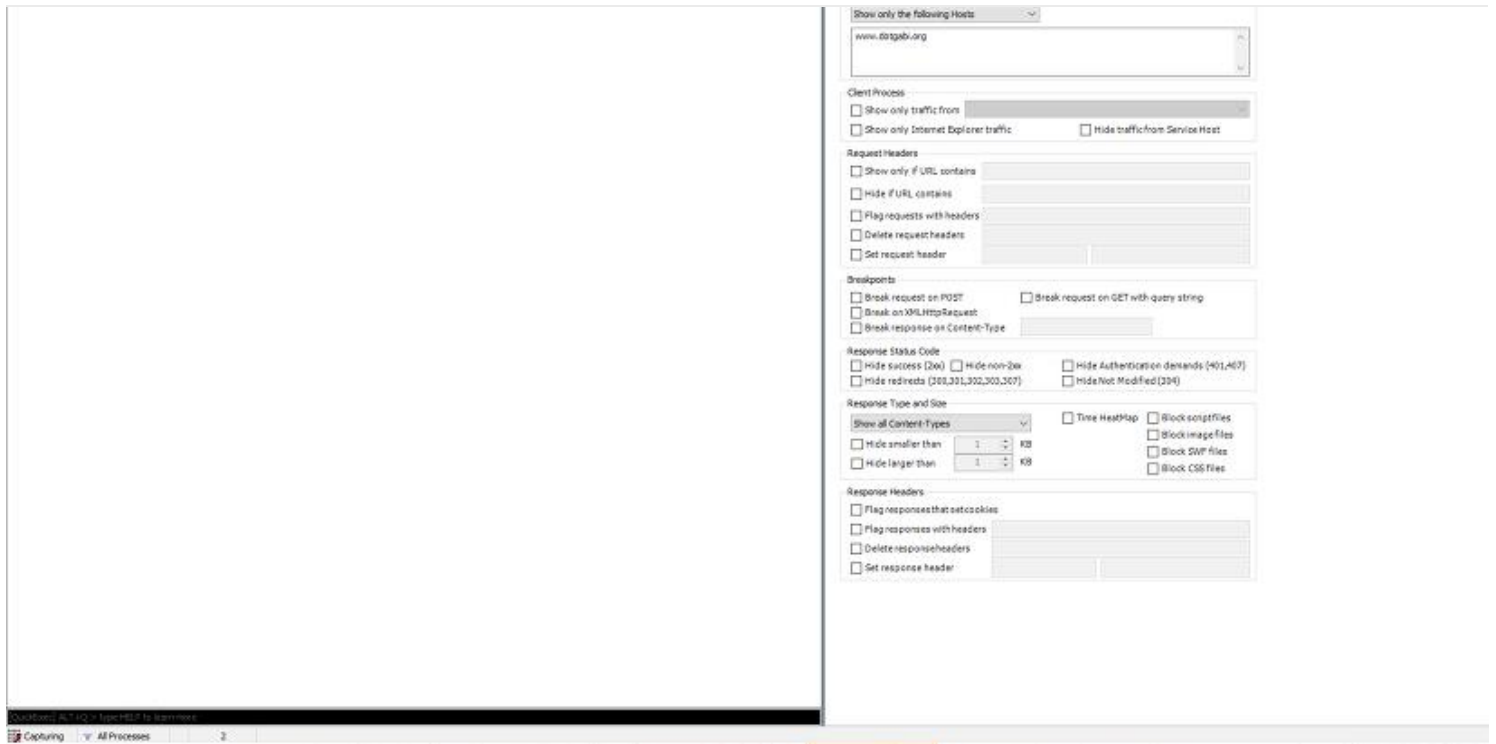
옵션이 인터넷/인트라넷, show/hide/flag등 다양한 기능이 포함되어 있다. Request/Response Header 내용에 따라서도 필터링이 가능하다.



NELpos

당신의 친구가 해커라면?

CATEGORY



4. Fiddler 웹 모의해킹 실전 활용

이제 Fiddler를 이용하여 웹 모의해킹 중에 간단한 파라미터 변조를 진행해 보겠다. 먼저 Fiddler를 실행시킨 후에 하단의 Quick 메뉴를 이용하여 Capturing과 Request Breakpoint를 클릭하여 활성화 시킨다.

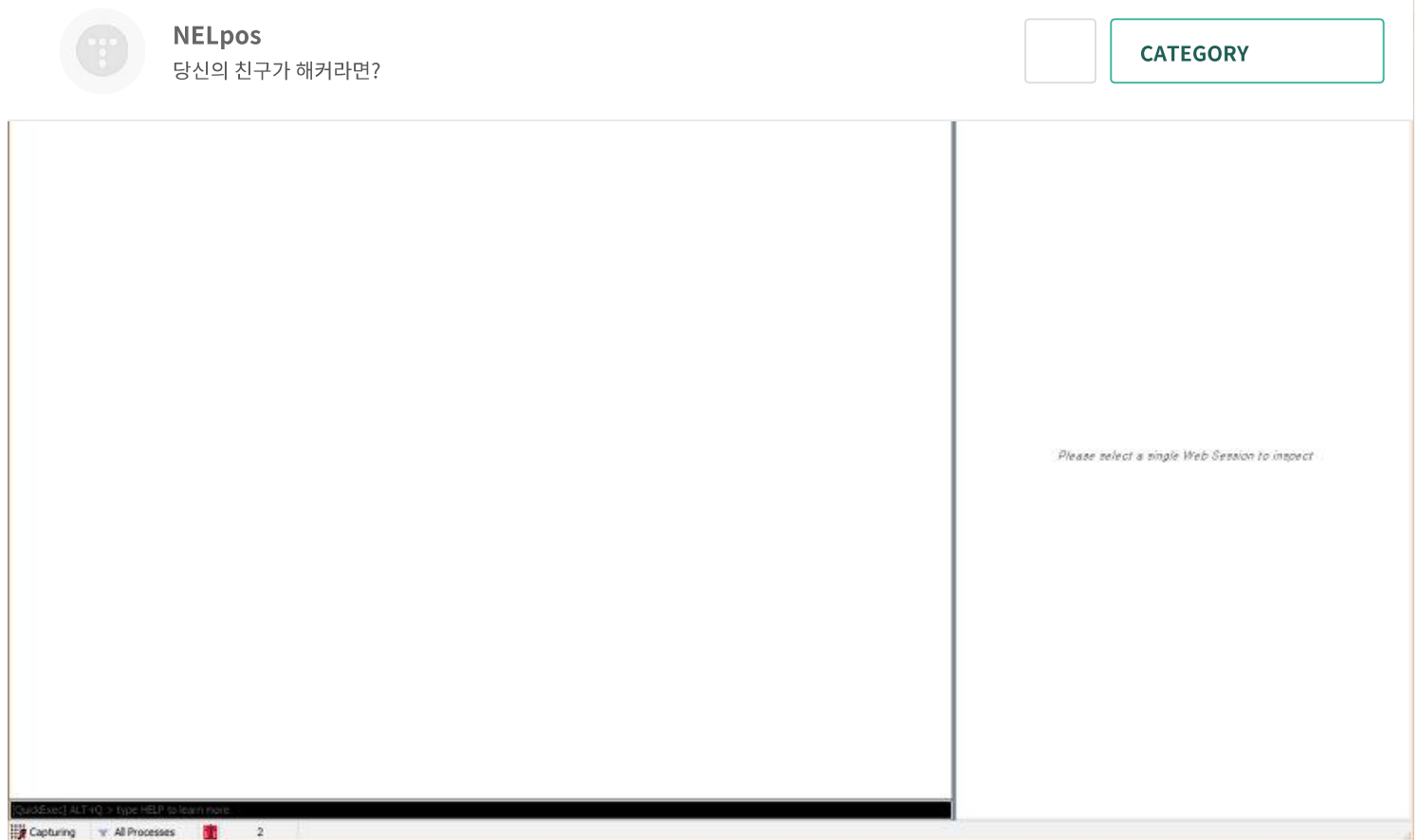
**NELpos**

당신의 친구가 해커라면?

CATEGORY



IE를 실행하였더니 초기 홈페이지를 www.naver.com 으로 요청이 전달되었다. 별도의 탭을 열어 로그인을 하기 위해 사이트 (www.dotgabi.org)에 접속을 시도했다. 현재 2개의 url이 요청된 상태이므로 fiddler에서 2개의 세션이 보이는 것을 알 수 있다. 좌측 세션 아이콘을 보면 Request Breakpoint가 걸려있는 2개의 세션을 확인할 수 있다.



이제 www.dotgabi.org 에 해당하는 세션만 클릭하고 Go를 누른다. Go를 누르게 되면 선택된 세션 아이콘이 변경되면서 Response(<>) 아이콘으로 변경된다.

(www.dotgabi.org 세션만 실행이 가능하다. 다른 세션은 현재도 breakpoint 걸려 있는 상태이다)



NELpos

당신의 친구가 해커라면?

CATEGORY

The screenshot shows the Fiddler web proxy interface. On the left, a list of intercepted HTTP requests is displayed, including details like status code (200), method (HTTP), and the tunnel endpoint (e.g., Tunnel to stats-public.grammarly.io:443). The main pane on the right shows the raw data of the selected request in hexadecimal and ASCII format. The bottom status bar indicates the current session is capturing traffic from http://www.dotgabi.org/.

이제 응답을 받은 후에 다음 /board/index.php를 요청하게 되는데 이때 다시 한번 breakpoint가 걸린다. 이걸 다시 Go로 연결해주면 www.dotgabi.org에서 css 랑 js 파일을 내려받는 것을 확인할 수 있다.



NELpos

당신의 친구가 해커라면?

CATEGORY

The screenshot shows the Fiddler web proxy interface. The left pane displays a list of captured HTTP requests. A red box highlights a series of requests to `www.dotgabi.org`, specifically those related to the `/board/index.php` endpoint. The right pane shows the raw data of the selected request, which is a JSON response. The status bar at the bottom indicates the current request is `http://www.dotgabi.org/board/index.php`.

세션이 너무 많은 경우 현재 내가 진행하려는 세션을 찾기 힘든 경우 FIND 기능을 이용해서 세션을 노란게 표시하는 것도 좋은 방법이다. 세션은 다중으로 선택해서 한번에 Go를 누르게 되면 선택한 세션은 모두 진행된다.

홈페이지에서 내려받는 js 파일은 Response breakpoint를 통해 다운받기 전에 해당 세션을 클릭하여 SyntaxView를 통하여 수정이 가능하다.



NELpos

당신의 친구가 해커라면?

CATEGORY

The screenshot shows the Fiddler web proxy interface. On the left, a list of captured requests is visible, with several highlighted in yellow. The main pane displays the details of a selected request, including the 'WebForm' tab which shows the HTML structure of the response. A red box highlights a specific JavaScript function in the response code, with a red text overlay that reads: 'Js 코드같은경우 Intercept 결렸을 때 수정 가능' (In the case of JavaScript code, it can be modified when the Intercept is triggered).

이제 로그인을 시도하여 ID/PW 파라미터를 변경을 시도해볼 것이다. 웹 Form에 ID/PW를 입력하고 로그인을 하면 Fiddler에 세션이 Request breakpoint 되면서 우측 Detail View의 Inspectors(WebForm/Raw)에서 파라미터 변경이 가능하다. 여기서 파라미터를 변경한 후 두가지를 선택할 수 있다.

Break on response : 해당 Request에 대한 Response break 걸기. 수정된 파라미터에 요청에 대한 Response Intercept

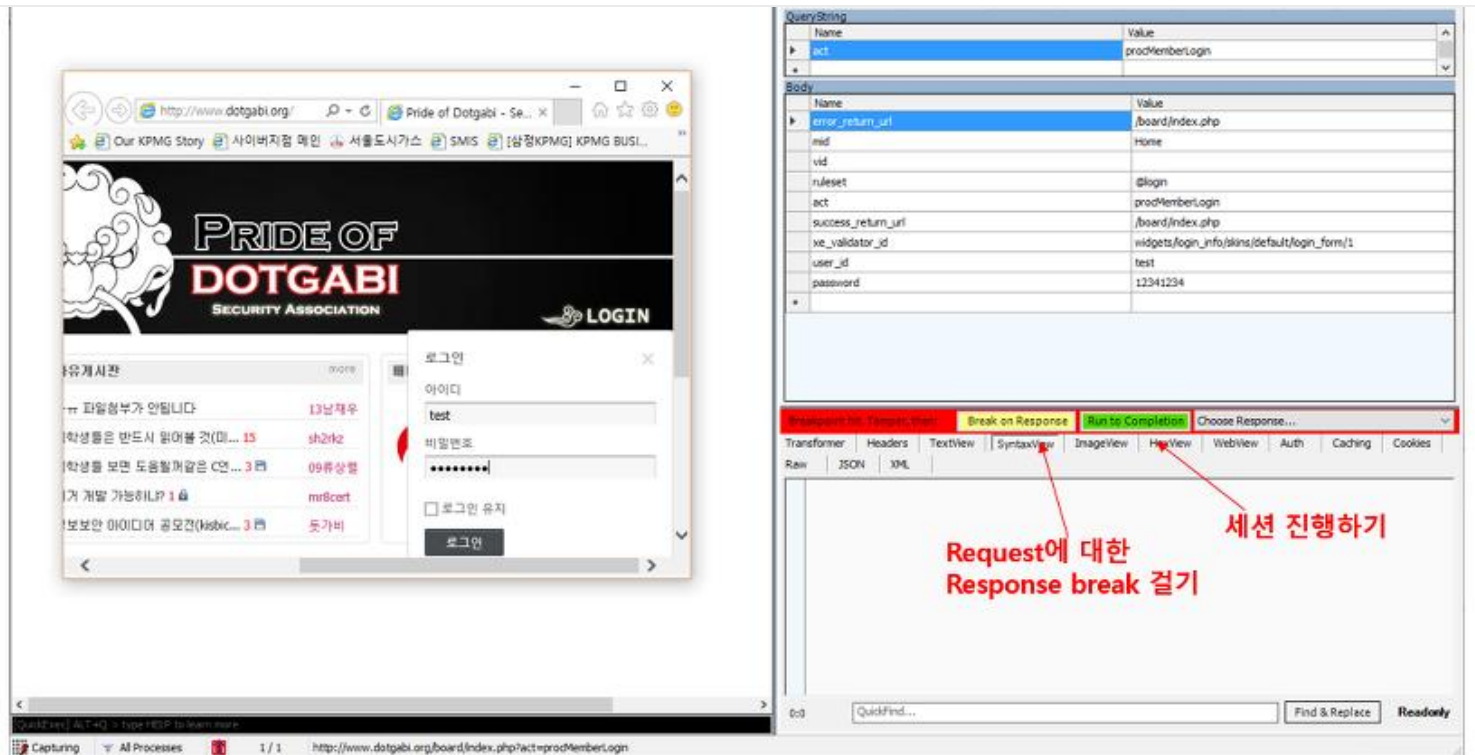
Run to Completion : 해당 세션 진행하기, Response 까지 완료된 상태



NELpos

당신의 친구가 해커라면?

CATEGORY



이렇게 Fiddler를 활용하여 웹 모의해킹의 기본인 파라미터 변경에 대해서 실습해 보았다.

5. Burp Suite와의 비교?

Burp Suite와 비교했을때 Fiddler는 다음과 같다고 생각한다.

1) IE 개발자 도구 기능 + Request/Response Intercept 기능을 함께 수행할 수 있다.

- 보통 js 코드를 수정하거나 css 를 수정하는 테스트를 진행할 때 개발자 도구를 수정한다음에 Burp Suite를 사용하는데 Fiddler를 이용하게 되면 실제 진단시 js코드를 수정하면서 파라미터 변조가 가능하기 때문에 보안 프로그램 우회 진단 수행이시 유용하게 사용이 가능하다.

2) 인코딩/디코딩을 활용할때 Burp Decoder보다 TextWizard에서 제공해주는 기능이 훨씬 많고 편하다.

- 한글 인코딩/디코딩도 지원
- C#, JS 개발 환경까지 고려한 인코딩/디코딩 기능
- 단, hackbar 만큼의 모의진단시 효율적인 코드 변환 기능을 제공하는 것은 아님.

3) Burp Suite에서는 메일 불필요한 세션을 넘겨서 내가 원하는 세션을 찾아야 했는데 Fiddler는 필요한 세션만 선택해서 모의해킹 진행이 가능하다.

- Burp Suite를 사용할때는 불필요한 세션이 걸리는 경우 ctrl+F를 통해 세션을 진행해야 되는 불편함이 있는데 피들러는 필요한 세션을 찾아서 해당 세션만 진행하면 된다.
- 또한 Burp Suite에서는 HTTP History를 살펴보고 Request/Response를 살펴봤었는데 Fiddler의 Find 기능(Ctrl+F)을 이용하여 효



NELpos

당신의 친구가 해커라면?



CATEGORY

- Burp Suite는 Extension을 이용하여 확장 플러그인 다운로드 및 등록이 가능하다. (Java, Jython, JRuby)
- Fiddler는 Session 필터링에 대한 Rule셋을 스크립트를 통해 개발이 가능하다.

6. 상세 Reference 참고

필자는 하나하나 메뉴를 찾아가면서 해당 포스트를 썼다.
Fiddler 사용법에 대해서 공식 Reference를 제공하고 있으니 참고하길 바란다.

<http://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/ConfigureWinHTTPApp>



'To be Red Team > Penetrate Tool Review' 카테고리의 다른 글

Fiddler를 활용한 웹 모의해킹 (0)

댓글 0

여러분의 소중한 댓글을 입력해주세요

이름

비밀번호

비밀글

입력

1 2 3 4

최근에 올랐온 글

- 파이썬에서의 한글 인코딩..
- Fiddler를 활용한 웹 모의..
- 파이썬을 통해 나라장터 파..

최근에 달린 댓글

- 조금 다른 접근이지만, 제 나..
- 혹시 풀 소스가 있으시면 공유..
- 미니어스님, 대박이네요

Total

27,150

Today	3
Yesterday	99



NELpos

당신의 친구가 해커라면?



CATEGORY

Blog is powered by [Tistory](#) / Designed by [Tistory](#)