# 개요

Burp Suite 는 웹 애플리케이션 분석에 사용할 수 있는 도구 입니다. HTTP Request 가로채기 및 수정, 로그 인 창에 Brute Force (무차별 대입) 공격 등 다양한 업무를 수행할 수 있습니다. 본 문서에서는 Burp Suite 의 주요기능에 대해 설명합니다.

# 다운로드

http://portswigger.net/burp/download.html

Burp Suite는 무료 버전과 유료 버전이 있으며, 무료 버전에서 지원하는 기능은 일부 Intruder 기능 및 Scanner 기능, 대상 분석기, 작업 스케줄러 등이 있습니다.

# 기능

### 1) Proxy

Proxy 기능은 Request를 가로채고 수정하는데 사용합니다. 해당 기능을 사용하기 위해 웹 트래픽이 Proxy 를 향하도록 구성해야 하며, 설정 기본 값은 127.0.0.1:8080 입니다.

000	고급	
[]] ···································	····································	
	프록시 설정	
연결	○ 프록시 사용 안 함	
Fire	○ 프록시 설정 자동 감지	
	○ 시스템 프록시 설정 사용	
캐수	<ul> <li>프록시 수동 설정:</li> </ul>	
	HTTP 프록시: 127.0.0.1 포트: 8080 🛟	
	□ 모든 프로토콜에 위의 프록시 설정 사용	
	SSL 프록시: 포트: 0 🗘	
	FTP 프록시: 포트: 0 🗘	
오프	SOCKS 호스트: 포트: 0 🛟	
	프록시 사용 안 함:	
<u>오</u> 프	localhost, 127.0.0.1	
	예: .mozilla.org, .net.nz, 192.168.1.0/24	
	○ 프록시 자동 설정 주소 (URL):	
	새로 고침	
?	취소         확인	

br@infeed3r

브라우저에서 설정이 끝나면, Burp Suite 를 열고 [Proxy]에서 [Intercept is on]으로 되어있는지 확인합니다.

[Alerts] 탭으로 가면 8080 포트로 proxy 기능이 작동하고 있는지 확인할 수 있으며, [Proxy] 아래 [Options] 탭에서 기본 설정에 대한 구성을 변경할 수 있습니다.

?	Proxy Liste	eners				
٢	Burp Proxy us	ses listeners t	o receive incoming H	TTP request	s from your brows	er. You will need to configure your b
	Add	Running	Interface	Invisible	Redirect	Certificate
		V	127.0.0.1:8080			Per-host
	Edit					
	000			Edit	proxy listener	
	Binding	Request han	dling Certificate			
?	P The Bind Bind	se settings co l to port: l to address:	<ul> <li>ontrol how Burp binds</li> <li>8080</li> <li>Loopback only</li> <li>All interfaces</li> <li>Specific address:</li> </ul>	the proxy li	stener.	

해당 탭에서 Edit 를 클릭해 수신하는 Proxy 포트를 수정할 수 있으며, Add 를 클릭해 새 Proxy Listener 를 추 가로 구성할 수 있습니다. Edit - [Binding] 탭 에서 Bind to address - Loopback only 대신 다른 옵션을 사 용해 네트워크 상의 또 다른 시스템의 Proxy 로 사용할 수 있습니다. 즉, 동일한 네트워크 상의 모든 호스트는 Burp Proxy 기능을 사용할 수 있으며, Proxy 를 통해 트래픽을 릴레이할 수 있습니다.

?	Proxy Lister	ners					
٢	Burp Proxy use	es listeners t	o receive incoming H	TTP requests	from your browser. Y	ou will need to configure your b	rows
	Add	Running	Interface	Invisible	Redirect	Certificate	
			127.0.0.1:8080			Per-host	
	Edit	000			Edit proxy	listener	
	Remove	Binding	Request handling	Certificate			
6	Intercept Cl Use these setti Intercept ro Add Edit Remove	P Th O	ese settings control t Use a self-signed ce Generate CA-signed Generate a CA-signed Use a custom certifi File: Password:	the server SS ertificate d per-host ce ed certificate cate (PKCS12	certificate that is pre rtificates with a specific hostna ):	esented to SSL clients.	

Burp 는 SSL 보호 웹 사이트에 인증서를 제공할 수 있는 옵션도 있습니다. 기본적으로 Burp 는 자체 서명된 CA 인증서를 생성합니다. 현재 선택된 옵션 즉, Generate CA-signed per-host certificates는 클라이언트에서 연결하려는 특정 호스트에 대해 Burp의 CA인증서로 서명한 인증서를 생성합니다. 웹 애플리케이션 분석 시 우려 할 유일한 일은 SSL(TLS)로 보호된 웹 사이트에 연결할 때 인증서 오류의 경고 수를 줄이는 것입니다.

?	Proxy Lister	ners				
٢	Burp Proxy use	es listeners to	o receive incoming H	FTP requests	from your browser. You	will need to configure your bro
	Add	Running	Interface	Invisible	Redirect	Certificate
			127.0.0.1:8080			Per-host
	Edit	000			Edit proxy list	ener
	Remove	Binding	Request handling	Certificate		
? ()	Intercept Cl Use these setti I Intercept re Add	P Th Re- Re- Inv	ese settings control v direct to host: direct to port: Force use of SSL risible proxy support Support invisible pro	whether Burp allows non-p oxying (enab	redirects requests receiv	red by this listener. nnect directly to the listener.

Support invisible proxying (enable only if needed) 옵션은 Proxy 를 사용하고 있는지 모르는 클라이언 트에서 사용합니다. 이는 Proxy 설정이 브라우저의 옵션이 아닌 다른 위치 (예: hosts) 에 있는 경우를 말합니 다. 이 경우의 Request 는 브라우저에서 설정한 경우의 Request 와 약간 다르기 때문에 해당 옵션을 사용함으 로써 Burp 에 알려주는 역활을 . Redirect to host, Redirect to port 는 옵션 이름과 같이 호스트와 포트를 설정 값으로 Redirect 합니다.

?	Intercept C	lient Requ	iests				
٢	Use these set	tings to cont	rol which req	uests are stalled for	viewing and editing in th	e Intercept tab.	
	🗹 Intercept i	requests bas	ed on the foll	owing rules:		N-	
	Add	Enabled	Operator	Match type	Relationship	Condition	1
		•		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^i	1
	Edit		Or	Request	Contains parameters		
			Or	HTTP method	Does not match	(get post)	
	Remove		And	URL	ls in target scope		•
	Up						
	Down						
	$\square$						-
0	Intercent S	erver Resi	nonses				
6	intercept 5	erver kes	polises				
14	Use these set	tings to cont	rol which res	ponses are stalled fo	or viewing and editing in t	the Intercept tab.	
0							
	🔲 Intercept i	responses ba	ased on the fo	llowing rules:			
	Add	Enabled	Operator	Match type	Relationship	Condition	
		•		Content type	Matches	text	1
	Edit		Or	Request	Was modified		
			Or	Request	Was intercepted		
	Remove		And	Response code	Does not match	^304\$	
	$\sum$		And	URL	ls in target scope		
	Up						1.1
	<u> </u>						
	Down						
	Automatic	ally undate (	Content-Leng	th header when the	response is edited		
1	- Automatic	any update (	soment Leng	the fourth of the second s	capanae la cuiteu		

"Intercept Client Requests", "Intercept Server Responses" 옵션 항목에서 지정하는 규칙에 따라 Request 와 Response 를 가로챌 수 있습니다. 트래픽이 많을 경우 우리가 원하는 일부 Request 만 가로채도 록 설정할 수 있습니다.

?	Response M	<b>Aodificatio</b>	n			7
٢	These settings	s are used to	perform automatic mod	ification of responses.		×.
	🔲 Unhide hid	lden form fie	lds			
	🔲 Enable disa	abled form fi	elds			
	🔲 Remove in	put field leng	th limits			
	Remove Jav	vaScript form	validation			
	Remove all	lavaScript				
	□ Remove <	object> tags				
		TTPS links to	иттр			
		fl fu	ni i r 			
	Kemove se	cure nag fro	m cookies			
?	Match and These settings	Replace s are used to	automatically replace pa	rts of requests and responses pa	assing through the Proxy.	
	Add	Enabled	Туре	Match	Replace	
			Request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (co	1
	Edit		Request header	^If-Modified-Since.*\$		
			Request header	^If-None-Match.*\$		
	Remove		Request header	^Referer.*\$		
			Response header	^Set–Cookie.*\$		
	Up					
	Down					

"Response Modification", "Match and Replace" 옵션 항목에서 서버로부터 받은 Response 를 수 정할 수 있습니다. 숨겨진 폼 필드를 표시(Unhide hidden from fields)하거나, 모든 자바 스크립트를 제거 (Remove all JavaScript) 할 수 있습니다. 또한, 특정 패턴에 대해 사용자 지정 문자열로 있습니다. "Match and Replace" 옵션 항목 작성 시 정규 표현식(RegEx)을 지정할 수 있습니다. Burp는 특정 패턴을 찾아서 지 정 문자열로 대체하기 위해, 자동으로 Request 또는 Response 분석할 것입니다.

여기까지 Proxy 기능에 대한 설정을 완료했다면, Request 및 Response 를 가로챌 수 있습니다. Request 를 보낼 때나 Response 를 받을 때 마다 Burp 에 의해 가로채어지므로, 일일이 수작업으로 해당 패킷들을 Forward 시켜야 합니다. 따라서 패킷의 내용을 수정해야 할 때만 [Intercept is on] 옵션을 유지 하는 것이 좋습 니다.

### 2) Spider

Burp Spider 는 웹 애플리케이션의 지도를 만들 때 사용합니다. 전체 웹 애플리케이션에 대한 상세 분석을 하기 위해 웹 애플리케이션을 자동으로 크롤링해서, 링크 및 모든 로그인 폼을 알려줄 것입니다. 이렇게 찾은 링크들은 세부 검색을 위해 Scanner 로 보내지게 됩니다. Spider 기능을 간단히 사용하기 위해 브라우저에서 취약한 웹 애플리케이션의 주소로 이동하여 Burp 가 가로챈 Request 에서 마우스 오른쪽 버튼 클릭 후 "Send to Spider" 항목을 선택합니다.

Intercept History Options		
Request to http://testasp.vulnweb.com:80	[87.230.29.167]	
Forward Drop I	ntercept is on Action	
Raw Params Headers Hex		
GET / HTTP/1.1		
Host: testasp.vulnweb.com		
User-Agent: Mozilla/5.0 (Macin	Send to Spider	Gecko/20100101
Accept: text/html,application/	Do an active scan	q=0.8
Accept-Language: ko-kr,ko;q=0.	Send to Intruder	
Accept-Encoding: gzip, deflate	Send to Repeater #+R	
COOKIE: ASPSESSIONIDCCASESS⇒3. Correction: keer alive	Send to Sequencer	
connection. Keep-alive	Send to Comparer	
	Send to Decoder	

이렇게 하면 경고 창이 팝업 되면서 Scope(범위)에 대상을 추가할 것인지 물어보는데 [Yes] 를 선택합니다. 여 기에서 Scope(범위)는 테스트를 실행 하고자 하는 대상 영역을 정의 합니다.

http://testasp.vul	nweb.com	Host			Method	URL
<ul> <li>/</li> <li>Default.asp</li> <li>Cogin.asp</li> <li>Register.asp</li> <li>Search.asp</li> <li>Search.asp</li> <li>Templatize.a</li> <li>robots.txt</li> <li>showforum.</li> <li>showforum.</li> <li>showthread</li> <li>http://testaspnet.</li> <li>http://testphp.vul</li> </ul>	asp asp asp vulnweb.com nweb.com	http://t http://t http://t http://t http://t http://t http://t http://t http://t	estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo estasp.vulnwo	e e e e e e e e	GET GET POST GET GET GET GET GET GET	/ /Defa /Logi /Logi /Logi /Logi /Logi /Logi /Logi
	http://testphp.vulnweb.com/ Add to scope Spider this host Actively scan this host Passively scan this host		st Respon Params H HTTP/1.1	Head	ers He	x ]

[Target] 의 [Site map] 탭으로 이동하면, Target에 웹 애플리케이션 URL이 추가되어 있는 것을 볼 수 있습니다. 또한, http://google.com 같은 다른 대상까지 목록에 추가 된 것을 볼 수 있을 것입니다. Burp 는 Proxy 기능을 사용 하는 동안, 사용자가 탐색하는 웹 애플리케이션을 자동으로 Target 의 대상 목록에 추가합니다. 어떤 대상이든지 마우스 오른쪽 버튼을 클릭하고 "Add item to scope" 항목을 선택해 [Scope]에 추가할 수 있습니다.

, ranger set	ope					
Define the in configure sc	n-scope targets cope is to brows	for your curre se to your targe	ent work. This configuration affect et and use the context menus in t	ts the beha he site map	wior of tools throughou p to include or exclude	ut the suite. All field URL paths.
Include in sc	ope					
Add	Enabled	Protocol	Host / IP range	Port	File	
		НТТР	^testasp\.vulnweb\.com\$	^80\$		
Edit						
Bamaya						
Kemove						· · · · · · · · · · · · · · · · · · ·
Deaths LIDI						
Paste UKL						
Paste UKL	·					
Paste UKL						
Exclude from	n scope					
Exclude from	n scope	Protocol	Hort / IP range	Port	File	
Exclude from	n scope	Protocol	Host / IP range	Port	File	
Exclude from	n scope	Protocol Any	Host / IP range	Port	File	
Exclude from Add Edit	n scope	Protocol Any Any	Host / IP range	Port	File logout logoff	
Exclude from Add Edit	n scope	Protocol Any Any Any Any	Host / IP range	Port	File logout logoff exit signout	
Exclude from Add Edit Remove	n scope Enabled	Protocol Any Any Any Any HTTP	Host / IP range	Port ^80\$	File logout logoff exit signout	Ď
Exclude from Add Edit Remove	n scope Enabled Ø Ø Ø Ø Ø	Protocol Any Any Any Any HTTP HTTPS	Host / IP range ^12app\.naver\.com\$ ^accounts\.google\.com\$	Port ^80\$ ^443\$	File logout logoff exit signout	
Exclude from Add Edit Remove Paste URL	n scope Enabled Ø Ø Ø Ø Ø Ø Ø Ø	Protocol Any Any Any Any HTTP HTTPS HTTP	Host / IP range Al2app\.naver\.com\$ Aaccounts\.google\.com\$ Aadmin\.blog\.naver\.com\$	Port ^80\$ ^443\$ ^80\$	File logout logoff exit signout	

[Scope] 탭으로 이동하면 취약한 웹 애플리케이션의 URL이 추가되었음을 확인할 수 있습니다.

?	Crawler Settings
٢	These settings control the way the Spider crawls for basic web content.
	☑ Check robots.txt
	Ø Detect custom "not found" responses
	✓ Ignore links to non-text content
	Request the root of all directories
	Make a non-parameterised request to each dynamic page
	Maximum link depth:     5       Maximum parameterised requests per URL:     50
_	
2	Passive Spidering
3	Passive spidering monitors traffic through Burp Proxy to update the site map without making any new requests.
	✓ Passively spider as you browse
	Link depth to associate with Proxy requests: 0

이제 [Spider] 탭에 가서 [Option] 탭을 선택합니다. 해당 탭에서 Burp Spider 가 작동 방식에 대한 다양한 옵 션을 설정할 수 있습니다. 웹 사이트 관리자가 검색 엔진에 인덱싱 되지 않도록 robots.txt 설정한 경우 파일 존재 여부에 대한 확인을 요청할 수 있습니다. 다른 중요 옵션은 [Passively spider as you browse] 입니다. 기본적 으로 Burp Spider는 Passive 와 Active 모드 모두에서 실행할 수 있습니다. Active 모드의 경우 Burp의 Proxy 기능을 사용하여 웹 애플리케이션 분석하는 동안, 새로운 링크와 콘텐트에 대한 Scanning 을 유지할 것 인지 묻습니다. Passive 모드의 경우 묻지 않고 유지합니다.

?	Application Login		
٢	These settings control how the Spider submits	s login forms.	
	<ul> <li>Don't submit login forms</li> </ul>		
	<ul> <li>Prompt for guidance</li> </ul>		
	<ul> <li>Handle as ordinary forms</li> </ul>		
	Automatically submit these credentials:		
	Username:		
	Password:		
?	Spider Engine These settings control the engine used for ma	king HTTP requests when spidering.	
	Number of threads:	10	
	Number of retries on network failure:	3	
	Pause before retry (milliseconds):	2000	
	Throttle between requests (milliseconds):	500	
	Add random variations to throttle		
?	Request Headers These settings control the request headers us	ed in HTTP requests made by the Spider.	
	Add Accept: */*		
	Accept-Language: en	anible: MSIE 0.0: Windows NT 6.1: Win64: v64: Trideet (5.0)	
	Edit User-Agent: Mozilia/5.0 (comp	pauble; MSIE 9.0; WINDOWS NT 6.1; WIN64; X64; Trident/5.0)	

또 다른 중요 옵션은 [Application Login] 입니다. "Automactically submit these credentials" 항목을 선 택해 Burp Spider 가 로그인 폼을 만날 때마다 자동으로 [admin/password] 같은 자격증명을 제출하도록 설 정할 수 있습니다. Burp Spider 는 자동으로 이 자격증명을 제출하고 추가 정보를 찾기 위해 크롤링을 계속 할 것 입니다. [Spider Engine] 옵션에서 사용자가 원하는 경우 쓰레드 수를 변경할 수도 있습니다.

Individuate forms	by: Action	IIPI methodia	und fields		
individuate forms	S Dy. Action	i okt, method a			
🔵 Don't submit	forms				
Prompt for gu	uidance				
Automatically	submit usin	a the following	rules to assign text field	d values:	
- Automatically	sabinit asin	g the following	rates to assign text field	a + 41 4 4 2 .	
Add	Enabled	Match type	Field name	Field value	
Add	Enabled 🗹	Match type Regex	Field name mail	Field value winter@example.com	
Add Edit	Enabled	Match type Regex Regex	Field name mail first	Field value winter@example.com Peter	
Add Edit	Enabled v v v	Match type Regex Regex Regex	Field name mail first last	Field value winter@example.com Peter Winter	-
Add Edit Remove	Enabled	Match type Regex Regex Regex Regex	Field name mail first last surname	Field value winter@example.com Peter Winter Winter Winter	-
Add Edit Remove	Enabled	Match type Regex Regex Regex Regex Regex Regex	Field name mail first last surname name	Field value winter@example.com Peter Winter Winter Peter Winter Peter Winter	-
Add Edit Remove	Enabled	Match type Regex Regex Regex Regex Regex Regex Regex	Field name mail first last surname name comp	Field value winter@example.com Peter Winter Winter Peter Winter Winter Winter Consulting	
Add Edit Remove Up	Enabled	Match type Regex Regex Regex Regex Regex Regex Regex Regex	Field name mail first last surname name comp addr	Field value winter@example.com Peter Winter Winter Peter Winter Peter Winter Winter Consulting 1 Main Street	

마지막으로 [Form Submission] 옵션에서 웹 페이지 폼의 사용자 입력 부에 대한 값을 자동으로 제출하도록 설 정할 수 있습니다. Proxy 기능의 [Match and Replace] 옵션과 같이 옵션 항목 작성 시 정규 표현식(RegEx) 을 지정할 수 있습니다. Burp는 폼 필드 이름의 특정 패턴을 찾아서 지정 문자열을 자동으로 제출하기 위해, 웹 페 이지를 분석할 것입니다.

Target Pr	оху	Spider	Scanner	Intruder	Rep	eater	Sec	luencer	Dec	oder	Com	nparer
Site map	Site map Scope											
Filter: Hiding	Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hic											
▼ http://testa	sp.vul	nweb.com	ı			Host				Metho	d l	JRL
D /						http:/	/tes	tasp.vuln	we	GET	1	Login.a
🗋 Defau	lt.asp				_	http:/	/tes	tasp.vuln	we	POST	/	Login.a
See Login	- 63 I	http://tes	tasn.vulnwe	h.com/Logi	n asn			asp.vuln	we	GET	/	Login.a
Regist		Demesia fr		bicom, cogi	masp			asp.vuln	we	GET	/	Login.a
Search Search	1	kemove tr	om scope					asp.vuln	we	GET	/	Login.a
► Solution	-	Spider this	s branch					asp.vuln	we	GET	/	Login.a
E Good		Actively s	can this bra	nch				asp.vuln	we	GET	/	Login.a
Showing the showing	F	Passively :	scan this br	anch				asp.vuln	we	GET	/	Login.a
http://testa	1 5	Send to In	truder			æ.	+1	asp.vuln	we	GET	/	Login.a
http://testu	9	Send to Re	epeater			æ.	+R	asp.vuln	iwe	GET		Login.a
	9	Send to Se	quencer					asp.vuin	we	GET	/	Login.a
	9	Send to Co	omparer (re	quest)								
	9	Send to Co	omparer (re	sponse)				Resp	onse	1		
	9	Show resp	onse in bro	wser				Kesp	onse			
	F	Request in	browser				►	arams	Head	lers	Hex	
	E	Engageme	nt tools [Pr	o version on	ly]		►	in.asp HTTP/1.1				
		C						lstasn	3711] 1	web	COM	

[Target] 의 [Site map] 탭에서 Spider 를 시작하려면, 웹 애플리케이션 URL을 선택하고 마우스 오른쪽 버튼 을 클릭하여 "Spider this branch" 항목을 선택합니다.

Targ	get	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer
Con	trol	Option	ns						
?	<mark>Spi</mark> Use cho	<mark>der Sta</mark> these se ose "Spic	<b>tus</b> ttings to r ler this ho	nonitor and st / branch'	control Bur	p Spider. To	begin spiderin	ig, browse to	o the target ap
	S Req	pider is r uests ma	running ide: 127	Clear o	queues			4	
	Req For	uests qu ms queue	eued: 0 ed: 76						
?	Spi ©	<mark>der Sco</mark> Use suite Use cust	ope e scope (de om scope	efined in Tar	get tab]				

이렇게 하면 Burp Spider 가 시작되고 [Spider] 의 [Control] 탭에서 Spider 가 자동으로 생성하고있는 Request 를 볼 수 있습니다. 또한, Burp Spider 에 대한 사용자 정의 Scope 를 지정할 수도 있습니다.

Spidering 이 완료되면, 웹 애플리케이션에 대한 새로 발견된 URL 들이 표시 됩니다. 이 URL 들은 매우 유용한 정보를 제공하며, Burp Scanner 와 같은 다른 Burp 기능에 보내어 취약점 탐색을 할 수 있습니다.

### 3) Intruder

Burp Intruder 는 Fuzzing, Brute Force(무차별 대입) 공격에 이용할 수 있습니다. 이번 예제에서는 Brute Force(무차별 대입) 공격 기능을 사용할 것입니다. Burp Suite에서 [Intercept is on] 으로 되어있는지 확인하 고 웹 페이지에서 로그인 합니다.

Forward Drop	Intercept is on Action				
Raw Params Headers Hex					
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1					
Host: testasp.vulnweb.com					
User-Agent: Mozilla/5.0 (Mac	<u>'-+ T-+-l W AG V 10 A.</u>	25 0	) Gecko/2		
Accept: text/html,application	Send to Spider		;q=0.8		
Accept-Language: ko-kr,ko;q=	Do an active scan				
Accept-Encoding: gzip, defla	Send to Intruder	<b>ℋ+</b> I	1		
Referer: http://testasp.vuln	Send to Repeater	9€±₽	2Easp%3F		
Cookie: ASPSESSIONIDCCASRSSS	Send to Repeater	36 T K			
Connection: keep-alive	Send to Sequencer				
Content-Type: application/x-	Send to Comparer				
Content-Length: 25	Send to Decoder				
tfUName=user&tfUPass=love	Request in browser	•			
	Engagement tools [Pro version only]	•			

가로챈 사용자 Request 에서 마우스 오른쪽 클릭 후 "Send to Intruder" 항목을 선택하여 [Intruder] 로 Request 정보를 보냅니다.

?	Payload Positions	
	Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload help for full details.	positions – see
	Attack type: Sniper	T
	<pre>POST /Login.asp?RetURL=\$%2FDefault%2Easp%3F\$ HTTP/1.1 Host: testasp.vulnweb.com User=Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept=Lencoding: gzip, deflate Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F Cookie: ASPSESSIONIDCCASRSSS=\$GMLDHKOAHFHFEENOCMJKCEPC\$ Content=Type: application/x=www=form=urlencoded Content=Length: 25 tfUName=\$user\$&amp;tfUPass=\$love\$</pre>	Add § Clear § Auto § Refresh

[Intruder] 탭으로 이동하여 Attack Target 을 확인합니다. [Positions] 탭을 선택하면 사용자가 Intruder 로 보낸 Request 를 볼 수 있으며, 일부 강조 표시가 되어있습니다. 강조 표시는 기본적으로 Brute Force(무차별 대입) 공격 시 변경 되어질 부분을 Burp 에서 추측한 것입니다. 예제에서는 단지 사용자 이름 및 암호가 변경될 것 이므로, Burp 의 강조 표시를 적절하게 수정합니다. 오른쪽에 [Clear] 버튼을 클릭하면. 강조 표시된 텍스트가 모두 제거됩니다. 공격에 대한 매개변수로 사용자 이름 및 암호만을 설정해야 합니다. 이 Request에서 tfUName(예제의 경우 "user")을 드래그하고 [Add] 버튼을 클 릭합니다. 마찬가지로 password인 "love"를 드래그하고 [Add] 버튼을 클릭합니다. 이렇게 하면 tfUName 과 tfUPass 가 첫 번째 및 두 번째 변수로 추가되어 다음과 같이 보일 것입니다.

?	Payload Positions
	Configure the positions where payloads will be inserted into the base request. The attack type help for full details.
	Attack type: Sniper
	<pre>POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1 Host: testasp.vulnweb.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25 Accept: text/html,application/xhtml+xml,application/xml;q=0.9, Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefaul Cookie: ASPSESSIONIDCCASRSSS=GMLDHKOAHFHFEENOCMJKCBPC Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 25 tfUName=SuserS&amp;tfUPass=SloveS</pre>

다음으로 Request 윗 부분에 있는 공격에 대한 유형 [Attack type]을 설정합니다. 기본 값으로 "Sniper"가 설 정되어 있으나 예제의 경우에는 "Cluster bomb" 항목을 사용해야 합니다.

아래는 Portswigger.net 에서 설명하는 공격의 종류 및 차이입니다.

	Intruder 공격 유형					
Sniper	단일 Payload Set 을 사용하며, 사용자 정의 매개변수 순서대로 Payload 를 입력합니 다. 주어진 Request 를 처리하는 동안 지정한 변수를 제외하고는 영향을 받지 않습니다. 이 공격 형식은 XSS 처럼 공통적이고 개별적인 다수의 필드를 테스트 하는 데 유용 합니 다. 위와 같이 tfUName 과 tfUPass 두 필드를 변수로 지정한 경우 tfUName 에 Payload 를 순서대로 입력하는동안 tfUPass 에는 Payload 를 입력하지 않습니다. tfUName 에 Payload Set 의 모든 요소가 입력되면 그 다음으로 tfUName 에는 기본 값 (user)을 유지하며, tfUPass 에 Payload 를 순서대로 입력합니다.					
Battering ram	단일 Payload Set 을 사용하며, 사용자 정의 매개변수에 동일한 Payload Set 을 한꺼번 에 입력합니다. 즉, tfUName 과 tfUPass 에 같은 Payload 값이 입력됩니다. 이 공격 유 형은 HTTP 요청 내 여러 위치에 같은 입력 값을 삽입할 경우에 유용합니다.					
Pitchfork	여러 Payload Set 을 사용하며, 사용자 정의 매개변수에 다른 Payload Set(최대 8개) 을 입력합니다. 예를 들어, 첫 번째 Request 는 변수 1에 Payload Set 1 의 첫 번째 값 을 입력하고, 변수 2에 Payload Set 2 의 첫 번째 값을 입력합니다. 두 번째 Request에 서는 Payload Set 1 의 두 번째 값을 변수 1에 입력하고, Payload Set 2의 두 번째 값 을 변수 2 에 입력합니다. 이 공격 유형은 서로 다르지만 관련된 입력을 다수의 위치에 적용 해야 할 경우(예를 들어, 사용자 이름과 사용자 번호 등)에 유용합니다.					

Intruder 공격 유형					
Cluster bomb	여러 Payload Set 을 사용하며, 사용자 정의 매개변수에 다른 Payload Set(최대 8개) 을 입력합니다. Pitchfork 유형과 다른점은 각 Payload Set 을 순서대로 반복해 모든 Payload 의 조합을 테스트한다는 것입니다. 예를 들어, 사용자 정의한 변수가 두 개 있는 경우, Payload Set 1 에서 첫 번째 값을 변수 1에 입력하고, Payload Set 2 의 모든 값 을 변수 2에서 반복 입력한 다음, Payload Set 1 의 두 번째 값을 변수 1에 입력하고, Payload Set 2 의 모든 값을 변수 2에 반복 입력합니다. 이 공격 유형은 서로 다르고 관 련이 없는 변수가 다수 위치에 있는 경우 (예를 들어, 사용자 이름과 패스워드)에 유용합니 다.				

예제에서는 공격 유형을 "Cluster bomb"으로 설정합니다.

[Payload] 탭으로 가서, Payload Sets 옵션에서 "Payload set: 1" 을 선택하고 있는지 확인하고, [Load …] 버튼을 클릭하고 사용자 이름 목록이 들어 있는 파일을 선택합니다. 사용자 이름 목록이 있는 파일을 불러오면 모 든 사용자 이름이 아래 그림처럼 보여집니다.

Targ	get	Positions	Payloads	Options				
?	Pay You payl	rioad Sets can define oad set, an	s one or more d each payloa	payload set: d type can l	s. The be cust	number of paylo comized in differ	ad sets ent wa	s depends on the a ys.
	Payl	oad set: (	1		•	Payload count	: 54	
	Payl	oad type: (	Simple list		•	Request count	: 2,916	5
?	Pay This	r <mark>load Op</mark> t payload ty	tions [Simp pe lets you co admin	<b>le list]</b> onfigure a si	imple li	ist of strings tha	at are u	sed as payloads.
		oad	administrato master webmaster	r			Ď	
	R	emove	manager guest					
		Clear	test tester					
			anonymous				V	
		Add	Enter a new it	em				
	Ad	ld from list	(Pro versio	n only]		V	)	

마찬가지로 "Payload set: 2" 를 선택하고 [Load …] 버튼을 클릭해 암호 목록이 들어 있는 파일을 선택합니다.

Targ	get Position	Payloads	Options			
?	Payload Se You can defi payload set,	e <b>ts</b> ne one or more and each paylo	payload set: ad type can l	s. The r be cust	number of payload omized in differer	d sets depends on the it ways.
	Payload set:	2			Payload count: 1	180
	Payload type	Simple list		•	Request count: 9	9,720
?	Payload O This payload Paste	ptions [Simp type lets you c tester	o <mark>le list]</mark> onfigure a si	mple li	st of strings that a	are used as payloads.
	Load	tester1234 admin qwer			$\square$	
	Remove	root test!@#\$			•	•
	Clear	1 12 21				
		123			V	
	Add	Enter a new	item			
	Add from li	st (Pro versio	on only]		<b>v</b>	

[Options] 탭으로 가서 Attack Results 옵션 아래에 "Store requests" 및 "Store responses" 항목이 설 정 되어 있는지 확인합니다.

?	Attack Results
I	These settings control what information is captured in attack results.
	Store requests
	✓ Store responses
	Make unmodified baseline request
	Use denial-of-service mode (no results)
	Store full payloads

공격을 하기 위한 설정이 다 되었습니다. 왼쪽 상단 메뉴바에서 [Intruder] 를 클릭하고 "Start attack" 항목을 선택합니다. 새 창이 팝업 되고 결과가 만들어지는 것을 확인할 수 있습니다.



그럼 Intruder 의 Request 가 성공한 것을 어떻게 알 수 있을까요? 일반적으로 성공한 Request는 실패한 Request 와 다른 Response 또는 다른 상태의 Response 를 반환할 것입니다. "Status" 와 "Length" 를 확 인하고 다른 상태 또는 길이를 가진 Response 의 Request 를 선택해 확인합니다.

Request 🔺	Payload1	Payload2	Status	Error	Timeout	Length
0			200			2592
1	admin	tester	200			2592
2	administrator	tester	200			2592
3	master	tester	200			2592
4	webmaster	tester	200			2592
5	manager	tester	200			2592
6	guest	tester	200			2592
7	test	tester	200			2592
8	tester	tester	200			2592
9	root	tester	200			2592
10	anonymous	tester	200			2592
11	ftpuser	tester	200			2592
12	system	tester	200			2592
13	admin001	tester	200			2592
14	admin01	tester	200			2502
Request	Response					
Raw Hea	Raw Headers Hex HTML Render					
HTTP/1.1 200 OK						
Connection: close						
Date: Fri, 20 Dec 2013 00:41:21 GMT						
Server: M	icrosoft-IIS/6.0					
X-Powered	-Bv: ASP.NET					

### 4) Repeater

Burp Repeater 를 사용해서 수동으로 Request 를 수정하고 Response 를 분석하기 위한 재전송 작업을 할 수 있습니다. [Intruder] 와 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭 후 "Send to Repeater" 항 목을 선택하여 [Repeater] 로 Request 정보를 보냅니다. Intruder, Proxy 등 다양한 탭에서 Request 를 [Repeater] 로 보낼 수 있습니다.

Request to http://testasp.vulnweb.com:80 [87.230.29.167]					
Forward	Drop Intercept is on Action				
Raw Params Header	s Hex				
POST /Login.asp?Ret	URL=%2FDefault%2Easp%3F HTTP/1.1				
Iost: testasp.vulnw	eb.com				
Jser-Agent: Mozilla	<u>/5.0 (Macintosh; Intel Mac OS X 10.9</u> ; rv:25.0) Gecko/2				
Accept: text/html,a	Send to Spider .9,*/*;q=0.8				
Accept-Language: Ko	Do an active scan				
leferer: http://tes	Send to Intruder %+I FDefault%2Easp%3F				
ookie: ASPSESSIONI	Send to Repeater ೫+R				
connection: keep-al	Send to Sequencer				
Content-Type: appli	Send to Comparer				
oncenc-hengen. 25	Send to Decoder				
fUName=user&tfUPas	Request in browser				
	Engagement tools [Pro version only]				

[Repeater] 탭으로 이동하여 방금 보낸 Request 를 볼 수 있습니다. Repeater 상단에 1, 2 로 되어있는 두 개 의 탭을 볼 수 있습니다. 각 Request 당 한 개의 탭을 사용합니다.

Go Cancel < >
Request
Raw Params Headers Hex
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F Cookie: ASPSESSIONIDCCASRSSS=GMLDHKOAHFHFEENOCMJKCBPC Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 25
? < + > Type a search term
Response
Raw Hex

Request 를 [Raw], [Params], [Headers], [Hex] 형식으로 출력할 수 있습니다.

Request 를 수정한 후 그리고 [Go] 버튼을 눌러 해당 Request 를 서버로 보냅니다. 그리고 Response 섹션 에서 Response 를 분석합니다.

#### 5) Sequencer

일반적으로 사용자 인증에 관련이 있기 때문에 웹 애플리케이션 보안 상 세션 토큰은 높은 임의성을 가지는 것이 중요합니다. Burp Sequencer 는 웹 애플리케이션이 자동으로 생성한 이러한 세션 토큰의 임의성을 파악하는 데 사용합니다.

세션 토큰을 반환하는 Request 를 보내 봅니다. 다른 기능과 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭하여 "Send to Sequencer" 항목을 선택하여 [Sequencer] 로 Request 정보를 보냅니다.

Intercept	History	Options				
Request to http://testasp.vulnweb.com:80 [87.230.29.167]						
Forward		Drop		rcept is on		tion
Raw Para	ams Hea	iders He	×			
POST /Logi Host: test	in.asp?F asp.vul	RetURL=%	2FDefaul <sup>.</sup> m	t%2Easp%3	F HTTP/	1.1
User-Agent	i s	end to Spid	er			X 10.9; rv:25.
Accept: te Accept-Lar	aui D	o an active)	scan			ion/xml;q=0.9,* =0.3
Accept-End	od: S	end to Intru	der		≆+I	
Referer: h	nttį S	end to Repe	ater		⊯ + R	URL=%2FDefault
Cookie: AS	SPSE S	end to Sequ	encer			(CBPC
Connection	1: S	end to Com	parer			
Content-Ty Content-Le	pe s	end to Deco	der	k.		
E	R	equest in b	rowser		•	
tfUName=us	ser( E	ngagement	tools [Pro v	ersion only]	•	

[Sequencer] 탭으로 이동하면 자동으로 ID 매개 변수를 식별한 것을 볼 수 있으며, 사용자 정의 설정을 위해 [Manual load] 를 사용할 수 있습니다.

Live	capture	Manual loa	d Analysis options			
?	Select L Send requ	. <b>ive Captu</b> uests here fr	<b>re Request</b> om other tools to conf	ìgure a live capt	ure. Select the request to	o use, configure the other
	Clear	# 1	Host http://testasp.v	ulnweb.com	Request POST /Login.asp?RetUI	RL=%2FDefault%2E
	Start li	ve capture				
?	Token I Select the	Location W	/ <mark>ithin Response</mark> he response where the	e token appears		
	<ul> <li>Cooki</li> <li>Form</li> </ul>	ie: field:	ASPSESSIONIDQCDRR	TQQ=IPJDIGLBL	KBOOLJPIKAMFHLH	
	Custo	om location:				Configure

작업을 시작 하려면 [Start live capture]를 클릭 합니다.

00	0	Burp	Sequencer [live capture #1:	http://tes	stasp.vulnweb.com]
?	Live capture (221 tokens)				
<u> </u>	Pause Copy tok	ens	🗌 Auto analyze (next: 300)	Requests:	221
	Stop Save toke	ans	Analyze now	Errors:	0

자동으로 생성하는 Request 수 및 수신하는 토큰 수를 볼 수 있습니다. 분석은 적어도 100~200 개의 토큰을 캡처하고 시작하는 것이 좋습니다. 더 많은 토큰이 더 나은 테스트 결과를 보여줄 수 있습니다. 충분한 토큰을 캡처 했다면, [Analyse now] 버튼을 클릭합니다.

결과는 아래 그림과 같이 표시 됩니다. 보이는 것처럼, 샘플의 전반적인 임의성은 우수한 것으로 추정합니다. 다양 한 유형의 분석의 결과를 보기 위하여 상단의 탭을 선택하여 다양한 유형의 분석 결과를 볼 수 있습니다.

Summary	Character-level analysis	Bit-level analysis	Analysis Options				
Overall r The overall At a signific	Overall result The overall quality of randomness within the sample is estimated to be: good. At a significance level of 1%, the amount of effective entropy is estimated to be: 55 bits.						
Effective	Note: Character-level analysis was not performed because the sample size is too small relative to the size of the character set used in the sampled tokens. Effective Entropy						
The chart s probability below this l required to	hows the number of bits of of the observed results occ evel, the hypothesis that the reject the hypothesis that t	effective entropy at e urring if the sample e sample is randomly he sample is random	each significance leve is randomly generate generated is rejecte , and so increases th	el, based on all tests. Each :d. When the probability of d. Using a lower significan e chance that non–randor	significance level f the observed res ice level means th n data will be trea	l defines a minimum sults occurring falls lat stronger evidence is lted as random.	
	>10% -						
	>1% -						
Signific	ance level >0.1% -						

#### 6) Comparer

Burp Comparer 는 Request, Response 등과 같은 데이터를 비교하는데 사용합니다. 예제에서는 위에서 Brute Force(무차별 대입) 공격 시 받은 Response 두 개를 비교해 보겠습니다. [Intruder] 의 [Result] 탭에 서 각각 Request 에 마우스 오른쪽 클릭 후 "Send to Comparer (response) 항목을 선택합니다.

109	admin [	- duatu		200
110	administrato	Result #109		200
111	master	Do an active scan		200
112	webmaster	Do a passive scan		200
113	manager	Send to Intruder	¥£+1	200
114	guest	Send to Repeater	96 L D	200
115	test	Send to Repeater	46 T K	200
116	tester	Send to Sequencer		200
117	root	Send to Comparer (request)		200
		Send to Comparer (response)		
Request	Response	Show response in browser		
		Request in browser	•	
Kaw He	aders Hex	Generate CSRF PoC		
HTTP/1.1	200 OK	Add to site map		
Connection: close		Request item again		
Date: Fri Demogra	1, 20 Dec	Define extract gren from response		
114 115 116 117 Request Raw He HTTP/1.1 Connection Date: Fri Server: N	guest test root Response eaders Hex 200 OK on: close i, 20 Dec ficrosoft-	Send to Repeater Send to Sequencer Send to Comparer (request) Send to Comparer (response) Show response in browser Request in browser Generate CSRF PoC Add to site map Request item again Define extract grep from response	#+R	200 200 200 200

[Comparer] 탭으로 이동합니다. 사용자가 보낸 두 개의 Response 를 볼 수 있습니다. 윗 부분(item 1) 첫 번 째 Response (#1)와 아래 부분(item 2) 두 번째 Response (#2) 를 클릭합니다.

Comparer			?
This function let other tools and t	s you do a word- or byte-level then select the comparison you	comparison between different data. You can load, paste, or send da a want to perform.	ta here from
Select item 1:			
#	Length	Data	Paste
1	2592	HTTP/1.1 200 OK Connection: close Date: Fri, 20 De	
2	2592	HTTP/1.1 200 OK Connection: close Date: Fri, 20 De	Load
			Remove
			Clear
Select item 2:			
#	Length	Data	
1	2592	HTTP/1.1 200 OK Connection: close Date: Fri, 20 De	
2	2592	HTTP/1.1 200 OK Connection: close Date: Fri, 20 De	1
			·
			Compare
			Compare Words

Comparer 에서는 Words 또는 Bytes 2가지 유형으로 선택한 아이템을 비교를 할 수 있습니다. [Words] 버튼 을 클릭하면 단어로 비교합니다. 결과는 아주 분명합니다. 두 응답의 세션 토큰이 다른 것을 확인할 수 있습니다.

0 0 0 Word	d compare of #1 a	and #2 (3 differences)	
Length: 2,592	💿 Text 🔘 Hex	Length: 2,592	🖲 Text 🔘 Hex
HTTP/1.1 200 OK Connection: close Date: Fri, 20 Dec 2013 00: <mark>48:27</mark> GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 2329 Content-Type: text/html Set-Cookie: ASPSESSIONIDQCDRRTQQ=CGJDIGLBDBCALPMFMBFC path=/ Cache-control: private	AMCF:	HTTP/1.1 200 OK Connection: close Date: Fri, 20 Dec 2013 00: <mark>41:21</mark> GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 2329 Content-Type: text/html Set-Cookie: ASPSESSIONIDQCDRRTQQ=NBJDIGLBIGKGHKJBIGPNCLM Cache-control: private	MK: path=/
<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01     Transitional//EN" "http://www.w3.org/TR/html4/loo <html><!-- InstanceBegin<br-->template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLIsLocked="false"&gt; <head> <!-- InstanceBeginEditable name="doctitle"--> <title>acuforum login</title> <!-- InstanceEndEditable--> <meta content="text/ht&lt;br&gt;charset=iso=8859=1" http-equiv="Content-Type"/></head></html></pre>	se.dtd">	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loos <html>    <!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLIsLocked="false"--> <head> <!-- InstanceBeginEditable name="doctitle"--> <html> <li>&lt;= InstanceEndEditable&gt; <meta content="text/htm charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="head"-->        <td>e.dtd"&gt;</td></li></html></head></pre>	e.dtd">
Key: Modified Deleted Added			Sync views

마찬가지로, 바이트를 사용하여 비교하면 다음과 같은 출력을 볼 수 있습니다.

000		Byte compare of #:	Land #2 (8 differences)	
Length: 2,592		🔾 Text 🖲 Hex	Length: 2,592	🔘 Text 🖲 Hex
0 48 54	4 54 50 2f 31 2e 31	20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK	0 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1	200 OK
1 0a 43	3 6f 6e 6e 65 63 74	69 6f 6e 3a 20 63 6c 6f Connection: clo	1 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f Connectio	on: clo 📉
2 73 65	5 Od Oa 44 61 74 65	3a 20 46 72 69 2c 20 32 se Date: Fri, 2	2 73 65 0d 0a 44 61 74 65 3a 20 46 72 69 2c 20 32 se Date: Fr	ri, 2
3 30 20	0 44 65 63 20 32 30	31 33 20 30 30 3a 34 38 0 Dec 2013 00:48	3 30 20 44 65 63 20 3 30 31 33 20 30 3a 34 31 0 Dec 201	3 00:41
4 3a 32	2 37 20 47 4d 54 0d	0a 53 65 72 76 65 72 3a :27 GMT Server:	4 3a 32 31 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a :21 GMT S	erver:
5 20 4d	d 69 63 72 6f 73 6f	66 74 2d 49 49 53 2f 36 Microsoft-IIS/6	5 20 4d 69 63 72 6f 73 6f 66 74 2d 49 49 53 2f 36 Microsoft-	-IIS/6
6 2e 30	0 0d 0a 58 2d 50 6f	77 65 72 65 64 2d 42 79 .0 X-Powered-By	6 2e 30 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 79 .0 X-Powe	red-By
7 3a 20	0 41 53 50 2e 4e 45	54 0d 0a 43 6f 6e 74 65 : ASP.NET Conte	7 3a 20 41 53 50 2e 4e 45 54 0d 0a 43 6f 6e 74 65 :ASP.NET	Conte
8 6e 74	4 2d 4c 65 6e 67 74	68 3a 20 32 33 32 39 0d nt-Length: 2329	8 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 33 32 39 0d nt-Length:	2329
9 0a 43	3 6f 6e 74 65 6e 74	2d 54 79 70 65 3a 20 74 Content-Type:t	9 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 Content-T	rype: t
a 65 78	8 74 2f 68 74 6d 6c	0d 0a 53 65 74 2d 43 6f ext/html Set-Co	a 65 78 74 2f 68 74 6d 6c 0d 0a 53 65 74 2d 43 6f ext/html 5	set-Co
b 6f 6b	b 69 65 3a 20 41 53	50 53 45 53 53 49 4f 4e okie: ASPSESSION	b 6f 6b 69 65 3a 20 41 53 50 53 45 53 53 49 4f 4e okie: ASPSi	ESSION
c 49 44	4 51 43 44 52 52 54	51 51 3d 43 47 4a 44 49 IDQCDRRTQQ=CGJDI	c 49 44 51 43 44 52 52 54 51 51 3d 4e 42 4a 44 49 IDQCDRRT	QQ=NBJDI
d 47 4c	c 42 44 42 43 41 4c	50 4d 46 4d 42 46 43 41 GLBDBCALPMFMBFCA	d 47 4c 42 49 47 4b 47 48 4b 4a 42 49 47 50 4e 43 GLBIGKGH	KJBIGPNC
e 4d 43	3 46 3b 20 70 61 74	68 3d 2f 0d 0a 43 61 63 MCF; path=/ Cac	e 4c 4d 4b 3b 20 70 61 74 68 3d 2f 0d 0a 43 61 63 LMK; path=	=/ Cac
f 68 65	5 2d 63 6f 6e 74 72	6f 6c 3a 20 70 72 69 76 he-control: priv	f 68 65 2d 63 6f 6e 74 72 6f 6c 3a 20 70 72 69 76 he-control	l: priv
10 61 74	4 65 0d 0a 0d 0a 0d	0a 3c 21 44 4f 43 54 59 ate DOCTY</td <td>10 61 74 65 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 ate <!--D</td--><td>ОСТҮ</td></td>	10 61 74 65 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 ate D</td <td>ОСТҮ</td>	ОСТҮ
11 50 45	5 20 48 54 4d 4c 20	50 55 42 4c 49 43 20 22 PE HTML PUBLIC "	11 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 PEHTMLPI	UBLIC "
12 2d 2f	f 2f 57 33 43 2f 2f	44 54 44 20 48 54 4d 4c -//W3C//DTD HTML	12 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c -//W3C//U	DTD HTML
13 20 34	4 2e 30 31 20 54 72	61 6e 73 69 74 69 6f 6e 4.01 Transition	13 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 4.01 Tran	sition
14 61 6c	c 2f 2f 45 4e 22 20	22 68 74 74 70 3a 2f 2f al//EN" "http://	14 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f al//EN" "ht	.tp://
15 77 77	7 77 2e 77 33 2e 6f	72 67 2f 54 52 2f 68 74 www.w3.org/TR/ht	15 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 www.w3.or	g/TR/ht
16 6d 6c	c 34 2f 6c 6f 6f 73	65 2e 64 74 64 22 3e 0d ml4/loose.dtd">	16 6d 6c 34 2f 6c 6f 6f 73 65 2e 64 74 64 22 3e 0d ml4/loose.	.dtd">
Key: Modified	Deleted Added			Sync views

### 7) Decoder

Burp Decoder는 암호화 된 데이터를 해독하거나 데이터를 암호화하는데 사용합니다. 수동으로 [Decoder] 에 데이터를 붙여 넣거나 인코딩 된 Request 를 Decoder 에 보낼 수 있습니다. 이 경우 base64 인코딩 형식으로 암호화된 사용자 이름 및 암호를 포함하는 HTML Basic 인증 Request 를 [Decoder] 로 보낼 것입니다. 다른 기능과 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭 후 "Send to Decoder" 항목을 선택하여 [Decoder] 로 Request 정보를 보냅니다.

GET / HTTP/1.1 Host: testasp.vu	llnweb.com		٨
User-Agent: Mozi	<u>lla/5.0 (Macintosh; Intel Ma</u>	<u>c os x</u>	10.9; rv:25.0)
Accept: text/htm	Send to Spider		xml;q=0.9,*/*
Accept-Language: Accept-Encoding:	Do an active scan		
Keep-Alive: 115	Send to Intruder	<b>ℋ+I</b>	
Proxy-Connection	Send to Repeater	3€+R	
DNT: 1	Send to Sequencer		
Authorization: E	Send to Comparer		
	Send to Decoder		
	Request in browser	•	
	Engagement tools [Pro version only]	•	

암호화된 부분을 드래그하고 [Decode as …] 버튼을 클릭하고 "Base64" 항목을 선택합니다.

Burp Decoder 가 base64로 암호화된 문자열을 해독하여 사용자 이름/암호를 평문으로 제공합니다.

Host: testasp.vulnweb.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3	Text O Hex      Text     Decode as
Accept-Encoding: gzip, deflate	Plain
Proxy-Connection: keep-alive	URL
DNT: 1	HTML
Authorization: Basic cmFlaHl1bmc6Z2VuaXVz	Base64
	ASCII hex
Host: testasp vulnweb.com	Hex
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0	Octal
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Binary
Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3	Gzip
Accept-Encoding: gzip, deflate	
Proxy-Connection: keep-alive	Hash
DNT: 1	
Authorization: Basic raehyung:genius	Smart decode

### 8) Scanner

Burp Scanner 는 가장 강력한 웹 애플리케이션 취약점 탐색 도구 중 하나입니다. 하지만, 다른 도구들처럼 완벽 하지 않으며, False Positive 가 발생할 수 있습니다. Burp Scanner 는 무료 버전에서는 사용할 수 없습니다.

# 응용: Burp Intruder via SQL Injection

Blind 방식이나 Error 기반의 취약점으로 작동할 수 있는 SQL Injection 도구들은 많이 존재하며, Kali 리눅스 같은 배포판 OS 에 미리 설치되어 실행할 준비가 되어 있습니다. SQLMap 은 그 좋은 예입니다. 이런 도구들은 데이터베이스에서 데이터를 추출하는 것 외 루트 권한을 획득하는 등 다른 많은 일을 할 수 있습니다. 하지만 이 문 서에서는 Burp Intruder 를 통해 구현할 수 있는 (단지 데이터 추출만을 위한) SQL 인젝션 기술을 설명하고자 합니다.

제일 먼저 해야할 일은 Request 를 확인을 통해 SQL Injection 에 취약한 부분을 발견하는 것입니다:

SQL Injection 공격이 가능해 보이는 Request 를 마우스 오른쪽 클릭 후 "Send to Intruder" 항목을 선택합니다.

다음과 같이 SQL 인젝션이 가능한 파라미터의 값을 Intruder 의 변수로 지정하며 단일 Payload Set 을 사용할 것이므로 공격 유형을 "Sniper" 로 지정합니다.

Payload Positions	
Configure the positions where payloads will be inserted into the base request. The attack type payloads are assigned to payload positions – see help for full details.	determines th
Attack type: Sniper	•
Host: testasp.vulnweb.com	
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25 Gecko/20100101 Firefox/25.0 Accert:	.0)
<pre>text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer:</pre>	3
http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3) Cookie: ASPSESSIONIDCCASRSSS=GMLDHKOAHFHFEENOCMJKCBPC; ASPSESSIONIDCCCTRQSQ=OIIMLDCDHOAIAGGFJJAEFBKD Connection: keen-alive	F
Content-Type: application/x-www-form-urlencoded Content-Length: 26	
tfUName=admin&tfUPass= <mark>§test§</mark>	,
? < + > Type a search term	0 matches

Intruder 의 변수는 파라미터 값 다음에 올 수도 있습니다.

Payload Positions		
Configure the positions where payloads payloads are assigned to payload position	will be inserted into the base request. The attack type on the set of the set	letermines th
Attack type: Sniper		•
Host: testasp.vulnweb.com User-Agent: Mozilla/5.0 (Ma Gecko/20100101 Firefox/25.0	cintosh; Intel Mac OS X 10.9; rv:25.	0)
<pre>text/html,application/xhtml Accept-Language: ko-kr,ko;c Accept-Encoding: gzip, defl Referer:</pre>	+xml,application/xml;q=0.9,*/*;q=0.8 {=0.8,en-us;q=0.5,en;q=0.3 ate	
http://testasp.vulnweb.com/ Cookie: ASPSESSIONIDCCASRSS ASPSESSIONIDCCCTRQSQ=OIIMLI Connection: keep-alive	Login.asp?RetURL=%2FDefault%2Easp%3F S=GMLDHKOAHFHFEENOCMJKCBPC; CDHOAIAGGFJJAEFBKD	
Content-Type: application/> Content-Length: 26	-www-form-urlencoded	
tfUName=admin&tfUPass=test	S	\ \
? < + > Type a se	earch term	0 matches

다음으로 Payload Set 을 지정합니다.



SQL Injection 가능 여부 확인을 위한 Payload Set 으로 다음과 같은 목록을 사용할 수 있습니다.

SQLi Test
•
н
/
/*
#
)
(
)'
('
and 1=1
and 1=2
and 1>2
and 1<=2
+and+1=1
+and+1=2
+and+1>2
+and+1<=2
/**/and/**/1=1
/**/and/**/1=2
/**/and/**/1>2
/**/and/**/1<=2

마지막으로 [Intruder]의 [Options] 탭에서 Grep 항목을 설정합니다. 여기서는 Intruder 프로세스 후 얻는 결 과 페이지 목록을 설정할 수 있습니다. 예를 들어 Grep 에서 "Cookie" 를 추가하면, 결과 페이지 중 "Cookie" 라는 단어가 존재하는 페이지만 결과 목록에 나타납니다.

Grep - Match				
These settings can be used to flag result items containing specified expressions.				
Flag result items with responses matching these expressions:				
Paste	error			
	exception			
Load	illegal			
	invalid			
Remove	fail			
	stack			
Clear	access			
Clear	directory			
	file			
	not found			
Add	Enter a new item			
Match type: 💿 Simple string				
Regex				

Grep 에 설정할 Payload Set 으로 다음과 같은 목록(SQL Error 메시지)을 사용할 수 있습니다.

SQL Error Message
unknown column
unknown
no record found
mysql_num_rows()
mysql_fetch_array()
Error Occurred While Processing Request
Server Error in '/' Application
Microsoft OLE DB Provider for ODBC Drivers error
error in your SQL syntax
Invalid Querystring
OLE DB Provider for ODBC
VBScript Runtime

br@infeed3r

SQL Error Message			
ADODB.Field			
BOF or EOF			
ADODB.Command			
JET Database			
<pre>mysql_fetch_row()</pre>			
include()			
mysql_fetch_assoc()			
<pre>mysql_fetch_object()</pre>			
mysql_numrows()			
GetArray()			
FetchRow()			
Input string was not in a correct format			
Microsoft VBScript			
A syntax error has occurred			
ADODB.Field error			
ASP.NET is configured to show verbose error	messages		
ASP.NET_SessionId			
Active Server Pages error			
An illegal character has been found in the	statement		
An unexpected token "END-OF-STATEMENT" was	Found		
CLI Driver			
Can't connect to local			
Custom Error Message			
DB2 Driver			
DB2 Error			
DB2 ODBC			
Died at			
Disallowed Parent Path			
Error Diagnostic Information			
Error Message : Error loading required libro	aries.		
Error Report			
Error converting data type varchar to numer	ic		
br@infeed3r 27/30	brainfeeder-git.github.io		

SQL	. Error Message	,
Fatal error		
Incorrect syntax near		
Index of		
Internal Server Error		
Invalid Path Character		
Invalid procedure call or argument		
Invision Power Board Database Error		
JDBC Driver		
JDBC Error		
JDBC MySQL		
JDBC Oracle		
JDBC SQL		
Microsoft OLE DB Provider for ODBC	Drivers	
Microsoft VBScript compilation erro	r	
Microsoft VBScript error		
MySQL Driver		
MySQL Error		
MySQL ODBC		
ODBC DB2		
ODBC Driver		
ODBC Error		
ODBC Microsoft Access		
ODBC Oracle		
ODBC SQL		
ODBC SQL Server		
OLE/DB provider returned message		
ORA-0		
ORA-1		
Oracle DB2		
Oracle Driver		
Oracle Error		
Oracle ODBC		
br@infeed3r	28/30	brainfeeder-git.github.io

SQL Error Message	
PHP Error	
PHP Parse error	
PHP Warning	
Parent Directory	
Permission denied: 'GetObject'	
PostgreSQL query failed: ERROR: parser: parse error	
SQL Server Driver][SQL Server	
SQL command not properly ended	
SQLException	
Supplied argument is not a valid PostgreSQL result	
Syntax error in query expression	
The error occurred in	
The script whose uid is	
Type mismatch	
Unable to jump to row	
Unclosed quotation mark before the character string	
Unterminated string constant	
Warning: Cannot modify header information - headers already sent	
Warning: Supplied argument is not a valid File-Handle resource in	
Warning: mysql_query()	
Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL	
You have an error in your SQL syntax near	
detected an internal error [IBM][CLI Driver][DB2/6000]	
error	
include_path	
invalid query	
is not allowed to access	
missing expression	
mySQL error with query	
mysql error	
on MySQL result index	
on line	
br@infeed3r 29/30 brainfeeder-git.gith	nub.io

**SQL Error Message** 

server at

server object error

supplied argument is not a valid MySQL result resource

unexpected end of SQL command

이제 Burp Intruder 를 실행하고 취약한 Request 를 확인합니다.

		-	-		<i></i>	<b>k</b>	
Request A Payload	Status	Error	Timeout	Length	Comment		
0	200			2525	baseline reque	st	
1 '	500			517			
Request Response							
Raw Headers Hex XML							
HTTP/1.1 500 Internal Server Er	ror						
Connection: close							
Date: Mon, 23 Dec 2013 02:22:52	GMT						
Server: Microsoft-IIS/6.0							
X-Powered-By: ASP.NET							
Content-Length: 303							
Content-Type: text/html							
Cache_control: private							
odono concret. France							
<font face="Arial" size="2"></font>							
<pre>state = "And the clients of the state = "Arial" size=2&gt;error '80040e14'</pre>							
<r><r><r><r><r></r></r></r></r></r>						,	
<pre><font face="Arial" size="2">Unclosed quotation mark after the character string 'test''.</font></pre>							
<font face="Arial" size="2">/Logi</font>	ι <b>n.asp<!--</b-->±0</b>	ont> <tor< td=""><td>nt face=</td><td>="Arial" :</td><td>size=2&gt;, li</td><th>ine 10<td>&gt;  </td></th></tor<>	nt face=	="Arial" :	size=2>, li	ine 10 <td>&gt;  </td>	>

같은 방법으로 발견한 Request 에 대해 Payload Set 을 변경하여 Intruder 를 다시 실행합니다. Payload Set 으로 알려진 SQL Injection 구문을 목록화하여 사용할 수 있습니다.

## 참고 문서

http://resources.infosecinstitute.com/burp-suite-walkthrough/ http://resources.infosecinstitute.com/fuzzing-sql-injection-burp-suite-intruder/