โปรแกรม Burp Suite

Burp Suite เป็นโปรแกรมสำหรับการทดสอบของเว็บแอปพลิเคชัน โดยคุณลักษณะหลักของ โปรแกรมนี้คือส่วนของ Proxy web นั่นคือเราสามารถคักจับการส่ง Request จาก Client และ Response ข้อมูลตอบกลับไปยัง Client โดยสามารถเลือกกระทำการใด ๆ กับข้อมูลนั้นก็ได้ แต่โปรแกรมนี้จะสามารถ ใช้งานได้เฉพาะบนเบราว์เซอร์ หรือ IP ของตัวเองเท่านั้น ซึ่งมีคุณลักษณะที่หลากหลายและคุณลักษณะของ โปรแกรม Burp Suite แบบฟรีและโปรแกรม Burp Suite แบบตัวเต็ม จะแตกต่างกันออกไป

ขั้นตอนการติดตั้งและการใช้ Burp Suite

- 1. ก่อนที่เราจะติดตั้งโปรแกรม Burp Suite ได้นั้น ภายในเครื่องคอมพิวเตอร์จะต้องมีโปรแกรม Eclipse
- 2. สามารถโหลดโปรแกรมใด้จาก <u>https://portswigger.net/burp/download.html</u>

← → C A https://	portswigger.net/burp/download.htm	nl			And a regarder of	• ☆ ≡
		GER Burp Su	uite, the leading toolki	t for web appli	kigin cation security testing	
	About Burp Success	s Stories Download	Buy Burp	SUPPORT	BLOG CONTACT	
	Home > Burp > Download					
	Download Burp Please choose the edition of	Suite Burp Suite that is right for yo	u, Help me choose i	T es	"Burp Suite Pro is an unbelievably powerful tool. The scanner is amazingly fast and accurate. I use Burp	
		Free Edition	Professional Edition \$290 per user per year	timonia	extensively and it has never let me down." Alex Lauerman, FishNet Security	
	Bulp Proxy	0	۲	c)	"If you test the security of web	
	Burp Spider	2	۵.		applications for a living, Burp	
	Burp Repeater	2	20		weapon you must have in your	
	Burp Sequencer	0	۲		arsenal.*	
	Burp Decoder	2	۲		Jack Mannino, CEO, nVisium	
	Burp Comparer	8	۲		Security Inc.	
	Burp Intruder 🛛 😡	Time-brottled demo	۲		Read more Success Stories +	
	Burp Scanner		S			
	Save and Restore 🚯		۲			
	Source 0		۲	e	Wednesday, August 26, 2015	
	Target Analyzer 😡		۷	m	New release cycle for Burp	
	Content Discovery		۲	30	Suite Free Edition	
	Task Schadular G		1 N N N N N N N N N N N N N N N N N N N	0		

3. ถ้าภายในเครื่องคอมพิวเตอร์มีโปรแกรม Eclipse ติดตั้งอยู่ จะสามารถเปิดไฟล์ได้ทันที

▲ burpsuite_free_v1.6.29 19/10/2558 23:53 Executable Jar File 12,663 KB

Burp Suite



4. ลักษณะ โดยรวมของโปรแกรม Burp Suite

Burp Suite Free Edition v1.6.29 – d						_ 8 ×
Burp Intruder Repeater Window Help						
Target Proxy Spider Scanner Intruder Repeater	Sequencer Decoder Cor	nparer Extender Options A	erts			
Site map Scope						
Filter Hiding not found items, hiding CSS, image and general bi	nary content, hiding 4xx respons	es, hiding empty folders				2
	Host	lethod URL	Params Status A Length	MIME type Title	Comment	Time requested
				-		
	Request Response					
	Raw Hex					piere
	1					ŕ
						F
	7 · · · ·	Type a search form				0 matches

5. เลือก IP เป้าหมายที่จะใช้ในการคักจับ

rp in	uuuer Kepe	ater willdow	Ticih	~	~	~		~	
Intruc	der R	epeater	Sequencer	Deco	ier	Comparer E	xtender	Options AI	lerts
	Target	Ĩ	Proxy	0	a.	Spider	ſ	Scanner	
terce	nt HTTP hi	story Webs	Sockets history	Options					_
				- Merenancen	-				
F	Proxy Liste	eners							
	Dura Danua								
5	Surp Proxy u	ses ilsteners ti	o receive incon	ning HTTP red	luesis iron	n your browser. You	will need t	o configure your brow	vser
Ĩ	Add	Running	Interface	Ir	visible	Redirect		Certificate	
			127.0.0.1:8	0			1	Per-host	
l	Edit		10.199.121	.61:80			1	Per-host	
1									
l									
l									
l									
l									
l									
l									
E	Each installati	on of Burp ge	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ins.
E	Each installati	on of Burp ger	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ins.
E	Each installati	on of Burp get lation of Burp.	nerates its own	n CA certifica	te that Pro	xy listeners <mark>can use</mark>	when nego	otiating SSL connectio	ins.
E	Each installati	on of Burp ger lation of Burp.	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ins.
Ea	Each installati another instal	on of Burp ger lation of Burp. port CA certific	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ins.
Ea	Each installati another instal	on of Burp ger lation of Burp. port CA certifi	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ns.
Ea	Each installati another instal Import / ex	on of Burp ger lation of Burp. port CA certific	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ns.
E a (Each installati another instal Import / ex	on of Burp gei lation of Burp. port CA certific	nerates its own cate Reg	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ns.
E a (Each installati another instal Import / ex	on of Burp ger lation of Burp. port CA certific Client Requ	nerates its own	n CA certifica	te that Pro	xy listeners can use	when nego	otiating SSL connectio	ins.
E a ())	Each installati another instal Import / ex Intercept (Jse these se	on of Burp ger lation of Burp. port CA certific Client Requ ttings to contro	nerates its own cate Reg rests	n CA certifica jenerate CA (te that Pro certificate	xy listeners can use	when negr	otiating SSL connectio	ns.
E a ())) U	Each installati another instal Import / ex Intercept (Jse these se	on of Burp gei lation of Burp. port CA certifii Client Requ	nerates its own cate Reg rests of which reque	n CA certifica jenerate CA o sts are stalle	te that Pro certificate	xy listeners can use	when nego	otiating SSL connectio	ns.
(())) (Each installati another install Import / ex Intercept C Jse these se	on of Burp gel lation of Burp. port CA certific Client Requ ttings to contro requests base	nerates its own cate Reg rests of which request of on the follow	n CA certifica ienerate CA (sts are stalle	te that Pro pertificate d for viewi	xy listeners can use	when negr	otiating SSL connectio	ns.
E a l l l l	Each installati another install Import / ex Intercept (Jse these se Intercept	on of Burp ger lation of Burp. port CA certific Client Requ ttings to contro	nerates its own cate Reg lests of which request ad on the follow	n CA certifica ienerate CA i sts are stalle	te that Pro pertificate d for viewi	xy listeners can use	when nego	otiating SSL connectio	ins.
(e e e e e e e e e e e e e e e e e e e	Each installati another install Import / ex Intercept (Jse these se Intercept Add	on of Burp ge lation of Burp. port CA certifin Client Requ ttings to contro requests base Enabled	nerates its own cate Reg rests of which request of which request of on the follow Operator	n CA certifica ienerate CA d sts are stalle ving rules: M Match typ	te that Pro certificate d for viewi aster intere e	xy listeners can use	when nego	otiating SSL connectio	ns.
E a a () ((((Each installati another install Import / ex Intercept C Jse these se Intercept Add	on of Burp ger lation of Burp. port CA certifit Client Requ ttings to contro requests base Enabled	ests d on the follow	n CA certifica enerate CA o sts are stalle ving rules: M Match typ File exten	te that Pro ertificate d for viewi aster intern e sion	xy listeners can use	when nego	b. Condition	sS/^
(• •	Each installation another install Import / ex Intercept (Jse these se Intercept Add Edit	on of Burp gei lation of Burp. port CA certifin Client Requ ttings to contro requests base Enabled	nerates its own cate Reg lests of which reque d on the follow Operator Or	n CA certifica enerate CA o sts are stalle ving rules: M Match typ File exten Request	te that Pro certificate d for viewi aster interr e sion	xy listeners can use	when nego	otiating SSL connectio	ns. sS ^
(• •	Each installati another instal Import / ex Intercept (Jse these se Intercept Add Edit	on of Burp gel lation of Burp. port CA certifie Client Requ titings to contre requests based Enabled	ests Or Or Or	n CA certifica enerate CA o sts are stalle ving rules: M Match typ File exten Request HTTP met	te that Pro pertificate d for viewi aster interc e sion nod	xy listeners can use	when nego Intercept ta	b. Condition (getipost)	ns. sSI^

เปิดเว็บเบราว์เซอร์ --> ตั้งค่า --> ตัวเลือกขั้นสูง --> คลิก เปลี่ยนการตั้งค่าพร็อกซี

ເບັ້ນດຳ ໃນ້ນຽກກາຣຄາດຕະແນກິຈະ ແລນ ຄິດທຽນຍາກຮ່ວນກນຳເທົ ຈາຍບານຮາຍຄະເລີຍຄອລ. ປາກປ້ວນອຸດແແລະລຸປກຣໜ໌ ໃນ້ມຽກການເງັ້ນເທື່ອປ່ວຍແຜ ຈຳລະຄືທີ່ກາງເນັ້ນາແລະຮ	ช่วยเต็มข้อความค้าหาแลง ไอการโหลดหน้าที่รวดเร็วอ่ เหตุการณ์ความปลอดภัย ของคุณจากเว็บไซต์อินตร เป็นข้อผิดพลาดในการสะเ	ะ URL ที่พัฒพ์ลงในแถบ วังขึ้น ดีเป็นไปได้ต่อ Google ' าย	ทีอยู่เว็บหรือช่องคันหาข โดยอัตโนมัติ	ตันก องเครื่องเรียกใช้ง	ารตั้งค่า ว <mark>น</mark>							
ใช้บริการดาดตะเมที่จะ แอป ดึงกริพยากรล่วงหน้าเท้ รายงานรายละเอียดของ ปกป้องคุณและอุปกรณ์ ใช้บริการเว็นเพื่อช่วยแก ส่งสถิติการใช้งานและร	ช่วยเดิมข้อความคันหาแลง ข้อการโหลดหน้าที่รวดเร็วอ่ งเหตุการณ์ความปลอดภัยา ของคุณจากเว็บไซต์อันตร ว่ไปขย้อผิดพลาดในการสะห	ะ URL ที่พัมพ์ลงในแถบ มิ่งขึ้น ที่เป็นไปได้ต่อ Google ' าย	ที่อยู่เว็บหรือช่องค้นหาข โดยอัดโนมิดิ	องเครื่องเรียกใช้ง	าน							
 ดึงทรัพยากรล่วงหน้าเท้ รายงานรายละเอียดของ ปกป้องคุณและอุปกรณ์ ให้บริการเว็บเพื่อช่วยแก่ ส่งสถิติการใช้งานและร 	มื่อการโหลดหน้าที่รวดเร็วย์ มเหตุการณ์ความปลอดภัย ของคุณจากเว็บไซต์อันตร เป็นข่อผิดพลาดในการสะย	ว่งขึ้น ที่เป็นไปได้ต่อ Google ' าย	โดยอัตโนมัติ									
 รายงานรายละเอียดของ ปกป้องคุณและอุปกรณ์ ใช้บริการเว็บเพื่อช่วยแสง ส่งสถิติการใช้งานและร 	บเหตุการณ์ความปลอดภัย ของคุณจากเว็บไซต์อันตร ว่ไขข้อผิดพลาดในการสะศ	ที่เป็นไปได้ต่อ Google ' าย	โดยอัตโนมัติ		🐼 ดึงทรัพยากรล่วงหน้าเพื่อการโหลดหน้าที่รวดเร็วยิ่งขึ้น							
 ปกป้องคุณและอุปกรณ์ ใช้บริการเว็บเพื่อช่วยแ/ ส่งสถิติการใช้งานและร 	ของคุณจากเว็บไซต์อันตร ว่ไขข้อผืดพล <mark>าดใ</mark> นการสะ <i>เ</i>	าย										
] ใช้บริการเว็บเพื่อช่วยแ <i>เ</i>] ส่งสถิติการใช้งานและร	า้ไขข้อผิดพลาดในการสะก											
📔 ส่งสถิติการใช้งานและร	🔲 ใช้บริการเว็บเพื่อช่วยแก้ไขข้อผิดพลาดในการสะกดศา											
	ายงานข้อขัดข้องไปยัง Go	ogle โดยอัตโนมัติ										
<mark>ส่งค</mark> ำขอ " ไ ม่ติดตาม" 1	vร้อมกับการเข้าชมของคุณ	i.										
ผ่านและฟอร์ม												
🛿 เปิดใช้งานป้อนอัตโนมัย	ดิเพื่อกรอกฟอร์มบนเว็บด้ว	ยการคลิกเพียงครั้งเดีย	จัดการการตั้งค่าป้อนอัง	ดโนมัติ								
🖞 เสนอการบันทึกรหัสผ่า	แเว็บของคุณ <mark>จัดการรหัส</mark> ผ	inu										
หาเว็บ												
นาดแบบอักษร: ขน	าดกลาง 🔻	กำหนดค่าแบบอักษร.										
ารชุมหน้าเว็บ: 100)% ▼											
บข่าย												
oogle Chrome กำลังใช้ก เปลี่ยนการตั้งค่าพร็อกซี	ารตั้งค่าพร้อกซีระบบของค	าอมพิวเต <mark>อร์เพื่อเชื่อมต่อ</mark>	กับเครือข่าย									
	ผ่านและฟอร์ม ยี่ เปิดโข่งานป้อนอัตโบมัย ยี่ เสนอการบันทึกรหัสผ่า หาเร็บ นาดแบบอักษร: ขณ ารชุมหนักเร็น: 100 มข่าย เปลี่ยนการสังศาพซ็อกซี เปลี่ยนการสังศาพซ็อกซี	 ผ่านและฟอร์ม เปิดใช่งานป้อนอัดโนภัติเพื่อกรอกฟอร์มบนเร็บต่อ เสนอการบันทึกรทัสผ่านเร็บของคุณ จัดการรทัสผ หาเร็บ นาดแบบอิกษร: ขนาดกลาง ● กรรุมหน้าเร็ม: 100% ● บข่าย ioogle Chrome ก่าสังไข่การดังค่าหรือกซี่ระบบของผ เปลี่ยนการดังค่าหรือกขี 	 ผ่านและฟอร์ม ปี เปิดโข่งานป้อนอัดโนมัติเพื่อกรอกฟอร์มบนเว็บด่วยการคลิกเพียงครั้งเดียะ สนอการบันทึกรทัสผ่านเว็บของคุณ จัดการรทัสผ่าน หาเร็บ นาดแบบอิกษร: ขนาดกลาง ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรทัส ภารบันทึกรที่สะทรบัสธ์ ภารบันทึกรที่สะเทรง ภารบันทึกรที่สะที่ระบบของคอมพิวเตอร์เพื่อเชื่อมต่อ เปลี่ยนการตั้งค่าหรือกขี 	<mark>ต่านและฟอร์ม</mark> 2ี เปิดโข้งานป้อนอัตโบมัติเทือกรอกฟอร์บบนเว็บด่วยการคลิกเพียงครั้งเดียว จิตการการตั้งค่าป้อนอั 2ี เสนอการบ้านที่กรทัสต่านเว็บของคุณ จิตการราไสต่าน หาเร็บ นาดแบบอีกษร: ขนาดกลาง ♥ กำหนดคำแบบอีกษร ารรุ่มหน้าเว็บ: 100% ♥ มข่าย เออgle Chrome กำสังใช้การตั้งค่าหรือกขี่ระบบของคอมพิวเตอร์เพื่อเนื่อมต่อกับเครือข่าย เปลี่ยนการตั้งค่าหรือกขี	ผ่านและฟอร์ม 2) เปิดโข้งานป้อนอัตโบมัติเทือกรอกฟอร์บบนเว็บด้วยการคลิกเพียงครั้งเดียว จิตการการตั้งค่าป้อนอัตโบมัติ 2) เสนอการบันทึกรทัสผ่านเว็บของคุณ จิตการราสัสผ่าน หาเร็บ นาดแบบอิกษร: ขนาดกลาง ♥ กำหนดค่าแบบอิกษร ารรุ่มหน้าเว็บ: 100% ♥ มข่าย เออgle Chrome กำสังใช้การตั้งค่าหรือกซี่ระบบของคอมพิวเตอร์เพื่อเชื่อมผ่อกับเครือข่าย เปลี่ยนการตั้งค่าหรือกขี							

7. คลิก LAN settings



8. ตั้งค่า proxy server เป็น ip address ของเครื่อง server ตัวอย่างเช่น ip 10.199.121.61 port 80 แล้วกด OK

Automatic con use of manual	figuration may over settings, disable au	rride man utomatic c	ual setting	gs. To ensure the ion.
Automatica	lly detect settings			
Use autom	atic configuration s	cript		
Address				
Use a prox dial-up or V	y server for your L/ PN connections).	AN (These	e settings	will not apply to
Address:	10.199.121.61	Port:	80	Advanced
Bypass	proxy server for lo	cal addre	sses	

9. ไปที่ Menu "Proxy" เลือกหัวข้อ intercept --> intercept on



เลือกเว็บไซต์ที่ต้องการ



11. ข้อมูลจะปรากฏโดยมีรายละเอียดดังภาพ ซึ่งเราจะสามารถตรวจสอบข้อมูลที่ส่งการร้องขอมาและ สามารถกระทำการใด ๆ กับข้อมูลนั้นได้



12. หากไม่เปลี่ยนแปลงข้อมูลใด ๆ แล้วกดปุ่ม Forward จะเป็นการส่ง Response กลับไป



13. ถ้าต้องการเปลี่ยนแปลงข้อมูล เช่น เปลี่ยนเป้าหมายจาก google.com เป็น youtube.com

Burp Suite Free Edition v1.6.29 -	
Burp Intruder Repeater Window Help	
Intruder Repeater Sequencer Decoder Comparer Extender Options	Alerts
Target Proxy Spider Scanner	
Intercept HTTP history WebSockets history Options	
Request to https://www.youtube.com:443 [216.58.221.238]	
Forward Drop Intercept is on Action Comment this item	:
Raw Params Headers Hex	
<pre>bst www.youtube.com Connection: keep-alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Upgrade=Insecure=Requests: 1 User-Agent: Mosilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko Chrome/46.0.2490.71 Safari/537.36 Accept-Language: gip, deflate, sdch Accept-Language: th=TH,th;q=0.8,en;q=0.6 Coohie: YSC=33YySx5A34, VISITOR_IMF01_LIVE=bxsWK9E91XA; wide=1; drv=590a5cd4461984d66d28de0de3834a58e30EAAAAdGxpcGnYEy2WHA==; PREF=fl=500000004f5=30</pre>	
? < + > Type a search term	0 matches

14. เมื่อกด Reward การตอบกลับจะกลายเป็น youtube.com

