Práctica Seguridade Informática: Métodos GET, POST + Proxy Burp Suite



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- Métodos GET e POST
- PortSwigger
- Burp Suite Community Edition

1. Configuración de rede

Na contorna gráfica abrir un terminal e executar:

kali@kali:~\$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

kali@kali:~\$ ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de rede: loopback(lo) e interna(eth0).

kali@kali:~\$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.

root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo networkmanager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflicto con este xestor.

root@kali:~# ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.

root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.

2. Crear formulario: arquivo index.php

kali@kali:~\$ mkdir /home/kali/web #Crear cartafol /home/kali/web, o cal será o DocumenRoot do noso servidor web, é dicir, será o cartafol por defecto que publicará o noso servidor web.

kali@kali:~\$ cat > /home/kali/web/index.php <<EOF #Crear arquivo que será visitado por defecto no noso servidor web. Este arquivo conteń o formulario co cal imos a probar os métodos GET e POST.

```
<?php
```

```
if(isset(\$_POST['user'],\$_POST['password'])):
  \$ POST['user'];
  \$password=\$ POST['password'];
  echo "<div class='metodo'>";
  echo "<h1>Método POST</h1>";
  echo "<h2>Usuario: ".\$user."<br>";
  echo "<h2>Contrasinal: ".\$password."<br>";
  echo "</div>";
elseif(isset(\$_GET['user'],\$_GET['password'])):
  \$ GET['user'];
  \$password=\$_GET['password'];
  echo "<div class='metodo'>";
  echo "<h1>Método GET</h1>";
  echo "<h2>Usuario: ".\$user."<br>";
  echo "<h2>Contrasinal: ".\$password."<br>";
  echo "</div>";
endif;
?>
<!DOCTYPE html>
<html>
  <head>
    <title>Formulario-GET-POST-Proxy</title>
    <style>
      .mtop0{margin-top:0px;}
      .mtop10{margin-top:10px;}
      .center{position: absolute;left: 50%;top: 50%;}
      .estilo,.metodo{border:1px dashed black;border-radius:10px; padding: 14px 14px;
      background-color:lightcyan;}
      .metodo{background-color:yellow;}
    </style>
  </head>
  <body>
    <div class='center estilo'>
      <h2 class='mtop0'>Autentificación</h2>
      <form>
      <!--<form method='GET'>-->
      <!--<form method='POST'>-->
        <input type="text" name="user" placeholder="Usuario" autofocus required>
        <br>
        <input class='mtop10' type="password" name="password" placeholder="Contrasinal" required>
        < br >
        <input class='mtop10' type="submit" value="Entrar">
      </form>
    </div>
  </body>
</html>
EOF
```

3. Lanzar e acceder ao servidor web (localhost)

kali@kali:~\$ sudo php -S localhost:80 -t /home/kali/web & #Executar en segundo plano (&) cos permisos de root(administrador) o comando *php -S localhost:80 -t /home/kali/web*, o cal activa no porto TCP 80 un servidor web php sendo /home/kali/web o DocumentRoot publicado.

kali@kali:~\$ firefox http://localhost:80 #Lanzar o navegador firefox na URL http://localhost no porto TCP 80, realizando a execución en primer plano, é dicir, acceder ao servidor web php do paso anterior.

Unha vez que accedamos á páxina paramos a execución do comando anterior premendo Ctrl+C no terminal onde executamos o comando firefox

4. Lanzar e acceder ao servidor web (192.168.120.100)

kali@kali:~\$ sudo php -S 192.168.120.100:80 -t /home/kali/web & #Executar en segundo plano (&) cos permisos de root(administrador) o comando *php -S 192.168.120.100:80 -t /home/kali/web*, o cal activa no porto TCP 80 un servidor web php sendo /home/kali/web o DocumentRoot publicado.

kali@kali:~\$ firefox http://192.168.120.100:80 & #Lanzar o navegador firefox na URL http://192.168.120.100 no porto TCP 80, realizando a execución en segundo plano (&), é dicir, acceder ao servidor web php do paso anterior.

5. Formulario: Método GET

- A. Introducir credenciais (usuario/contrasinal) no formulario, por exemplo usuario *kali* e contrasinal *abc123*.
- B. Premer no botón Enviar

Podemos observar no código do arquivo index.php que na etiqueta <form> non está definido ningún método o que equivale ao método GET, é dicir, se non se indica método por defecto o envío do formulario farase mediante o método GET. Que acontece coa URL? Agora aparecen os parámetros na propia URL, é dicir, podemos ver os valores das variables user e password na propia URL separadas mediante o caracter &: http://192.168.120.100/?user=kali&password=abc123.

C. Modificar o código do arquivo index.php para que o método a empregar no formulario sexa o método GET, é dicir, comentar a liña 36 e descomentar a liña 37:

<!--<form--> <form method='GET'> <!--<form method='POST'>-->

D. Realizar de novo os pasos 5A e 5B

Podemos observar que agora no código do arquivo index.php na etiqueta *form* está definido o método GET. Que acontece coa URL? Agora aparecen os parámetros na propia URL, é dicir, podemos ver os valores das variables user e password na propia URL separadas mediante o caracter &: http://192.168.120.100/?user=kali&password=abc123.

- E. Modificar a URL como segue: http://192.168.120.100/?user=alumnado&password=12345678
- F. Premer Enter na URL. Que acontece?

6. Formulario: Método POST

A. Modificar o código do arquivo index.php para que o método a empregar no formulario sexa o método POST, é dicir, comentar a liña 37 e descomentar a liña 38:

```
<!--<form-->
<!--form method='GET'>-->
<form method='POST'>
```

- B. Abrir unha nova lapela e acceder á URL http://192.168.120.100:80
- C. Realizar de novo os pasos 5A e 5B

Podemos observar que agora no código do arquivo index.php na etiqueta *form* está definido o método POST. Que acontece coa URL? Agora non aparecen os parámetros na propia URL, é dicir, non podemos ver os valores das variables user e password na propia URL separadas mediante o caracter &

7. Proxy burpsuite

- A. Imos visualizar as variables introducidas co método POST mediante o Proxy burpsuite. Así, abrir un novo terminal e executar:
 - kali@kali:~\$ burpsuite & #Executar o proxy burpsuite en segundo plano (&).

B. Aceptar Todo

	Your JRE appears to be vers Burp has not been fully test	ion 11.0.13 from Debian ed on this platform and you may	experience problems.		
	Don't show again for this	s JRE	ок		
				J Tr	
	Burp Suite	Community Edition		3	
ms a	and Conditions				
se re 1s.	ead the following terms and con	ditions carefully, and indicate w	ether you accept their		
se Bu rred t censo ce Co	urp Suite Community Terms an to in it ("Terms") constitute the or") will grant to any user ("Lice mmunity Edition ("Burp Suite (d Conditions of Supply together e terms and conditions on which nsee") a licence to use the softw Community Edition" or the "Soft	with the documents PortSwigger Ltd Ire comprising Burp ware"), following		
follo	nce of an order as detailed below	r. Terms:			
e Bu	rrp Suite Community Licence Ag	preement;			
e Ge	eneral Terms and Conditions;				
e Pri	ivacy Policy; and				
e Pri	ivacy Policy; and p improve Burp by submitting a	nonymous feedback about its pe	formance		
Help	ivacy Policy; and p improve Burp by submitting a	nonymous feedback about its pe	formance		
Help	ivacy Policy; and p improve Burp by submitting a	nonymous feedback about its pe	formance		
Help	ivacy Policy; and p improve Burp by submitting a	nonymous feedback about its pe	formance cline IAccept		
Help	ivacy Policy; and p improve Burp by submitting a	nonymous feedback about its pe I De Burp Suite Communit	formance Line LAccept yEdition v2021.10.2		•
e Pri Help We	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi	nonymous feedback about its pe I De Burp Suite Communit ty Edition. Use the options belov	formance cline IAccept y Edition v2021.10.2 vto create or open a project.		Burp Si
e Pri Help We <i>No</i>	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ste: Disk-based projects are only	nonymous feedback about its pe I De Burp Suite Communit ty Edition. Use the options below y supported on Burp Suite Profes	formance cline I Accept y Edition v2021.10.2 vto create or open a project. sional.		Burp Su Community E
We No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only	nonymous feedback about its pe I De Burp Suite Communit ty Edition. Use the options below <i>y supported on Burp Suite Profes</i>	formance cline I Accept y Edition v2021.10.2 y to create or open a project. sional.		BurpSu Community E
We No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project	nonymous feedback about its pe I De Burp Suite Communit ty Edition. Use the options below	formance cline IAccept y Edition v2021.10.2 r to create or open a project. sional.		S Burp St Community E
We	p improve Burp by submitting a p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project	nonymous feedback about its pe I De Burp Suite Communit ty Edition. Use the options below <i>y supported on Burp Suite Profes</i>	formance cline I Accept y Edition v2021.10.2 rto create or open a project. sional.		Burp Si Community E
We No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project) New project on disk Name File	nonymous feedback about its pe	formance cline I Accept y Edition v2021.10.2 y to create or open a project. sional.		Some of the second seco
We	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project) New project on disk Name File	nonymous feedback about its pe	formance cline IAccept y Edition v2021.10.2 (to create or open a project. sional.		S Burp St Community E
We No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project) New project on disk Name File) Open existing project	nonymous feedback about its pe	formance cline IAccept y Edition v2021.10.2 rto create or open a project. sional.	File	S Burp St Community E
We No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi- ste: Disk-based projects are only Temporary project New project on disk Name File) Open existing project	nonymous feedback about its pe	formance cline I Accept y Edition v2021.10.2 rto create or open a project. sional.	File	Community E
Wee No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project New project on disk Name File) Open existing project	nonymous feedback about its pe	formance cline IAccept y Edition v2021.10.2 vto create or open a project. sional.	File	S Burp St Community E
Wee No	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi- ote: Disk-based projects are only Temporary project New project on disk Name File) Open existing project	nonymous feedback about its pe	formance cline Accept y Edition v2021.10.2 rto create or open a project. sional.	File	Community E
We No	ivacy Policy; and p improve Burp by submitting a elecome to Burp Suite Communi ote: Disk-based projects are only Temporary project New project on disk Name File) Open existing project	nonymous feedback about its pe	formance cline IAccept y Edition v2021.10.2 vto create or open a project. sional.	File	S Burp Su Community E
Wee Pri-	ivacy Policy; and p improve Burp by submitting a elcome to Burp Suite Communi ote: Disk-based projects are only Temporary project New project on disk Name File Open existing project File	nonymous feedback about its pe	formance cline Accept y Edition v2021.10.2 to create or open a project. sional.	File	Choose f
We No	ivacy Policy; and p improve Burp by submitting a elecome to Burp Suite Communi ote: Disk-based projects are only Temporary project New project on disk Name File Open existing project File	nonymous feedback about its pe	formance cline Accept / Edition v2021.10.2 / to create or open a project. sional.	File	S Burp Su Community E Choose f

		Burp Suite Co	ommunity E	dition v2021.10.2			8	
Ð	Select the configuration that you v	vould like to load for t		S Burp Suite Community Edition				
	🔘 Use Burp defaults							
	O Use options saved with project	rt						
	O Load from configuration file				File			
		File:				Choose file		
	Default to the above in future							
	Disable extensions							
					Cancel B	ack Start Burp		
							'	
		Burp Suite Comm	unity Editio	n v2021.10.2 - Ten	nporary Project		00	
		Window Help		D	Lateral and	B		
rp	Project Intruder Repeater Dashboard	Target		ProxV	Intruder	Kepea	ter	

Burp Suite - a guided video tour

C. Seleccionar a lapela Proxy e executar o navegador embebido (Open browser)

Getting started with Burp Suite

urp	Project	Intruder	Repeater	Window	Help				
Se	quencer	De	coder	Compar	er	Logger	Ext	tender	P
	Dasl	nboard		Ta	rget		Ргоху		
Inter	cept	HTTP histo	ory We	bSockets his	story	Options			
F	- manual		Deen	Interes		0 - 41 -		Onen Re	
	Use Bu	rp's em	bedded	Interce	ept is on	Actio		Use a	diffe
	Use Bu browse	rp's em er	bedded			Actio		Use a	diffe
	Use Bu browse	rp's em er	bedded		BurpSuite	Actio		Use a You'll ne	diffe ed to pe
	Use Bu browse	rp's em er need to co	bedded nfigure your		Burp Suite	Actio		Vou'll ne steps to o settings.	ed to per configu For tes
	Use Bu browse There's nc proxy sett embeddec start testi	rp's em r need to co ings manua Chromium ng right aw	bedded nfigure your illy. Use Burp browser to ay.		BurpSale	Actic		Vou'll ne steps to (settings, also need certificat	diffe ed to pe configu For tes I to inst e.
	Use Bu browse There's nc proxy sett embeddec start testi	rp's em r r need to co ings manua Chromium ng right aw	bedded nfigure your illy. Use Burp browser to ay.		BarySale	Action		Use a You'll ne steps to settings. also neec certificat	ed to per configu For tes to inst e.



D. Realizar de novo os pasos 6B e 6C

o Suite x +	Surp Suite Community Edition v2021.10.2 - Temporary Project								
	Burp Project Intruder Repeate	r Window Help							
X (i) 192.168.120.100	Sequencer Decoder	Comparer	Logger Extender	Project options	User options	Learn			
	Dashboard	Target	Proxy	Intruder	Repeat	ter			
	Intercept HTTP history V	VebSockets history O	ptions						
	A Designed to here //102.158.120.100.1	20							
	V Request to http://192.168.120.1003	50							
	Forward Drop	Intercept is on	Action Open	Browser Comment ti	his item 🛛 🤎	HTTP/1 (
	Pretty Raw Hex 🚍 \n	=				-			
	1 GET (HTTP/1 1								
	2 Host: 192.168.120.100								
	3 Upgrade-Insecure-Requests:	1 NT 10 0. WinCA.	weat and webyit (507 of	(KUTMI] (he Ceeles) Che	(05 0 4620 60	-			
	Safari/537.36	ndows NT 10.0; W1064;	x64) Applewebkit/53/.5	5 (KHIML, LIKE GECKO) Chr	ome/95.0.4638.69				
	5 Accept:					9			
Keep up with the	text/html, application/xhtml	+xml,application/xml;	q=0.9,image/avif,image/	vebp,image/apng,*/*;q=0.8	,application/signed	l-exch			
late at universality	ange; v=b3; q=0.5 6 Accept-Encoding: gzip. defl:	ate							
latest vulnerabili	7 Accept-Language: en-US, en; q	=0.9							
	8 Connection: close								
	10								

Intercept	cer Decoder	Con	nparer	Logger	Exte	nder	Pr	oject optio	าร	User opti	ons	Learn	
intercept	Dashboard	WebCashet	Target	Ontines	Proxy			Intrude	r		Repeater		
iltor: Listi-	HITPhistory	webSocket	shistory	Options									6
inter. Hidir	ng CSS, image and general	binary cont	ent							1			(?
# ^	Host	Method		URL		Params	Edited	Status	Length	MIME type	Extension		
http http	://192.168.120.100 ://192.168.120.100	GET	;										
http	://192.168.120.100	GET	1					200	894	HTML	• 755.2	Formul	ari
http	://192.168.120.100	POST	/tavicon.ico			1		200	990	HTML	100	404 No Formul	t F
Request	Response					- 🖸	INS	PECTOR				?	>
Pretty R	aw Hex 🚍 \n	≡					Rei	quest Attril	outes				~
1 POST / 2 Host: 3	HTTP/1.1 192.168.120.100						Во	dy Paramet	ers (2)				~
4 Cache-(5 Upgrade	Control: max-age=0 e-Insecure-Requests: bttp://192.168.120	1					Rei	quest Head	ers (12)				~
7 Content	t-Type: application/	x-www-for	m-urlencode	ed	w. Liz'i		Re	sponse Hea	ders (5)				~
i user=ka	ali&password=abcl23.												
	 O proxy burpst O navegador e (127.0.0.1:808) Todas as petici Por defecto ter calquera petici quixeramos qu Intercept a Off Unha vez intro escoller a com 	uite está mbebido 0). .óns do o nos no F .ón do cl e tivera para pe ducidas unicació	activo po o xa está cliente qu Proxy \rightarrow In liente pas lugar a p ermitir too as crede on POST \in	or defecto configurad nedaran ga ntercept C se a través petición po das as peti nciais pod o visualizan as variable	na int lo para ardada)n, polo do pro demos icións emos o r as va	erface l a facer s na lar o cal de oxy e po descar do clier observa riables	loopba petici pela H ebemo pida c rtala p nte pa r en H introo	ack na l óns a tr TTP Hi s prem omunic premen ra revis HTTP H ducidas	P 127. ravés d story. er en F arse co do en I salas lo istory a . A mai	0.0.1 e n o proxy h o servido Drop. Tar go na laj as petició ores se t	o porto l purpsuite para perr r web. So nén pode pela HTT jons realiz iveramo	mitir o e non eriamo P His zadas s Inte	D8 JU D8 JU D8 JU



Dn