CHANDIGARH UNIVERSITY UNIVERSITY INSTITUTE OF ENGINEERING DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



Submitted By:	Submitted To:
Subject Name	WMS Lab
Subject Code	20CSP-338
Branch	BE-CSE
Semester	5 th Sem

LAB INDEX

NAME: UID: SECTION:

SUBJECT NAME: SUBJECT CODE: 20CSP-338

Sr.	Program	Date		Eva	luatio	n	Sign
No			LW	VV	FW	Total	
			(12)	(10)	(8)	(30)	





Worksheet Experiment 1

Student Name: Branch: CSE Semester: 5th Sem Subject Name: WMS Lab UID: Section/Group: Date of Performance: Subject Code: 20CSP-338

1. Aim/Overview of the practical:

Open any website on computer system and identify http packet on monitoring tool like Wireshark.

2. Objective:

To analyse http traffic.

3. Introduction:

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

4. Steps/Method:



1. Open Wireshark

- 2. Click on "Capture > Interfaces". A pop-up window will display.
- 3. You'll start capture traffic that goes through your ethernet driver.





- 4. Visit the URL that you wanted to capture the traffic from.
- 5. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
- 6. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.
- 5. Outcomes:

ttp 1017	Time					(W) (****
1017	Time					
1017	Tarine.	Source	Destination	Protocol	Length Info	
	234.724248	172.18.40.87	13.224.22.59	HTTP	274 GET //MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fv%3D%3D HTTP/1.1	
27	234.739881	13.224.22.59	172.18.40.87	OCSP	359 Response	
77	234.783542	172.18.40.87	143.204.253.56	HTTP	304 GET /MFQwUjBQME4wTDAJBgUrDgMCGgUABBSIfaREXmfqfJR3TkMYnD705MhzEgQUnF8A36oB1zAr0IiiuG1KnPIRkYMCEwZ%2F1EoqJ83z%2BsKuKwH5CO65xMY%3D HTTP/1.	.1
83	234.798589	143.204.253.56	172.18.40.87	OCSP	162 Response	
16	234.859658	172.18.40.87	143.204.253.59	HTTP	309 GET /MFQwUjBQME4wTDAJBgUrDgMCGgUABBRPWaOUU8%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMhTTsvAyUlC4IWZzHshBOCggCEwZ%2FlFeFh%2Bisd96yUzJbvJmLVg0%30 HTT	FP/1.1
23	234.879935	143.204.253.59	172.18.40.87	OCSP	1480 Response	
me	1017: 274 bv	:es on wire (2192 b)	its). 274 bytes captur	ed (2192 bi	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0	
ne cc	1017: 274 by 4 2 24 dd 7 7	tes on wire (2192 b) fa e0 be 03 76 9a 08 9a 6a 00 20	its). 274 bytes captur 30 88 00 45 00 NS- 12 32 57 4 co	ed (2192 bi	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0	
ne cc 01	1017: 274 by 4e 24 dd 77 64 04 44 40 5 b er 66 44 40	tes on wire (2192 b) fa e0 be 03 76 9a 00 80 06 00 00 ac 5 be af 7 63 75	its). 274 bytes captur 30 08 00 45 00 - 165 12 28 57 00 40	ed (2192 bi w v 0 9 & p	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- NP PP	
ne cc 01 16 04	1017: 274 by 4 24 dd 77 4 04 0d 44 40 5 3b ec 06 00 4 05 f9 7a 00	es on wire (2192 b) fa e0 be 03 76 9a 08 80 06 00 00 ac 50 be af 7f 63 f5 06 47 45 24 20 2f	its). 274 bytes captur 30 08 00 45 00 - 115 12 28 57 04 00 - 00 26 b5 70 50 18 - ; 26 4d 45 6f 77 ;2	ed (2192 bi w·····(W P·····(W P·····(%) GE T //ME	bits) on interface \Device\NPF_10DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- P- PP- MEGW	
ne 01 16 04 53	1017: 274 bv - 4e 24 dd 77 64 6d 44 40 5 3b ec 66 00 4 05 f9 7a 00 44 42 47 4d	tes on wire (2192 b) fa e0 be 03 76 9a 00 80 06 00 00 ac 30 be af 7 f6 3 f5 30 be 74 5 54 20 2f 55 177 51 56 a 41	its). 274 bytes captur 30 08 00 45 00 - 115 12 28 57 0d e0	ed (2192 bi w · · · v 0 P · · c & p · · GE T //HE HCQW Q1A1B	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}. id 0 E- (Ա PP WEow Bgur	
ne 01 16 04 53 44	1017: 274 by - 4e 24 dd 77 L 04 04 44 0 - 3b ec 06 00 - 5 79 7a 00 - 44 22 47 4d - 67 4d 43 47	tes on wire (2192 b) fa e0 be 03 76 9a 08 00 60 00 ac 50 be af 7f 63 f5 45 51 77 51 6a 41 77 55 41 42 42 53	its). 274 bytes captur 30 08 00 45 00	ed (2192 bi w v. 0 @	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- P- PP- MEGw BgUr ZEGE	
me 01 16 04 53 44 57	1017: 274 by 4e 24 dd 77 64 9d 44 40 5 3b ec 66 00 05 45 7a 00 144 42 47 4d 67 4d 43 47 35 67 64 59	es on wire (2192 b) fa e0 be 03 76 9a 00 80 06 00 00 ac 50 be af 7 76 3 75 00 47 45 54 20 2f 45 51 77 51 6a 41 67 55 41 42 42 53 39 55 61 53 45	its). 274 bytes captur 30 08 00 45 00 - NG 12 28 57 00 e0	ed (2192 bi w - v 0 - (W P - c & p GE T //ME MEQW QjAJBg 5gUA BBSLw2 FgUA BBSLw2	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}. id 0 E- (W pP- MEOw BGUF WZGE Jjj	
ne 01 16 04 53 44 57 45	1017: 274 by 4 42 4 dd 77 6 4 04 44 40 5 3b ec 6 06 4 65 f9 7a 00 4 44 42 47 4d 4 67 4d 43 47 7 35 67 64 59 5 4 4e 74 6b	tes on wire (2192 b) fa e0 be 03 76 9a 08 00 60 00 ac 50 be af 7f 63 f5 45 51 77 51 6a 41 63 59 55 61 53 45 63 39 55 61 53 45 43 51 55 76 31 25	its). 274 bytes captur 30 08 00 45 00 116 12 85 70 40 60 00 26 b5 70 50 18 3; 24 42 6 75 57 25 50 44 45 67 55 72 50 61 61 4c 69 68 50 61 61 4c 69 68 50 7000 61 61 4c 69 68 50 7000	ed_ (2192 bi w· v.0. P c.%.p GE T //ME EQW QJAJBSLWZ SgUA BBSLWZ 	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP- MEGw BgUr WZ65 BJJ BJG	
ne 01 16 04 53 44 57 45 37	1017: 274 by 4 e 24 dd 77 64 6d 44 40 5 3b ec 06 00 8 44 42 47 4d 65 79 7a 00 8 44 42 47 4d 67 4d 43 47 7 35 67 64 59 5 54 4e 74 6b 7 54 48 34 62	tes on wire (2192 b) fa e0 be 03 76 9a 00 80 00 00 00 ac 500 47 45 54 20 2f 51 77 51 6a 41 67 55 41 42 42 53 39 55 61 53 45 41 51 55 76 31 25 57 31 55 76 31 25	its) 274 bytes capture 30 06 06 45 00 113 215 76 76	ed (2192 bi 	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- \P- \P- MEOW BQUP WZGE wZGE sljj B30C COMB	
ne 01 16 04 53 44 57 45 37	1017: 274 by 4 42 24 dd 77 4 44 04 44 40 5 3b ec 06 06 4 65 19 7a 06 4 44 24 74 4 42 44 43 47 5 54 44 74 6b 5 54 48 74 6b 5 54 48 74 62 7 64 98 44 62 5 76 69 44 63	es on wire (2192 b) fa e0 be 03 76 9a 08 00 60 00 ac 50 be af 7f 63 f5 45 51 77 51 6a 41 63 39 55 61 53 45 63 39 55 61 53 45 13 55 54 13 65 44 15 155 76 31 25 36 57 31 57 73 33 34 35 14 56 44	its) 274 bytes capture 30 86 45 60 115 12 85 70 60 84 60 15 12 85 70 81 31 7 72 50 81 31 7 7 24 42 67 55 72 506 61 46 67 55 72 506 61 61 46 64 64 64 64 64 61 61 44 63 61 11 44 63 51 71 44 44 63 51 71 44 45 35 11 44 63 51 71 44 45 35 71 44 45 35 71 44 45 35 71 44 45 35 71 44 45 35 71 44 45 35 71 44 44 45 35	ed (2192 bi w · · · · 0 P · · c & p · · · C & p · · · · C & T //HE · C & S · · · · · V · · · · · · · · · · · · · · · · · · ·	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP- %P- KEow BgUr &Z6E aLjj 830- COwg PMHI	
ne 01 16 04 53 44 57 36 45 37 36	1017: 274 by 2 42 4 dd 77 64 94 44 40 5 3b 65 60 8 44 424 44 65 7b 60 8 44 424 44 67 44 43 47 75 55 47 46 54 48 34 62 76 69 47 63 3 36 67 72 25	tes on wire (2192 b) fa e0 be 03 76 9a 06 80 06 00 06 05 55 00 47 45 54 06 41 55 57 15 16 41 167 55 41 42 42 53 39 55 61 31 45 53 57 51 53 45 39 55 61 31 45 53 55 77 33 34 45 15 33 64 20 34 42 0 34	its). 274 bytes capture 30 60 45 60 115 12 28 57 64 68 115 12 28 57 64 68 57 72 21 44 45 65 77 5006 44 57 5006 44 56 77 5006 32 42 33 36 67 Thitt 44 45 57 50 50 21 12 33 66 195 32 42 33 36 67 Thitt 46 <td< td=""><td>ed (2192 bi % · · · · · · · · · · · · · · · · · · ·</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E. \W PP. MEGW BQUF AZGE ALJJ D30C CQmg DMMI TT/</td><td></td></td<>	ed (2192 bi % · · · · · · · · · · · · · · · · · · ·	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E. \W PP. MEGW BQUF AZGE ALJJ D30C CQmg DMMI TT/	
me 01 16 04 53 44 57 36 45 37 36 45 37	1017: 274 bV 4e 24 dd 77 (04 dd 44 40 35 bc 06 00 60 5 19 7a 00 44 42 47 44 43 55 57 44 43 47 35 57 64 43 78 64 43 34 78 56 74 60 78 64 45 34 78 64 45 78 64 63 78 64 63 78 64 63 78 64 63 78 64 65 78 65 78 65 78 64 78 74 78 75 78 75 76 76 76 76 76 76 76 76 76 76 76 76 76	tes on wire (2192 b) fa e0 be 03 76 98 96 00 <t< td=""><td>its). 274 bytes capture 30 08 08 08 18 </td><td>ed (2192 bi</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP- VECw BgUr WZGE aLjj B30c CQwg DPHI TTF/ TTF/ TTF/ TTF/ TTF/ TTF/ TTF/ TTF</td><td></td></t<>	its). 274 bytes capture 30 08 08 08 18	ed (2192 bi	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP- VECw BgUr WZGE aLjj B30c CQwg DPHI TTF/ TTF/ TTF/ TTF/ TTF/ TTF/ TTF/ TTF	
me cc 01 16 53 44 57 36 37 36 31 20 65	1017: 274 by 4 c 24 d d77 6 4 c 24 d d77 6 4 c 34 d d77 10 4 c 4 d 44 d 5 b c c 06 60 14 4 4 2 47 4d 5 4 5 7 d 5 4 59 7 6 4 4 5 3 4 7 7 6 5 4 f 5 7 6 5 4 f 5 3 3 6 6 7 7 55 1 2 3 1 6 d 5 4 2 3 1 2 3 1 6 d 5 4 2 3 1 2 3 1 6 d 5 7 1 7 2 5 1 2 3 1 0 d 3 4 b 5 5 7 7 5 1 2 3 1 0 d 3 1 3	tes on.wire (2192 b) fa e0 b2 37 6 98 96 90 90 60 90 60 90 61 91	its) 274 bytes capture 30 86 96 16 93 14 93 93 14 93 93 14 93 96 16 96 16 96 16 96 16 16 16 36 Kee 16 16 16 16 16 16 16 16 16 16 16 16 16 16 36 Kee 16 16 16	ed (2192 bi w · · · v Ø · · Ø · · · · · (W P· · c & p · o E T //W KSW 05A38 gul ABSLw (C9U aSEaaL AQU v1X28 SMU W SNcQ CCQ c NokyM SNS 3D HTT · Con mectio -A1 ive · A */ · · · · · · · · ·	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E. (M MEON	
me ccc 011 64 53 44 57 45 37 45 37 45 37 45 37 65 67	1017: 274 bV 4e 24 dd 77 64 64 44 35 b c 64 b 64 36 c 67 67 63 55 57 68 59 56 64 59 36 67 63 53 52 54 67 64 53 52 54 67 64 53 52 54 67 63 53 52 53 66 73 53 66 64 53 55 54 67 63 53 52 12 23 36 64 73 33 66 73 33 64 54 56 56 56 56 74 34 74 44 44 44 44 44 44 44 44 44 44 45 45 56 56 74 34 74 44 44 44 44 <td>tes on wire (2192 b) fa e0 be 03 76 98 96 00 80 96 00 80 96 00 80 96 00 80 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 96 95 96 97 97 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 94 93 94 93 94 93 94 93 94 <t< td=""><td>its). 274 bytes capture 30 86 96 76 7 32 85 96 76 7 26 55 75 50 88 3 26 55 75 50 88 3 27 53 64 55 72 50 61 61 46 64 54 56 06/00 24 23 36 36 57 7 44 63 51 7 7 44 45 30 17 67 64 44 63 06/00 64 54 56 64 54 56 64 54 54 56 64 54 54 56 56 56 56 56 56 56 56 56 56 56 56 56 56 76 56 57 26 56 76 57 76 <td< td=""><td>ed (2192 bi w v. 0. p c.&.p. c.&.p. c.&.p. c. d. T //ME MEQw 0jADg SgLM B85Lw2 d. T d. d. T d. d. T d. d. T d. d. T d</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP. VECw BgUr wZ6E aljj B30c CQwg DPHI TTTT TTT TTT TTT TTT TTT TTT TTT TTT</td><td></td></td<></td></t<></td>	tes on wire (2192 b) fa e0 be 03 76 98 96 00 80 96 00 80 96 00 80 96 00 80 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 98 96 00 96 95 96 97 97 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 93 94 93 94 93 94 93 94 93 94 <t< td=""><td>its). 274 bytes capture 30 86 96 76 7 32 85 96 76 7 26 55 75 50 88 3 26 55 75 50 88 3 27 53 64 55 72 50 61 61 46 64 54 56 06/00 24 23 36 36 57 7 44 63 51 7 7 44 45 30 17 67 64 44 63 06/00 64 54 56 64 54 56 64 54 54 56 64 54 54 56 56 56 56 56 56 56 56 56 56 56 56 56 56 76 56 57 26 56 76 57 76 <td< td=""><td>ed (2192 bi w v. 0. p c.&.p. c.&.p. c.&.p. c. d. T //ME MEQw 0jADg SgLM B85Lw2 d. T d. d. T d. d. T d. d. T d. d. T d</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP. VECw BgUr wZ6E aljj B30c CQwg DPHI TTTT TTT TTT TTT TTT TTT TTT TTT TTT</td><td></td></td<></td></t<>	its). 274 bytes capture 30 86 96 76 7 32 85 96 76 7 26 55 75 50 88 3 26 55 75 50 88 3 27 53 64 55 72 50 61 61 46 64 54 56 06/00 24 23 36 36 57 7 44 63 51 7 7 44 45 30 17 67 64 44 63 06/00 64 54 56 64 54 56 64 54 54 56 64 54 54 56 56 56 56 56 56 56 56 56 56 56 56 56 56 76 56 57 26 56 76 57 76 <td< td=""><td>ed (2192 bi w v. 0. p c.&.p. c.&.p. c.&.p. c. d. T //ME MEQw 0jADg SgLM B85Lw2 d. T d. d. T d. d. T d. d. T d. d. T d</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP. VECw BgUr wZ6E aljj B30c CQwg DPHI TTTT TTT TTT TTT TTT TTT TTT TTT TTT</td><td></td></td<>	ed (2192 bi w v. 0. p c.&.p. c.&.p. c.&.p. c. d. T //ME MEQw 0jADg SgLM B85Lw2 d. T d. d. T d. d. T d. d. T d. d. T d	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- .pP. VECw BgUr wZ6E aljj B30c CQwg DPHI TTTT TTT TTT TTT TTT TTT TTT TTT TTT	
ne 01 16 04 53 44 57 36 45 37 36 45 37 36 45 37 45 37 37 36 45 37 37 36 37 37 37 36 37 37 37 37 37 37 37 37 37 37 37 37 37	1017: 274 by 4 c 24 d d 77 6 d c 24 d d 77 6 d c 34 d d 78 10 d c 4 d 4 4 4 6 d 4 d 4 4 6 d c 4 4 4 6 d c 4 4 6 d c 5 f 7 8 d c 7 d d 3 3 7 d 6 5 f 7 6 d 4 3 3 d c 7 d d 3 3 7 d 6 f 7 7 d 6 4 f 6 5 d a 7 7 d 6 4 f 6 5 f 7 7 d 6 4 f 6 7 d 7 8 d 7 7 d 6 4 d 6 7 d 7 7 d 7 8 d 7 7 d 7 8 d 7 7 d 7 8 d 7 7 d 7	tes on.wire (2192 b) fa e0 b2 37 6 98 96 90 e0 90 60 90 e2 50 ba 47 45 51 71 53 41 21 53 63 39 55 61 53 42 42 53 53 57 73 33 43 51 43 54 42 53 34 36 43 54 42 53 34 36 43 54 42 53 34 26 43 34 35 14 36 43 56 43 56 44 26 73 44 27 33 44 25 33 44 26 37 47 40 64 56 63 24 41 64 52 24 40 65 26 26 26 26 26 26 26 26 26 26	its) 274 bytes capture 30 86 04 56 116 12 85 70 60 18 ; 12 85 70 60 18 ; 12 85 70 61 81 7 7 24 45 67 55 72 506 64 45 56 72 506 64 45 54 52 52 516 64 63 144 65 65 72 506 52 24 33 63 57 64 64 63 53 14 63 51 71 74 44 64 63 51 71 74 44 63 63 14 63 14 64 63 14 64 63 14 64 63 14 64 63 14 64 63 14 64 64 64	ed (2192 bi w · v 0 B · c .8. p · GE T //We HEQw QJAJBg JQAJBSLW (GU 4552a) MIL WSJNQ CCQ C 0RbyM S30% JD HTT (CO n ectio -Al ive · A */ · UJser : Mi crosoft torsoft Coop F1/10.8	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 - E. (H - pow pow BgUr BgUr BGE aljj B302 CONG	
me ccc 01 16 04 53 44 57 45 36 45 37 45 36 43 43 43 43 43 43 43 43 43 43	1017: 274 bV 4e 24 dd 77 94 64 44 39 bc 67 95 57 69 69 64 42 47 46 54 67 64 59 76 65 57 56 64 59 76 64 59 56 67 54 34 64 54 56 57 56 47 36 67 54 34 56 57 56 47 36 56 77 36 56 77 36 56 77 36 56 77 36 56 77 36 56 77 37 36 57 76 74 36 56 57 78 36 56 57 78 36 56 57 78 36 57 57 78 36 57 78 36 57 75 78 74	tes on wire (2192 b) fa e0 be 03 76 98 96 90 60 80 96 90 80 96 90 80 96 90 80 96 90 80 96 90 80 96 90 80 96 90 <t< td=""><td>its). 274 bytes capture 30 86 96 96 71 20 87 96 71 72 21 87 96 86 71 22 85 96 71 72 24 42 67 55 72 50 61 61 64 64 05 06 42 32 77 59 63 1.1 44 54 54 50 21 1.11 45 34 74 69 67 1.51 45 34 74 69 67 1.51 45 45 45 45 45 1.41 45 45 45 45 45 45 46 46 46 3.51 4.11 1.11 72 27 2.44 4.24 4.24 1.11 73 26<</td><td>ed (2192 bi % ··· v.0·· % ···</td><td>bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- E- yP- MEGW BgUr &CE aljj BaBe CQ08</td><td></td></t<>	its). 274 bytes capture 30 86 96 96 71 20 87 96 71 72 21 87 96 86 71 22 85 96 71 72 24 42 67 55 72 50 61 61 64 64 05 06 42 32 77 59 63 1.1 44 54 54 50 21 1.11 45 34 74 69 67 1.51 45 34 74 69 67 1.51 45 45 45 45 45 1.41 45 45 45 45 45 45 46 46 46 3.51 4.11 1.11 72 27 2.44 4.24 4.24 1.11 73 26<	ed (2192 bi % ··· v.0·· % ···	bits) on interface \Device\NPF {0DFAC098-E8D4-418F-98FF-59C179578016}, id 0 E- E- yP- MEGW BgUr &CE aljj BaBe CQ08	







Learning outcomes (What I have learnt):

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe single small file (e.g., simple html file) request/response behavior and the request/response behavior for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behavior. Observe request/response behavior for a page that needs authentication.

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30

Worksheet Experiment 2

Student Name: Branch: CSE Semester: 5th Sem Subject Name: WMS Lab UID:

Section/Group: Date of Performance: Subject Code: 20CSP-338



🖂 egov@cumail.in





1. Aim/Overview of the practical:

Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.

2. Objective:

To test HTML and XSS injection.

3. Steps/Method:

HTML Injection

1. Open website : OWASP Mutillidae II: Web Pwn in Mass Production

(URL:http://128.198.49.198:8102/mutillidae/index.php?page=documentation/usageinstruct ions.php)

- 2. Now, we'll be redirected to the web page which is suffering from an HTML Injection vulnerability which allows the user to submit his entry in the blog.
- 3. On the left-hand side, click on OWASP 2017 A1-injection(others) HTML injection Add to your blog
- 4. Welcome to blog window will appear on the screen. Now, let's try to inject malicious code. Enter the HTML code inside the given text area in order to set up the HTML attack.







XSS Injection:

1. Open the link https://xss-game.appspot.com/level1 (or Google XSS game website). 2. If the search field is vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script as shown below: "<script>alert ("Hello") </script>"

- 3. Then after clicking on the "Search" button, the entered script will be executed. The script typed into the search field gets executed. This just shows the vulnerability of the XSS attack.
- 4. Outcomes:

HTML Injection

CONT_20CSP-338::WEB	AND M 🛛 M Wireshark - shiwanisinghal212@	CONT_20CSP-338:WEB AND MC M Wireshark - shiwanisinghal212 V Classic Old Song Mashup N S Welcome to Chandigarh Universi S Chandigarh University Managerr 128.198.49.198.8102/mutillid x + v - C X						
⊲ ⊳ C	□ ▲ Not secure 128.198	49.198:8102/mutillidae/index.php?page=d			😳 🔺	★ ₹ ⊡		
M Gmail 🕥 Summer 1	fraining II 🛞 Internshala Trainings (A)	💲 Software Testing 🏾 👩 Shiwani-Singhal (Sh	. 🏹 naukri 🚯 Angular VAC 🙆 ML					
							-	
		OWASP Mutillidae	e II: Web Pwn in Ma	ass Producti	on			
	Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In							
	Home Login/Re	aister Togale Hints Show Popup Hin	nts Toggle Security Enforce SSL Re	eset DB View Log View	/ Captured Data		11	
	A1 - Injection (SOL)		······································	,,			11	
OWASP 2017	A1 - Injection (Other)	Application Log Injection	Usage Instruction	s				
OWASP 2013	A Projection (other)	Buffer Overflow						
OWASP 2010	Session Management	Cascading Style Injection						
OWASP 2007	A3 - Cross Site Scripting (XSS)	CBC-bit Flipping						
Web Services	A4 - Broken Access Control	Command Injection	s from the OWASP Top 10 2013, 20	010 and 2007 in PHP. Add Information disclosure vul	ditionally nerabilities have			
HTML 5	A5 - Security Misconfiguration	Frame Source Injection						
Others	A6 - Sensitive Data Exposure	HTML Injection (HTMLi)	Add to your blog					
others		HTMLi via HTTP Headers	Browser Info					
Documentation	(CSRF)	HTMLi Via DOM Injection	DNS Lookup					
Resources	A9 - Using Components with Known	HTMLi Via Cookie Injection	Pen Test Tool Lookup					
	Vulnerabilities	HTTP Parameter Pollution	• Text File Viewer	ages				
Want to Help?	A10 - Underprotected APIS	JavaScript Injection	User Info (SQL)	ide security and secure				
Traile to Holp !		JavaScript Object Notation (JSON)	User Info (XPath)	P requests to HTTPS				
You		Parameter Addition	Set Background Color					
Video Tutorials		XML External Entity Injection	HIMLS Web Storage					
Theo futorials		XML Entity Expansion						
<u> </u>		XML Injection	Document Viewer					
Announcements		XPath Injection	Arbitrary File Inclusion	vulnerabilities will be in	more than one			
Announcements		Some pages have half a dozen a	r Poll Question	the same page. The pa	unerabilities. Ige will appear in			
		the menu under each vulnerability	y Register User	,				
Cotting Started		A listing of vulnerabilities is availa	Login	y clicking here.				
Getting Started			Those "Back" Buttons					
128.198.49.198:8102/mutillida	ae/index.php?page=add-to-your-blog.php		AL 11 11 11 101 1				-	







d Þ C		A Not secure 128.198.4	9.198 :8102/mutillidae/index.		our-blog.php	😳 .	A	*	a 🖪	
M Gmail () Summer Training II	0	Internshala Trainings 📣 🗧	Software Testing 🕥 Shiwa Help Me!	ni-Singhal (Sh 🌂 I	naukri 🚷 Angular VAC 🧰 ML					
OWASP 2007		🕹 Hin	ts and Videos							
HTML 5	A	dd New Blog Entry								
Others Documentation			(Add blog for anonymous					J.
Resources >			(Note: ,<	and <u> are now allowed in blog entries</u>					
Donate Want to Help?										
You										
Video Tutorials			Ĺ		Save Blog Entry	4				
Announcements	9	View Blogs							_	
1				3 Current Blog	Entries				_	
		Name	Da	ite	Comment				_	
Getting Started	1	anonymous	2022-08-25 10:48:59			CU blog	html attack		_	
	2	anonymous	2022-08-25 10:48:56			CU blog	html attack			
	3	anonymous	2009-03-01 22:27:11		An anonymous blog? Huh?					11
	C	SRF Protection Inform	ation		Posted Token:					

XSS Injection







📴 CONT_20CSP-338:WEB AND MC 🕅 Wireshark - shiwanisinghal212 🖉 S Welcome to Chandigarh Universi S Chandigarh University Managem 🚦 128:198:49.198:8102/mutillidae/i	XSS game: Level 1	× +	~ - 🗆 X
↓ ↓ ↓ xss-game.appspot.com/level1		I 🤍 🔺	🗯 🖬 🗄
🍽 Gmail 🛞 Summer Training II 🤣 Internshala Trainings 🔞 💲 Software Testing 🌎 Shiwani-Singhal (Sh 🄾 naukri 🚷 Angular VAC 😫 ML			
[1/6] Level 1: Hello, world of XSS			
Mission Description			
This level demonstrates a common cause of cross-site scripting where user is directly included in the page without proper escaping.	input		
Interact with the vulnerable application window below and find a way to m execute JavaScript of your choosing. You can take actions inside the vuln window or directly edit its URL bar.	ake it erable		
Mission Objective			
Inject a script to pop up a JavaScript alert() in the frame below.			
Once you show the alert you will be able to advance to the next level			
Your Target			
👔 Lam vulnerable 🛛 🗶 💌			
URL https://xss-game.appspot.com/level1/frame	Go		
FourOrFour			
Enter query here Search			
			~





🖂 egov@cumail.in





Learning outcomes (What I have learnt):

We have learned what HTML injection is and XSS injection. An overview of how these attacks is constructed and applied to real system. If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system. As a result, the attacker can steal the user's active session cookie and can be the harmful for the website.

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30

