CSCI 5234 Web Security

Lab1

Cross Site Request Forgery (CSRF) Attacks

Configure the Virtual Machines:

- 1. Follow the instructions given in the <u>Lab Setup</u> page to download and install the virtual machines (VMs).
- Configure the Virtual Machines after having installed the VMs: NOTE: A VM must be off in order to be configured. Click and open the Settings (Figure 1).

New Settings Disc	ard Show	Preview	^
Name: Operating System: Settings File Location:	CSRF Ubuntu (32-bit) X:\VirtualBox\Machines \CSRF\CSRF		
System		E rearie	

Figure 1: Configuring the VMs

- 3. Open the settings for the Server virtual machine.
 - a. In the General: Advanced tab, set Shared Clipboard and Drag'n'Drop to Bidirectional.
 - In the Network: Adapter 1 tab, set the "Attached to" field to Bridged Adapter.Click the arrow to show advanced settings and change "Promiscuous Mode" to Allow VMs.
- Right click on the Server VM and select Clone. (Note: the VM must be Powered Off). Name the new virtual machine "Attacker", select "Reinitialize the MAC address", and create a Full Clone.
- 5. Lab environment setup:

In the Victim VM, modify the /etc/hosts file to map the domain name of www.csrflabattacker.com and www.csrflabelgg.com to the attacker machine's IP address. (modify 192.168.0.165 to the attacker machine's IP address)

192.168.0.165www.csrflabelgg.com192.168.0.165www.csrflabattacker.com

6. Apache configuration: Restart apache

Task 1: Observing HTTP Request in Victim VM

1. Open the Firefox and click the button on the right corner and click add-ons. On the search bar, enter "HTTP Header Live" (Figure 2).



Figure 2: Configuring the Firefox

2. Click HTTP Header Live to add it to the Firefox.

HTTP Header Live displays the HTTP header and allows the user to edit the header and send it (Figure 3).



Figure 3: HTTP Header Live in Firefox

3. In the Firefox, observe <u>http://www.csrflabelgg.com/</u> (Figure 4).



Figure 4: Observing the HTTP traffic in the Firefox

 Open a browser window and login as Alice on the csrflabelgg.com page (Figure 5). You will be able to view the report produced by the HTTP Header Live page about that login session (Figure 6).

😣 🖱 🗊 moz-extension://36d2a2e9-11a3-48fb-ad59-1a920057e2f9 - HTTP Header Live 🖡
http://www.csrtlabelgg.com/action/login
Host: www.csrltabetgg.com User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US, en; q=0.5
Accept-Encoding: g21p, dettate
Content Type: application (x-y-way form urlenceded
Content-Length 90
Cookie: Elag=hganfacbllul4gsdiv3tmaba97
Connection: keep-alive
Upgrade-Insecure-Requests: 1
elgg token=eYlYpFF6Gk-Q72pddS99Qq& elgg ts=1580243287&username=alice&passwor
POST: HTTP/1.1 302 Found
Date: Tue, 28 Jan 2020 20:29:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookle: Elgg=91(r05q4e590)698q/baukqpv/; patn=/
Control Longt Longt Longt
Keen Alive timeout=5 max=100
Connection: Keep-Alive
Content-Type: text/html:charset=utf-8
http://www.csrflabelgg.com/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: g21p, deltate
Concise: Flag=011r0SadesQ61608g76au/apv7
Clear Options File Save 🛛 Record Data 🖾 autoscroll

Figure 5. Observing the login session using HTTP Header Live

You should be able to see the username and password captured by the HTTP Header Live (Figure 6).



Figure 6. username and password captured by the HTTP Header Live

Task 2: CSRF Attack using GET Request

In this task, we need two people in the Elgg social network: Alice and Boby. You can use only one VM login and out or clone the other VM as Boby.

1. On the attacker VM, open the Firefox and login to www.csrflabelgg.com as Boby and add Alice to friend (Figure 7).



Figure 7: CSRF Lab Site

2. Observing HTTP request (Figure 8)



Figure 8: HTTP POST request

3. Now, login as Alice to <u>www.csrflabelgg.com</u> on the other VM, we can see that Boby is not on Alice's friend list (Figure 9).



Figure 9: Boby on Alice's profile

4. In order to add Alice to Boby's friend list automatically, we need to prepare an attractive malicious webpage. Create a file "index.html" in /var/www/CSRF/attacker and make a webpage as shown below (Figure 10).

<html> <body>

<h1>Win Free Electronic Gadgets</h1>

 </body>

</html>



Figure 10: index.html

Now, Boby sent a message to Alice with the malicious webpage's URL to attract Alice (Figure 11).

	Account »
CSRF Lab Site	
Activity Blogs Bookmarks Files Groups More »	
Messages Compose a message	Search
Mice O	Boby
Write recipient's username here. Subject:	Blogs Bookmarks
Win Free Electronic gadgets	Files
Message: Edit HTML	Pages
BIUIx S≓≣ ≅ ♠ ♥ ♥ ⊑ ?? ₪ ₪ X	Wire posts
You can win free gaogets by clicking on this link: www.csmabattacker.com	0

Figure 11: Boby sends a message to Alice

6. When Alice sees the message, she curies and visits the URL given in the message (Figure 12).

i		Account »
CSI	RF Lab Site	
Activity	Blogs Bookmarks Files Groups More »	
Messages Inbox	Compose a message Search Image: Search Image: Search Image: Search <td></td>	
	Files Pages Wire posts	

Figure 12: Alice's inbox

7. Once Alice clicks on the URL, she is redirected to the web page we created on step 4 (Figure 13).



Figure 13: www.csrflabattacker.com

8. After redirected to the www.csrflabattacker.com, Alice added Boby automatically (Figure 14).



Figure 14: Alice redirected to CSRF Lab Site

9. When we observe HTTP request, we can see the HTTP request referrer to www.csrflabattacker.com (Figure 15).

😣 🗐 🗊 moz-exter	nsion://36d2a2e9-11a3-48fb-ad59-1a920057e2f9 - HTTP Header Live Sub - Mozill
GET Y http://w	/www.csrflabelgg.com/action/friends/add?friend=43
Host: www.csrflabel User-Agent: Mozilla Accept: */* Accept-Language: en Accept-Encoding: gz Referer: http://www Cookie: Elgg=ltbat/ Connection: keep-al	gg.com /5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 -US,en;q=0.5 ip. deflate .csrflabattacker.com/ t4anmq/roiglir9mdKo2 ive
Send	Content-Length:0

Figure 15: HTTP GET request

Task 3: CSRF Attack using POST Request

1. Boby sends the other message to Alice to change Alice's profile (Figure 16).

E	1 🕗			Account »
CS	RF La	b Site		
Activit	v Blogs Book	marks Files Groups	More »	
Message: Inbox			Compose a message	Search
	Boby Chane	e to win a trip to Vegas for FRI	EEIII 3 minutes 🗙 ago	∓ ⊠ A We Alice
	visit: http://www.csrflabattac	ker.com/		Blogs Bookmarks
	Boby Win F	ree Electronic gadgets	4 hours X	Files Pages
	You can win free gadgets bj	v clicking on this link: www.csrflabattac	ker.com	Wire posts

Figure 16: Boby sends a message to Alice

2. In /var/www/CSRF/attacker, we modify the script and add JavaScript (Figure 17).



Figure 17: Added JavaScript on index.html

3. After we created the web page, Alice clicks the web page and you should see it connect the malicious page and then it redirected back to Alice's profile automatically (Figure 18, Figure 19).



Figure 18: www.csrflabattacker.com



Figure 19: The malicious website redirected to Alice's profile

4. In HTTP request, you should see the HTTP request referrer to www.csrflabattacker.com (Figure 20).



Figure 20: HTTP POST request

Task 4: Implementing a countermeasure for Elgg

 In this task, we need to turn countermeasure on and off by modifying the file "ActionsServices.php" in /var/www.CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg/ (Figure 21).



Figure 21: ActionsServices.php

2. Clear cookies on the victim's browser and click www.csrflabattacker.com, you should see the given below (Figure 22).



Figure 22: www.csrfattacler.com

Because we turn off the countermeasure, the attacker cannot modify Alice's profile anymore (Figure 23).



Figure 23: The malicious website redirected to Alice's profile

3. Observing HTTP request, you should see POST and GET as given below (Figure 24, Figure 25).

🛞 🖨 🗊 moz-extension://36d2a2e9-11a3-48fb-ad59-1a920057e2f9 - HTTP Header Live Sub - Mozill
GET http://www.csrflabelgg.com/profile/alice/edit Host: www.csrflabelgg.com User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate
Kererer: http://www.csrtabelgg.com/profile/alice Cookie: Elgg=gc6c352qeijbqpsuodd8k7gt62 Connection: keep-alive Upgrade-Insecure-Requests: 1
Send Content-Length:0

Figure 24: HTTP GET request

⊗ 🖨 🗊 moz-extension://36d2a2e9-11a3-48fb-ad59-1a920057e2f9 - HTTP Header Live Sub - Mozill
POST ~ http://www.csrflabelgg.com/action/profile/edit
POST http://www.csrflabelgg.com/action/profile/edit Host: www.csrflabelgg.com User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-language: en-US,en;q=0.5 Accept: Encoding: gzip, deflate Referer: http://www.csrflabattacker.com/ Content-Type: application/x-www-form-urlencoded Content-Length: 172 Cookie: Elgg=2e67qm45dsgc8pslmuq30icv03 Connection: keep-alive Upgrade-Insecure-Requests: 1 name=Alice&description=Boby is my Hero!&accesslevel[description]=2&briefdescription=&accesslevel[bright]
Send Content-Length:158

Figure 25: HTTP POST request