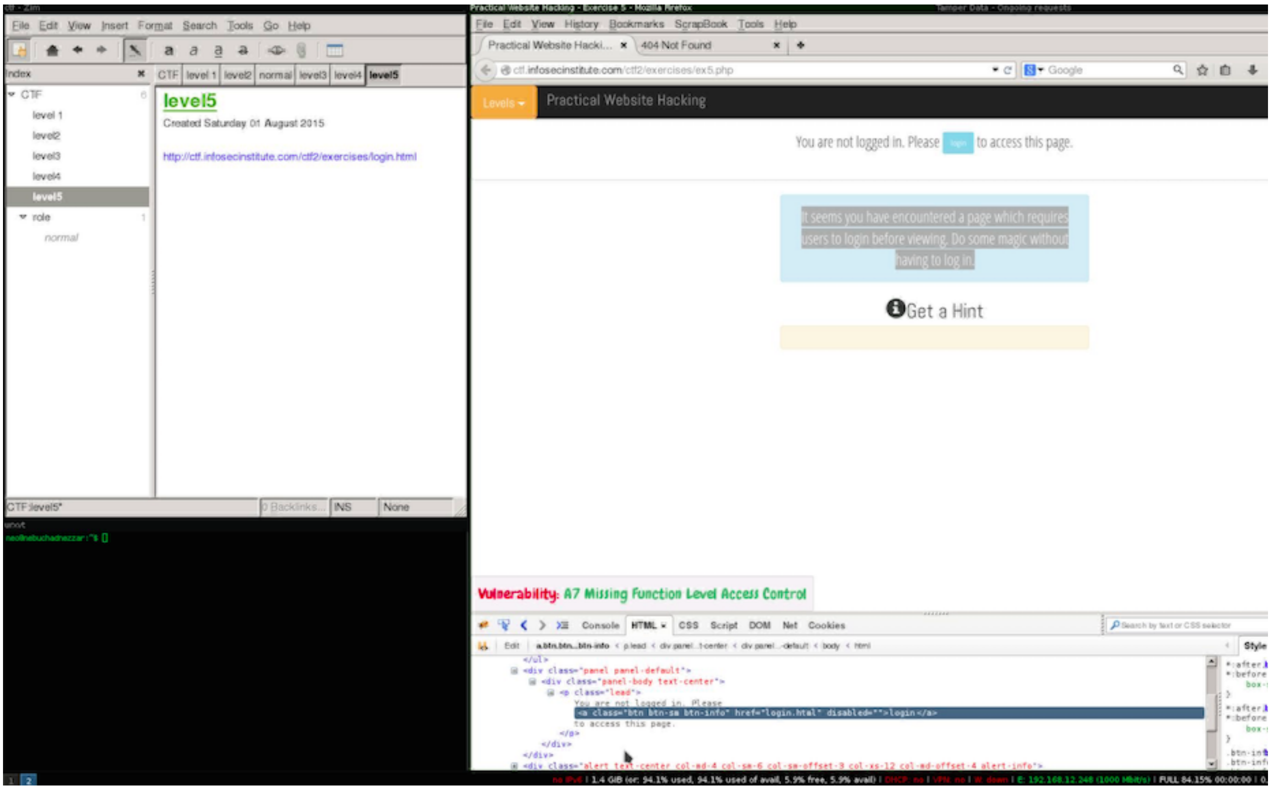
Infosecinstitute CTF 2 - LEVEL 5

This will be solution for Level 5 Practical Web Hacking CTF #2.

In this Level is about access controls, this vulnerability happeds when an application either has bad access control implementation, the most common is related to session management, issues like the use of md5 or any other depercated week hashing algorithm, unsafe random. Im both cases the application follows the execution without proper validation, Access control.

In this case the objective is to make the server assume that i'm valid and autheticated user.


File Edit View Insert Format Search Tools Go Help
CTF level 1 level2 normal level3 level4 level5
Index
CTF
level 1
level2
level3
level4
level5
role
normal
CTF:level5*
0 Backlinks...
INS
None
Practical Website Hacking - Exercise 5 - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
Practical Website Hacki...
404 Not Found
ctf.infosecinstitute.com/ctf2/exercises/ex5.php
Levels
Practical Website Hacking
Get a Hint
Console HTML CSS Script DOM Net Cookies
Search by text or CSS selector
Style

level5

Created Saturday 01 August 2015

http://ctf.infosecinstitute.com/ctf2/exercises/login.html

You are not logged in. Please login to access this page.

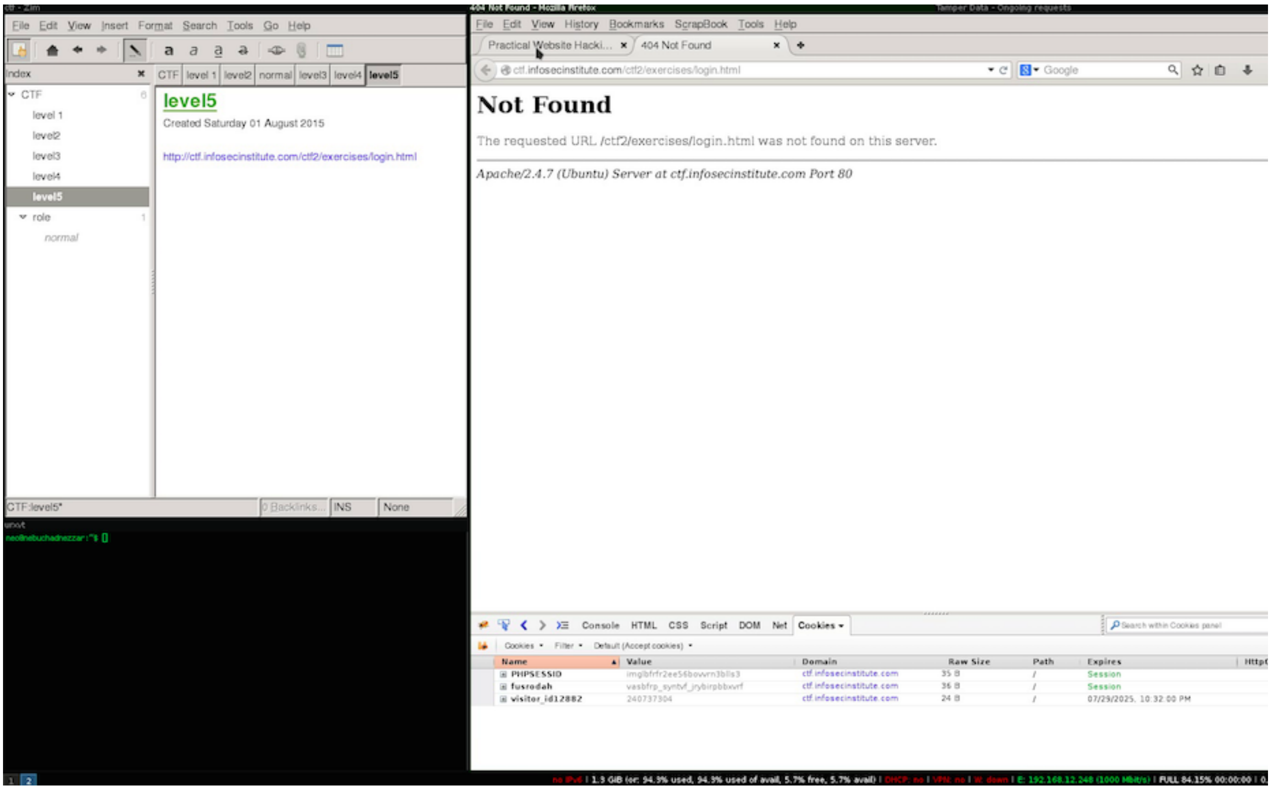
It seems you have encountered a page which requires users to login before viewing. Do some magic without having to log in.

Vulnerability: A7 Missing Function Level Access Control

```
</ul>
<div class="panel panel-default">
  <div class="panel-body text-center">
    <p class="lead">
      You are not logged in. Please
      <a class="btn btn-sm btn-info" href="login.html" disabled="">login</a>
      to access this page.
    </p>
  </div>
</div>
<div class="alert text-center col-md-4 col-sm-6 col-sm-offset-3 col-xs-12 col-md-offset-4 alert-info">
```

This vulnerabilities are very easy to exploit and very common, for this types for vulnerabilites my usual check list is as folows:

1. Check for week sessions and\or depercated hashing algorithms.
2. Session id guessing.
3. Credetial guessing \ bruteforce.
4. Redirects


File Edit View Insert Format Search Tools Go Help
Index
CTF
level 1
level2
level3
level4
level5
role
normal
CTF:level5*
0 Backlinks...
INS
None
File Edit View History Bookmarks ScrapBook Tools Help
Practical Website Hacki...
404 Not Found
Google
Console HTML CSS Script DOM Net Cookies
Cookies Filter Default (Accept cookies)

level5

Created Saturday 01 August 2015

http://ctf.infosecinstitute.com/ctf2/exercises/login.html

ctf.infosecinstitute.com/ctf2/exercises/login.html

Not Found

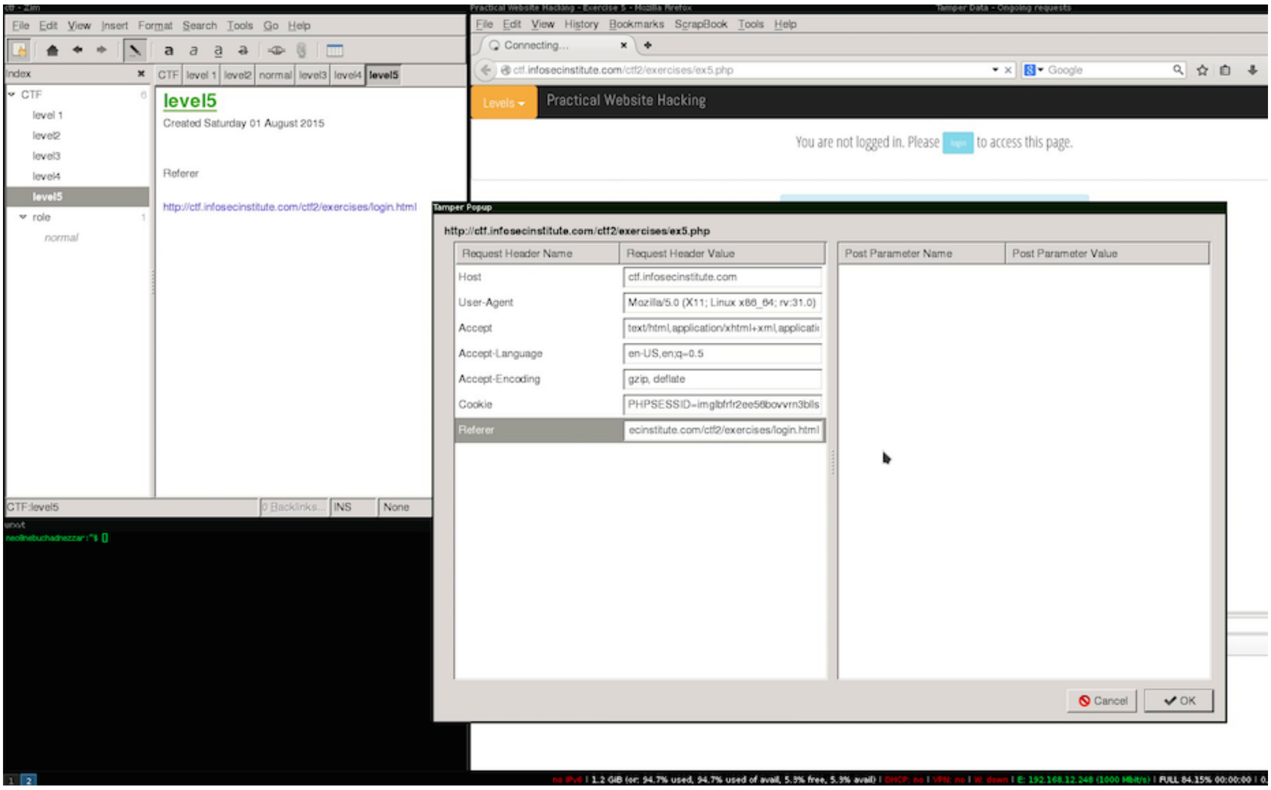
The requested URL /ctf2/exercises/login.html was not found on this server.

Apache/2.4.7 (Ubuntu) Server at ctf.infosecinstitute.com Port 80

Name	Value	Domain	Raw Size	Path	Expires
PHPSESSID	imglbfrfr2ee56bovvrn3blls3	ctf.infosecinstitute.com	35 B	/	Session
fusrodah	vasbfrp_syntvf_jrybirpbbxvrf	ctf.infosecinstitute.com	36 B	/	Session
visitor_id12882	240737304	ctf.infosecinstitute.com	24 B	/	07/29/2025, 10:32:00 PM

```
no IPv6 | 1.3 GiB (or: 94.3% used, 94.3% used of avail, 5.7% free, 5.7% avail) | DHCP: no | VPN: no | W: down | E: 192.168.12.248 (1000 Mbit/s) | FULL 84.15% 00:00:00 | 0.
```

After the initial inspection where i tryed to access the login.html page contained on the disabled login button i noticed that it doen't exist. this excludes options **2** and **3** and leaves us with one and **1** and **4** i decided to go with the last one.


File Edit View Insert Format Search Tools Go Help
Index
CTF
level 1
level2
level3
level4
level5
role
normal
CTF:level5
0 Backlinks...
INS
None
File Edit View History Bookmarks ScrapBook Tools Help
Connecting...
Google
Levels
Practical Website Hacking
Tamper Popup
Cancel
OK

level5

Created Saturday 01 August 2015

Referer

http://ctf.infosecinstitute.com/ctf2/exercises/login.html

ctf.infosecinstitute.com/ctf2/exercises/ex5.php

You are not logged in. Please login to access this page.

http://ctf.infosecinstitute.com/ctf2/exercises/ex5.php

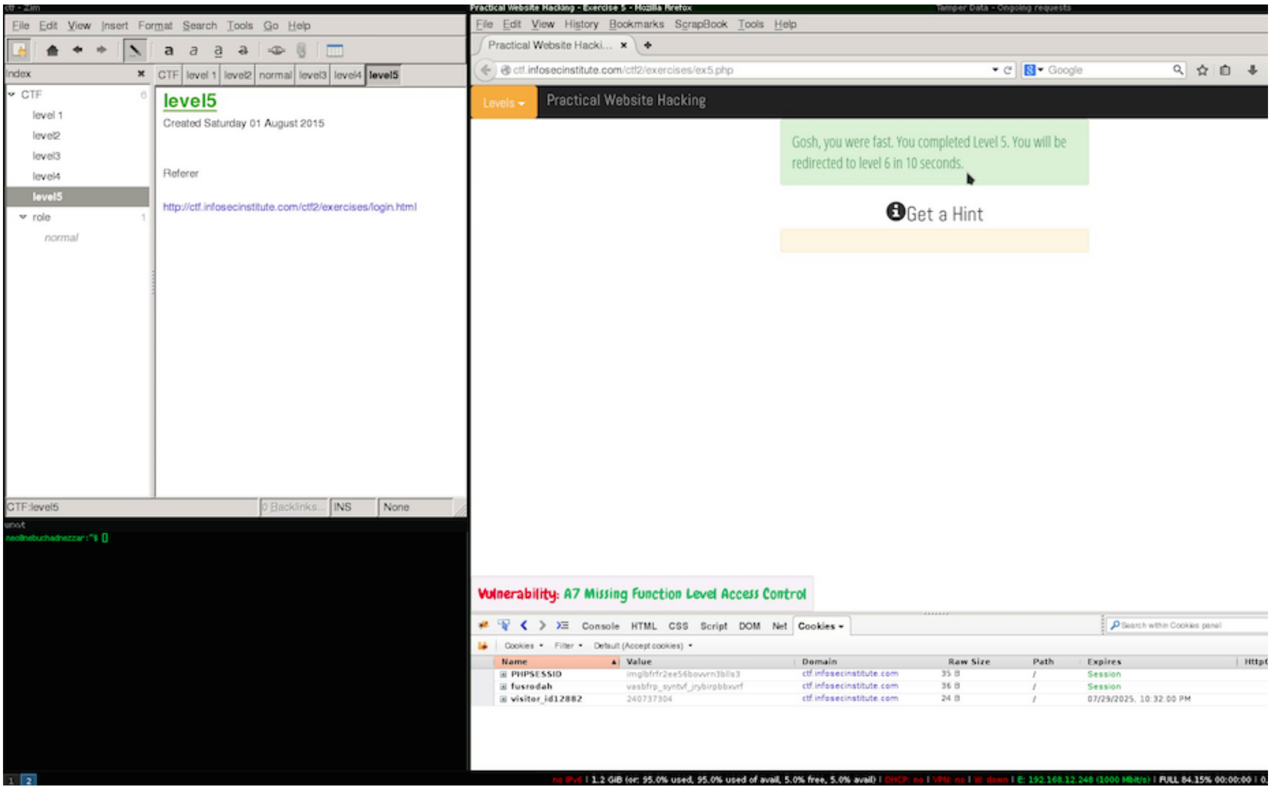
Request Header Name	Request Header Value
Host	ctf.infosecinstitute.com
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:31.0)
Accept	text/html,application/xhtml+xml,applicati
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Cookie	PHPSESSID=imglbfrfr2ee56bovvrn3blls
Referer	ecinstitute.com/ctf2/exercises/login.html

Post Parameter Name	Post Parameter Value

```
no IPv6 | 1.2 GiB (or: 94.7% used, 94.7% used of avail, 5.3% free, 5.3% avail) | DHCP: no | VPN: no | W: down | E: 192.168.12.248 (1000 Mbit/s) | FULL 84.15% 00:00:00 | 0.
```

Tasks

1. Execute a Get Request.
2. Intercept the get Request before its sent of to the serve.
3. Add http referer header to.
4. Sumit and verify.



ctf - Zim
File Edit View Insert Format Search Tools Go Help
Index
CTF level 1 level2 normal level3 level4 level5
CTF
level 1
level2
level3
level4
level5
role
normal
CTF:level5
0 Backlinks...
INS
None
Practical Website Hacking - Exercise 5 - Mozilla Firefox
Tamper Data - Ongoing requests
File Edit View History Bookmarks ScrapBook Tools Help
Practical Website Hacki...
Google
Levels
Practical Website Hacking
Get a Hint
Console HTML CSS Script DOM Net Cookies
Search within Cookies panel
Cookies Filter Default (Accept cookies)

level5

Created Saturday 01 August 2015

Referer

http://ctf.infosecinstitute.com/ctf2/exercises/login.html

```
urxvt
neo@nebuchadnezzar:~$
```

ctf.infosecinstitute.com/ctf2/exercises/ex5.php

Gosh, you were fast. You completed Level 5. You will be redirected to level 6 in 10 seconds.

Vulnerability: A7 Missing Function Level Access Control

Name	Value	Domain	Raw Size	Path	Expires
PHPSESSID	imglbfrfr2ee56bovvrn3blls3	ctf.infosecinstitute.com	35 B	/	Session
fusrodah	vasbfrp_syntvf_jrybirpbbxvrf	ctf.infosecinstitute.com	36 B	/	Session
visitor_id12882	240737304	ctf.infosecinstitute.com	24 B	/	07/29/2025, 10:32:00 PM

```
no IPv6 | 1.2 GiB (or: 95.0% used, 95.0% used of avail, 5.0% free, 5.0% avail) | DHCP: no | VPN: no | W: down | E: 192.168.12.248 (1000 Mbit/s) | FULL 84.15% 00:00:00 | 0.
```

Success!

Video

0x4E0x650x6F
0x4E0x650x6F