اِنَّا كُلَّ شَیۡءٍ خَلَقۡنٰهُ بِقَدَرٍ

PAE

The Pakistan Academy of Engineering

Cybersecurity

Fundamentals: Penetration Testing 101

Dr. Jawwad A Shamsi

Professor and Dean - Fast NUCES (City Campus)

Dated: 20-May-2023 (Saturday)

SYSLAB (My Research Group at FAST-NUCES)

- Systems Research Laboratory
  - Developing Capable Systems through integration
    - Artificial Intelligence
    - Cloud Computing
    - Security
    - High Performance Computing
    - Health
    - Education

Penetration Testing

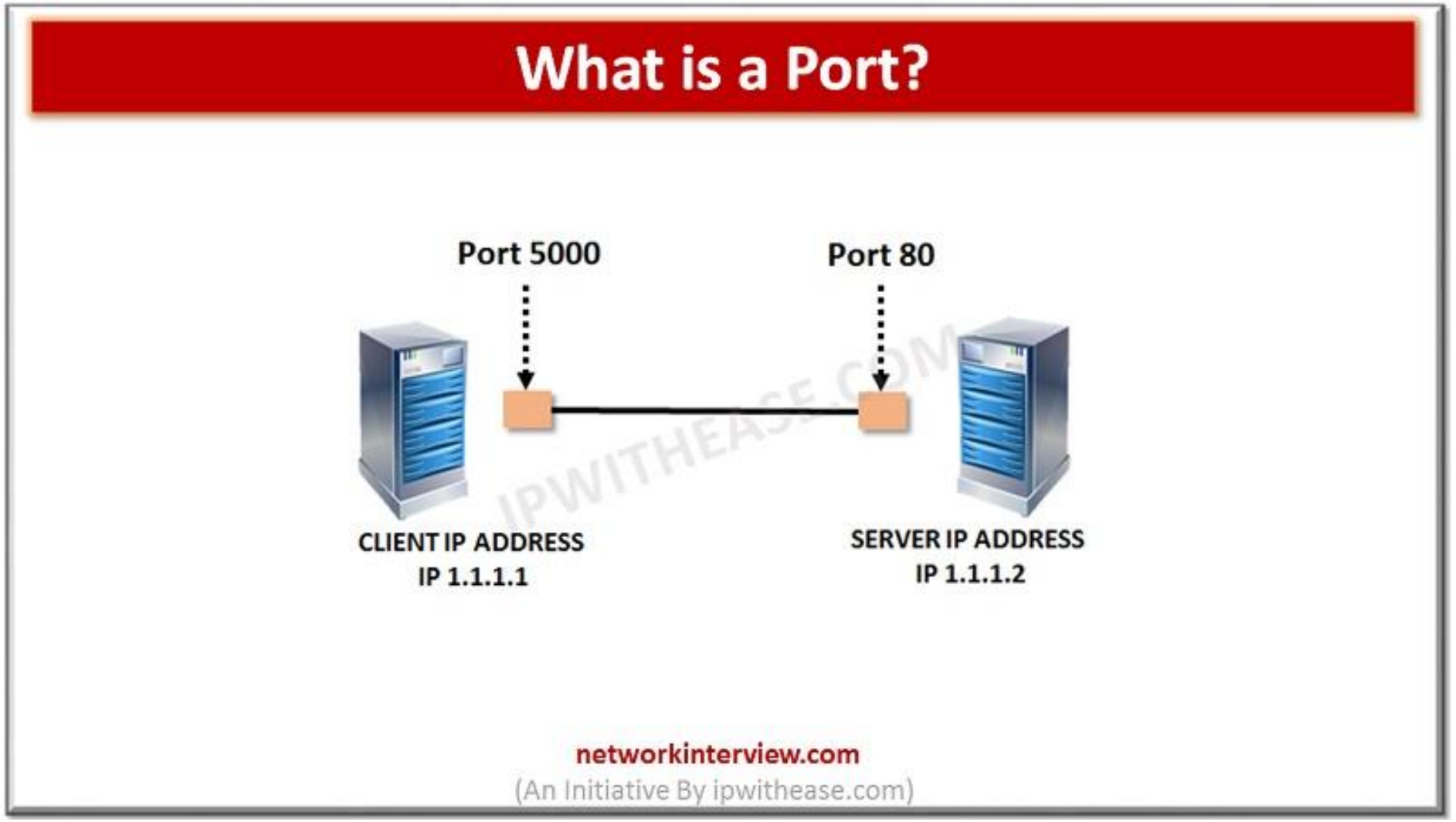
- A systematic Process
  - Probing vulnerabilities
    - Applications
    - Networks

Platform

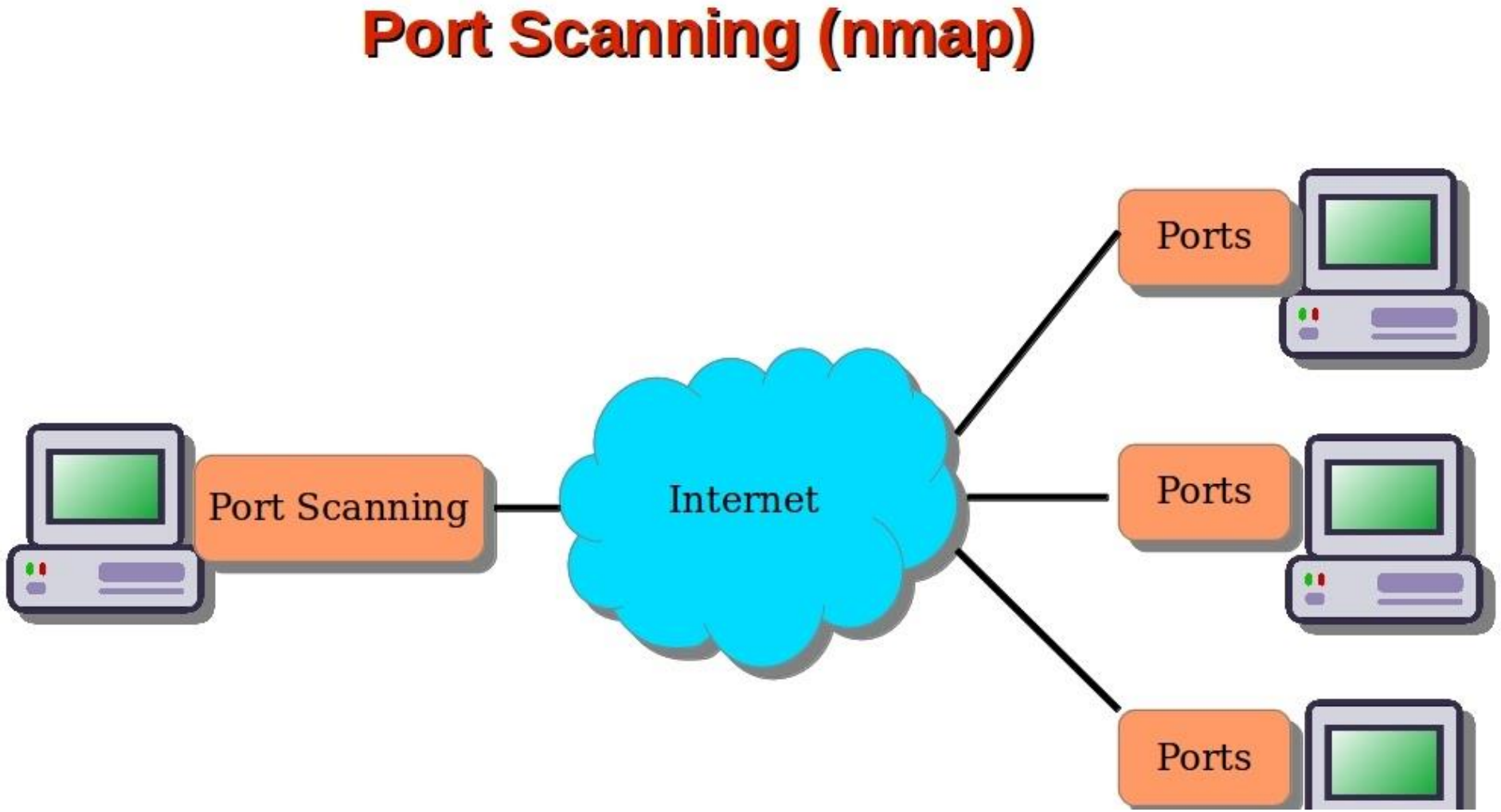
- VirtualBox
- Kali Linux
    - Pre-installed security tools

Port Scanning

Port


What is a Port?
Port 5000
Port 80
CLIENT IP ADDRESS
IP 1.1.1.1
SERVER IP ADDRESS
IP 1.1.1.2
networkinterview.com
(An Initiative By ipwithease.com)

Port Scanning



nmap scanme.nmap.org

nmap localhost

sudo nmap -v -sT -sV -O localhost

Start ssh – Secure Shell on Local host

systemctl start ssh.socket

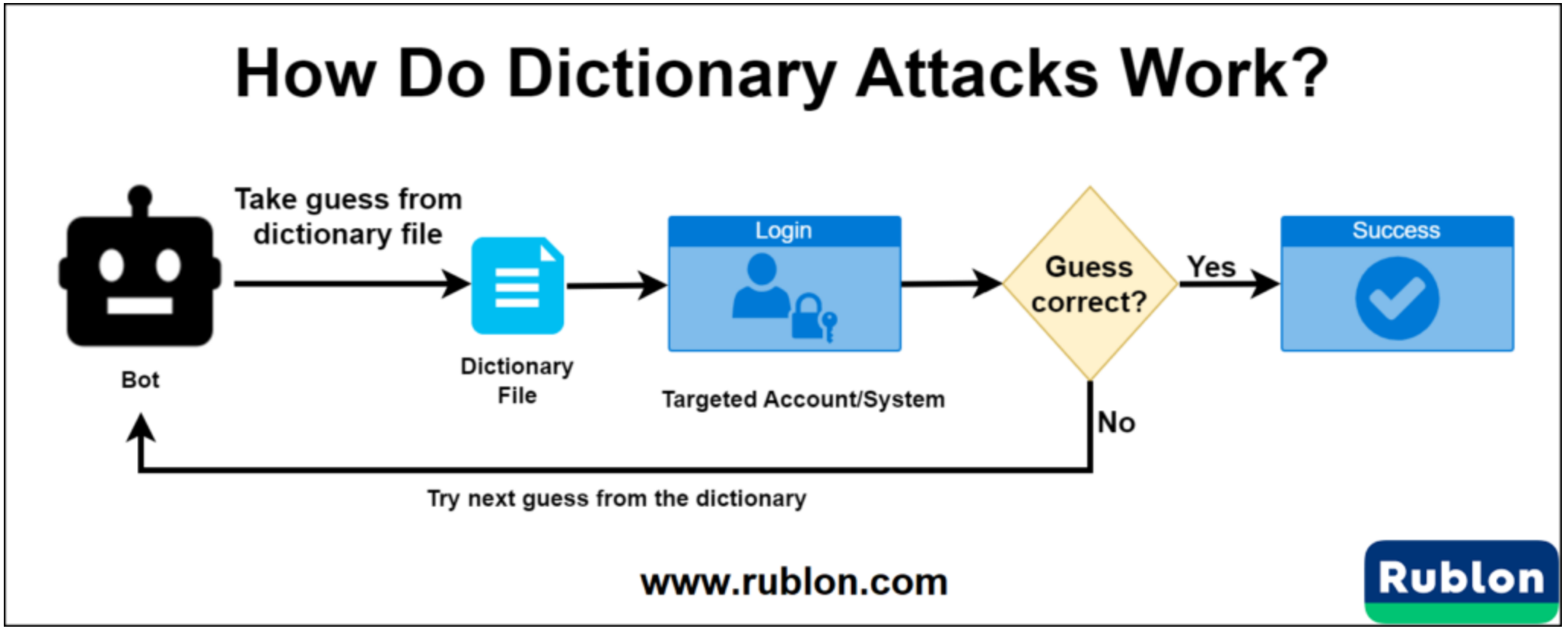
systemctl stop ssh.socket

- nmap localhost
- sudo nmap -v -sT -sV -O localhost

Dictionary Attack

Dictionary Attack

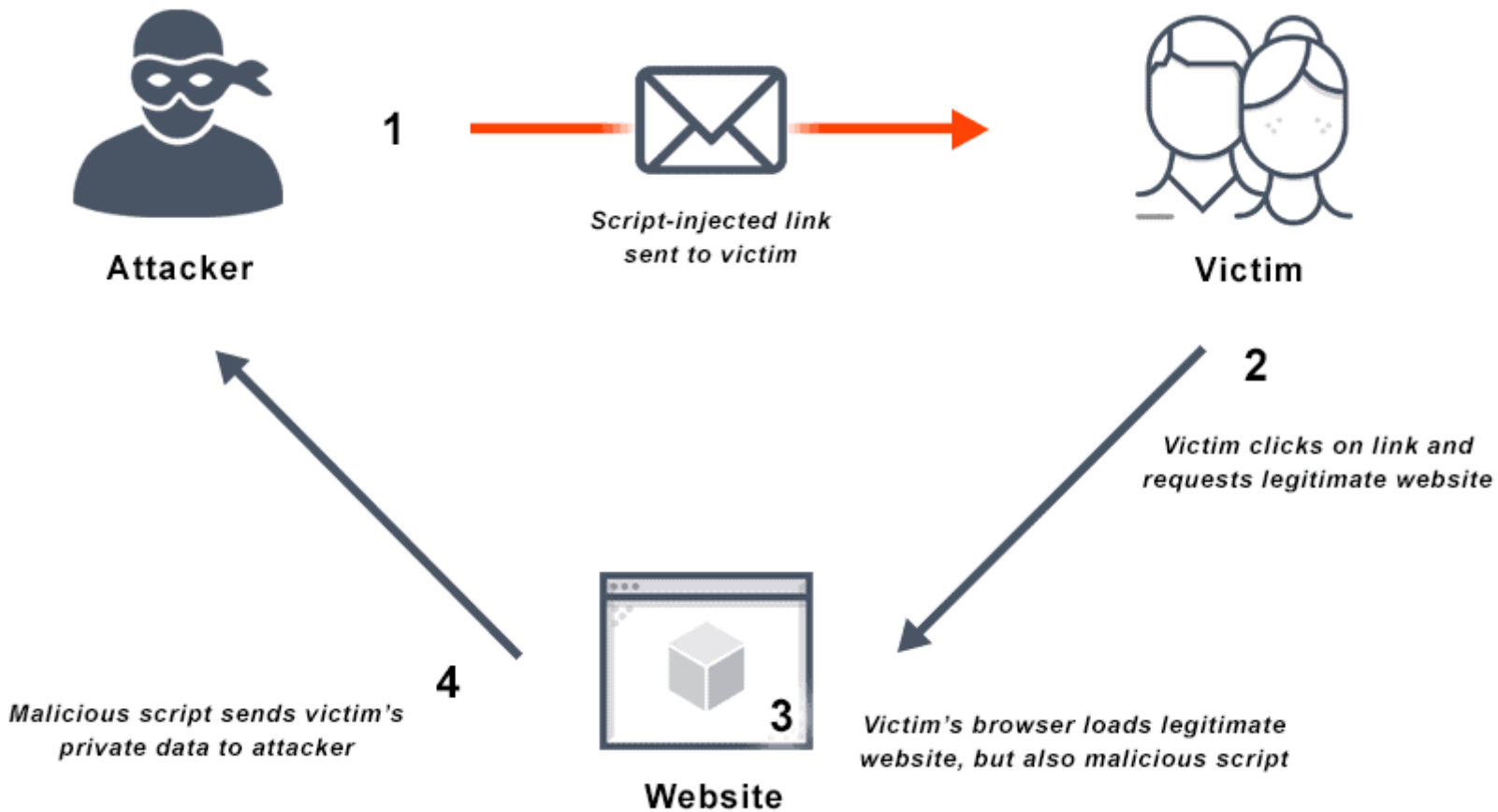
Dictionary Attack



Password Cracking using Hydra

Cross-site Scripting Attack (XSS)

- Inject client-side scripts
  - Through web browser
  - For malicious Activity


Attacker
1
Script-injected link
sent to victim
Victim
2
Victim clicks on link and
requests legitimate website
3
Website
Victim's browser loads legitimate
website, but also malicious script
4
Malicious script sends victim's
private data to attacker

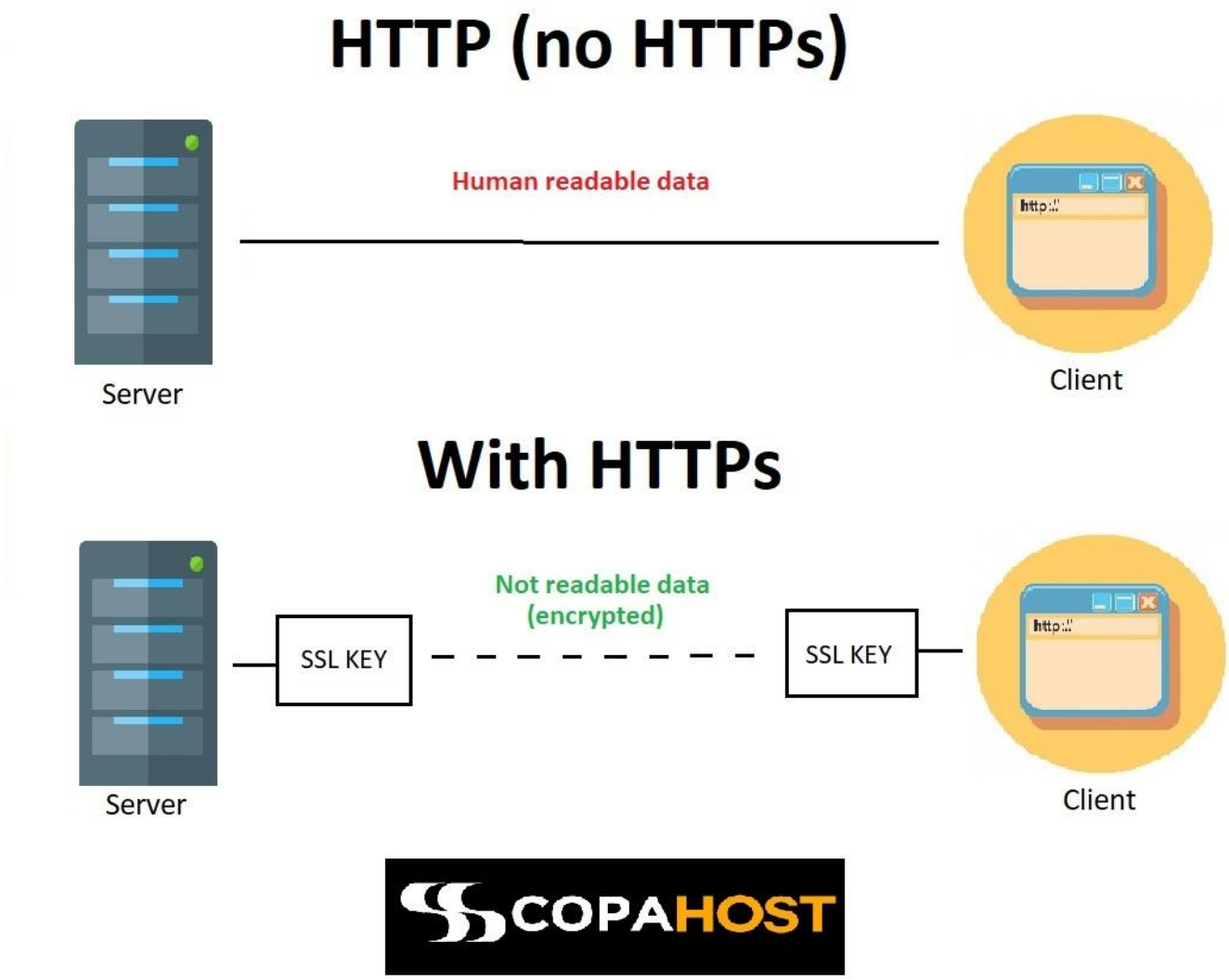
Activity

- https://xss-game.appspot.com

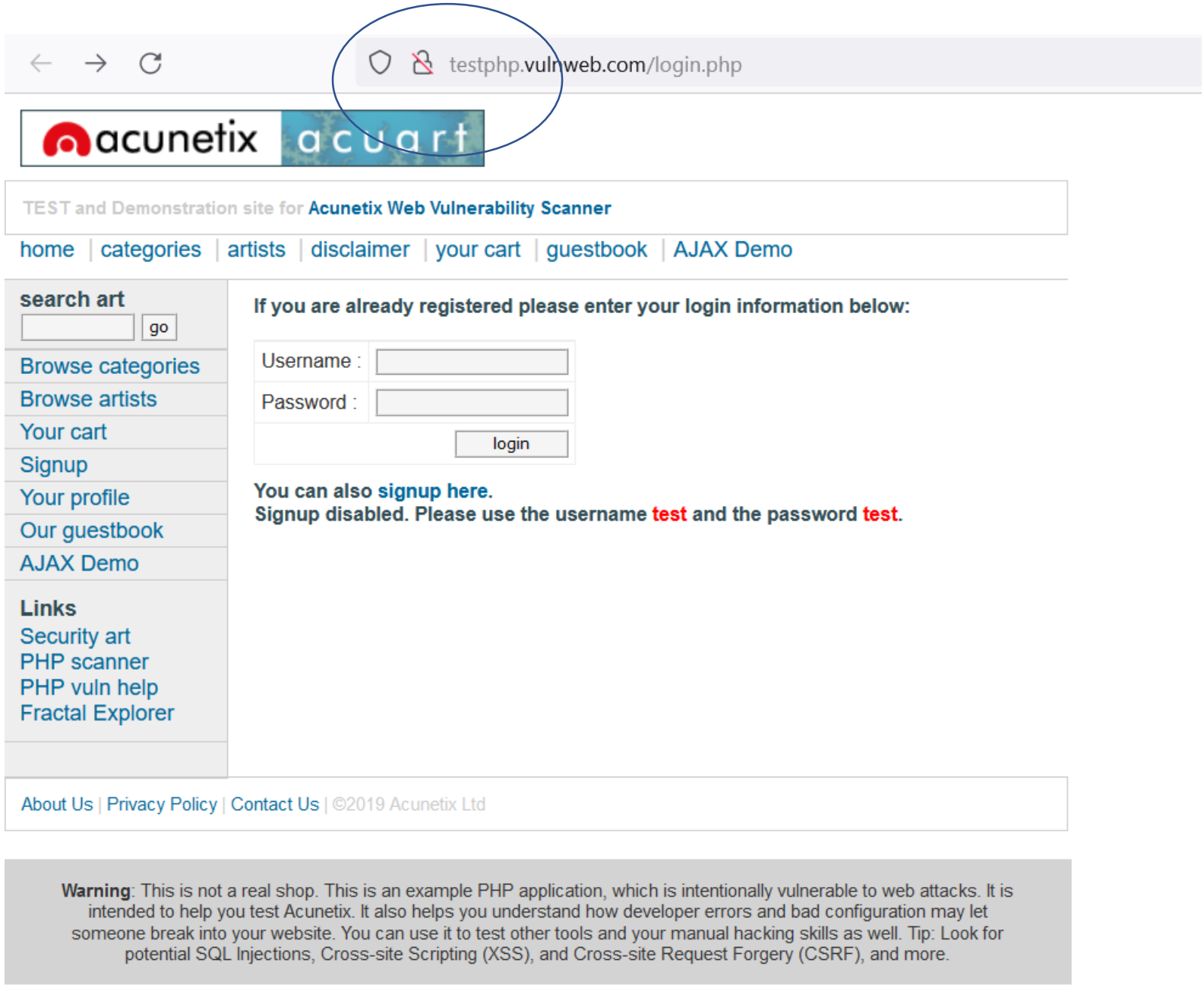
- How can we inject Java Script via different means

Password Sniffing with wireshark for http

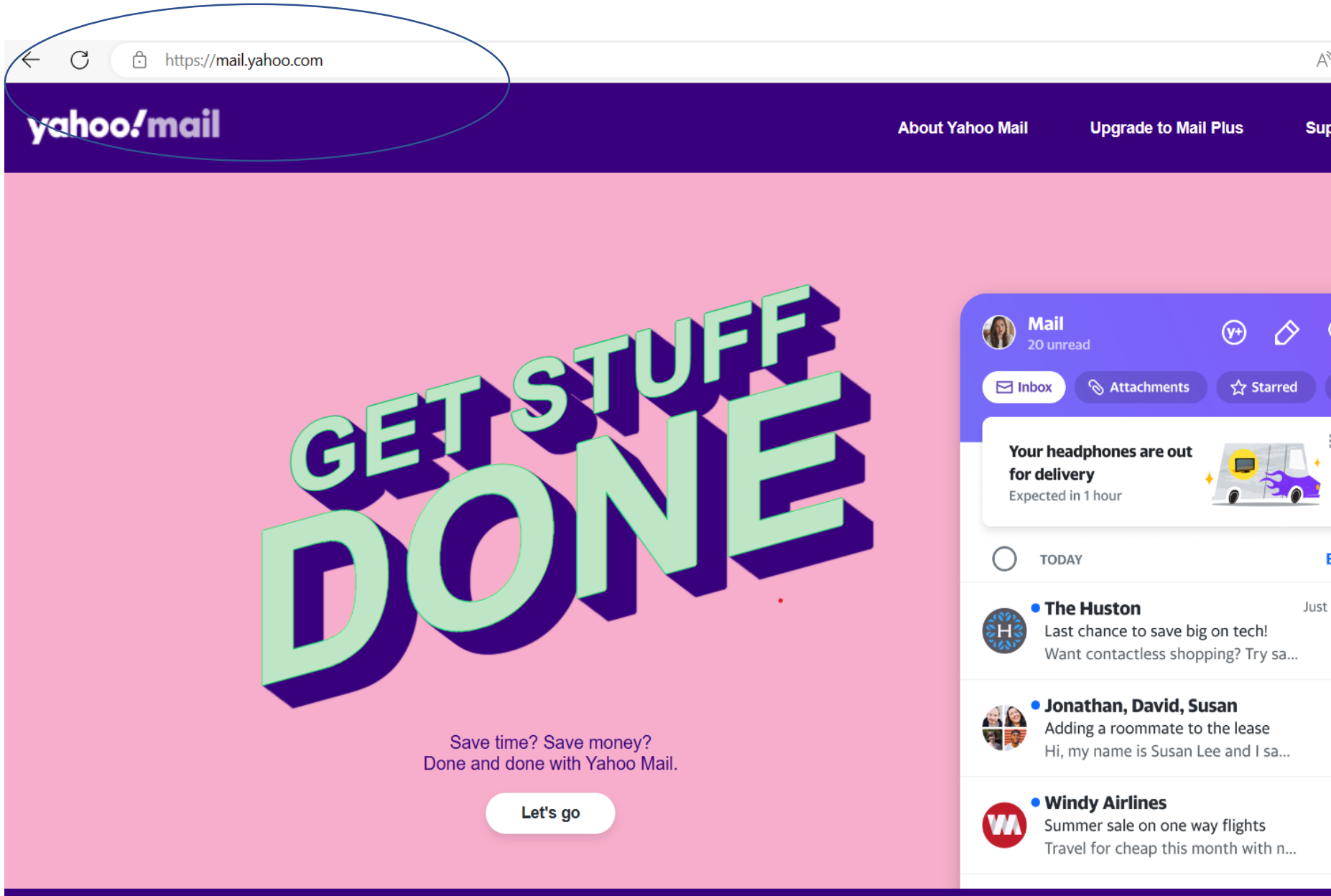
HTTP vs HTTPs

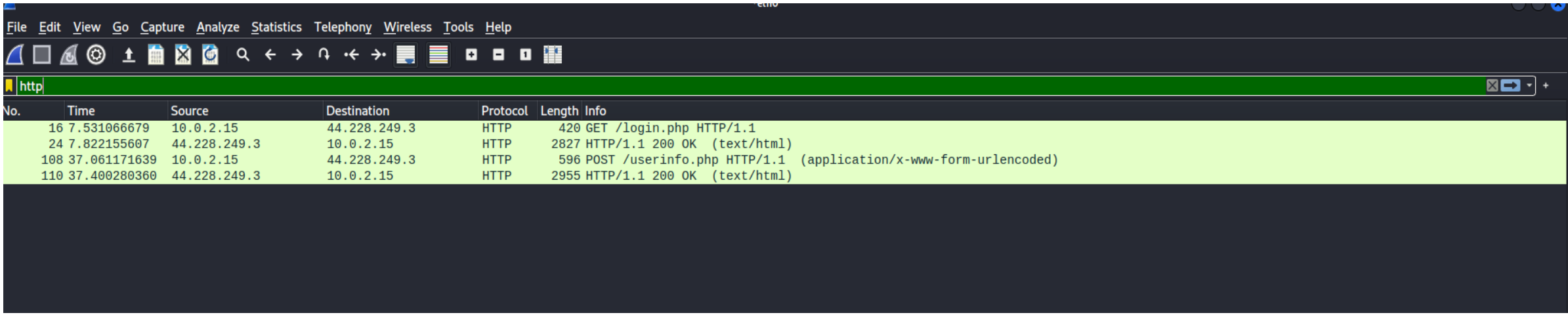


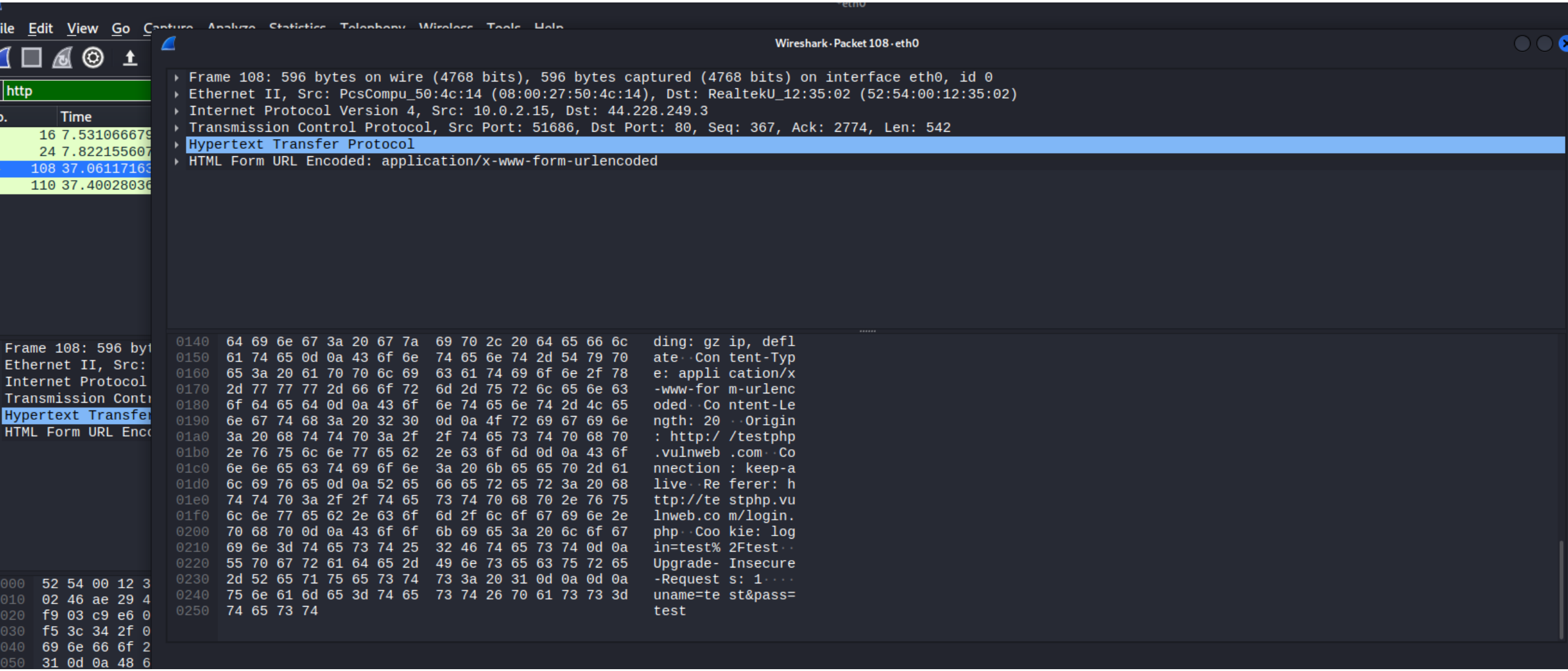
HTTP


testphp.vulnweb.com/login.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username :
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

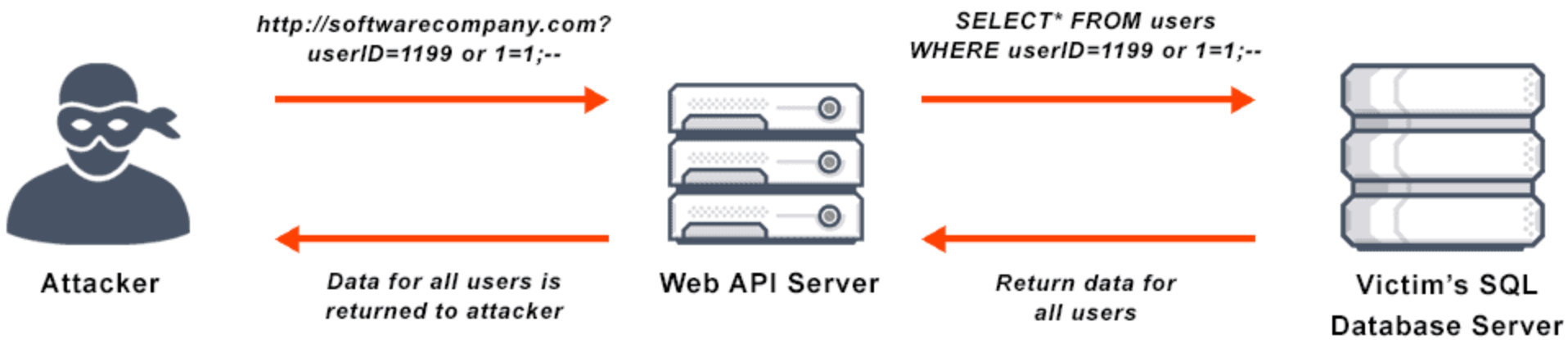
HTTPS


https://mail.yahoo.com
yahoo!mail
About Yahoo Mail
Upgrade to Mail Plus
GET STUFF DONE
Save time? Save money?
Done and done with Yahoo Mail.
Let's go
Mail
20 unread
Inbox
Attachments
Starred
Your headphones are out for delivery
Expected in 1 hour
TODAY
The Huston
Just
Last chance to save big on tech!
Want contactless shopping? Try sa...
Jonathan, David, Susan
Adding a roommate to the lease
Hi, my name is Susan Lee and I sa...
Windy Airlines
Summer sale on one way flights
Travel for cheap this month with n...


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
16 7.531066679 10.0.2.15 44.228.249.3 HTTP 420 GET /login.php HTTP/1.1
24 7.822155607 44.228.249.3 10.0.2.15 HTTP 2827 HTTP/1.1 200 OK (text/html)
108 37.061171639 10.0.2.15 44.228.249.3 HTTP 596 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
110 37.400280360 44.228.249.3 10.0.2.15 HTTP 2955 HTTP/1.1 200 OK (text/html)


ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
o. Time
16 7.531066679
24 7.822155607
108 37.06117163
110 37.40028036
Frame 108: 596 byt
Ethernet II, Src:
Internet Protocol
Transmission Contr
Hypertext Transfer
HTML Form URL Enc
000 52 54 00 12 3
010 02 46 ae 29 4
020 f9 03 c9 e6 0
030 f5 3c 34 2f 0
040 69 6e 66 6f 2
050 31 0d 0a 48 6
Wireshark · Packet 108 · eth0
Frame 108: 596 bytes on wire (4768 bits), 596 bytes captured (4768 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_50:4c:14 (08:00:27:50:4c:14), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 51686, Dst Port: 80, Seq: 367, Ack: 2774, Len: 542
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0140 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
0150 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 ate··Con tent-Typ
0160 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 e: appli cation/x
0170 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 -www-for m-urlenc
0180 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 oded··Co ntent-Le
0190 6e 67 74 68 3a 20 32 30 0d 0a 4f 72 69 67 69 6e ngth: 20 ··Origin
01a0 3a 20 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 70 : http:/ /testphp
01b0 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
01c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
01d0 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 live··Re ferer: h
01e0 74 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 ttp://te stphp.vu
01f0 6c 6e 77 65 62 2e 63 6f 6d 2f 6c 6f 67 69 6e 2e lnweb.co m/login.
0200 70 68 70 0d 0a 43 6f 6f 6b 69 65 3a 20 6c 6f 67 php··Coo kie: log
0210 69 6e 3d 74 65 73 74 25 32 46 74 65 73 74 0d 0a in=test% 2Ftest··
0220 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure
0230 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a -Request s: 1····
0240 75 6e 61 6d 65 3d 74 65 73 74 26 70 61 73 73 3d uname=te st&pass=
0250 74 65 73 74 test

SQL Injection Attacks


http://softwarecompany.com?
userID=1199 or 1=1;--
SELECT* FROM users
WHERE userID=1199 or 1=1;--
Attacker
Data for all users is
returned to attacker
Web API Server
Return data for
all users
Victim's SQL
Database Server