

Challenge Basic Injection: 30 Points

Very simple query injection just entered 'or 1 or' returned with the flag.

The image shows a web browser window with multiple tabs. The active tab is 'web.ctflearn.com/web4/'. The page title is 'You know what to do'. It features an 'Input:' field with the text 'or 1 or' and a 'Submit' button. Below the input, it displays the 'Original Query: SELECT * FROM webfour.webfour where name = '\$_input'' and the 'Your Resulting Query: SELECT * FROM webfour.webfour where name = 'or 1 or''. The results show a list of names and data, including 'Name: Luke', 'Data: I made this problem.', 'Name: Alec', 'Data: Steam boys.', 'Name: Jalen', 'Data: Pump that iron fool.', 'Name: Eric', 'Data: I make cars.', 'Name: Sam', 'Data: Thinks he knows SQL.', 'Name: fl4g_giv3r', 'Data: CTFlearn(th4t_js_why_you_n33d_to_sanitiz3_inputs)', 'Name: snoutpop', 'Data: jowls', 'Name: Chunbucket', and 'Data: @datboiiii'.

The bottom part of the image shows the CTFlearn challenge page for 'Basic Injection' (30 points, Easy). The description says: '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](#).' The 'Flag' field contains 'CTFlearn{h4ck3d}' and the status is 'Solved'. The page also shows a 'Top10' leaderboard and a 'Rating - Please Rate' section with a 4.60 rating.

Rank	Username
1	natjef20
2	javier
3	drmad
4	limyunkai19
5	sebwit20
6	yukimo
7	teamaardvark
8	witchcraft
9	aiyam
10	blackndoor

Rating	Count
5 stars	10
4 stars	10
3 stars	10
2 stars	10
1 star	10

Challenge Forensics 101: 30 points

Using strings I just looked for anything that had the string flag using grep and it showed the flag.

The image shows a screenshot of the CTFLEARN website and a terminal window. The website displays the 'Forensics 101' challenge, which is worth 30 points and is marked as 'Easy'. The challenge description asks the user to find a flag in a file located at https://mega.nz/#!OHohCbTawbg60PARf4u6E6juuvK9-aDRe_bgEL937VO01ElmM7c. The user has entered the flag 'CTFlearn{h4ck3d}' and the challenge is marked as 'Solved'. The challenge has 33406 solves and a rating of 4.48.

The terminal window shows the user's commands and the output of the 'strings' command used to find the flag:

```
root@kali: /home/saifezzat/Downloads
root@kali) ~ [ /home/.../Desktop/security/ctf/pwn-simple-rip ]
# cd ..
root@kali) ~ [ /home/saifezzat/Desktop/security/ctf ]
# cd ..
root@kali) ~ [ /home/saifezzat/Desktop/security ]
# cd ..
root@kali) ~ [ /home/saifezzat/Desktop ]
# cd ..
root@kali) ~ [ /home/saifezzat ]
# cd Downloads
root@kali) ~ [ /home/saifezzat/Downloads ]
# ls
95f6edfb66ef42d774a5a34581f19052.jpg 'simple-rip(1).tar.gz'
bof.c simple-rip.tar.gz
root@kali) ~ [ /home/saifezzat/Downloads ]
# strings 95f6edfb66ef42d774a5a34581f19052.jpg | grep flag
flag{wow!_data_is_cool}
```

Challenge My Blog: 20 point

In this challenge the admin hid the flag in the code, using inspect and the hint given, 'Application' 'Memory' I found the flag in application storage.

The screenshot shows a web browser with the address bar displaying `blog.noxtal.com`. The page content includes a header with a colorful circular logo and the title "Noxtal's Blog". Below the header, there is a welcome message: "Welcome to my blog! In other words, it is a website on which I post writeups for cybersecurity challenges, tutorials and offer good ways to learn programming and hacking. My goal is to make people from the coding and hacking community to the next level and mostly share the things I create. I am not in any way a certified hacker or pentester, but I do that as a passion because of my young age. Enjoy your stay!". Below the message are social media icons for Twitter, GitHub, and RSS. The main content area is titled "Latest Articles" and lists four articles: "CTFlearn 887 - Suspicious message", "The Ultimate KOTH Defense Guide", "H@ctivityCon - Template Shack", and "The Essentials - My Favorite Tools and Commands".

The browser's developer tools are open, showing the "Application" tab. The left sidebar lists various storage areas, including "Local Storage", "Session Storage", "IndexedDB", "Web SQL", "Cookies", "Private State Tokens", "Interest Groups", "Shared Storage", "Cache Storage", and "Background Services". The "Local Storage" section is expanded, showing a list of keys. The key `flag` is selected, and its value is displayed in the right pane: `flag{n7f_l0c4l_570r463_15n7_53cur3_570r463}`. The console shows two messages: "Audit usage of navigator.userAgent, navigator.appVersion, and navigator.platform" and "Page layout may be unexpected due to Quirks Mode".

CTFLEARN

Learn Challenges Scoreboard Dashboard

Learn++

My Blog ✓

20 points Easy

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{.

Flag: Solved

Web · Noxtal 8514 solves

Top10

1 Lia_V	6 satwiktandukar
2 stigru	7 ill_advisor
3 vanya829	8 cuuuuaa123
4 KavenOZ	9 CdiviNFx
5 lamchcl	10 Krzyychuu

Rating - Please Rate

4.38










5 ★
4 ★
3 ★
2 ★
1 ★


★★★★★

Challenge Capture the flag: 50 points

In this challenge I used wireshark to try and read the data of the img. The img was pixlated from the bottom part of it so I assumed it would have some sort of corruption. I saved the file as .cap and opened it via wireshark. Found the MSG up top so I converted it to base 64 then ran it using echo and it printed the flag.

Please verify your email. Click to resend.

CTFLEARN    Learn  Challenges  Scoreboard  Dashboard   

A CAPture of a Flag ✓  50 points Medium

This isn't what I had in mind, when I asked someone to capture a flag... can you help? You should check out Wireshark.
https://mega.nz/#!3WhAWKwR!1T9cw2srN2CeOQWuWuCm0ZVXgwk-E2v-TrPsZ4HUQ_f4

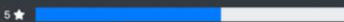
Flag


Forensics · hazy 5203 solves

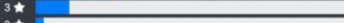
Top10


1 vidar	6 zaknafein
2 kronos	7 pedro
3 qbert513	8 bockrockman
4 santy	9 CatPawn
5 thekidofarcana	10 redcode


Rating - Please Rate 4.37

5 ★ 

4 ★ 

3 ★ 

2 ★ 

1 ★ 

★★★★★

Discussion

Wireshark · Follow TCP Stream (tcp.stream eq 5) · flag (4).cap

File Edit View

tcp.stream

No.	Time	Source	Destination	Protocol	Length	Info
227	2.200000	192.168.1.101	192.168.1.1	HTTP	115	GET /?msg=ZmxhZ3tBRmxhZ0luUENBUH0= HTTP/1.1
237	2.200000	192.168.1.1	192.168.1.101	HTTP	115	Host: www.hazzy.co.uk
238	2.200000	192.168.1.1	192.168.1.101	HTTP	115	Connection: keep-alive
247	2.200000	192.168.1.1	192.168.1.101	HTTP	115	Upgrade-Insecure-Requests: 1
254	2.200000	192.168.1.1	192.168.1.101	HTTP	115	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.78 Safari/537.36
255	2.200000	192.168.1.1	192.168.1.101	HTTP	115	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
259	2.200000	192.168.1.1	192.168.1.101	HTTP	115	Accept-Encoding: gzip, deflate
3691	11.200000	192.168.1.1	192.168.1.101	HTTP	115	Accept-Language: en-GB,en;q=0.8
3864	11.200000	192.168.1.1	192.168.1.101	HTTP	115	Cookie: language=en-gb; currency=USD
3865	11.200000	192.168.1.1	192.168.1.101	HTTP	115	HTTP/1.1 200 OK
				Server		nginx
				Date		Fri, 04 Aug 2017 14:03:25 GMT
				Content-Type		text/html; charset=UTF-8
				Content-Length		498
				Connection		keep-alive
				Vary		Accept-Encoding
				Content-Encoding		gzip

Frame 255 selected

Ethernet II, Src: Intel(R) Ethernet Controller (3:0:1:0), Dst: 08:00:27:00:00:00

Internet Protocol Version 4, Src: 192.168.1.1, Destination: 192.168.1.101

Transmission Control Protocol, Src Port: 80, Destination Port: 54321

Hypertext Transfer Protocol

Line-based text

.....]o.0....+. .@p.8N[.v..h6Q.k+Z..q..Nb-.+.L...C.H.EHH.....8.
 {...^N7_V...~s;...w.....x.w..?..U....bg.....-\$.n.j.-%.UB.....{...C4....
 %.qn.n...oB...~...*"d..1..9.&..V..j.....s!.....t..q..M6..
 #...F..e.#..[I1...u..bs^[.j..
 2%...j...g...N..Y...C...w^G.Aa...!...RHs\..x..

Packet 255. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,150 bytes) Show data as ASCII Stream 5

root@kali: /home/saifezzat/Downloads

File Actions Edit View Help

GET /?msg=ZmxhZ3tBRmxhZ0luUENBUH0= | base64 -d
flag{AFlagInPCAP}

(root@kali)-[/home/saifezzat/Downloads]
echo ZmxhZ3tBRmxhZ0luUENBUH0= | base64 -d
flag{AFlagInPCAP}

(root@kali)-[/home/saifezzat/Downloads]
curl -s -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36" -H "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;q=0.8" -H "Accept-Encoding: gzip, deflate" -H "Accept-Language: en-GB,en;q=0.8" -H "Cookie: language=en-gb; currency=USD" http://www.hazzeq.com/

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 04 Aug 2017 14:03:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 498
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

.....]o.....+...Bp.BN[.v..h6Q.k+Z..q..Nb-..+..L....C.H.EHH....8..
{..."^N7_V..~s...w.....x.w...?..U....bg.....-\$.n.j..-%.UB.....{...C4...
%.qn.n...oB...-...*"d..1..9.&..V..j....s..l.....t..q..M6..
#....F..e.#...[1...u..bs^..j..[.....N..Y.....G.....wG..Ag.....'....Rhs\..x..
2%.....j.....Q.....

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,150 bytes) Show data as ASCII Stream 5