APPENDIX

Impact Components. We further conducted experiments on V8 to study two major impact components for CovRL-Fuzz: the CovRL-based finetuning epochs and alpha. As with the earlier ablation studies, we conducted each experiment for 5 hours, repeated 5 times. In order to ensure fairness, any training time that exceeded one epoch was not included in the experiment duration for the CovRL-based finetuning epochs.

Table A1 compares the coverage based on finetuning epochs. Our observation revealed a negative correlation between the number of epochs and the error rate, indicating that as the epochs increased, the error rate decreased. However, the decrease in error rate was also followed by a decrease in coverage. It indicates that overfitting starts at the second epoch, which may restrict the generation of diverse test cases. Table A2 represents the comparison of coverage based on different values of α. α refers to the momentum rate in Eq. 6, which adjusts the weight between the previous and current IDF^{cov}. The experimental results demonstrated that applying a momentum rate of 0.6 led to better results compared to the absence of momentum.

Real-World Bugs. Table A3 presents bugs found by CovRL-Fuzz. In total, we discovered 58 real-world bugs in 9 JS engines, including 15 CVEs. Out of these, 50 were previously undiscovered bugs.

Table A1: Ablation: Impact of finetuning epochs

	V8		
Epoch	Error (%)	Coverage	
		Valid	Total
0 Epoch	74.91%	58,230	61,947
1 Epoch	61.53%	**71,319**	**74,574**
2 Epoch	59.43%	66,017	69,764
3 Epoch	**56.93%**	67,079	69,517

Table A2: Ablation: Impact of α

α		0.0	0.2	0.4	**0.6**	0.8	1.0
Cov.	Valid	68,248	68,635	69,247	**71,319**	69,955	69,330
	Total	71,906	71,692	72,415	**74,574**	72,623	72,218

Table A3: Summary of Detected Real-World Bugs

#	Target	Bug Type	Status	Bug ID
1	V8	Invalid size error	Known	Issue 1201626
2	V8	Out of Memory	Known	Issue 7970
3	JSC	Out-of-bounds Read	Known	Internal Fixed
4	JSC	Crash by load()	Known	Bug 222542
5	JSC	Use After Free	Confirmed	Bug 256952
6	Chakra	Undefined Behavior	Known	Issue 6688
7	Chakra	Out of Memory	Known	Issue 6752
8	Chakra	Undefined Behavior	Confirmed	Issue 6890
9	Chakra	Out of Memory	Confirmed	Issue 6891
10	Chakra	Out of Memory	Confirmed	Issue 6892
11	Chakra	Undefined Behavior	Confirmed	Issue 6893
12	Chakra	Undefined Behavior	Confirmed	Issue 6919
13	Chakra	Out-of-bounds Read	Reported	Issue 6920
14	Chakra	Undefined Behavior	Confirmed	Issue 6921
15	Jerry	Undefined Behavior	Known	Issue 5061
16	Jerry	Undefined Behavior	Known	Issue 5062
17	Jerry	Undefined Behavior	Reported	Issue 5063
18	Jerry	Heap Buffer Overflow	Reported	CVE-2023-31908
19	Jerry	Undefined Behavior	Reported	CVE-2023-31919
20	Jerry	Undefined Behavior	Reported	CVE-2023-31920
21	Jerry	Undefined Behavior	Reported	CVE-2023-31921
22	Jerry	Out of Memory	Reported	CVE-2023-31914
23	Jerry	Heap Buffer Overflow	Reported	CVE-2023-31907
24	Jerry	Heap Buffer Overflow	Reported	CVE-2023-31910
25	Jerry	Undefined Behavior	Reported	CVE-2023-34867
26	Jerry	Undefined Behavior	Reported	CVE-2023-34868
27	Jerry	Stack Overflow	Reported	Issue 5074
28	Jerry	Heap Buffer Overflow	Reported	CVE-2023-38961
29	QJS	Stack Overflow	Fixed	CVE-2023-31922
30	QJS	Out-of-bounds Read	Confirmed	Issue 249
31	Jsish	Out-of-bounds Read	Confirmed	Issue 97
32	Jsish	Stack Overflow	Confirmed	CVE-2024-24186
33	Jsish	Use After Free	Confirmed	Issue 99
34	Jsish	Use After Free	Confirmed	CVE-2024-24189
35	escargot	Undefined Behavior	Fixed	Issue 1304
36	escargot	Undefined Behavior	Confirmed	Issue 1305
37	escargot	Undefined Behavior	Fixed	Issue 1306
38	escargot	Out-of-bounds Read	Fixed	Issue 1307
39	escargot	Out-of-bounds Read	Confirmed	Issue 1308
40	escargot	Out-of-bounds Read	Confirmed	Issue 1309
41	escargot	Stack Overflow	Fixed	Issue 1310
42	escargot	Undefined Behavior	Confirmed	Issue 1311
43	escargot	Undefined Behavior	Fixed	Issue 1313
44	escargot	Undefined Behavior	Fixed	Issue 1314
45	escargot	Undefined Behavior	Fixed	Issue 1315
46	escargot	Stack Overflow	Fixed	Issue 1316
47	escargot	Undefined Behavior	Fixed	Issue 1317
48	escargot	memcpy-param-overlap	Fixed	Issue 1318
49	escargot	Undefined Behavior	Fixed	Issue 1323
50	escargot	Null pointer dereference	Fixed	Issue 1324
51	escargot	dynamic-Stack-buffer-overflow	Confirmed	Issue 1332
52	escargot	global-buffer-overflow	Confirmed	Issue 1333
53	escargot	Out-of-bounds Read	Confirmed	Issue 1334
54	escargot	Invalid pointer passed to free()	Fixed	Issue 1335
55	escargot	Null pointer dereference	Fixed	Issue 1336
56	Espruino	Out-of-bounds Read	Fixed	CVE-2024-25201
57	Espruino	Stack Overflow	Fixed	CVE-2024-25200
58	hermes	Undefined Behavior	Confirmed	Issue 1357