03 연구 결과 > 도구 개발 > Redos > 기존 연구 소개

Redos Detector 관련 연구 소개

Redos Detector 종류

▪Static Method

- Redos 패턴에 대해 Rule 기반으로 탐지하는 방법론
- 정확도는 떨어지지만 소요시간이 짧음

▪Dynamic Method

- 정규표현식이 대한 실제 동작을 통해 악성 여부를 탐지하는 방법론
- 정확도는 높지만 소요 시간이 높음

▪Hybrid Method

- Static Method 와 Dynamic Method 를 둘 다 사용하는 방법론
- 최근 가장 높은 성능을 가진 방법론

| REDOS 탐지 방법론 별 통계 |

Approach	TY	TP	FP	FN	Precision	Recall	Avg Time (s)
RXXR2	S	1,488	105	174,362	93.41%	0.85%	0.3428
NFAA	S	3,949	284	171,901	93.29%	2.25%	1.5499
Rexploiter	S	8,689	3,450	167,161	71.58%	4.94%	0.6186
safe-regex	S	13,537	21,799	162,313	38.31%	7.70%	0.4865
Regexploit	S	888	32	174,962	96.52%	0.50%	**0.0007**
ReScue	D	1,107	**0**	174,743	**100.00%**	0.63%	3.5782
Regulator	D	26,479	**0**	149,371	**100.00%**	15.06%	336.0527
Revealer	H	4,720	**0**	171,130	**100.00%**	2.68%	1.3685
ReDoSHunter	H	44,005	**0**	131,845	**100.00%**	25.02%	1.5543
RENGAR	H	**175,850**	**0**	**0**	**100.00%**	**100.00%**	0.5828

03 연구 결과 > 도구 개발 > Redos > 기존 연구 소개

Rengar「Effective_ReDoS_Detection_by_Principled_Vulnerability_Modeling_and_Exploit_Generation」

Approach	TY	TP	FP	FN	Precision	Recall	Avg Time (s)
Revealer	H	4,720	0	171,130	**100.00%**	2.68%	1.3685
ReDoSHunter	H	44,005	0	131,845	**100.00%**	25.02%	1.5543
RENGAR	H	**175,850**	0	**0**	**100.00%**	**100.00%**	0.5828

RedosHunter 대비 Rengar 개선점

1. 정적 분석 알고리즘 개선

- 기존 RedosHutner나 Reveraler 의 패턴에는 정규표현식에 대해 제대로 해석하지 못하여 오탐, 미탐이 존재 ➔ 이를 위한 정적 분석 알고리즘 제시

순번	정규표현식	Redos Hunter	Reveral	Rengar
1	^(a(b|b)c)+$	미탐	탐지	탐지
2	^(a|ab)+$	오탐	탐지	탐지
3	^(a|b|ab)+$	탐지	미탐	탐지

RedosHunter

EOD Pattern:

R = $(r_1|r_2|\ldots|r_k\{m,n\})$, R is 취약하다.
regex if ∃ p ≠ q , $r_p.first \cap r_q.first \neq \emptyset$
or $r_q.first \cap r_q.followlast \neq \emptyset$

탐지 ^(a|b|ab)+$

r_1 r_2 r_3

∃ $r_1.first \cap r_2.first$ = {a} ≠ ∅ => Vuln

Reveral

Branch-in-Loop

$R = r_0(r_1(r_2|r_3)r_4) * r_5$, $r_1r_2r_4$ 와 $r_1r_3r_4$ 가 공통 문자열을 가지는 경우 취약하다.
or 문이 2개가 있을 경우까지는 고려하지 못함

$r_0 = r_1 = r_4 = r_5 = \varepsilon$

미탐 ^(a|b|ab)+$

r_2 r_3

∄ $r_1r_2r_4$ *and* $r_1r_3r_4$ 가 공통적인 문자열을 가지고 있으면 취약

Rengar

EOLS Pattern:

Quantifier (+, * 등) 가 존재하는 경우 펼쳐서 공통적인 것이 존재하는지를 확인

r_1 r_2 r_3

탐지 ^(a|b|ab)+$

{r1, r2, **r3**, r1r1, **r1r2**, …}

{a, b, **ab**, aa, **ab**, …}