2025년 전남대학교 소프트웨어중심대학사업
소·중·대 산학협력프로젝트(캡스톤디자인) 결과보고서

<table>
<tr><td colspan="2">프로젝트명</td><td colspan="6">분산 IP 기반 크리덴셜스터핑 탐지 및 방어</td></tr>
<tr><td colspan="2">Github url 주소</td><td colspan="6">https://github.com/choisein/3D.git</td></tr>
<tr><td colspan="2">팀 명</td><td colspan="2">3D</td><td>과제수행기간</td><td colspan="2">2025. 9. 24. ~ 12. 19.</td></tr>
<tr><td colspan="2">지도교수</td><td>학 과</td><td colspan="2">인공지능학부</td><td>성 명</td><td>조영준</td></tr>
<tr><td rowspan="8">프로젝트
수행인원
(※팀장은
첫줄에 기입)</td><td colspan="2">이 름</td><td>학과(부·복수전공)</td><td>학년</td><td>학번</td><td>연락처(HP)</td><td>E-Mail</td></tr>
<tr><td>팀장</td><td>최세인</td><td>소프트웨어공학과</td><td>3</td><td>231344</td><td>010-2429-2245</td><td>choisein8520@naver.com</td></tr>
<tr><td rowspan="5">팀원</td><td>손유채</td><td>소프트웨어공학과</td><td>3</td><td>214940</td><td>010-9967-0832</td><td>thsdbco@naver.com</td></tr>
<tr><td>조승범</td><td>소프트웨어공학과</td><td>4</td><td>213269</td><td>010-2721-7531</td><td>joeseungbeom@gmail.com</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">참여
기업</td><td colspan="2">기업명</td><td>멘토명</td><td>직위</td><td>연락처(HP)</td><td>E-Mail</td></tr>
<tr><td colspan="2">애드시티</td><td>조세근</td><td>대표</td><td>010-5583-5004</td><td>adct@adct.co.kr</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td><td></td></tr>
</table>

위와 같이 2025년 전남대학교 소프트웨어중심대학사업
산학협력프로젝트 지원 프로그램 결과보고서를 제출합니다.

2025년 12월 17일

신청자명(대표학생) : 최세인 (인)

지도교수 : 조영준 (인)

전남대학교 소프트웨어중심대학사업단장 귀하

산학협력프로젝트(캡스톤디자인) 결과보고서(요약)

프로젝트명	분산 IP 기반 크리덴셜스터핑 탐지 및 방어			
수행기간	2025. 9. 24. ~ 12. 19.		**소요예산**	96,874
소요예산 세부내역	chatgpt구독			
참여인원	**구분**	**인원수**	**성명(모두 기재)**	
	교수	1	김명진	
	석박사과정			
	학부생	3	최세인, 손유채, 조승범	
	기업체	1	(멘토) 조세근	
	계			

추진배경

○ 크리덴셜 스터핑은 유출된 계정 정보를 재사용해 다수의 서비스에 무단 접근을 시도하는 자동화된 사이버 공격으로, 개인정보·금융 정보 유출과 기업의 신뢰도 하락, 법적·재정적 손실을 초래한다. 특히 봇 기반 대규모 로그인 시도로 서비스 성능 저하까지 유발하므로, 이를 효과적으로 탐지하고 방어하는 체계 구축이 필수적이다.

목표 및 내용

○ 목표

위험 점수 기반 탐지 기법의 실효성을 검증하고 실제 서비스 환경에 적용 가능한 크리덴셜 스터핑 방어 체계를 제안한다. HTTP 헤더 기반 점수산정을 통해 공격 요청을 사전에 탐지하고 높은 탐지율을 확보한다. 또한 복잡한 고비용 모델 대신 규칙 기반 로직을 활용해 경제성과 효율성을 확보하며 오탐·미탐을 최소화하는 방향의 방어 구조를 설계한다.

○ 내용

로그인 요청 시 HTTP 헤더를 분석해 정상 사용자 환경과의 차이를 위험 점수로 정량화하고 점수가 높을수록 공격 가능성이 크다고 판단한다. 이를 기반으로 단계적 방어를 적용하며, 추가 방어 수단으로 인간의 반응 속도를 활용한 버튼 캡차를 제안한다. 해당 캡차는 사람과 봇의 물리적 차이를 이용해 자동화 공격을 효과적으로 구분하는 방어 기법이다.

기대효과

1. 위험 점수 기반 탐지 기법의 성능 검증
2. 실제 서비스 적용 가능성 확인
3. 오탐 및 미탐 최소화
4. 경제성 및 효율성 증대

1. 프로젝트 개요

프로젝트명	분산 IP 기반 크리덴셜스터핑 탐지 및 방어
주제영역	☐ 생활 ☐ 업무 ☐ 공공/교통 ☐ 금융/핀테크 ☐ 의료 ☐ 교육 ☐ 유통/쇼핑 ☐ 엔터테인먼트
기술분야	☐ IoT ☐ 모바일 ☐ 데스트톱 SW ☐ 인공지능 ☑ 보안 ☐ 가상현실 ☐ 빅데이터 ☐ 자동제어기술 ☐ 블록체인 ☐ 영상처리 ☐ 기타( )
성과목표	☐ 논문게재 및 포스터발표 ☐ 앱등록 ☐ 프로그램등록 ☐ 특허 ☐ 기술이전 ☐ 실용화 ☐ 공모전(*공모전명*) ☑ 기타(프로젝트 경험)

2. 프로젝트 추진배경

크리덴셜 스터핑(Credential Stuffing)이란 대규모 데이터 유출을 통해 확보한 사용자 계정 정보(ID/PW 쌍)를 재활용하는 사이버 공격이다. 이러한 공격은 다수의 사용자가 여러 웹사이트에서 동일한 패스워드를 사용하는 경향을 악용하는 것이며 한 곳에서 유출된 계정 정보를 가지고 다른 서비스로 무단 접근을 시도한다. 단순히 하나의 서비스만을 위협하는 것을 넘어 다수의 플랫폼에 걸쳐 광범위한 피해를 유발하는 지능적이고 연쇄적인 보안 위협이다.
공격 성공 시, 계정 소유자는 금융 정보 유출, 개인정보 도용 등의 직접적인 피해를 보게 되며 기업 측면에서도 고객 신뢰도 하락, 법적 책임, 시스템 복구 비용 등 막대한 손실이 발생한다. 또한 크리덴셜 스터핑 공격은 주로 봇(Bot)을 이용하여 초당 수십에서 수천 건의 로그인 시도를 자동화하기 때문에 대규모의 비정상적인 트래픽이 서비스의 성능 저하를 유발할 수 있다. 따라서 이를 탐지하고 방어하는 것은 서비스를 운영하는 데 있어 필수적이다.

3. 프로젝트(주제) 목표 및 내용

-목표
1. 위험 점수 기반 탐지 기법의 성능 검증
프로젝트에서 구현한 웹 페이지에 공격을 시도한 결과 공격의 약 83%가 7점 이상으로 높게 측정됨으로써 점수 기반 탐지 로직의 효용성을 확인하였다.

2. 실제 서비스 적용 가능성 확인
현재 단계에서는 실제 로그인 데이터와 로그인 로직을 확보하여 분석하는 데 한계가 존재한다. 따라서 추후 과제로 구축한 방어 시스템이 실제 환경에서 얼마나 효과적으로 작동할지 검증이 필요하다.

3. 오탐 및 미탐 최소화
1차 탐지에서 87%의 탐지율과 13%의 미탐률을 확인하였다. 의심 로그인 요청을 효과적으로

선별할 수 있는 비교적 높은 수준의 탐지 성능을 나타낸다. 비록 2차 방어 수단인 캡차의 유효성은 검증하지 못하였으나 1차 탐지만으로도 공격의 대부분을 사전에 식별할 수 있음을 확인하였다.

4. 경제성 및 효율성 증대
고비용의 복잡한 모델 대신, HTTP 헤더를 통한 환경 분석이라는 단순한 규칙 기반 로직을 설계하여 비용을 절감하였다. 개발된 시스템이 실제 서비스에 적용될 수 있도록 추가적인 분석을 진행한다면 RBA 상용화에 기여할 수 있을 것으로 생각된다.

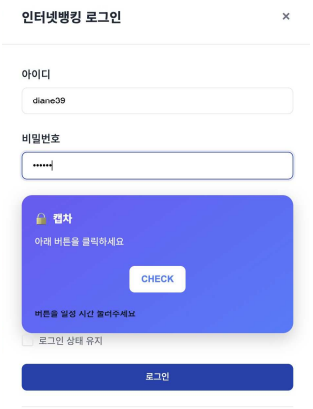
-내용
1) 탐지 방법: 정상 사용자 로그인 기록 분석을 통한 현재 로그인 요청 점수산정

서버는 사용자로부터 로그인 요청이 들어오고 로그인에 성공할 때마다 요청에 대한 HTTP 헤더 요소들을 기록하고 다음 요청이 들어오면 이 기록에서 얼마나 벗어났는지를 정량적으로 측정한다. 사용자의 환경 정보를 통해 측정된 점수는 위험 점수이며 점수가 높을수록 공격자로 간주한다.
이러한 시스템은 공격자가 정상 사용자의 모든 고유 환경 요소를 완벽하게 재현하기는 어렵다는 점을 이용한다.

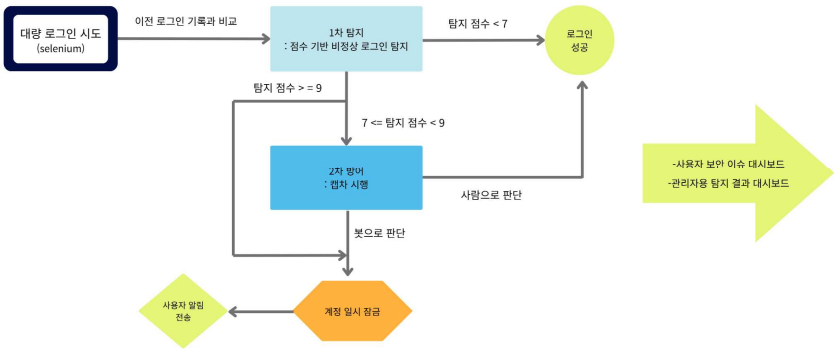
lognum	Usernum	IP	location	date	riskscore	risklevel	success (로그인 성공 여부 (1=성공, 0=실패))
4590	5607	69.172.211.61	United States Los Angeles	2025-12-12 20:25:26	17	17	0
4591	8276	59.15.58.10	South Korea Yeongdeungpo-gu	2025-12-12 20:25:28	9	9	0
4592	7452	118.34.196.170	South Korea Osan	2025-12-12 20:25:30	5	5	0
4593	1410	220.76.29.78	South Korea Jongno-gu	2025-12-12 20:25:32	9	9	0
4594	6817	89.188.14.66	The Netherlands Lelystad	2025-12-12 20:25:34	8	8	0
4595	9430	211.178.201.40	South Korea Seoul	2025-12-12 20:25:36	8	8	0
4596	5586	120.241.40.221	China Guangzhou	2025-12-12 20:25:39	9	9	0
4597	2650	118.35.39.152	South Korea Changwon	2025-12-12 20:25:41	9	9	0
4598	5015	69.172.148.86	Canada Chilliwack	2025-12-12 20:25:43	9	9	0
4599	2376	211.178.110.176	South Korea Gangseo-gu	2025-12-12 20:25:44	16	16	0
4600	9700	175.209.158.8	South Korea Seocho-gu	2025-12-12 20:25:46	10	10	0
4601	9825	91.241.129.100	Russia Simferopol	2025-12-12 20:25:48	16	16	0
4602	2350	175.210.126.243	South Korea Incheon	2025-12-12 20:25:50	15	15	0
4603	4438	172.218.198.104	Canada Squamish	2025-12-12 20:25:52	19	19	0
4604	1541	220.76.85.25	South Korea Songpa-gu	2025-12-12 20:25:55	18	18	0
4605	5698	183.233.248.74	China Shenzhen	2025-12-12 20:25:57	17	17	0
4606	5927	118.34.179.188	South Korea Suwon	2025-12-12 20:26:00	8	8	0
4607	2506	175.210.201.102	South Korea Bucheon-si	2025-12-12 20:26:02	6	6	0

2) 방어 기법: 반응 속도를 이용한 버튼 캡차

산정된 위험 점수를 기준으로 방어 단계를 두어 오탐률을 최소화하고 방어 효용성을 극대화한다. 프로젝트에서 제안하는 버튼 캡차는 인간의 고유한 반응 속도에 대한 한계를 이용하는 새로운 캡차이다.
사람의 클릭은 손가락이나 마우스로 버튼을 누르고 유지했다가 떼는 과정이며 이 과정에는 일정 시간이 소요된다. 페이지가 짧은 간격으로 렌더링 될 때 버튼 눌림 횟수를 측정한다면 사람과 봇을 구분할 수 있다.
짧은 시간 안에 여러 번의 신호가 들어온다면 사람으로, 단 한 번의 신호가 들어온다면 봇으로 판단한다.
이러한 방어 시스템은 인간의 물리적 한계와 프로그램의 정확성을 이용한다.



4. 시스템 구성 및 내용



5. 프로젝트 결과물에 대한 기술

1) 위험 점수 산정표

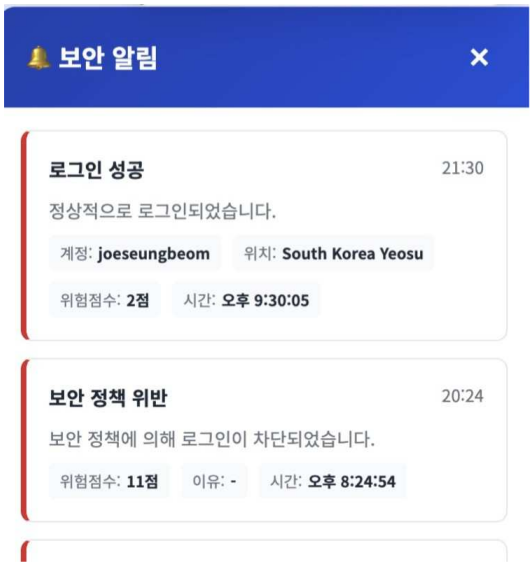
	항목	점수 기준
사용자 환경 비교용	ip	동일 도시, 다른 IP인가 ⇒1점 동일 국가, 다른 IP인가 ⇒ 2점 다른 국가 IP인가 ⇒ 3점 알려진 악성 ip인가 ⇒ 10점
	user-agent	브라우저/os의 버전이 다른가 ⇒ 1점 os가 변경되었나 ⇒ 2점 누락, 비어있는가 ⇒ 1점 스캐너 및 봇인가 ⇒ 10점
	accept-language	클라이언트가 다른 언어를 지원하는가 ⇒ 2점
정상적인 login context 확인용	referer	referer 헤더가 없는가 ⇒ 2점 host 헤더와 일치하지 않는 외부 도메인인가 ⇒ 2점
	accept	accept 헤더가 비었는가 ⇒ 2점 브라우저(user-agent) 정보와 다른가 ⇒ 10점
	sec-fetch	최신 브라우저인데 sec-fetch 헤더가 없는 경우 ⇒ 10점

2) 캡차 시행 기준

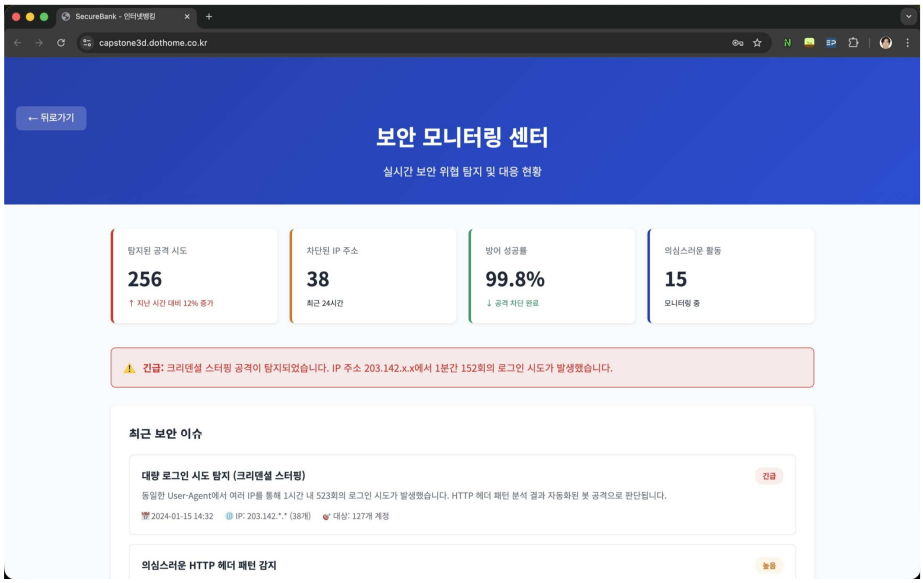
점수	총 빈도 (건)	전체 공격 시도에서 차지하는 비율
3점	9	0.51%
4점	24	1.35%
5점	38	2.14%
6점	213	12.01%
7점	207	11.67%
8점	364	20.53%
9점	918	51.78%
합계	1,773	100.00%

공격의 약 83%인 7점 이상을 캡차 시행 기준으로 선정

3) 사용자 대시보드 (보안 알림)



관리자 대시보드 (보안 모니터링)



구분	기능정의	세부기능 설명
1.	위험 점수산정표	1) IP 및 HTTP 헤더 기반 점수산정 ㄱ. 사용자 환경 비교 사용자 환경의 변화를 감지하기 위해 IP, User-Agent, Accept-Language를 분석한다. ㄴ. 정상적인 login context 확인 요청의 출처와 구성이 정상적인 로그인 시나리오에 부합하는지 확인하여 비정상적인 접근 시도를 탐지한다. 이를 위해 Referer, Accept, Sec-Fetch 헤더를 분석한다. 2) 요소별 점수 기준 ㄱ. 위험도 등급별 점수 분류 *확실한 봇: 10점 *위험도 높음: 3점 *위험도 중간: 2점 *위험도 낮음: 1점
2.	캡차 시행 기준	6점 이상을 캡차 기준 점수로 선정할 경우 공격의 약 96%가 탐지되어 정상 사용자가 섞여 있을 확률이 높다. 따라서 오탐을 줄이고 사용자 경험을 높이기 위해 캡차 임계치를 7점으로 설정하였다.
3.	로그인 성공/차단 점수 임계치	7점 미만: 로그인 성공 7점 이상 9점 미만: 캡차 시행 9점 이상: 로그인 차단 (메인페이지로 돌아감)
4.	버튼 캡차	1. 동적 버튼 교체 기반 CAPTCHA 방어 메커니즘 ㄱ. 핵심 원리: DOM 요소를 10ms 간격으로 제거 후 재생성하여 사람과 봇의 물리적 반응 속도 차이를 활용한다. 봇이 버튼 참조를 저장해도 10ms 후 해당 메모리 주소의 요소는 이미 삭제됨으로 사전에 이벤트 리스너를 등록하거나 DOM 조작을 시도하는 모든 자동화 공격을 무력화한다. ㄴ. 판정 기준: ▷ 0회: 버튼을 클릭하지 않음 → 재시도 (50점) ▷ 1회: DOM 재생성을 감지하지 못한 단순 봇 →

		봇 확정 (80점) ▷ 2~50회: 정상적인 사람의 반응 속도 → 정상 (0점) ▷ 50회 초과: 물리적으로 불가능한 속도 → 봇 확정 (100점) 2. 마우스 궤적 분석을 통한 이중 검증 ㄱ. 분석 지표 1) 직선성 (Linearity): ▷ 사람: 0.5~0.8 (곡선 형태의 자연스러운 이동) ▷ 봇: 0.9~1.0 (거의 완벽한 직선) 2) 속도 표준편차 (Std Deviation): ▷ 사람: 0.3~0.8 (가속→감속 반복) ▷ 봇: 0.01~0.1 (일정한 속도) 직진성, 속도 표준편차에 각각 +30점씩 가중치 부여했으며 50점이 넘으면 봇으로 판정한다.
5.	사용자 알림/ 관리자 대시보드	1) 사용자 알림 사용자 계정 로그인 시 로그인 성공 (위험 점수, 로그인 시간) 알림이 뜬다. 해당 계정으로 로그인 공격 시도가 있었고 차단 된 경우, 알림이 전송된다. 2)관리자 대시보드 탐지된 공격 시도, 의심되는 로그인 시도 등을 관리할 수 있는 모니터링 페이지이다. 대량 로그인 시도나 의심스러운 헤더 패턴이 감지될 시 관리자 대시보드에 나타난다.
6.	탐지율 및 미탐률	버튼 캡차의 경우 스크립트 기반의 캡차 자동 통과 로직을 구현하지 못하여 2차 방어 단계의 유효성을 확인하지 못하였다. 따라서 최종 로그인 성공 횟수는 1차 탐지를 우회한 횟수이다. - 탐지율 및 미탐률 (2차 방어를 제외한 1차 탐지의 결과) • 총 유효 계정 시도 (P): 200회 • 캡차 요구 및 차단된 시도 (TP): 51회(캡차) + 123회(차단) = 174회

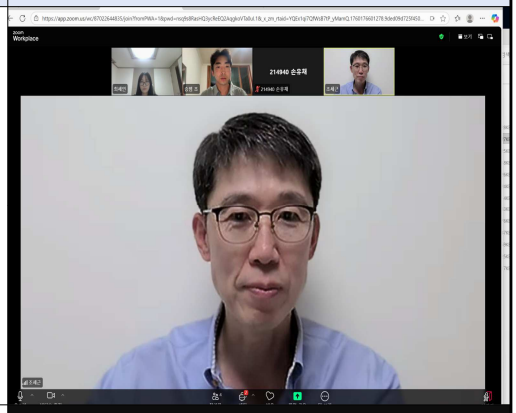
		• 로그인 성공 시도 (FN): 26회 탐지율 (TPR) = $\frac{\text{캡차/차단 횟수}}{\text{총 유효 시도 횟수}} = \frac{174}{200} = 0.87\,(87\%)$ 미탐률 (FNR) = $\frac{\text{로그인 성공 횟수}}{\text{총 유효 시도 횟수}} = \frac{26}{200} = 0.13\,(13\%)$

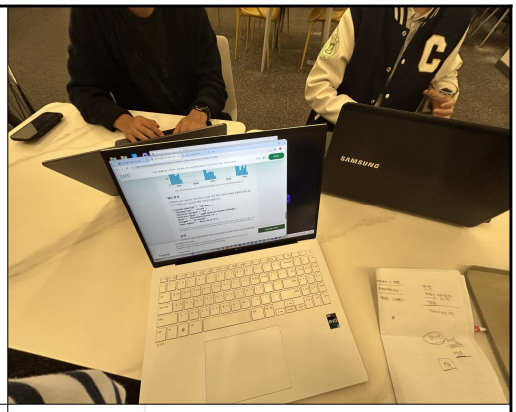
6. 프로젝트 진행내용

1) 참여인원 및 담당 역할

연번	소속학과	성명	수행역할 분담내용
1	소프트웨어공학과	최세인	보안 로직, 공격/점수산정 스크립트 작성
2	소프트웨어공학과	손유채	백엔드
3	소프트웨어공학과	조승범	프론트엔드

2) 회의 및 SW멘토링 진행

번호	일시/장소	회의/멘토링 내용(상세히 작성)	관련 사진
1	2025.10.11. 19시 (줌)	- 프로젝트 계획서 검토 및 방향성에 대한 멘토링 진행	
2	2025.11.25. 19시 (줌)	- 결과보고서 작성 및 발표 점검에 대한 멘토링 진행	

3	2025.10.29. 18시 (카페)	-진행상황 점검 및 탐지 방법 추가 아이디어 논의 진행	
4	2025.11.28. 13시 (도서관 그룹스터디룸)	- 진행상황 점검 - 모의 공격 시도	2025.11.28 O 13:00~14:30 그룹스터디룸 09호 사용완료
5.	2025.12.02. 18시 (도서관 그룹스터디룸)	- 최종 발표를 위한 점검 및 탐지율 측정	2025.12.02 O 18:00~20:00 그룹스터디룸 10호 사용완료

7. 프로젝트 세부일정 및 내용

No.	작업 내용	9월				10월				11월				12월				담당자	비고
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
	크리덴셜 스터핑 공격원리 및 기존 방어 학습			■	■														
	사용자 계정 +데이터베이스 구축			■	■														
	웹서비스 로그인 페이지 개발					■	■												
	점수 기반 로직 개발							■	■										
	공격 및 점수 산정 스크립트 작성									■	■								
	로그인 공격 시도+ 캡차 개발											■	■	■	■				
	관리자/사용자 페이지 개발													■	■				
	탐지율 테스트													■	■				

8. 결과물에 대한 향후 활용계획

-프로젝트의 개선 방향

1. 실제 환경 기반 로직 재검토 및 검증

주요 서비스의 로그인 트래픽을 확보하고 심층적으로 분석하여 현재 설정된 각 항목의 점수 기준과 위험 임계치를 재조정해야 한다. 또한 실제 서비스 인증 방법들을 심층적으로 분석하여 본 프로젝트의 탐지 및 방어 로직의 보완이 필요하다.

2. 버튼 캡차 검증

캡차를 통과할 수 있는 자동화 스크립트를 작성하고 캡차의 유효성을 확인하는 과정이 필요하다. 공격 시도에 대해 2차 방어까지 거친 최종 탐지율을 확인해야 한다.

개선 방향을 바탕으로 향후 과제를 해결하고 다음 프로젝트에 연계하여 실시간성 도입 및 ai 모델 활용을 고려하고 있다.

9. 참고자료 및 문헌

[1] Vincent Unsel, Stephan Wiefling, Nils Gruschka, and Luigi Lo Iacono. 2023. Risk-Based Authentication for OpenStack: A Fully Functional Implementation and Guiding Example: Data/Toolset paper. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY'23), April 24–26, 2023, Charlotte, NC, USA. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3577923.3583634

[2] A Study on User Authentication Model Using Device Fingerprint Based on Web Standard* Sohee Park,1† Jinhyeok Jang,2 Daeseon Choi3‡ KERIS(Administration Specialist), 2,3Kongju National University(Graduate student, Professor

[3] Stephan Wiefling, Luigi Lo Iacono1 and Markus D¨urmuth
Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild