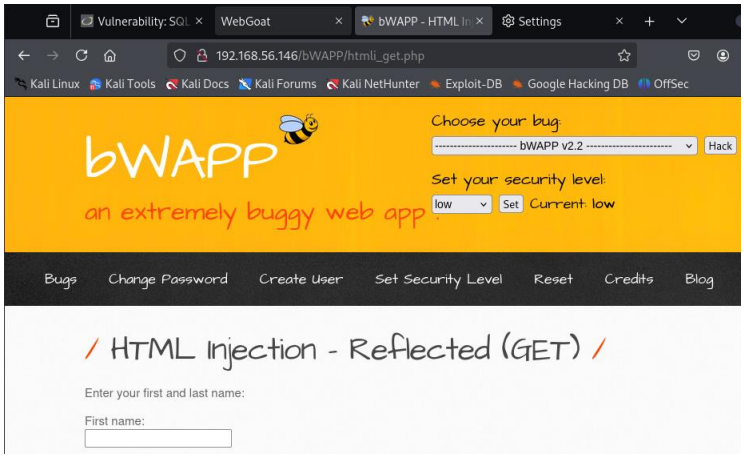
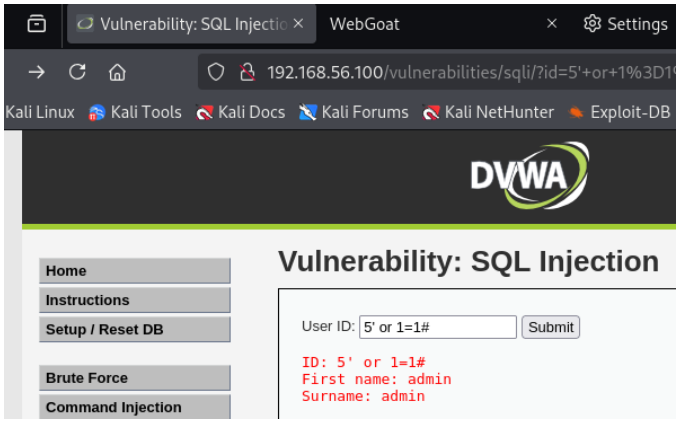
1.1 ~ 1.2 애플리케이션보안과 관련하여 OWASP(Open Web Application Security Project)에 대해 간단히 서술하시오.

OWASP (Open Worldwide Application Security Project) 란 웹 애플리케이션 보안 향상을 위한 오픈 소스 프로젝트이다. 주요 목적으론 애플리케이션 보안 인식 증진, 개발자들이 보안 코딩을 쉽게 배울 수 있게 지원하고 표준화된 보안 가이드라인을 제공하는 것이다. 전 세계 개발자, 보안 전문가, 연구자들이 자발적으로 참여하여 실용적인 자료와 도구를 무료로 제공한다.

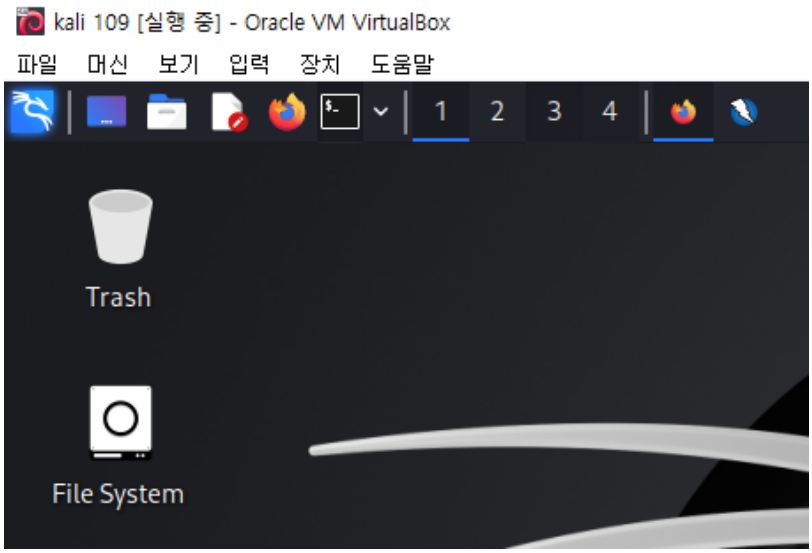
1.2 실습에 필요한 도구들을 설치하고 점검하여 정상적으로 운영이 가능하도록 설정하시오.



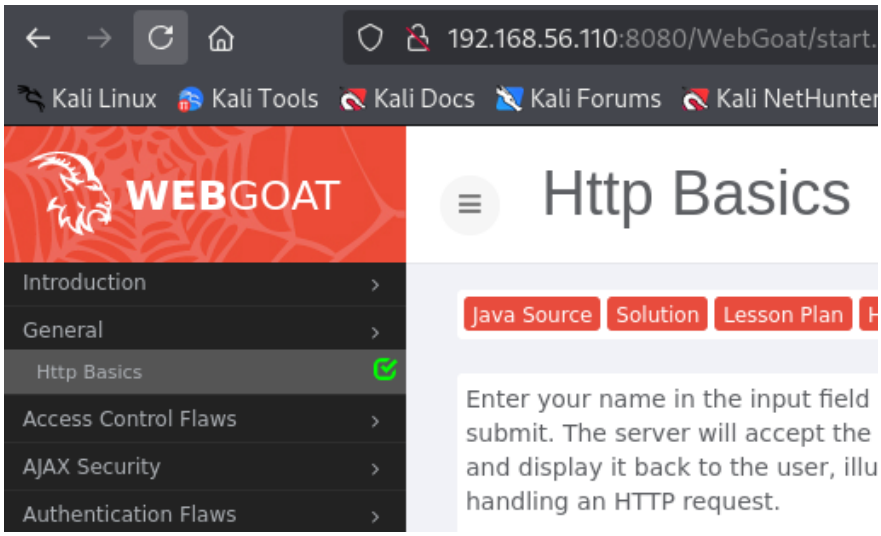
bWAPP



DVWA



Kali Linux



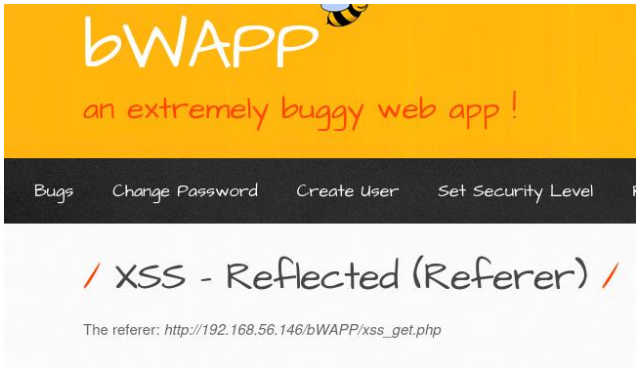
WebGoat

```
<IfModule mod_security2.c>
    # Default recommended configuration
    SecRuleEngine On
    SecRequestBodyAccess On
    SecRule REQUEST_HEADERS:Content-Type "text/xml" \
         "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"
    SecRequestBodyLimit 13107200
    SecRequestBodyNoFilesLimit 131072
    SecRequestBodyInMemoryLimit 131072
    SecRequestBodyLimitAction Reject
    SecRule REQBODY_ERROR "!@eq 0" \
    "id:'200001', phase:2,t:none,log,deny,status:400,msg:'Failed to parse request body.',l
or_msg}',severity:2"
    SecRule MULTIPART_STRICT_ERROR "!@eq 0" \
    "id:'200002',phase:2,t:none,log,deny,status:400,msg:'Multipart request body \
```

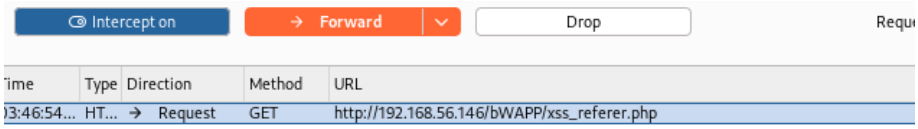
WAF (ModSecurity 모듈이 Apache 웹 서버에 설치될 때 자동으로 생성되는 설정 파일 내용)

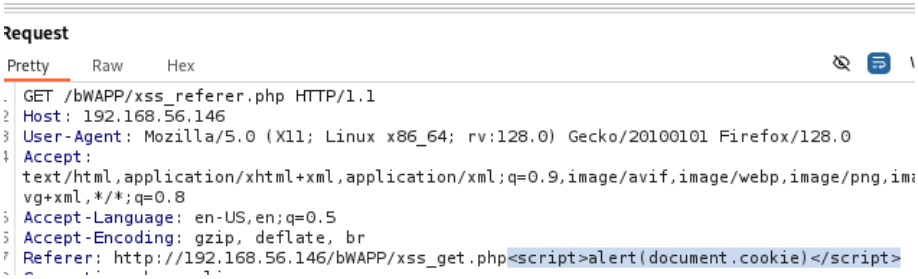
2.1 ~ 2.3 bWAPP / DVWA에서 XSS 취약점에 대해 공격을 실행하고 그 대응 방안에 대해서 테스트 및 서술하여 화면 저장하시오.

bWAPP : XSS - Reflected (Referer)



Burf suite로 Intercept On 후 페이지 새로고침

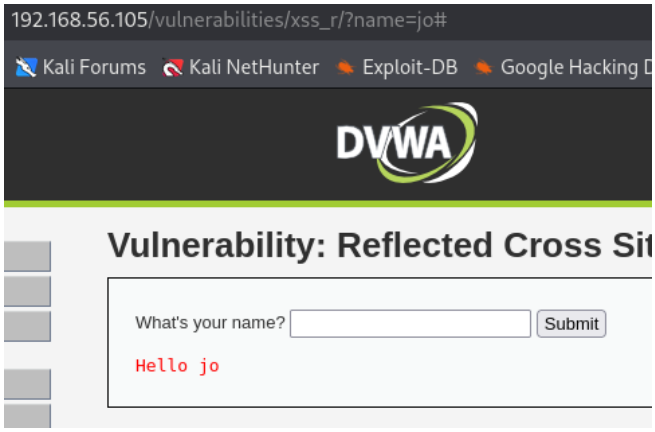




Referer 뒤에 cookie 값을 출력하는 스크립트를 삽입한다

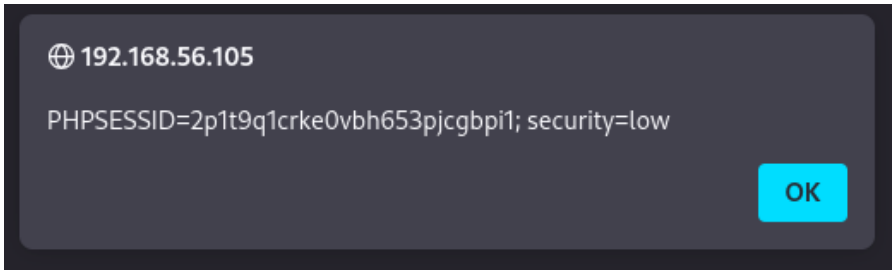
Forward 후 bWAPP 웹을 확인하면 스크립트 그대로 출력되는걸 확인

DVWA : Vulnerability: Reflected Cross Site Scripting (XSS)



이름을 입력하면 출력이 되는 형식이다

작성 가능한 칸에 cookie 값을 출력하는 스크립트를 입력한다



취약점이 존재해 스크립트 명령어 그대로 출력되는 모습을 확인

XSS 취약점 대응 방안은 입력 검증 (사용자 입력 제한), 출력 이스케이프 (HTML/JS 출력 시 <, > 변환), 템플릿 엔진 활용 (자동 이스케이프 지원), CSP 적용 (브라우저에서 스크립트 제한), HttpOnly 쿠키 (JS로 세션 탈취 방지) 등이 있다.

2.4 최신의 애플리케이션 보안 솔루션 동향을 파악하고 어떤 솔루션들이 있는 지 서술하시오.

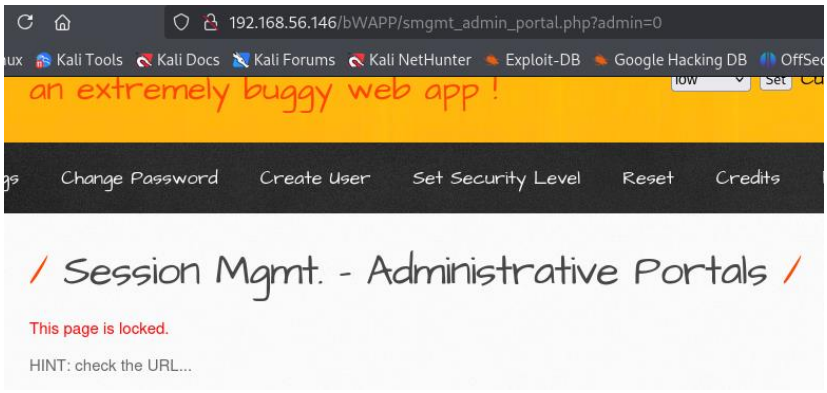
애플리케이션 보안은 점차 지속적이고 자동화된 보안 테스트, 클라우드 기반 대응, 그리고 개발 환경에 통합된 보안 활동으로 진화하고 있다. 이를 위해 다양한 유형의 보안 솔루션이 존재하며, 조직의 환경에 맞는 솔루션을 선택하고 통합하는 것이 중요해 졌다. 또한 AI 및 머신러닝 기반 기술을 활용해, 사용자 행위 이상 탐지(UEBA), 자동화된 위협 분석, 악성 요청 패턴 탐지 등의 기능을 수행하는 보안 솔루션이 늘어나고 있다. 이를 통해 알려지지 않은 위협에 대해서도 보다 능동적인 대응이 가능해지고 있다. 이러한 보안 솔루션을 통해 애플리케이션의 신뢰성과 안전성을 확보할 수 있다.

주요 보안 솔루션으론 아래 목록 등이 있다.

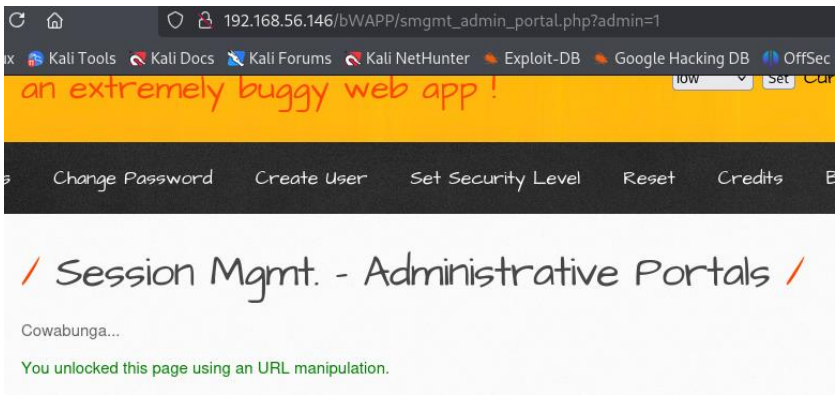
SAST - 코드 분석 (SonarQube, Fortify)
DAST - 실행 중 테스트 (ZAP, Burp Suite)
SCA - 오픈소스점검 (Snyk, Black Duck)
WAF – 웹 방화벽 (Cloudflare WAF, AWS WAF)
컨테이너 보안 – 이미지 검사 (Aqua, Prisma Cloud)

3.1 ~ 3.2 Kali 에서 WebGoat/bWAPP 로 2 개 이상의 취약점에 대해 공격을 실행하여 테스트하여 화면 저장하시오.

bWAPP : Session Mgmt. - Administrative Portals



주소창을 자세히 보면 admin 파라미터가 그대로 노출되어있는 것을 확인 할 수 있다



파라미터값을 1 로 바꾸면 성공

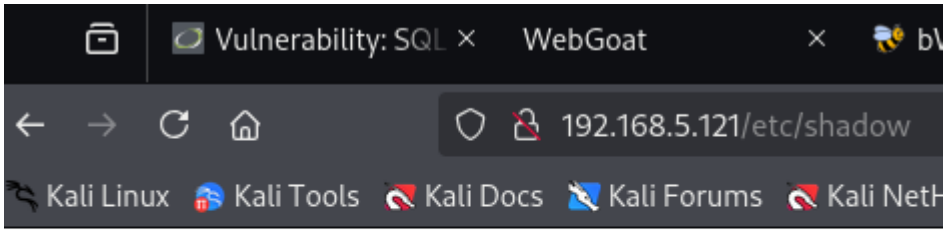
bWAPP : HTML5 Web Storage (Secret)

개발자 도구로 들어가 Storage 목록을 살펴보면 Local Storage 에 secret 가 숨겨져 있는 것을 찾을 수 있다.

3.3 ~ 3.4 Kali -> Wordpress 로의 웹해킹 공격에 대해 WAF(mod_security)의 Rule 설정을 완료하고 공격에 대한 로그를 탐지하고 확인하시오.

```
SecDefaultAction "phase:2,deny,log,status:406"
SecRule REQUEST_URI "etc/passwd" "id:'300001'"
SecRule REQUEST_URI "etc/shadow" "id:'300002'"
SecRule REQUEST_URI "../" "id:'300003'"
```

WAF rule 설정



Not Acceptable

An appropriate representation of the requested resource

```
[Tue Apr 15 16:30:43.153163 2025] [:error] [pid 2938:tid 2977] [client 192.168.5.109:58558] [client 192.168.5.109] ModSecurity: Access denied with code 406 (phase 2). Pattern match "etc/passwd" at REQUEST_URI. [file "/etc/httpd/modsecurity.d/activated_rules/ruleset-01.conf"] [line "2"] [id "300001"] [hostname "192.168.5.121"] [uri "/etc/passwd"] [unique_id "Z_4LI7qCku6D-pgU84DxKgAAAMs"]
```

```
[Tue Apr 15 16:31:07.132387 2025] [:error] [pid 2938:tid 2980] [client 192.168.5.109:34232] [client 192.168.5.109] ModSecurity: Access denied with code 406 (phase 2). Pattern match "etc/shadow" at REQUEST_URI. [file "/etc/httpd/modsecurity.d/activated_rules/ruleset-01.conf"] [line "3"] [id "300002"] [hostname "192.168.5.121"] [uri "/etc/shadow"] [unique_id "Z_4LO7qCku6D-pgU84DxKwAAAM4"]
```

```
[Tue Apr 15 16:29:43.039799 2025] [:error] [pid 2938:tid 2966] [client 192.168.5.109:52404] [client 192.168.5.109] ModSecurity: Access denied with code 406 (phase 2). Pattern match "../" at REQUEST_URI. [file "/etc/httpd/modsecurity.d/activated_rules/ruleset-01.conf"] [line "4"] [id "300003"] [hostname "192.168.5.121"] [uri "/wp-includes/js/wp-emoji-release.min.js"] [unique_id "Z_4K57qCku6D-pgU84DxKQAAAMA"], referer: http://192.168.5.121/
```

Kali -> Wordpress 로 설정한 룰대로 각 공격을 실행한 결과 접속이 제한되고 rule 300001 ~ 300003 이 실시간 탐지되는 것을 확인

4.1 ~ 4.3

OWASP TOP 10 및 신규 위협에 대비하기 위해 애플리케이션 보안 솔루션(소소코드 취약점 진단)에 대한 특징과 업데이트 하는 방법에 대해 서술하시오.

소스코드 취약점 진단 도구는 애플리케이션 개발 중 또는 배포 전에 코드를 분석해 보안 취약점을 자동으로 탐지하는 도구로, OWASP Top 10 과 같은 보안 기준을 기반으로 동작한다. 정적 분석(SAST) 방식을 사용해 실제 실행 없이 빠르고 반복적인 분석이 가능하며, SQL Injection, XSS 등 주요 취약점을 자동으로 찾아낸다. 대부분의 도구는 IDE 나 CI/CD 와 연동되어 개발 단계에서 실시간 보안 경고를 제공하고, 수정 가이드를 함께 제시한다. 일부 도구는 코드 품질 분석도 지원해 개발 효율성까지 높일 수 있다.

최신 보안 위협에 대응하기 위해서는 도구의 정기적인 업데이트가 필요하다. OWASP 최신 규칙셋 적용, 도구 및 플러그인의 버전 유지, 그리고 새로운 언어나 프레임워크에 대한 진단 기능 추가 등이 주요 업데이트 방법이다.