



# 최종 보고서

클라우드 기반 보안 인프라 설계와 웹 해킹 로그 데이터 분석

팀장 : 정진욱  
팀원: 김해겸, 이해경, 임성준





# 목차

1. 목적 및 개요
2. **WBS**
3. 클라우드 아키텍처
4. **pfsense**
5. 웹 해킹
6. **ELK**
7. 진행하면서 어려웠던 점





### 프로젝트의 주요 목적:

클라우드 기반 웹 서비스 환경에서의 보안 취약점을 파악하고 이를 해결하는 방법을 학습하는 것입니다. AWS와 같은 클라우드 환경에서 웹 서비스를 구축하고, 실제 해킹 시나리오를 통해 보안 취약점을 찾아내는 과정을 통해, 실제 웹 서비스 운영에 대한 깊은 이해와 보안 강화 방법에 대한 지식을 얻는 것이 목표입니다.

### 개요:

본 프로젝트는 크게 세 가지 단계로 구성되어 있습니다.

- 1. 클라우드 환경 구축:** AWS VPC 설정과 EC2 인스턴스 설계 등으로 클라우드 기반 인프라를 구축합니다.
- 2. 서비스 환경 설정:** 웹 서버와 데이터베이스 연동, ELK Stack 설정 등으로 실제 서비스가 운영될 수 있는 환경을 만듭니다.
- 3. 보안 설정 및 검증:** pfSense 방화벽 설정과 같은 보안 조치를 적용하고, 실제 해킹 시나리오를 수행하여 그 효과를 검증합니다.





**1. 클라우드 기반 서비스의 중요성:** 현재 IT 트렌드에서 클라우드 기반 서비스의 중요성은 더욱 증가하고 있습니다. 다양한 기업들이 자신들의 비즈니스를 클라우드 환경으로 이전하면서, 해당 환경에서의 보안 지식이 필수적인 역량으로 부상하였습니다.

**2. 보안 취약점에 대한 실질적인 이해:** 실제 해킹 시나리오를 통해 보안 취약점을 직접 찾아내고, 그 해결 방법을 모색하는 과정은 이론적인 학습만으로는 얻기 어려운 깊은 이해와 경험을 얻을 수 있습니다.

**3. 실질적인 보안 강화 방법 학습:** pfSense 등 실제로 널리 사용되는 보안 도구와 방법론에 대한 학습은 저와 팀원들이 IT 업계에서 요구되는 실질적인 역량을 키울 수 있는 좋은 기회라고 생각했습니다.

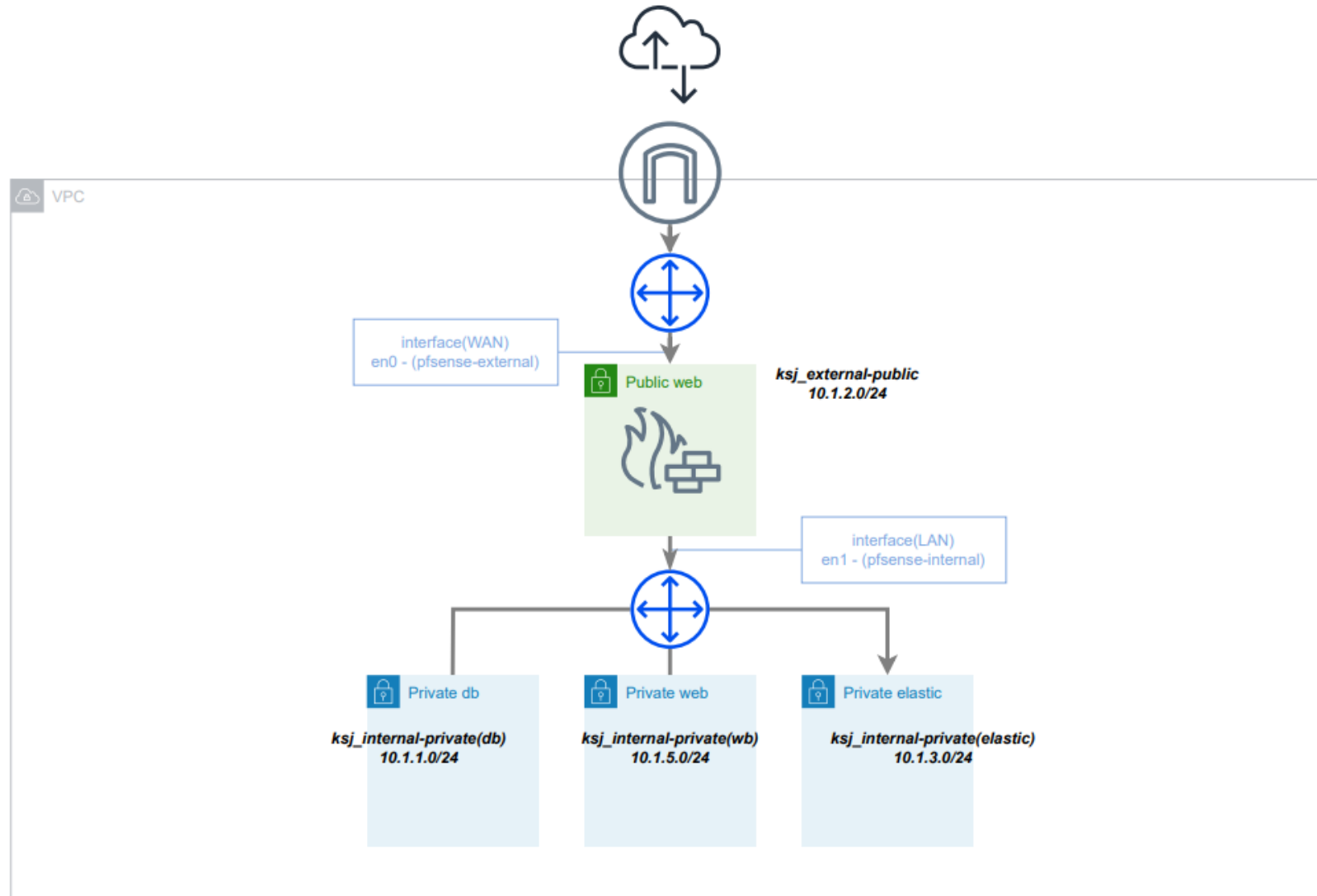
이러한 이유를 기반으로 본 프로젝트를 통해 참여자들이 클라우드 환경과 웹 서비스 보안에 대한 깊은 지식과 경험을 쌓게 되어, IT 분야에서 더욱 전문적인 역량을 갖추 수 있게 될 것이라고 생각합니다.





구분	주요 업무	세부 업무	1M				결과물
			1	2	3	4	
프로젝트 계획 및 설계	프로젝트 일정 계획	WBS 작성	■				WBS
		팀원 역할 분배 및 일정 조율	■				
	프로젝트 설계	클라우드 아키텍처 설계	■	■			클라우드 아키텍처
클라우드 환경 구축	AWS 환경 설정	vpc설정		■	■		
	인프라 구축	WEB, DB 연동		■	■		
		인스턴스 설계 및 인프라 구축		■	■	■	
		ELK Stack		■	■	■	
	네트워크 환경 구축	pfsense 방화벽			■	■	
웹 해킹	웹 서버 환경 구축		■				
		웹 페이지 제작		■	■	■	웹 사이트
	웹 해킹	웹 해킹 시나리오 작성			■		
		웹 해킹 공격 수행				■	웹 해킹 보고서
최종 결과	최종 보고서 작성	최종 보고서 작성				■	최종 보고서
		발표 자료 준비 및 발표				■	발표 자료







## VPC - 10.1.0.0/16

VPC (1/2) 정보

↺ 1 ↻

VPC 생성

Name	VPC ID	상태	IPv4 CIDR	IPv6 CIDR	DHCP 옵션 세트	기본 라우팅 테이블	기
-	vpc-0c1972f04a515f22f	Available	172.31.0.0/16	-	dopt-00c1419b50aaa5...	rtb-08dc56025debd99be	ac
test_tutorial	vpc-095cbe9d8d260ed1c	Available	10.1.0.0/16	-	dopt-00c1419b50aaa5...	rtb-07347514fb7dc23e3	ac

vpc-095cbe9d8d260ed1c / test\_tutorial

세부 정보

리소스 맵

CIDR

플로우 로그

태그

통합

세부 정보

VPC ID

vpc-095cbe9d8d260ed1c

태연시

Default

기본 VPC

아니요

네트워크 주소 사용 지표

비활성화됨

상태

Available

DHCP 옵션 세트

dopt-00c1419b50aaa59dc

IPv4 CIDR

10.1.0.0/16

Route 53 Resolver DNS 방화벽 규칙 그룹

-

DNS 호스트 이름

활성화됨

기본 라우팅 테이블

rtb-07347514fb7dc23e3

IPv6 플

-

소유자 ID

795691197490

DNS 확인

활성화됨

기본 네트워크 ACL

acl-087ad8e6e46bb0175

IPv6 CIDR(네트워크 경계 그룹)

-



# Internet gateway



인터넷 게이트웨이 (1/2) 정보

Q 인터넷 게이트웨이 필터링

< 1 > ⚙

🔄

작업 ▼

인터넷 게이트웨이 생성

<input type="checkbox"/>	Name ▼	인터넷 게이트웨이 ID ▼	상태 ▼	VPC ID ▼	소유자 ▼
<input checked="" type="checkbox"/>	pfsense-tutorial	igw-027f0ebb9a2453501	✔ Attached	vpc-095cbe9d8d260ed1c   test_tutorial	795691197490
<input type="checkbox"/>	-	igw-0e874f338892a4850	✔ Attached	vpc-0c1972f04a515f22f	795691197490

igw-027f0ebb9a2453501 / pfsense-tutorial

세부 정보

태그

세부 정보

인터넷 게이트웨이 ID

📄 igw-027f0ebb9a2453501

상태

✔ Attached

VPC ID

vpc-095cbe9d8d260ed1c | test\_tutorial

소유자

📄 795691197490







subnet-01260126942a21a14 / ks\_j\_external-public(web)

[세부 정보](#) | [플로우 로그](#) | [라우팅 테이블](#) | [네트워크 ACL](#) | [CIDR 예약](#) | [공유 중](#) | [태그](#)

## 세부 정보

서브넷 ID subnet-01260126942a21a14	서브넷 ARN arn:aws:ec2:ap-northeast-2:795691197490:subnet/subnet-01260126942a21a14	상태 Available	IPv4 CIDR 10.1.2.0/24
사용 가능한 IPv4 주소 250	IPv6 CIDR -	가용 영역 ap-northeast-2a	가용 영역 ID apne2-az1
네트워크 경계 그룹 ap-northeast-2	VPC vpc-095cbe9d8d260ed1c   test_tutorial	라우팅 테이블 rtb-07347514fb7dc23e3   ks_j_pfsense-externalpublic	네트워크 ACL acl-087ad8e6e46bb0175
기본 서브넷 아니요	퍼블릭 IPv4 주소 자동 할당 아니요	IPv6 주소 자동 할당 아니요	고객 소유 IPv4 주소 자동 할당 아니요
고객 소유 IPv4 풀 -	Outpost ID -	IPv4 CIDR 예약 -	IPv6 CIDR 예약 -

- public (ks\_j\_external-pulick(web)) - 10.1.2.0/24

subnet-037f5efd0521e3b49 / ks\_j\_internal-private(web)

[세부 정보](#) | [플로우 로그](#) | [라우팅 테이블](#) | [네트워크 ACL](#) | [CIDR 예약](#) | [공유 중](#) | [태그](#)

## 세부 정보

서브넷 ID subnet-037f5efd0521e3b49	서브넷 ARN arn:aws:ec2:ap-northeast-2:795691197490:subnet/subnet-037f5efd0521e3b49	상태 Available	IPv4 CIDR 10.1.5.0/24
사용 가능한 IPv4 주소 249	IPv6 CIDR -	가용 영역 ap-northeast-2a	가용 영역 ID apne2-az1
네트워크 경계 그룹 ap-northeast-2	VPC vpc-095cbe9d8d260ed1c   test_tutorial	라우팅 테이블 rtb-01c968814e36126e4   ks_j_internalroutes	네트워크 ACL acl-087ad8e6e46bb0175
기본 서브넷 아니요	퍼블릭 IPv4 주소 자동 할당 아니요	IPv6 주소 자동 할당 아니요	고객 소유 IPv4 주소 자동 할당 아니요
고객 소유 IPv4 풀 -	Outpost ID -	IPv4 CIDR 예약 -	IPv6 CIDR 예약 -
IPv6 전용		리소스 이름 DNS A 레코드	리소스 이름 DNS AAAA 레코드

- private1 (ks\_j\_internal-private(web)) - 10.1.5.0/24





subnet-05deef7223e00762e / ks\_j\_internal-private(db)

[세부 정보](#) | [플로우 로그](#) | [라우팅 테이블](#) | [네트워크 ACL](#) | [CIDR 예약](#) | [공유 중](#) | [태그](#)

## 세부 정보

서브넷 ID subnet-05deef7223e00762e	서브넷 ARN arn:aws:ec2:ap-northeast-2:795691197490:subnet/subnet-05deef7223e00762e	상태 Available	IPv4 CIDR 10.1.1.0/24
사용 가능한 IPv4 주소 244	IPv6 CIDR -	가용 영역 ap-northeast-2a	가용 영역 ID apne2-az1
네트워크 경계 그룹 ap-northeast-2	VPC vpc-095cbe9d8d260ed1c   test_tutorial	라우팅 테이블 rtb-01c968814e36126e4   ks_j_internalroutes	네트워크 ACL acl-087ad8e6e46bb0175
기본 서브넷 아니요	퍼블릭 IPv4 주소 자동 할당 아니요	IPv6 주소 자동 할당 아니요	고객 소유 IPv4 주소 자동 할당 아니요
고객 소유 IPv4 풀 -	Outpost ID -	IPv4 CIDR 예약 -	IPv6 CIDR 예약 -
IPv6 전용		리소스 이름 DNS A 레코드	리소스 이름 DNS AAAA 레코드

- private2 (ks\_j\_internal-private(db)) - 10.1.1.0/24

subnet-08e57b04969f4e15e / ks\_j\_internal-private(elastic)

[세부 정보](#) | [플로우 로그](#) | [라우팅 테이블](#) | [네트워크 ACL](#) | [CIDR 예약](#) | [공유 중](#) | [태그](#)


## 세부 정보

서브넷 ID subnet-08e57b04969f4e15e	서브넷 ARN arn:aws:ec2:ap-northeast-2:795691197490:subnet/subnet-08e57b04969f4e15e	상태 Available	IPv4 CIDR 10.1.3.0/24
사용 가능한 IPv4 주소 250	IPv6 CIDR -	가용 영역 ap-northeast-2a	가용 영역 ID apne2-az1
네트워크 경계 그룹 ap-northeast-2	VPC vpc-095cbe9d8d260ed1c   test_tutorial	라우팅 테이블 rtb-01c968814e36126e4   ks_j_internalroutes	네트워크 ACL acl-087ad8e6e46bb0175
기본 서브넷 아니요	퍼블릭 IPv4 주소 자동 할당 아니요	IPv6 주소 자동 할당 아니요	고객 소유 IPv4 주소 자동 할당 아니요
고객 소유 IPv4 풀 -	Outpost ID -	IPv4 CIDR 예약 -	IPv6 CIDR 예약 -
IPv6 전용		리소스 이름 DNS A 레코드	리소스 이름 DNS AAAA 레코드

- private3 (ks\_j\_internal-private(elastic)) - 10.1.3.0/24







 Private subnet




**Web Server**


 Private subnet




**DB Server**




**DB Log**




**Backup Server**


 Private subnet



**Kibana**

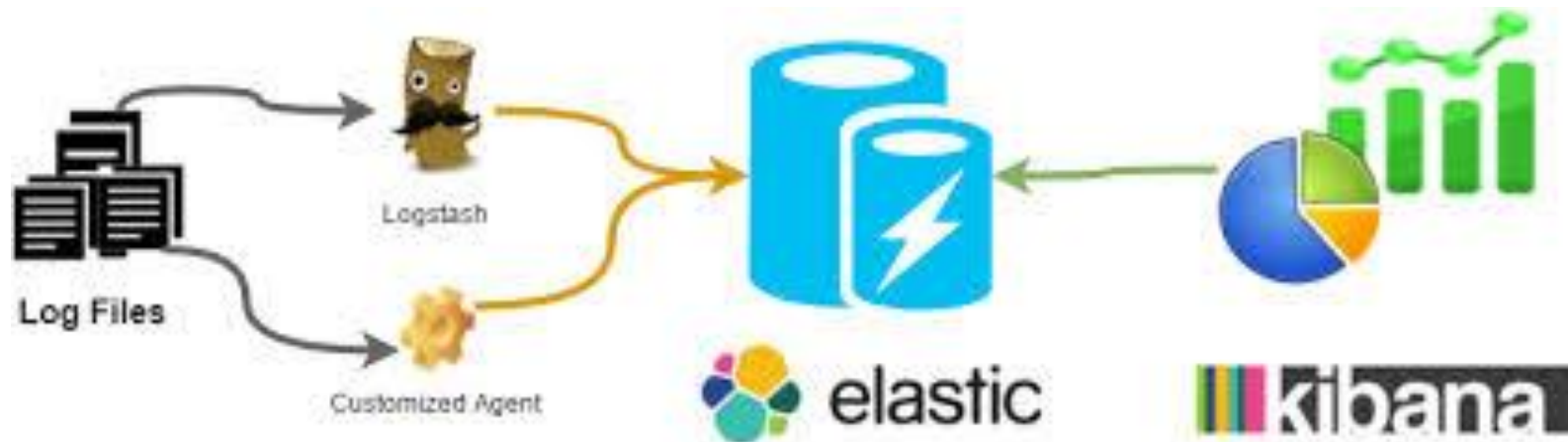


**Elastic Search Service**



**Logstash**







- Interface

방화벽 기본 인터페이스 이외에 추가로 연결(eth1=en1)

네트워크 인터페이스 (1/15) 정보

네트워크 인터페이스 ID

서브넷 ID

VPC ID

가용 영역

보안 그룹 이름

보안 그룹 ID

인터페이스 유형

<input type="checkbox"/>	eni-04a13ae1cde00748c	subnet-05deef7223e00762e	vpc-095cbe9d8d260ed1c	ap-northeast-2a	sg_ksj_DB	sg-0f4a7760e6fd3b...	탄력적 네트워크 인터페...
<input type="checkbox"/>	test_route	eni-04a98e9d2de033172	subnet-07d6d48df6fb4149	vpc-095cbe9d8d260ed1c	ap-northeast-2a	default	탄력적 네트워크 인터페...
<input checked="" type="checkbox"/>	pfsense-internal	eni-04337028c5006f996	subnet-05deef7223e00762e	vpc-095cbe9d8d260ed1c	ap-northeast-2a	default	탄력적 네트워크 인터페...

네트워크 인터페이스: eni-04337028c5006f996(pfsense-internal)

세부 정보

플로우 로그

태그

네트워크 인터페이스 세부 정보

네트워크 인터페이스 ID

eni-04337028c5006f996

네트워크 인터페이스 상태

Available

VPC ID

vpc-095cbe9d8d260ed1c

소유자

795691197490

소스/대상 확인

아니요

IP 주소

프라이빗 IPv4 주소

10.1.1.200

퍼블릭 IPv4 주소

이름

pfsense-internal

인터페이스 유형

탄력적 네트워크 인터페이스

서브넷 ID

subnet-05deef7223e00762e

요청자 ID

AIDA3SQXEEQZPNWSi6LEN

프라이빗 IPv4 DNS

ip-10-1-1-200.ap-northeast-2.compute.internal

퍼블릭 IPv4 DNS

설명

pfsens-tutorial

보안 그룹

sg-08af6f3975721e18e (default)

가용 영역

ap-northeast-2a

요청자 관리형

아니요

Elastic Fabric Adapter

아니요

IPv6 주소





← → ↺ ⚠ 주의 요함 | https://43.202.46.74

pfSense + System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 2 🔄

Status / Dashboard + ?

System Information ⚙️ - ✕

Name	pfSense.home.arpa
User	admin@61.39.155.24 (Local Database)
System	Amazon Web Services Netgate Device ID: 96c338df3c8ce1ca014b
BIOS	Vendor: Amazon EC2 Version: 1.0 Release Date: Mon Oct 16 2017
Version	23.05.1-RELEASE (amd64) built on Wed Jun 28 03:57:27 UTC 2023 FreeBSD 14.0-CURRENT  The system is on the latest version. Version information updated at Fri Oct 13 3:03:55 UTC 2023 ↻
CPU Type	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2 CPU(s) : 1 package(s) x 1 core(s) x 2 hardware threads AES-NI CPU Crypto: Yes (inactive) IPsec-MB Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 08 Minutes 24 Seconds
Current date/time	Fri Oct 13 3:04:35 UTC 2023
DNS server(s)	• 127.0.0.1 • 10.1.0.2
Last config change	Fri Oct 13 3:04:23 UTC 2023

Netgate Services And Support - ✕

Contract type Community Support  
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

• Upgrade Your Support

• Community Support Resources

• Netgate Global Support FAQ

• Official pfSense Training by Netgate

• Netgate Professional Services

• Visit Netgate.com

Interfaces ⚙️ - ✕

WAN	↑ Unknown <full-duplex>	10.1.2.40
-----	-------------------------	-----------





pfsense +

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

2

Interfaces / Interface Assignments

?

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface

Network port

WAN

ena0 (02:e5:99:a5:d7:30)

LAN

ena1 (02:5d:ff:90:bb:5c)

Delete

Available network ports:

ovpns0 (Netgate Auto Remote Access VPN)

Add

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

pfsense +

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

2

Firewall / NAT / Port Forward

?

Port Forward

1:1

Outbound

NPt

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WAN	TCP	*	*	WAN address	81	10.1.5.111	81	<div><div></div><div></div><div></div></div>

↑ Add

↓ Add

Delete

Toggle

Save

+ Separator

Legend

▶

Pass

↔

Linked rule





**pfsense +** System Interfaces Firewall Services VPN Status Diagnostics Help

2

Firewall / Rules / WAN

[Floating](#)
[WireGuard](#)
[WAN](#)
[OpenVPN](#)

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓ 0/977 KiB	IPv4 ICMP	*	*	WAN address	*	*	none		Default ICMP rule	
<input type="checkbox"/>	✓ 0/977 KiB	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Default SSH rule _replace_src_with_mgmtnet_	
<input type="checkbox"/>	✓ 0/977 KiB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none		Default HTTPS rule _replace_src_with_mgmtnet_	
<input type="checkbox"/>	✓ 0/977 KiB	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		Default HTTP rule _replace_src_with_mgmtnet_	
<input type="checkbox"/>	✓ 0/977 KiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Default OpenVPN rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	10.1.5.111	81	*	none		NAT	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

룰 추가







## 진행한 해킹 기법

1. HTML Injection – GET, POST
2. XSS(Cross Site Scripting)
3. File Upload





## - HTML Injection

취약한 매개변수에 악의적인 HTML 코드를 삽입하는 공격

### 01. GET



*`http://3.39.252.169/board.jsp?content=<img  
src=http://3.39.252.169/img/banner1.png>&form=submit`*





## 01. GET



### 문의내역

분류	회원관리
날짜	2023년10월12일11시59분25초

그러 시



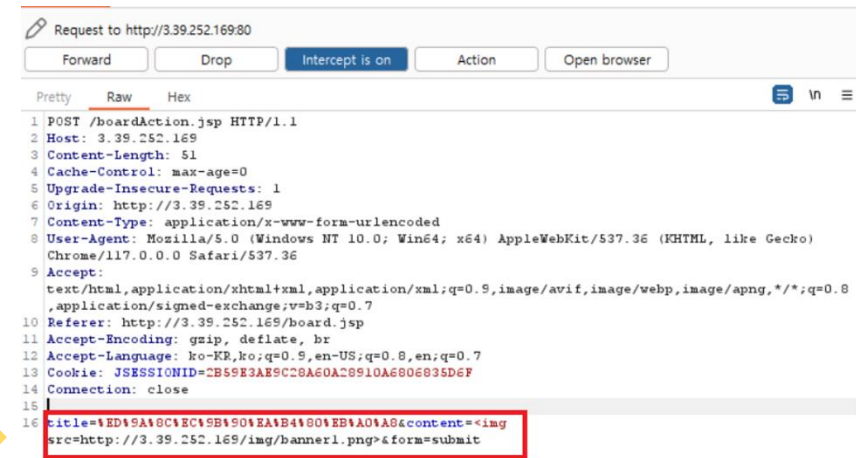
입력 값을 검증하지 않고 이미지 게시한 것 확인





## 02. POST

- POST 메서드 사용하여 데이터 전송
- Burp Suite 이용한 전송



title=%ED%9A%8C%EC%9B%90%EA%B4%80%EB%A0%A8&content=<img  
src=http://3.39.252.169/imag/banner1.png>&form=subimt





## 02. POST



### 문의내역

분류	회원관련
날짜	2023년10월12일12시11분14초



forward 후 이미지가 게시된 것 확인

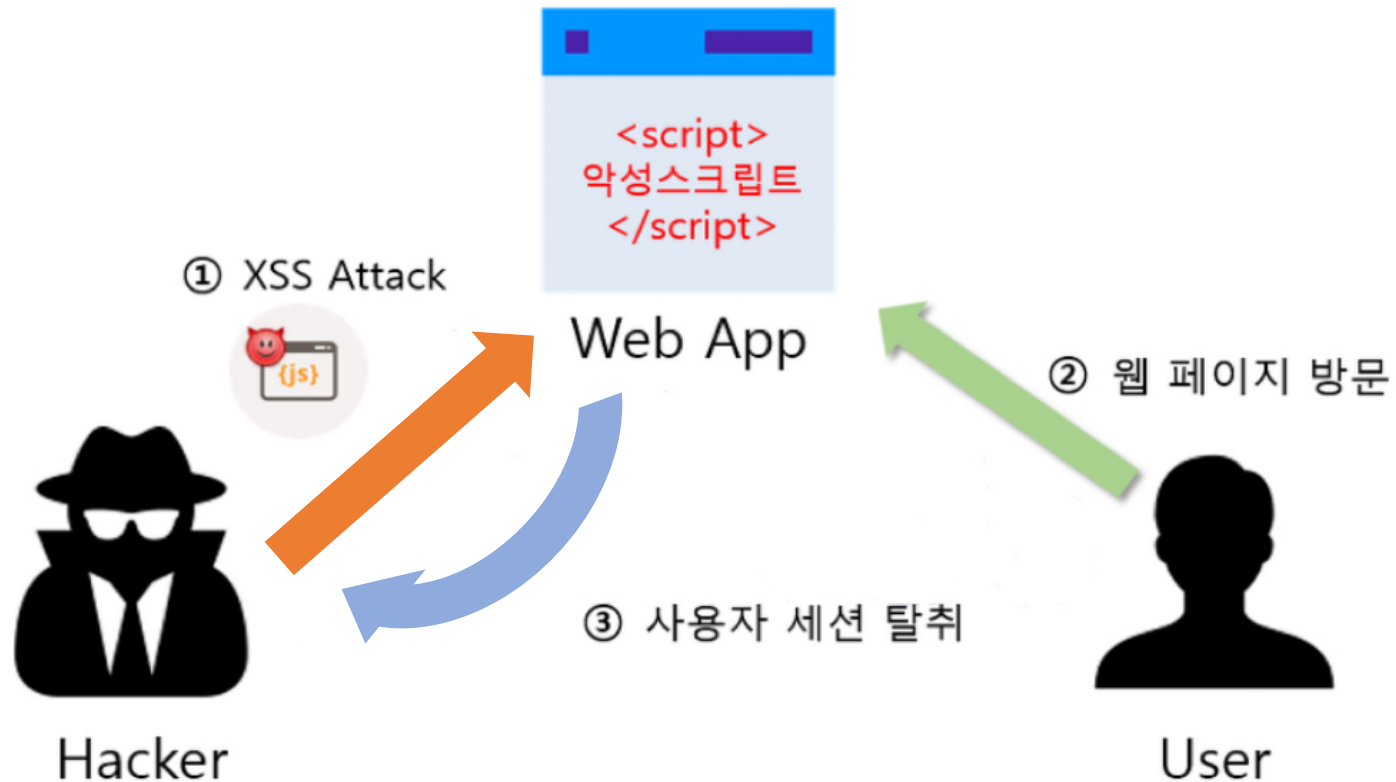




## - XSS(Cross-Site Scripting)

웹 애플리케이션에서 일어나는 취약점

관리자가 아닌 권한이 없는 사용자가 웹 사이트에 스크립트를 삽입하는 공격





## 01. board.jsp

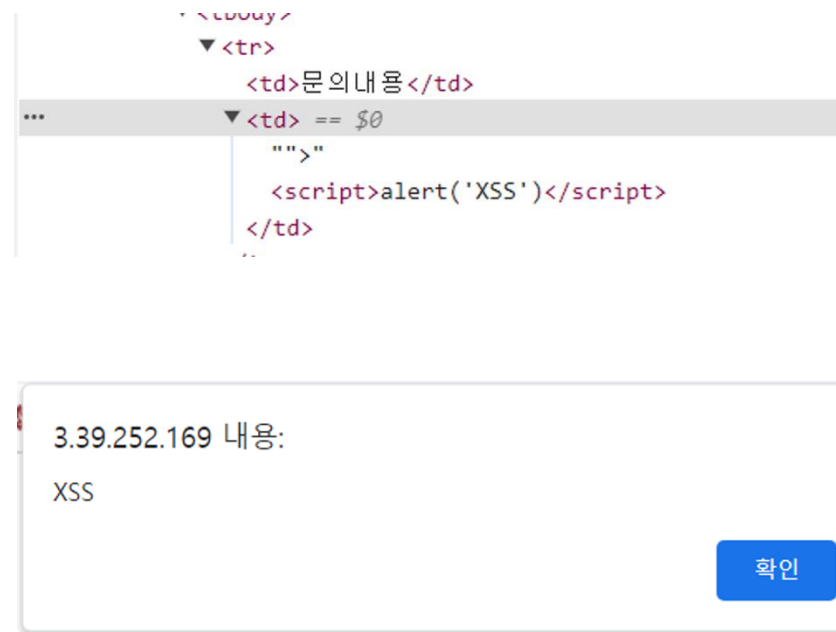
주제 회원관련

내용

"><script>alert('XSS')</script>

등록 취소

- 텍스트 필드에 "><script>alert('XSS')</script>" 입력하여 공격 시도



- 게시물 접속 시 "XSS" 경고 문구가 화면에 나온 것 확인

```
- - [12/Oct/2023:12:38:23 +0000] "POST /boardAction.jsp HTTP/1.1" 302 190 "http://3.39.252.169/board.jsp" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36"
```

- /var/log/apache2/access.log 에서 로그 확인





## 02. bookAdd.jsp

← → ↻ ⚠ 주의 요함 | 3.39.252.169/bookAdd.jsp

 **부크부크** 소설 취미/여행 만화 문제집

분류

소설

에세이

건강

교양

초/중/고

제목

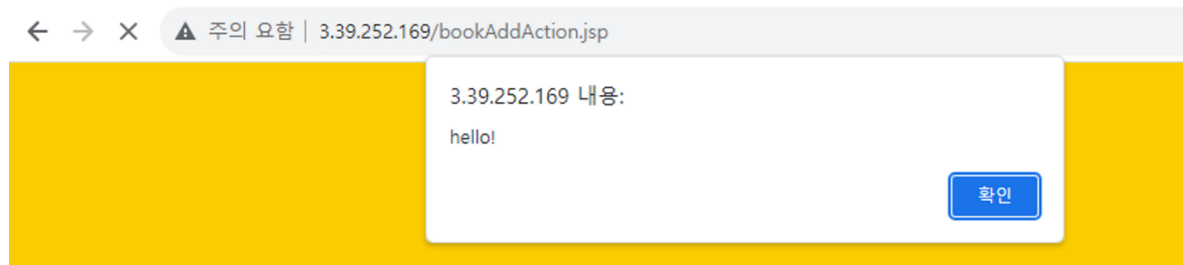
지은이 저 | 출판사 | 가격 원

`<script>alert("hello!")</script>`

이미지 선택

상품등록

- 상품 등록 게시글에서 공격 시도



- 상품을 등록하자 "hello" 경고 문구가 화면에 나온 것 확인







## - File Upload

게시판 등의 파일 업로드할 수 있는 기능을 악용한 취약점  
악의적인 파일(웹셸) 업로드를 통해 시스템을 장악하는 공격





분류 만화 ▼

청소년 ▼

건강 ▼

교양 ▼

초/중/고 ▼

funnybook

kisec 저 ksheild 10000 원

This is funnybook!

book.png 상품등록

- **book.png**을 첨부하여 게시글을 올리려고 함.

```
This is funnybook!  
-----WebKitFormBoundarylMexhWvIyBmTIDzB  
Content-Disposition: form-data; name="myimg"; filename="book.png"  
Content-Type: image/png
```

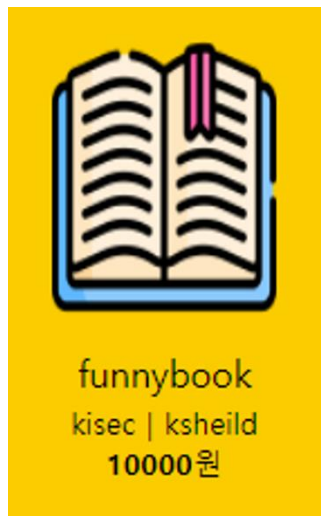
PNG

```
This is funnybook!  
-----WebKitFormBoundarylMexhWvIyBmTIDzB  
Content-Disposition: form-data; name="myimg"; filename="fileupload.aps"  
Content-Type: image/png
```

png

- Burp Suite를 통해 filename을 '**book.png**'에서 '**fileupload.aps**' 파일로 변경





*book.png*



*fileupload.asp*

- 파일 업로드 공격을 통해 '**book.png**' 대신 '**fileupload.asp**' 파일이 업로드 된 것 확인

```
34820 vice (1c1 2ab332a0-ad0b-401c-bc49-b3a004d9d19c; report http://amzn.to/1V3ZAD1) - - [12/Oct/2023:12:17:01 +0000] "GET /bookAddForm.jsp HTTP/1.1" 200 1512 "http://3.39.252.169/bookAddAction.jsp" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36"
```

- /var/log/apache2/access.log 파일에서 로그 확인





WEB, DB서버 ELK와 연동

## Hosts

Last event: 1 minute ago

[Data sources](#) ▾

### Hosts

2



### User authentications

0 success 0 fail

All values returned zero

All values returned zero

### Unique IPs

0 source 0 destination

All values returned zero

All values returned zero

[All hosts](#) [Authentications](#) [Uncommon processes](#) [Events](#) [External alerts](#)

## All hosts

Showing: 2 hosts

Host name	Last seen	Operating system	Version
ip-10-1-1-173	1 minute ago	Ubuntu	22.04.2 LTS (Jammy Jellyfish)
ip-10-1-5-206	1 minute ago	Ubuntu	22.04.2 LTS (Jammy Jellyfish)





## WEB, DB서버 로그 로드

elastic

Search Elastic

Observability Logs Stream

Settings Alerts and rules Add data

Observability

Overview Alerts Cases

Logs

Stream

Anomalies Categories

Metrics

Inventory Metrics Explorer

APM

Services Traces Dependencies Service Map

Uptime

Monitors TLS Certificates

User Experience

Dashboard

### Stream

Search for log entries... (e.g. hostName: host-1)

Customize Highlights

Last 1 day

Stop streaming

Oct 13, 2023	event.dataset	Message
20:31:53.918		L, like Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.68
20:31:54.538		121.148.164.78 - - [13/Oct/2023:11:31:52 +0000] "GET /img/banner3.png HTTP/1.1" 404 1046 "http://3.39.252.169/index.jsp" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.68"
20:31:54.538		231013 11:31:53 64588 Connect root@ip-10-1-5-206.ap-northeast-2.compute.internal on book using TCP/IP
20:31:54.538		64588 Query SELECT @@max_allowed_packet, @@wait_timeout
20:31:54.538		64588 Quit
20:31:54.538		64588 Query set autocommit=1, sql_mode = concat(@@sql_mode, 'STRICT_TRANS_TABLES'), session_track_schema=1, tx_isolation='REPEATABLE-READ'
20:31:54.538		64588 Query SET SESSION TRANSACTION READ WRITE
20:31:54.538		64588 Query SELECT id FROM productNum
20:31:54.919		15.177.22.122 - - [13/Oct/2023:11:31:53 +0000] "GET / HTTP/1.1" 200 1999 "-" "Amazon-Route53-Health-Check-Service (ref 2ab332a6-ad6b-40fc-be49-b3a884d9d19c; report http://amzn.to/1vsZADi)"
20:31:55.928		15.177.50.124 - - [13/Oct/2023:11:31:55 +0000] "GET / HTTP/1.1" 200 1999 "-" "Amazon-Route53-Health-Check-Service (ref 2ab332a6-ad6b-40fc-be49-b3a884d9d19c; report http://amzn.to/1vsZADi)"

Last update now

Streaming new entries





- 1. 복잡한 클라우드 환경 설정:** AWS VPC 설정과 같은 클라우드 환경 설정은 많은 세부 사항들을 고려해야 하며, 이는 초기 단계에서 상당한 시간과 노력을 요구하였습니다. 특히, WEB과 DB의 연동 및 EC2 인스턴스 설계 등의 작업은 복잡성을 추가로 더했습니다.
- 2. ELK Stack 구축:** 로그 데이터 관리와 분석을 위한 ELK Stack(Elasticsearch, Logstash, Kibana) 구축도 어려움 중 하나였습니다. 각 컴포넌트의 동작 방식과 서로 어떻게 연동되는지 이해하는 데 시간이 걸렸으며, 실제로 구현하는 과정에서도 여러 문제에 직면했습니다.
- 3. 보안 설정:** pfSense 방화벽 설정 등의 보안 관련 작업은 기술적인 지식 외에도 보안 정책 및 규정에 대한 충분한 이해가 필요하여 많은 도전이었습니다.
- 4. 웹 해킹 시나리오 개발 및 실행:** 실제 해커처럼 웹 해킹 시나리오를 개발하고 실행하는 것은 많은 창의성과 전략적 사고를 요구하였습니다. 특히 방화벽 등의 보안 장치가 있는 상황에서 원하는 결과를 얻기 위해서는 다양한 우회 기법에 대한 지식이 필요하였습니다.



마무리

