
AWS WAFv2 최대한 활용하기

ATP Rule 적용, ManagedRule의 예외처리, 로그 분석까지.

목차

1. ATP(Account Takeover Prevention)이란?

- 1.1 Why?
- 1.2 What?
- 1.3 How?
- 1.4 Result to Test
- 1.5 Pricing
- 1.6 Result

2. WAF Honey Tips

- 2.1 Logging
- 2.2 Excluded Rules
- 2.3 Analysis

3. Q&A

ATP(Account Takeover Prevention)이란?

1.1 Why? - (1)

이미 노출된 정보로 해킹, 동행복권 책임 비율은?

입력 2023.11.07. 오후 12:58 | 기사판문
남혁우 기자

18 38

| 한국인터넷진흥원·국가정보원 등 사건경위 조사 중

로또 등 복권사업 운영자인 동행복권에 해킹 공격으로 인한 피해가 발생했다. 개인정보 유출 가능성은 확인됐지만 동행복권 측의 책임이 크진 않을 전망이다.

동행복권은 정부에서 제시한 보안 시스템과 인증을 구축하고 있으며, 이번 해킹은 사전에 유출된 외부 정보를 이용한 것으로 예상되기 때문이다.

7일 특권위원회 측에 따르면 한국인터넷진흥원(KISA), 국가정보원 등과 함께 자세한 사건 경위를 조사하고 있다.



동행복권

동행복권은 지난 6일 외부 공격으로 인한 개인정보 유출 가능성을 확인했다고 공식홈페이지를 통해 밝혔다.

상품권 피해부터 누드사진 유출까지... '크리덴셜 스타팅'



LG유플러스 울산사옥, / 사진=연합뉴스

크리덴셜 스타팅 피해는 최근 빈번하게 발생하고 있다. 지난 11일 인터파크는 크리덴셜 스타팅으로 추정되는 사이버 공격을 받았다고 밝혔다. 회사 측에 따르면 신원 미상의 공격자가 사전에 외부에서 수집한 것으로 보이는 아이디와 비밀번호를 이용해 인터파크에 로그인 시도를 했다. 지난해 12월에는 LG유플러스에서는 유사한 공격이 발생해 회원 일부의 요금제 정보 등이 변경된 사례도 있다. 국내뿐 아니라 해외에서 발생한 피해 사례도 많다.

최근에는 미국에서도 간편결제 서비스 페이팔(Paypal) 가입자 3만5000명의 개인정보가 크리덴셜 스타팅 공격으로 외부에 유출되는 사고가 발생하기도 했다. 과거 할리우드 배우 제니퍼 로렌스의 클라우드 계정에 있는 누드 사진 등 생활자료도 유사한 방법으로 유출된 바 있다.

[더페어] 노민영 기자=SK스토어 고객 계정 12만 5천여 건이 해킹당했다.

지난 21일 SK스토어는 내부 트래픽 점검 중 특정 IP에서 다량의 부정 로그인이 시도된 사실을 파악하고 피해 사실을 관계 기관에 신고했다. 해당 IP는 12만 5천여 명의 고객 계정에 무단으로 로그인을 한 것으로 확인돼 큰 충격을 주고 있다.

문제의 IP는 현재 로그인이 차단된 상태이며, 로그인이 시도된 계정들도 모두 잠금 조치가 취해졌다. 그러나 무단 로그인을 통해 고객들의 이름, 연락처, 생년월일, 주소지, 이메일 등의 개인정보가 이미 유출되었을 가능성이 크다.

SK스토어 측은 사건 최초 인지 이후 뛰어 지난 23일 자사 홈페이지를 통해 부정 로그인이 시도된 사실을 고객에게 공지했으며, 해킹 피해 고객들에게는 사설 고지 및 비밀번호 변경 안내 문자를 발송한 상태다.

공지사항

개인정보 침해 사고 전 문장 사과 드립니다

SK스토어 이용해 주신는 고객님께 사과 드립니다.

SK스토어는 2023.11.21(화) 00:00~06:00까지 SK스토어 앱에 보호 로그인 사용한 회원을 발견하였습니다. 준비로 고객 ID 로그인 정보를 확인하였으며 이를 통해 지난 12월 5천여 명의 고객 개인정보가 유출될 가능성이 있다고 판단하였습니다.

유출 가능성이 있는 개인정보 목록은 아래 표로, **회원정보, 패스워드, 결제정보, 이메일, 생년월일, 주민등록번호, 주민번호, 전화번호, 주소, 이메일주소, 비밀번호**입니다.

SK스토어는 이 사실을 인천지방경찰청에 알리고 개인정보 보호법 위반으로 고발되었음을 모도하고 조사하겠습니다. 이와 함께 민사적 입장은 차후에 예상되며 2024년 11월 22일(수) 해당 고객에게 개인정보유출 위반 책임분담, 면책, 손해구제 등을 명시해 드립겠습니다.

이번 일은 관계자에게 보이콧, 비난 등 2차 피해가 우려되고 있습니다. 본체에서는 해당 고객님을 대상 벌칙규정을 바탕으로 일정 분은 책임 면제, 면책 및 개인정보 유출 책임자로 조사하고자 했습니다. 반드시 닉네임의 예측ability을 바탕으로 일정하시기를 부탁드립니다.

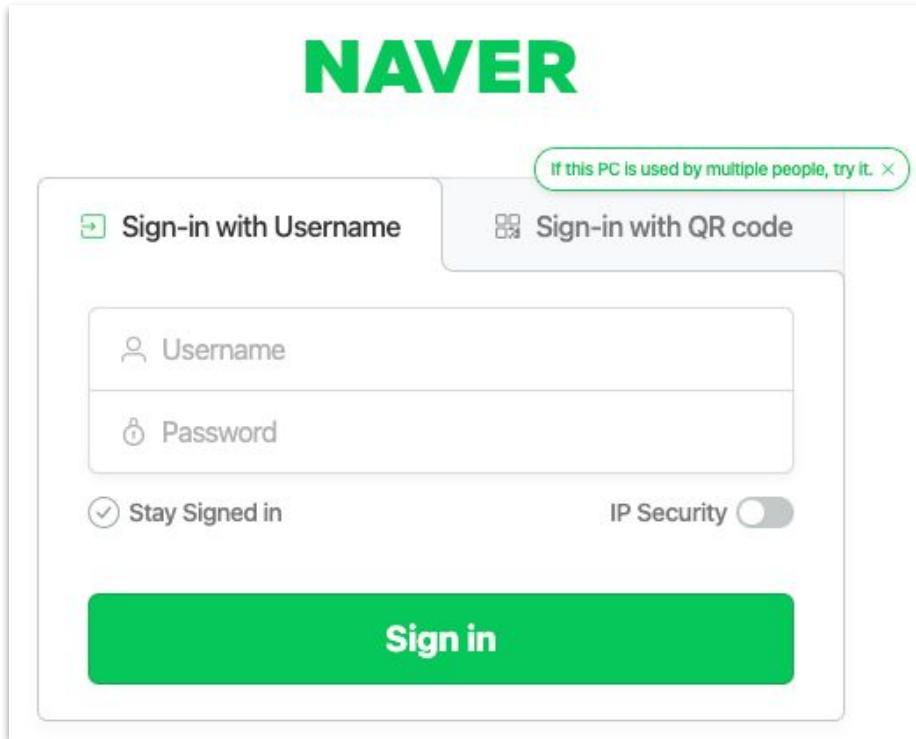
사진=SK스토어 공지사항 캡처

다량의 계정 정보가 유출된 경위에 대해 관계기관이 조사를 진행하고 있는 가운데 SK스토어 측은 사고 원인으로 크리덴셜 스타팅(Credential stuffing)을 지목하고 있다.

크리덴셜 스타팅이란 미상의 특정인이 여러 사이트를 통해 수집한 ID 및 패스워드 정보를 특정 웹사이트나 앱 로그인에 이용하는 방식이다. 이는 디수의 인터넷 이용자들이 동일한 아이디 및 비밀번호를 여러 계정에 둘러쓸다는 점을 이용한 해킹 수법이다.

Brute Force VS Credential Stuffing

1.2 What? - (1)



The NAVER login interface features a large green "NAVER" logo at the top. Below it are two sign-in options: "Sign-in with Username" (selected) and "Sign-in with QR code". A green callout bubble above the QR code option says "If this PC is used by multiple people, try it." There are input fields for "Username" and "Password", a checked "Stay Signed in" checkbox, and an "IP Security" toggle switch. A large green "Sign in" button is at the bottom.

NAVER

If this PC is used by multiple people, try it. ×

Sign-in with Username

Sign-in with QR code

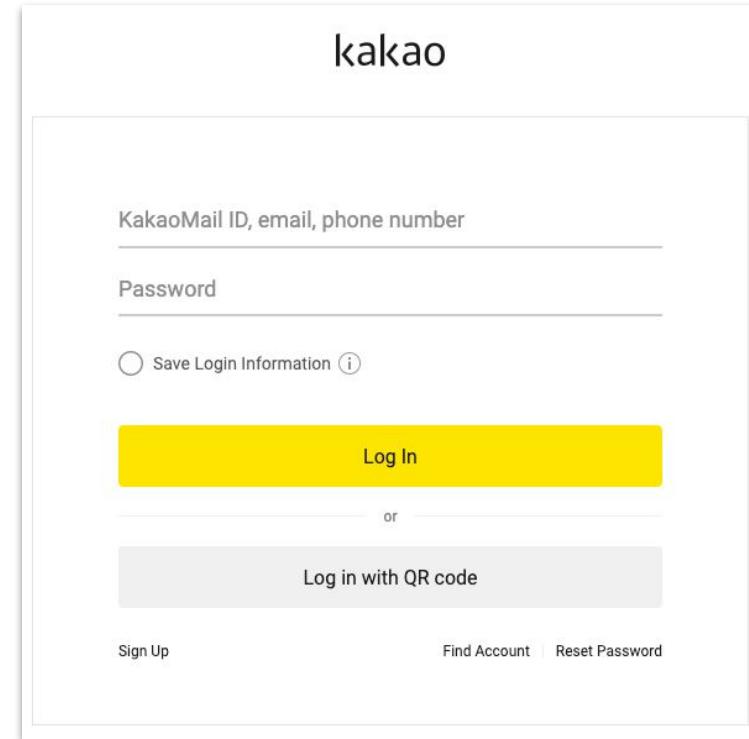
Username

Password

Stay Signed in

IP Security

Sign in



The kakao login interface has a "kakao" logo at the top. It includes fields for "KakaoMail ID, email, phone number" and "Password". There is a "Save Login Information" checkbox, a yellow "Log In" button, and a "Log in with QR code" button. At the bottom, there are links for "Sign Up", "Find Account", and "Reset Password".

kakao

KakaoMail ID, email, phone number

Password

Save Login Information ⓘ

Log In

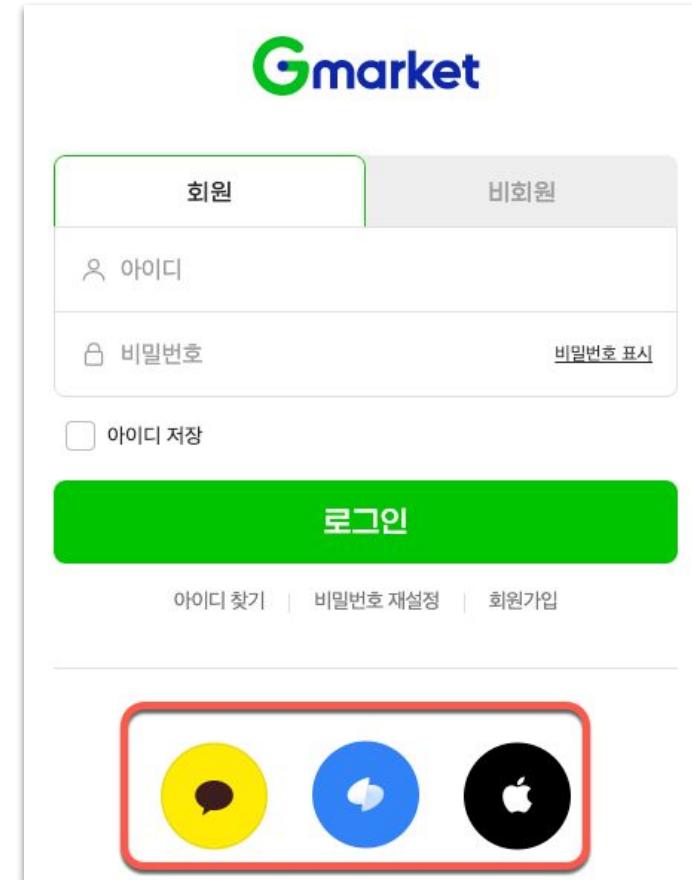
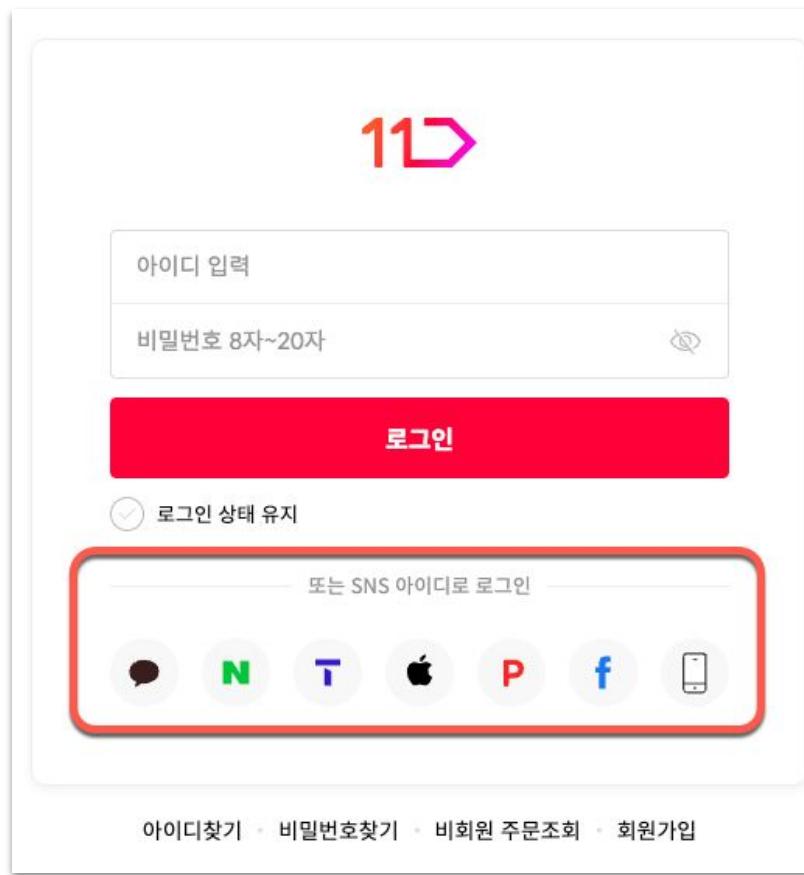
or

Log in with QR code

Sign Up

Find Account | Reset Password

1.2 What? - (2)



1.3 How?

Account takeover prevention

Description	Pricing
Provides protection for your login page against stolen credentials, credential stuffing attacks, brute force login attempts, and other anomalous login activities. With account takeover prevention, you can prevent unauthorized access that may lead to fraudulent activities, or inform legitimate users to take a preventive action. Learn More	<ul style="list-style-type: none">\$10 per month (prorated hourly)Tiered fee model for requests analyzed AWS WAF Pricing
Capacity	50

Scope of inspection

Choose the scope of inspection
You can inspect all web requests or only the requests that match the criteria in a scope-down rule statement. [Learn More](#)

Inspect all web requests
 Only inspect requests that match a scope-down statement

[Rule visual editor](#) [Rule JSON editor](#)

If a request matches the statement

Statement

Inspect: URI path
Match type: Exactly matches string
String to match: [REDACTED]

Text transformation: None

Add text transformation: You can add up to 10 text transformations.



Rule group configuration

Provide login page details and optionally provide login response information. The rule group uses login details to narrow the scope of the web requests it inspects and to validate credentials usage. The rule group uses login response information to inspect the responses to login requests.

Use regular expression in paths

Login path
Enter the path of the login endpoint for your application. Login paths that start with the path you provide are considered a match.
[REDACTED]

Request inspection
Specify how login requests are formatted and populated.

Payload type
FORM_ENCODED

Field names
Enter the names of the fields within the request body where the username and password are provided. For JSON payloads, specify the field names in JSON pointer syntax. For form encoded payloads, use the HTML form names.

Username field: username

Password field: password

1.4 Result to Test - (1)

AWS-AWSManagedRulesATPRuleSet	AWS#AWSManagedRulesATPRuleSet#SignalMissingCredential



SignalMissingCredential

Inspects for requests with credentials that are missing the username or password.

Rule action: Block

Label: awswaf:managed:aws:atp:signal:missing_credential

1.4 Result to Test - (2)

The image shows two side-by-side instances of the Burp Suite Community Edition interface, version v2023.10.3.6, titled "Temporary Project". Both instances have the "Intruder" tab selected.

Left Instance:

- Payload sets:** Payload set 1, Payload count: 102, Payload type: Simple list, Request count: 102.
- Payload settings [Simple list]:** A list of strings including "car", "root", "admin", "test", "gue", "info", and "123456". The string "123456" is highlighted.
- Payload processing:** An empty table with columns "Add", "Enabled", and "Rule".
- Payload encoding:** A checkbox labeled "URL-encode these characters: /><?+&:;{}|^#".

Right Instance:

- Payload sets:** Payload set 2, Payload count: 102, Payload type: Simple list, Request count: 102.
- Payload settings [Simple list]:** A list of strings including "123456", "password", "12345678", "qwerty", "123456789", "12345", and "1234". The string "qwerty" is highlighted.
- Payload processing:** An empty table with columns "Add", "...", and "Rule".
- Payload encoding:** A checkbox labeled "URL-encode these characters: /><?+&:;{}|^#".

1.4 Result to Test - (3)

Results	Positions	Payloads	Resource pool	Settings			
Filter: Showing all items							
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0	car	123456	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
1	root	password	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
2	admin	12345678	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
3	test	qwerty	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
4	guru	123456789	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
5	admin	12345	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
6	info	12345	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
7	ad	12345	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
8	mi	111111	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
9	wire	peter	400	<input type="checkbox"/>	<input type="checkbox"/>	0	
10	use	1234567	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
11	ad	dragon	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
12	ora	123123	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
13	ftp	baseball	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
14	pit	abc123	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
15	put	football	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
16	ans	monkey	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
17	ec	letemen	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
18	vat	shadow	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
19	azu	master	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
20	act	66666666	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
21	act	qwertyuiop	400	<input type="checkbox"/>	<input type="checkbox"/>	985	
22	act	123221	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
23	act	mustang	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
24	act	1234567890	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
25	act	michael	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
26	act	654321	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
27	act	superman	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
28	act	1qaz2wsx	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
29	act	77777777	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
30	act	121212	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
31	act	0	403	<input type="checkbox"/>	<input type="checkbox"/>	647	

WAF에서 차단된 403 ERROR



1.4 Result to Test - (4)

3. Intruder attack of https://groot-gw.accountd.iguplusdev.com - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0	[REDACTED]	[REDACTED]	400	<input type="checkbox"/>	<input type="checkbox"/>	924	
1	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
2	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
20	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
21	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
22	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
23	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
24	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
25	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
26	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
27	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
28	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
29	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
30	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
31	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
32	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
33	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
43	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
44	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1257	
45	[REDACTED]	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	647	
46	[REDACTED]	[REDACTED]	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
47	[REDACTED]	[REDACTED]	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
48	[REDACTED]	[REDACTED]	403	<input type="checkbox"/>	<input type="checkbox"/>	647	
49	[REDACTED]	[REDACTED]	403	<input type="checkbox"/>	<input type="checkbox"/>	647	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Server: awselb/2.0
3 Date: Thu, 23 Nov 2023 08:03:08 GMT
4 Content-Type: text/html
5 Content-Length: 520
6
7 <html>
8   <head>
9     <title>
10    403 Forbidden
11   </title>
12 </head>
13 <body>
14   <center>
15     <h1>
16       403 Forbidden
17     </h1>
18   </center>
19 </body>
20 </html>
21 <!-- a padding to disable MSIE and Chrome friendly error page -->
22 <!-- a padding to disable MSIE and Chrome friendly error page -->
23 <!-- a padding to disable MSIE and Chrome friendly error page -->
24 <!-- a padding to disable MSIE and Chrome friendly error page -->
25 <!-- a padding to disable MSIE and Chrome friendly error page -->
26 <!-- a padding to disable MSIE and Chrome friendly error page -->
27 <!-- a padding to disable MSIE and Chrome friendly error page -->
28 <!-- a padding to disable MSIE and Chrome friendly error page -->
29 <!-- a padding to disable MSIE and Chrome friendly error page -->
30 <!-- a padding to disable MSIE and Chrome friendly error page -->
31 <!-- a padding to disable MSIE and Chrome friendly error page -->
32 <!-- a padding to disable MSIE and Chrome friendly error page -->
33 <!-- a padding to disable MSIE and Chrome friendly error page -->
```

45번째까지는 정상적으로 로그인 성공

46번째부터 WAF에서 차단

1.4 Result to Test - (5)

VolumetricIpHigh

Inspects for high volumes of requests sent from individual IP addresses. A high volume is more than 20 requests in a 10 minute window.

Note

The thresholds that this rule applies can vary slightly due to latency. For the high volume, a few requests might make it through beyond the limit before the rule action is applied.

Rule action: Block

Label: `awswaf:managed:aws:atp:aggregate:volumetric:ip:high`

The rule group applies the following labels to requests with medium volumes (16-20 requests per 10 minute window) and low volumes (11-15 requests per 10 minute window), but takes no action on them:

`awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` and

`awswaf:managed:aws:atp:aggregate:volumetric:ip:low`.

VS

Rate limiting caveats

AWS WAF rate limiting is designed to control high request rates and protect your application's availability in the most efficient and effective way possible. It's not intended for precise request-rate limiting.

- AWS WAF estimates the current request rate using an algorithm that gives more importance to more recent requests. Because of this, AWS WAF will apply rate limiting near the limit that you set, but does not guarantee an exact limit match.
- AWS WAF estimates the rate of requests about every 30 seconds, using requests for the prior 5 minutes each time. Due to this and other factors such as propagation delays, it's possible for requests to be coming in at too high a rate for up to 30 seconds before AWS WAF detects and rate limits them. Similarly, the request rate can be below the limit for up to 30 seconds before AWS WAF detects the decrease and discontinues the rate limiting action. Usually, this delay is below 20 seconds.

1.5 Pricing?

Pricing components

AWS WAF

Bot Control

Fraud Control

AWS WAF Fraud Control are AWS Managed Rules that protects your login and sign-up pages against attacks such as credential stuffing, credential cracking and fake account creation attacks.

AWS WAF Fraud Control consists of Account Takeover Prevention and Account Creation Fraud Prevention. You will be charged a request fee as per the following table for the total requests analyzed by Account Takeover Prevention and Account Creation Fraud Prevention. You also pay a subscription fee of \$10 per month per WebACL for using the AMR.

Requests	Request fee analysis
0 to 10k	Included
10K to 2M	\$1,000 per Million requests analyzed
2M to 5M	\$700 per Million requests analyzed
5M to 15M	\$400 per Million requests analyzed
15M to 30M	\$200 per Million requests analyzed
30M and above	\$50 per Million requests analyzed

CAPTCHA attempt is when a user completes a CAPTCHA challenge that is submitted to AWS WAF for analysis, regardless of multiple attempts.

Challenge response is when a user is served a challenge page by AWS WAF as a result of a challenge action, regardless of multiple responses.

Request	Pricing	Requests	Request fee analysis	비용
1,000,000	\$1000	1,000,000	1,000	1,000
10,000,000	\$6100	2,000,000	1,000	2,000
15,000,000	\$8100	3,000,000	700	2,700
		4,000,000	700	3,400
		5,000,000	700	4,100
		6,000,000	400	4,500
		7,000,000	400	4,900
		8,000,000	400	5,300
		9,000,000	400	5,700
		10,000,000	400	6,100
		11,000,000	400	6,500
		12,000,000	400	6,900
		13,000,000	400	7,300
		14,000,000	400	7,700
		15,000,000	400	8,100
		16,000,000	200	8,300

1.6 Result



가즈아!!!!!!

WAF Honey Tips

2.1 Logging - (1)

Logging destination
Select a destination for your web ACL traffic logs.

CloudWatch Logs log group
 Kinesis Data Firehose stream
 S3 bucket

Amazon S3 bucket
Select a S3 bucket in your account that begins with 'aws-waf-logs-' or create one in the Amazon Simple Storage Service (S3) console. You must use a S3 bucket that's associated with your account.

Select an S3 bucket

1 Create an S3 bucket in the centralized logging account in your selected Region

1. [Create an S3 bucket](#) in the centralized logging account for your selected AWS Region.
2. Enter a bucket name that starts with the prefix aws-waf-logs-. For example, name your bucket similar to aws-waf-logs-example-bucket.

2 Create and add a bucket policy to the S3 bucket

Add the following [S3 bucket policy](#) to your S3 bucket:

3 Configure your web ACLs to send the logs to the desired S3 bucket

Note: If you receive errors when running AWS Command Line Interface (AWS CLI) commands, make sure that you're using the most recent AWS CLI version.

You must configure your web ACLs to send the AWS WAF logs to the centralized logging account's S3 bucket. To configure a web ACL, run the [put-logging-configuration](#) AWS CLI command from the account that owns the web ACL.

2.1 Logging - (2)

Redacted fields

Select the data fields that you want to omit from the logs.

Redacted fields

- HTTP method
- Query string
- URI path
- Single header

Redacted headers

Specify the headers you want to redact from the logs.

Enter header

Add header

Remove

Sampled request for metric [REDACTED]

Source IP	Rule inside rule group	Action	Time
[REDACTED]	-	ALLOW	Thu Dec 14 2023 01:19:41 GMT+0900 (한국 표준시)
Country	URI		
KR	[REDACTED]		

Request

```
GET /api/v1/[REDACTED]/options? [REDACTED]  
host: [REDACTED]  
accept: application/json, text/plain, */*  
authorization: Bearer [REDACTED]  
  
[REDACTED]  
  
sec-fetch-site: cross-site  
accept-language: ko-KR,ko;q=0.9  
accept-encoding: gzip, deflate, br  
sec-fetch-mode: cors  
origin: [REDACTED]  
user-agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_1_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)  
Mobile/ [REDACTED]  
referer: [REDACTED] /  
sec-fetch-dest: empty
```

2.1 Logging - (3)

Filter logs

Add filters to control which web requests are logged. If you add multiple filters, AWS WAF evaluates them starting from the top.

Filter 1

Filter requirement
Criteria for a request to be a match for the filter conditions.

Match all of the filter conditions
 Match at least one of the filter conditions

Filter conditions
Select the filtering criteria.

Condition type Rule action on request

Condition value

Select an action Allow

Allow
Block
Count
CAPTCHA
EXCLUDED_AS_COUNT
Challenge

Filter behavior
Select the action to take for requests that match the filter.

Keep in logs
 Drop from logs

Add condition Add filter

Default logging behavior

Default logging behavior
Indicate how to handle requests that don't match any of the specified log filters.

Keep in logs
 Drop from logs

2.1 Logging - (3)

Filter logs

Add filters to control which web requests are logged.

Filter 1

Filter requirement
Criteria for a request to be a match for the filter condition.

- Match all of the filter conditions
- Match at least one of the filter conditions

Filter conditions
Select the filtering criteria.

Condition type

Request has label

Enter label

Add condition

Filter behavior
Select the action to take for requests that match the filter criteria.

- Keep in logs
- Drop from logs

Add filter

AWSManagedRulesSQLIRuleSet labels

Labels are applied to requests starting from the top.

Move down Remove

- aws:managed:aws:sql-database:SQL_Body
- aws:managed:aws:sql-database:SQL_URIPath
- aws:managed:aws:sql-database:SQL_QueryArguments
- aws:managed:aws:sql-database:SQL_Cookie
- aws:managed:aws:sql-database:SQLExtendedPatterns_QueryArguments

Amazon IP reputation list managed rule group

VendorName: AWS, Name: AWSManagedRulesAmazonIpReputationList, WCU: 25

The Amazon IP reputation list rule group contains rules that are based on Amazon internal threat intelligence. This is useful if you would like to block IP addresses typically associated with bots or other threats. Blocking these IP addresses can help mitigate bots and reduce the risk of a malicious actor discovering a vulnerable application.

This managed rule group adds labels to the web requests that it evaluates, which are available to rules that run after this rule group in your web ACL. AWS WAF also records the labels to Amazon CloudWatch metrics. For general information about labels and label metrics, see [Labels on web requests](#) and [Label metrics and dimensions](#).

Rule name	Description and label
AWSManagedIPReputationList	Inspects for IP addresses that have been identified as bots. Rule action: Block Label: aws:managed:aws:amazon-ip-list:AWSManagedIPReputationList
AWSManagedReconnaissanceList	Inspects for connections from IP addresses that are performing reconnaissance against AWS resources. Rule action: Block Label: aws:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList
AWSManagedIPDoSList	Inspects for IP addresses that have been identified as actively engaging in DDoS activities. Rule action: Count Label: aws:managed:aws:amazon-ip-list:AWSManagedIPDoSList

Anonymous IP list managed rule group

VendorName: AWS, Name: AWSManagedRulesAnonymousIpList, WCU: 50

The Anonymous IP list rule group contains rules to block requests from services that permit the obfuscation of viewer identity. These include requests from VPNs, proxies, Tor nodes, and web hosting providers. This rule group is useful if you want to filter out viewers that might be trying to hide their identity from your application. Blocking the IP addresses of these services can help mitigate bots and evasion of geographic restrictions.

This managed rule group adds labels to the web requests that it evaluates, which are available to rules that run after this rule group in your web ACL. AWS WAF also records the labels to Amazon CloudWatch metrics. For general information about labels and label metrics, see [Labels on web requests](#) and [Label metrics and dimensions](#).

Rule name	Description and label
AnonymousIPList	Inspects for a list of IP addresses of sources known to anonymize client information, like TOR nodes, temporary proxies, and other masking services. Rule action: Block Label: aws:managed:aws:anonymous-ip-list:AnonymousIPList
HostingProviderIPList	Inspects for a list of IP addresses from web hosting and cloud providers, which are less likely to source end-user traffic. The IP list does not include AWS IP addresses. Rule action: Block Label: aws:managed:aws:anonymous-ip-list:HostingProviderIPList

2.2 Excluded Rules

Core rule set

Description
Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. [Learn More](#)

Version
Default (using Version_1.10)

Capacity
700

Scope of inspection

Choose the scope of inspection
You can inspect all web requests or only the requests that

Inspect all web requests
 Only inspect requests that match a scope-down statement

Core rule set

Description
Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. [Learn More](#)

Version
Default (using Version_1.10)

Capacity
700

Amazon SNS topic
Subscribe to notifications about this rule group from its provider.
[arn:aws:sns:us-east-1:248400274283:aws-managed-waf-rule-notifications](#)

Scope of inspection

Choose the scope of inspection
You can inspect all web requests or only the requests that match the criteria in a scope-down rule statement. [Learn More](#)

Inspect all web requests
 Only inspect requests that match a scope-down statement

[Rule visual editor](#) [Rule JSON editor](#)

If a request matches the statement

Statement

Inspect
[Choose an Inspection option](#)

Core rule set rules

The rules apply actions and labels to requests that match their criteria. [Learn More](#)

By default, the rule group uses its configured rule actions. You can override the actions for all rules and for individual rules. For a single rule, use the rule dropdown to specify an override action or to remove an override.

Allow and Block actions terminate web ACL evaluation for matching requests. Count action counts matching requests and continues the web ACL evaluation. [Learn More](#)

Override all rule actions

[Choose rule action override](#) [Remove all overrides](#)

NoUserAgent_HEADER Rule action: Block	UserAgent_BadBots_HEADER Rule action: Block	SizeRestrictions_QUERYSTRING Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
SizeRestrictions_Cookie_HEADER Rule action: Block	SizeRestrictions_BODY Rule action: Block	SizeRestrictions_URI_PATH Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
EC2MetaDataSSRF_BODY Rule action: Block	EC2MetaDataSSRF_COOKIE Rule action: Block	EC2MetaDataSSRF_URI_PATH Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
EC2MetaDataSSRF_QUERYARGUMENTS_TS Rule action: Block	GenericLFI_QUERYARGUMENTS Rule action: Block	GenericLFI_URI_PATH Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
GenericLFI_BODY Rule action: Block	RestrictedExtensions_URI_PATH Rule action: Block	RestrictedExtensions_QUERYARGUMENTS_TS Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
GenericRFI_QUERYARGUMENTS Rule action: Block	GenericRFI_BODY Rule action: Block	GenericRFI_URI_PATH Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
CrossSiteScripting_COOKIE Rule action: Block	CrossSiteScripting_QUERYARGUMENTS_TS Rule action: Block	CrossSiteScripting_BODY Rule action: Block
Choose rule action override	Choose rule action override	Choose rule action override
CrossSiteScripting_URI_PATH Rule action: Block		
Choose rule action override		

2.2 Excluded Rules

Core rule set rules
The rules apply actions and labels to requests that match their criteria. [Learn More](#)

By default, the rule group uses its configured rule actions. You can override the actions for all rules and for individual rules. For a single rule, use the rule dropdown to specify an override action or to remove an override.

Allow and Block actions terminate web ACL evaluation for matching requests. Count action counts matching requests and continues the web ACL evaluation. [Learn More](#)

Override all rule actions

NoUserAgent_HEADER Rule action: Block
UserAgent_BadBots_HEADER Rule action: Block
SizeRestrictions_QUERYSTRING Rule action: Block

SizeRestrictions_Cookie_HEADER Rule action: Block
SizeRestrictions_BODY Rule action: Block
SizeRestrictions_URI PATH Rule action: Block

Choose rule action override **Remove all overrides**



If a request matches all the statements (AND)

Statement 1 Remove

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.
 Negate statement results
Inspect Has a label
Labels Labels are strings that rules add to the web request. You can evaluate labels that are added by rules that run before this one in the same web ACL.
Match scope Label Namespace Managed key
Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or aws:s:managed:aws:managed-rule-set:namespace1:name.
Q aws:managed:aws:core:rule-set:SizeRestrictions_Body X

AND

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.
 Negate statement results
Inspect URI path
Match type Exactly matches string
String to match /api/v1/upload

Text transformation
AWS WAF applies all transformations to the request body when transformations are applied in the order listed.
None Add text transformation You can add up to 10 text transformations

Then

Action
Choose an action to take when a request matches the statements above.
 Block Allow Count CAPTCHA Challenge
▶ Custom response - optional
▶ Add label - optional
Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

Add rule

2.2 Excluded Rules

Set rule priority [Info](#)

Rules (6)

▲ Move up

▼ Move down

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
<input type="radio"/>	AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="radio"/>	excluded-managed-core-rule	3	Block

2.3 Analysis - (1)

If a request matches the statement

Statement

Inspect

URI path

Match type

Contains string

String to match

/.

Text transformation

AWS WAF applies all transformations to the request before evaluating it. If multiple transformations are applied in the order presented below with the top of the list.

None

Add text transformation

You can add up to 10 text transformations.

Sampled requests (105)

Samples of requests from the past 3 hours.

All metrics

Metric name	Source IP	URI	Rule inside rule group	Action
AWSManagedRulesCommonRuleSet	20 [REDACTED] 3.210 (ID)	/env.backup	AWS#AWSManagedRulesCommonRuleSet#RestrictedExtensions_URIPATH	BLOCK
AWSManagedRulesCommonRuleSet	20 [REDACTED] 3.210 (ID)	/env.bak	AWS#AWSManagedRulesCommonRuleSet#RestrictedExtensions_URIPATH	BLOCK
AWSManagedRulesCommonRuleSet	66 [REDACTED] .119 (US)	/well-known/security.txt	AWS#AWSManagedRulesCommonRuleSet#NoUserAgent_HEADER	BLOCK
AWSManagedRulesCommonRuleSet	20 [REDACTED] 3.210 (ID)	/aws/credentials	AWS#AWSManagedRulesCommonRuleSet#GenericLFI_URIPATH	BLOCK
AWSManagedRulesCommonRuleSet	71 [REDACTED] 00 (US)	/well-known/security.txt	AWS#AWSManagedRulesCommonRuleSet#NoUserAgent_HEADER	BLOCK
[REDACTED]-dotfiles-rule-group	20 [REDACTED] .163 (US)	/api/.env	-	BLOCK
[REDACTED]-dotfiles-rule-group	13 [REDACTED] 4.48 (FR)	/env	-	BLOCK
[REDACTED]-dotfiles-rule-group	2.5 [REDACTED] .13 (IT)	/env.prod	-	BLOCK
[REDACTED]-dotfiles-rule-group	20 [REDACTED] .163 (US)	/local/.env	-	BLOCK
[REDACTED]-dotfiles-rule-group	51 [REDACTED] .6 (GB)	/env	-	BLOCK

2.3 Analysis - (2)

2.3 Analysis - (2)

If a request matches the statement

Statement

Inspect

Single header

Header field name user-agent

Match type Exactly matches string

String to match ELB-HealthChecker/2.0

Text transformation

AWS WAF applies all transformations to the request before evaluating it. If multiple text transformations are added, then text transformations are applied in the order presented below with the top of the list being applied first.

None

Add text transformation

You can add up to 10 text transformations.

Then

Action

Choose an action to take when a request matches the statements above.

Allow

Block

Count

Add label - optional

Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

Label

Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or aws:managed;aws:managed-rule-set:namespace1:name.

- Each namespace or name can have up to 128 characters.
- You can specify up to 5 namespaces in a label.
- Labels are case sensitive.
- You can't use reserved names in labels. Reserved names include "aws:awsf", "aws", "waf", "rulegroup", "webacl", "regexpatternset", "ipset", and "managed".

logdrop:healthchecker

Remove

Add another label

Cancel Add rule

Set rule priority [Info](#)

Rules (6)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Name	Capacity	Action
drop-elb-healthchecker	3	Allow
○		
○		
○		
○		
○		

[Move up](#) [Move down](#)

Filter logs

Add filters to control which web requests are logged. If you add multiple filters, AWS WAF evaluates them starting from the top.

Filter 1

Filter requirement

Criteria for a request to be a match for the filter conditions.

Match all of the filter conditions

Match at least one of the filter conditions

Filter conditions

Select the filtering criteria.

Condition type Condition value

Request has label [Remove](#)

Enter any fully qualified label. For example, aws:awsf:managed:aws:linux-os:LFI_header. [Learn More](#)

Add condition

Filter behavior

Select the action to take for requests that match the filter criteria.

Keep in logs

Drop from logs

Add filter

Default logging behavior

Default logging behavior

Indicate how to handle requests that don't match any of the specified log filters.

Keep in logs

Drop from logs

Cancel Save

Q&A

Question

Answer

마치며.

보안은 상상력과 영감의 영역

상상력과 영감을 믿자

보안이라 하면 딱딱하고 내 일이 아니고 성가시고 가급적 피해야 할 일인가? 상당히 많은 사람이 그러한 감정을 느낀다. 그러나 그 감정이 두려움에서 비롯되지 않는지 차분히 생각해보자. 조직의 경계를 넘어선 협의가 필요하기 때문에 힘든가? 일이 많은데 보안까지 감안하려니 벅찬가? 실은 생산성과 보안을 모두 잡기가 어렵기 때문에 더 즐겁고 보람찰 수 있다. 그리고 가장 중요하고 희망적인 소식은 두려움을 걷어내고 나면 실제 상황은 훨씬 좋다는 것이다.

핵심은 상상력과 영감이다. 뜯구름 잡는 소리 같겠지만 이것이야말로 내가 할 수 있는 최선의 조언이다. 어렵기 때문에 새로운 관점에서 문제를 바라봐야 하며 때로는 매우 편의주의적인 꼼수를 짜내야 한다.

`ssh`와 같이 외부에서 내부로 접근하는 수단을 어떻게 보호할 것인지 고민인가? 차라리 고민의 방향을 바꾸면 어떤가? 내부에서 외부로 접속을 뚫는 것은 어떠한가? 잘 찾아보면 상용/비상용 솔루션이 있다. 내가 처음하는 생각은 아니지만 발상을 해내야 그러한 솔루션을 찾아낼 수 있다.

한술 더 떠보자. `ssh`가 애초에 필요한 이유는 무엇인가? 장애시 문제 진단을 하려 접근하는 경우가 99%인가? 그렇다면 로그 분석 등 모니터링 체계를 제대로 갖추기만 해도 대부분의 문제가 해결되지 않는가? HA 구성과 프로비저닝을 제대로 갖추면 어떠한가? 문제가 되는 노드를 새 노드로 교체하는 것만으로도 장애 대응이 된다면 굳이 `ssh` 접속을 할 필요가 있는가?

코로나 19 때문에 재택근무가 많아져 고민인가? 업무망에서만 접근가능하던 백오피스를 VPN으로 열어주려니 비개발자에게 교육을 제공하고 전에 없던 접근제어체계를 구축해야 하니 힘든가? 그런데 말이지. VPN이 유일한 접근제어 솔루션인가? VPN 대신 [AWS AppStream](#)을 쓰면 어떠한가? AppStream 서비스에만 백오피스의 방화벽을 열면 되므로 많이 설정할 게 없다. 접근제어와 로깅은 클라우드 서비스 사업자가 제공하므로 구현하느라 애쓸 필요가 없다.

보안은 지루한 일이 아니다. 되려 상상력이 끔찍히도 많이 요구되는 흥미로운 업무이다. 더 많은 사람이 이를 깨닫는 조직은 현대적 보안을 더 손쉽게 구현할 것이다.

보안은 서비스를 안전하게 하는 것이 목적이다.

