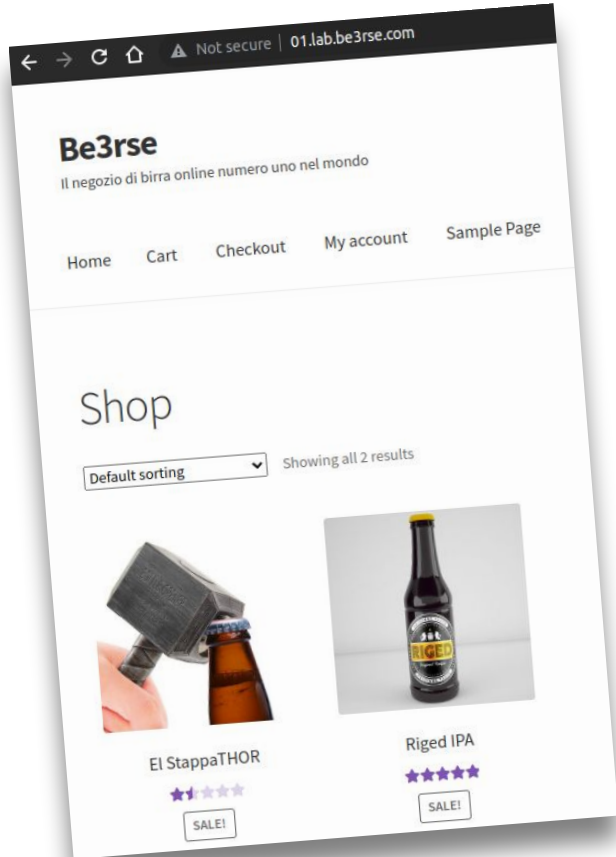


rev3rse  
Security Lab

Be3rse online Beer Shop

Numero 1 nel mondo

Inventori della premiata **FleboBeer**



Security Team

WooCommerce

AWS Cloud

Ogni partecipante ha un numero

<numero>.lab.be3rse.com

Risorse su AWS per <numero>

code.<numero>.lab.be3rse.com:8080

esempio: 01.lab.be3rse.com

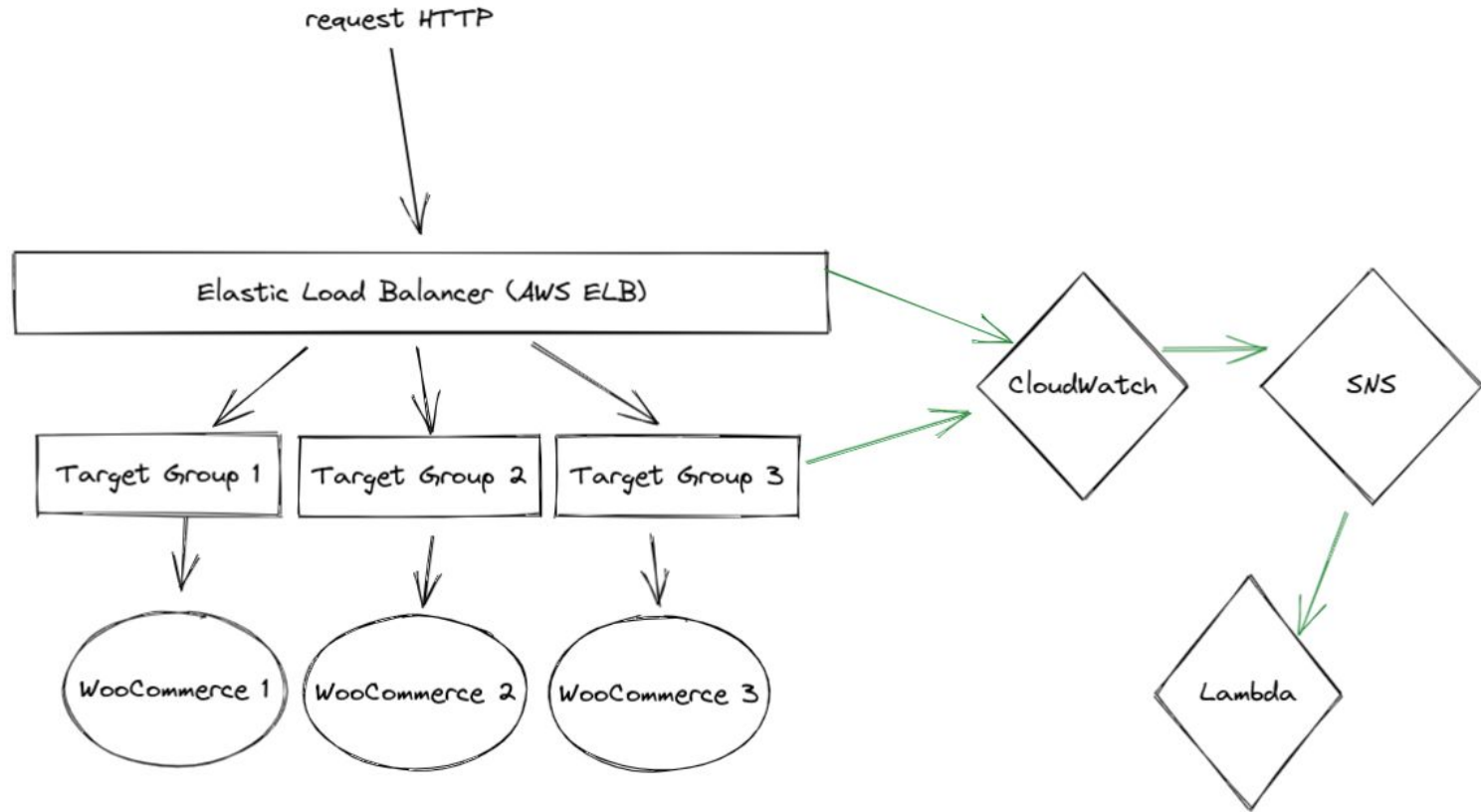
Elastic Load Balancer (ELB)

Target Group

Simple Notification Service (SNS)

CloudWatch

Lambda



## Security Threats:

DoS Layer 7 (booters)

Coupon Code Cracking

Minacce gruppo hacktivisti  
**“Alcolisti Anonymous”**



# “Alcolisti Anonymous”: Gruppo di Hacktivististi contro l'uso di alcolici

## Servizi di booter/stresser (DoS for hire)

\$23.99 1 month	\$34.99 1 month	\$44.99 10 years
1 Month Gold	1 Month Diamond	Lifetime Bronze
Time per boot	2400 sec	3600 sec
Concurrents	1	2
Total network	220Gbps	220Gbps
Tools	Included	Included
Support	24/7	24/7
Buy with Paypal 	Buy with Paypal 	Buy with Paypal 
 <b>bitcoin</b>	 <b>bitcoin</b>	 <b>bitcoin</b>

Our Pricing				
1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent *	1 Concurrent *	1 Concurrent *	1 Concurrent *	1 Concurrent *
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now




## “Alcolisti Anonymous”:

Gruppo di Hacktivististi contro l'uso di alcolici

## Brute-Force codici di sconto

Cart

Product	
	<a href="#">El StappaTHOR</a>
<input type="text" value="BE3RSE-123"/>	Apply coupon

```
Going to http://01.lab.be3rse.com/cart
Found coupon nonce: b26a7bcc3c
Applying coupon...

[SKIP] Coupon BE3RSE-0 not applied (status code 200)
[ERROR] Coupon BE3RSE-1 something went wrong (status code 200).
[SKIP] Coupon BE3RSE-2 not applied (status code 200)
[SKIP] Coupon BE3RSE-3 not applied (status code 200)
[SKIP] Coupon BE3RSE-4 not applied (status code 200)
[SKIP] Coupon BE3RSE-5 not applied (status code 200)
[SKIP] Coupon BE3RSE-6 not applied (status code 200)
[SKIP] Coupon BE3RSE-7 not applied (status code 200)
[SKIP] Coupon BE3RSE-8 not applied (status code 200)
[SKIP] Coupon BE3RSE-9 not applied (status code 200)
[OK] -----> Coupon BE3RSE-10 applied successfully
```

## Challenge JavaScript:

"obbligare" il browser a eseguire JS per accedere al sito  
o accedere a funzionalità come "apply coupon"

automatismi non in grado di interpretare JS

obfuscation tramite JSFuck

```
document.cookie="dosp=deadbeef1234"
```

```
document.cookie="dosp=de" + (![][+[]])[+!+[]] + "dbeef1234"
```

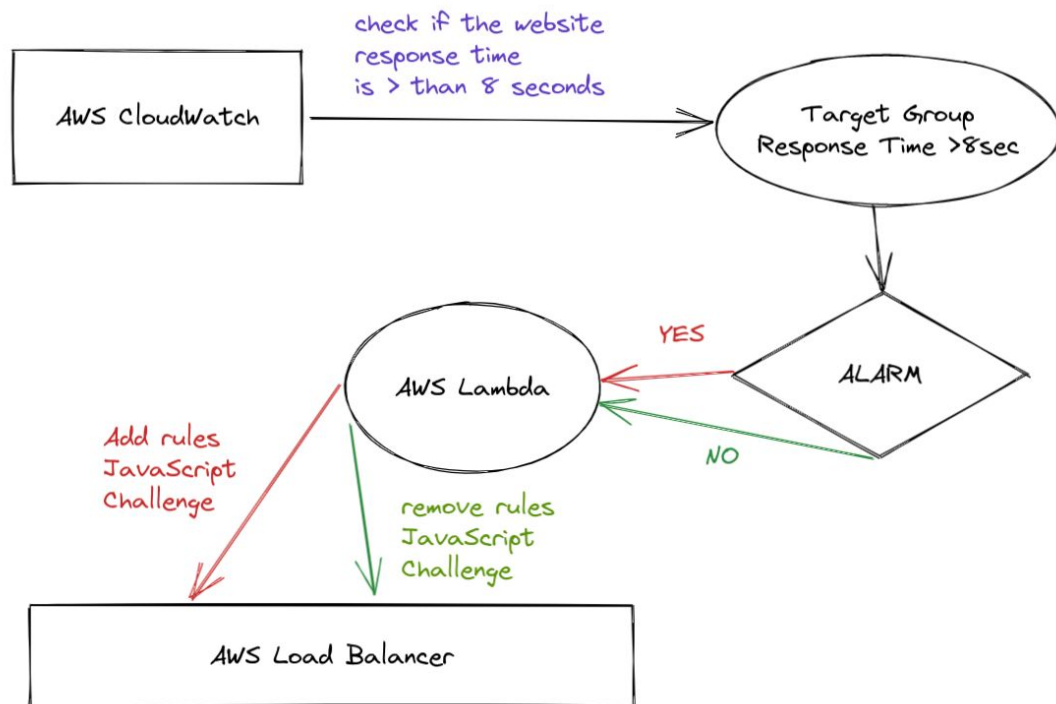
# Challenge JavaScript JSFuck:

```

0 = [ + [ ] ] + [ ]
1 = [ + ! + [ ] ] + [ ]
2 = [ ! + [ ] + ! + [ ] ] + [ ]
3 = [ ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
4 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
5 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
6 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
7 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
8 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
9 = [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + [ ]
a = ( ! [ ] + [ ] ) [ + ! + [ ] ]
...

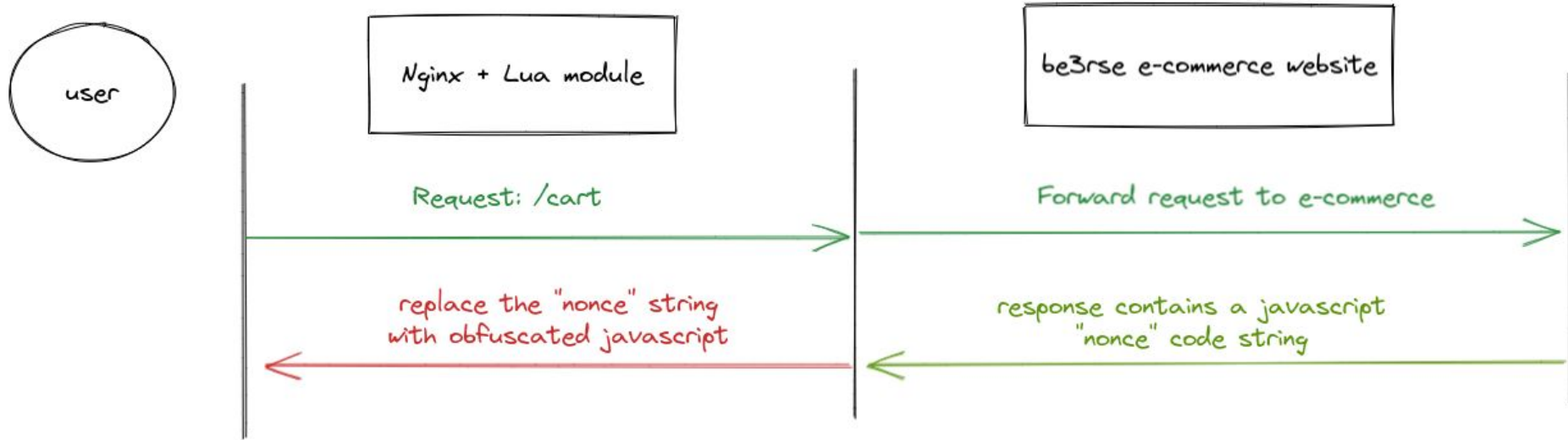
```

# DoS Protection automation AWS



1. Create Lambda
2. Create SNS Topic
3. Registrare SNS su Lambda
4. Create CloudWatch Alarm
5. Test DoS

# Apply Coupon Nonce Obfuscation



rev3rse  
Security Lab