

SOLUTION

1. Find the vulnerability

- On the fake E-Shop page, you will find a user login symbol. Click on it, and follow the **Not a member? Sign up** link to create a user account.
- Log in using your newly created credentials.
- Click on the **ORDERS** link in the top menu.
- You'll notice a search field here. You can try an injection here, for example:

' OR 1=1 --

- The injection works! The application discloses detailed information about paying customers:

Your Payments

Payment ID: 3414835d-8420-42e8-b782-ce4aa22e5b2a Name: Luigi Rossi Billing Address: via Ospedale, 01, Cagliari (CA) Total: \$699.98	Credit Card: 4023 3617 6532 0997 CVV: 456 Expiration Date: 2025/11/31
Payment ID: 5yta835d-8420-42e8-b782-c788722e5b2a Name: John Milan Billing Address: 679 Fifth Street Tucson, AZ 85718 Total: \$29.48	Credit Card: 6394 8269 2835 7263 CVV: 092 Expiration Date: 2034/01/31
Payment ID: 3414835d-8420-42e8-b782-ce3aa22e5b2a Name: Mario Bianchi Billing Address: via Goito, 15, Cagliari (CA) Total: \$399.98	Credit Card: 4023 5757 7346 7788 CVV: 306 Expiration Date: 2029/02/31
Payment ID: 5714835d-8420-42e8-b782-ce3aa22e5b2a Name: Giuseppe Verdi Billing Address: via delle Sedie Volanti, 143, Oristano (OR) Total: \$68.48	Credit Card: 4064 5333 3459 7681 CVV: 988 Expiration Date: 2030/07/31
Payment ID: 5714835d-8420-42e8-b782-ceaha22e5b2a Name: Federico Barbarossa Billing Address: via Della Pазienza Roma (RO) Total: \$128.49	Credit Card: 4063 7859 1254 0978 CVV: 187 Expiration Date: 2032/03/31
Payment ID: 5yta835d-8420-42e8-b782-ceaha22e5b2a Name: Frank Daniels Billing Address: 981 N. Marconi Street Cornelius, NC 8031 Total: \$198.98	Credit Card: 5547 5828 1686 6830 CVV: 683 Expiration Date: 2022/06/31
Payment ID: 5yta835d-kawj-42e8-b782-c788722e5b2a Name: Paul Arthur Billing Address: 25 S. Virginia Street Harrison Township, MI 48045 Total: \$24.00	Credit Card: 7879 9181 5540 0454 CVV: 581 Expiration Date: 2031/02/31

2. Use Seer Box to Create a Protection Rule

- Access Seer Box's web interface and navigate to the **Detection → Alerts** section. You'll see an alert for the vulnerability you've just discovered.

Detection

Alerts

Order by Last seen

ATTACK TYPE	REQUEST HOST	ATTACK PATTERN ⓘ	STATUS CODES	DETAILS
SQL Injection Injection	baltimore:8082	' OR 1=1 -- Parameter value	✓ Server success 200	13/10/2026 18:34:32 1 malicious clients

- Click on the magnifying glass icon :mag: to inspect the alert's details, then click on **Advanced Protection** at the top right

← Alerts

Alerts

Advanced protection

ID alert
EdaXySLmZNVCF5OVA8mPMMfRFqrGgK+P£VtWdrerZLk=

Attack Type
SQL Injection / [Injection](#)

CWE

[CWE-707](#) [CWE-74](#) [CWE-943](#) [CWE-89](#)

Attack pattern
' OR 1=1 --
Parameter value

Status codes
✓ Server success
200

Alert movements

First seen: Tue Oct 13 2026 18:34:32 GMT+0200
Last seen: Tue Oct 13 2026 18:34:32 GMT+0200
Detected: Tue Oct 13 2026 18:34:34 GMT+0200

[Alert specifications](#) [Http traffic](#) [Http clients](#)

REQUEST HOST	PATH	PARAMETER KEY	TARGET	PAYLOAD
baltimore:8082	/orders	filter	Parameter value	' OR 1=1 --

- Build a new rule leaving all values and firewall actions unmodified (click **Next** until you reach the final step of the rule creation wizard), then click on **Add Rule** and finally **Save** it using the button at the top

CyberSuite Hackathon Challenge: Seer Box

← Alerts

Alerts

Cancel

Save

Advanced protection

Build a new rule

Define the rule conditions

1

2

3

4

Strategy

Application rule

Context

One host ^

Conditions

Targets parameter_value	Operator Contains	Expressions ' OR 1=1 --
Targets parameter_key	Operator Is equal	Expressions filter
Targets path	Operator Is equal	Expressions /orders

Add condition

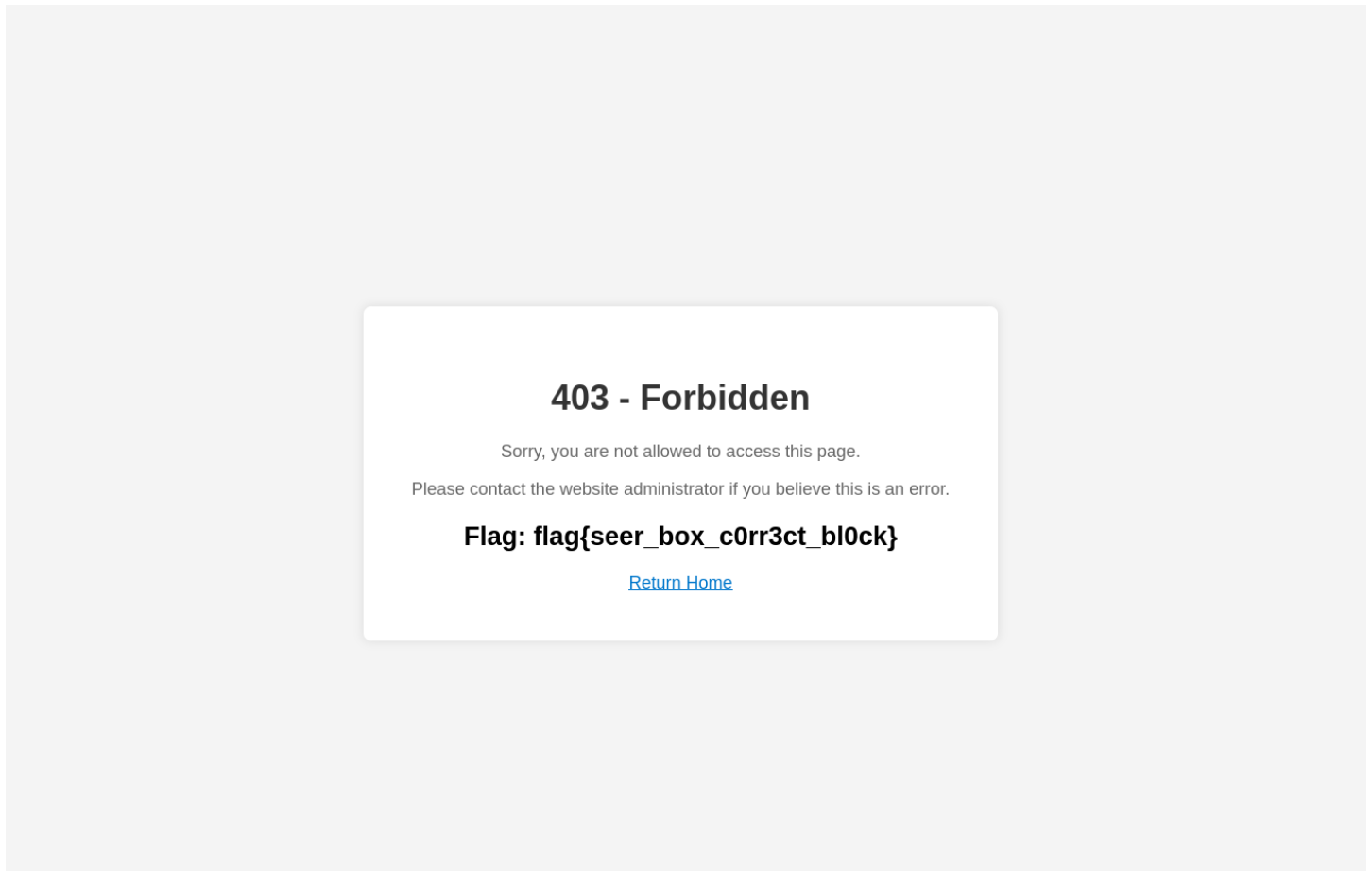
Previous

Next

- The new rule has been created and activated. You're now ready to complete the challenge

3. Collect the flag

- If you try to repeat the same malicious SQL Injection input, **the firewall will block you** and you'll be able to collect your flag, as shown in the screen below:



- You've successfully submitted the flag and completed the challenge!