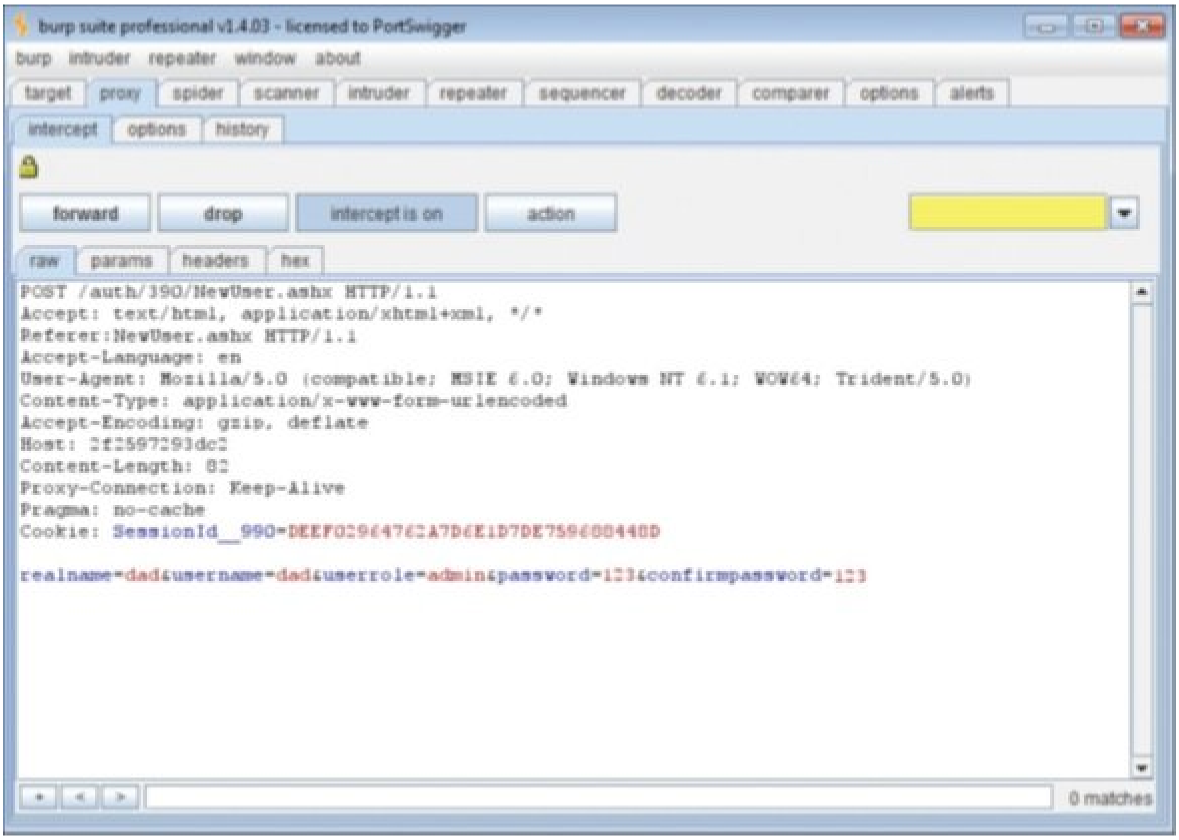
[illegible] CEH ([illegible]): [illegible]

[illegible]

[illegible] CEH [illegible].

[illegible] SQL [illegible] Burp Proxy [illegible].

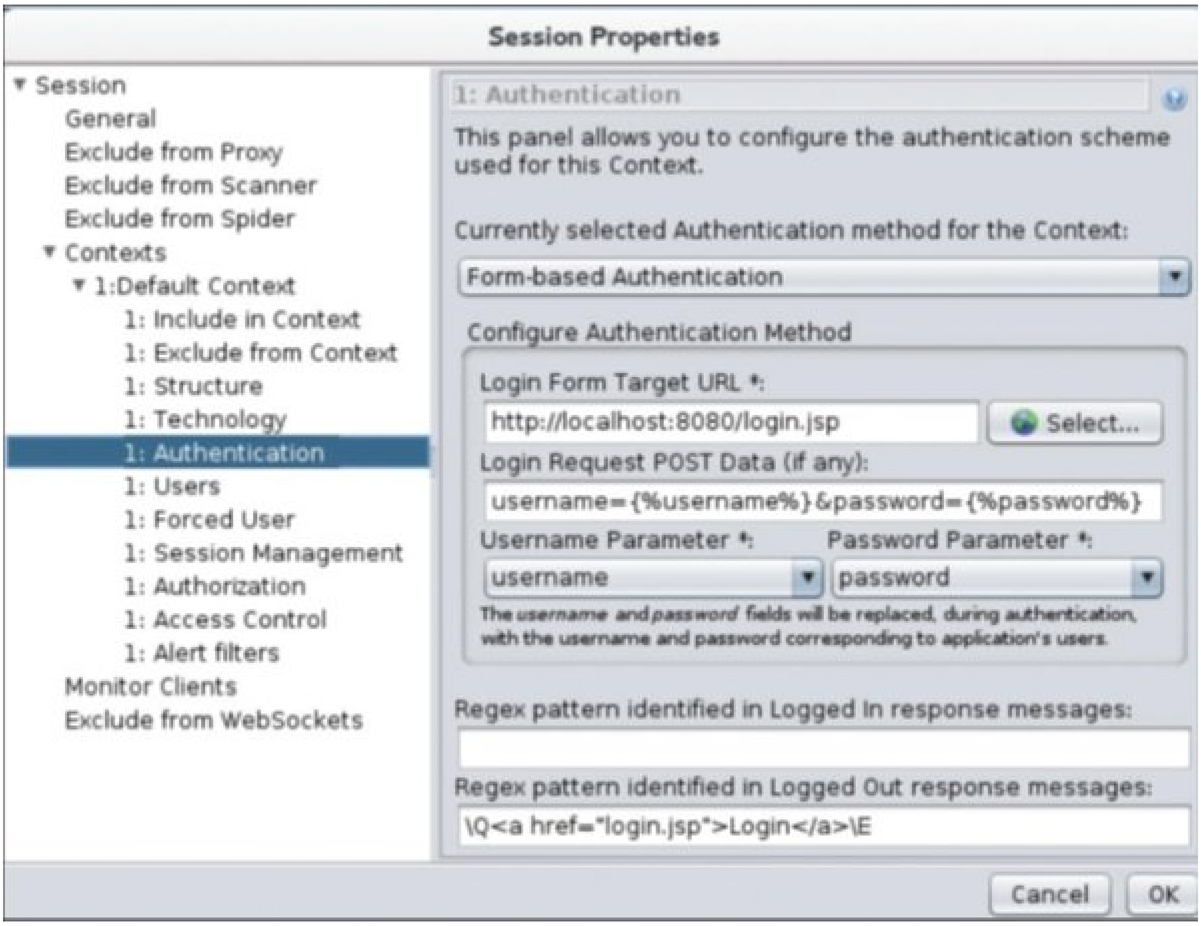

burp suite professional v1.4.03 - licensed to PortSwigger
burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
forward
drop
intercept is on
action
raw params headers hex
+ < >
0 matches

```
POST /auth/390/NewUser.ashx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer:NewUser.ashx HTTP/1.1
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 2f2597293dc2
Content-Length: 82
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: SessionId__990=DEEF02964762A7D6E1D7DE759688440D

realname=dad&username=dad&userrole=admin&password=123&confirmpassword=123
```

[illegible]. [illegible]. [illegible].

[illegible] OWASP ZAP [illegible]. [illegible].



1: Authentication

This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *: http://localhost:8080/login.jsp

Login Request POST Data (if any): username={%username%}&password={%password%}

Username Parameter *: username

Password Parameter *: password

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Regex pattern identified in Logged In response messages:

Regex pattern identified in Logged Out response messages: \QLogin\E

[illegible] CEH [illegible] RFC 5216 [illegible]

[illegible]

[illegible]

[illegible]:

■ Flawfinder: [illegible].

■ Rough Auditing Tool for Security : [illegible] XML [illegible] PHP [illegible] Perl [illegible] C ++ [illegible] C [illegible] Python [illegible].

■ StackGuard: [illegible] stackmashing [illegible]. [illegible] Stack-Smash [illegible] StackGuard [illegible].

[illegible]. [illegible]:

■ Whisker: [illegible]. [illegible] CGI (Common Gateway Interface) [illegible]. [illegible] CGI [illegible]. [illegible] (Perl) [illegible].

■ N-Stalker: [illegible] 30،000 [illegible].

■ WebInspect: [illegible] 1500 [illegible].

■ Nikto: [illegible].

■ AppDetectivePRO: [illegible].

[illegible].
Fuzzing [illegible].

SQL [illegible]

[illegible] (SQL Injection Attacks) [illegible].

[illegible] SQL

[illegible] SQL [illegible]:

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] SQL [illegible]

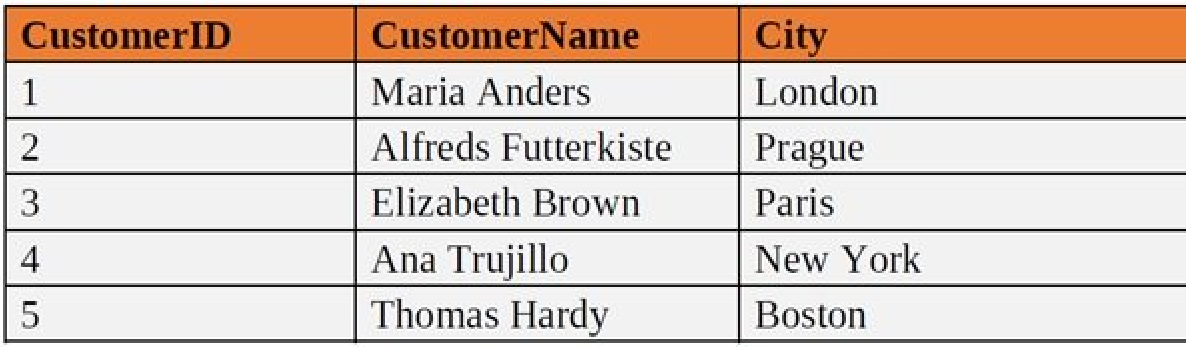
[illegible] SQL [illegible]. [illegible] SQL [illegible].

[SELECT * FROM [Orders

[illegible] "[illegible]" [illegible].

[illegible] SQL

[illegible] DELETE [illegible]. [illegible] "[illegible]" [illegible]. [illegible] "[illegible]" [illegible]:

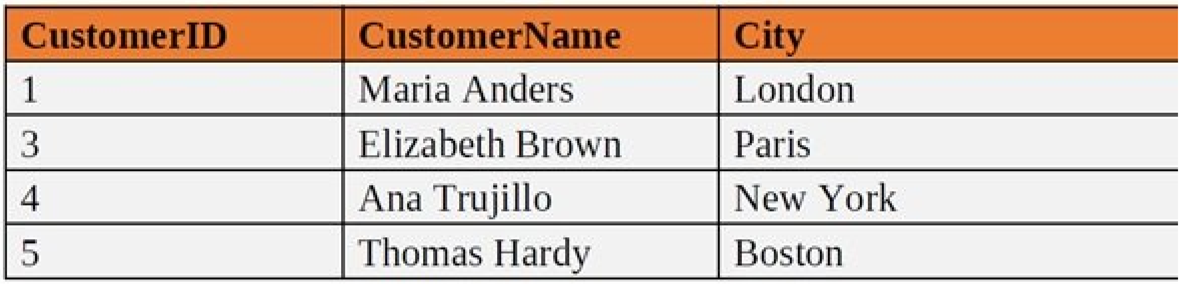


CustomerID	CustomerName	City
1	Maria Anders	London
2	Alfreds Futterkiste	Prague
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

[illegible] delete [illegible].

```
DELETE FROM Customers
;'WHERE CustomerName='Alfreds Futterkiste
```

:[illegible]



CustomerID	CustomerName	City
1	Maria Anders	London
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

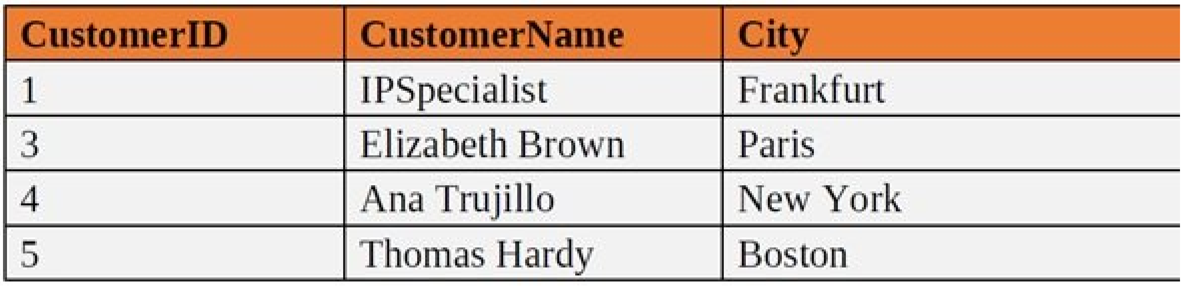
[illegible] Delete [illegible] SQL [illegible] .[illegible]

SQL [illegible]

:[illegible] .[illegible] UPDATE [illegible]

```
UPDATE Customers
'SET ContactName = 'IPSpecialist, City= 'Frankfurt
;WHERE CustomerID = 1
```

:[illegible]



CustomerID	CustomerName	City
1	IPSpecialist	Frankfurt
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

SQL [illegible]

:[illegible] SQL [illegible]

BSQL Hacker

Marathon Tool

SQL Power Injector

Havij

[illegible]

.[illegible] SQL [illegible]

In-band SQLi .1

Inferential SQLi .2

Out-of-band SQLi .3

In-Band SQL[illegible]

[illegible] In-Band [illegible]
:[illegible] In-Band [illegible] .[illegible]

Error-based SQL Injection .1

Union based SQL Injection .2

[illegible]

[illegible] in-band [illegible] .[illegible] SQL [illegible] .[illegible] SQL [illegible] :[illegible]

System Stored Procedure

End of Line Comment

Illegal / Logically incorrect Query

Tautology

Union SQL [illegible]

UNION [illegible] In-Band [illegible] Union SQL [illegible]
.[illegible] SELECT [illegible]

```
SELECT <column_name(s)> FROM <table_1>

UNION

SELECT <column_name(s)> FROM <table_2>;
```

Inferential SQL [illegible]

[illegible] Blind Injection [illegible] .[illegible] .[illegible] Blind-time-based SQL injection [illegible] Blind-Boolean-based SQL injection [illegible]
.[illegible]

Boolean Exploitation [illegible]

[illegible] .[illegible] Blind SQL [illegible]

[illegible] HTTP [illegible]

[illegible] Out-of-band SQL Injection

[illegible] DNS [illegible] HTTP [illegible]

[illegible] SQL

[illegible] SQL

[illegible]

[illegible]

[illegible] **CEH** [illegible]:

[illegible] CEH

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
13:50 - 11/04/1399
[illegible]:
[illegible] CEH - [illegible] CEH - [illegible] CEH - [illegible] - [illegible] CEH v10 - [illegible] - [illegible] CEH10 - [illegible] - [illegible] - [illegible] - [illegible] SQL

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/17025/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A8%D9%87-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%88%D8%A8%E2%80%8C%D9%85%D8%AD%D9%88%D8%B1-%D8%AD%D9%85%D9%84%D9%87-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF%D8%9F