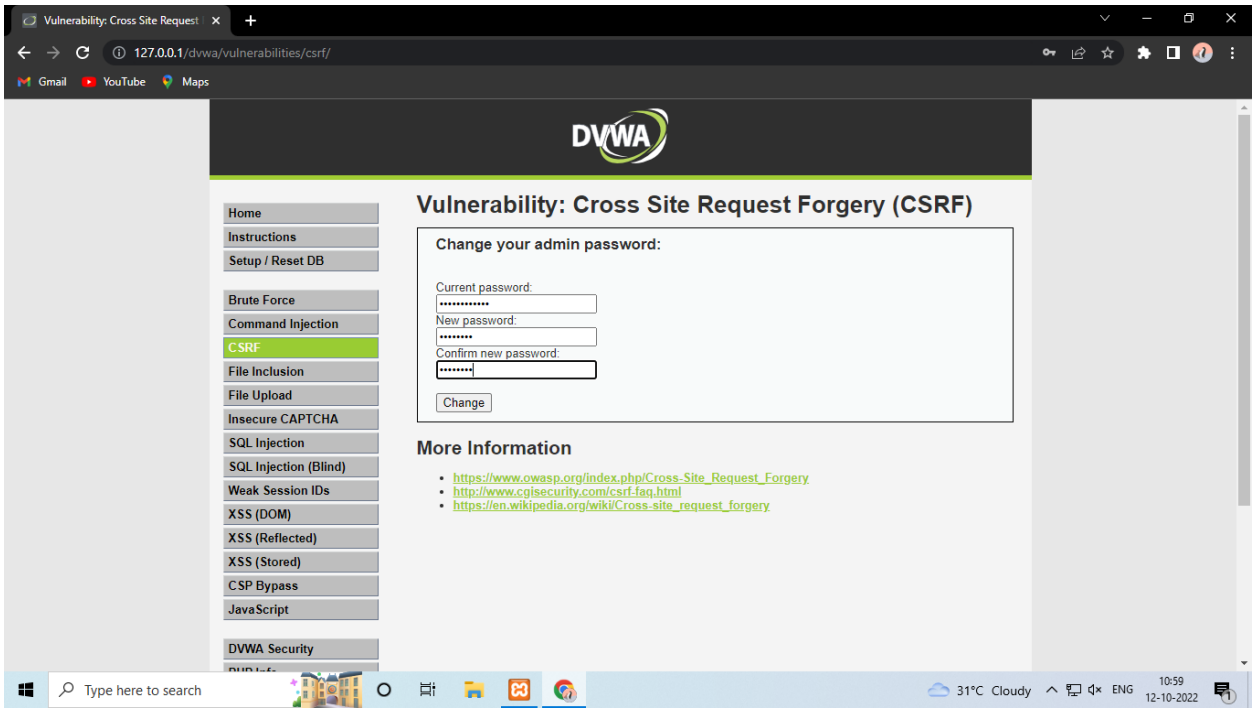
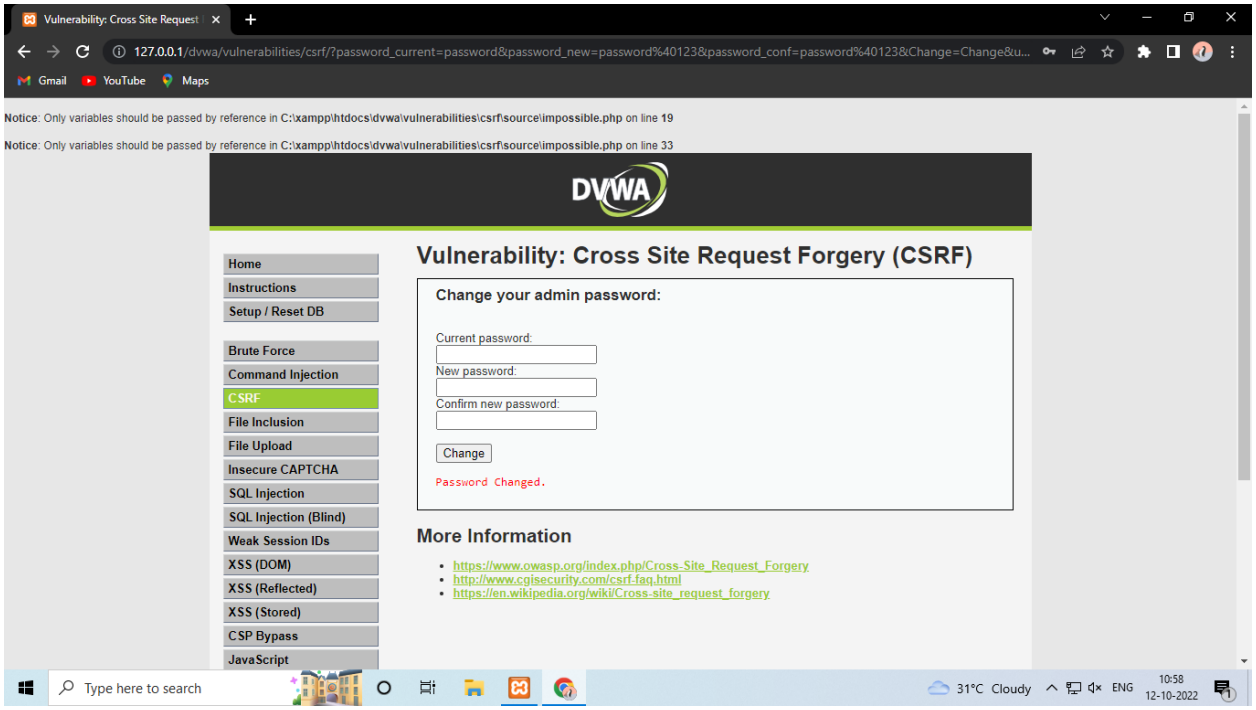

DVWA Security :: Damn Vulnerab
127.0.0.1/dvwa/security.php
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
PHPIDS
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in
Type here to search
31°C Cloudy
ENG
10:57
12-10-2022


Vulnerability: Cross Site Request
127.0.0.1/dvwa/vulnerabilities/csrf/
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
Vulnerability: Cross Site Request Forgery (CSRF)
Change your admin password:
Current password:
New password:
Confirm new password:
Change
More Information
https://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
https://en.wikipedia.org/wiki/Cross-site_request_forgery
Type here to search
31°C Cloudy
ENG
10:59
12-10-2022


Vulnerability: Cross Site Request
127.0.0.1/dvwa/vulnerabilities/csrf/?password_current=password&password_new=password%40123&password_conf=password%40123&Change=Change&u...
Gmail
YouTube
Maps
Notice: Only variables should be passed by reference in C:\xampp\htdocs\dvwa\vulnerabilities\csrf\source\impossible.php on line 19
Notice: Only variables should be passed by reference in C:\xampp\htdocs\dvwa\vulnerabilities\csrf\source\impossible.php on line 33
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Cross Site Request Forgery (CSRF)
Change your admin password:
Current password:
New password:
Confirm new password:
Change
Password Changed.
More Information
https://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
https://en.wikipedia.org/wiki/Cross-site_request_forgery
Type here to search
31°C Cloudy
ENG
10:58
12-10-2022


Login :: Damn Vulnerable Web A
127.0.0.1/dvwa/login.php
Gmail
YouTube
Maps
DVWA
Username
admin
Password
Login
Login failed
Damn Vulnerable Web Application (DVWA)
Type here to search
31°C Cloudy
ENG
10:58
12-10-2022