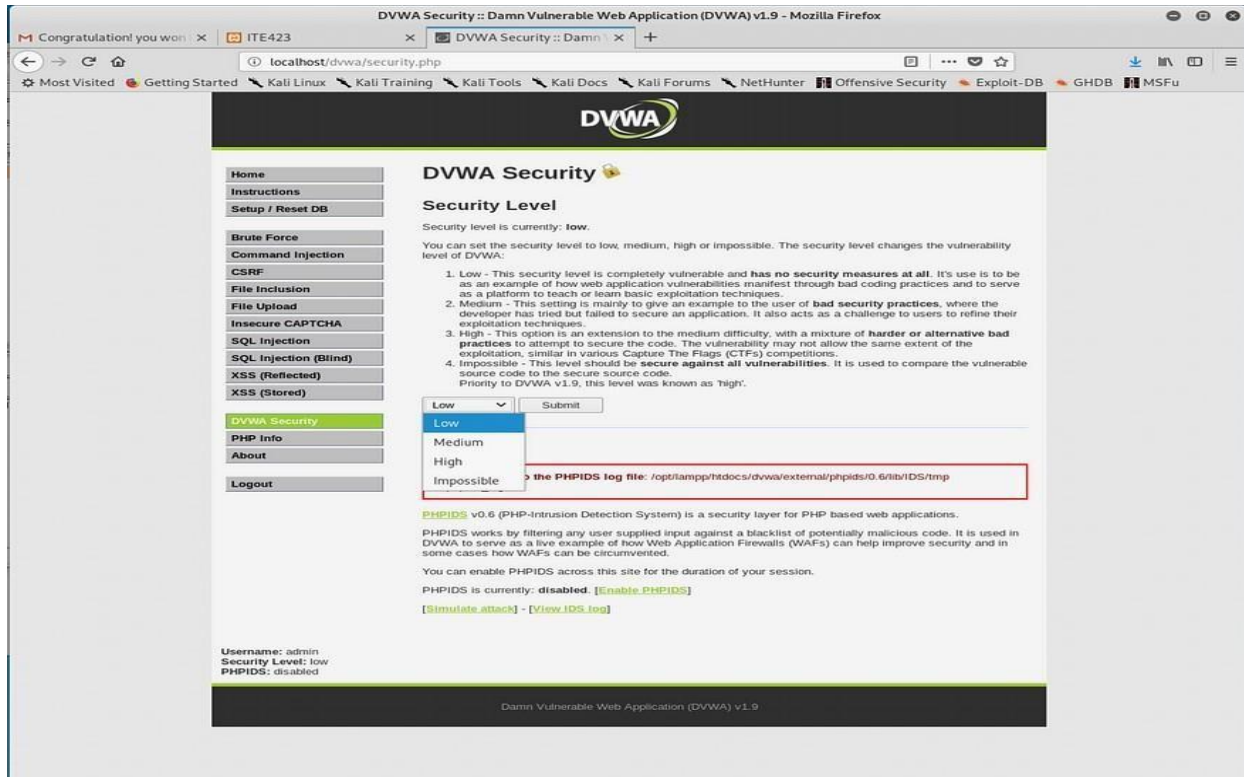


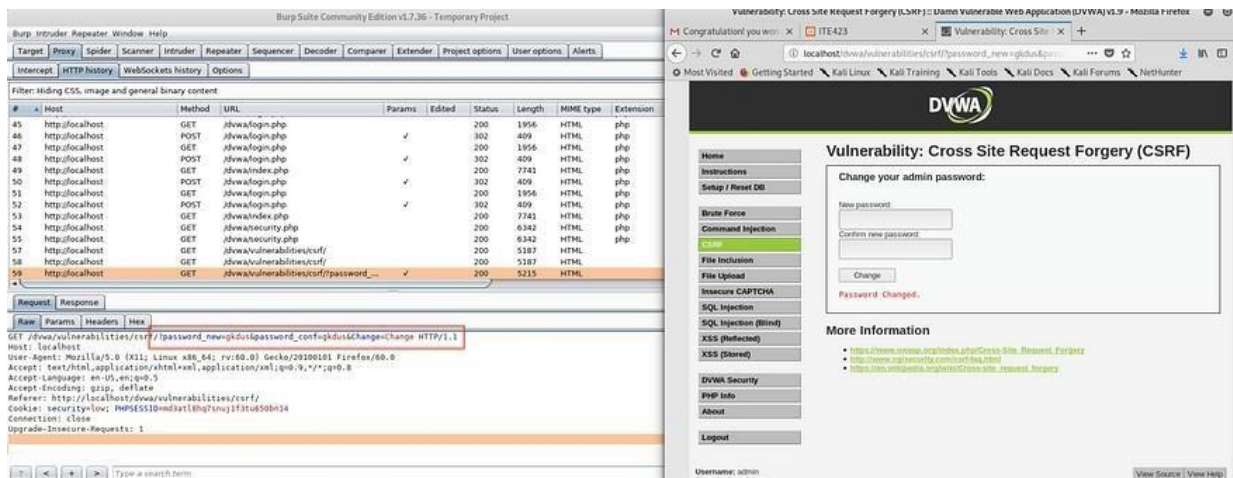
# Experiment-08:Cross – Site Request Forgery (CSRF)

## Changing Security Level to low



The screenshot shows the DVWA Security page in a Mozilla Firefox browser. The page title is "DVWA Security :: Damn Vulnerable Web Application (DVWA) v1.9". The left sidebar contains navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and "Security Level". It states: "Security level is currently: low. You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:". Below this, there are four numbered points explaining the security levels. A dropdown menu is open, showing "Low" selected. A red box highlights the text: "to the PHPIDS log file: /opt/lampp/htdocs/dvwa/external/phpids/0.6/lib/IDS/tmp". Below this, it says "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 some cases how WAFs can be circumvented. You can enable PHPIDS across this site for the duration of your session. PHPIDS is currently: disabled. [Enable PHPIDS] [Simulate attack] - [View IDS log]". At the bottom, it says "Username: admin Security Level: low PHPIDS: disabled".

## find the HTTP request on Burp-suite



The screenshot shows two windows. The left window is Burp Suite Community Edition v1.7.36 - Temporary Project. It displays a list of HTTP requests. The selected request is a GET request to http://localhost/dvwa/vulnerabilities/csrf/?password\_new=gidspassword\_conf=gidspassword\_change HTTP/1.1. The right window is a Mozilla Firefox browser showing the DVWA "Vulnerability: Cross Site Request Forgery (CSRF)" page. The page has a form titled "Change your admin password:" with fields for "New password:" and "Confirm new password:". Below the form, it says "Password Changed.". The left sidebar of the browser shows the same navigation links as the first screenshot. The bottom of the browser shows "Username: admin Security Level: low".

Get method to transfer new password being used On left, you can find request has successfully transferred / On right is the screen of csrf.html

The image shows two side-by-side windows. The left window is Burp Suite Community Edition v1.7.36, displaying the HTTP history tab. A list of requests is shown, with the last request (ID 58) highlighted. This request is a GET method to `http://localhost:8080/vulnerability/csrf/password_new=ghdus&password_conf=ghdus&Change=Change HTTP/1.1`. The right window is a Mozilla Firefox browser showing a page titled "Vulnerability: Cross Site Request Forgery (CSRF)". The page contains a "Click me" button. Below the button, a small dialog box says "CSRF Complete".

Try to distinguish between normal request (left) and malicious request(right)

The image shows Burp Suite's Compare tool. It is comparing two requests. The left pane shows a normal request (Length: 497) with the parameter `password_new=ghdus`. The right pane shows a malicious request (Length: 420) with the parameter `password_new=haryang`. The tool highlights the differences between the two requests, showing that the malicious request has a shorter length and a different password value.

## Checking the response — it fails to change password after Changing security level to medium

The screenshot shows Burp Suite Community Edition v1.7.36 on the left and a web browser on the right. In Burp Suite, the HTTP history list shows a GET request to `http://localhost:127.0.0.1/csrf.html` with status 200. The selected request is expanded, showing the raw response body:

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 200
Server: Apache/2.4.18 (Ubuntu)

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:
Confirm new password:

[Change]

That request didn't look correct.
```

The web browser on the right shows the page titled "Vulnerability: Cross Site Request Forgery (CSRF)". It contains a "Click me" button and a "CSRF Complete" dialog box with an "OK" button.

Changing file name makes attack successful!

The screenshot shows Burp Suite Community Edition v1.7.36 on the left and a web browser on the right. In Burp Suite, the HTTP history list shows a GET request to `http://localhost:127.0.0.1/csrf.html` with status 200. The selected request is expanded, showing the raw response body:

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 200
Server: Apache/2.4.18 (Ubuntu)

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:
Confirm new password:

[Change]

Password Changed
```

The web browser on the right shows the page titled "Vulnerability: Cross Site Request Forgery (CSRF)". It contains a "Click me" button and a "CSRF Complete" dialog box with an "OK" button.