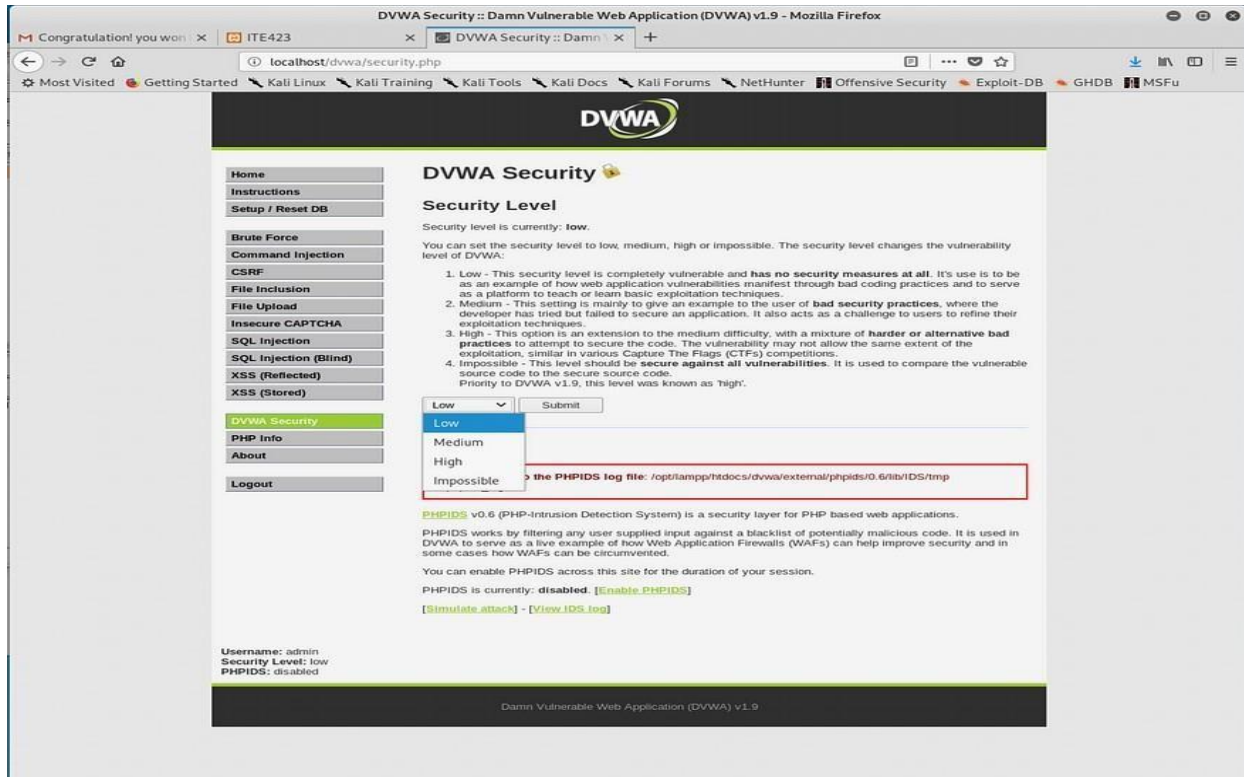


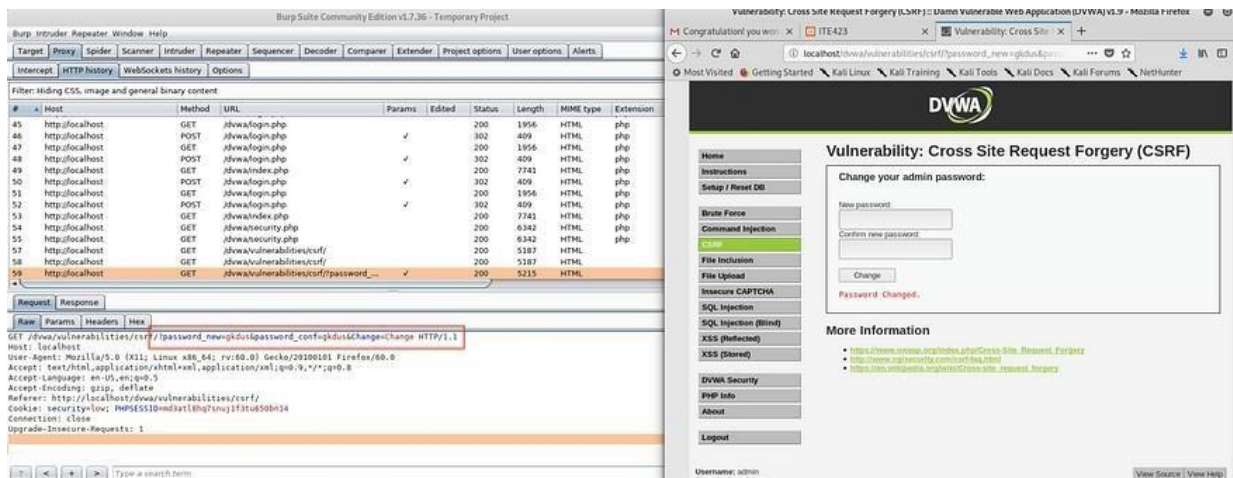
Experiment-08:Cross – Site Request Forgery (CSRF)

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 a menu with options: 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 for "Security Level" is open, showing options: Low (selected), Medium, High, and Impossible. A red box highlights the "PHPIDS log file: /opt/lampp/htdocs/dvwa/external/phpids/0.6/lib/IDS/tmp" link. 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=q&id=password_conf=q&id=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." in red. The page also has a "More Information" section with links to various security resources.

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 a list of HTTP requests. The right window is a Mozilla Firefox browser showing a 'Vulnerability: Cross Site Request Forgery (CSRF)' tutorial page. The browser page has a 'Click me' button and a 'CSRF Complete' dialog box.

Burp Suite HTTP History:

#	Host	Method	URL	Params	Status	Length	MIME type	Extension
45	http://localhost	GET	/jvwa/login.php		200	1956	HTML	php
46	http://localhost	POST	/jvwa/login.php		303	409	HTML	php
47	http://localhost	GET	/jvwa/login.php		200	1956	HTML	php
48	http://localhost	POST	/jvwa/login.php		303	409	HTML	php
49	http://localhost	GET	/jvwa/index.php		200	7748	HTML	php
50	http://localhost	POST	/jvwa/login.php		303	409	HTML	php
51	http://localhost	GET	/jvwa/login.php		200	1956	HTML	php
52	http://localhost	POST	/jvwa/login.php		303	409	HTML	php
53	http://localhost	GET	/jvwa/index.php		200	7748	HTML	php
54	http://localhost	GET	/jvwa/securing.php		200	6342	HTML	php
55	http://localhost	GET	/jvwa/securing.php		200	6342	HTML	php
56	http://localhost	GET	/jvwa/vulnerabilities/csrf/		200	5197	HTML	php
57	http://localhost	GET	/jvwa/vulnerabilities/csrf/		200	5197	HTML	php
58	http://localhost	GET	/jvwa/vulnerabilities/csrf/		200	5197	HTML	php
59	http://localhost	GET	/jvwa/vulnerabilities/csrf/password_...		200	5215	HTML	php

Request Details (Request #59):

```
GET /jvwa/vulnerabilities/csrf/password_new=ghdus&password_conf=ghdus&Change=Change HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/jvwa/vulnerabilities/csrf/
Cookie: security=low; PHPSESSID=md3at18q7huq1f7u650bn14
Connection: close
Upgrade-Insecure-Requests: 1
```

Browser Page: Vulnerability: Cross Site Request Forgery (CSRF) tutorial. Once clicking the button, password will be changed. A 'Click me' button is present. A 'CSRF Complete' dialog box is shown.

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

The image shows two side-by-side windows. The left window is Burp Suite Community Edition v1.7.36, displaying the Comparer tool. The right window is a Mozilla Firefox browser showing a 'Vulnerability: Cross Site Request Forgery (CSRF)' tutorial page with a 'Change your admin password' form.

Burp Suite Comparer:

Select item 1:

#	Length	Data
1	497	GET /jvwa/vulnerabilities/csrf/password_new=ghdus&password_conf=ghdus&Change=Change HTTP/1.1
2	420	GET /jvwa/vulnerabilities/csrf/password_new=haryang&password_conf=haryang&Change=Change HTTP/1.1

Select item 2:

#	Length	Data
1	497	GET /jvwa/vulnerabilities/csrf/password_new=ghdus&password_conf=ghdus&Change=Change HTTP/1.1
2	420	GET /jvwa/vulnerabilities/csrf/password_new=haryang&password_conf=haryang&Change=Change HTTP/1.1

Browser Page: Vulnerability: Cross Site Request Forgery (CSRF) tutorial. Change your admin password: [Form fields for password change]

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 tab is active, showing a list of requests. The selected request is a GET to `/jvwa/vulnerabilities/csrf/?password=...`. The response tab shows a 200 status with HTML content. The web browser displays a page titled "Vulnerability: Cross Site Request Forgery (CSRF)". The page has a sidebar with navigation links like "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", "PHP Info", "About", and "Logout". The main content area shows a form titled "Change your admin password:" with fields for "New password:" and "Confirm new password:", a "Change" button, and a message "That request didn't look correct."

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
58	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5187	HTML	
59	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5215	HTML	
60	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5215	HTML	
61	http://detectportal.firefox.com	GET	/success.txt			200	379	text	txt
62	http://localhost	GET	/jvwa/security.php			200	6342	HTML	php
63	http://localhost	GET	/jvwa/security.php			200	6342	HTML	php
64	http://localhost	POST	/jvwa/security.php			302	505	HTML	php
65	http://localhost	GET	/jvwa/security.php			200	6434	HTML	php
66	http://localhost	GET	/jvwa/security.php			200	6434	HTML	php
67	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML	
68	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML	
69	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML	
70	http://localhost	GET	/jvwa/vulnerabilities/view_source.php			200	7593	HTML	php
71	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5240	HTML	
72	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5240	HTML	

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 tab is active, showing a list of requests. The selected request is a GET to `/jvwa/vulnerabilities/csrf/?password=...`. The response tab shows a 200 status with HTML content. The web browser displays a page titled "Vulnerability: Cross Site Request Forgery (CSRF)". The page has a sidebar with navigation links like "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", "PHP Info", "About", and "Logout". The main content area shows a form titled "Change your admin password:" with fields for "New password:" and "Confirm new password:", a "Change" button, and a message "Password Changed".

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
61	http://detectportal.firefox.com	GET	/success.txt			200	379	text	txt	
62	http://localhost	GET	/jvwa/security.php			200	6342	HTML	php	DVWA Security :: Damn...
63	http://localhost	GET	/jvwa/security.php			200	6342	HTML	php	DVWA Security :: Damn...
64	http://localhost	GET	/jvwa/security.php			200	6342	HTML	php	DVWA Security :: Damn...
65	http://localhost	POST	/jvwa/security.php			302	505	HTML	php	DVWA Security :: Damn...
66	http://localhost	GET	/jvwa/security.php			200	6434	HTML	php	DVWA Security :: Damn...
67	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML		Vulnerability: Cross Site...
68	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML		Vulnerability: Cross Site...
69	http://localhost	GET	/jvwa/vulnerabilities/csrf/			200	5196	HTML		Vulnerability: Cross Site...
70	http://localhost	GET	/jvwa/vulnerabilities/view_source.php			200	7593	HTML	php	Damn Vulnerable Web...
71	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5240	HTML		Vulnerability: Cross Site...
72	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5240	HTML		Vulnerability: Cross Site...
73	http://127.0.0.1	GET	/csrf_localhost.html			200	905	HTML	kind	Vulnerability: Cross Site...
74	http://localhost	GET	/jvwa/vulnerabilities/csrf/?password=...			200	5224	HTML		Vulnerability: Cross Site...