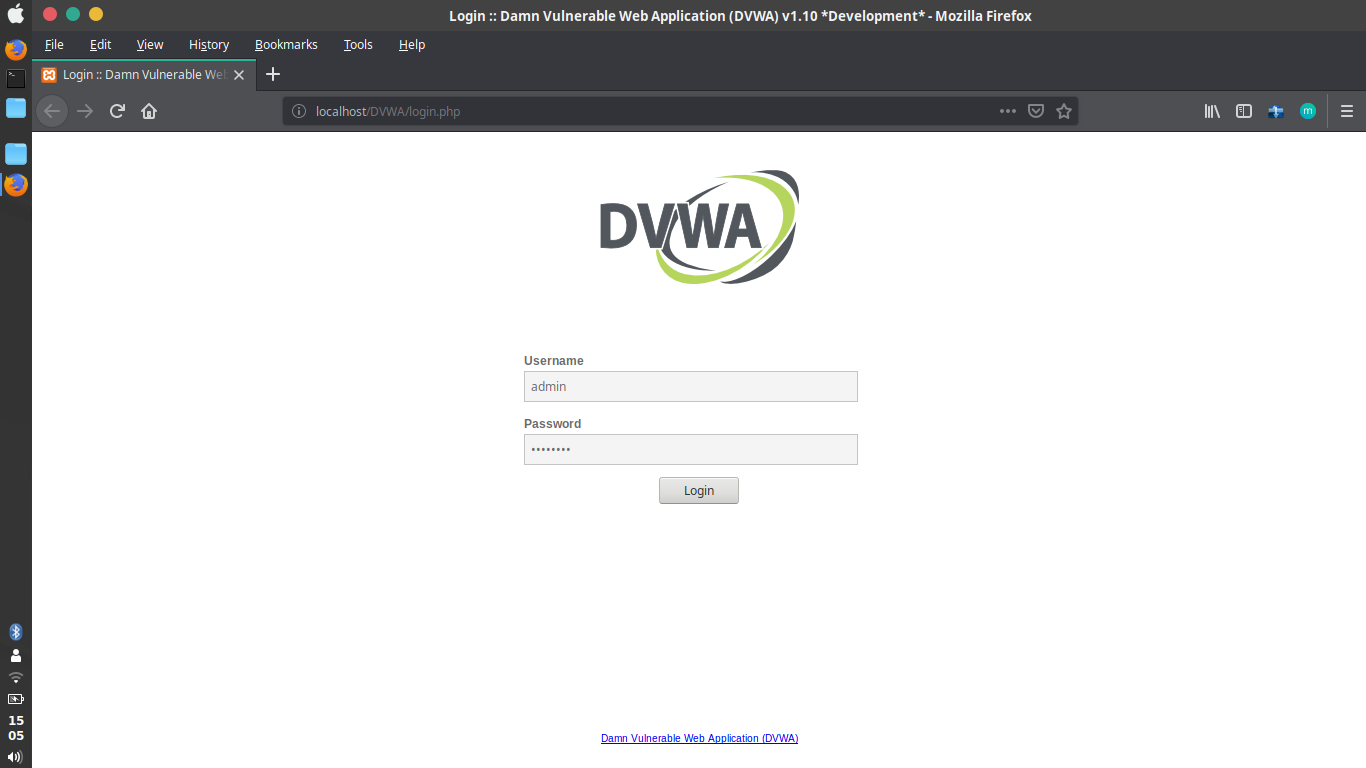
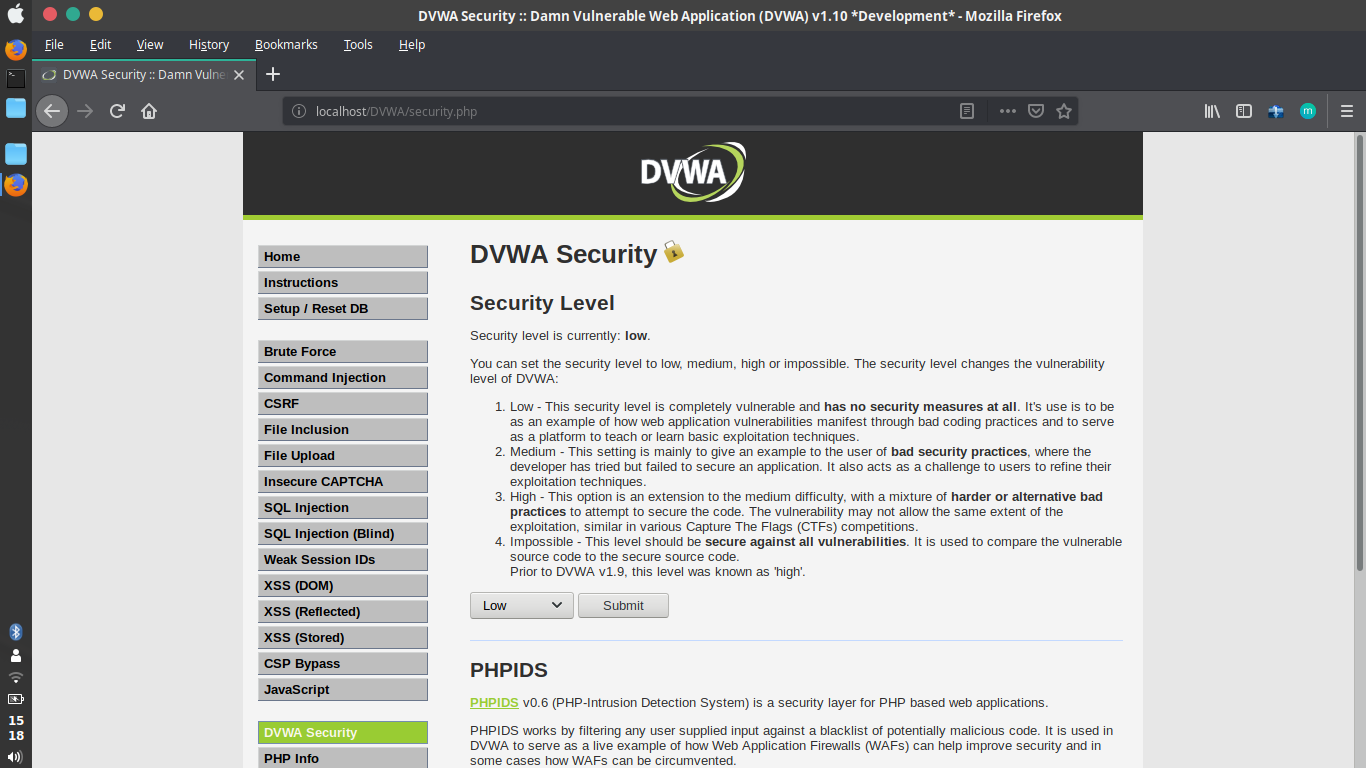
Mencoba DVWA.

DIsini saya menggunakan DVWA terbaru yang saya dapat dari github karena DVWA yang telah diberikan masih menggunakan versi php 5 yang sudah jarang dipakai, sehingga saya mencari DVWA yang paling terbaru dan menemukanya di github. Lalu menginstallnya pada server local.

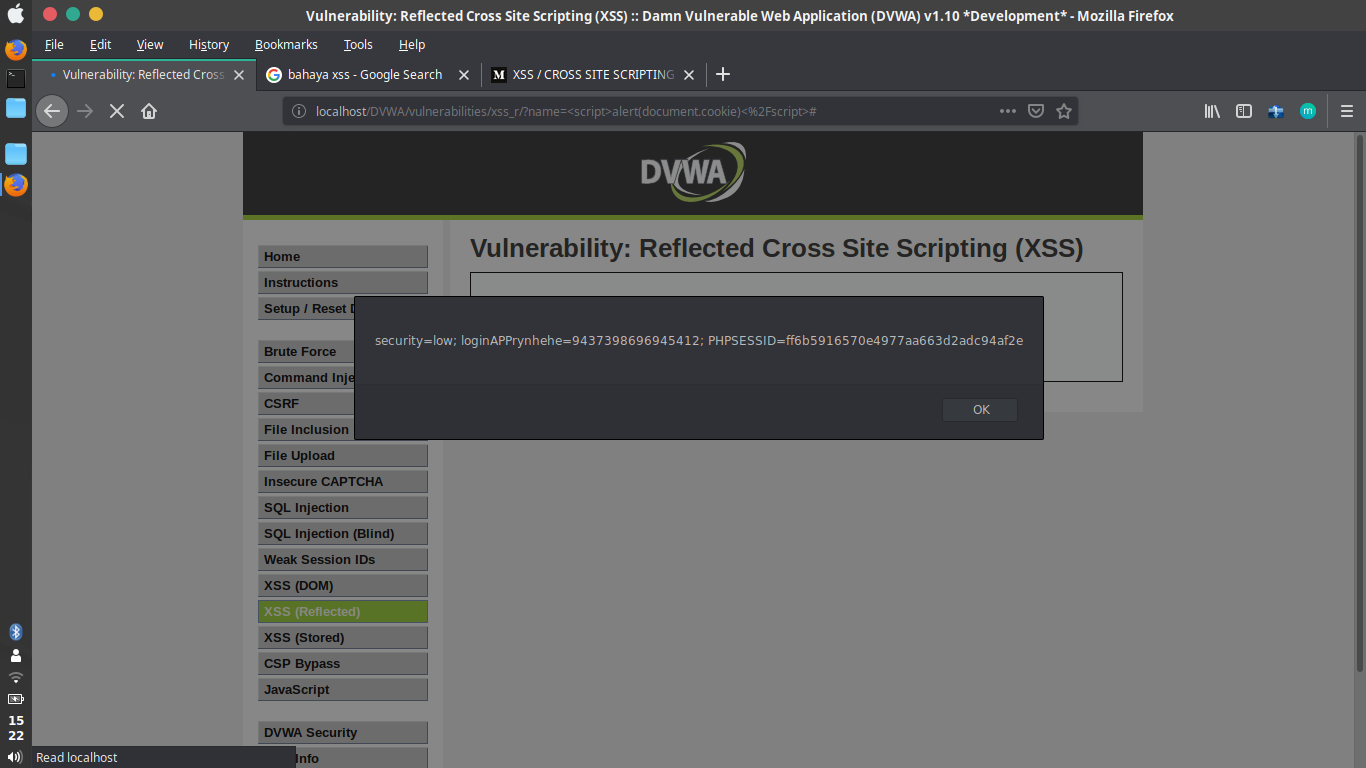
Source: <https://github.com/ethicalhack3r/DVWA>



Diatas adalah tampilan DVWA yang berhasil saya install di server local. Login dengan akun default yang disediakan, yaitu usname ‘admin’ dan password ‘password’.



Dan diatas adalah tampilan setelah login, terdapat navigator halaman website dengan berbagai celah keamanan. Lalu saya klik DVWA setting untuk mengubah tingkat keamananya menjadi low/rendah.



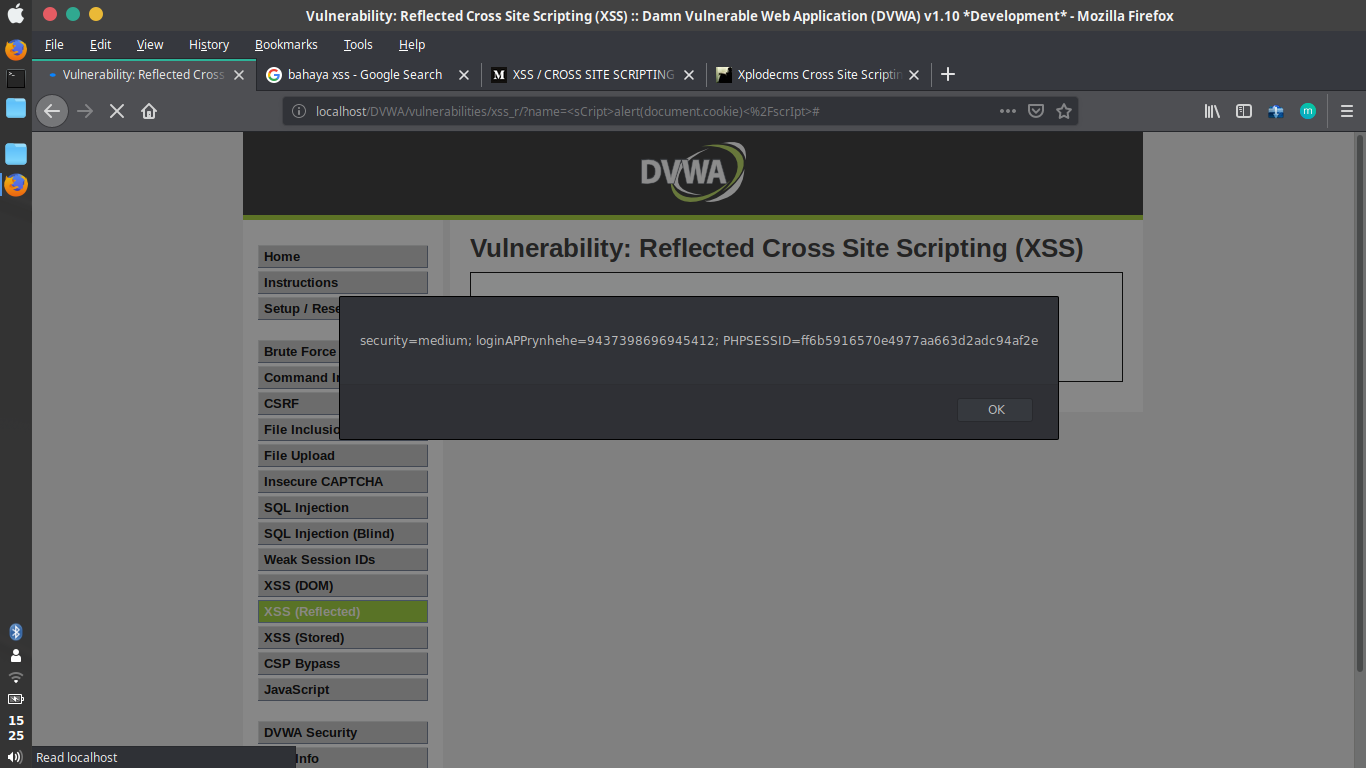
Lalu memilih halaman yang memiliki celah pada XSS reflected, halaman yang memiliki celah keamanan XSS reflected itu hanya berupa tampilan input dan inputan tadi ditampilkan lagi tanpa menyimpan ke database.

Disini pertama saya coba memasukkan tag <script> dan berhasil masuk lalu di proses oleh browser. Bahaya dari celah ini adalah kita bisa mengambil session info yang berakibat pemalsuan identitas login.

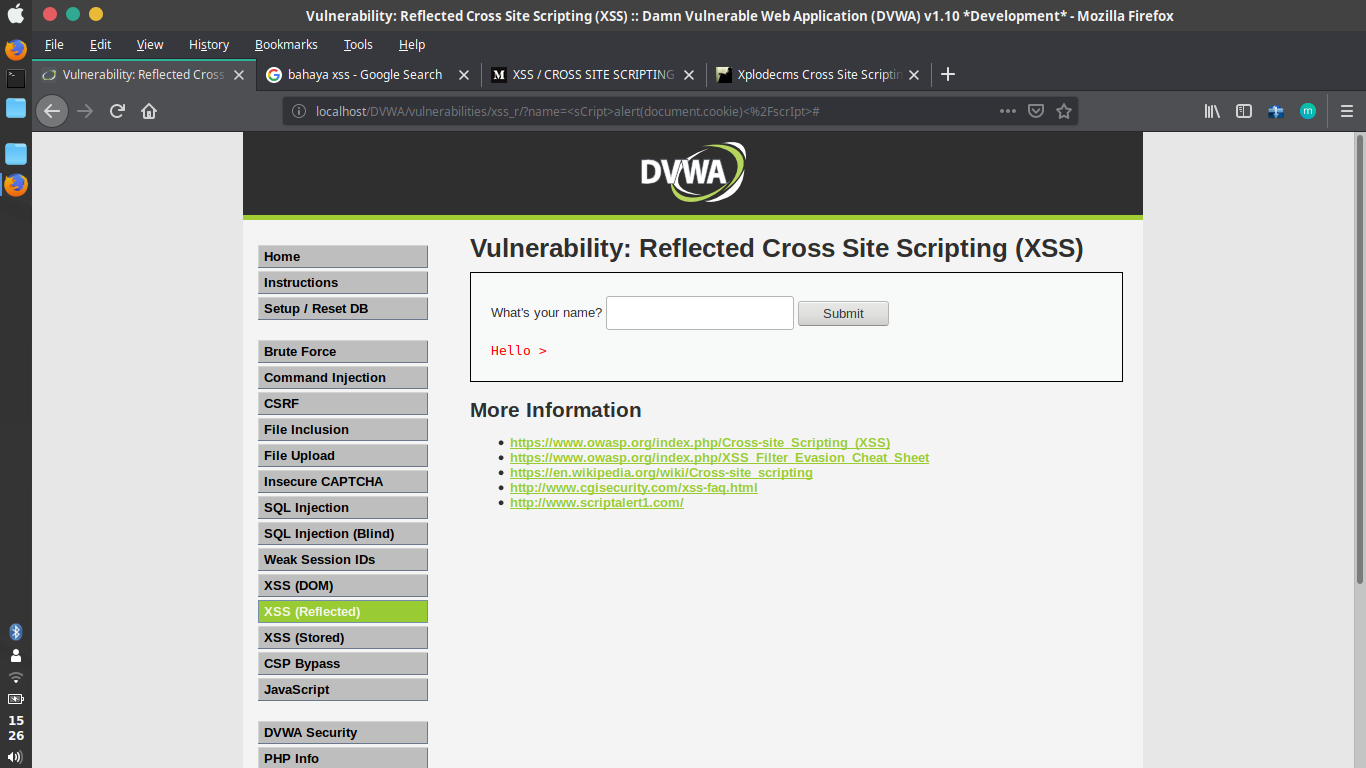


Setelah tingkat keamanan rendah berhasil di serang, saya tingkatkan ke tingkat selanjutnya yaitu tingkat menengah.

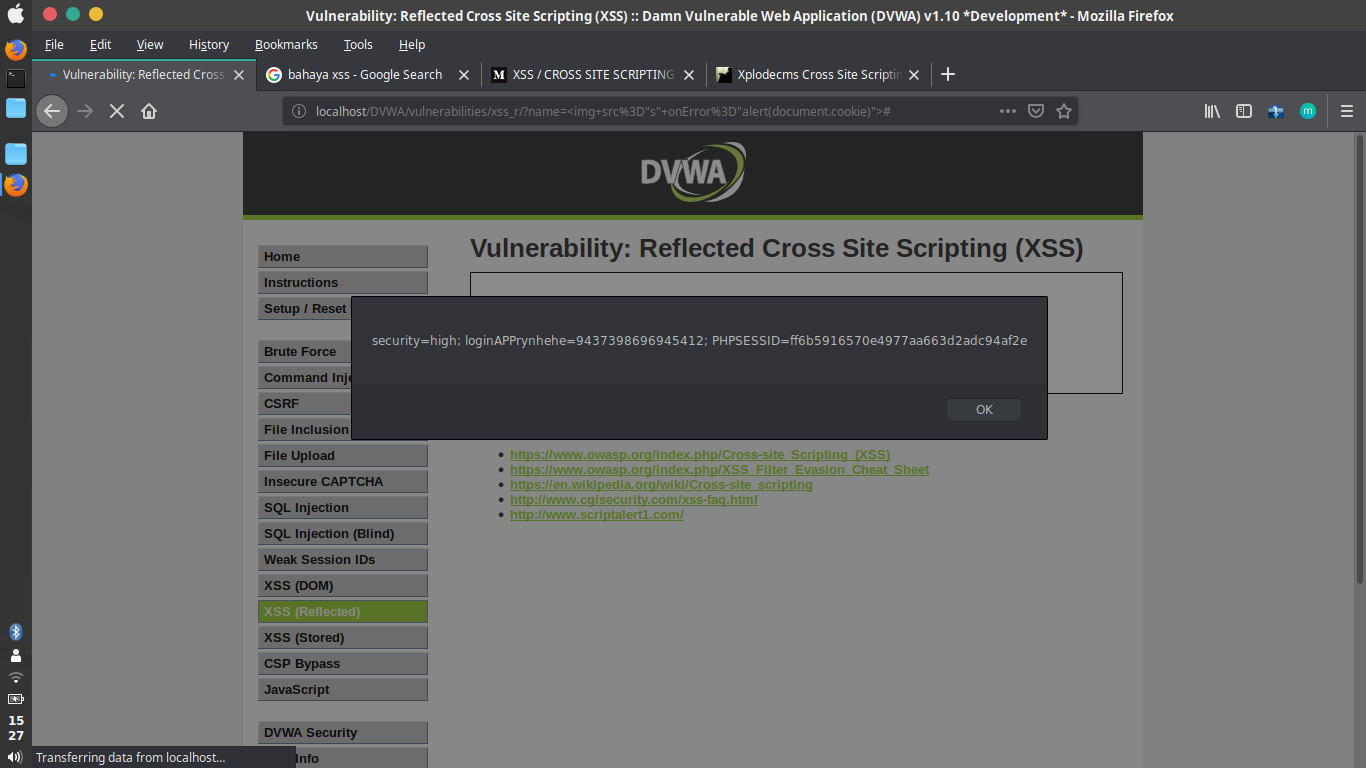
Saya coba memasukkan tag <script> seperti tadi tidak berhasil, lalu saya coba memanfaatkan salah satu fitur browser dimana ada fitur autocomplete sehingga saya coba menuliskan tag <script> dengan tulisan besar kecil yaitu <sCript> dan ditutup dengan <scrIpt> maka akan tampil seperti gambar dibawah yang artinya serangan XSS berhasil.



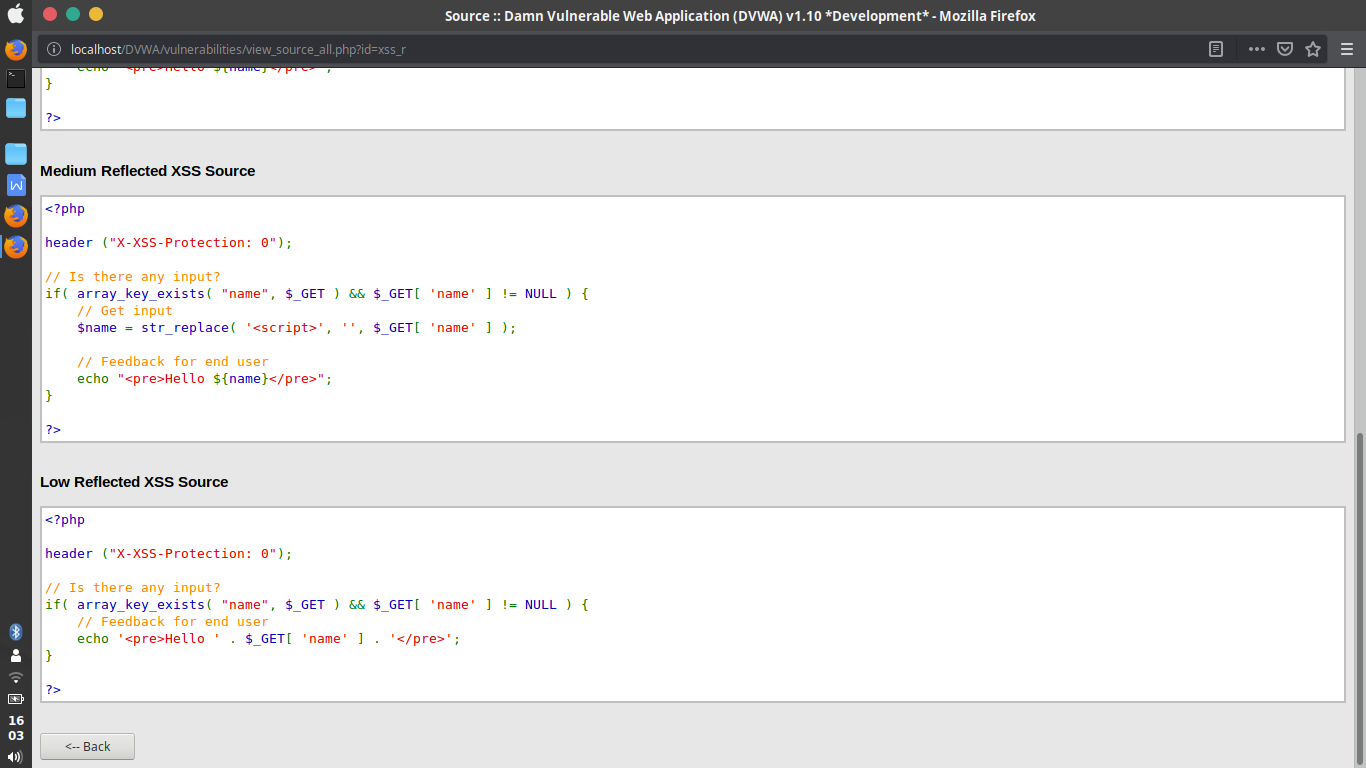
Setelah itu menaikkan tingkat keamanan ke level tinggi dan mencobanya kembali dengan mengakali besar kecil huruf ternyata sudah tidak berhasil.



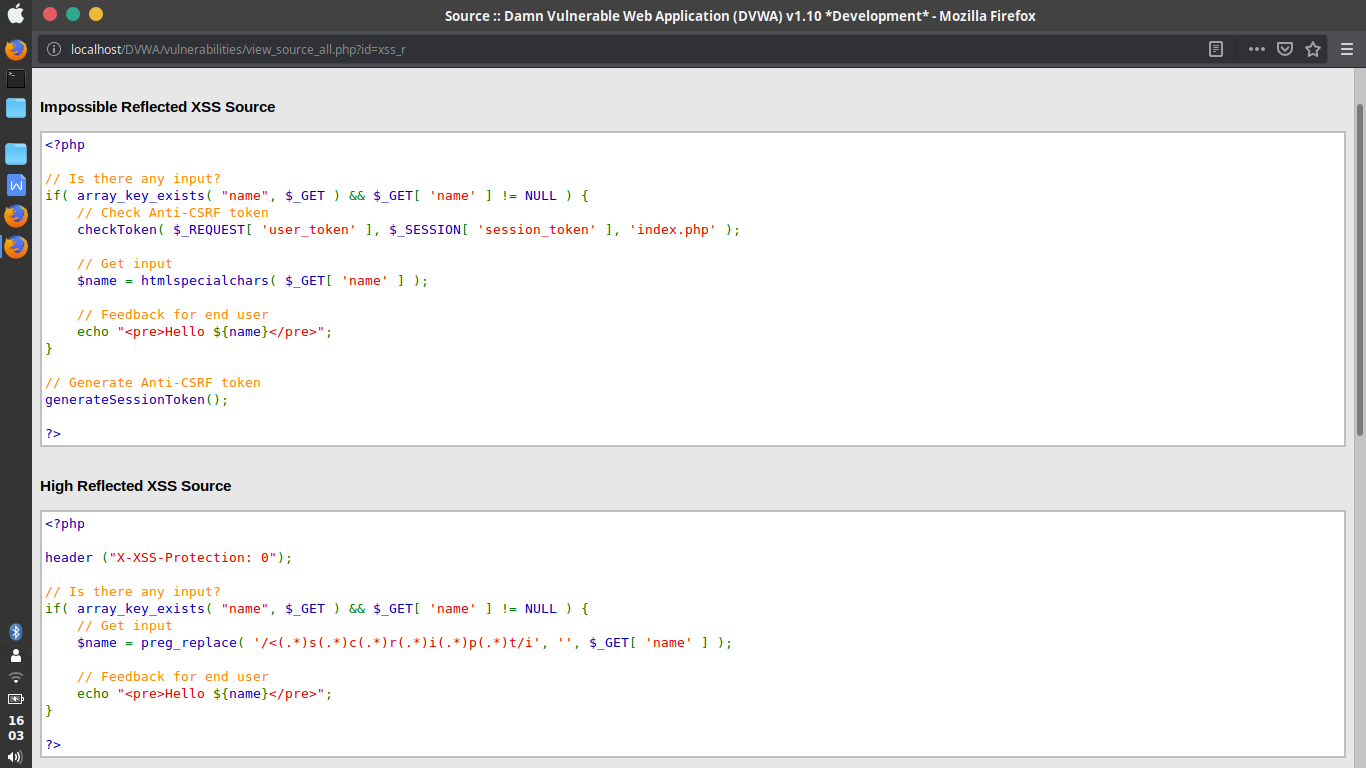
Lalu mencoba cara baru dengan memasukkan tag html lain salah satunya adalah tag <img>. dan tag tersebut berhasil masuk. Lalu pada tag tersebut diberi atribut berupa script js dan berhasil masuk dan mendapat cookie yang diinginkan. Seperti gambar di bawah.



Setelah melihat source code yang disediakan :



Untuk yang low, tidak ada baris kode untuk memfilter inputan yang diberi user sehingga apapun inputanya akan di olah begitu saja. Lalu pada medium memiliki filter berupa menghilangkan jika ada tag <script> dan masih bisa di akali dengan tag script yang diatur besar kecil seperti contoh tadi <sCript> dan </scrIpt>.



Untuk yang high, filter yang diberikan adalah menghapus karakter yang kemungkinan menjadi script javascript, namun tidak untuk tag lain dalam hal ini image(<img>) dan disitulah celahnya.

Sekian pembahasan mengenai DVWA dari celah keamanan CSS reflected. Untuk yang imposible belum dapat menemukan celah atau memang tidak ada celah. Terima kasih.