

##### 

##### 

Vulnerability analysis of web applications using Kali Linux

Punuan:

Abdullah Rexha

Drilon Shala

Muhamet Rexhepi

**1.Hyrje**

**1.1-Hyrje në Nikto-s**

Rritja e perdorimit të web-applikacioneve në internet rriti poashtu edhe nevojen e domosdoshme për sigurinë e të dhënave të cilat qarkullojnë në ato applikacione në internet.Për arsyje se ne shumë raste ne e neglizhojme sigurine ne web dhe si rezultat ne shpesh krijojme web-apps të cilat janë të prekshme(vulnerable web apps) dhe sulmuesit mund të perfitojnë(marrin) të dhenat e faqes.Në këtë seminar ne trajtojmë veglen Nikto që paraqet nje skaner të aplikacioneve ne web.Përdorimi I Nikto-s kryesishte përfshine identifikimin e çeshtjeve te sigurise ne web.Për dallim nga shumë web skanera te tjerë Nikto performone për të gjitha llojet e web-ave ,qoftë ai web I ndertuar me anë të wordpress ,Wix apo vegla të tjera me të cilat ndertohet nje Web .Pra Nikto kërkon vetëm një ip adresë ose një link ku ai do të përformojë dhe vlen për të gjitha llojet e web-eve.

**1.2-Historia e Nikto-s**

Nikto eshte „web server“ vegel që teston web-serverat për CGI/files,softverat e serverit (se a jane Update) etj.Nikto 1.00 Beta u lancua më 27 dhjetor 2001 (menjeherë pas ketijë versioni u lancua edhe Nikto 1.01).Përgjatë dy viteve të ardhshme Kodi I Niktos evuloi në njeren prej veglave më të përdorura për gjetjen e pikave te dobëta ne nje web-faqe.Versioni 2.0 u lancua ne Nëntorë të 2007.Emrin Nikto e ka marrë nga filmi „The day the earth Stood still“ .

**1.3-Përshkrimi i Nikto-s**

Ekzaminimi i nje web-serveri me qëllim të gjetjes te ndonjë problem potencial dhe pika te dobëta ne sigurine e webit ,duke përfshirë:

* Server and software misconfigurations
* Default files and programs
* Insecure files and programs
* Outdated servers and programs

Nikto është ndërtuar ne LIBWhisker2(by RFP) dhe mund te përdorët në secilen platformë(OS).Përkrahë SSL,proxies,host authentication ,attack encoding etj.Si vegel mund te përditsohet direkt nga Command-Line.

**1.4-Kërkesat**

Secili Sistem Operativ(Windows,Linux,Mac OSX) që përkrahë instalimin e Perl ,duhet qe te lejoje qe Nikto te ekzekutohet ne atë sistem operativ.Nikto eshte testuar ne:

* Windows(duke perdorur ActiveState Perl dhe Strawberry Perls),Disa nga karakteristikat e Niktos mund te mos punojne ne Windows SO
* MAC OSX
* Linux (duke perfshirë RedHat,Solaris,Debian,Ubuntu,BackTrack,etc.) në disa versione te Linux siç është Kali-Linux ,Nikto vjen e instaluar .

**2.Nikto-Intro**

Para sulmit që mund ti bëhet një web applikacioni është e rëndësishme të bëjmë një përmbldhje informatash lidhur me atë web faqe ,këto informata që do të marrim na tregojnë shumë në lidhje me web faqen të cilen ne deshirojmë ta sulmojmë ndër informatat të cilat ne I mbledhim janë :konfigurimi i serverit(çfarë konfigurimi përdorë web serverin në fjalë).Duke bërë vetëm disa konfigurime të vogla ky llojë sulmi u mundëson sulmuesve të kursejnë shumë kohën e tyre përgjatë gjetjes së konfigurimit të një web serveri ose web applikacion .

Për gjetjen e shumë informatave të një web serveri qoftë ai Real,Virtual apo localhost ne sherbehemi me veglen Nikto .

Nikto është një vegel Open Source që përdoret si web skaner ,nikto performon teste të ndryshme duke përfshirë 6700 teste për gjetjen e files/programs që paraqesin rrezik për serverin,1250 teste të ndryshme për skadimin e licenses së një softveri në server dhe lloje tjera testesh.Nikto nuk është e dizajnuar si një vegel vjedhese .Nikto skanon një web server në menyrë shumë të shpejtë dhe efficiente.

**2.1-Komandat ne Nikto**

Komandat në nikto mund të gjinden duke shkruar ne terminal Nikto –h ne Kali Linux.

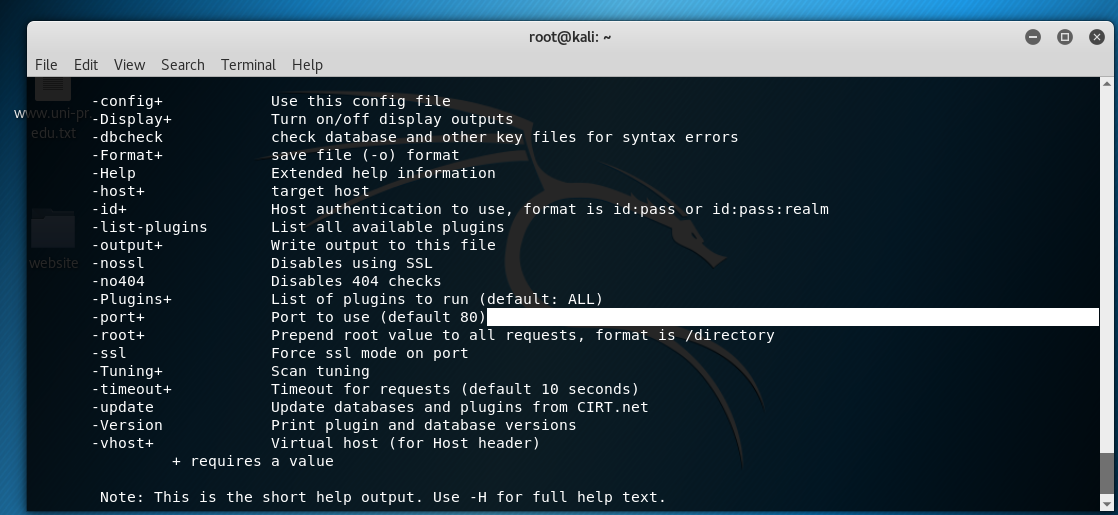
****

foto 1:Komandat e Nikto-s

* **ask**-Nëse duhet pyetur për perditsimin e dergimeve:PO(pyetë për të gjithë),Jo(mos pyetë thjeshte dërgo),auto(mos pyetë thjeshte dërgo)
* **config**-Specifiko një tjetër config file të përodoret në vend të nikto.conf që gjendet në install directory
* **Display**-Kontrollo daljen që Nikto tregon ka disa menyra të perdorimit:

1. Show redirects
2. Show cookies received
3. Show all 200/OK responses
4. Show URLs which require authentication
5. Debug Output me anë të -D
6. Display all HTTP errors me anë të -E
7. Print progress to STDOUT me anë të -P
8. Verbose Output me anë të –V

* **Dbcheck-**Shikonë në databazat e web serverit dhe fileve kyç se a kanë ndonjë error ne sintaks
* **Evasion-**Teknika të enkodimit

Random URI encoding (non-UTF8)

2 - Directory self-reference (/./)

3 - Premature URL ending

4 - Prepend long random string

5 - Fake parameter

6 - TAB as request spacer

7 - Change the case of the URL

8 - Use Windows directory separator (\)

A - Use a carriage return (0x0d) as a request spacer

B - Use binary value 0x0b as a request spacer

* **Format-**Ruaje fajllin e marrë ne forma të ndryshme ,format valide janë:

1. csv - a comma-seperated list
2. html - an HTML report
3. msf - log to Metasploit
4. txt - a text report
5. xml - an XML report

* **Help-**Paraqit ndihmen(help) ne formë të zgjeruar
* **Host-**Targeti që dëshirojmë ta skanojme qoftë ai ip adresë apo link
* **Nossl-**Mos përdore ssl për konektim në server
* **Ssl-**Përdorë ssl gjatë konetkimit në server
* **Save-**Ruaje kërkimin në direktoriumin e caktuar
* **Port-**Porti në të cilin dëshironi të skanoni
* **Scan tunninga-**Skan tuning përdoret kryesisht për uljen e numrit të testeve ,duke specifikuar formën e testit ,për shembull ,në rastet kur ne nuk dëshirojmë ta skanojmë për XSS ose ndonjë file tjeter.Për ti bërë testet e dëshiruara thjesht shtypim –T(Tuning) dhe testin që dëshirojmë ,testet përfshijnë:

0 - File Upload. Exploits which allow a file to be uploaded to the target server.

1 - Interesting File / Seen in logs. An unknown but suspicious file or attack that has been seen in web server logs (note: if you have information regarding any of these attacks, please contact CIRT, Inc.).

2 - Misconfiguration / Default File. Default files or files which have been misconfigured in some manner. This could be documentation, or a resource which should be password protected.

3 - Information Disclosure. A resource which reveals information about the target. This could be a file system path or account name.

4 - Injection (XSS/Script/HTML). Any manner of injection, including cross site scripting (XSS) or content (HTML). This does not include command injection.

5 - Remote File Retrieval - Inside Web Root. Resource allows remote users to retrieve unauthorized files from within the web server's root directory

6 - Denial of Service. Resource allows a denial of service against the target application, web server or host (note: no intentional DoS attacks are attempted).

7 - Remote File Retrieval - Server Wide. Resource allows remote users to retrieve unauthorized files from anywhere on the target.

8 - Command Execution / Remote Shell. Resource allows the user to execute a system command or spawn a remote shell.

9 - SQL Injection. Any type of attack which allows SQL to be executed against a database.

a - Authentication Bypass. Allows client to access a resource it should not be allowed to access.

b - Software Identification. Installed software or program could be positively identified.

c - Remote source inclusion. Software allows remote inclusion of source code.

x - Reverse Tuning Options. Perform exclusion of the specified tuning type instead of inclusion of the specified tuning type.

**2.2-Nikto and Tor**

Instalimi I Proxychains do të lejojë aplikacionin të ekzekutohet nëpërmjet rrjetit Tor.Përdorimi I vegles Tor do ta rrisë sado pak anonimitetin .Rasti kur ne deshirojmë qe pala që e pergjon komunikimin mes dy palëve të mos ketë mundësi ta lexojë u përdorte Enkriptimi ,mirëpo kur ne deshirojmë që pala përgjuesëve dhe pala marrëse(web server )të mos e dijë se me kë po komunikojmë atëhere përdoret Vegla apo browser Tor. Le të themi se Tor për komunikim me nods përdore enkriptimin simetrik AES ku me secilin node gjeneron një çelës të veçantë me anë të metodes Diffi-Hellman,fillimish tor e enkripton mesazhin 3 herë me 3 çelësa të mundshëm ,pas kësaj nodhë dekriptimi dhe kërkesa shkon në web ku webi nuk ka njohuri se kush ka bërë kërkesë.Secila node e dine vetem nga ka ardhur dhe nga do të shkojë.Rreziku qendron te Exit Node(Noda e fundit) sepse mesazhi aty është plaintext kshtu që nuk preferohet që me tor browser të kyçemi facebook-un.Tor përdoret për qasje ne Dark-Web

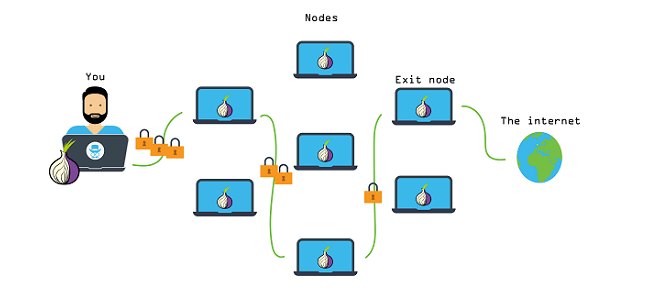


foto 2:Vegla(Browseri) Tor

Ne mund ta përdorim veglen Tor gjatë skanimit me Nikto për vulnerabilities(pika të dobëta ) dhe kjo do na mbajë anonim.Po nëse makina që ekzekuton Nikton mund ti qaset target hostit nëpërmjet http proxy-it ,testi mund të përformohet duke përdorur komande –useproxy.

**3.Testimi**

**3.1-Basic Testing**

Për të skanuar një web server me anë të Niktos thjesht duhet shkruar nikto –h(ip adresa ose linku ),pastaj ne mund të caktojmë portin në të cilin ne dëshirojmë të skanojme me anë të komandes –p [porti].Nëse nuk caktohet porti bydefault do të jetë porti 80



foto 3:Testi i pare

Për të skanuar një web server në porte të tjera perveq atijë 80 ne perdorim komanden –p[porti].Gjatë skanimit të një porti të caktuar ne mund të përdorim komande –ssl në qoftëse porti të cilen dëshirojmë ta skanojmë ka ssl ,mirëpo nuk është e nevojshme të përdoret për arsye që nikto fillimisht bënë testimin sikur të ishte http dhe nëse ky testim dështon atëhere përdore https.



foto 4:Testimi ne portin 443 te tcp

Rezultati nga testimi I portit 443 që njëkohësisht paraqet edhe portin e TCP:

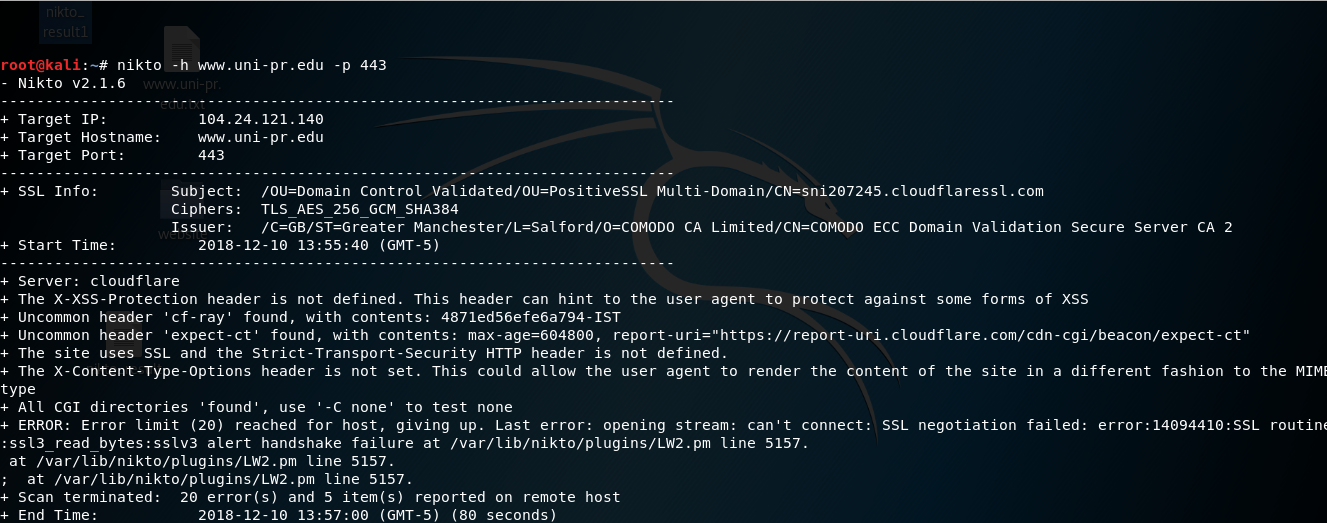


foto 5:Rezultati i skanimit te portit 443

Testimi mund të behet edhe në ndonje virtual server apo localhost në LAN ,për të skanuar në vend të linkut ne shkruajmë ip adresen si më poshtë



foto 6:Skanimi në LAN

Rezultati nga testimi I web serverit I cili gjendet në LAN

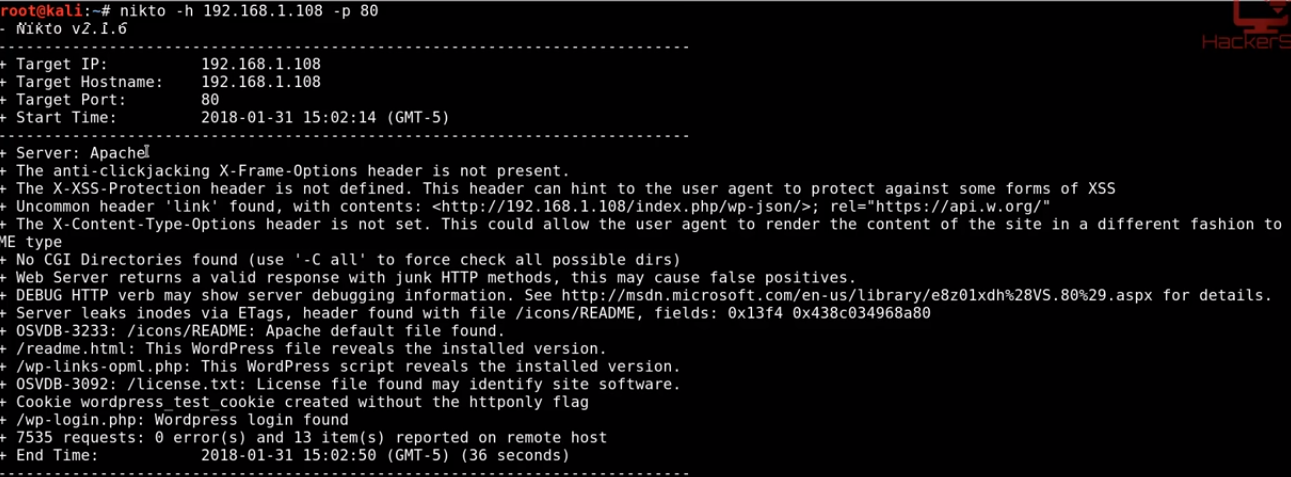


foto 7:Rezultatet e testit në LAN

**3.2-Testimi në shumë porte**

Vegla Nikto mund të skanojë më shumë se një port në një session të njëjtë të skanimit.Për të testuar më shumë se një thjesht specifiko listen e porteve të cilën dëshironi ta skanoni -p[porta0,port1...portaX]



foto 8:Testimi në më shumë se një port

**3.3.Output formatet**

**3.3.1.Formati txt**

Nikto lejon vendosjen e rezultatit të skanimit në forma të ndryshme si :CSV,HTML,XML,NBE.Kur ne perdorim komanden –output për paraqitjen e rezultatit në ndonje llojë fajlli dhe formatin ja caktojmë me anë të komandes –Format .Nëse ne nuk e përcaktojmë Nikto me anë të file extension(.txt,.html etj) provon ta qëllojë formën e saktë.



foto 9:Forma për paraqitjen e skanimit në fajll

Gjatë skanimit të një web serverit është shumë e rëndësishme të ruhen të gjitha testimet ,në rastin tonë konkret është ruajtur në një file.txt(fajll tekst) dhe pastaj me ato të dhena mund të manipulohet.Shembull konkret do të ishte një fajll CSV ku me ndonjë program që shkruajmë me python do të merrnim të dhenat e deshiruara.

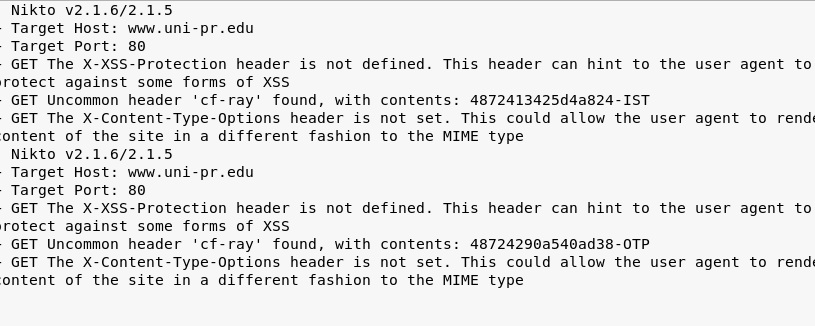


foto 10:Fajlli ku ruhet skanimi

**3.3.2.Formati Html**



foto 11:Paraqitja ne Html (1)



foto 12:Paraqitja ne Html (2)



foto 13:Paraqitja ne Html (3)



foto 14:Paraqtija ne Html (4)

Në figurat më lartë është paraqitur një skanim i Nikto-s me output formatin HTML.

Si header i këtij skanimi janë paraqitur Target IP e cila paraqet IP e hostit në të cilin është kryer skanimi,Target hostname që paraqet emrin e hostit, Target Port që paraqet Portin ne te cilin është kryer skanimi, HTTP Server që paraqet serverin e targetit i cili në këtë rast është ‘Apache/2.4.7’.

Pas headerit janë të paraqitura vulnerabilities me radhë ku si vlerë e parë është URI(Uniform Resource Identifier) që identifikon një resurs, si vlerë e dytë është ‘HTTP Method’ që tregon nëse metoda e përdorur është GET apo POST, Description paraqet përshkrimin e secilit Vulnerability të gjetur gjatë skanimit, Test Links janë linqet përkatëse të targetit, OSVDB(Open Sourced Vulnerability Database) Entries që ka qenë një databazë e pavarur dhe open-source me mbi 100.000 vulnerabilities qe ka shërbyer për të dhënë informacione mbi vulnerability security por e cila që nga viti 2016 nuk përdoret.

Në vazhdim do ti komentojmë disa prej Vulnerabilities te gjetura gjatë këtij testimi.

“The anti-clickjacking X-Frame-Options header is not present.”

Clickjacking është kur një sulmues përdor shtresa transparente apo të errëta për ta mashtruar një përdorues ne klikimin e një butoni apo linku në një faqe tjetër kur ata synojnë të klikojnë brenda faqes në të cilën gjenden, kështu sulmuesi është duke “hijcacking”(rrëmbyer) klikimet duke i dërguar në faqe tjera, prandaj edhe mungesa e anti-clickjacking headerit paraqet një vulnerability

“The X-XSS-Protection header is not defined”

Cross-site scripting i njohur edhe si XSS, është një mënyrë për të injektuar kod që kryen aksione në shfletuesin e përdoruesit në emër të faqes. Ndonjëherë kjo shihet nga përdoruesi dhe ndonjëherë mund të kryhet në prapavijë pa u vërejtur nga përdoruesi. X-XSS-Protection headeri është i dizajnuar për të mundësuar XSS filterin i cili gjendet në shfletuesit modern.

“The X-Content-Type-Options header is not set”

X-Content-Type-Options headeri përdoret për tu mbrojtur nga MIME sniffing vulnearbilities. Këto vulnerability mund të paraqiten kur një faqe lejon përdoruesit të ngarkojnë përmbajtje në faqen e tyre por përdoruesi mbulon llojin e përmbajtjes si diçka tjetër. Kjo mund të ju jap atyre mundësinë për të kryer një cross-site scripting dhe të rrezikoj faqen.

 “/config.php:PHP Config file may contain database IDs and passwords”

Prej gjetjeve më interesante gjatë këtij skanimi është gjetja e fajllit me emrin config.php në të cilin mund të jenë të ruajtur ID-të dhe fjalëkalimet e administratorëve apo përdoruesve dhe kjo paraqet një rrezik direkt për faqen ngase kushdo mund të ketë qasje në ato të dhëna.

“/phpmyadmin/: phpMyAdmin directory found”

Gjetja e direktoriumit të phpMyAdmin paraqet nje vulnerability ngase sulmuesit mund të shfrytëzojnë një cenueshmëri të tillë, duke përdorur SQL Injection për të thirrur load\_file() për të lexuar emrin e përdoruesit dhe fjalëkalimin në plain tekst në fajllin e konfigurimit dhe pastaj të hyjnë përmes phpMyAdmin ose tcp port 3306. Apo edhe mundësia për gjetjen e fjalëkalimit përmes ‘brute force’.

Në fund te HTML dokumentit të skanimit te krijuar kemi edhe të dhënat se kur ka filluar skanimi kur ka përfunduar, kohëzgjatja dhe statistikat e kërkesave gabimeve dhe gjetjeve nga skanimi.

**3.3.3.Formati XML**

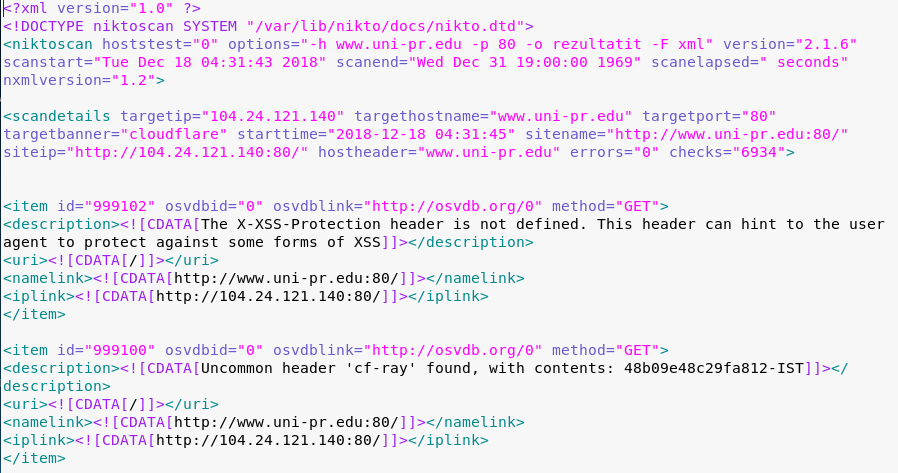
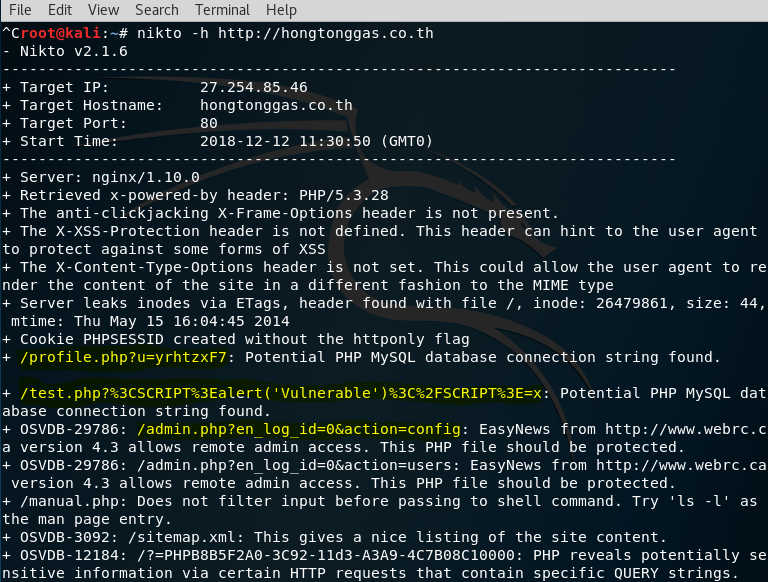
****

foto 15:Formati XML

**3.4-Gjeta e dobësive me anë të Nikto-s**



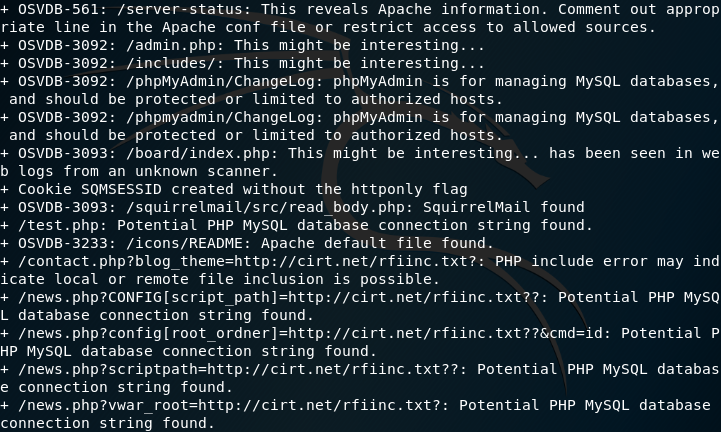


foto 10:Rezultatet e skanimit të një web serveri

Gjatë skanimit të një web serveri kemi gjetur të dhëna që kanë të bëjnë me databazën ose më saktë stringje të cilat bëjnë lidhjen e PHP me databazën në MySQL . Disa prej tyre janë theksuar me ngjyrë të verdhë në figurën më lartë(Figuën 10). Gjithashtu janë gjetur edhe dopsi të tjera siq janë: 1.OSVBD-29786 - Easynews nuk kontrollon siç duhet për të siguruar që një administrator është identifikuar me emrin e saktë të përdoruesit dhe fjalëkalimin, vetëm kontrollon nëse id me të bëhet kyqja është id e adminit, $ admin [$ en\_login\_id] == "true" .

2. OSVDB-3092 - Vulnerability lejon sulmuesit të shkruajnë kudo në sistemin e skedarëve.

3. OSVBD-561 -   
Apache Web Server përmban një të metë që mund të çojë në një zbulim të paautorizuar të informacionit. Çështja nxitet kur një sulmues kërkon një direktivë të statusit të serverit nga një paisje e largët, e cila do të zbulojë një shumëllojshmëri të gjerë të informacionit të web serverit duke përfshirë trafikun në internet, ngarkesën e CPU, versionin e serverit, lidhjet aktuale dhe të tjera.

Etj.



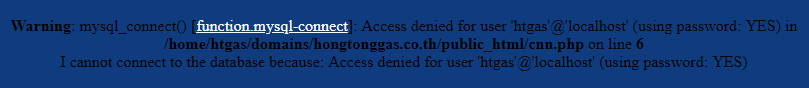


foto 16:Testimi në web browser dhe warning i cili paraqitet

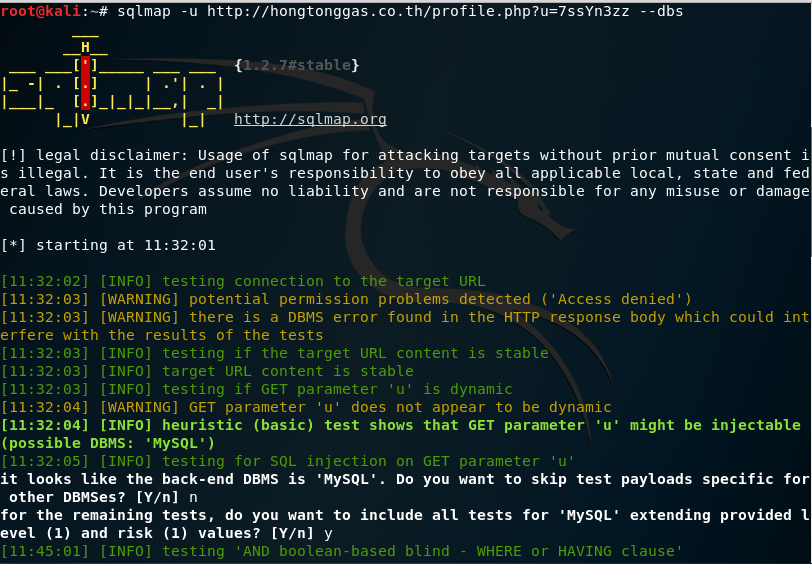


foto 17:Testimi në sqlmap i njërit prej stringjeve që kanë të bejnë me databazën

Duke përdorur të dhënat e gjetura përmes veglës Nikto kemi bërë një kërkim me Sqlmap për të gjetur më shumë të dhëna që kanë të bëjnë me databazën.

**4.Konkluzioni**

Nikto është vegel që përdoret për web skanimin ,për dallim nga veglat tjera si WPscan që perdoret vëtëm për skanim të wordpress serverave apo vegla tjera që janë specifike vetëm për server të caktuar Nikto përdoret për krejt llojet e web servereve.

**Referencat**

Nikto v2.1.5-The Manual

Computerphile Kanali në YouTube

NullByte –Faqja e NullByte