# Leeruitkomst 1: Ethical Hacker

Luc van den Acker

Cyber Security semester 4

Contents

[Leeruitkomst 1: Ethical Hacker 1](#_Toc124947841)

[Path Traversal, (remote) File inclusion and Command Injection 2](#_Toc124947842)

[Wat is Path Traversal en hoe werkt het? 2](#_Toc124947843)

[Wat is (Remote) File Inclusion en hoe werkt het? 3](#_Toc124947844)

[Wat is Command Injection en hoe werkt het? 4](#_Toc124947845)

[SQL Injection 5](#_Toc124947846)

[Cross-Site Scripting(XSS) 7](#_Toc124947847)

[Cross-Site Request Forgery(CSRF) 7](#_Toc124947848)

[Sniffing 8](#_Toc124947849)

[Spoofing 9](#_Toc124947850)

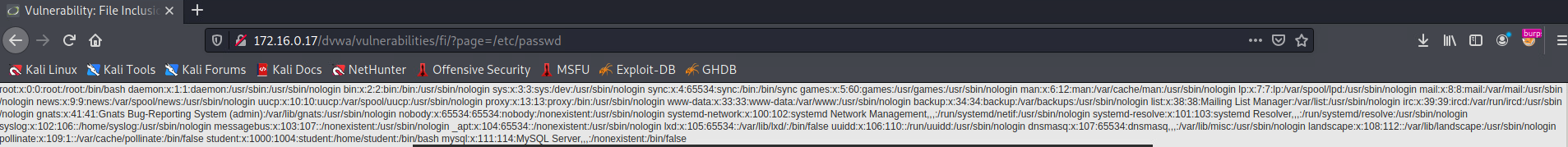
[Wireless Hacking 10](#_Toc124947852)

## Path Traversal, (remote) File inclusion and Command Injection

### Wat is Path Traversal en hoe werkt het?

Het doel van een Path Traversal Attack is om toegang te krijgen tot bestanden of directories buiten de web root folder. Door variabelen te manipuleren in file references(bijvoorbeeld “../” toevoegen) is het mogelijk om toegang te krijgen tot bestanden die niet toegankelijk horen te zijn. Wanneer een webapplicatie goed is beveiligd, wordt een Path Traversal Attack natuurlijk lastiger. Met een Path Traversal Attack is het dus mogelijk om toegang te krijgen tot gevoelige bestanden, directories of zelfs source code.

DVWA Path Traversal

Onder het kopje File Inclusion is het mogelijk misbruik te maken van Path Traversal. Wanneer een bestand aangeklikt wordt, verwijst de app naar een nieuwe pagina. De URL van deze pagina is: 172.16.0.17/dvwa/vulnerabilities/fi/?page=file3.php. Door deze URL aan te passen tot 172.16.0.17/dvwa/vulnerabilities/fi/?page=/etc/passwd, wordt data weergegeven die de gebruiker niet hoort te zien(onderstaand screenshot). Gelukkig zijn de wachtwoorden niet zichtbaar, maar de usernames van alle gebruikers zijn wel zichtbaar. Voor een brute force attack is een aanvaller dus al halverwege.

Wanneer het Security Level naar “high” wordt gezet, werkt de bovenstaande URL niet meer. Door misbruik te maken van Uniform Resource Identifiers(URI) is het echter alsnog mogelijk om toegang te krijgen. Een URI is een unieke benaming voor een stuk data. In dit geval is het mogelijk gebruik te maken van de “file” URI. De URL ziet er dan als volgt uit: 172.16.0.17/dvwa/vulnerabilities/fi/?page=file:///etc/passwd.

A screenshot of a computer

Description automatically generated with medium confidenceDoor de URL aan te passen naar 72.16.0.17/dvwa/vulnerabilities/fi/?page=/proc/version is het ook mogelijk om meer informatie te vinden over het Operating System van de slachtoffer(onderstaand screenshot).

### Wat is (Remote) File Inclusion en hoe werkt het?

Een File Inclusion kwetsbaarheid geeft een aanvaller de mogelijkheid om een bestand te uploaden naar de server van een website. Meestal wordt hierbij misbruik gemaakt van “dynamic file inclusion” functionaliteiten. Meestal staat er een script in het bestand, wat uitgevoerd wordt op de server. Andere gevolgen kunnen zijn:

* Code execution op de client kant, bijvoorbeeld cross site scripting(XSS).
* Denial of Service (DoS)
* Gevoelige informatie wordt gelekt.

DVWA Remote File Inclusion

Graphical user interface, application

Description automatically generatedHet doel van deze opdracht is het gebruiken van een bestand dat gehost wordt op de machine van de aanvaller. In dit geval is het doel om Google te hosten via de DVWA. Door De URL aan te passen van 172.16.0.17/dvwa/vulnerabilities/fi/?page=include.php naar 172.16.0.17/dvwa/vulnerabilities/fi/?page=http://google.com wordt google weergegeven in de pagina van de DVWA. Zoals in het screenshot hiernaast te zien is, staat de bekende zoekbalk van google bovenaan de pagina weergegeven.

Als de Security Level verhoogd wordt naar “medium” is het niet meer mogelijk om slechts <http://google.com> aan de URL toe te voegen. De website vervangt “http” nu met “https”. Echter wordt enkel exact “http” vervangen door “https”. Het filter herkent bijvoorbeeld “Http” niet meer door de hoofdletter, dus door dit in de URL te zetten in plaats van “http” is google.com nog steeds beschikbaar. De enige aanpassing die gemaakt hoeft te worden is de “h” in “http” vervanger met een hoofdletter, waardoor de URL er als volgt uitziet: 72.16.0.17/dvwa/vulnerabilities/fi/?page=Http://google.com. Het resultaat blijft hetzelfde als in het bovenstaande screenshot.

Om (Remote) File Inclusion tegen te gaan, wordt gebruik gemaakt van validatieprotocollen. Wanneer alle bestanden blind worden geaccepteerd, is het natuurlijk heel simpel om malafide software te uploaden. Daarom is het verstandig om alle bestanden te valideren voordat ze naar de server geüpload worden. Wanneer een gebruiker bijvoorbeeld online een CV moet kunnen uploaden, is het aan te raden om alleen word/PDF bestanden te accepteren.

### Wat is Command Injection en hoe werkt het?

Command Injection, ook wel Shell Injection genoemd, is een kwetsbaarheid in een web applicatie, waardoor een aanvaller OS commands kan uitvoeren op de server waar de applicatie op draait. Door een command uit te voeren op de server kan een aanvaller delen van de infrastructuur van de host om zeep helpen.

DVWA Command Injection

Text

Description automatically generatedTijdens deze opdracht wordt geprobeerd om gegevens op te halen door middel van command injection. Waar de DVWA een IP-adres verwacht, wordt er geen validatie uitgevoerd voor de input, waardoor alle karakters ingevoerd kunnen worden. Door eerst een cijfer(1) in te voeren, met daarna een commando, wordt het systeem om de tuin geleid en wordt het meegegeven commando uitgevoerd. Wanneer 1;cat /etc/passwd in wordt gevoerd, gaat het systeem een cat-commando uitgevoerd, en wordt alle data uit de passwd folder weergegeven, zoals in het screenshot hiernaast te zien is.

Als de Security Level verhoogd wordt naar “medium”, worden tekens als “;” of “&&” gefilterd door de DVWA. Het commando hierboven zal dus niet meer werken. In de DVWA is dus een filter toegevoegd, waardoor bepaalde character arrays gefilterd worden. Het nadeel hieraan is echter dat een computer dit letterlijk leest, en alleen de bovenstaande teksten filtert. “&&” is dus geen mogelijkheid, maar “&” is nog prima te gebruiken. Om hetzelfde resultaat te krijgen als in het screenshot hierboven, moet de “;” in het bovenstaande commando vervangen worden door een teken dat niet gefilterd wordt, maar er wel voor zorgt dat de DVWA de weg kwijt is. Het commando komt er dan als volgt uit te zien: 1&cat /etc/passwd. In dit commando wordt de “;” dus vervangen door “&”. Omdat dit niet meegenomen wordt in het filter, kan het commando alsnog uitgevoerd worden.

## SQL Injection

SQL Injection is een kwetsbaarheid waarbij gebruik wordt gemaakt van SQL-statements. Met deze SQL-statements wordt geprobeerd data opgehaald, opgeslagen, gewijzigd of verwijderd. Indien deze statements niet of niet voldoende gecontroleerd worden, kan er misbruik van gemaakt worden, zoals in het voorbeeld hieronder te zien is.

DVWA SQL Injection

De DVWA biedt een pagina aan waarop een gebruiker een ID in kan voeren, en vervolgens de volledige naam van de bijbehorende gebruiker krijgt, inclusief het bijbehorende ID. De DVWA gebruikt de volgende query om tot dit resultaat te komen: SELECT first\_name, last\_name FROM users WHERE user\_id = ‘$id’;. Vervolgens wordt gekeken of de applicatie kwetsbaar is voor SQL Injection. Door in het invoerveld 3’ OR ‘1’ = ‘1 in te voeren, is het mogelijk om alle gebruikers op te halen, wat betekent dat de applicatie inderdaad kwetsbaar is voor SQL Injection. Vervolgens wordt gekeken of het mogelijk is om erachter te komen welke tabellen bestaan in de database, met behulp van de volgende query:

A picture containing text

Description automatically generated3' UNION SELECT table\_schema,table\_name FROM information\_Schema.tables;#. De “UNION SELECT” in deze query geeft aan dat de gegevens uit twee of meerdere “SELECT” commando’s samengevoegd moeten worden. “table\_schema” geeft aan waar een tabel staat, en “table\_name” geeft de naam van de tabel aan. Deze gegevens worden opgevraagd uit “information\_Schema.tables”. Deze bevat informatie over alle tabellen in de database. Door aan het einde “#” toe te voegen, wordt aangegeven dat er na deze query niks meer uitgevoerd moet worden. Wanneer dit allemaal uitgevoerd wordt, worden de namen en locaties van alle tabellen in de database opgehaald, zoals in het screenshot hierboven te zien is. De locatie van de tabellen staat bij “First name” en de naam van de tabellen staat bij “Surname”.

Text

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedDoor de Security Level op te krikken naar “medium” is het niet meer mogelijk om simpelweg een SQL-query in te voeren in een tekstbalk, aangezien deze vervangen is door een drop-down. De query zal dus via Burpsuite aangepast moeten worden. Vanuit daar wordt de POST-request onderschept. Op regel 15(zie screenshot hiernaast) is te zien welke parameters meegegeven worden in de query. Door daaraan OR 1=1 toe te voegen, wat altijd waar is, geeft de server alle gebruikers terug. Leuk, maar waarom werkt de OR 1=1 nu wel? Omdat er geen tekstveld is waarop de gebruiker dit soort parameters mee kan geven, lijkt het erop dat de developers er vanuit gaan dat het risico afgedekt is. In het screenshot hiernaast is te zien dat dit echter niet het geval is. Aangezien alleen de security op de web applicatie gewijzigd is, veranderen de risico’s niet. Via Burpsuite zijn alle trucjes van de “low” security nog steeds mogelijk, alleen de plek waar de parameters aangepast worden zijn anders.

## Cross-Site Scripting(XSS)

XSS is een aanvalstype waarbij malafide scripts geïnjecteerd worden in websites die normaal gesproken betrouwbaar horen te zijn. Het script wordt dan bijvoorbeeld op de server van de website geüpload, waardoor het betrouwbaar lijkt te zijn. De browser van een andere gebruiker heeft dus geen idee dat het script niet betrouwbaar is, waardoor toegang tot cookies, sessies of andere gevoelige data verstrekt wordt. Hierdoor is een andere eindgebruiker vaak het slachtoffer van dit soort aanvallen. Het effect van zo’n XSS aanval kan variëren van een licht risico tot een serieus risico, afhankelijk van de gevoeligheid van de betreffende data en de security van de website.

DVWA Cross-Site Scripting

Text

Description automatically generatedHet doel van deze opdracht om een script te uploaden naar de server van de DVWA, om vervolgens dit script uit te laten voeren bij de eindgebruiker. Met dit script wordt de Security Level van de DVWA verhoogd naar “impossible”. De Security Level wordt in een cookie opgeslagen, waardoor het toevoegen van een cookie voldoet om de Security Level te verhogen. Omdat het invoerveld voor Messages een maximale lengte van 50 karakters heeft, moet dit eerst verhoogd worden via de “inspector”(zie screenshot hierboven, maxLenght geeft aan hoeveel karakters er ingevoerd mogen worden). Vervolgens is de maximale lengte groot genoeg om het volgende script in te voeren:

<script>document.cookies = “security=impossible”</script>. Zoals in het screenshot hiernaast te zien is, wordt de Security Level na het uitvoeren van het script automatisch op “impossible” gezet.

## Cross-Site Request Forgery(CSRF)

Via CSRF wordt een eindgebruiker met behulp van Social Engineering gedwongen om ongewenste acties uit te voeren op een geauthentiseerde webapplicatie. Social Engineering is een vorm van hacken waarbij de aanvaller zich richt op de zwakste schakel van het systeem, namelijk de mens. Door bijvoorbeeld een link via een email of chatbericht te versturen, misleidt een aanvaller de eindgebruiker om misbruik te maken van normaal gesproken beveiligde data/functionaliteiten. Wanneer de eindgebruiken een normale gebruiker is, kan een succesvolle aanval leiden tot een hoop zorgen bij de eindgebruiker. Een voorbeeld van een CSRF-aanval is bijvoorbeeld een SMS-bericht/email van de ING, waarin aangegeven staat dat de gebruiker via de link in het bericht zijn wachtwoord moet wijzigen. Wanneer de gebruiker op deze link klikt, krijgt de aanvaller toegang tot de bankgegevens van de gebruiker, wat natuurlijk enorme gevolgen kan hebben. Wanneer het slachtoffer een administratief account heeft, kan de schade nog veel groter zijn, en kan bijvoorbeeld een hele webapplicatie gesloopt worden.

## Sniffing

Met network sniffing wordt het afluisteren van internetverkeer op een netwerk of netwerksegment bedoeld. Wanneer iemand binnen een netwerk aan het internetten is, kan dat afgeluisterd worden. In principe is al het verkeer binnen een geselecteerd netwerk af te luisteren. Wanneer het internetverkeer echter versleuteld is, zoals bij een HTTPS-verbinding altijd het geval is, zal deze data niet te lezen zijn. In dat geval zijn er enkel rare tekentjes te zien, waar een mens niks zinnigs uit kan halen. Wanneer het verkeer echter niet versleuteld is, kan iedereen dit eenvoudig uitlezen. Hieronder staat een klein voorbeeld van sniffing in Wireshark.

Wireshark is een heel nuttige tool om dit verkeer uit te lezen. Hieronder is een screenshot te zien van een HTTP-pakket. Hierin is de HTTP-data weergeven. Hierin is in plaintext uit te lezen wat er precies uitegvoerd wordt op het internet. Wanneer we een beveiligde verbinding pakken, zoals HTTPS, of bijvoorbeeld ook TCP, UDP of DHCP, zien we dit niet. Er is nog steeds te zien wat het source-IP en destination IP is. Echter is er niet uit te lezen wat er precies gezegd wordt. Aangezien nagenoeg al het verkeer tegenwoordig versleuteld is, zal sniffing steeds lastiger worden.

Text

Description automatically generated

## Spoofing

Bij spoofing hebben we het over het vervalsen van de identiteit van een computer. Door bijvoorbeeld de ING te imiteren, is het mogelijk enorm veel schade aan te richten. In dat geval communiceert een gebruiker met de malafide host, die vervolgens communiceert met de ING. Zo lijkt het alsof een gebruiker met de ING communiceert, maar stiekem zit er iemand tussenin die alle data kan onderscheppen en aanpassen.

Een andere vorm van spoofing is E-mail spoofing. Hierbij wordt dus een mail verstuurd vanaf een malafide mailadres, maar het lijkt alsof het vanaf een ander adres afkomstig is. In de screenshots hieronder is een E-mail te zien die afkomstig lijkt te zijn van ene Rudy Bouland. Op het eerste aanzicht lijkt de mail legitiem. De mail is echter alles behalve legitiem. Deze mail is verstuurd via een service(<https://emkei.cz>) waarbij gebruikers zelf kunnen kiezen vanaf welk mailadres de mail lijkt te komen. Echter wordt het verstuurd vanaf een mailadres van deze service, wat niet zichtbaar is op het eerste opzicht.

Graphical user interface, application

Description automatically generated

## Graphical user interface, text, application, email Description automatically generated

## Wireless Hacking

Als we spreken over wireless hacking, gaat het over het hacken van draadloze verbindingen, zoals wifi of bluetooth. Hieronder staat beschreven hoe een wifi netwerk dat gebruik maakt van WPA2 te hacken is met behulp van een “deauth” aanval en aircrack-ng.

1. Sluit een wifi-adapter aan en zet deze in monitor mode. Om deze adapter in monitor mode te krijgen moeten een aantal commando’s uitgevoerd worden.
   1. Allereerst is het belangrijk om airmon-ng check kill uit te voeren. Met dit commando worden alle netwerkmanagers uitgeschakeld. Hierdoor krijgt airmon-ng vrij spel.
   2. Nu alle netwerkmanagers uitgeschakeld zijn, is het tijd om de netwerkadapter in monitor mode te zetten, door middel van het volgende commando: airmon-ng start wlan0. Wlan0 is hierin dus de naam van de adapter interface. De adapter staat nu in monitor mode. Om te controleren of de adapter daadwerkelijk in monitor mode staat, wordt het volgende commando uitgevoerd: iwconfig.Graphical user interface, text

      Description automatically generated
2. Start airodump-ng om een handshake op te vangen. Met airodump-ng is het mogelijk om al het verkeer over een netwerk af te lezen en op te slaan in een lokaal bestand. Wanneer een device verbinding wil maken met het netwerk, wordt het wachtwoord dus vanaf dit device naar de access point verstuurd. Het wachtwoord wordt dus ook gelezen en in een file gedumpt.
   1. Om het netwerkverkeer af te lezen, moeten we natuurlijk wel een target kiezen. Door airmon-ng wlan0mon uit te voeren, wordt een lijst weergegeven met alle gevonden netwerken in de buurt. Hieruit wordt het target gekozen, en wordt het bijbehorende MAC-adres en channel genoteerd.
   2. Nu er een target gekozen is, in dit geval het netwerk behorende bij MAC-adres 2E:5F:FD:BF:E2:79(LucsNetwerk), kan het echte werk beginnen. Al het verkeer dat op dit access point voorbij komt dient afgelezen te worden, aangezien de volgende stap ervoor gaat zorgen dat er een handshake plaats gaat vinden. Met het volgende commando kan het verkeer afgelezen en opgeslagen worden: airodump-ng -c 1 --bssid 2E:5F:FD:BF:E2:79-w test wlan0mon. Hierin staat [-c 1] voor het gebruikte wifi kanaal, [-w test] is het bestand waar het verkeer in opgeslagen wordt. BSSID is het MAC-adres van het access point en wlan0mon is nog steeds de interface van de wifiadapter.

Text

Description automatically generated

1. Gebruik aireplay-ng om een deauth-aanval uit te voeren. Een deauth-aanval is het verstoren van de verbinding tussen een device en de access point. Omdat deze verbinding verstoord wordt, moet dit device opnieuw verbinden met het access point, en wordt de handshake dus opnieuw uitgevoerd. Aircrack kan hierdoor het wachtwoord afvangen.
   1. Met het volgende commando wordt een deauth-aanval gestart, en dus de verbinding tussen een voorheen verbonden apparaat en de access point verbroken: aireplay-ng -0 0 -a 2E:5F:FD:BF:E2:79 wlan0mon. hierin staat [-0] voor deauthentication, oftewel een deauth-aanval. [0] staat voor het aantal deauths dat verstuurd moet worden. In dit geval wordt 0 ingevoerd, wat inhoudt dat er deauths verstuurd blijven worden, tot het commando handmatig gestopt wordt. [-a 2E:5F:FD:BF:E2:79] staat voor het MAC-adres van het access point. Het is mogelijk om het MAC-adres van de client toe te voegen aan dit commando, door achter het MAC-adres van de access point [-c {MAC}] toe te voegen. Aangezien er geen MAC-adressen van clients bekend zijn, doen we dat in dit geval niet.

Text

Description automatically generated

1. Gebruik aircrack-ng om het wachtwoord te kraken. Aircrack-ng maakt gebruik van een password.lst-bestand, met daarin een hele verzameling van de meest voorkomende wachtwoorden. De hashes van deze wachtwoorden worden vergeleken met de hash van het onderschepte wachtwoord. Is er een match? Dan is het wachtwoord gekraakt.
   1. Indien de handshake opgevangen is met behulp van de deauth-aanval, kunnen we gaan proberen om het wachtwoord van het wifi netwerk te achterhalen. Hiervoor wordt het volgende commando gebruikt: aircrack-ng -w password.lst -b 2E:5F:FD:BF:E2:79 test\*.cap. [password.lst] staat hierin voor de dictionary file met daarin een lijst van veel voorkomende wachtwoorden. [test\*.cap] betekent dat de password.lst vergeleken moet worden met de alle data in alle bestanden die beginnen met test.

Calendar

Description automatically generated