AWAF v15.1
ãĆżãČČãČĹãĆćãČČãČŮãĆňãĆďãČĽ

Nov 02, 2021

çŻőæňą:

æIJĂçţĆæŻťæŰřæŮě: 2021åźť4æIJĹ23æŮě

CHAPTER 1

ãĄŕãĄŸãĆĄãĄń

ãĄŞãĄőãČŽãČijãĆÿãĄğãĄŕãĂĄãĄŞãĆŇãĆĽãĄőãĆłãČŢãĆčãĆůãČčãČńãĄłãČĽãĆ■ãČěãČąãČşãČĹãĄőèčIJèűşãĄĺãĄłãĆŃèşĞæŰŹã
F5ãĄőãĆłãČŢãĆčãĆůãČčãČńãĄłãČĽãĆ■ãČěãČąãČşãČĹãĄŕãĄŞãĄąãĆĽãĄńãĄŤãĄŰãĄĎãĄ¿ãĄŹãĂĆ

- AskF5: https://support.f5.com/csp/home
- F5 Cloud Docs: https://clouddocs.f5.com/
- F5 DevCentralïijĹãĆşãČ§ãČěãČŃãČĘãĆčïijĽ: https://devcentral.f5.com/

CHAPTER 2

ãĆşãČşãČĘãČşãČĎ

ãĄŞãĄąãĆĽãĄőãČŽãČijãĆÿãĄğãĄŕãĂĄäžëäÿŃãĄőåĘĚåőźãĆŠãĄŤçťźäžŃãĄŮãĄęãĄŁãĆŁãĄ¿ãĄŹãĂĆ

- æIJňãĆżãČČãČĹãĆćãČČãČŮãĆňãĆd'ãČL'ãĄńãĄęãĂĄF5 Advanced WAFïijĹäžëäÿŃãĂĄAWAFïijL'ãĄőãČİãČłãĆůãČijãĄőèĺ■å
- AWAFãĄŕãĂĄWebãĆćãČŮãČłãĆśãČijãĆůãČğãČşãČŢãĆąãĆd'ãĆćãĆęãĆl'ãČijãČńãĄğãĄŹãĂĆ
- AWAF ãĄńãĆĹãĄčãĄęãĂĄWeb ãĆćãČŮãČłãĆśãČijãĆůãČğãČşçL'źæIJL'ãĄőæŤżæŠČãĄńåŕ¿ãĄŹãĆŃéŸšå¿ąãĄŇåŔŕèČ¡ãĄĺãĄ
- Botåŕ¿ç■Űæl'§èČ¡ãĂĄL7ãČňãČŹãČńãĄőDoSæŤżæŠČãĄńåŕ¿ãĄŹãĆŃéŸšå¿ąæl'§èČ¡ãĆĆåĚijãĄ■åĆŹãĄĹãĄęãĄĎãĄ¿ãĄŹãĂĆ
- æIJňãĆňãĆd'ãČL'ãĄğãĄŕãĂĄAWAFãĆŠãĄŤèşijåĚěãĄĎãĄ§ãĄäãĄĎãĄęãĄŹãĄŘãĄńWAFãĆŠåřŐåĚěéäĆãĄŚãĆŃãĆĹãĄĘãĄ
- æIJňãĆňãĆd'ãČL'ãĄğãĄŕãĂĄF5 JapanãĄńãĄŁãĄŚãĆŃãČŔãČşãĆžãĆłãČşãČĹãČňãČijãČŃãČşãĆřãĄőãĆşãČijãĆźãĄğãĆĆåĹl'

2.1 AWAFèĺ■åőŽåĹiçťŽçůĺ

æIJňçńäãĄğãĄŕãĂĄå§žæIJňçŽĎãĄŁAWAFãĄőèĺ■åőŽåĘĚåőźãĄńãĄd'ãĄĎãĄęãĄŤçť'źäžŃèĞť'ãĄŮãĄ¿ãĄŹãĂĆ

2.1.1 AWAFãĄĺãĄŕ

F5 Advanced WAFïijĹçŢěãĄŮãĄęAWAFïijL'ãĄĺãĄŕãĂĄOWASP TOP10ãĄőæŤżæŠČãĂĄãĆęãĆğãČŰãĆćãČŮãČłãĆśãČijãĆůãČğãČş

AWAFãĄğãĄĆãĆŃãĄŕãĂĄãĆźãĆ£ãČşãČL'ãĆćãČ■ãČijãČşæğŃæĹŘãĂĄBIG-IP LTMïijĹAD-
CïijL'ãĄńãĆćãČL'ãĆłãČşãĄŮãĄęåĹl'çŤĺãĄŹãĆŃæğŃæĹŘãĆŠåŘŰãĆŃãĄŞãĄĺãĄĺãĄŃåŔŕèČ¡ãĄğãĄŹãĂĆãĄİãĄŮãĄęãĂĄãĆłãČşãĆ
Cloud ãĄğãĆĆPrivate CloudãĄğãĆĆåŃŢä¡IJãĄŹãĆŃãĄ§ãĆĄãĂĄãČĞãČŮãČ■ãĆd'åăť'æL'ĂãĆŠéĄÿãĄşãĄ¿ãĄŻãĆŞãĂĆ

èĞłçd'¿ãĄğæ§Ťèž§ãĄŁWAFãČİãČłãĆůãČijãĆŠä¡IJæĹŘãĄŮãĄ§ãĄĎãĄŁåőćæğŸãĂĄAWAFãĆŠåĹl'çŤĺãĄŮãĄęéńŸåžęãĄŁWAFãĆţã

ãĄİãĄőäžŰãĂĄAWAFãĄőçL'źéŢůãĆĎåĹl'çŤĺãĆąãČłãĆČãČĹãĄŕäžëäÿŃãĄőèĺŸäžŃãĆŠãĄŤçćžèł■äÿŃãĄŢãĄĎãĂĆ

- K85426947: BIG-IP ASM operations guide
- K07359270: Succeeding with application security

2.1.2 AWAFãĆźãĆ£ãČşãČĽãĆćãČ■ãČşæğŃæĹŘãČ■ãČČãČĹãČŕãČijãĆŕãĆţãČşãČŮãČń

æIJňæĽŃéăĘæŻÿãĄğãĄŕäżěäÿŃãĄőãĆţãČşãČŮãČńãČ■ãČČãČĹãČŕãČijãĆŕæğŃæĹŘãĄğèĺ■åőŽãĆŠèąŇãĄĐãĄ¿ãĄŹãĂĆ
ïijĹF5ãČŔãČşãĆžãĆłãČşçŠřåćČãĄğãĆĆåŘŇæğŸãĄőãČ■ãČČãČĹãČŕãČijãĆŕæğŃæĹŘãĆŠåĹľçŤĺãĄŮãĄęãĄĐãĄ¿ãĄŹãĂĆïijĽ

1. æIJňãĆňãĆďãČĽãĄńãĄŁãĄŚãĆŃæğŃæĹŘãĆďãČąãČijãĆÿ

Note:

- **v15.1.2.1äżěäÿŁ** ãĄőãČŘãČijãĆÿãČğãČşãĆŠãĄŤåĹľçŤĺäÿŃãĄŢãĄĐãĂĆ(2021åźť3æIJĹè£¡èÍŸ)
- ïijĹåŘĎF5äżčçŘĘåžŮãĄğãĆţãČÍãČijãČĹåŕŕèČ¡ãĄłçfĎåŻšãĄńãĄŁãĄĐãĄęãĂĄïijĽæěţåŁŻæIJĂæŰřãĄőãČŘãČijãĆÿãČğ

2.1.3 åĹİæIJ§èĺ■åőŽïijĹãČŮãČ■ãČŞãĆÿãČğãČŃãČşãĆŕãĂĄãČ■ãČČãČĹãČŕãČijãĆŕãĄőèĺ■åőŽç■L

1. åĹİæIJ§ãČŠãĆźãČŕãČijãČĽïijĹUsername:admin, Password:adminïijĽãĄğãČ■ãĆŕãĆd'ãČşãĄŮãĂĄF5ãČŔãČşãĆžãĆłãČşãČĹãČ

2. ãČŚãĆźãČŕãČijãČL'åď'L'æŻť'ãĄńæĹŘåŁ§ãĄŮãĄ§ãĆL'ãĂĄåď'L'æŻť'å¿ŇãĄőãČŚãĆźãČŕãČijãČL'ïijĹUsername:admin, Password:ilovef5ïijL'ãĄğãČ■ãĆřãĆď'ãČşãĄŮãĄ¿ãĄŹãĂĆ

3. *Next* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

4. ãČľãĆďãĆżãČşãĆźãĆćãĆŕãČĘãĆčãČŹãČijãĆůãČğãČşãĆŠèąÑãĄĐãĄ¿ãĄŹãĂĆãČľãĆďãĆżãČşãĆźæŁŢåĚěæÿĹãĄ£ãĄőåăť åŘ
ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

5. ãČŮãČ■ãČŞãĆÿãČğãČŃãČşãĆřãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Application Security(ASM)** ãĄőãĄ£ãĆŠéĄÿæŁđãĄŮãĂĄ*Next* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

6. ãČŮãČ■ãČŞãĆÿãČğãČŃãČşãĆřãĄńãĄŕåřŚãĄŮæŹĆéŰŞãĄŇãĄŃãĄŃãĆŁãĄ¿ãĄŹãĂĆçţĆäžĘãĄŮãĄ§ãĆĽãĂĄ*Continue* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

7. ãČĞãČŘãĆďãĆźèÍijæŸŐæŻÿãĄőçćžèł■ãĆŠãĄŮãĂĄ*Next* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

8. **Host Name** ãĄńãĂĄ**big80.f5jp.local** ãĄĺèĺ■åőŽãĄŮãĂĄ**Time Zone** ãĄń **Japan**

ãĆŠéĄÿæŁđãĄŮãĂĄ**Root Account** ãĄőãČŚãĆźãČŕãČijãČĽãĄń **ilovef5** ãĄĺèĺŸåĚěãĄŮãĂĄ*Next*
ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆïijĹF5ãČŔãČşãĆžãĆłãČşãČĹãČňãČijãČŃãČşãĆřäżěåď˙ŰãĄőåät˙åŘĹãĄŕãĂĄãĄİãĆŃ

9. *Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

10. External VLANãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Network >> VLANs : VLAN List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄń **external** ãĄĺèĺ■åőŽãĄŮãĂĄ**Interface** ãĄń **1.1(Untagged)** ãĆŠéĄÿæŁđãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

11. Internal VLANãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Network >> VLANs : VLAN List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄń **internal** ãĄĺèĺ■åőŽãĄŮãĂĄ**Interface** ãĄń **1.2(Untagged)** ãĆŠéĄÿæŁđãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

12. äžěäÿŃãĄőãĆĹãĄĘãĄńãĄłãĆŁãĄ¿ãĄŹãĂĆ

13. External SelfIPãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Network >> Self IP List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄń **external-selfip** ãĄĺèĺ■åőŽãĄŮãĂĄ**IP Address** ãĄń **10.1.10.80** ãĂĄ**Netmask** ãĄń **255.255.255.ïijŘ** ãĂĄ**VLAN/Tunnel** ãĄń **external** ãĆŠéĄÿæŁđãĄŮãĂĄ**Port Lockdown** ãĄń **Allow None** ãĆŠéĄÿæŁđãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

14. Internal SelfIPãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Network >> Self IP List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄń **internal-selfip** ãĄĺèĺ■åőŽãĄŮãĂĄ**IP Address** ãĄń **10.1.20.80** ãĂĄ**Netmask** ãĄń **255.255.255.ïijŘ** ãĂĄ**VLAN/Tunnel** ãĄń **internal** ãĆŠéĄÿæŁđãĄŮãĂĄ**Port Lockdown** ãĄń **Allow Default** ãĆŠéĄÿæŁđãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

15. äžěäÿŇãĄõãĆĹãĄĘãĄńãĄłãĆŁãĄ¿ãĄŹãĂĆ

16. Default GatewayãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**Network >> Routes** ãĄńãĄęãĂĄ*Add* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄńäżæĎŔãĄőåŘ■åĽ■ãĆŠèĺ■åőŽãĄŮãĂĄ**Destination** , **Netmask** ãĄń **0.0.0.0** ãĆŠèĺ■åőŽãĄŮãĂĄ**Gateway Address** ãĄń **10.1.10.1** ãĆŠèĺ■åőŽãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

17. WEBãĆţãČijãČŘãĄÿãĄőãČńãČijãČĘãĆčãČşãĆřèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆïijĹäżěäÿŇãĄŕèĺ■åőŽä¿ŇãĄĺãĄłãĆŁãĄ¿ãĄŹã

18. äżěäÿŃãĄőãĆĹãĄĘãĄńãĄłãĆŁãĄ¿ãĄŹãĂĆ

19. DNSãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**System >> Configuration : Device : DNS**
ãĄńãĄęèĺ■åőŽãĄŮãĄ¿ãĄŹãĂĆïijĹF5ãČŔãČşãĆžãĆłãČşãČĹãČňãČijãČŃãČşãĆřãĄğãĄŕäžĹãĆĄèĺ■åőŽãĄŢãĆŇãĄęãĄĎãĄ¿ãĄ

20. NTPãĄőèĺ■åőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆ**System >> Configuration : Device : NTP** ãĄńãĄęãĂĄNTPãĆŠèĺ■åőŽãĄŮãĂĄ*Update* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ F5ãČŔãČşãĆžãĆłãČşãČĹãČňãČijãČŃãČşãĆřãĄğãĄfNICTãĄőNTPãĆŠåĹľçŤĺãĄŮãĄ¿ãĄŹãĂĆ

2.1.4 ïijĹèĎĘåijśãĄłïijĽ'WEBãĆţãČijãČŘãĄőçŹżéŇš

1. Virtual ServerãĆŠä¡IJæĹŘãĄŮãA¿ãĄŹãĂĆ**Local Traffic >> Virtual Servers : Virtual Server List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãA¿ãĄŹãĂĆ

2. **Name** ãĄńäżæĎŔãĄőåŘ■çğřãĆŠèÍŸè£řãĄŮãĂĄ**Destination Address/Mask** ãĄń **10.1.10.180**ãĂĄ**Service Port** ãĄń **443** ãĆŠèÍ■åőŽãĄŮãĂĄ**HTTP Profile (Client)** ãĄńãĄę **HTTP** ãĆŠéĄÿæŁđãĂĄ**SSL Pofile(Client)** ãĄńãĄę **clientssl** ãĆŠéĄÿæŁđãĄŮãA¿ãĄŹãĂĆ

3. **Source Address Translation** ãĄńãĄęãĂĄ**Automap** ãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

4. **Default Pool** ãĄńãĄęãĂĄ+ ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

5. PoolãĆŠä¡IJæĹŘãĄŮãĄ¿ãĄŹãĂĆ**Name** ãĄńãĄęãĂĄäżżæĎŔãĄőåŘ■çğřãĆŠåĚěåŁŻãĄŮãĂĄ**Health Monitors** ãĄńãĄę **gateway_icmp** ãĆŠéĄÿæŁđãĄŮãĂĄNew MembersãĄńãĂĄWEBãĆţãČijãČŘïijĹ**Address** : **10.1.20.202**, **Service Port** : **80** ïijĽãĆŠåŁăăĄĹãĄę *Add* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

6. **Default Pool** ãĄńPoolãĄŇè£¡åŁãăĄŢãĆŇãĄ§ãĄŞãĄÍãĆŠçćžèł■ãĄŮãĂĄ*Finished* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

7. WindowsãĆŕãČľãĆd'ãĆćãČşãČĹãĆŠèţůåŃŢãĄŮãĂĄhttps://10.1.10.180/DVWA/login.php ãĄńãĆćãĆŕãĆżãĆźãĄŮãĄ¿ãĄŹãĂĆUsername: **admin**ãĂĄPassword: **password** ãĄğãČ■ãĆŕãĆd'ãČşãĄŮãĄ¿ãĄŹãĂĆ

8. **DVWA Security** ãĄńãĆćãĆŕãĆżãĆźãĄŮãĂĄ**Security Level** ãĆŠ **Low** ãĄńèĺ■åőŽãĄŮãĄ¿ãĄŹãĂĆ

9. **SQL Injection** ãĄńãĆćãĆŕãĆżãĆźãĄŮãĂĄ**User ID** ãĄń **âĂŸ or 1=1 #** ãĄĺåĚěåŁŻãĄŮãĂĄSQLãĆďãČşãĆÿãĆğãĆŕãĆůãČğãČşæŤżæŠČãĆŠãĄŮãĄ¿ãĄŹãĂĆ(æIJńãĆňãĆďãČL'ãĄŃãĆL'ãĆşãČđãČşã

10. SQLãĆďãČşãĆÿãĆğãĆŕãĆůãČğãČşæŤżæŠČãĄŇæĹŘåŁ§ãĄŮãĂĄUser IDãĄŇèď'ĞæŢřèąĺçď'žãĄŢãĆŇãĆŃãĄŞãĄĺãĆŠçćžèł■ã

2.1.5 Guided configurationãĄńãĆĹãĆŃWAFãČİãČłãĆůãČijãĄőä¡IJæĹŘ

1. **Security >> Guided Configuration** ãĆŠéŰŃãĄ■ãĄ¿ãĄŹãĂĆGuided ConfigurationãĄőãČŘãČijãĆÿãČğãČşãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆïijĹGuided ConfigurationãĄőèţůåŃŢãĄńãĄŕåřŠãĄŮæŹĆéŰŞãĄŇãĄŃãĄŃãĆŁãĄ¿ãĄŹãĂĆïijĽ

2. ASKF5ãĄőDownloadãĆţãĆďãČĹ ãĄńãĄęãĂĄæIJĂæŰřçĽĹãĄőGuided Configura-
tionãĆŠãČĂãĆęãČşãČ■ãČijãČĽãĄŮãĄ¿ãĄŹãĂĆãČĂãĆęãČşãČ■ãČijãČĽãĄńãĄŕAskF5ãĄőãĆćãĆńãĆęãČşãČĹçŹżéŇšãĄŇå£
ClientãČĞãĆźãĆŕãČĹãČČãČŮäÿŁãĄőãČĂãĆęãČşãČ■ãČijãČĽæÿĹãĄ£ãĄőãČŢãĆąãĆd'ãČńãĆŠãĄŤåĹľçŤĺäÿŃãĄŢãĄĎãĂĆïij

3. AWAFãĄőåĚĹçÍŃãĄőçŤżéÍćãĄńæĹżãĆŁãĂĄåŔşäÿŁãĄő **Upgrade Guided Configuration** ãĆŠãĆŕãČłãČČãĆŕãĄŮãĂĄãČĂãĆęãČşãČ■ãČijãČĽãĄŮãĄ§Guided ConfigurationãČŢãĆąãĆďãČńïijĹxxx.tar.gzïijĽãĆŠãĆćãČČãČŮãČ■ãČijãČĽãĂĄãĆďãČşãĆźãČĹãČijãČńãĄŮãĄ¿ãĄŹãĂĆ

4. ãĆďãČşãĆźãČĹãČijãČńãĄŮãĄęãĄĎãĆŃéĂŤäÿ■ãĄőãĆďãČąãČijãĆÿãĄğãĄŹãĂĆ

5. ãĆďãČşãĆźãČĹãČijãČńãĄÑçţĆäžĘãĄŮãĄ§ãĆĽãĂĄ*Continue* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

6. Guided ConfigurationãĄőãČŘãČijãĆÿãČğãČşãĄŇãĆćãČČãČŮãČĞãČijãČĹãĄŢãĆŇãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄ

7. **Web Application Protection** ãĄő **Web Application Protection** ãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

8. **DNS**, **NTP**, **Routing** ãĄŇèĺ■åőŽOKãĄĺãĄłãĄčãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĂĄ*Next*

ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

9. åŔşäÿŁãĄő **Show Advanced Setting** ãĆŠãĆŕãČŁãČČãĆŕãĄŮãĂĄ**Security Policy Name** ãĄńäżżæĎŔãĄőåŘ■åĽ■ãĆŠèĺ■åőŽãĄŮãĂĄ**Enforcement Mode** ãĄńãĄę **Transparent** ãĆŠéĄÿæŁđãĄŮãĂĄ**type of policy to protect application** ãĄńãĄęãĂĄ**Generic** ãĆŠéĄÿæŁđãĄŮãĂĄ**Server Technologies** ãĄńãĄęåĹľçŤĺãĄŮãĄęãĄĎãĆŃãČ§ãČĽãČńãĆęãĆğãĆćãĆĎèĺĂèłđãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆF5ãČŔãČşãĆžãĆłãČşçŠřåćČã **MySQL**, **PHP** ãĆŠéĄÿæŁđãĄŮãĂĄ*Next* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

10. æŮćãĄńVirtual ServerãĄŕä¡IJæĹŘæÿĹãĄ£ãĄłãĄőãĄğãĂĄãĄŞãĄŞãĄğãĄŕãĂĄ**Assign Policy to Virtual Server(s)** ãĄńãČĄãĆğãČČãĆŕãĆŠåĚěãĆŇãĂĄ**Use Existing** ãĆŠéĄÿæŁđãĄŮãĂĄä¡IJæĹŘæÿĹãĄ£ãĄőVirtul ServerãĆŠåŔşãĄńçğżåŃŢãĄŢãĄŻãĂĄ*SaveïijĘNext* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

11. åĘĚåőźãĆŠçćžèł■ãĄŮãĂĄ*Deploy* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

12. ä¡IJæĹŘãĄŮãĄ§WAFãĄőãČİãČŁãĆůãČijãĄńLogging ProfileãĆŠãĆćãĆ£ãČČãČĄãĄŮãĄ¿ãĄŹãĂĆ**Security >> Overview:Summary** ãĄńãĄęãĂĄä¡IJæĹŘæÿĹãĄ£ãĄőVirtual ServerãĆŠéĄÿæŁđãĄŮãĂĄ**Attach** ãĄő **Logging Profile** ãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

13. **Log illegal requests** ãĆŠéĄÿæŁđãĄŮãĂĄ*Attach* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

14. **Local Traffic >> Virtual Servers:Virtual Server List** ãĄńãĄęä¡IJæĹŘæÿĹãĄ£ãĄőVirtul ServerãĆŠéĄÿæŁđãĄŮãĂĄ**Security** ãĆ£ãČŰãĄő **Policies** ãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ**Application Security Policy** ãĄĺãĂĂ**Log Profile** ãĄŇãĄİãĆŇãĄđãĆŇèĺ■åőŽãĄŢãĆŇãĄęãĄĎãĆŇãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

15. æňąãĄńèłďæďIJç§ěåŕ¿ç■ŰãĂĄèšăè■ůéŸšæ■ćåŕ¿ç■ŰãĆŠèĺ■åőŽãĄŮãĄ¿ãĄŹãĂĆïijĹå£ĚéăĹãĄğãĄŕãĄĆãĆŁãĄ¿ãĄŻãĆŞãĂĆï
    Security >> Application Security : Policy Building : Learning and Blocking Settings ãĆŠéŰŃãĄ■ãĄ¿ãĄŹãĂĆæŮěæIJňèłđãĆţãĆd'ãČĹãĄőèłď'æď'IJç§ěãĄőéŸšæ■ćç■ŰãĄĺãĄŮãĄęãĂĄ**Failed to convert character** ãĆŠOFFãĄńãĄŮãĄ¿ãĄŹãĂĆãĄ¿ãĄ§ãĂĄ**Data Guard:Information Leakage Detected** ãĆĆãČŚãČŢãĆl'ãČijãČđãČşãĆźéİćãĆŠèĂČæĚőãĄŮãĄęOFFãĄńãĄŮãĂĄ*Save* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

16. *Apply Policy* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĂĄãČİãČłãĆůãČijãĆŠåŔ■æŸăăĄŢãĄŻãĄ¿ãĄŹãĂĆ

2.1.6 ãĆůãĆřãČ■ãČĄãČčãĄőçŁűæĚŃçćžèł■

1. **Security >> Application Security : Policy Building : Learning and Blocking Settings** ãĆŠéŰŃãĄ■ãĄ¿ãĄŹãĂĆ**Attack Signatures** ãĄőãĄĺãĄşãĆ■ãĄğãĂĄ**Enable Signature Staging** ãĄńãČĄãĆğãČČãĆŕãĄŇåĚěãĄčãĄęãĄĎãĆŃãĄşãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

2. **Security >> Application Security : Security Policies : Policies List** ãĆŠéŰŃãĄ■ãĄ¿ãĄŹãĂĆä¡IJæĹŘæÿĹãĄ£ãĄőãĆżãĆ■ãČěãČłãČĘãĆčãČĬãČłãĆůãČijãĆŠãĆŕãČłãČČãĆŕãĄŮãĄ¿ãĄŹãĂĆ

3. **Attack Signatures** ãĆŠãĆŕãČłãČČãĆŕãĄŮãĄ¿ãĄŹãĂĆä¡IJæĹŘæÿĹãĄ£ãĄőãĆżãĆ■ãČěãČłãČĘãĆčãČĬãČłãĆůãČijãĆŠãĆŕãČłã
Staging ãĄĺãĄłãĄčãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

Note: Staging(ãĆźãČĘãČijãĆÿãČşãĆřãČćãČijãČL'ãĄĺãĄfãĂĄLearn/Alarm/BlockèĺĺåőŽãĄŇçĎąåŁźåŇŰãĄŢãĆŇãĂĄæŤżæŠ
Traffic LearningãĂĺãĄğåĺęç£ŠãĄŹãĆŃãĄăãĄŚãĄőåŃŢä¡IJãĄĺãĄłãĆŃãČćãČijãČL'ãĄğãĄŹãĂĆ

2.1.7 ãĆźãČĘãČijãĆÿãČşãĆřãČĺãĆřãĄőèĺĺåőŽ

ãĆźãČĘãČijãĆÿãČşãĆřãĄőãČĺãĆřãĆŠEvent Logs ãĄńåĞžåŁŻãĄŹãĆŃãĄ§ãĆĄãĄőèĺĺåőŽãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆïijĹå£ĚéăĹãĄğã

1. **Security >> Event Logs : Logging Profiles** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆäżżæĎŘãĄőåŘĺåL'ĺãĆŠè
   Security ãĄőãĄĺãĄŞãĆĺãĄğãĂĄ**Enabled** ãĆŠãČĄãĆğãČČãĆŕãĄŮãĂĄ**Request type** ãĄńãĄęãĂĄ**Illegal requests, and requests that include staged attack signatures âĂę** ãĆŠéĄÿæŁđãĄŮãĂĄ*Create* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

2. **Security >> Overview : Summary** ãĄńãĄęãĂĄä¡IJæĹŘæÿĹãĄ£ãĄőVirtual ServerãĄńãČĄãĆğãČČãĆfãĆŠãĄŮãĂĄäÿĂæŮęãĂĄãĆćãĆ£ãČČãČĄãĄŮãĄ§ **Logging Profile(s)** ãĆŠãĄfãĄŽãĄŮãĄ¿ãĄŹãĂĆ

3. åĘ■åžęãĆćãĆ£ãČČãČĄãĄőèĺ■åőŽãĆŠãĄŮãĄ¿ãĄŹãĂĆ

4. ä¡IJæĹŘæÿĹãĄ£ãĄő **Logging Profile(s)** ãĆŠãĆćãĆ£ãČČãČĄãĄŮãĄ¿ãĄŹãĂĆ

2.1.8 ãĆůãĆřãČ■ãČĄãČčãĄőåŃŢä¡IJçćžèł■

1. WindowsãĆřãČľãĆd'ãĆćãČşãČĹãĆŠèţůåŃŢãĄŮãĂĄhttps://10.1.10.180/DVWA/login.php ãĄńãĆćãĆřãĆżãĆźãĄŮãĄ¿ãĄŹãĂĆUsername: **admin**ãĂĄPassword: **password** ãĄğãČ■ãĆřãĆd'ãČşãĄŮãĂĄ**SQL Injection** ãĄńãĆćãĆřãĆżãĆźãĄŮãĂĄ**User ID** ãĄń **âĂŸor 1=1 #** ãĄĺåĚěåŁŻãĄŮãĂĄSQLãĆd'ãČşãĆÿãĆğãĆřãĆůãČğãČşæŤżæŠČãĆŠãĄŮãĄ¿ãĄŹãĂĆ(æIJňãĆňãĆd'ãČL'ãĄŃãĆL'ãĆşãČđãČşã

2. **Security >> Event Logs : Application : Requests** ãĄńãĄęãĂĄ**Staged** ãĄğSQLãĆďãČşãĆÿãĆğãĆŕãĆůãČğãČşãĄŇæďIJåĞžãĄŢãĆŇãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

3. äÿŁèÍŸçŤżéİćãĄőSuggestionsãĄő **ViewâĂę** ãĆŠãĆŕãČłãČČãĆŕãĄŹãĆŃãĄĺãĂĄTrafficLearningãĄőçŤżéİćãĄğãĆĆ **Attack signature detected** ãĄŇçćžèł■ãĄğãĄ■ãĄ¿ãĄŹãĂĆïijĹ **Security >> Application Security : Policy Building : Traffic Learning** ãĄğãĆĆãĄ§ãĄľãĆŃãĄ¿ãĄŹãĂĆïijĽ

2.1.9 ãĆůãĆřãČ■ãČĄãČčãĄőãĆźãČĘãČijãĆÿãČşãĆřèğčéŹď

1. ãĆźãČĘãČijãĆÿãČşãĆřãĆŠèğčéŹď ãĄŹãĆŃãĄĺãĂĄEvent logãĄńæŤżæŠČãĄĺãĄŮãĄęèÍŸéŇšãĄŢãĆŃãĄ¿ãĄŹãĂĆ**Security >> Application Security : Security Policies : Policies List >> DVWA_policy** ãĄńãĄęãĂĄ**Attack Signatures** ãĆŠéĄÿæŁđãĄŮãĂĄçŤżéİćåŕşäÿŁãĄő **Enforce all Staged Signatures** ãĆŠéĄÿæŁđãĄŮãĂĄãĆźãČĘãČijãĆÿãČşãĆřãĆŠèğčéŹď ãĄŮãĄ¿ãĄŹãĂĆ

2. ãĆźãČĘãČijãĆÿãČşãĆřãĄŇèğčéŹďãĄŢãĆŇãĆŃãĄĺãĂĄ**Status** ãĄŇ **Enforced** ãĄĺãĄłãĆŁãĄ¿ãĄŹãĂĆ

3. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

4. åĘ■åžęWindowsãĆŕãČl'ãĆd'ãĆćãČşãČĹãĄŃãĆL'SQLãĆd'ãČşãĆÿãĆğãĆŕãĆůãČğãČşãĆŠèl'ęãĄ£ãĄ¿ãĄŹãĂĆ

5. **Security >> Event Logs : Application : Requests** ãĄńãĄęãĂĄ**Alarm Learn** ãĄğSQLãĆďãČşãĆÿãĆğãĆŕãĆůãČğãČşãĄŇæďIJåĞžãĄŢãĆŇãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

2.1.10 BlockingãČćãČijãČĽãĄÿãĄőåďĽæŻť

1. BlockingãČćãČijãČĽãĄÿåďĽæŻťãĄŹãĆŃãĄĺãĂĄEvent logãĄńæŤżæŠČãĄĺãĄŮãĄęèĺŸéŇšãĄŢãĆŇãĂĄæŻťãĄńãČŰãČ■ãČ
   >> Application Security : Security Policies : Policies List >> DVWA_policy ãĄńãĄęãĂĄ**General Settings** ãĆŠéĄÿæŁđãĄŮãĂĄ**Enforcement Mode** ãĆŠ **Blocking** ãĄńåď'ĽæŻť'ãĄŮãĂĄ*Save* ãČIJãĆ£ãČşãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

2. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

3. åE■åžęWindowsãĆŕãČl'ãĆd'ãĆćãČşãČĹãĄŃãĆL'SQLãĆd'ãČşãĆÿãĆğãĆŕãĆůãČğãČşãĆŠèl'ęãĄ£ãĄ¿ãĄŹãĂĆ

4. **Security >> Event Logs : Application : Requests** ãĄńãĄęãĂĄ**Block Alarm Learn** ãĄğSQLãĆďãČşãĆÿãĆğãĆŕãĆůãČğãČşãĄŇæďIJåĞžãĄŢãĆŇãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

2.1.11 ãĆůãĆřãČ■ãČĄãČčãĄőãČĄãČěãČijãČŃãČşãĆř

ãĂĂèłďæďIJç§ěãĄŇçŹžçŤ§ãĄŮãĄ§åăťåŘĹãĄőåŕ¿åĞęä¿ŃãĆŠãĄŢçťźäżŃãĄŮãĄ¿ãĄŹãĂĆ
äžěäÿŃãĄğåő§æŰ¡ãĄŹãĆŃåĘĚåőźãĄŕãĂĄWebãĆćãČŮãČłãĆśãČijãĆůãČğãČşãĄőåŘĎãČŠãČľãČąãČijãĆ£ãĄőå¡źåL'šãĄŇåĚĺãĄęæł

äžěäÿŃãĄŕèłďæďIJç§ěãĄőä¿ŃãĄğãĄŹãĂĆ

1. åĚěåŁŻåĘĚåőźãĄńãĄ§ãĄ¿ãĄ§ãĄ¿æŤżæŠČãĄńéŰćéĂčãĄŹãĆŃãČŠãČľãČąãČijãĆ£ãĄŇåŘńãĄ¿ãĆŃãĄęãĄŮãĄ¿ãĄčãĄ§ãĄĺã

2. æŻÿãĄ■è¿ijãĄ£ãĆŠèąÑãĄĘãĄÍãĂĄAWAFãĄğæŤżæŠČãĄÍãĄŮãĄęæď IJç§ěãĄŢãĆŇãĄęãĄŮãĄ¿ãĄĎãĄ¿ãĄŹãĂĆ

äżěéŹ■ãĂĄïijŠãĄď ãĄőåŕ¿ç■Űä¿ŃãĆŠãĄŤçt' źäżŃãĄŮãĄ¿ãĄŹãĂĆ

èłď æď IJç§ěãĄŮãĄ§ãČŚãČľãČąãČijãĆ£ãĆŠãČŻãČŕãĆďãČĹãČłãĆźãČĹåŇŰ

1. Event logãĄğèłď æď IJç§ěãĄŮãĄ§ãČ■ãĆŕãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

2. **Occurences** ãĆŠãĆřãČłãČČãĆřãĄŮãĂĄèłď'æď'IJç§ěãĄŮãĄ§ãČŚãČl'ãČąãČijãĆ£åŘ■ïijĹmtxMessageïijL'ãĄĺãĆůãĆřãČ■ãČĄãČ

3. **Security >> Application Security : Parameters : Parameters List** ãĄńãĄęãĂĄ*Create* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

4. **Parameter Name** ãĄńèłďæď'IJç§ěãĄŮãĄ§ãČŚãČľãČąãČijãĆ£åŘ■ïijĹmtxMessageïijL'ãĆŠåĚěåŁŻãĄŮãĂĄãČĄãĆğãČČãĆŕBC
Value Type ãĄńãĄęãĂĄ**Ignore Value** ãĆŠéĄÿæŁđãĄŮãĂĄ*Create* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

5. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

6. WindowsãĄńãĄęåĘ■åžęæŻÿãĄ■è¿ijãĄ£ãĆŠèąŇãĄĘãĄĺãĂĄæŻÿãĄ■è¿ijãĄ£ãĄŇæĹŘåŁ§ãĄŹãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ã

èłďæďIJç§ěãĄŮãĄ§ãČŠãČľãČąãČijãĆ£ãĄğèľšå¡ŞãĆůãĆřãČ■ãČĄãČčãĆŠçĎąåŁźåŇŰ

1. äżŁåžęãĄŕåĚĹçÍŃä¡IJæĹŘãĄŮãĄ§ParameterãĄő **Parameter Value Type** ãĄńãĄęãĂĄ**User-Input Value** ãĆŠéĄÿæŁđãĄŮãĂĄ**Attack Signatures** ãĆ£ãČŰãĄńãĄęãĂĄèłďæďIJç§ěãĄŮãĄ§ãĆůãĆřãČ■ãČĄãČčIDïijĹ200002835ïijL'ãĆŠ ãĄńãĄŮãĂĄ*Update* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

2. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

3. WindowsãĄńãĄęåĘ■åžęæŻÿãĄ■è¿ijãĄ£ãĆŠèąÑãĄĘãĄĺãĂĄæŻÿãĄ■è¿ijãĄ£ãĄÑæĹŘåŁ§ãĄŹãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ã

2.1.12 Threat campaignsãĆůãĆřãČ■ãČĄãČčãĄőèĺ■åőŽ

ãĂĂWebãĆćãČŮãČłãĆśãČijãĆůãČğãČşãĄőèĎĚåĺĄåŕ¿ç■ŰãĆŠèąŇãĄĘäÿŁãĄğãĂĄåő§éŽŻãĄőæŤżæŠČãĄĺãČŢãĆĺ'ãČijãČńãĆźãČİã

ãĂĂãĄŞãĄőåŢŔéąŇãĄŕãĂĄæd'IJæ§żãĄŹãĆŃãČĞãČijãĆ£ãĄŇãĆůãČşãĆřãČńãČİãĆd'ãČşãČĹãĄğãĄĆãĆŃãĄŞãĄĺãĄńãĄĆãĆŁãĄ¿
CampaignsãĆůãĆřãČ■ãČĄãČč ãĄĺãĄĎãĄĘçŃňèĞłãĄőãĆůãĆřãČ■ãČĄãČčãĆŠæŔŘä¿ŻãĄŮãĄęãĄĎãĄ¿ãĄŹãĂĆ**Threat**
CampaignsãĆůãĆřãČ■ãČĄãČč ãĄŕãĂĄåő§éŽŻãĄőæŤżæŠČãĆ■ãČčãČşãČŽãČijãČşãĆŠåĚČãĄńèd'ĞæŢřãĄőæİąäżűãĆŠãČđãČČãČ

ãĂĂãĄŞãĄőéăĚãĄğãĄŕãĂĄThreat CampaignsãĆůãĆřãČ■ãČĄãČčãĄőèĺ■åőŽçćžèł■ãĄĺãĂĄãČĘãĆ■ãĆźãČĹäÿŁãĄńãĄęæŤżæŠČãĆţã

1. **Security >> Application Security : Policy Building : Learning and Blocking Settings** ãĄğèąĺçd'žãĄŢãĆŇãĄ§çŤżéİćãĄńãĄęãĂĄThreat Campaigns ãĄő **Alarm** ãĄĺ **Block** ãĄŇæIJL'åŁźãĄńãĄłãĄčãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆïijĹLearnãĄŕå■ŸåIJĺãĄŮãĄ¿ãĄŻãĆŞãĂĆïijL'

2. æŤżæŠČãĆŠåŔŮãĄŠãĄ§ãĄĺäżőåőŽãĄŮãĄęãĂĄEveng LogsãĄğãČ■ãĆřãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆïijĹF5ãČŔãČşãĆžãĆłãČşãĄ
Rating ãĄŇ **5:Request is most likely a threat** ãĄĺãĄłãĄčãĄęãĄĎãĆŃãĄŞãĄĺãĄŇåĹĘãĄŃãĆŁãĄ¿ãĄŹãĂĆãĄŞãĆŃãĄŕThreat
CampaignsãĆůãĆřãČ■ãČĄãČčãĄŇåő§éŽŻãĄőæŤżæŠČãĆŠåĚČãĄńä¡IJæĹŘãĄŢãĆŃãĄęãĄŁãĆŁãĂĄãĄżãĄijãČŢãĆľãČijãČń

Note: Threat CampaignsãĆůãĆřãČ■ãČĄãČčãĆŠåĹľçŤĺãĄŹãĆŃãĄńãĄŕãĂĄåĹěéĂŤãĆţãČŰãĆźãĆŕãČŁãČŮãĆůãČğãČşãČľãĆďãĆżã

2.1.13 ãĆůãĆřãČ■ãČĄãČčãĂĄTCãĆůãĆřãČ■ãČĄãČčãĄőãĆćãČČãČŮãČĞãČijãČĹ

1. ãĆůãĆřãČ■ãČĄãČčãĄŇæŻťæŰřãĄŢãĆŃãĄ§åăťåŘĹãĄńãĂĄãĆźãČĘãČijãĆÿãČşãĆřãČćãČijãČL'ãĄğéĄŃçŤĺãĄŹãĆŃãĄŃãĂ
>> Application Security : Policy Building : Learning and Blocking Settings ãĄő **Attack Signatures**
ãĄńãĄęèąĺçď'žãĄŢãĆŃãĄ§çŤżéĺćãĄğãĂĄå£ĚèęĄãĄńå£IJãĄŸãĄęåÿŇæIJŻãĄŹãĆŃåŃŢä¡IJãĄÿãĄőèĺ■åőŽåď'L'æŻť'ãĆŠåő§æ
ApplyPolicyãĄğåŘ■æŸăãĄŢãĄŻãĄ¿ãĄŹãĂĆïijL'

Note:

Enforce updated rule immediately for non-staged signatures: Enforcement
çŁűæĚŃ(Non-Staging)ãĄőæŮćå■ŸãĆůãĆřãČ■ãČĄãČčãĄŇãĆćãČČãČŮãČĞãČijãČĹ
ãĄŢãĆŇãĄ§åăť'åŘĹãĂĄæŻť'æŰřãĄŢãĆŇãĄ§ãĆůãĆřãČ■ãČĄãČčãĆĆ Non-Staging
ãĄĺãĄŮãĄ¿ãĄŹãĂĆ

Retain previous rule enforcement and place updated rule in staging: Enforcement
çŁűæĚŃ(Non-Staging)ãĄőæŮćå■ŸãĆůãĆřãČ■ãČĄãČčãĄŇãĆćãČČãČŮãČĞãČijãČĹ
ãĄŢãĆŇãĄ§åăť'åŘĹãĂĄæŻť'æŰřåĽ■ãĄőãĆůãĆřãČ■ãČĄãČčãĄŕ Non-Staging
ãĄőãĄ¿ãĄ¿ãĄĺãĄŮãĂĄæŻť'æŰř ãĄŢãĆŇãĄ§ãĆůãĆřãČ■ãČĄãČčãĆŠ Stag-
ing ãĄĺãĄŮãĄ¿ãĄŹãĂĆæŻť'æŰřãĄŢãĆŇãĄ§ãĆůãĆřãČ■ãČĄãČčãĄő Staging
æIJ§éŰŞãĄŇçţĆäžĘãĄŮãĄ§éŽŻãĄńãĂĄæŻť'æŰřåĽ■ãĄő ãĆůãĆřãČ■ãČĄãČčãĄŇåĽŁéŹď'ãĄŢãĆŇãĂĄæŻť'æŰřãĄŢãĆ
Non-Staging ãĄĺãĄłãĆŁãĄ¿ãĄŹãĂĆïijĹManualãČćãČijãČĽãĄğãĄőéĄŇçŤĺãĄőåăť'åŘĹãĄŕãĂĄæĽ'ŃåŃŢãĄğStaging-
>Non-StagingãĄőèĺ■åőŽãĄŇå£ĚèęĄãĄğãĄŹãĂĆïijĽ

2. **System >> Software Management : Live Update** ãĄğèąĺçď'žãĄŢãĆŇãĄ§çŤżéĺćãĄğãĂĄ**Check for Updates** ãĆŠãĆŕãČłãČČãĆŕãĄŮãĄęãĂĄãĆůãĆřãČ■ãČĄãČčæŻť'æŰřãĄőæIJĽçĎąãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

3. ãČĄãĆğãČČãĆŕäÿ■ãĄőãĆďãČąãČijãĆÿãĄğãĄŹãĂĆ(ãČĄãĆğãČČãĆŕãĄńãĄŕæŢřåĹĘãĄŃãĄŃãĆŁãĄ¿ãĄŹãĂĆ)

4. æŻťæŰřåŔŕèČ¡ãĄłãĆůãĆřãČ■ãČĄãČčãĄŇãĄĆãĆŃåăťåŘĹãĂĄäžëäÿŃãĄőãĆĹãĄĘãĄńèąĺçďžãĄŢãĆŇãĄ¿ãĄŹãĂĆâŸŞãĆŠæ
updates found ãĄĺèąĺçďžãĄŢãĆŇãĄ¿ãĄŹãĂĆãČĂãĆęãČşãČ■ãČijãČĽæÿĹãĄ£ãĄőãĆůãĆřãČ■ãČĄãČčãĄŕéżĎèĽšãĄĎç§ćå■řã
StatusãĄĺãĄłãĄčãĄęãĄĎãĄ¿ãĄŹãĂĆ)

5. åĚĺãĄęãĆŠãĆďãČşãĆźãČĹãČijãČńãĄŮãĄ§ãĄĎåăťåŘĹãĄŕãĂĄInstallAllUpdatesãĆŠãĆŕãČŁãČČãĆŕãĄŮãĄ¿ãĄŹãĂĆ

6. ãĆůãĆřãČ■ãČĄãČćæŻťæŰřäÿ■ãĄŕãĂĄäžëäÿŃãĄőãĆĹãĄĘãĄńèąĺçďžãĄŢãĆŇãĄ¿ãĄŹãĂĆ(æŻťæŰřãĄńãĄŕæŢřåĹĘãĄŃãĄŃ

7. Install ãĄŇåőŇäžĘãĄŹãĆŃãĄĺäżëäÿŃãĄőãĆĹãĄĘãĄńãĄłãĆŁãĄ¿ãĄŹãĂĆâŸŞãĆŠæŐĺãĄŮãĂĄçŤżéİćãĆŠéŰĽãĄŸãĄ¿ãĄŹã

8. äžëäÿŃãĄŇæŻťæŰřå¿ŇãĄőãĆďãČąãČijãĆÿãĄĺãĄłãĆŁãĄ¿ãĄŹãĂĆCurrentlyInstaslledãĆźãČĘãČijãĆ£ãĆźãĄőãĆůãĆřãČ■ãČA

9. UpdateãĄŢãĆŇãĄ§SignatureãĄőæČĚåăśãĄŇèąĺçď˙žãĄŢãĆŇãĄ¿ãĄŹãĂĆåŘĎEntityãĆŠãĆŕãČłãČČãĆŕãĄŹãĆŇãĄĺãĂĄèľšå¡Ş

10. Update ãĄŇãĄłãĄĎåăť˙åŘĹãĄŕ Install Updates ãĆŠãĆŕãČłãČČãĆŕãĄŮãĄęãĆĆäžëäÿŇãĄőãĆĹãĄĘãĄńèąĺçď˙žãĄŢãĆŇãĄ¿ãĄŹ

11. è£¡åŁăăĄŢãĆŇãĄ§ãĆůãĆŕãČ■ãČĄãČčãĄŇãĆźãČĘãČijãĆÿãČşãĆŕãĄńãĄłãĄčãĄęãĄĎãĆŇãĄŇãĄľãĄĘãĄŇãĄőçćžèł■æŰźæş
    >> Application Security : Security Policies : Policies List >> DVWA_policy
    ãĄğèąĺçď˙žãĄŢãĆŇãĄ§çŤżéİćãĄğãĂĄ**Status** ãĆŠ **Staging** ãĄğãČŢãĆčãČńãĆ£ãČłãČşãĆŕãĄŮãĄ¿ãĄŹãĂĆ

12. è£¡åŁăăĄŢãĆŇãĄ§ãĆůãĆřãČ■ãČĄãČčãĄŇãĆźãČĘãČijãĆÿãČşãĆřãĄĺãĄłãĄčãĄęãĄĎãĆŃãĄŞãĄĺãĄŇåĹĘãĄŃãĆŁãĄ¿ãĄŹãĂ

Note: F5ãČŔãČşãĆŻãĆłãČşãĄğãĄŕæL'ŃéăĘãĄőéŰćä£ĆäÿŁãĂĄåŃŢä¡IJçćžèł■ãĄőå¿ŇãĄńãĆůãĆřãČ■ãČĄãČčãĆŠãĆćãČČãČŮãČĞ
æŰřãĄŮãĄĎãĆůãĆřãČ■ãČĄãČčãĆŠãĆćãČČãČŮãČĞãČijãČĹãĄŹãĆŃãĄŞãĄĺãĄğæŰřãĄ§ãĄłæŤżæŠČãĄńåŕ¿å£IJãĄŹãĆŃãĄŞãĄĺã

- K82512024: Managing BIG-IP ASM Live Updates (14.1.x and later)

2.1.14 CVEçŢłåŔůãĄńãĆĹãĆŃãĆůãĆřãĆŹãČ■ãČĄãČčãĄőæď'IJçť'ć

åŘĎãĆůãĆřãČ■ãČĄãČčãĄÑãĄľãĄőCVEãĄńåŕ¿å£IJãĄŮãĄęãĄĎãĆŃãĄŃçćžèł■ãĄŹãĆŃãĄŞãĄĺãĄÑåŔřèČ¡ãĄğãĄŹãĂĆ

1. **Security >> OptionsÂă:ÂăApplication SecurityÂă:ÂăAttack SignaturesÂă:ÂăAttack Signature List** ãĄğèąĺçď'žãĄŢãĆŇãĄ§çŤżéÍćãĄő **Show Filter Details** ãĆŠãĆřãČłãČČãĆřãĄŹãĆŃãĄĺãĂĄäżěäÿŃãĄõãĆĹãĄĘãĄłçŤżéÍćãĄŃèąĺçď'žãĄŢãĆŇãĄ¿ãĄŹãĂĆ**References** ãĄŃãĆĽ **CVE** ãĆŠéĄÿæŁđãĄŮãĂĄCVEçŢłåŔůãĆŠåĚěåŁŻãĄŮãĄę *Go* ãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

äÿŁèĺŸãĄő CVE çŢłåŔů(CVE-2017-5638)ãĄŕãĂĄApache Struts2ãĄőèĎĘåijśæĂğãĄńåŕ¿å£IJãĄŮãĄ§ãĆůãĆřãČ■ãČĄãČčäÿĂè
ãĄğãĄŕãĂĄ1ãĄďãĄőCVEçŢłåŔůãĄńéŰćéĂčãĄŮãĄ§ãĆůãĆřãČ■ãČĄãČčãĄŇèďĞæŢřå■ŸåIJĺãĄŮãĄęãĄĎãĆŃãĄŞãĄĺãĄŇã

2.1.15 GeolocationãĄőèĺ■åőŽ

Geolocation Enforcement ãĄőèĺ■åőŽãĆŠèąŇãĄĘãĄŞãĄĺãĄğãĂĄæŐěçűŽãĄŢãĆŇãĆŃäžĹåőŽãĄőãĄłãĄĎåŻ¡ãĄŃãĆĽãĄőæŐěçűŽã

1. **Security >> Application SecurityÂă:ÂăPolicy BuildingÂă:ÂăLearning and Blocking Settings** ãĄő **IP Addresses/Geolocations** ãĄńãĄŁãĄĎãĄęãĂĄ**Access from disallowed Geolocation** ãĄő Learn/Alarm/Block ãĄŇãČĄãĆğãČČãĆŕãĄŢãĆŇãĄęãĄĎãĆŃãĄŞãĄĺãĆŠçćžèł■ãĄŮãĄ¿ãĄŹãĂĆ

2. **Security >> Application SecurityÂă:ÂăGeolocation Enforcement** ãĄńãĄęãĂĄæŐěçűŽãĄŹãĆŃäžĹåőŽãĄőãĄłãĄĎåŻ¡ãĆŠ **Disallowed Geolocations** ãĄńçğżåŃŢãĄŮãĂĄ*Save* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

3. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

2.1.16 IP IntelligenceïijĹIPĺïijL'ãĄőèĺ■åőŽ

IP Intelligence ãĆŠèĺ■åőŽãĄŹãĆŃãĄŞãĄĺãĄğãĂĄæŮćç§ěãĄőæĆłæĎŘãĄĆãĆŃIPãĆćãČL'ãČňãĆźãĄŃãĆL'ãĄőæŤżæŠČãĆŠBlockãA
SecurityåĞęçŘEąãĄőåL'■æőţãĄğ IPãĆćãČL'ãČňãĆźãĄőèl'Ţä¿ąãĄŃèąŃãĆŘãĆŃãĆŃãĄ§ãĆĄãĂĄCPU
èšäè■ůéńŸéĺřãĆŠåŠŇãĆL'ãĄŠãĆŃåŁźæđIJãĄŃãĄĆãĆŁãĄ¿ãĄŹãĂĆWAF ãĄĺ L7DDoS ãĄńãĄŁãĄĎãĄę IP Intelligence ãĆŠåĹl'çŤĺãĄŹãĆŃãĄŞãĄĺãĄŃåŘŕèČ¡ãĄğãĄŹãĂĆïijĹF5ãĆŘãČşãĆžãĆŁãČşãĄğãĄŕèĺ■åőŽçŤżéİćãĄőãĄ£ãĄőçćžèł■ãĄĺãĄłãĆ

1. **Security >> Application SecurityÂă:ÂăIP AddressesÂă:ÂăIP Intelligence** ãĄńãĄŁãĄĎãĄęãĂĄ **IP Ingelligence** ãĄő **Enabled** ãĆŠãČĄãĆğãČČãĆŕãĄŮãĄ¿ãĄŹãĂĆ

2. ãČĄãĆğãČČãĆŕãĄŮãĄ§ãĄĎãĆńãČĘãĆťãČŁãĄőAlarmãĄ¿ãĄ§ãĄŕBlockãĄńãČĄãĆğãČČãĆŕãĆŠåĚěãĆŇãĄ¿ãĄŹãĂĆ

3. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

Note: äÿŁèĺŸãĄőäżŰãĂĄL7DoS Shun ãĄĺ IP Intelligence ãĆŠçţĎåŘĹãĄŻãĆŃãĄŞãĄĺãĄńãĆĹãĄčãĄęãĂĄIP Intelligence ãĄő IPãČńãČŤãČěãČĘãČijãĆůãČğãČşDB ãĄőãČłãĆźãČĹãĆŠL7DoS år¿ç■ŰãĄőShun list(Auto-blacklisting)ãĄĺãĄŮãĄęåĽľçŤĺãĄŇåŘŕèČ¡ãĄğãĄŹãĂĆ

IP IntelligenceãĆŠåĽľçŤĺãĄŹãĆŃãĄńãĄŕãĂĄåĹééĂŤãĆţãČŰãĆźãĆŕãČłãČŮãĆůãČğãČşãČľãĆďãĆżãČşãĆźãĄŇå£ĚèęĄãĄĺãĄłãĆŁ

2.1.17 BlockingãČćãČijãČĽçŤżéĺćãĄőãČąãČČãĆżãČijãĆÿãĆńãĆźãĆ£ãČđãĆďãĆž

æŤżæŠČãĆŠãČŰãČ■ãČČãĆŕãĄŮãĄ§éŽŻãĄńãČęãČijãĆűãĄńè£ŤãĄŢãĆŇãĆŃãČňãĆźãČİãČşãĆźãČŽãČijãĆÿãĄőåĘĚåőźãĆŠåď'L'æŻ

1. **Security >> Application SecurityÂă:ÂăSecurity PoliciesÂă:ÂăPolicies List >> ãČİãČłãĆůãČijåŘ■** ãĄńãĄŁãĄĎãĄęãĂĄ **Response and Blocking Pages** ãĆŠéĄÿæŁđãĄŹãĆŃãĄĺäžěäÿŇãĄŇèąĺçď'žãĄŢãĆŇãĄ¿ãĄŹãĂĆ

2. **Response Body** ãĆ£ãČŰãĄńãĄęãĂĄ**Custom Response** ãĆŠéĄÿæŁđãĄŮãĄ¿ãĄŹãĂĆ

3. **Response Body** ãĄńãĄŁãĄĎãĄęãĂĄèąĺçď˙žãĄŢãĄŻãĄ§ãĄĎãČąãČČãĆżãČijãĆÿãĄńåď˙L˙æŻť˙ãĄŮãĄ¿ãĄŹãĂĆ

4. åŔşäÿŁãĄőæđăãĄőãĆĹãĄĘãĄłãČIJãĆ£ãČşãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

5. ãČŰãČ■ãČČãĆŕãČŽãČijãĆÿãĄőãČňãČŞãČěãČijãĄŇèąĺçď žãĄŢãĆŇãĄ¿ãĄŹãĂĆ

6. ãČąãČČãĆżãČijãĆÿãĄŇèąĺçď žãĄŢãĄŻãĄ§ãĄĎåĘĚåőźãĄĺäÿĂèĞť ãĄŮãĄęãĄĎãĆŇãĄřãĂĄ*save* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

7. *Apply Policy* ãĆŠæŁijãĄŮãĄ¿ãĄŹãĂĆ

8. Windows ClientãĄńãĄęãĂĄåĘ■åžęSQLãĆd'ãČşãĆÿãĆğãĆŕãĆůãČğãČşæŤżæŠČãĆŠèąŇãĄĎãĄ¿ãĄŹãĂĆãČŰãČ■ãČČãĆŕãČąã

2.2 AWAFèĺ■åőŽäÿ■çť Žçůĺ

Comming soon!