Web alkalmazások védelme Modsecurity segítségével

Ellenőrzése

1. Ellenőrizze, hogy elérhető-e az előző alkalommal készült webszerveren a főoldal: www1.zonaX.tilb.sze.hu
2. Nézze meg, hogy a weboldal megnyitható-e a bin/bash paraméterrel! https://www1.zonaX.tilb.sze.hu/index.html?bin/bash

Modsecurity telepítése, beállítása

3. Telepítse fel az Apache2-höz készült Modsecurity modult!

```
libapache2-mod-security2 modsecurity-crs
```

4. Figyelje folyamatosan a www1 SSL sitehoz tartozó access logot:

```
tail -f /var/log/apache2/www1.zonaX.tilb.sze.hu_access_log
```

5. Frissítse a böngészőjében az előzőleg megnyitott URL-t és közben figyelje a log állományt! (www1.zonaX.tilb.sze.hu/index.html?bin/bash)
6. Engedélyezze a www1 SSL sitehoz tartozó konfigurációs állományban a főkönyvtárban lévő állományokhoz a Modsecurityt!

```
…
<Directory /var/www/www1>
SecRuleEngine On                    #Modsecurity engedélyezése
Options FollowSymLinks
AllowOverride None
</Directory>
…
```

7. Indítsa újra az Apache2-őt:

```
systemctl restart apache2
```

8. Frissítse a böngészőjében az előzőleg megnyitott URL-t és közben figyelje a log állományt! (www1.zonaX.tilb.sze.hu/index.html?bin/bash) Figyelje meg, mit tapasztalt!
   Mely Modsecurity szabályok nem engedték az URL megnyitását?
   Nyissa meg egy másik böngészőben a www2 sitehoz tartozó index.html-t a a bin/bash paraméterrel! https://www1.zonaX.tilb.sze.hu/index.html?bin/bash
9. Tiltsa le a problémát okozó szabályokat az index.html állomány megnyitásához a www1 SSL sitehoz tartozó konfigurációs állományban!

```
…
<Location /var/www/www1/index.html>
```

```
SecRuleRemoveById <ID>
SecRuleRemoveById <ID>
SecRuleRemoveById <ID>
…
</Location>
…
```

10. Indítsa újra az Apache2-őt:

```
systemctl restart apache2
```

11. Frissítse a böngészőjében az előzőleg megnyitott URL-t és közben figyelje a log állományt! (www1.zonaX.tilb.sze.hu/index.html?bin/bash)
    Frissítse a másik böngészőben a www2-höz tartozó index.html-t a bin/bash paraméterrel! https://www1.zonaX.tilb.sze.hu/index.html?bin/bash
12. Mit figyelt meg? Mire alkalmazható a Modsecurity? Mire használható egy adott szabály kikapcsolása?