HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

CROATIAN ACADEMIC AND RESEARCH NETWORK

Rezultati postupka certifikacije aplikacije Knowledge Exchange (Knex3)

Autor:	CARNet
Verzija:	v. 1.0
Revizija:	
Datum:	13.8.2013.
URL:	

Sadržaj

1. Uvod

Odlukom Ministarstva znanosti, obrazovanja i sporta aplikacije koje pristupaju sustavu e-Matica moraju proći postupak ispitivanja sigurnosti, kako je navedeno u Obavijesti o certificiranju vanjskih aplikacija koje pristupaju e-Matici putem web servisa od 7. prosinca 2012. (Klasa: 650-01/12-01/00052, Urbroj: 533-21-12-0005). Navedeni postupak ima za cilj identificirati i otkloniti eventualne sigurnosne probleme koji bi mogli imati značajan utjecaj na sigurnost i stabilnost sustava e-Matica. Provođenje postupka certifikacije povjereno je CARNetu koji je postupak certifikacije aplikacije Knowledge Exchange okončao.

1.1. Podaci o provedenom postupku certifikacije

Početak ispitivanja: 1.7.2013.

Završetak ispitivanja: 12.7.2013.

Dostava izvještaja autoru: 16.7.2013.

Dostava ispravljene verzije aplikacije: 9.8.2013.

Završetak ispitivanja ispravljene verzije aplikacije: 13.8.2013.

2. Prvotno utvrđene ranjivosti i način njihovog uklanjanja

2.1. Neadekvatna obrada korisničkog unosa

- **Tip ranjivosti**: Umetanje SQL koda
- **Rizik**: Visok

Tijekom inicijalnog ispitivanja aplikacije ustanovljeno je kako u datoteci *download.php* ne postoji adekvatno filtriranje parametara koje datoteka prihvaća čime je bilo moguće izvesti umetanje SQL koda.

2.1.1. Način uklanjanja

Ispitivanjem ispravljene verzije aplikacije alatom Sqlmap te uvidom u izvorni kôd ustanovljeno je kako je u datoteci *download.php* implementirano filtriranje korisničkog unosa.

2.2. Slabe administratorske lozinke

- **Tip ranjivosti**: Slabe lozinke
- **Rizik**: Visok

Analizom lozinki zapisanih u bazi podataka ustanovljeno je kako se za njihovo sažimanje (*eng*. hash) koristi algoritam MD5 u kojem postoji više poznatih ranjivosti. Pored toga, u aplikaciji nije postojala adekvatna kontrola kvalitete korisničkih lozinki čime je bilo moguće koristiti slabe lozinke.

2.2.1. Način uklanjanja

Ustanovljeno je kako su u ispravljenoj verziji aplikacije slabe lozinke zamijenjene s lozinkama veće kvalitete te da je implementirana kontrola kvalitete lozinki. Postavljena kontrola kvalitete lozinki podrazumijeva minimalnu duljinu lozinke od 6 znakova pri čemu se one moraju sastojati od slova i brojeva. Iako navedena kontrola kvalitete predstavlja značajno povećanje razine sigurnosti lozinki u odnosu na prethodno ispitanu verziju aplikacije, i dalje se preporuča postavljanje minimalne duljine lozinki na **8 znakova** pri čemu one moraju sadržavati **alfanumeričke** i **specijalne znakove**.

2.3. Prijenos povjerljivih podataka u čitljivom obliku

- **Tip ranjivosti**: Enkripcija
- **Rizik**: Visok

Pristup ispitanom poslužitelju bio je omogućen putem protokola HTTP koji podatke prenosi u čitljivom obliku čime je na mrežnoj razini bilo moguće neovlašteno presresti korisnička imena i lozinke kao i cjelokupni promet.

2.3.1. Način uklanjanja

Tijekom ponovljenog ispitivanja aplikacije ustanovljeno je kako je na poslužitelju instaliran elektronički poslužiteljski certifikat tvrtke GeoTrust čime se komunikacija s poslužiteljem odvija putem kriptiranog kanala komunikacije korištenjem protokola HTTPS.

3. Zaključak postupka certifikacije – završno mišljenje

Tijekom dodatnog ispitivanja sigurnosti koje je obavljeno na novoj verziji aplikacije Knowledge Exchange utvrđeno je kako su nedostaci pronađeni u prvom ispitivanju ispravljeni.

Ispravljeni su propusti u datoteci *download.php* i uspostavljen je kriptirani komunikacijski kanal korištenjem protokola HTTPS, no još uvijek ima prostora za dodatno unapređenje sigurnosti korisničkih lozinki.

Trenutno postavljene kriterije kvalitete lozinki u aplikaciji Knowledge Exchange smatramo uglavnom prihvatljivima no naglašavamo kako se adekvatna razina sigurnosti lozinki postiže korištenjem lozinki od **minimalno 8 znakova (preporučeno 10-12 znakova)** koje se sastoje od **alfanumeričkih** i **specijalnih znakova**. Navedena preporuka se temelji na procjeni vjerojatnosti pogađanja lozinki nastaloj na temelju prosječne procesorske snage dostupnih suvremenih računalnih resursa i algoritama za pogađanje lozinki. Više informacija o aktualnoj problematici kvalitete lozinki može se pronaći na lokaciji:

http://en.wikipedia.org/wiki/Password_strength

Izvještaj o rezultatima certifikacije bit će dostavljen Ministarstvu znanosti, obrazovanja i sporta koje na temelju istog donosi daljnje odluke.

Rezultat certifikacije: **USPJEŠAN**