

# 2013 januari examen

## 26 Januari 2013

- Orden 5 verschillende aanvallen en leg je ordening uit.
- In een dokterskabinet staat een computer met patientengegevens, geef zoveel mogelijk manieren om deze gegevens te verkrijgen.
- Geef zoveel mogelijk voorbeelden (uit teksten of eigen voorbeelden) van hoe je de integriteit van code/tekst kan bewijzen
- Enkele statements met ja/nee en leg uit
  - Een computer met encryptie kan geen dataverlies hebben (Neen, aanvallen zijn nog mogelijk wanneer de computer uitstaat zoals de keys worden uit het werkgeheugen gehaald, backdoors,...)
  - Encryptie zorgt voor integriteit (Neen, veel denken dit maar iets dat geencrypteert is zijn maar bytes wanneer integriteit net is dat je zeker bent dat alles er is ofzoiets)
  - Kan een IDS CSRF aanvallen detecteren (Neen, dit kan hij niet)
- Schrijf op de achterkant van dit blad wat je voor project hebt gemaakt, wat je hebt afgegeven en met wie je evt hebt samengewerkt.

## Maandag 14 januari 2013

1. In een dokterskabinet staat een computer met patientengegevens, geef zoveel mogelijk manieren om deze gegevens te verkrijgen.
2. Zet de volgende 5 vulnerabilities in volgorde van minst naar meest gevaarlijk en hoe ze op te lossen.
3. Juist/fout:
  1. Voor een DOS aanval heb je meerdere computers nodig.
  2. Een IDS kan CSRF aanvallen detecteren.
  3. Een stuk code met een digitale handtekening moet altijd door de gebruiker handmatig gecontroleerd worden.
4. Geef zoveel mogelijk voorbeelden (uit teksten of eigen voorbeelden) van "Principle of least privilege"
5. Schrijf op de achterkant van dit blad wat je voor project hebt gemaakt, wat je hebt afgegeven en met wie je evt hebt samengewerkt.

## Maandag 7 januari 2013

1. Geef zoveel mogelijk mogelijkheden om een website onbereikbaar te maken en zeg erbij hoe de eigenaar zich ertegen kan beschermen. Rangschik de technieken van minst naar meest moeilijk.bvb:
  1. (D)Dos Voorkomen: Dos kan gedetecteerd worden, DDos is veel moeilijker
  2. Inbreken op webserver en afsluiten. Voorkomen: up to date houden, Firewall, IDS, ..
  3. DNS cache poisoning Voorkomen: DNSSec
  4. ARP poisoning Voorkomen: bvb statische MAC adressen instellen
  5. Fysiek onklaar maken: kabel uittrekken/oversnijden of electriciteit uitzetten.  
Voorkomen: serverruimte beveiligen en UPS
2. 5 exploits over Microsoft producten die je moet rangschikken op basis van meest belangrijkste eerst oplossen en wat doen als er nog geen patch beschikbaar is:
  1. attacker can execute remote code when user open specially crafted office file with embedded content. -> redelijk erg: kan bvb als attachment binnenkomen.
  2. attacker can execute remote code when user browses to dir with certain subfile/subdir with special name. -> voor interpretatie vatbaar
  3. On a SQLite server, certain custom made FTP packets may reveal information (ongeveer). -> niet zo leuk maar er wordt geen data aangepast
  4. XSS attack on SSRS page, user may elevate privilege mode and execute remote code as target user. -> zeer gevaarlijk. privileges zijn er voor een reden. Bovendien is 'SSRS' de admin pagina (volgens Gerben) dus kan bvb de admin cookie gestolen worden
  5. Remote desktop may execute remote code when certain custom made packets are received. Remote desktop is standard disabled under Windows. -> Hangt van situatie af. gebruikt bedrijf Remote Desktop? oplossen: whitelisting van RD gebruikers
3. juist/fout + uitleg
  1. een proces in een sandbox zonder rechten is nutteloos -> Niet waar, een process hoeft geen gebruik te maken van externe resources. (niet 100% zeker van antwoord, verificatie nodig)
  2. een certificaat dat niet ondertekend is door een CA is niet handig. -> Niet waar, bvb eigen certificaten of vreemde certificaten toevoegen om later MITM te voorkomen
  3. een site waar geen invoervelden zijn daar kan een hacker in het slechtste geval de hele databank op het scherm dumpen. -> Hangt ervan af: welke privileges heeft SQL-server? Stored procedures gebruikt? Welke rechten heeft de user: READ/WRITE/UPDATE?
4. geef zoveel mogelijk voorbeelden van slechte security door gebruikers/gebruiksvriendelijkheid
5. schrijf op de achterkant wat je project was en met wie je eventueel samenwerkte en wat je geüpload hebt. (en dan een paar vraagjes)

---

Revision #1

Created 31 October 2021 22:24:53 by Jasper G.

Updated 16 January 2022 15:02:33 by Jasper G.