InformacijskaVarnost.zip

IT varnost po razkritju aktivnosti NSA

mag. Borut Žnidar, *CISSP, CISA*

borut.znidar@astec.si

si.linkedin.com/in/borutznidar/

Astec d.o.o.
Stegne 31
SI-1000 Ljubljana

T: 01 / 200 83 00
E: info@astec.si
W: www.astec.si

Vsebina

- NSA zgodba
- Tehnologija zaščite
- Revizija varnosti
- Varnost v razvoju programskih rešitev
- Postavitev in upravljanje varnostnih rešitev

Astec varnostne novice

Hekerji ukradli 250.000 Twitter računov

Hekerji so prevzeli p
gesel in e
prestrege
prevzetin
u

Previdr

Raziskova

Uporabniki Evernote morajo spremeniti gesla

Neznani hekerji so pridobili podatke o uporabnikih (račune, gesla, elektronske nasl

Ranljivost v najnovejši raz

Varnost dosežemo z razpršenostjo

Svetovno priznani strokovnjak za informacijsko varnost Bruce Schneier v intervjuju za National

atrjuje,
odatke
.
nega

Stuxnet - črv, ki me
starejši, kot so misl

Na srečanju med Iranom i
prejšnji teden potekalo v K
javnosti, da je bil črv Stuxn
kot so mislili doslej. Venda
mnogo milejša od novejših
ranljivost sistema delovan
urana. Verzije iz let 2009 i
sedem ranljivosti.
Preberite celotni članek.

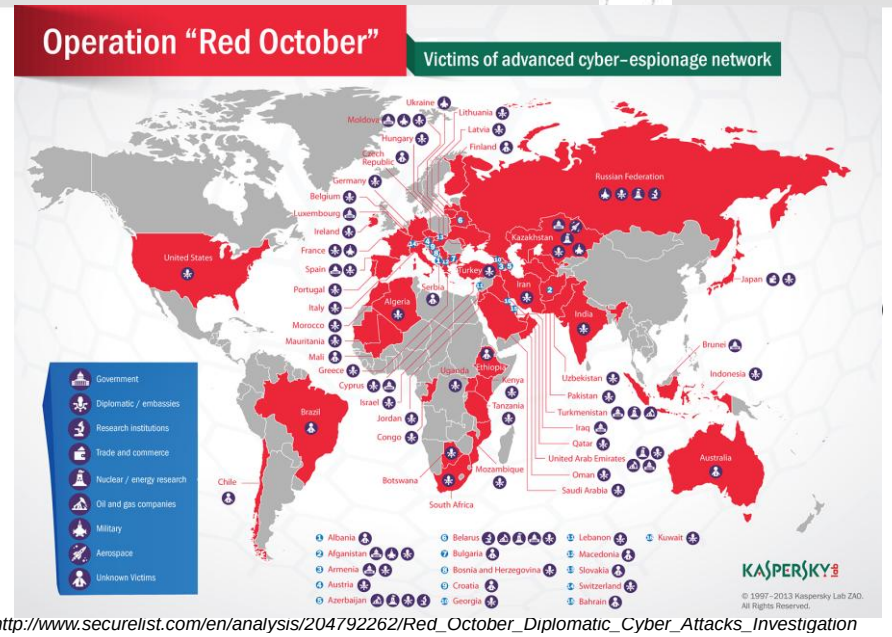
Ruske radarje onesposobil trojanec

V Rusiji se oblasti spopadajo s "sovražniki" policijskih radarjev. Trojanec je napadel radarje, potem ko je podjetje SK Region, ki izdeluje radarje, izgubilo 172 milijonov vreden razpis za vzdrževanje radarske opreme. Zaradi nedelovanja naprav je na razpisu izbrano podjetje IntechGeoTrans že skoraj izgubilo vzdrževalno pogodbo, nato po
strežnika na policiji v Moskvi
radarske naprave. Preberite

nika,

Prijava na Varnostne novice

Operacija **Red October**



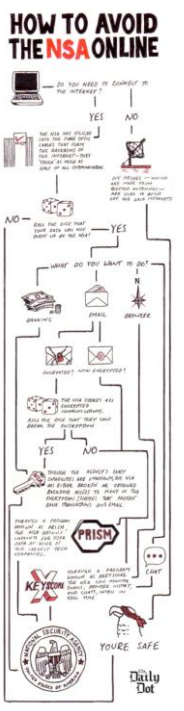
http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation

Svet po Snowdenu
Kaj smo se naučili?
Slovenija?
Mi?

NSA zgodba

NSA, kot ga pokaže Edward Snowden

- Prisluškujejo vsemu na Internetu:
  - 20 milijard „dogodkov“ dnevno,
  - Dosegljivo NSA analitikom v 60 minutah
- Razbili večino šifriranj
- Zaloga ranljivosti, ki jih uporabijo za vdiranje v ciljne računalnike
- NSA deli tehnologijo z ostalimi v skupini “Five eyes”: USA, Canada, UK, Australia, New Zealand



Zmožnosti NSA

Razbita večina šifriranja na Internetu

- Dogovor za prisluškovanje s Telco operaterji v ZDA in Angliji
- Mrežne naprave z vključenim prisluškovanjem
- Backdoor in oslabljena implementacija šifriranja

  DES dolžina ključa, CryptoAG,
  _NSAKEY v Windows NT, Lotus Notes key,
  Dual_EC_DRBG random generator v Windows Vista,
  SHA-3?
- Napad na Tor omrežje
  - Iskanje Tor uporabnikov → Firefox ranljivosti → FOXACID
- Hecking, npr. NSA+UK →BelgaCom (EU institucije)
  - Quantum Insert attack: MitM na Google strežnike → FOXACID
- FOXACID
  - Bogata zbirka za izrabo ranljivosti: od neznanih in nepopravljenih do znanih
  - http://baseball2.2ndhalfplays.com/nested/attribs/bins/1/define/forms9952_z1zzz.html
  - Analiza tveganja: cost-benefit glede na vrednost tarče in tehnično zahtevnost

Kaj pa mi?

Kako ostati varen pred NSA (Bruce Schneier):

1. **Hide** in the network. E.g. Tor
   The less obvious you are, the safer you are.
2. **Encrypt** your communications.
   E.g. TLS, IPsec. *You're much better protected than if you communicate in the clear.*
3. If you have something really important, use an **Air Gap**.
   Might not be bulletproof, but it's pretty good.
4. Be **suspicious of commercial** encryption software, especially from large vendors.
5. Try to use **public-domain encryption** that has to be compatible with other implementations.
   - TLS vs. BitLocker.
   - Prefer symmetric cryptography over public-key cryptography.
   - Prefer discrete-log-based systems over elliptic-curve systems.

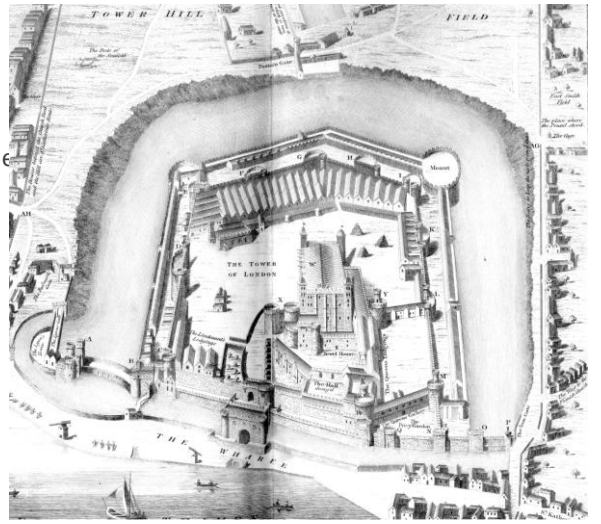
Trdnjava → Letališče
Zrelostna pot varnosti
Šifriranje
Certifikati

Tehnologije zaščite

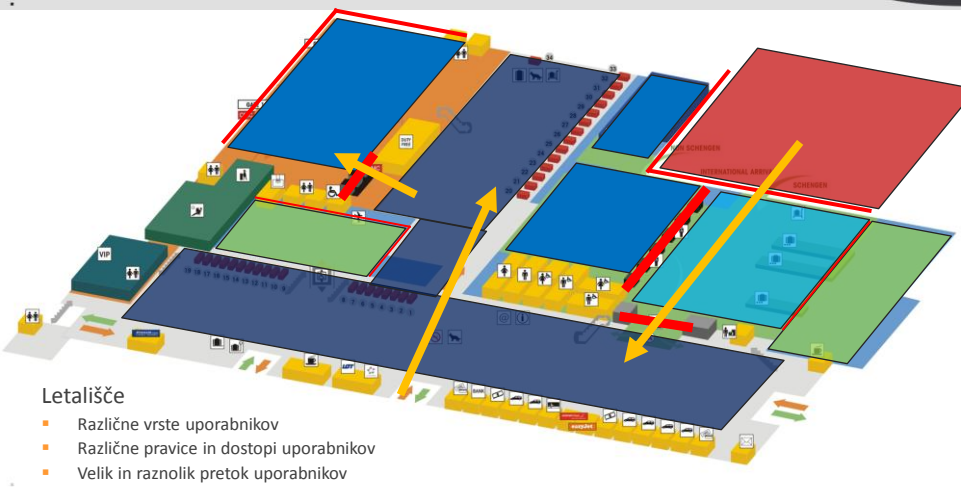
Informacijska varnost – včeraj

Trdnjava

- The Tower of London
- Dobro definirana varnostna področja: Zunanji svet, Okolica, Obrambno področje, Notranjost
- Močna zaščita med posameznimi področji
- Definirani ozki in dobro nadzorovani prehodi
- Majhna prepustnost prehodov
- Zaupanje v notranje ljudi, nezaupanje v zunanje ljudi



Informacijska varnost – danes



Letališče

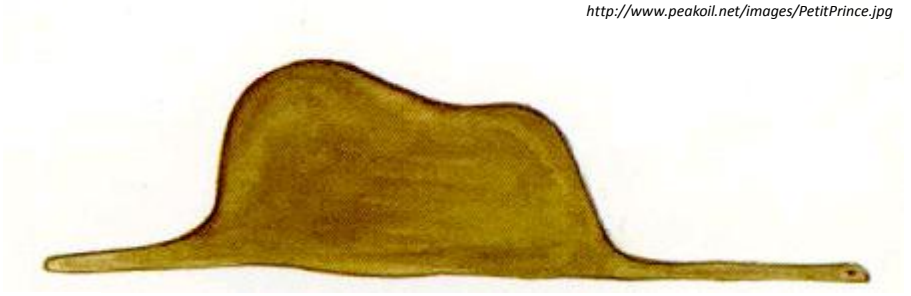
- Različne vrste uporabnikov
- Različne pravice in dostopi uporabnikov
- Velik in raznolik pretok uporabnikov
- Različne vrste storitev
- Velika varnostna izpostavljenost
- Raznoliki in prekrivajoči se mehanizmi za zagotovitev delovanja in varnosti
- Varnost ne sme omejevati delovanja

Zagotovitev varnosti:

- Različne **varnostne cone** in **tokovi** potnikov

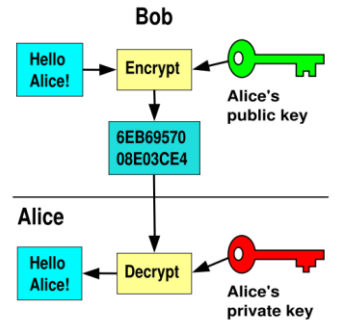
Zrelostna pot varnosti

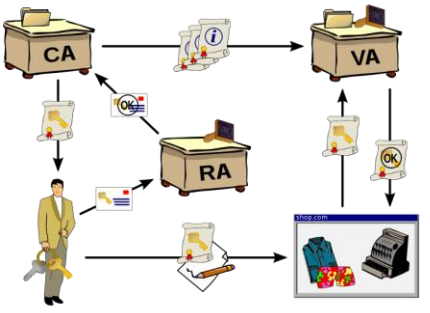
vir:
http://www.peakoil.net/images/PetitPrince.jpg



Šifriranje

- Simetrični ključi
  (DES, TripleDES, AES, RC5)
- Asimetrični ključi
  (RSA, Ellyptic curve)
- Enosmerne Hash funkcije
  (MD5, SHA-1)
- Šifriranje
- Podpisovanje
- Certifikati
- PKI infrastruktura



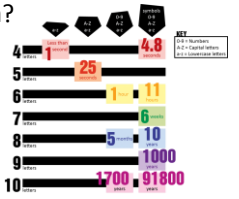


Uporabniška gesla

Namen: zaščita podatkov

Izbiranje gesel

1. Kako hekerji ugibajo gesla?
2. Dolžina in kompleksnost.
3. Domišljija pri izboru.



Uporaba gesel

1. Shranjevanje – Kje?
2. Različna gesla za različne namene (služba / banka / socialna omrežja)
3. Postopki ob izgubi oz. pozabljanju.
4. Skupinska gesla.
5. Ne „posojajte“. Niti po telefonu. ☹

Slovenska

1. 123456
2. 111111
3. geslo
4. slovenija
5. 654321
6. adidas
7. lasko
8. simpsons
9. asdfasdf
10. abrakadabra

Google

1. Ime hišnega ljubljenčka
2. Pomembni datumi
3. Datum rojstva bližnje osebe
4. Ime otroka
5. Ime člana družine
6. Rojstni kraj
7. Priljubljeni praznik
8. Nekaj v zvezi z najboljšo športno ekipo
9. Ime trenutnega partnerja
10. Beseda „password“

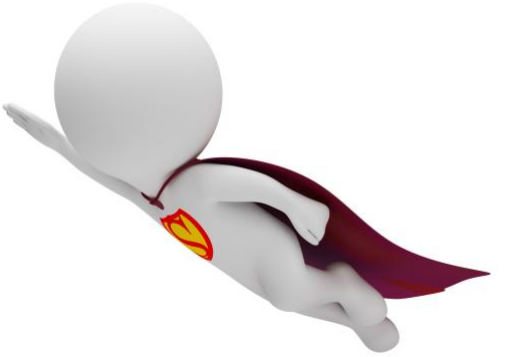
Varnostni pregled / Etični heking

Pregled industrijskih sistemov

Man-In-the-Middle

Računalniška forenzika

Revizija varnosti



Tipične ranljivosti IKT infrastrukture

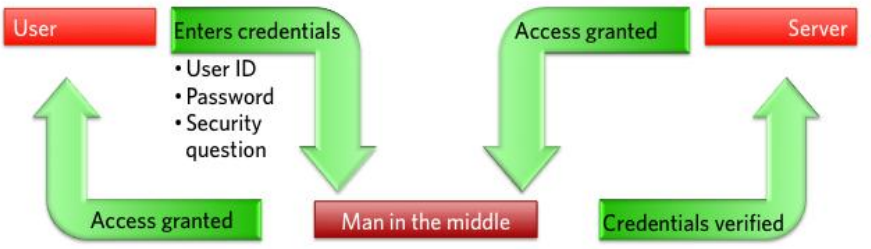
1. Nepodprti (out-of-support) strežniški operacijski sistemi
2. Nenadgrajena (unpatched) strežniška programska oprema
3. Nenadgrajeni Sistemi za upravljanje vsebin (CMS)
4. Omogočene nepotrebne storitve
   - NTP, FTP, RDP, VNC, DB
5. Dosegljivi testni/razvojni strežniki
   - Zelo ranljivi
   - S kopijo produkcijskih podatkov
6. Privzeta gesla za administracijo oz. uporabo storitev

Glavne ranljivosti pri varnostnih pregledih v Sloveniji

1. Nepravilna avtorizacija dostopov do podatkov,
2. Neustrezna avtentikacija uporabnika,
3. XSS (cross-site scripting),
4. Neoptimalno upravljanje uporabniške seje,
5. Konfiguracija in posodobljenost HTTP strežnika.

Man-in-the-Middle napad

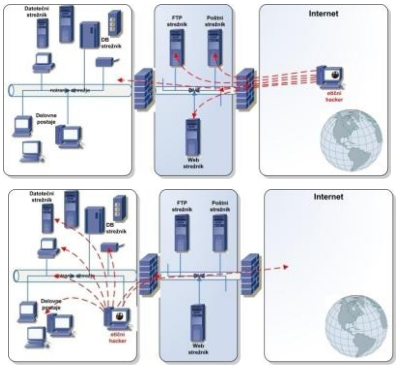
- ARP spoofing
- Le client avtentikacija
- Zasebna Wifi točka
- Zasebna bazna postaja

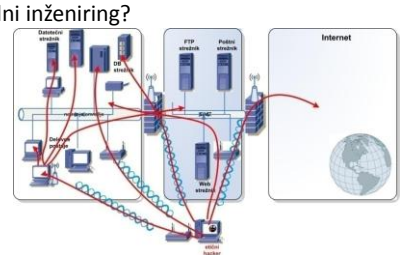


Varnostni pregled / Etični heking

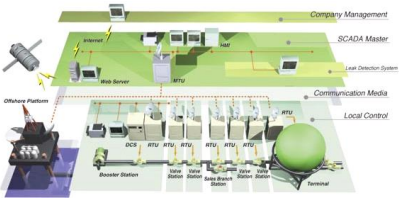
Neodvisni varnostni pregled Informacijske infrastrukture in aplikacij

- Testiranje iz Interneta ali iz podjetja?
- Testiranje zunanjega napadalca ali zaposlenega?
- Brezžične ali žične povezave?
- Mobilne naprave?
- Slepo ali znano okolje?
- Spletni strežnik? Aplikacija? Podatkovni strežnik?
- Izvorna koda?
- Denial of Service (DoS, DDos)?
- Socialni inženiring?





Industrijski (Scada) sistemi

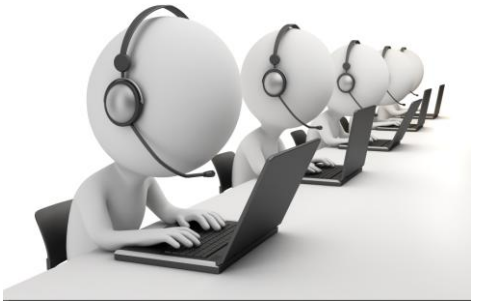


Uporaba

- Vodni sistemi, sistemi odpadnih voda,
- Naftni in plinski sistemi,
- Prenos in distribucija električne energije,
- Nadzor zgradb, letališč, ladij, vesoljskih sistemov,
- HVAC, nadzor dostopa, poraba energije.

Glavne varnostne ranljivosti

- Pomanjkanje varnosti ob načrtovanju, vpeljavi in upravljanju,
- Povezava Scada sistem s poslovnim omrežjem in Internetom,
- Standardni operacijski sistemi (Windows, Linux): Splošni, ranljivosti, ne-nadgrajevanje,
- Specializirani in zaprti protokoli – Security by Obscurity,
- Ranljivosti SCADA programske opreme,
- Fizično varovanje,
- Avtentikacija naprav.

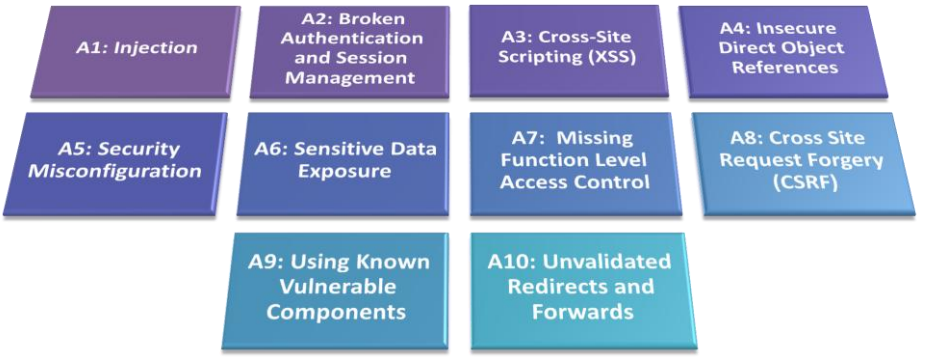


OWASP Top-10

Priporočila za programerje

Varnost pri razvoju programske opreme

OWASP Top Ten 2013



2013-A1 – Injection

Injection means…

- Tricking an application into including unintended commands in the data sent to an interpreter

Interpreters…

- Take strings and interpret them as commands
- SQL, OS Shell, LDAP, XPath, Hibernate, etc…

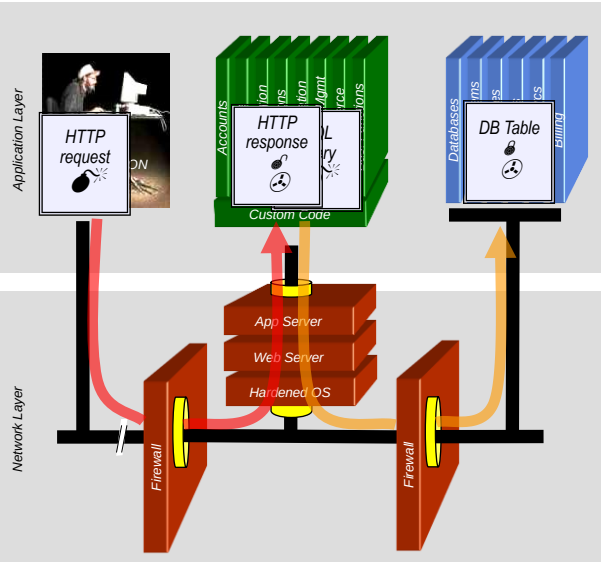
SQL injection is still quite common

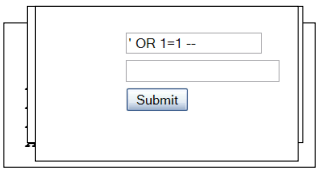
- Many applications still susceptible (really don't know why)
- Even though it's usually very simple to avoid

Typical Impact

- Usually severe. Entire database can usually be read or modified
- May also allow full database schema, or account access, or even OS level access

SQL Injection – Illustrated





1. Application presents a form to the attacker

2. Attacker sends an attack in the form data

3. Application forwards attack to the database in a SQL query

4. Database runs query containing attack and sends encrypted results back to application

5. Application decrypts data as normal and sends results to the user

A1 – Avoiding Injection Flaws

Recommendations

- **Avoid the interpreter entirely, or**
- **Use an interface that supports bind variables (e.g., prepared statements, or stored procedures),**
  - **Bind variables allow the interpreter to distinguish between code and data**
- **Encode all user input before passing it to the interpreter**
- **Always perform 'white list' input validation on all user supplied input**
- **Always minimize database privileges to reduce the impact of a flaw**

References

- **For more details, read the https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet**

A2 – Broken Authentication and Session Management

HTTP is a "stateless" protocol

- Means credentials have to go with every request
- Should use SSL for everything requiring authentication

Session management flaws

- SESSION ID used to track state since HTTP doesn't
  - and it is just as good as credentials to an attacker
- SESSION ID is typically exposed on the network, in browser, in logs, …

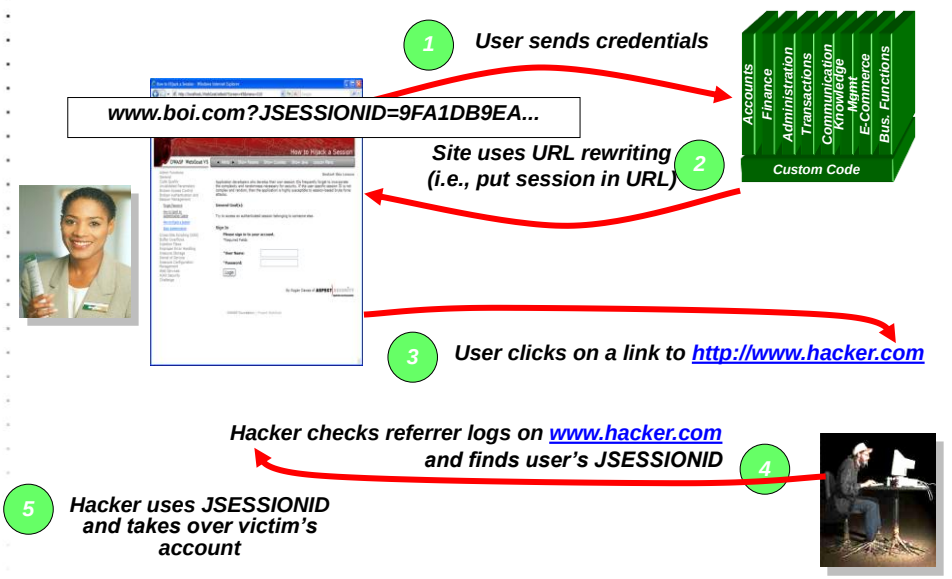
Beware the side-doors

- Change my password, remember my password, forgot my password, secret question, logout, email address, etc…

Typical Impact

- User accounts compromised or user sessions hijacked

Broken Authentication Illustrated



A2 – Avoiding Broken Authentication and Session Management

Verify your architecture

- Authentication should be simple, centralized, and standardized
- Use the standard session id provided by your container
- Be sure SSL protects both credentials and session id at all times

Verify the implementation

- Forget automated analysis approaches
- Check your SSL certificate
- Examine all the authentication-related functions
- Verify that logoff actually destroys the session
- Use OWASP's WebScarab to test the implementation

Follow the guidance from

- https://www.owasp.org/index.php/Authentication_Cheat_Sheet

A3 – Cross-Site Scripting (XSS)

Occurs any time…

- Raw data from attacker is sent to an innocent user's browser

Raw data…

- Stored in database
- Reflected from web input (form field, hidden field, URL, etc…)
- Sent directly into rich JavaScript client

Virtually every web application has this problem

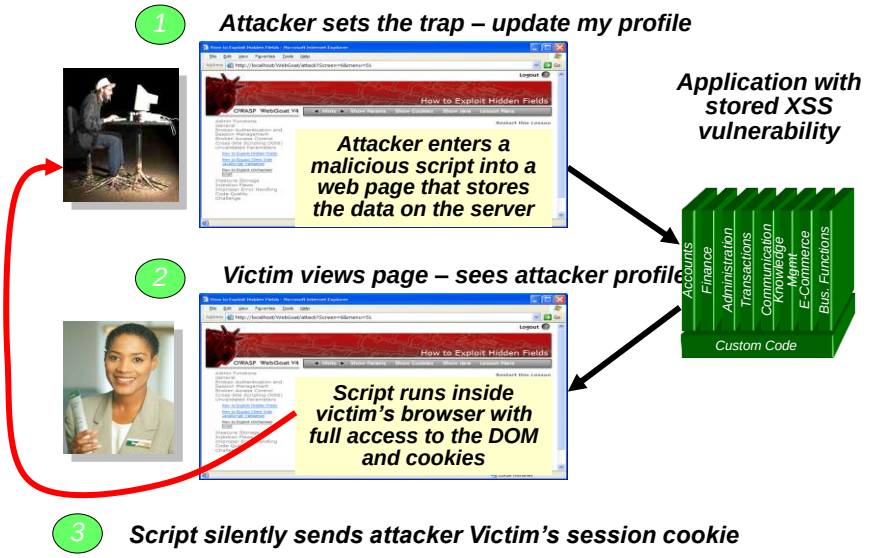
- Try this in your browser – javascript:alert(document.cookie)

Typical Impact

- Steal user's session, steal sensitive data, rewrite web page, redirect user to phishing or malware site
- Most Severe: Install XSS proxy which allows attacker to observe and direct all user's behavior on vulnerable site and force user to other sites

31

Cross-Site Scripting Illustrated



Avoiding XSS Flaws

- **Recommendations**
  - Eliminate Flaw
    - Don't include user supplied input in the output page
  - Defend Against the Flaw
    - Use Content Security Policy (CSP)
    - Primary Recommendation: Output encode all user supplied input (Use OWASP's ESAPI or Java Encoders to output encode)
      https://www.owasp.org/index.php/ESAPI
      https://www.owasp.org/index.php/OWASP_Java_Encoder_Project
    - Perform 'white list' input validation on all user input to be included in page
    - For large chunks of user supplied HTML, use OWASP's AntiSamy to sanitize this HTML to make it safe
      See: https://www.owasp.org/index.php/AntiSamy
- **References**
  - For how to output encode properly, read the https://www.owasp.org/index.php/XSS_(Cross Site Scripting) Prevention Cheat Sheet

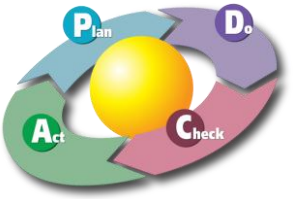

(AntiSamy)

Varnostne naprave
Varnostne rešitve
Operacija Čebula

Postavitev in upravljanje varnostnih rešitev

Osnovni principi varnosti

- Demingov krog
- Zaupnost, Celovitost, Razpoložljivost – CIA

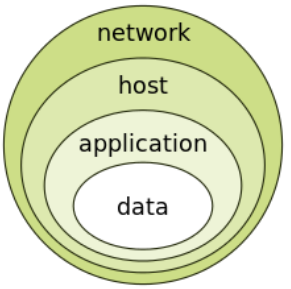


- Delitev odgovornosti (Separation of Duties)
- Princip štirih oči
- Princip najmanjšega privilegija (Least privilege)
- Princip čebule – Globinska obramba (Defence in depth)
- Najšibkejši člen (Weakest link)
- Umri varno (Fail securely)
- Varnostne cone

Postavitev varnostnih rešitev

Princip nivojev

- Vlan
- Network access / 802.1x
- Požarna pregrada
- IPS - odkrivanje vdorov
- Avtentikacija
- IdM
- DLP
- SIEM



?
?
?
?
?