Upplýsingar um gátlista

Gátlistinn er hugsaður sem tól til að aðstoða vefstjóra við framkvæmd prófana á veflausn. Í gátlistanum er að finna upplýsingar um hvað ber að hafa í huga þegar kemur að helstu þáttum sem þurfa að fara gegnum prófanaferli þegar veflausn er innleidd eða gerðar eru uppfærslur eða breytingar á virkni fyrirliggjandi veflausnar.

Gátlistinn er ekki tæmandi og er eingöngu hugsaður sem tól sem vefstjórar geta nýtt til stuðnings við gerð áætlana um prófanir veflausna.

Ekki er ætlast til að vefstjórar búi yfir þekkingu á öllum þeim atriðum sem koma fram í gátlistanum.
Gátlistinn styður við kafla 2.5. Prófanir í UT handbókinni.
Ef vefstjórar nota gátlistann er gott að setja inn athugasemdir þar sem við á og vista eintak af gátlistanum til uppflettingar.

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti til að nýta við framkvæmd prófana á öryggi veflausna.Gátlisti er tæknilegur og krefst töluverðar þekkingar og tæknikunnáttu.

A.2.5 Gátlisti til að nýta við prófanir

Samantekt yfir atriði tengt prófunum

Atriði	Athugasemdir
Aðgangsstýring	
☐ Er stöðugt verið að framfylgja aðgangsstýringu óháð því hvort notandi hafi auðkennt sig? Dæmi um reikningsyfirlit: http://example.com/app/accountInfo?acct=notmyacct - Ef aðgangsstýring væri bundin við auðkenningu en væri ekki stöðugt framfylgt þá væri í þessu dæmi hægt að komast yfir reikningsyfirlit annara aðila.	
☐ Er meginreglum um lágmarksaðgang framfylgt? Þ.e.a.s. eru ákvarðanatökur byggðar á lágmarksréttindum? Er aðgangur almennt óheimilaður nema að hann sé sérstaklega leyfður?	
☐ Er þess gætt að ekki sé notuð bein tilvísun í vefhlut? Er aðgangi stýrt með tilliti til auðkenndra notenda og byggt á upplýsingum miðlaramegin? Sjá dæmi um reikningsyfirlit að ofan.	
☐ Eru notaðar ósannreyndar áframsendingar? Í einhverjum tilfellum getur verið nauðsynlegt að áframsenda notendur á aðrar síður t.d. ef reynt er að fara inn á síðu sem er ekki til. Passa þarf að óprúttnir aðilar geti ekki nýtt sér þetta eins og t.d. á eftirfarandi hátt: http://www.example.com/redirect.jsp?url=evil.com	
Auðkenning	
☐ Tryggja þarf að notendanöfn og lykilorð séu ekki harðkóðuð (skilgreind í forritunarkóða)	
☐ Tryggja að virkni við endursetningu lykilorða á veflausn sé útfærð á öruggan hátt. Ef notast er við öryggisspurningar, þá þurfa þær að vera erfiðar að giska á auk þess sem passa þarf upp á að ekki séu gefnar upplýsingar um hvort viðkomandi notandanafn sé til eða ekki.	
☐ Útfæra þarf læsingu aðgangs ef reynt er að skrá sig inn of oft (til þess að koma í veg fyrir e. „Brute force“ árásir). Hægt er að læsa aðgangi tímabundið. Hér er æskilegt að gefa sömu villuboð eins og þegar aðgangi er læst, rangt lykilorð er slegið inn og þegar að notandi er ekki til	
☐ Passa þarf að villuboð gefi ekki of mikið af upplýsingum. Á sama tíma og villuboð þurfa að vera skýr þá er æskilegt að þau gefi ekki upplýsingar um virk notendanöfn. Forðast ber að nota villuboð sem taka fram að lykilorð sé ekki rétt, það gefur í skyn að notandinn sé til. "Brute force" árásir ganga út á það að reyna mismunandi notendanöfn og lykilorð í þaula þangað til að aðgangi er náð að viðkomandi upplýsingakerfi.	
☐ Veflausn ætti að keyra með lágmarksréttindum. Hér ætti t.d. að takmarka aðgang veflausnarinnar við það sem hún þarf t.d. Les- og skrifaðgang, sem og aðgang að öðrum gögnum og gagnagrunnum sem ekki er þörf á.	
Inntaks og úttaksmeðhöndlun	
☐ Tryggja þarf að úttaksgögn séu kóðuð eftir samhengi áður en þau eru send til notenda. Það fer eftir staðsetningu í HTML kóða hvernig úttak er kóðað. T.d. þurfa gögn sem eru notuð í URL samhengi að vera kóðuð öðruvísi en gögn sem eru notuð í JavaScript samhengi. Dæmi: Ef gert er ráð fyrir því að taka við texta frá notanda sem verður birtur á annari síðu þá ætti ekki að leyfa sértákn sem væri hægt að nota í slæmum tilgangi eins og t.d. "<" og ">" í <script>alert("XSS");</script>	
☐ Nota á hvítlista fram yfir svartlista þegar verið er að taka á móti gögnum frá notendum. Hér er hægt að takmarka inntak einungis við þau tákn sem eru leyfileg. Hægt er að nota svartlista fyrir aukin sveigjanleika. Í stað þess að búa til svokallaðan svartan lista yfir sértákn sem eru ekki leyfð eins og ef við skoðum táknið "<", þá er hægt að tákna það á a.m.k. 70 mismunandi vegu. Hér eru nokkur dæmi: "<", "%3C", “&lt”, “<”, “&LT”, “<”, “&#60”, “&#060”, “&#0060” o.s.frv.	
☐ Passa þarf að nota (e.) Parameterized SQL queries til þess að verjast SQL innspýtingarárásum Dæmi um rétta leið (tekið frá OWASP): String custname = request.getParameter("customerName"); String query = "SELECT account_balance FROM user_data WHERE user_name = ? "; PreparedStatement pstmt = connection.prepareStatement(query); pstmt.setString(1, custname); ResultSet results = pstmt.executeQuery( );	
☐ Nota ætti tákn (e. Token) á vefsíðum til þess að koma í veg fyrir (e.) Cross Site Request Forgery (e. CSRF) Dæmi um CSRF veikleika (tekið frá OWASP): Til þess að fyrirbyggja CSRF árásir ætti að nota óútreiknanlegt token í hverri HTTP fyrirspurn. Slík token ættu í það minnsta að vera einkvæm fyrir hverja notendalotu.	
☐ Passa þarf að innsendar skrár séu sannreyndar. Sannreyna á stærð, tegund, innihald auk þess sem gæta þarf þess að ekki sé hægt að hafa áhrif á hvar skráin er vistuð á miðlara.	
☐ Nota ætti nosniff hausinn: Content-Type-Options: nosniff Sjá nánari upplýsingar um nosniff hausinn: https://www.owasp.org/index.php/List_of_useful_HTTP_headers	
☐ Nota ætti X-Frame-Options til þess að sporna gegn click-jacking árásum	

- [ ]

Sjá nánari upplýsingar um X-Frame-Options hausinn: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

- [ ] Nota ætti CSP eða X-XSS protection til þess að sporna gegn endurspegluðum XSS árásum

Sjá nánari upplýsingar um CSP og X-XSS hausana: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Lotustjórnun

- [ ] Tryggja þarf að Session Identifiers séu nægjanlega óútreiknanlegir (sufficiently random) þannig að árásaraðilar geti ekki giskað á þá og tekið yfir lotu annarra.
- [ ] Eru lotutákn (e. Session Identifier) endurnýjuð? T.d. eftir auðkenningu eða eftir að skipt er milli dulkóðaðra samskipta yfir í ódulkóðuð samskipti eða öfugt
- [ ] Er búið að útfæra sjálfvirka útskráningu notenda sem hafa ekki verið virkir í einhvern tíma?
- [ ] Er lotunotanda lokað ef einhver merki eru um hagræðingu eða svik (e.tampering)?
- [ ] Er lota ógild eftir að notandi hefur skráð sig út?
- [ ] Er útskráningartakki á hverri síðu?
- [ ] Er búið að virkja örugga vafrakökuþætti (e. Cookie attributes) (Httponly and Secure Flags)

Sjá nánari upplýsingar: https://www.owasp.org/index.php/SecureFlag

- [ ] Er búið að stilla vafraköku lén (e. cookie domain) og slóð (e. path) rétt

Sjá nánari upplýsingar: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

- [ ] Er búið að skilgreina endingartíma á vafraköku? Forðast á vafrakökur sem hafa ekki skilgreind gildislok.

Sjá nánari upplýsingar: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Verndun gagna

- [ ] Er SSL dulkóðun notuð alls staðar? Ef ekki er mögulegt að nota SSL alls staðar skal nota SSL á öllum staðfestingarsíðum ásamt þeim síðum þar sem notendur auðkenna sig.

SSL (Secure Socket Layer) er dulkóðunar samskiptastaðall. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Ttext Transfer Protocol), þá er talaða um HTTPS (Hyper Text Transfer Protocol Secured).
TLS (Transfer Layer Security) er dulkóðunar samskiptastaðall sem hefur tekið við af SSL.

- [ ] Er búið að gera HTTP aðgang óvirkan fyrir alla virkni veflausnarinnar sem á að fara yfir SSL/TLS?
- [ ] Er (e.) „Strict-Transport-Security“ hausinn notaður?

Sjá nánari upplýsingar: https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

- [ ] Eru lykilorð vistuð með því að nota nokkrar ítranir af öruggu tætifalli af því ásamt slembigögnum (e. Salt)?
- [ ]

Ef veflausn styðst við/notar dulkóðun, hefur hún þá verið útfærð á þann veg að hún tryggi örugg skipti á dulkóðunarlyklum?

- [ ] Ef dulkóðunarlyklar eru notaðir, er búið að skilgreina sýslunarferli fyrir dulkóðunarlyklana til þess að takmarka aðgang að þeim?
- [ ] Er búið að óvirkja stuðning við veika dulkóðunarmöguleika yfir SSL?
- [ ] Eru rafræn skilríki sem notuð eru við SSL samskipti gefin út af traustum aðilum (e. Trusted certificate authority)?
- [ ] Er búið að óvirkja geymslu gagna í flýtiminni (e. Data caching) með því að nota HTTP hausa eða metatag?
- [ ] Er búið að takmarka notkun og geymslu viðkvæmra gagna.

Villumeðhöndlun og atvikaskráning

- [ ]

Er einungis birt almenn villuskilaboð? Þ.e.a.s. án þess að birta smáatriði um innra ástand hugbúnaðarins (e. Application)?

- [ ] Er þess gætt að allar undantekningar (e. Exception) séu meðhöndlaðar?
- [ ] Er passað upp á að gefa ekki upp viðkvæmar upplýsingar við villumeldingar?
- [ ] Eru allar auðkenningar (e. Authentication activities) skráðar (e. Log) sama hvort þær heppnist eður ei?
- [ ] Eru allar breytingar á réttindum skráðar (e. Log)? T.d. ef réttindastig notanda breytist ætti að skrá það.
- [ ] Eru allar stjórnunarbreytingar (e. Administrative changes) skráðar (e.Log)?
- [ ] Er allur aðgangur að viðkvæmum gögnum skráður (e. Log)? Þetta á sér í lagi við stofnanir sem þurfa að hlíta ákveðnum stöðlum um öryggi og meðhöndlun gagna
- [ ] Er þess gætt að óviðeigandi gögn séu ekki skráð? Gögn sem flokkast sem óviðeigandi gögn eru t.d. viðkvæm gögn (e. Sensitive data)
- [ ] Eru skráningar (e. Logs) geymdar á öruggan hátt og þannig komið í veg fyrir gagnatap eða breytingar af hálfu tölvuþrjóta?