OWASP Topp 10 2013

De 10 allvarligaste riskerna i webbapplikationer

2013-10-03
OWASP East Sweden: Uppstartsmöte

Vad är OWASP Topp 10?

- Är ett av OWASP mest populära projekt
- Är inte en standard
- Fokuserad på att hantera risker, inte bara undvika dem
- Riktar sig till utvecklare, inte enbart säkerhetsintresserade
- Finns på engelska, franska, kinesiska, koreanska och portugisiska
  - Snart på svenska ☺
- Refereras av bl.a. MITRE, PCI DSS, DISA, FTC m.fl.
- Underhålls av Aspect Security
- Begränsa er inte till OWASP topp 10!

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP East Sweden

Siffror

- Första versionen kom 2003, baserad på förekomst
- Andra versionen kom redan 2004, därefter vart tredje år (2007, 2010, 2013)
- Från version 2010 och framåt baseras listan på risk
- Bygger på 8st datainsamlingar från 7st företag
  - 4 konsultfirmor
  - 3 programföretag
  - 500 000 sårbarheter

OWASP East Sweden

Värdering

Värderas och prioriteras efter OWASP riskvärderings-metod;

- **Exploaterbarhet:** Svårt, Medel, Lätt
- **Förekomst:** Ovanlig, Vanlig, Välspridd
- **Upptäckbarhet:** Svårt, Medel, Lätt
- **Påverkan:** Lite, Begränsad, Allvarlig

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

OWASP East Sweden

A1 Injektion

”Injektionsbrister, såsom SQL-, OS- och LDAP-injektioner, uppstår när opålitlig data skickas till en interpreterare som en del av ett kommando eller fråga. Attackerarens illasinnade data kan lura interpretatorn att exekvera oönskade kommandon eller komma åt skyddad data.”

Exploaterbarhet: Lätt (3)
Förekomst: Vanlig (2)
Upptäckbarhet: Medel (2)
Påverkan: Allvarlig (3)

OWASP East Sweden

A1 Injektion - exempel

```
query = "SELECT * FROM pages WHERE id=" + http.get[id] + ";"
http://example.com/?id=1                        => SELECT * FROM pages WHERE id=1;
http://example.com/?id=1337                     => SELECT * FROM pages WHERE id=1337;
http://example.com/?id=1;%20DROP%20pages        => SELECT * FROM pages WHERE id=1; DROP pages;

query = "SELECT * FROM pages WHERE id='" + http.get[id] + "';"
http://example.com/?id=1                        => SELECT * FROM pages WHERE id='1';
http://example.com/?id=1337                     => SELECT * FROM pages WHERE id='1337';
http://example.com/?id=1;%20DROP%20pages        => SELECT * FROM pages WHERE id='1; DROP pages';
http://example.com/?id=1';%20DROP%20pages;--%20  => SELECT * FROM pages WHERE id='1'; DROP pages;-- ';

query = "SELECT * FROM pages WHERE id='" + (int)http.get[id] + "'";
query = "SELECT * FROM pages WHERE id='#param1'", http.get[id];
```

OWASP East Sweden

A2 Bristfällig autentisering och sessionshantering

”Funktionalitet relaterat till autentisering och sessionshantering är inte alltid korrekt implementerade. Detta kan leda till att en attackerare får tillgång till lösenord, nycklar, sessionsbiljetter eller på annat vis kan överta en annan användares identitet.”

Exploaterbarhet: Medel (2)
Förekomst: Välspridd (3)
Upptäckbarhet: Medel (2)
Påverkan: Allvarlig (3)

OWASP East Sweden

A2 Bristfällig autentisering och sessionshantering - exempel

Sessions-ID i URL:n

```
http://example.com/?sessionid=T1dBU1AgRWFzdCBTd2VkZW4=
```

Sessions-ID inte som HTTP-only

```
Set-Cookie: sessionid=T1dBU1AgRWFzdCBTd2VkZW4=; Domain=example.com; Path=/; HttpOnly
```

Lösenord lagras i klartext

```
+----+-------------+----------+
| id | username    | password |
|----|-------------|----------|
|  1 | admin       | password |
|  2 | servicedesk | 123456   |
+----+-------------+----------+
```

Andra exempel

- Återställ lösenord-svaret inte krypterat
- Inloggningen kvar efter stängt ner webbläsaren, t.ex. bibliotek

Återuppfinn inte hjulet – använd befintliga lösningar!

OWASP East Sweden

A3 Cross-site scripting (XSS)

”XSS-brister uppstår när en applikation tar opålitlig data och sänder den till besökarens webbläsare utan korrekt validering eller escaping. XSS möjliggör attackerare att exekvera skript i offrets webbläsare vilket kan kapa sessioner, byta ut element på sidan eller omdirigera till en annan skadlig hemsida.”

Exploaterbarhet: Medel (1)
Förekomst: Väldigt välspridd (4)
Upptäckbarhet: Lätt (3)
Påverkan: Begränsad (2)

OWASP East Sweden

A3 Cross-site scripting (XSS) - exempel

Reflekterad

```
html = "<h1>Söker efter '" + http.get[query] + "'</h1>"
http://example.com/?query=n%E5got%20oskyldigt
  => <h1>Söker efter 'något oskyldigt'</h1>
http://example.com/?query=%3Cscript%3Edocument.write(document.cookie);%3C/script%3E
  => <h1>Söker efter '<script>document.write(document.cookie);</script>'</h1>
```

Lagrad

```
html = "<b>Författare:</b> " + sql.row[author] + "<br />" + sql.row[comment]
```

OWASP East Sweden

A3 Cross-site scripting (XSS) - exempel

DOM-baserad

```
Välj språk:
<select>
  <script>
    url = decodeUri(document.location.href);
    document.write("<option>" + url.substring(url.indexOf("lang=") + 5) + "</option>");
    document.write("<option>Engelska</option>");
  </script>
</select>


http://example.com/?lang=Svenska
  => Välj språk:
     <select>
       <option>Svenska</option>
       <option>Engelska</option>
     </select>
```

OWASP East Sweden

A3 Cross-site scripting (XSS) - exempel

DOM-baserad

```
Välj språk:
<select>
  <script>
    url = decodeUri(document.location.href);
    document.write("<option>" + url.substring(url.indexOf("lang=") + 5) + "</option>");
    document.write("<option>Engelska</option>");
  </script>
</select>
```

```
http://example.com/?lang=%3Cscript%3Ealert(document.cookie);%3C/script%3E
  => Välj språk:
     <select>
       <option><script>alert(document.cookie);</script></option>
       <option>Engelska</option>
     </select>
```

OWASP East Sweden

A3 Cross-site scripting (XSS) - exempel

DOM-baserad

```
Välj språk:
<select>
  <script>
    url = decodeUri(document.location.href);
    document.write("<option>" + url.substring(url.indexOf("lang=") + 5) + "</option>");
    document.write("<option>Engelska</option>");
  </script>
</select>


http://example.com/#lang=%3Cscript%3Ealert(document.cookie);%3C/script%3E
  => Välj språk:
     <select>
       <option><script>alert(document.cookie);</script></option>
       <option>Engelska</option>
     </select>
```

OWASP East Sweden

A4 Osäkra direktreferenser

”En direktreferens uppstår när en utvecklare exponerar en referens till ett internt objekt, t.ex. en fil, mapp eller databasrad. Utan tillräcklig verifiering eller andra kontroller kan en attackerare modifiera referensen för att få tillgång till skyddad data.”

Exploaterbarhet: Lätt (3)
Förekomst: Vanlig (2)
Upptäckbarhet: Lätt (3)
Påverkan: Begränsad (2)

OWASP East Sweden

A4 Osäkra direktreferenser - exempel

Icke-validerad kontoinformation

```
http://example.com/account_info?id=1
http://example.com/account_info?id=1337
```

Obegränsad filtillgång

```
http://example.com/documents/internal_report.pdf
```

Katalogtraversering

```
http://example.com/show_file?file=../../etc/passwd
```

OWASP East Sweden

A5 Felaktig konfiguration

”Bra säkerhet kräver en säker konfiguration för applikationer, ramverk, applikations-, webb- och databasservrar och inte minst operativsystemet. Säkerhetsinställningen bör vara definierade, implementerade och underhållna, då standardinställningar ofta är osäkra. Slutligen bör all mjukvara hållas uppdaterade.”

Exploaterbarhet: Lätt (3)
Förekomst: Vanlig (2)
Upptäckbarhet: Lätt (3)
Påverkan: Begränsad (2)

OWASP East Sweden

A5 Felaktig konfiguration - exempel

Standardlösenord

```
mysql –u root –p root
```

Pratsamma felsidor

```
Microsoft OLE DB Provider for SQL Server error '80040e07'
Conversion failed when converting the nvarchar value 'liljon' to data type int.
```

Gammal mjukvara

```
uname –a
Debian GNU/Linux 4.0 (2.6.30.5-ph33r)
```

OWASP East Sweden

A6 Exponering av känslig data

”Många webbapplikationer saknar tillräckligt skydd av känslig data, t.ex. kreditkortsnummer, personuppgifter och inloggningsuppgifter. Attackerare kan stjäla eller modifiera data för att genomföra kreditkortbedrägeri, identitetsstöld och andra brott. Känslig data förtjänar extra åtgärder, såsom kryptering både vid lagring och transport.”

Exploaterbarhet: Svårt (1)
Förekomst: Ovanlig (1)
Upptäckbarhet: Medel (2)
Påverkan: Allvarlig (3)

OWASP East Sweden

A6 Exponering av känslig data - exempel

Okrypterad trafik

```
http://example.com/do_login
```

Skyddad data säkerhetskopieras till oskyddad disk

```
rsync /var/www backupuser@backupserver:/var/www
```

Lösenord lagras i klartext

```
+----+-------------+----------+
| id | username    | password |
|----|-------------|----------|
|  1 | admin       | password |
|  2 | servicedesk | 123456   |
+----+-------------+----------+
```

OWASP East Sweden

A7 Bristande åtkomstkontroll på funktionsnivå

”De flesta webbapplikationer verifierar funktionsrättigheter när funktionen görs synlig för användaren, däremot saknas samma kontroll när funktionen utförs. Ifall en funktionsbegäran inte kontrolleras kan en attackerare utan rätt behörighet utföra funktionen.”

Exploaterbarhet: Lätt (3)
Förekomst: Vanlig (2)
Upptäckbarhet: Medel (2)
Påverkan: Begränsad (2)

OWASP East Sweden

A7 Bristande åtkomstkontroll på funktionsnivå - exempel

Icke-validerad kontoadministration

```
http://example.com/edit_account?id=1
http://example.com/edit_account?id=1337
```

Ingen rättighetskontroll back-end

```
http://example.com/api/account/delete/1
```

OWASP East Sweden

A8 Cross-site request forgery (CSRF)

”En CSRF-attack tvingar en inloggad offers webbläsare att skicka en HTTP-begäran, inkl. offrets kakor eller andra autentiseringsuppgifter, till en sårbar webbapplikation. Detta möjliggör för en attackerare att skapa begäran som den sårbara applikationen tror är legitima begäran från offret.”

Exploaterbarhet: Medel (2)
Förekomst: Vanlig (2)
Upptäckbarhet: Lätt (3)
Påverkan: Begränsad (2)

OWASP East Sweden

A8 Cross-site request forgery (CSRF) - exempel

Get-parametrar utan hemlighet

```
https://examplebank.com/transfer_funds?amount=1500&dest_acc=12345678
```

```
<img src="https://examplebank.com/transfer_funds?amount=1500&dest_acc=13371337" />
```

Post-parametrar utan hemlighet

```
<form action="change_password" method="post">
  <input type="password" name="new_password" />
  <button type="submit" />
</form>
```

```
xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "http://example.com/change_password", true);
xmlhttp.setRequestHeader("Content-type","application/x-www-form-urlencoded");
xmlhttp.send("new_password=lolichangedyourpassword");
```

OWASP East Sweden

A9 Använda komponenter med kända sårbarheter

”Komponenter, t.ex. bibliotek, ramverk eller andra moduler, kör nästan alltid med fulla rättigheter. Ifall en sårbar komponent utnyttjas kan en sådan attack åsamka stora skador. Applikationer som använder sårbara komponenter kan underminera säkerhetsåtgärder och öppnar för en rad möjliga attackvektorer.”

Exploaterbarhet: Medel (2)
Förekomst: Välspridd (3)
Upptäckbarhet: Svårt (1)
Påverkan: Begränsad (2)

OWASP East Sweden

A9 Använda komponenter med kända sårbarheter

- Aspect Security & Sonatype analyserade nerladdningar från Maven
  - 31st bibliotek
  - 61 800 organisationer
  - 113,9 miljoner nerladdningar under 2011

https://www.aspectsecurity.com/news/the-unfortunate-reality-of-insecure-libraries/

OWASP East Sweden

A10 Ickevaliderade vidarebefordringar

”Webbapplikationen dirigerar ofta om användare till andra sidor och hemsidor och använder opålitlig data för att avgöra destinationen. Utan tillräcklig validering kan en attackerare vidarebefordra offer till phising- eller malware-siter, eller använda vidarebefordringen för att ge sig själv tillgång till skyddade sidor.”

Exploaterbarhet: Medel (2)
Förekomst: Ovanlig (1)
Upptäckbarhet: Lätt (3)
Påverkan: Begränsad (2)

OWASP East Sweden

A10 Ickevaliderade vidarebefordringar - exempel

Ickevaliderad vidarebefodran

```
http://example.com/redirect?url=google.com
http://example.com/redirect?url=malware.nu
http://example.com/redirect?url=example.ru
```

Ickevaliderad intern vidarebefordran

```
http://example.com/wizard?next_step=db_config
```

OWASP East Sweden

Tack!

Frågor?

David Johansson, Gustav Nyqvist, Åke Bengtsson
david.johansson@owasp.org, gustav.nyqvist@owasp.org, ake.bengtsson@owasp.org