XSS Attacks

Session Hijacking using XSS

ZDResearch

www.zdresearch.com

ZDResearch Advanced Web Hacking

Exdemy.com
Personal property of Keith Samborski
l_my69@yahoo.com

Copyright © Exdemy.com

Session hijacking using XSS

- In the first attempt in the lecture, why didn't we obtain PHPSESSID?
- Does the second attempt (grabbing cookies from headers) will always work?

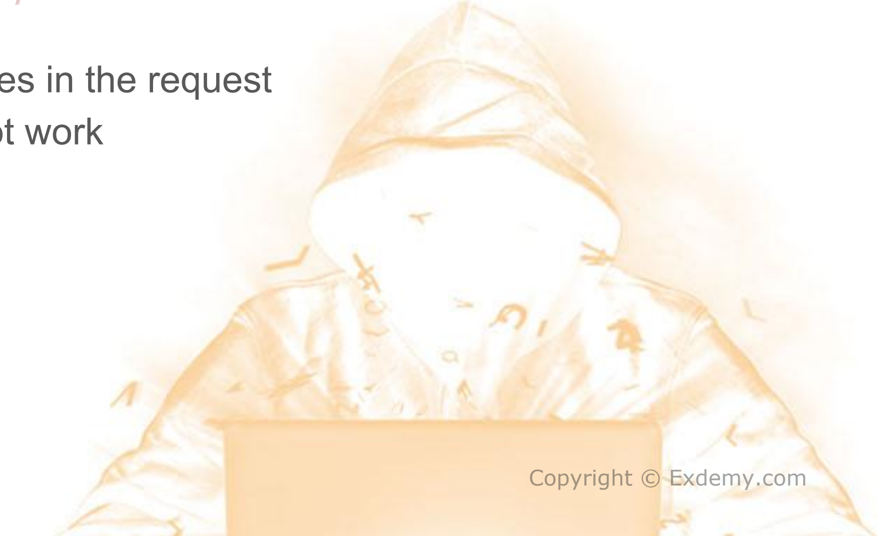
Exdemy.com
Personal property of Keith Samborski
l_my69@yahoo.com

Copyright © Exdemy.com

Session hijacking using XSS - Solution

- Q1:
  - Because PHPSESSID cookie had the secure flag (httponly) and was not accessible through Javascript code
- Q2:
  - No. Because in this example our Cookie Grabber was on the same domain and cookie path as the vulnerable application
  - The cookie domain let the browser send cookies in the request
  - But in real-world scenarios, this method will not work

Exdemy.com
Personal property of Keith Samborski
l_my69@yahoo.com



ZDResearch

Copyright © Exdemy.com

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com

Exdemy.com
Personal property of Keith Samborski
l_my69@yahoo.com

Copyright © Exdemy.com