

Destructor

I had a lot of fun during the process of writing this. I truly hope that you learned something new and enjoyed reading this.

You've learned a bit about protecting your applications from users, and users from themselves; securing your communication via HTTPS; safe password encryption techniques; role-based access control; and about popular attack vectors.

Please get in contact¹ if you want to learn more about any of the subjects covered here or just argue over the meaning of life.

Thanks for reading.

¹feedback@buildsecurephpapps.com.

Index

■ A

Access control, 33–40, 49
Algorithms, 10, 18–23, 25–27, 29
Apache, 14–15, 39
API, 7, 28, 37
Authentication, 10, 20, 23, 27–29, 33–41

■ B

BCrypt, 21–22, 28, 30
Brute force, 28

■ C

Caching, 11
Certificate authority, 10, 12–14
Collision attacks, 18–19
Cross site request forgery (CSRF), 44–46
Cross site scripting (XSS), 41–47
Cryptography, 31
CSRF. *See* Cross site request forgery (CSRF)

■ D

Dynamic typing, 42

■ E

Encryption, 11–12, 17–31, 49
Escaping Input, 3

■ F, G

File handling, 33–40

■ H, I, J, K

Hashing, 18, 20–23, 26, 29, 38
HTTPS, 9–16, 49

■ L

Lookup tables, 18–19

■ M

Man in the middle, 9–10, 12
Mass assignment, 4–5
MD5, 20–21, 28, 30

■ N

NGINX, 15
Nonce, 45

■ O

Obfuscation, 37–38
One time use token, 44–46

■ P, Q

Parameterized queries, 3
Passwords, 2, 17–31, 34, 41, 49
PDO, 3

■ R

Race conditions, 47
Rainbow tables, 18–19

■ INDEX

■ **S**

Safe defaults, 41–47
Salting, 18–21, 23–26
Sanitizing input, 1–8
Sanitizing output, 3, 7–8
Session hijacking, 9–10
SHA1, 21, 30
Sidejacking, 9
SQL injection, 1–4
SSL, 9–16

SSL certificate, 12–15
Stored procedures, 3, 26, 43

■ **T, U**

Typecasting, 5–6

■ **V, W, X, Y, Z**

Validating redirects, 36–37
Validation, 4, 12, 22–23, 36, 40, 41, 46
Virtual hosts, 10–11, 15