

Curso de curta duração ministrado por:

**Marcell Guilherme**

Contato: [github.com/mazuh](https://github.com/mazuh)



# **BÁSICO DE HACKING PARA PROTEGER SISTEMAS EM PHP**

# Objetivos

- Conhecer a cultura e ética hacker;
- Compreender os objetivos dos hackers;
- Examinar as fragilidades das aplicações feitas para navegadores;
- Aprender hacking básico para esse tipo de sistema;
- Produzir soluções simples às brechas encontradas.

# Terminologia: HACK

- O que é hack?



# Terminologia: HACK

- O que é hack?
- Em tradução-livre: “cortar [grosseiramente]”;



# Terminologia: HACK

- O que é hack?
- Em tradução-livre: “cortar [grosseiramente]”;
- **Uso popular: ato de atacar/usar de forma maliciosa um software;**



# Terminologia: HACK

- **O que é hack?**
- Em tradução-livre: “cortar [grosseiramente]”;
- Uso popular: ato de atacar/usar de forma maliciosa um software;
- **Definição adequada: ato de explorar os limites de algo (normalmente hardware e/ou software) através da experimentação, construção, criação, modificação e aprendizado.**

# Variações por estrangeirismo

- “Fazer o *hack*”
  - (substantivo, produto);
- “Fazer *hacking*”
  - (substantivo, processo);
- “*Hackear*”
  - (verbo *to hack* aportuguesado);
- “*Hacker*”
  - (substantivo/adjetivo, quem pratica hacking).



# O que é ser um hacker

- **Dedicar-se intensamente a conhecer, criar e modificar dispositivos, programas e redes de computadores;**
- **Hábil na programação;**
- **Nem sempre disciplinado.**



# De que lado você está?



- Hackers éticos se intitulam de *white hats*;
- Crackers se rotulam de *black hats*;
- Grey hats crackeiam, mas sem danos.



H3LLS1NG @Sh4dowNetwork · 11 de out

vcs deviam ter nascido deficientes pra n digitar tanta bosta



20



22



H3LLS1NG @Sh4dowNetwork · 10 de out

Raqueamento das 4i20

nacklada dos  
anénomos



8



H3LLS1NG @Sh4dowNetwork · 8 de out

Pero que si pero que no

# SQL Injection #1



StefanYohansson opened this issue 28 days ago · 3 comments



StefanYohansson commented 28 days ago

O sistema ainda é muito passível de SQL Injection.  
Sugiro algo como:

- Usar PDO ao invés de mysqli puro. A classe de "Connection" pode ser um **singleton** para o PDO.
- Usar PDO::bindValue ou PDO::bindParam ao invés de concatenar strings.

ex:

Eleitor.php:95

```
$sql = "update usuario";  
$sql .= " set chapa_votada=$this->chapa_votada, momento_voto=current_timestamp()";  
$sql .= " where id=$this->id";
```

deve ser algo como:

```
$statement = "update usuario set chapa_votada=:chapa_votada, momento_voto = current_timestamp() whe  
  
$statement->bindValue(':chapa_votada', $this->chapa_votada, PDO::PARAM_STR);  
$statement->bindValue(':id', $this->id, PDO::PARAM_INT);
```

# Outras categorias de hacker



- Newbie, noob, nb;
- Lammer, lamer, script kiddie;
- Phreaker;
- Hacktivist.

# Ética hacker

- Livro “Hackers: Heroes of the Computer Revolution” (LEVY, Steven. 1984);
- Richard Stallman, o “último verdadeiro hacker”;
- Massachusetts Institute of Technology (MIT).



# Princípios da ética hacker

- O acesso a computadores (e qualquer coisa que possa te ensinar como o mundo funciona) deve ser ilimitado e total:
  - Laboratórios com acesso limitado são depressivos para hackers;
- Toda informação deve ser livre;
- Desacredite a autoridade, promova a descentralização do poder;

# Princípios da ética hacker

- Hackers devem ser julgados pelo seu hacking (e por nenhuma forma de preconceito de nível acadêmico, gênero, raça, cor, religião ou idade);
- Hacking também é arte, singular;
- Computadores podem mudar sua vida para melhor.





# Hacktivista Aaron Swartz



- Aaron era hacktivista e palestrava desde a pré-adolescência;
- Reddit, RSS, Creative Commons, W3C, PACER, Tor;
- Ajudou a impedir as leis SOPA e PIPA.



# Aaron Swartz: sua morte

- Foi acusado exemplarmente pelo governo dos EUA após um incidente com a JSTOR;
- Aaron Swartz, depressivo, suicidou-se em janeiro de 2013 em seu apartamento;
- As acusações foram retiradas após isso;
- “Ou você morre herói, ou vive bastante para ver você mesmo virando vilão.”  
(Batman, The Dark Knight)

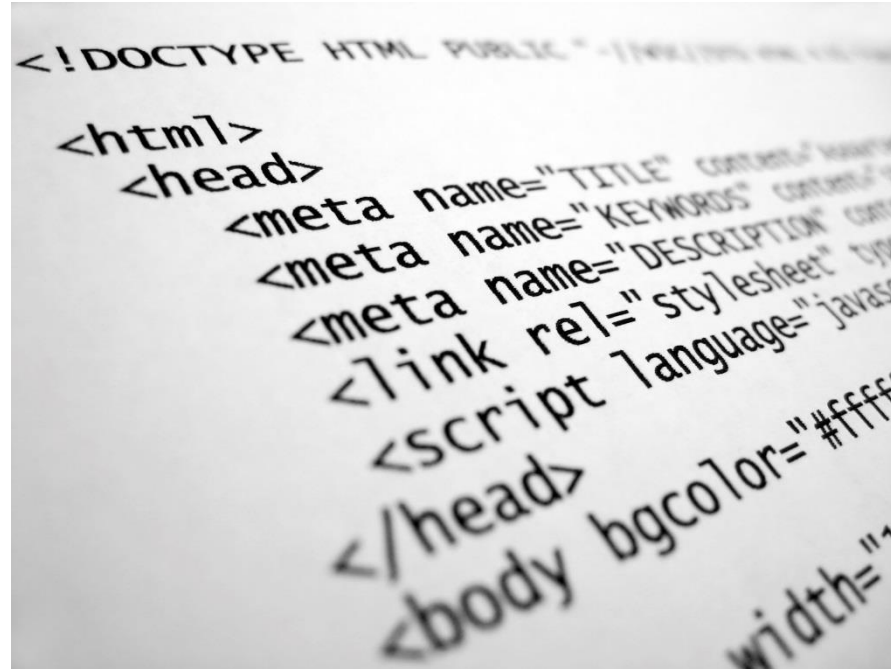
# Preparação para as práticas

- **Baixar e instalar o ambiente de testes:**
  - Baixar zip do repo “Minicurso-HackingPHP” em: <<https://github.com/Mazuh/>>;
  - Dezipar para dentro da ‘C:\xampp\htdocs’;
- **Pesquisar no menu iniciar pelo “XAMPP Control Panel” e o executar:**
  - Ligar os serviços Apache e MySQL;
- **Abrir o site The Hackbook no navegador:**
  - ‘localhost/Minicurso-HackingPHP-master/src’

# The Hackbook

- Feito para ser explorado neste minicurso.
- Sistema de simples de múltiplos blogs;
- Codificado com o que é normalmente aprendido no curso Técnico.

# Roteiro das práticas I



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head>
    <meta name="TITLE" content="...">
    <meta name="KEYWORDS" content="...">
    <meta name="DESCRIPTION" content="...">
    <link rel="stylesheet" type="text/css" href="...">
    <script language="javascript" src="...">
  </head>
  <body bgcolor="#ffffff" width="100%">
```

- Extraindo recursos do HTML;
- Utilizando HTML injection.

# Hacker Samy Kamkar

- Incidente “Samy is my hero”:
  - `<http://samy.pl/popular/>`;
- Punido exemplarmente por 3 anos;
- Hoje não mais gray hat, mas sim white hat;
- Cross-site scripting (XSS).



# Roteiro das práticas II



- Ataques com script injection;
- Proteção contra script injection;
- Ataques com SQL injection;
- Proteção contra SQL injection.

# Roteiro das práticas III

- Ataques com PHP injection via upload;
- Proteção contra upload de PHP;
- Ataques com PHP injection via include;
- Proteção contra include de script estranho.



# Uso de frameworks

- **Prós:**
  - Ganho de produtividade;
  - Ganho de segurança;
  - Fácil manutenção;
  - De programadores para programadores.
- **Contras:**
  - Perca insignificante de autonomia.
- **Exemplos: CakePHP, Zend, Django etc.**



# Cuidados extras contra ataques

- **Infraestrutura:**
  - Permissões de arquivos no servidor,
  - Configurações do servidor,
  - Estrutura física do servidor protegida;
- **Rede onde os dados trafegam;**
- **Criptografia de senhas:**
  - Nunca descriptografar;
- **Ter bom suporte.**



# Roteiro das práticas IV

- Software livre;
- Colaborando via GitHub:
  - Reportando issues,
  - Resolvendo as issues.



# Referências bibliográficas:

- <https://www.wesecure.nl/upload/documents/tinymce/Hacking-for-Dummies-e-book.pdf>
- [https://pt.wikipedia.org/wiki/Hacker\\_\(hobbysta\)](https://pt.wikipedia.org/wiki/Hacker_(hobbysta))
- <https://pt.wikipedia.org/wiki/Hack>
- <http://pensador.uol.com.br/frase/MTA2NjQ1MA/>
- <http://www.soportugues.com.br/secoes/estrangeirismos/>
- <http://www.prolificwebsolutions.com/black-hat-vs-white-hat-whats-the-difference/>
- <https://mitpress.mit.edu/books/new-hackers-dictionary>
- [http://www.temarium.com/wordpress/wp-content/documentos/Levy\\_S-Hackers-Heroes-Computer-Revolution.pdf](http://www.temarium.com/wordpress/wp-content/documentos/Levy_S-Hackers-Heroes-Computer-Revolution.pdf)
- <http://blog.corujadeti.com.br/o-que-e-hacktivismo-e-como-ele-funciona/>
- <http://oglobo.globo.com/sociedade/tecnologia/aaron-swartz-hacker-fundador-do-reddit-comete-suicidio-aos-26-anos-7278368>
- <https://tecnoblog.net/122114/morre-aaron-swartz/>
- <http://www.youtube.com/watch?v=2uj1EeiUK5U>
- <http://www.redesegura.com.br/2012/01/saiba-mais-sobre-o-cross-site-scripting-xss/>
- <http://samy.pl/popular/>
- <http://www.rlsystem.com.br/curso/curso-seguranca-php-online>
- <http://www.techhive.com/article/139812/article.html>
- <http://fusion.net/story/180919/samy-kamkar-is-a-white-hat-hacking-hero/>
- <http://symfony.com/pt-br/why-use-a-framework>

# Fontes de imagens:

- <http://securityaffairs.co/wordpress/wp-content/themes/titan/images/sidebar/sidebar.jpg>
- <http://setdecinema.com.br/wp-content/uploads/2015/07/g31.jpg>
- <http://i.mlcdn.com.br/1500x1500/rack-para-tv-55-dj-havana-1-portadj-moveis-121793581.jpg>
- [http://olhardigital.uol.com.br/uploads/acervo\\_imagens/2013/10/20131002214057\\_660\\_420.jpg](http://olhardigital.uol.com.br/uploads/acervo_imagens/2013/10/20131002214057_660_420.jpg)
- <http://bp.i.uol.com.br/arquivo/legacy/camera/pasquale01.jpg>
- <http://blog.e-max.it/wp-content/uploads/2014/05/Spy-vs-Spy.jpg>
- <http://3.bp.blogspot.com/-xmhuHdC-v0/TaM0sIUy8aI/AAAAAAAAAI4/VvgyNOL0MXo/s1600/lammer.bmp>
- [https://upload.wikimedia.org/wikipedia/commons/thumb/c/c2/Richard\\_Stallman\\_at\\_Marlboro\\_College.jpg/800px-Richard\\_Stallman\\_at\\_Marlboro\\_College.jpg](https://upload.wikimedia.org/wikipedia/commons/thumb/c/c2/Richard_Stallman_at_Marlboro_College.jpg/800px-Richard_Stallman_at_Marlboro_College.jpg)
- <https://www.unocero.com/wp-content/uploads/2013/01/Gobierno-retira-cargos-contr-Aaron-Swartz.jpg>
- <https://avatars1.githubusercontent.com/u/411832?v=3&s=460>
- <http://www.hacoder.com/wp-content/uploads/2015/08/sql-injection-logo.jpg>
- [http://static.comicvine.com/uploads/scale\\_super/11114/111144184/4687062-7044983538-BfK6q.jpg](http://static.comicvine.com/uploads/scale_super/11114/111144184/4687062-7044983538-BfK6q.jpg)
- [http://www1.netsecuritysolutionsltda.com/wp-content/uploads/2014/02/soporte-tecnico-pc-abonos-mantenimiento-redes-y-servidores-5522-MLA4466350763\\_062013-F1.png](http://www1.netsecuritysolutionsltda.com/wp-content/uploads/2014/02/soporte-tecnico-pc-abonos-mantenimiento-redes-y-servidores-5522-MLA4466350763_062013-F1.png)
- [https://github.com/images/modules/dashboard/bootcamp/octocat\\_collabocats.png](https://github.com/images/modules/dashboard/bootcamp/octocat_collabocats.png)
- <http://emmanuelatsu.com/wp-content/uploads/2015/06/matrix-neo-hacker.jpg>