

# Obsah

<b>Předmluva</b>	<b>7</b>
<b>Úvod</b>	<b>9</b>
<hr/>	
<b>Pravidla</b>	<b>10</b>
<b>Příklady</b>	<b>11</b>
<b>Kapitoly</b>	<b>12</b>
<b>Co v této knize nenaleznete?</b>	<b>13</b>
<b>Poznámka autora</b>	<b>13</b>
<b>Odezva</b>	<b>14</b>
<b>KAPITOLA 1</b>	<b>15</b>
<b>Počátky</b>	<b>15</b>
<hr/>	
<b>HTTP</b>	<b>15</b>
Požadavky a odpovědi	16
Hlavička Referer	19
Ukládání do mezipaměti (cache)	20
Soubory cookie	21
<b>Relace</b>	<b>22</b>
Krádež relace	23
<b>HTTPS</b>	<b>26</b>
<b>Závěr</b>	<b>29</b>
<b>Chcete se dozvědět více?</b>	<b>29</b>
<b>KAPITOLA 2</b>	<b>31</b>
<b>Přenos dat do subsystémů</b>	<b>31</b>
<hr/>	
<b>SQL Injection</b>	<b>32</b>
Příklady, příklady a zase příklady	32
Využívání chybových hlášení k získávání informací	39
Jak se vyhnout útoku typu SQL Injection	41
<b>Shell Command Injection</b>	<b>46</b>

## Obsah

Příklady	47
Ochrana před útokem Shell Command Injection	49
<b>Povídání k programům napsaným v jazycích C/C++</b>	<b>54</b>
Příklad	54
<b>Proradná funkce Eval</b>	<b>56</b>
<b>Řešení problémů s metaznaký</b>	<b>56</b>
Interpretace metaznaků na více úrovních	57
Architektura	58
Strategie defense in depth	
– současné zabezpečení prostřednictvím několika mechanismů	59
<b>Shrnutí</b>	<b>60</b>
<b>KAPITOLA 3</b>	<b>63</b>
<b>Vstup uživatele</b>	<b>63</b>
<b>Co se vlastně skrývá za slovem vstup?</b>	<b>63</b>
Neviditelná bezpečnostní bariéra	68
Zvláštnosti programovacích jazyků: zcela neočekávaný vstup dat	70
<b>Kontrola vstupu</b>	<b>72</b>
Bílá listina oproti černé listině	76
<b>Ošetření neplatného vstupu</b>	<b>78</b>
Zaznamenávání událostí do protokolu	80
<b>Rizika kontroly vstupu na straně klienta</b>	<b>83</b>
<b>Problémy s přístupovými oprávněními</b>	<b>86</b>
Nepřímý přístup k datům	87
Když se klientovi předává příliš mnoho dat	89
Když chybí kontrola oprávnění	93
Ověření přístupu utajením	94
<b>Ochrana vstupu vytvořeného serverem</b>	<b>95</b>
<b>Shrnutí</b>	<b>98</b>
<b>KAPITOLA 4</b>	<b>99</b>
<b>Ošetření výstupu: útok Cross-site Scripting</b>	<b>99</b>
<b>Příklady</b>	<b>100</b>
Krádež relace	101
Úprava textu	104
Útok Cross-site Scripting vedený metodou sociálního inženýrství	105
Krádež hesel	108
Příliš málo znaků pro skripty?	110
<b>Problém</b>	<b>111</b>
<b>Řešení</b>	<b>112</b>
Kódování HTML	113
Výběrové filtrování značek	114
Návrh programu	119
<b>Znakové sady používané v prohlížečích</b>	<b>120</b>

<b>Shrnutí</b>	<b>121</b>
<b>Chcete se dozvědět více?</b>	<b>121</b>
<b>KAPITOLA 5</b>	<b>123</b>
<b>Trojské koně</b>	<b>123</b>
<b>Příklady</b>	<b>123</b>
<b>Problém</b>	<b>128</b>
<b>Řešení</b>	<b>128</b>
<b>Shrnutí</b>	<b>130</b>
<b>KAPITOLA 6</b>	<b>131</b>
<b>Hesla a další tajné informace</b>	<b>131</b>
<b>Šifrování</b>	<b>131</b>
Symetrické šifrování	132
Asymetrické šifrování	133
Hašovací funkce	134
Digitální podpisy	135
Certifikáty	136
<b>Ověřování uživatelů pomocí hesel</b>	<b>137</b>
O nešifrovaných heslech	137
Zapomenutá hesla	139
Prolomení hašů hesel	140
Pamatujete si na mě?	143
<b>Utajené identifikátory</b>	<b>145</b>
<b>Únik tajných informací</b>	<b>147</b>
Únik informací v požadavcích přenášených metodou GET	148
Chybějící šifrování	150
<b>Dostupnost kódu na straně serveru</b>	<b>150</b>
Problematické názvy souborů	151
Chyby v systémových aplikacích	152
<b>Shrnutí</b>	<b>153</b>
<b>Chcete se dozvědět více?</b>	<b>154</b>
<b>KAPITOLA 7</b>	<b>155</b>
<b>Nepřátelé bezpečného kódu</b>	<b>155</b>
<b>Nedostatek informací</b>	<b>155</b>
<b>Nepořádnost</b>	<b>157</b>
<b>Uzávěrka</b>	<b>163</b>
<b>Prodejci</b>	<b>164</b>
<b>Poznámky na závěr</b>	<b>165</b>
<b>Chcete se dozvědět více?</b>	<b>165</b>

KAPITOLA 8	167
<b>Přehled pravidel pro vytváření bezpečného kódu</b>	<b>167</b>
<hr/>	
PŘÍLOHA A	175
<b>Chyby ve webovém serveru</b>	<b>175</b>
<hr/>	
PŘÍLOHA B	179
<b>Zachytávání paketů (Packet Sniffing)</b>	<b>179</b>
<hr/>	
Naučte se základy protokolu TCP/IP během čtyř minut	179
Zachytávání paketů	181
Útok man in the middle	182
MITM ve spojení s protokolem HTTPS	183
Shrnutí	183
Chcete se dozvědět více?	184
<hr/>	
PŘÍLOHA C	185
<b>Odesílání e-mailů ve formátu HTML s falešnou adresou odesílatele</b>	<b>185</b>
<hr/>	
PŘÍLOHA D	187
<b>Další informace</b>	<b>187</b>
<hr/>	
Diskusní fóra	187
OWASP	188
<b>Odkazy</b>	<b>191</b>
<b>Zkratky</b>	<b>199</b>
<hr/>	