

Blog Simple.



Web Application Penetration Testing Course

In Security Tags bug bounty, hack, pentest, security August 11, 2018 449 Views  Aishee

Web Application Penetration Testing



Phase 1 – History

1. History of Internet – <https://www.youtube.com/watch?v=9hIQjrMHTv4>

Phase 2 – Web and Server Technology

1. Basic concepts of web applications, how they work and the HTTP protocol – <https://www.youtube.com/watch?v=RsQ1tFLwldY&t=7s>
2. HTML basics part 1 – https://www.youtube.com/watch?v=p6fRBGI_BY0
3. HTML basics part 2 – <https://www.youtube.com/watch?v=Zs6lzuBVK2w>

4. Difference between static and dynamic website – <https://www.youtube.com/watch?v=hlq6q6OFoxQ>
5. HTTP protocol Understanding – <https://www.youtube.com/watch?v=JFZMyhRTVt0>
6. Parts of HTTP Request – <https://www.youtube.com/watch?v=pHFWGN-upGM>
7. Parts of HTTP Response – <https://www.youtube.com/watch?v=c9sMNc2PrMU>
8. Various HTTP Methods – <https://www.youtube.com/watch?v=PO7D20HsFsY>
9. Understanding URLs – https://www.youtube.com/watch?v=5Jr-_Za5yQM
10. Intro to REST – <https://www.youtube.com/watch?v=YCcAE2SCQ6k>
11. HTTP Request & Response Headers – <https://www.youtube.com/watch?v=vAuZwirKjWs>
12. What is a cookie – <https://www.youtube.com/watch?v=I01XMRo2ESg>
13. HTTP Status codes – <https://www.youtube.com/watch?v=VLH3FMQ5BIQ>
14. HTTP Proxy – <https://www.youtube.com/watch?v=qU0PVSJCKcs>
15. Authentication with HTTP – <https://www.youtube.com/watch?v=GxiFXUfKo1M>
16. HTTP basic and digest authentication – <https://www.youtube.com/watch?v=GOmhCbDhMzk>
17. What is “Server-Side” – <https://www.youtube.com/watch?v=JnCLmLO9LhA>
18. Server and client side with example – <https://www.youtube.com/watch?v=DcBB2Fp8WNI>
19. What is a session – <https://www.youtube.com/watch?v=WV4DJ6b0jhq&t=202s>
20. Introduction to UTF-8 and Unicode – https://www.youtube.com/watch?v=sqPTR_v4qFA
21. URL encoding – <https://www.youtube.com/watch?v=Z3udiqgW1VA>
22. HTML encoding – <https://www.youtube.com/watch?v=liAfCLWpgII&t=109s>
23. Base64 encoding – <https://www.youtube.com/watch?v=8qkxeZmKmOY>
24. Hex encoding & ASCII – <https://www.youtube.com/watch?v=WW2SaCMnHdU>

Phase 3 – Setting up the lab with BurpSuite and bWAPP

MANISH AGRAWAL

1. Setup lab with bWAPP – https://www.youtube.com/watch?v=dwtUn3giwTk&index=1&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
2. Set up Burp Suite – https://www.youtube.com/watch?v=hQsT4rSa_v0&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=2
3. Configure Firefox and add certificate – https://www.youtube.com/watch?v=hfsdJ69GSV4&index=3&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
4. Mapping and scoping website – https://www.youtube.com/watch?v=H-_iVteMDRo&index=4&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
5. Spidering – https://www.youtube.com/watch?v=97uMUQGie14&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=5
6. Active and passive scanning – https://www.youtube.com/watch?v=1Mjom6AcFyU&index=6&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
7. Scanner options and demo – https://www.youtube.com/watch?v=gANi4Kt7-ek&index=7&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
8. Introduction to password security – https://www.youtube.com/watch?v=FwcUhcLO9iM&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=8
9. Intruder – https://www.youtube.com/watch?v=wtMg9oEMTa8&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=9
10. Intruder attack types – https://www.youtube.com/watch?v=N5ndYPwddkQ&index=10&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
11. Payload settings – https://www.youtube.com/watch?v=5GpdlbtL-1Q&index=11&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV

12. Intruder settings – https://www.youtube.com/watch?v=B_Mu7jmOYnU&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=12

ÆTHER SECURITY LAB

1. No.1 Penetration testing tool – <https://www.youtube.com/watch?v=AVzC7ETqpDo&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=1>
2. Environment Setup – <https://www.youtube.com/watch?v=yqnUOdr0eVk&index=2&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA>
3. General concept – https://www.youtube.com/watch?v=udl4oqr_ylM&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=3
4. Proxy module – <https://www.youtube.com/watch?v=PDTwYFkjQBE&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=4>
5. Repeater module – https://www.youtube.com/watch?v=9Zh_7s5csCc&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=5
6. Target and spider module – <https://www.youtube.com/watch?v=dCKPZUSOl8&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=6>
7. Sequencer and scanner module – <https://www.youtube.com/watch?v=G-v581pXerE&list=PLq9n8iqQJFDrwFe9AEDBIR1uSHEN7egQA&index=7>

Phase 4 – Mapping the application and attack surface

Spidering – https://www.youtube.com/watch?v=97uMUQGie14&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=5

1. Mapping application using robots.txt – <https://www.youtube.com/watch?v=akuzgZ75zrk>

2. Discover hidden contents using dirbuster – <https://www.youtube.com/watch?v=--nu9Jq07gA>
3. Dirbuster in detail – <https://www.youtube.com/watch?v=2tOQC68hAcQ>
4. Discover hidden directories and files with intruder – <https://www.youtube.com/watch?v=4Fz9mJeMNkI>
5. Identify application entry points – <https://www.youtube.com/watch?v=IgJWPZ2OKO8&t=34s>
6. Identify application entry points –
[https://www.owasp.org/index.php/Identify_application_entry_points_\(OTG-INFO-006\)](https://www.owasp.org/index.php/Identify_application_entry_points_(OTG-INFO-006))
7. Identify client and server technology – https://www.youtube.com/watch?v=B8jN_iWjtyM
8. Identify server technology using banner grabbing (telnet) –
<https://www.youtube.com/watch?v=O67M-U2UOAg>
9. Identify server technology using httprecon – <https://www.youtube.com/watch?v=xBBHtS-dwsM>

Phase 5 – Understanding and exploiting OWASP top 10 vulnerabilities

1. A closer look at all owasp top 10 vulnerabilities – https://www.youtube.com/watch?v=avFR_Af0KGk

IBM

1. Injection – <https://www.youtube.com/watch?v=02mLrFVzIYU&index=1&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>
2. Broken authentication and session management – <https://www.youtube.com/watch?v=iX49fqZ8HGA&index=2&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>

3. Cross-site scripting – <https://www.youtube.com/watch?v=x6I5fCupLLU&index=3&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>
4. Insecure direct object reference – <https://www.youtube.com/watch?v=-iCyp9Qz3CI&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=4>
5. Security misconfiguration – <https://www.youtube.com/watch?v=cIplXL8idyo&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=5>
6. Sensitive data exposure – <https://www.youtube.com/watch?v=rYlzTQlF8Ws&index=6&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>
7. Missing functional level access controls – https://www.youtube.com/watch?v=VMv_gyCNGpk&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=7
8. Cross-site request forgery – https://www.youtube.com/watch?v=_xSFm3KGxh0&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=8
9. Using components with known vulnerabilities – <https://www.youtube.com/watch?v=bhJmVBJ-F-4&index=9&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>
10. Unvalidated redirects and forwards – <https://www.youtube.com/watch?v=L6bYKiLtSL8&index=10&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d>

F5 CENTRAL

Injection – https://www.youtube.com/watch?v=rWHvp7rUka8&index=1&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

1. Broken authentication and session management – https://www.youtube.com/watch?v=mruO75ONWy8&index=2&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

2. Insecure deserialisation – https://www.youtube.com/watch?v=nkTBwbnfesQ&index=8&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
3. Sensitive data exposure – https://www.youtube.com/watch?v=2RKbacrkUBU&index=3&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
4. Broken access control – https://www.youtube.com/watch?v=P38at6Tp8Ms&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=5
5. Insufficient logging and monitoring – https://www.youtube.com/watch?v=IFF3tkUOF5E&index=10&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
6. XML external entities – https://www.youtube.com/watch?v=g2ey7ry8_CQ&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=4
7. Using components with known vulnerabilities – https://www.youtube.com/watch?v=IGsNYVDKRV0&index=9&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
8. Cross-site scripting – https://www.youtube.com/watch?v=luzU4y-UjLw&index=7&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
9. Security misconfiguration – https://www.youtube.com/watch?v=JuGSUMtKTPU&index=6&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

LUKE BRINER

1. Injection explained – https://www.youtube.com/watch?v=1qMggPJpRXM&index=1&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X
2. Broken authentication and session management – https://www.youtube.com/watch?v=fKnG15BL4AY&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=2
3. Cross-site scripting – https://www.youtube.com/watch?v=ksM-xXeDUNs&index=3&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X

4. Insecure direct object reference – https://www.youtube.com/watch?v=ZodA76-CB10&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=4
5. Security misconfiguration – https://www.youtube.com/watch?v=DfFPHKPCofY&index=5&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X
6. Sensitive data exposure – https://www.youtube.com/watch?v=Z7hafbGDVEE&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=6
7. Missing functional level access control – https://www.youtube.com/watch?v=RGN3w831Elo&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=7
8. Cross-site request forgery – https://www.youtube.com/watch?v=XRW_US5BCxk&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=8
9. Components with known vulnerabilities – https://www.youtube.com/watch?v=pbvDW9pJdng&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=9
10. Unvalidated redirects and forwards – https://www.youtube.com/watch?v=bHTglpgC5Qg&list=PLpNYIUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=10

Phase 6 – Bypassing client-side controls

1. What is hidden forms in HTML – <https://www.youtube.com/watch?v=orUoGsgaYAE>
2. Bypassing hidden form fields using tamper data – <https://www.youtube.com/watch?v=NXkGX2sPw7I>
3. Bypassing hidden form fields using Burp Suite (Purchase application) – <https://www.youtube.com/watch?v=xahvJyUFTfM>
4. Changing price on eCommerce website using parameter tampering – <https://www.youtube.com/watch?v=A-ccNpP06Zg>

5. Understanding cookie in detail – https://www.youtube.com/watch?v=_P7KN8T1boc&list=PLWPirh4EWFpESKWJmrgQwmsnTrL_K93Wi&index=18
6. Cookie tampering with tamper data- <https://www.youtube.com/watch?v=NgKXm0lBecc>
7. Cookie tamper part 2 – https://www.youtube.com/watch?v=dTCt_I2DWgo
8. Understanding referer header in depth using Cisco product –
<https://www.youtube.com/watch?v=GkQnBa3C7WI&t=35s>
9. Introduction to ASP.NET viewstate – <https://www.youtube.com/watch?v=L3p6Uw6SSXs>
10. ASP.NET viewstate in depth – https://www.youtube.com/watch?v=Fn_08JLsrmY
11. Analyse sensitive data in ASP.NET viewstate – <https://msdn.microsoft.com/en-us/library/ms972427.aspx?f=255&MSPPError=-2147217396>

Phase 7 – Attacking authentication/login

1. Attacking login panel with bad password – Guess username password for the website and try different combinations
2. Brute-force login panel – https://www.youtube.com/watch?v=25cazx5D_vw
3. Username enumeration – <https://www.youtube.com/watch?v=WCO7LnSlSkE>
4. Username enumeration with bruteforce password attack –
<https://www.youtube.com/watch?v=zf3-pYJU1c4>
5. Authentication over insecure HTTP protocol – <https://www.youtube.com/watch?v=ueSG7TUqoxk>
6. Authentication over insecure HTTP protocol – https://www.youtube.com/watch?v=_WQe36pZ3mA
7. Forgot password vulnerability – case 1 – <https://www.youtube.com/watch?v=FEUIdWWnZwU>

8. Forgot password vulnerability – case 2 – <https://www.youtube.com/watch?v=j7-8YyYdWL4>
9. Login page autocomplete feature enabled – <https://www.youtube.com/watch?v=XNjUfwDmHGc&t=33s>
10. Testing for weak password policy –
[https://www.owasp.org/index.php/Testing_for_Weak_password_policy_\(OTG-AUTHN-007\)](https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007))
11. Insecure distribution of credentials – When you register in any website or you request for a password reset using forgot password feature, if the website sends your username and password over the email in cleartext without sending the password reset link, then it is a vulnerability.

Phase 8 – Phase 8 – Attacking access controls (IDOR, Priv esc, hidden files and directories)

Completely unprotected functionalities

1. Finding admin panel – <https://www.youtube.com/watch?v=r1k2lgvK3s0>
2. Finding admin panel and hidden files and directories – <https://www.youtube.com/watch?v=ZOVAPbATy1A>
3. Finding hidden webpages with dirbusater – <https://www.youtube.com/watch?v=-nu9Jq07gA&t=5s>

Insecure direct object reference

1. IDOR case 1 – <https://www.youtube.com/watch?v=gci4R9Vkulc>
2. IDOR case 2 – <https://www.youtube.com/watch?v=4DTULwuLFS0>
3. IDOR case 3 (zomato) – <https://www.youtube.com/watch?v=tCJBLG5Mayo>

Privilege escalation

1. What is privilege escalation – <https://www.youtube.com/watch?v=80RzLSrczmc>
2. Privilege escalation – Hackme bank – case 1 – https://www.youtube.com/watch?v=g3lv__87cWM
3. Privilege escalation – case 2 – https://www.youtube.com/watch?v=-i4O_hjc87Y

Phase 9 – Attacking data stores (Various types of injection attacks – SQL|MySQL|NoSQL|Oracle, etc.)

Bypassing login panel

1. Basics of MySQL – <https://www.youtube.com/watch?v=yPu6qV5byu4>
2. Bypassing login panel -case 1 – <https://www.youtube.com/watch?v=TSqXkkOt6oM>
3. Bypass login panel – case 2 – https://www.youtube.com/watch?v=J6v_W-LFK1c

SQL injection

1. Part 1 – Install SQLi lab – https://www.youtube.com/watch?v=NJ9AA1_t1lc&index=23&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
2. Part 2 – SQL lab series – https://www.youtube.com/watch?v=TA2h_kUqfhU&index=22&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
3. Part 3 – SQL lab series – <https://www.youtube.com/watch?v=N0zAChmZIZU&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=21>
4. Part 4 – SQL lab series – <https://www.youtube.com/watch?v=6pVxm5mWBVU&index=20&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>

5. Part 5 – SQL lab series – <https://www.youtube.com/watch?v=0tyerVP9R98&index=19&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
6. Part 6 – Double query injection – <https://www.youtube.com/watch?v=zaRlcPbfX4M&index=18&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
7. Part 7 – Double query injection cont.. – <https://www.youtube.com/watch?v=9utdAPxmvaI&index=17&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
8. Part 8 – Blind injection boolean based – <https://www.youtube.com/watch?v=u7Z7AIR6cMI&index=16&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
9. Part 9 – Blind injection time based – https://www.youtube.com/watch?v=gzU1YBu_838&index=15&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
10. Part 10 – Dumping DB using outfile – <https://www.youtube.com/watch?v=ADW844OA6io&index=14&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
11. Part 11 – Post parameter injection error based – <https://www.youtube.com/watch?v=6sQ23tqiTXY&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=13>
12. Part 12 – POST parameter injection double query based –
<https://www.youtube.com/watch?v=tjFXWQY4LuA&index=12&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
13. Part 13 – POST parameter injection blind boolean and time based –
<https://www.youtube.com/watch?v=411G-4nH5jE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=10>
14. Part 14 – Post parameter injection in UPDATE query – <https://www.youtube.com/watch?v=2FgLcPuU7Vw&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=11>
15. Part 15 – Injection in insert query – <https://www.youtube.com/watch?v=ZJiPsWxXYZs&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=9>

16. Part 16 – Cookie based injection – <https://www.youtube.com/watch?v=A3vVqfP8pA&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=8>
17. Part 17 – Second order injection – <https://www.youtube.com/watch?v=e9pbC5BxiAE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=7>
18. Part 18 – Bypassing blacklist filters – 1 – <https://www.youtube.com/watch?v=5P-knuYoDdw&index=6&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro>
19. Part 19 – Bypassing blacklist filters – 2 – <https://www.youtube.com/watch?v=45BjuQFt55Y&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=5>
20. Part 20 – Bypassing blacklist filters – 3 – https://www.youtube.com/watch?v=c-Pjb_zLpH0&index=4&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
21. Part 21 – Bypassing WAF – <https://www.youtube.com/watch?v=uRDuCXFpHXc&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=2>
22. Part 22 – Bypassing WAF – Impedance mismatch – https://www.youtube.com/watch?v=ygVUebdv_Ws&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=3
23. Part 23 – Bypassing addslashes – charset mismatch – <https://www.youtube.com/watch?v=du-jkS6-sbo&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=1>

NoSQL injection

1. Abusing NoSQL databases – <https://www.youtube.com/watch?v=lcO1BTNh8r8>
2. Making cry – attacking NoSQL for pentesters – <https://www.youtube.com/watch?v=NgsesuLpyOg>

Xpath injection

1. Detailed introduction – https://www.youtube.com/watch?v=2_UyM6Ea0Yk&t=3102s

2. Practical 1 – bWAPP – <https://www.youtube.com/watch?v=6tV8EuaHI9M>
3. Practical 2 – Mutillidae – <https://www.youtube.com/watch?v=fV0qsgcScI4>
4. Practical 3 – webgoat – <https://www.youtube.com/watch?v=5ZDSPVp1TpM>

LDAP injection

1. Introduction and practical 1 – <https://www.youtube.com/watch?v=-TXFlg7S9ks>
2. Practical 2 – https://www.youtube.com/watch?v=wtahzm_R8e4

Phase 10 – Attacking back-end components (OS command injection, XML interpreters, mail services, etc.)

OS command injection

1. OS command injection in bWAPP – <https://www.youtube.com/watch?v=qLlkGJrMY9k>



Aishee



Previous Post:

For-1: Malware Traffic Analysis Example

Next Post:

Mobile app traffic analysis — For Fun



Related Posts:



HOLD THE SHIT — PHP Backdoor for fun

Pentest tutorial — Methods to do

Machine learning for Web Application Firewall (WAF)

Leave a reply:

Your email address will not be published.

Post Comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

About Me



My name is Nguyen Anh Tai. I am an independent security researcher, bug hunter and leader a security team. Security Researcher at CMC INFOSEC. I developed the every system for fun :D. My aim is to become an expert in security and xxx!

Tags



pentest tool

Privilege

ps

ps command

security

subdomain

token

unix

unprivileged

URL malicious

waf

webstorage


webview

Tweets

 **Aishee** RT @cyb3rops: Oh my gosh, this is the noisiest RAT that I've ever seen. Drops .js, .ps1, .bat, .exe, .exe as .jpg, ssh service, TeamViewer,...


about 18 days ago



 **Aishee** RT @axi0mX: EPIC JAILBREAK: Introducing checkm8 (read "checkmate"), a permanent unpatchable bootrom exploit for hundreds of millions of iOS...

about 19 days ago



 **Aishee** 7% through "The Simulation Hypothesis: An MIT..." by Rizwan Virk. Try the book for free: <https://t.co/iaDzmZri9Y> <https://t.co/oq5dvJoUyr>

about 4 months ago



Make by Aishee - A blog simple for social